ISSN: 1646-9895

risti

Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

A b r i l 2 2 • A p r i l 2 2



©RISTI 2022 http://www.risti.xyz

Nº E49

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Edição / Edition
N.º E49, 04/2022

ISSN: 1646-9895

Indexação / Indexing
Academic Journals Database, CiteFactor, Dialnet, DOAJ, DOI, EBSCO, GALE, IndexCopernicus, Index of Information Systems Journals, Latindex, ProQuest, QUALIS, SCImago, SCOPUS, SIS, Ulrich's.

Publicação / Publication
RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação
Rua Quinta do Roseiral 76, 4435-209 Rio Tinto, Portugal
Web: http://www.risti.xyz

Director
Álvaro Rocha, University of Lisbon, PT

Coordenadores da Edição / Issue Coordinators
Carlos Hernán Fajardo-Toro, Escuela Superior de
Administración Pública - ESAP, CO
José María Riola, Escuela Naval de Cadetes "Almirante Padilla" – ENAP, CO

Conselho Editorial / Editorial Board
A. Augusto Sousa, FEUP, University of Porto, PT
Abel Méndez Porras, Technological Institute of Costa Rica, CR
Abel Suing, Private Technical University of Loja, EC
Adolfo Lozano-Tello, University of Extremadura, ES
Adrián Hiebra Pardo, University of Santiago de Compostela, ES
Alberto Fernández, Universidad Rey Juan Carlos, ES
Alberto Freitas, FMUP, University of Porto, PT
Alcinia Zita Sampaio, IST, University of Lisbon, PT
Alejandro Peña, Escuela de Ingeniería de Antioquia, CO
Alexandre L'Erario, Federal Technological University of Paraná, BR
Alicia Garcia-Holgado, University of Salamanca, ES
Alma Gomez-Rodriguez, University of Vigo, ES
Ana Amélia Carvalho, University of Coimbra, PT
Ana Beatriz Blanco-Ariza, Universidad Simón Bolívar, CO
Ana Isabel Veloso, University of Aveiro, PT
Ana Maria Correia, ISEGI, New University of Lisbon, PT
Ana Paula Afonso, Polytechnic Institute of Porto, PT
Anabela Mesquita, Polytechnic Institute of Porto, PT
Anacleto Correia, Naval School, PT
Angelica Caro, Universidad del Bio-Bio, CL
Ana Calvão, University of Aveiro, PT
Ana Carla Amaro, University of Aveiro, PT
Ana Melro, University of Aveiro, PT
Ania Cravero, University of La Frontera, CL
Aníbal Zaldivar-Colado, Universidad Autonoma de Sinaloa, MX

António Abreu, ISCAP, Polytechnic of Porto, PT
António Coelho, FEUP, University of Porto, PT
Antonio Fernández-Caballero, University of Castilla-La Mancha, ES
António Godinho, ISLA-Gaia, PT
Antonio Jesus Garcia Loureiro, University of Santiago de Compostela, ES
Antonio Jiménez-Martín, Polytechnic University of Madrid, ES
António Palma dos Reis, ISEG, University of Lisbon, PT
António Pereira, Polytechnic Institute of Leiria, PT
Armando Mendes, University of the Azores, PT
Arnaldo Martins, University of Aveiro, PT
Arturo J. Méndez, University of Vigo, ES
August Climent Ferrer, La Salle Open University, AD
Baltasar Garcia Perez-Schofield, Universidad de Vigo, ES
Beatriz Rodriguez, University of the Republic, UY
Beatriz Sainz de Abajo, University of Valladolid, ES
Bernabé Escobar-Perez, University of Seville, ES
Borga Bordel, Polytechnic University of Madrid, ES
Bráulio Alturas, ISCTE - University Institute of Lisbon, PT
Brenda L. Flores-Rios, Universidad Autónoma de Baja California, MX
Carlos Alexandre Silva, Federal Institute of Minas Gerais, PT
Carlos Carreto, Polytechnic Institute of Guarda, PT
Carlos Morais, Polytechnic Institute of Bragança, PT
Carlos Regalao Noriega, Universidad Simón Bolívar, CO
Carlos Vaz de Carvalho, Polytechnic Institute of Porto, PT
Carmen Galvez, University of Granada, ES
Carlos Rabadão, Polytechnic of Leiria, PT
Carlos Rompante Cunha, Polytechnic of Bragança, PT
Cesar Colazzos, Universidad del Cauca, CO
Ciro Martins, University of Aveiro, PT
Cristina MR Caridade, ISEC, Polytechnic of Coimbra, PT
Dalila Durães, University of Minho, PT
Daniel Poland, University of Aveiro, PT
Daniel Riesco, National University of San Luis, AR

Dante Carrizo, University of Atacama, CL
David Fonseca, Universitat Ramon Llull, ES
David Ramos Valcarcel, University of Vigo, ES
Diana Cecilia Yacchirema Vargas, Escuela Politécnica Nacional, EC
Dora Simões, University of Aveiro, PT
Edna Dias Canedo, University of Brasilia, BR
Eduardo Amadeu Dutra Moresi, Catholic University of Brasilia, BR
Eduardo Sánchez Vila, University of Santiago de Compostela, ES
Edwin Juvenal Cedeño Herrera, University of Panama, PA
Enric Mor, Universitat Oberta de Catalunya, ES
Eusébio Ferreira da Costa, School of Technologies of Fafe, PT
Eva Villegas, La Salle - Universitat Ramon Llull, ES
Fábio Marques, University of Aveiro, PT
Fernando Bandeira, Fernando Pessoa University, PT
Fernando Bobillo, University of Zaragoza, ES
Fernando Moreira, Portucalense University, PT
Fernando Paulo Belfo, ISCAC, Polytechnic of Coimbra, PT
Fernando Ribeiro, Polytechnic of Castelo Branco, PT
Fernando Suarez, CPEIG, ES
Filipe Caldeira, Polytechnic of Viseu, PT
Filipe Montargil, Polytechnic of Lisbon, PT
Filipe Portela , University of Minho, PT
Flower by María Sánchez Aguirre, Universidad César Vallejo, PE
Francisca Rosique Contreras, Polytechnic University of Cartagena, ES
Francisco Arcega, University of Zaragoza, ES
Francisco Javier Lena-Acebo, University of Cantabria, ES
Francisco Restivo, Portuguese Catholic University, PT
Franyelit Suarez, University of the Americas, EC
Gabriel Alberto Garcia-Mireles, University of Sonora, MX
Gabriel Guerrero-Contreras, University of Cádiz, ES
Gerardo Gonzalez Filgueira, University of Coruña, ES
Gladys Tenesaca Luna, Universidad Técnica Particular de Loja, EC
Gloria Maritza Valencia Vivas, Universidad de las Fuerzas Armadas, EC

Gloria Piedad Gasca-Hurtado, University of Medellín, CO
Guilhermina Lobato Miranda, University of Lisbon, PT
Helder Gomes, University of Aveiro, PT
Helder Zagalo, University of Aveiro, PT
Hélia Guerra, University of the Azores, PT
Henrique S. Mamede, Open University, PT
Higino Ramos, University of Salamanca, ES
Inês Domingues, CI-IPOP, PT
Inés López, University of Alcalá, ES
Isabel de la Torre, University of Valladolid, ES
Isabel Pedrosa, Polytechnic Institute of Coimbra, PT
Isidro Navarro, Polytechnic University of Catalonia, ES
Ismael Etxeberria-Agiriano, Universidad del País Vasco (UPV/EHU), ES
Ivaldir de Farias Junior, University of Pernambuco, BR
Ivan Garcia, Universidad Tecnologica de la Mixteca, MX
João Paulo Ferreira, ISEC, Polytechnic of Coimbra, PT
João Reis, University of Aveiro, PT
João Roberto de Toledo Quadro, CEFET/ RJ, BR
Jacinto Estima, European University, PT
Javier Garcia Tobio, CESGA-Centro de Supercomputacion de Galicia, ES
Javier Medina, Universidad Distrital Francisco José de Caldas, CO
Jeimy Cano, Universidad de los Andes, CO
Jezreel Mejia, Center for Research in Mathematics (CIMAT), MX
João Balsa, FC, University of Lisbon, PT
João Paulo Costa, University of Coimbra, PT
João Tavares, FEUP, University of Porto, PT
João Vidal de Carvalho, ISCAP, Polytechnic of Porto, PT
Joaquim Reis, ISCTE - University Institute of Lisbon, PT
Jorge Bernardino, ISEC, Polytechnic of Coimbra, PT
Jorge Buele, Universidad Tecnológica Indoamérica, EC
Jorge Eduardo Ibarra-Esquer, Universidad Autónoma de
Baja California, MX
Jorge da Silva Correia-Neto, Federal Rural University of Pernambuco, BR
Jose Alfonso Aguilar, Autonomous University of Sinaloa, MX

José Alvarez-Garcia, University of Extremadura, ES
José Borbinha, IST, University of Lisbon, PT
José Carlos Ribeiro, Polytechnic of Leiria, PT
José Cascalho, University of the Azores, PT
José Felipe Cocón Juárez, Universidad Autónoma del Carmen, MX
José Luís Pereira, University of Minho, PT
José Luís Silva, University Institute of Lisbon (ISCTE-IUL), PT
José Paulo Lousado, Polytechnic Institute of Viseu, PT
José Luis Pestrana Brincones, University of Malaga, ES
Jose M Molina, Carlos III University of Madrid, ES
José Machado, University of Minho, PT
Jose Maria de Fuentes, Carlos III University of Madrid, ES
Jose RR Viqueira, University of Santiago de Compostela, ES
José Silvestre Silva, Military Academy, PT
José Torres, Fernando Pessoa University, PT
Josep M. Marco-Simó, Universitat Oberta de Catalunya, ES
Juan Angel Contreras Vas, University of Extremadura, ES
Juan D'Amato, PLADEMA-UNCPBA-CONICET, AR
Juan M. Santos Gago, University of Vigo, ES
Jugurta Lisboa-Filho, Federal University of Viçosa, BR
Klinge Orlando Villalba-Condori, Catholic University of Santa María, PE
Leila Weitzel, Fluminense Federal University, BR
Leonardo Bermon, National University of Colombia, CO
Leticia Morales Trujillo, University of Seville, ES
Lilia Muñoz, Technological University of Panama, PA
Lucila Ishitani, PUC Minas, BR
Lucila Romero, Universidad Nacional del Litoral, AR
Luis Alvarez Sabucedo, University of Vigo, ES
Luís Bruno, Polytechnic Institute of Beja, PT
Luis Camarinha-Matos, New University of Lisbon, PT
Luís Cavique, Open University, PT
Luis Chamba Eras, National University of Loja, EC
Luis Enrique Sánchez Crespo, Universidad de Castilla-La Mancha, ES
Luis Fernández Sanz, University of Alcalá, ES

Luís Ferreira, Polytechnic Institute of Cávado and Ave, PT
Luis Vilan-Crespo, University of Vigo, ES
Luis Maria Romero-Moreno, University of Seville, ES
Luisa Miranda, Polytechnic Institute of Bragança, PT
Lus Sussy Bayona Ore, Universidad Nacional Mayor de San Marcos, PE
Luz María Hernández Cruz, Autonomous University of Campeche, MX
Magdalena Arcilla Cobián, National University of Distance Education, ES
Manuel Fernández-Veiga, University of Vigo, ES
Manuel Jose Fernandez Iglesias, University of Vigo, ES
Marcelo Marciszack, National Technological University, AR
Marcelo de Paiva Guimarães, Federal University of São Paulo, BR
Marcelo Zambrano Vizuete, Universidad Tecnica del Norte, EC
Marco Javier Suarez Barón, Pedagogical and Technological
University of Colombia, CO
Marco Painho, ISEGI, New University of Lisbon, PT
Margarita Ramirez Ramirez, Universidad Autonoma de
Baja California, MX
Maria Amelia Eliseu, Mackenzie Presbyterian University, BR
Maria Cristina Marcelino Bento, UNIFATEA, BR
Maria de la Cruz del Río-Rama, University of Vigo, ES
Maria de los Milagros Gutierrez, National Technological University, AR
Maria del Mar Miras Rodriguez, University of Seville, ES
Maria do Rosário Bernardo, Open University, BR
Maria Hallo, Escuela Politécnica Nacional, EC
Maria Helena Garcia Ruiz, University of Camtabria, ES
María J. Lado, University of Vigo, ES
Maria João Ferreira, Portucalense University, PT
Maria João Gomes, University of Minho, PT
Maria José Angélico, Polytechnic Institute of Porto, PT
Maria José Escalona, University of Seville, ES
Maria José Sousa, European University, PT
Mario Chacón-Rivas, Technological Institute of Costa Rica, CR
Mario José Diván, National University of La Pampa, AR
Marisol B. Correia, University of Algarve, PT

Maristela Holanda, University of Brasilia, BR
Martín Llamas Nistal, University of Vigo, ES
Martín López Nores, University of Vigo, ES
Matías Garcia Rivera, University of Vigo, ES
Mercedes Ruiz, University of Cádiz, ES
Miguel A. Brito, University of Minho, PT
Miguel Angel Conde, University of Leon, ES
Miguel Angel Olivero Gonzalez, University of Seville, ES
Miguel Bugalho, European University, PT
Miguel Casquilho, IST, University of Lisbon, PT
Miguel Ramón González Castro, Ence, Energía y Celulosa, ES
Mirna Ariadna Muñoz Mata, Center for Investigation in Mathematics (CIMAT), MX
Nelson Rocha, University of Aveiro, PT
Nuno Lau, University of Aveiro, PT
Nuno Melão, Polytechnic of Viseu, PT
Nuno Ribeiro, Fernando Pessoa University, PT
Oscar Mealha, University of Aveiro, PT
Patricia Dias, State University of Minas Gerais, BR
Patricia Oliveira, University of Aveiro, PT
Paula Prata, University of Beira Interior, PT
Paulo Martins, University of Trás-os-Montes and Alto Douro, PT
Paulo Pinto, FCT, New University of Lisbon, PT
Paulo Rurato, Fernando Pessoa University, PT
Paulo Urbano, FC, University of Lisbon, PT
Pedro Araújo, University of Beira Interior, PT
Pedro Palos, University of Seville, ES
Pedro Sanz Angulo, University of Valladolid, ES
Pedro Sobral, Fernando Pessoa University, PT
Pedro Sousa, University of Minho, PT
Pilar Mareca Lopez, Polytechnic University of Madrid, ES
Ramiro Delgado, Universidad de las Fuerzas Armadas, EC
Ramon Alcarria, Polytechnic University of Madrid, ES
Raul Laureano, ISCTE - University Institute of Lisbon, PT

Renato Maurício Toasa Guachi, Universidad Tecnológica Israel, EC
Rene Faruk Garzozi-Pincay, State University of Santa Elena Peninsula, EC
Ricardo Andrés Garcia León, Francisco de Paula University
Santander Ocaña, MX
Ricardo J. Rodríguez, University of Zaragoza, ES
Ricardo Linden, FSMA, BR
Rita Oliveira, University of Aveiro, PT
Rita Santos, University of Aveiro, PT
Robero Marichal, University of La Laguna, ES
Roberto Theron, University of Salamanca, ES
Rodolfo Miranda Barros, State University of Londrina, BR
Roman Lara, Universidad de las Fuerzas Armadas, EC
Rubén González Crespo, International University of La Rioja, ES
Rui Cruz, IST, University of Lisbon, PT
Rui Pedro Marques, University of Aveiro, PT
Rui S. Moreira, Fernando Pessoa University, PT
Samuel Sepulveda, University of La Frontera, CL
Santiago Gonzales Sánchez, Universidad Inca Garcilaso de la Vega, PE
Sara Balderas-Díaz, University of Cádiz, ES
Saulo Barbara de Oliveira, Federal Rural University of Rio de Janeiro, BR
Sérgi F. Lopes, University of Minho, PT
Sergio Araya Guzmán, Universidad del Bío-Bío, CL
Sergio Gálvez Rojas, University of Malaga, ES
Sérgio Guerreiro, Lusophone University of Humanities and
Technologies, PT
Silvia Fernandes, University of Algarve, PT
Solange N Alves de Souza, University of São Paulo, BR
Telmo Silva, University of Aveiro, PT
Teresa Guarda, Península de Santa Elena State University, EC
Tomas San Feliu, Polytechnic University of Madrid, ES
Thiago Dias, CEFET-MG, BR
Valéria Farinazzo Martins, Mackenzie Presbyterian University, BR
Vera Pospelova, University of Alcalá, ES
Verónica Vasconcelos, ISEC, Polytechnic of Coimbra, PT

Vicente Morales, Technical University of Ambato, EC
Victor Flores, Catholic University of the North, CL
Victor H. Andaluz, Universidad de las Fuerzas Armadas ESPE, EC
Victor Hugo Medina Garcia, Universidad Distrital
Francisco José de Caldas, CO
Vitor Carvalho, Polytechnic Institute of Cávado and Ave, PT
Vitor Santos, ISEGI, New University of Lisbon, PT
Wagner Tanaka Botelho, Federal University of ABC, BR

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 06/10/2021
Aceitação/Acceptance: 09/01/2022

Editorial

Las Tecnologías Duales, una oportunidad para desarrollo y transferencia tecnológica

Dual Technologies, and opportunity for develop and transfer technology

Carlos Hernán Fajardo-Toro[1], José María Riola[2]

carlosh.fajardo@esap.edu.co; chema.riola@rga-psi.es

[1] Escuela Superior de Administración Pública - ESAP

[2] Escuela Naval de Cadetes "Almirante Padilla" – ENAP. Cartagena de Indias, Colombia

Pages: xi-xiii

1. Introducción

Se entienden por tecnologías de uso dual, las tecnologías con aplicaciones civiles y militares. Desde que el hombre es creador de tecnología, las tecnologías de uso dual tienen su razón de ser, y así a lo largo de la historia, aplicados con fines pacíficos o bélicos, los desarrollos tecnológicos aprovechan su potencial civil y militar. Ejemplos de ello son la invención de la pólvora que tenía un uso religioso y posteriormente uno militar; los altos hornos en China en el siglo V y la fundición del hierro, lo cual tuvo una aplicación frecuente en construcción de armas, así como herramientas de agricultura. También en la antigua Grecia, el desarrollo que realizaron para la extracción de hierro, dada la dificultad para obtener bronce, lo que generaba una escasez de armas y que se necesitaba para enfrentarse a los llamados pueblos del mar, progreso que también permitió muchos otros usos civiles como el desarrollo de herramientas para la construcción de barcos con quilla.

Ahora bien, este término hasta los años 80, se refería a las tecnologías civiles que planteaban problemas de exportación a países del Pacto de Varsovia, como los microprocesadores o los materiales para la fabricación de armamento nuclear, que podían posibilitar mejores sistemas de armas. Así, se creó la cultura del control de la trasferencia de tecnología entre naciones, para impedir la transmisión de sistemas avanzados fuera de su país de origen.

La Guerra Fría dio lugar al desarrollo de sistemas de innovación dedicados en exclusiva al sector militar, con especificaciones técnicas y requisitos operativos sobre los que trabajaban grandes corporaciones del sector en un entorno cerrado. Esas inversiones fueron un catalizador indiscutible de I+D, situando al sector de la Defensa en la vanguardia de la innovación tecnológica y propiciaron que la transferencia tecnológica fuese principalmente del ámbito militar al civil como ocurrió con el propio Internet, el radar, microondas, sonar, GPS, energía nuclear, fibra óptica, etc. Esta tendencia se invierte a partir de la década de los 90 con la caída de inversión de I+D en Defensa y los grandes desarrollos civiles relacionados con las tecnologías de la información y las comunicaciones (TICs), desde entonces se ha exportado tecnología de forma masiva al ámbito militar, como es el caso de las tecnologías de computación y los microprocesadores.

Así, en este siglo, el concepto de tecnologías de uso dual se refiere a aquellas tecnologías susceptibles de producir aplicaciones en el ámbito civil como el militar, extendiendo la necesidad de una base tecnológica en el ámbito civil como requisito para una potente industria de Defensa. Este apoyo del sector Defensa a la base tecnológica y científica del ámbito civil ha promovido una apertura de la industria de Defensa, promoviendo la trasferencia continua de conocimiento y tecnologías entre ambos ámbitos.

En la actualidad, las diferencias entre la aplicación al ámbito civil y militar están cada vez más difuminadas y en la mayoría de los casos varían en un pequeño conjunto de especificaciones particulares. Es así como Caviggioli et al. (2022) establecen, en un estudio de patentes registradas, concluyendo que mientras los desarrollos militares tengan un alcance tecnológico amplio mayor será la probabilidad de un uso civil, donde la redistribución en diversos sectores es útil en aplicaciones civiles; pero así mismo también establecen que en las patentes no está estrictamente definido su uso civil o militar.

Por otra parte, Sezal & Giumelli (2022) en un estudio de la dinámica transferencia tecnológica e industria militar en Países Bajos, estableciendo como se ha pasado de una transferencia desde lo militar a hacia lo civil a un proceso inverso. Es decir, las tecnologías se están desarrollando en el entorno civil, especialmente gracias a la revolución digital, y están siendo implementadas en sistemas de defensa.

Todo lo anterior muestra como la unión entre un sistema de defensa y sus desarrollos con empresas civiles, resultan siendo un entorno el cual se pueden alimentar y favorecer mutuamente través de spin-off o spin-in, generando un crecimiento económico y la creación de un ecosistema I+D+i que permita el desarrollo y transferencia de tecnologías.

2. Estructura

Los artículos presentados en esta edición fueron seleccionados de los artículos aceptados La Conferencia Internacional Multidisciplinaria de Investigación Aplicada a la Defensa y Seguridad (MICRADS 2022), que se celebró en la Escuela Naval de Suboficiales ARC "Barranquilla", en Barranquilla, Colombia, entre 11 y 13 de julio de 2022.

MICRADS 2022, es un foro internacional para investigadores y profesionales para presentar y discutir las recientes innovaciones, tendencias, resultados, experiencias y preocupaciones en las diversas perspectivas de la Defensa y Seguridad.

El conjunto de artículos publicados en este número de RISTI, fue el resultado de la selección de algunos trabajos presentados por los autores de los Talleres y otros de la conferencia principal.

En este número de la Revista Ibérica de Sistemas y Tecnologías de la Información (RISTI), aborda temas multidisciplinares relacionados a: Big Data Analytics y Aplicaciones; Ciberseguridad y Ciberdefensa; Estrategia, geopolítica y Oceanopolítica; Ética, Computadoras y Seguridad; Medios, Tecnología Aplicada y Comunicación; Redes informáticas, Movilidad y Sistemas Penetrantes; Sistemas de Software, Arquitecturas, Aplicaciones y Herramientas; Tecnologías de la Información en Educación.

Agradecimientos

Expresamos nuestro agradecimiento a todos los autores y revisores involucrados en esta edición, esperando que este número de RISTI resulte una lectura útil para todos.

Un agradecimiento especial a AISTI, y a todas las entidades que contribuyeron a este emprendimiento, haciendo de RISTI una referencia: CiteFactor, Compendex, Dialnet, DOAJ, DOI, EBSCO, GALE, IndexCopernicus, Index of Information Systems Journals, Web of Knowledge, Latindex, ProQuest, QUALIS, SciELO, SCImago y Scopus.

Referencias

Caviggioli, F., de Marco, A., Gkotsis, P., Scellato, G., & Vezzani, A. (2022). Dual use inventions: identification and characterization using patent data. Economics of Innovation and New Technology. https://doi.org/10.1080/10438599.2022.2026221

Sezal, M. A., & Giumelli, F. (2022). Technology transfer and defence sector dynamics: the case of the Netherlands. European Security. https://doi.org/10.1080/09662839.2022.2028277

Índice / Index

EDITORIAL

Las Tecnologías Duales, una oportunidad para
desarrollo y transferencia tecnológica xi
Carlos Hernán Fajardo-Toro, José María Riola

ARTIGOS / ARTICLES

Avaliação da Segurança de Sistemas de Informação nas Autarquias Locais:
Um Estudo de Caso num Município do Médio Tejo 1
Célio Gonçalo Marques, Sofia Cassis, Carlos Trigacheiro

O Código dos Contratos Públicos como instrumento potenciador da economia,
eficiência e eficácia nas despesas públicas de segurança em Portugal 17
Cláudio Lopes, Luís Malheiro, José Silva, Pedro Pereira[4], Luís Ribeiro

A Igualdade de Género na União Europeia: a implementação
da agenda mulheres, paz e segurança 28
Luís Malheiro, Sofia Menezes, João Reis, Paulo Machado,
Ana Romão, Fernando Bessa

Os Diferentes Paradigmas da Administração
Pública nas Forças Armadas Portuguesas 51
Ana Castanho, Tiago Gonçalves

Integración de una microrred solar fotovoltaica al sistema
eléctrico de un buque de apoyo logístico y cabotaje liviano BALC-L 65
M. P. Arrieta, A. M. Castaño, C. Marrugo, R. R. Mendoza

Análisis OSINT aplicado a la investigación de Fraudes Financieros 80
Christian Vaca, David Martínez, Renato M. Toasa

Módulos de misión del Buque de Apoyo Logístico y
Cabotaje Liviano (BALC-L) para operaciones humanitarias
y atención de desastres en el Pacífico Colombiano 92
Farah Inés Vergara Chadid, José María Riola, Juan Carlos Martínez,
Priscilla Areiza Frieri

Cloud Computing – Quem garante a segurança dos dados? 105
Nuno Miguel Carvalho Galego, Nelson Duarte, Domingos Martinho

La informática y la ciencia de datos utilizando Deep learning..... 116
Javier Guaña-Moya, Nelson Salgado-Reyes, Charles Escobar-Terán

Aplicación del Criterio de Minimización de Movimientos Totales en una Fábrica de armas y municiones.....128
Ana Alvarez, David Andrés Guachamín, Alexis Suárez del Villar

Detección y Seguimiento de Drones con Cámaras de Vigilancia Estáticas para Lugares Estratégicos 139
Rubén León[1], Alexis Tinoco-S, Álvaro Chisaguano, Héctor Tufiño, Héctor Moya, Fernando Lara

Evolução do Nível de Proficiência das Competências de Liderança no Ensino Superior: Estudo de Caso dos Cadetes Alunos da Academia Militar Portuguesa 152
José Rouco, João Montez

Um diagnóstico sobre o processo de comunicação sigilosa entre os órgãos do Sistema Brasileiro de Inteligência.....169
Cileno de Magalhães Ribeiro, Rafael Rabelo Nunes, Robson de Oliveira Albuquerque

Proceso de desarrollo de vehículos de superficie no tripulados en instituciones Navales Colombianas.....184
José María Riola, Shamir Sánchez, Enrique Sierra, Carlos Hernán Fajardo-Toro

Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990 – 2021.....197
Diego Edison Cabuya Padilla, Carlos Fabián Alvarado Carvajal, Ramiro Alfonso Carrascal Ortiz, Stefany Patricia Escandón Bernal, José María Riola, Carlos Hernán Fajardo-Toro

Modelo conceptual del Sistema del Poder Marítimo a nivel estratégico en Colombia..... 211
Diego Andrés Alba Rocha, Juan Ricardo Ortegón Vega, Diego Edison Cabuya Padilla, José María Riola, Carlos Hernán Fajardo-Toro

Sistema Inteligente para Control y Monitorización de una Estación Robótica usando Motion Control y Visión Artificial..... 222
Lesly Tarira Montalvan, Edisson Jordan, Edith Tubón, Sandra Carrillo, Eduardo Heredia, Franklin Salazar

Perfil Psicológico del Líder: Un Estudio Exploratorio con Estudiantes de la Carrera de Administración de Negocios Internacionales.....237
Ivan Iraola-Real, Alonso Iraola-Arroyo, Daniel Iraola, Keita Nakamine

Evaluación de la Gestión Virtual Educativa en Ingeniería Industrial:
Una Experiencia en el Contexto de Enseñanza Remota de Emergencia..... 249
Ivan Iraola-Real, Alonso Iraola-Arroyo

Análisis de ataques DoS en redes de datos basadas en hardware y software 262
Anthony Albarracín-Estrada, Darío Enrique Soto-Duran,
Juliver Gil-Herrera , Fabio Alberto Vargas-Agudelo

Análisis previo para la implementación de un
plan de instrucción y entrenamiento estándar NATO
en el sistema remotamente pilotado Scaneagle.....276
Capitán Tiria Contreras Christian Mauricio

Política de língua como vetor de projeção de poder:
o caso de Timor-Leste.....288
Rui Pereira, Luís Malheiro

Avaliação da Rotina Operacional do Operador Nacional do
Sistema Elétrico Brasileiro (ONS) em Relação às Ações de
Gerenciamento de Riscos Associados à Segurança Cibernética.....301
Eduardo De Oliveira Lima, Fernando Rocha Moreira,
Flávio Elias Gomes de Deus, Georges Daniel Amvame Nze,
Rafael Timóteo de Sousa Júnior, Rafael Rabelo Nunes

Gestão de Riscos Cibernéticos no Ambiente Operacional
do Sistema Elétrico Brasileiro (ARCiber ONS): uma
avaliação do processo de recuperação de dados pelo sistema SCADA.....313
Eduardo de Oliveira Lima, Fernando Rocha Moreira,
Carlos André de Melo Alves, Rafael Rabelo Nunes

El gran juego interminable: estudio de caso afgano..... 326
Rui Pereira, Luís Malheiro

Factores clave en la evaluación del software libre o propietario
para su uso en organizaciones militares y de defensa 335
Lewis Mahecha Ardila, Ricardo Naranjo Faccini,
Carlos A. Castaneda-Marroquín, José María Riola, Carlos Hernán Fajardo-Toro

Control Ganadero: Aplicación móvil para gestionar la información
de producción de leche de vaca aplicado a la granja UFPSO 347
María Camila Sánchez-Velasquez, Jesús Alberto Rodríguez-Rodríguez,
Luis Anderson Coronel-Rojas, Dewar Rico-Bautista

Nuevas tecnologías militares en el ámbito aéreo y espacial:
Tendencias y cambios en el Derecho Internacional 360
Zully Ximena Rojas Ortiz, Paula Alejandra Prieto Ararat

Producción biológica de ácidos grasos volátiles a partir de lodo primario y lodo digerido de una planta de tratamiento de aguas residuales como fuente de productos biopolímeros en la industria militar 374
Gracia Jeniffer, Cabeza Iván, Montenegro Carlos, Paola Acevedo

Tendencias de la acumulación de biogás como fuente energética en la fase acidogénica de la producción de ácidos grasos volátiles a partir de lodos de aguas residuales municipales 386
Gracia Jeniffer, Cabeza Iván, Montenegro Carlos, Ferrasse Jean-Henry

Evaluación de riesgos en ciberseguridad: una revisión bibliométrica 396
Christian Obando-Ibarra, Luis Fernando Garcés-Giraldo, Jefferson Quiroz-Fabra, Martha Benjumea-Arias, Alejandro Valencia-Arias, Luisa Rodríguez Zavala, Camilo Patiño-Vanegas

Tendencias investigativas en el uso de tecnologías de Big Data en sistemas de ciberseguridad..... 410
Luis Fernando Garcés-Giraldo, Martha Benjumea-Arias, Olga Inés Vélez Bernal, Alejandro Valencia-Arias, Luis Tadeo Celi Saavedra, Camila Bermeo-Giraldo, Jefferson Quiroz-Fabra

Definición de Estrategia de Encadenamientos Productivos para el Desarrollo Económico del Municipio de Pore-Casanare..... 421
Elkin Olaguer Pérez Sánchez, Mauricio Antonio Bedoya Villa, Jesus Manuel Ramos Garcia, María Quisphi González, Patricia Eugenia Escobar Martínez, Francisco Javier Arias Vargas

Análisis de los frameworks de ciberseguridad en IIoT existentes..... 436
Herberth Alberto Ausecha, Katerine Márceles Villalba, Siler Amador Donado

Buenas prácticas para el desarrollo de software sostenible 449
Darío Enrique Soto-Duran, Adriana Xiomara Reyes-Gamboa, Juan Camilo Giraldo-Mejía, Aixa Villamizar-Jaimes, Fredy Alonso Vidal-Alegría

Mapeo de Recursos y Capacidades para el fortalecimiento en la Gestión de la Innovación: Un Estudio de Caso en una Pyme del Sector Salud..... 461
Mauricio Antonio Bedoya Villa, Elkin Olaguer Pérez Sanchez, Jesús Manuel Ramos Garcia, Juan Carlos Avella, Paul Andrés Marino López

Mapeo sistemático sobre la integración de tecnologías de inteligencia artificial y recursos TIC en aprendizaje-enseñanza musical 479
Cristian Fabian Bravo Mosquera, Manuel Francisco Silva Joaqui, Maria Isabel Vidal Caicedo, Eleonora Palta Velasco

Diseño de una aplicación gamificada como apoyo en los cursos de Física Cinemática en la Institución Universitaria Colegio Mayor del Cauca.....491
Sebastian Quilindo, Royer Muñoz, Maria Isabel Vidal

Pasos para diseñar un modelo de madurez con marco de trabajo ágil para la implementación a sistemas de gestión de la seguridad de TI alineado a las políticas de gobierno colombiano para el sector público.....501
Katerine Márceles Villalba, Siler Amador Donado

Saber Pro en programas de formación militar y policial: minería de datos para la identificación de factores asociados a los resultados 508
Gladys Irene Arboleda-Posada, David Alberto García-Arango, Aura María Vasco-Ospina, Santiago Restrepo Garizabal, Jairo Andrés Sastoque-Zapata

Modelo de Datos - Contexto Universitario: premisa para agilidad, disponibilidad y toma de decisiones apoyado en información..... 517
Javier Condor, Nelson Salgado, Henry N. Roa, Juan Francisco Chafla

Competencias para el Emprendimiento en el Contexto Covid-19..... 528
Sussy Bayona-Oré

Benefícios e Riscos do Uso da Computação em Nuvem no Setor Público: uma análise baseada em artigos disponibilizados em bases dados acadêmicas de 2017 a 2021 537
Davidson Juarêz David, Carlos André de Melo Alves, Rafael Rabelo Nunes, Roque Magno de Oliveira

Contaminación cero: la propulsión basada en hidrógeno del buque colombiano de apoyo a catástrofes 550
Diana Ramírez, Omar Vásquez, José María Riola

Sistema de telemedicina IoT de monitoreo de signos vitales y alertas de distanciamiento físico para enfermedades respiratorias..... 560
Steven Pérez, Juan P. Pallo, Santiago Manzano, Marco Jurado, Dennis Chicaiza

Mitigação dos Riscos à Privacidade através da Anonimização de Dados 573
Juliano Rodrigues Ferreira, João Alberto Pincovscy, Cileno de Magalhães Ribeiro, Edna Dias Canedo, Fábio Lúcio Lopes de Mendonça

Modelos analíticos para identificar patrones de delitos financieros: Una revisión sistemática de la literatura 586
Maritza Murillo Ortíz, Lillyana María Giraldo Marín, Herman Horacio Jaramillo Villegas, Carlos César Piedrahita Escobar

Emprego dual - civil e militar - do 5G na defesa brasileira:
uma proposta para o SISFRON, sob domínio do Exército 599
Ricardo Cincinato Freitas de Oliveira, Georges Daniel Amvame Nze, Ugo Silva Dias

Protocolos de Autenticação e Controle de Acessopara
Aplicação das Forças Armadas e Orgãos de Segurança
Pública em Redes Móveis 4G/LTE e 5G 616
Jose Ricardo, Ugo Dias

Metodología para la detección de minería ilegal
mediante el uso de imágenes de radar Sentinel como
herramienta para la defensa y seguridad del territorio:
Caso de estudio Río Quito, Chocó 629
Jonathan Sandoval, Luis Castillo, Erika Upegui

Continuidad operacional de las redes de gas en Chile..... 643
Manuel Sepulveda, Vicente Salas, Gustavo Gatica, John Ríos

Minería de datos educativos: Incidencia de factores
socioeconómicos en el aprovechamiento escolar 654
*Jorge Pincay-Ponce, Jorge Herrera-Tapia, Jackeline Terranova-Ruiz,
Marely Cruz-Felipe, Juan Sendón-Varela, Lytyet Fernández-Capestany*

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 14/10/2021
Aceitação/Acceptance: 02/01/2022

Avaliação da Segurança de Sistemas de Informação nas Autarquias Locais: Um Estudo de Caso num Município do Médio Tejo

Célio Gonçalo Marques[1], Sofia Cassis[2], Carlos Trigacheiro[3]

celiomarques@ipt.pt; sofia.cassis@gmail.com; carlostrigacheiro@ipt.pt

[1] Laboratório de Inovação Pedagógica e Educação a Distância (LIED.IPT), Instituto Politécnico de Tomar, Portugal Centro de Administração e Políticas Públicas (CAPP), Universidade de Lisboa, Portugal

[2] Instituto Politécnico de Tomar, Portugal

[3] Instituto Politécnico de Tomar, Portugal

Pages: 1-16

Resumo: Numa Era caracterizada pela importância da informação, a generalidade das organizações depende fortemente dos Sistemas de Informação para o desempenho da sua missão. Para as Autarquias Locais, onde se verificam constantes mudanças nos processos organizacionais com o objetivo de uma melhor utilização económica, eficiente e equitativa dos recursos públicos, os Sistemas de Informação são um fator-chave. Ao lidarem diariamente com informação confidencial estão sujeitas a obrigações de conformidade ética e legal que geram grande responsabilidade na gestão da informação que tratam e produzem. Com este estudo de caso pretendeu-se aferir, através da aplicação de um inquérito por questionário baseado na ISO/IEC 27002:2013 associado a um modelo de maturidade qual o grau de maturidade dos controlos de segurança do Sistema de Informação num Município do Médio Tejo (MMT). A aplicação destas ferramentas permitiu identificar quais as áreas mais críticas e formas de melhorar os processos.

Palavras-chave: Autarquias Locais; ISO/IEC 27002:2013; modelo de maturidade; Segurança da Informação.

Evaluation of Information Systems Security in Local Municipalities: a Case Study in a Médio Tejo Municipality

Abstract: In a time characterized by the importance of information, most organizations strongly depend on information systems for the fulfilment of their mission. For local Municipality Halls, where there are constant changes in organizational processes aimed at economically, efficiently and equitably improving the usage of public resources, information systems are key factors. Dealing daily with confidential information, they are subject to obligations of ethical and legal conformity that imply great responsibility in the management of the information they process and generate. This study aimed at understanding, through a questionnaire based on ISO/IEC 27002:2013 associated with a maturity model,

what is the degree of maturity of the security controls in the information system of a municipality in the Médio Tejo region (MMT). The application of these tools allowed the identification of the most critical areas and ways to improve processes.

Keywords: Local Municipality Hall; ISO/IEC 27002:2013; maturity model, information security.

1. Introdução

Numa Era em que todas as organizações lidam no seu dia a dia com informação dos seus colaboradores, fornecedores, parceiros, utilizadores, etc., esta tornou-se um ativo essencial, que precisa de ser adequadamente protegido.

Gouveia e Ranito (2004) referem que para as autarquias locais, que tratam com dados muito sensíveis e oficiais, a pressão é ainda maior, uma vez que as comunicações eletrónicas com o cidadão/munícipe, criam portas de entrada potencialmente perigosas, se não forem devidamente acauteladas.

A par da evolução das tecnologias da informação e comunicação, da dependência crescente entre o bom funcionamento das organizações e o normal funcionamento dos Sistemas de Informação, está o aumento da criminalidade Informática, que se manifesta através de técnicas de intrusão e aproveitamento de vulnerabilidades, impondo melhorias constantes aos paradigmas da segurança.

Beal (2005) refere que as organizações precisam adotar controlos de segurança (medidas de proteção que abranjam uma grande diversidade de iniciativas) que sejam capazes de proteger adequadamente dados, informações e conhecimentos.

A Segurança da Informação é conseguida através da implementação de um conjunto de controlos adequados (políticas, procedimentos, processos, estruturas organizacionais) que têm de ser estabelecidos, implementados, monitorizados, revistos e melhorados continuamente de forma a proteger o Sistema de Informação impedindo o acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados da informação, preservando a confidencialidade, integridade/autenticidade e disponibilidade da informação.

De acordo com Gouveia e Ranito (2004) sendo a informação umas das preocupações mais dominantes da sociedade é necessário que as organizações atribuam uma parcela aceitável do seu esforço no desenvolvimento infraestruturas adequadas para a sua recolha, armazenamento, processamento, representação e distribuição.

Nos últimos anos tem-se verificado um desenvolvimento de normas e frameworks, reconhecidas internacionalmente, que definem princípios, conceitos, controlos e componentes de gestão de segurança de informação, que visam apoiar as organizações na implementação de um Sistema de Gestão de Segurança da Informação.

Pedro (2010) refere que, devido aos novos Sistemas de Informação que estão a ser adotados por muitas organizações, foi necessária a evolução das normas técnicas de boas práticas ou standards relacionados com as Tecnologias de Informação e Comunicação de forma a acompanharem esta nova realidade.

O mesmo autor considera ainda que estes novos standards técnicos podem ser utilizados em auditoria como referenciais para avaliação comparativa de conformidade e controlo dos Sistemas de Informação e procedimentos instituídos, pois ilustram procedimentos aceites generalizadamente.

Estas normas e frameworks são aplicáveis às Autarquias Locais, representam baixos custos e são uma ótima opção, pois podem ser aplicadas pelos recursos internos, não sendo necessário recorrer à contratação de serviços externos.

Com este estudo de caso pretende-se:

- Efetuar uma análise de segurança aos controlos de segurança do Sistema de Informação do Município baseada nos controlos previstos na norma ISO/IEC 27002;
- Classificar o nível de maturidade dos controlos utilizando um modelo de maturidade de segurança;
- Apresentar resultados sob a forma quantitativa permitindo de forma simples identificar as áreas mais críticas.

No domínio da investigação observa-se a existência de um número razoável de estudos sobre Segurança de Sistemas de Informação e sobre a aplicação da ISO 27002, contudo, o número de estudos aplicados a Autarquias Locais em Portugal é praticamente inexistente, com este trabalho visa contribuir-se para colmatar esta lacuna.

O Município não possui um método de avaliação da adequação dos controlos de segurança do Sistema de Informação implementados, este facto pode levar a que os controlos adotados não sejam os ideais, originando uma maior exposição ao risco.

Este estudo irá contribuir para uma melhoria dos procedimentos atuais de proteção da informação no Município, pois uma avaliação baseada na ISO/IEC 27002:2013 permite uma visão abrangente de todo o Sistema de Informação, possibilitando uma melhor perceção da adequação dos controlos utilizados e se necessário melhorá-los de forma a obter um Sistema de Informação mais robusto.

Esta avaliação pode também ser utilizada como suporte para a tomada de decisões relacionadas com melhorias e investimento necessários para assegurar a Segurança da Informação, bem essencial da organização.

Por uma questão de segurança e confidencialidade, o nome do Município foi omitido, sendo usada a designação Município do Médio Tejo (MMT).

Começamos por efetuar um breve enquadramento teórico do trabalho, onde se destaca a apresentação da norma ISO 27002:2013. Segue-se a descrição das opções metodológicas e a apresentação dos resultados, onde é feita uma análise dos diferentes pontos da norma. Terminamos com as considerações finais do estudo.

2. Fundamentação Teórica

Com o aumento da dependência em relação às tecnologias de informação também a Administração Pública Local se deparara com um conjunto de questões que, até ao momento, não se colocavam.

Carneiro (2002) refere que é necessária a aplicação de diferentes mecanismos de proteção, deteção e reação, bem como a formulação de políticas de segurança que contribuam para a preservação da confidencialidade, integridade e disponibilidade da informação.

Os munícipes esperam que as autarquias modernizem os seus Sistemas de Informação, disponibilizando serviços que melhorem o seu bem-estar e a sua qualidade de vida.

Torna-se necessário que os Sistemas de Informação utilizados transmitam confiança aos munícipes, sendo para isso necessário garantir a existência de segurança nos portais de acesso, a proteção das redes de transmissão e tecnologias de suporte à informação e comunicação e, a confidencialidade das bases de dados.

Lopes (2012) refere que no caso particular das autarquias, onde a informação pública e pessoal deve ser protegida pelos responsáveis, deve haver a preocupação de entender a segurança como algo a considerar, logo desde o início, nas atividades de planeamento e desenvolvimento de SI.

Analisadas algumas das principais metodologias utilizadas na área de gestão de Segurança da Informação (ISO 27002:2013, COBIT e ITIL) concluiu-se que aquela que mais se adequava à realização deste trabalho é a ISO 27002:2013.

A ISO 27002:2013 é um código de boas práticas para a gestão da segurança dos Sistemas de Informação. Esta norma estabelece diretrizes e procedimentos para iniciar, implementar, manter e melhorar a gestão de segurança de uma organização e, em conjunto com um modelo de maturidade de segurança, permite medir a performance da Segurança da Informação nas organizações.

"Trata-se, no fundo, de um código de boas práticas que inclui um extenso conjunto de controlos que indicam a forma de atuação para que os objetivos definidos nas políticas possam ser atingidos" (Carvalho, 2018, p. 18).

O facto de ser integralmente fundamentada na Segurança da Informação torna-a a solução mais completa e abrangente, a sua amplitude e facilidade de aplicação tornaram esta norma não apenas alvo de destaque, mas a primeira escolha para uma análise mais aprofundada.

Esta norma tem como objetivo fornecer diretrizes para práticas de gestão de Segurança da Informação e normas de Segurança da Informação para as organizações, incluindo a seleção, a implementação e gestão de controlos, levando em consideração os ambientes de risco da Segurança da Informação da organização (ISO/IEC 27002:2013, 2013).

A norma está estruturada em 19 secções, do 0 a 4 são a introdução, a partir da 5 são sobre Segurança da Informação. Estas 14 secções contêm 35 objetivos de controlo e 114 controlos.

As 14 secções sobre Segurança da Informação, abrangem a Segurança da Informação em todos os seus aspetos, tratando de ferramentas, processos e pessoas, envolvendo soluções tecnológicas, documentação de processos e consciencialização de pessoas.

A utilização de um modelo de maturidade permite identificar lacunas que representam riscos de segurança e pontos de melhoria, é como um guia para avaliar e perceber em

que ponto a organização se encontra e orientar melhorias de forma a chegar a um nível de maturidade mais elevado, sempre em busca da excelência.

A utilização destes modelos insere o fator tempo no processo de gestão da Segurança da Informação, o que incute transparência ao processo, permitindo a comparação entre ciclos de avaliação e, até mesmo, entre organizações (benchmark).

O modelo utilizado, de Trigacheiro (2012), define seis níveis para medir a maturidade dos processos de TI.

0 - Inexistente – A organização não reconhece a existência de um processo a ser seguido.

1 – Inicial / ad hoc – O processo de segurança está deficientemente definido. Há evidências de que a organização reconhece que o processo existe, no entanto, os processos não estão normalizados, isto é, são aplicados de forma ad-hoc e casuística.

2 – Repetitivo / consistente – Abordagem repetitiva e disciplinada à realização do processo de segurança. Os processos são desenvolvidos de forma semelhante por pessoas que desenvolvem a mesma tarefa. Não há uma política de formação e comunicação de procedimentos normalizados. Há um alto grau de dependência do conhecimento dos indivíduos e, portanto, os erros são prováveis.

3 – Definido / integrado – Existem procedimentos para melhorar e aprofundar a segurança dos Sistemas de Informação. Os processos estão normalizados e documentados e são divulgados em formação. É obrigatório que os processos sejam seguidos, pelo que é improvável que sejam detetados desvios. Os processos não são sofisticados, mas existe a formalização das práticas existentes.

4 – Gerido e mensurado – Os procedimentos de segurança estão interligados e suportam o planeamento estratégico da organização. A gestão faz a monitorização e mensuração da conformidade com os procedimentos e toma medidas quando os procedimentos não atuam efetivamente. Os processos são melhorados frequentemente de acordo com as boas práticas. São usados automatismos e ferramentas de forma limitada e fragmentada.

5 - Otimizado – Processo de melhoria contínua. Os processos são refinados ao nível das boas práticas, baseados nos resultados de contínuas melhorias e de modelagem de maturidade com outras organizações. As tecnologias de informação são usadas de forma integrada para automatizar o fluxo de trabalho, fornecendo ferramentas para melhorar a qualidade e eficácia, tornando a organização rápida na adaptação

3. Metodologia

Num trabalho a definição do método de investigação está diretamente relacionada com o problema a ser estudado. Nesta situação específica recorreu-se ao estudo de caso por ser a opção metodológica que nos conduz ao alcance do objetivo preconizado para a investigação: avaliação da segurança de Sistemas de Informação num Município do Médio Tejo.

As técnicas de recolha de dados utilizadas neste estudo foram o inquérito por questionário (fonte principal) e a análise documental (fonte secundária, principalmente de apoio à compreensão do enquadramento da temática no Município).

Foi elaborado um questionário fundamentado na norma ISO/IEC 27002:2013, ao qual se associou um modelo de maturidade como escala, obtendo assim um questionário de resposta fechada, cujo preenchimento ficou a cargo do próprio respondente.

A cada controlo (114 no total) fez-se corresponder uma questão cuja resposta apresenta numa escala de Likert entre 0 e 5, correspondendo à classificação do grau da maturidade. Foram fornecidas as diretrizes de implementação e a tabela com a discriminação dos seis níveis de maturidade para apoiar a resposta.

A estrutura do questionário (figura 2) foi baseada na estrutura da norma (figura 1).

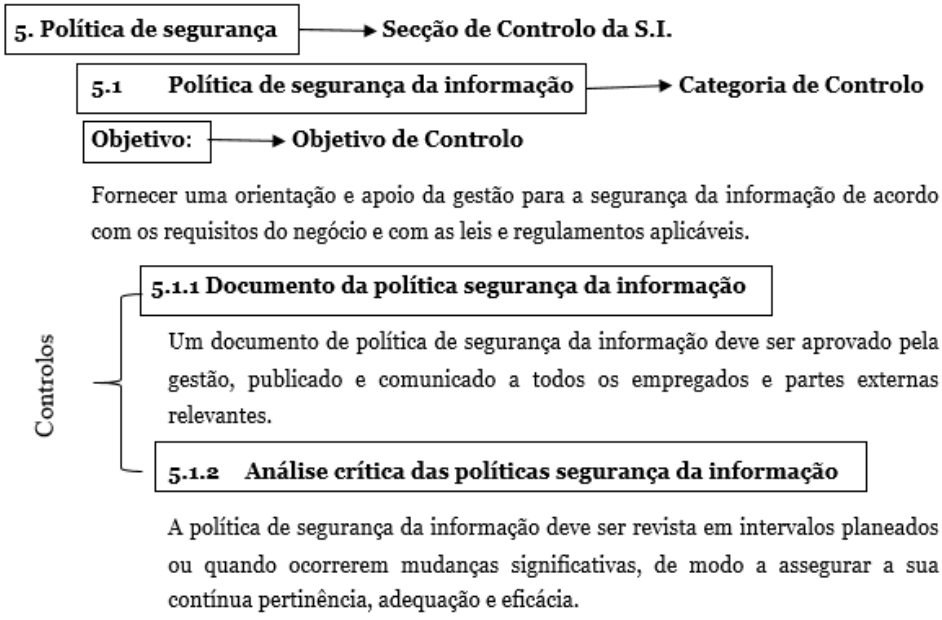


Figura 1 – Estrutura da norma

A análise dos questionários e tratamento de dados foi efetuada recorrendo-se ao auxílio de uma folha de cálculo (Microsoft Excel), onde foi efetuada a estatística descritiva. Com base nas respostas chegou-se a um nível de maturidade médio por categoria de controlo, por secção de controlo e geral. A partir dos resultados obtidos é possível perceber em que ponto se encontra o Município em termos de Segurança dos Sistemas de Informação, efetuar uma análise detalhada e verificar quais as lacunas, as vulnerabilidades, as áreas mais fracas e as mais fortes, bem como identificar os pontos de melhoria.

A.5 Política de segurança

A.5.1 Política de segurança da informação

Objetivo: Proporcionar uma orientação e apoio da gestão para a segurança da informação de acordo com os requisitos de negóci
e com as leis e regulamentações aplicáveis.

Standard		Controlo	Nível CMMI
A.5.1.1	Documento da política de segurança da informação	Um documento de política de segurança da informação deve ser aprovado pela gestão, publicado e comunicado a todos os empregados e partes externas relevantes.	0 1 2 3 4 5
		Notas:	
A.5.1.2	Análise crítica das políticas de segurança da informação	A política de segurança da informação deve ser revista em intervalos planeados ou quando ocorrerem mudanças significativas, de modo a assegurar a sua contínua pertinência, adequação e eficácia.	0 1 2 3 4 5
		Notas:	

Figura 2 – Estrutura do questionário

4. Análise de Resultados

Os resultados da análise efetuada ao Município estão evidenciados na tabela 1, onde é apresentada a maturidade média por controlo e a maturidade média geral.

Secção	Descrição	Maturidade Média	Maturidade Média Geral
A.5	Política de segurança	3,00	
A.6	Organização da segurança da informação	3,15	
A.7	Segurança em Recursos Humanos	3,00	
A.8	Gestão de ativos	2,83	
A.9	Controlo de acesso	3,90	
A.10	Criptografia	3,50	
A.11	Segurança física e do ambiente	3,19	
A.12	Segurança nas operações	4,00	**3,21**
A.13	Segurança das comunicações	3,67	
A.14	Aquisição, desenvolvimento e manutenção de sistemas	3,11	
A.15	Relação com fornecedores	2,58	
A.16	Gestão de incidentes de segurança de informação	2,14	
A.17	Aspetos da Segurança da Informação na gestão da continuidade do negócio	3,50	
A.18	Conformidade	3,37	

Tabela 1 – Avaliação geral e por secção, efetuada com base no modelo de maturidade

Através da análise dos resultados obtidos no inquérito, verifica-se que o MMT possui um nível de maturidade médio de 3,21, o que significa que, em média, os seus procedimentos de segurança estão definidos, mas existem procedimentos a melhorar para aprofundar a segurança dos Sistemas de Informação. Os processos estão normalizados e documentados e são divulgados em formação. É obrigatório que os processos sejam seguidos, pelo que é improvável que sejam detetados desvios. Os processos não são sofisticados, mas existe a formalização das práticas existentes.

Para cada secção será feita uma análise dos pontos que se destacam e que mais contribuem para a caracterização do estado atual da Segurança da Informação do MMT, sempre que se detetem fragilidades recomendar-se-ão ações corretivas.

4.1. A.5 - Política de segurança

Verifica-se que o MMT possui um documento onde estão definidas as políticas de segurança (Regulamento Interno da Informática), este documento foi aprovado em reunião de câmara e é do conhecimento de todos os colaboradores. No entanto, o mesmo não é revisto com regularidade, apesar de as políticas de segurança serem ajustadas sempre que necessário o documento não acompanha estas atualizações.

Recomenda-se que o regulamento seja revisto e atualizado, de forma a espelhar a realidade das políticas de segurança adotadas, só assim se assegura a sua contínua pertinência, adequação e eficácia.

4.2. A.6 - Organização da Segurança da Informação

Relativamente às orientações desta secção verifica-se que no MMT as responsabilidades pela Segurança da Informação estão atribuídas e bem definidas, mas não formalmente.

Seguindo as recomendações do controlo A.6.1.1 o MMT deverá definir claramente as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de Segurança da Informação específicos, deverá ainda associar orientações detalhadas às responsabilidades.

O mesmo controlo recomenda ainda que as pessoas com responsabilidades definidas pela Segurança da Informação devem delegar as tarefas de Segurança da Informação para outros, continuando responsáveis por verificar se as tarefas delegadas estão a ser executadas corretamente. Esta delegação de tarefas não se verifica no MMT.

A segregação de funções é uma preocupação no MMT e encontra-se bem implementada.

Verifica-se que o MMT não possui um procedimento que especifique quando e quais as autoridades a ser contactadas em caso de incidente de Segurança da Informação, situação que deverá ser corrigida.

O MMT mantém um reduzido contacto com associações, grupos especializados ou fóruns da área de Segurança da Informação, situação que deverá ser colmatada pois estes contactos são muito úteis para ampliar conhecimentos sobre as melhores práticas, para os especialistas do MMT se manterem atualizados, receberem previamente alertas, ter acesso a consultoria especializada em Segurança da Informação.

A Segurança da Informação na gestão de projetos é sempre considerada pela Informática, no entanto, os promotores dos projetos nem sempre têm esta preocupação, situação que deverá ser melhorada através de sensibilização e formação interna.

No que se refere ao trabalho remoto falta identificar e documentar por escrito as regras e políticas para que sejam incluídas no Regulamento Interno da Informática, esta questão revelou-se de grande importância na situação pandémica que se está a viver.

4.3.A.7 - Segurança em Recursos Humanos

A seleção e as condições de contratação são procedimentos devidamente instituídos na instituição e obedecem a regras bem definidas decorrentes de obrigações legais.

Recomenda-se uma maior consciencialização para a problemática da Segurança da Informação através de ações de formação interna para todos os recursos humanos do MMT.

Ao nível do processo disciplinar verifica-se que não está documentado nem prevista a existência de um processo formal, situação que deverá ser revista, uma vez que as boas práticas recomendam a existência de um processo disciplinar implementado e comunicado a aplicar a funcionários que cometam uma violação de Segurança da Informação.

Relativamente à rescisão ou mudança de contrato verifica-se que nem sempre a Informática é informada quando estas ocorrerem, o que pode implicar, durante algum período, falhas no controlo da segurança neste ponto. Deverá ser definido um circuito interno e identificados os responsáveis por informar a Informática quando ocorrem rescisões ou mudanças de contrato, este procedimento deverá ser incluído no Regulamento Interno da Informática.

4.4.A.8 - Gestão de Ativos

Esta secção apresenta um nível da maturidade médio de 2,83, sendo uma das secções que está abaixo da média.

Relativamente aos ativos associados à informação, os chamados ativos primários (processos e atividades de negócio, informação) é utilizado um sistema de gestão documental onde estão contidos todos os documentos gerados na execução dos processos, permitindo a associação de qualquer ficheiro em formato eletrónico. Este sistema de gestão permite constituir um arquivo digital corrente, intermédio e histórico de acordo com as normas legais estabelecidas.

Associada a cada documento integrado no sistema de gestão documental acima referido existe uma classificação da informação, no entanto esta está a ser revista e melhorada, o que implica que, provavelmente, nem toda a informação tem a classificação mais adequada.

Por sua vez, os ativos associados aos recursos de processamento da informação, os designados ativos secundários, (hardware, software, rede, etc...) encontram-se todos inventariados, com um responsável associado e com regras de utilização e devolução definidas no Regulamento Interno da Informática.

O objetivo A.8.3 tem a classificação de 1, situação que se deve ao facto de não existir um procedimento documentado relativo à utilização de dispositivos amovíveis de armazenamento de dados, situação que deverá ser corrigida

Deverão ser documentados e implementados procedimentos que definam as regras desde a utilização até à eliminação de dispositivos amovíveis de armazenamento de dados de forma a prevenir a divulgação não autorizada, a modificação, remoção ou destruição de informação armazenada nestes dispositivos.

4.5. A.9 - Controlo de Acesso

A secção A.9 é a segunda secção mais bem classificada, com um nível médio de maturidade de 3,90.

Os recursos humanos do MMT apenas têm acesso à informação e aos recursos de processamento da informação que a Informática autoriza. O fornecimento dos acessos necessários é solicitado, por escrito, pelos superiores hierárquicos à Informática e as configurações dos acessos são efetuadas pelos técnicos responsáveis em cada sistema informático.

Tal como já referido na análise à secção A.7 – segurança de recursos humanos, verifica-se que, por vezes, quando ocorrem situações de cessação de emprego, contrato ou acordo, a Informática não é informada no imediato, podendo assim eventualmente implicar, durante algum período, falhas no controlo de segurança.

Recomenda-se que seja definido um circuito interno e identificados os responsáveis por informar a Informática quando ocorrem situações de cessação de emprego, contrato ou acordo. Este procedimento deverá ser incluído no Regulamento Interno da Informática.

Relativamente à responsabilidade dos utilizadores verificam-se algumas situações de post-it com passwords colados no ecrã.

Recomenda-se uma maior consciencialização para a importância da proteção das informações de autenticação através de ações de formação interna para todos os recursos humanos do MMT.

O acesso aos sistemas e às aplicações é feito através de *login/password* que obrigam a políticas de *password* segura impedindo o uso de *passwords* simples e exigindo a sua alteração frequente.

4.6. A.10 - Criptografia

O MMT utiliza controlos criptográficos para a proteção da informação, estando atualmente em curso a migração de sistemas em falta, sobretudo de acesso externo para sistemas com criptografia.

Os certificados das chaves criptográficas são alterados em períodos inferiores a 3 meses.

4.7. A.11 - Segurança Física e do Ambiente

O MMT possui edifícios distribuídos pela cidade, verificando-se que, em alguns deles, não existe um adequado controlo de acesso e circulação de pessoas externas.

As salas com equipamento informático crítico, centro de dados e salas técnicas têm meios de controlo de acesso restritos, possuem alarme e o acesso é permitido apenas aos técnicos responsáveis pela administração de sistemas.

Sugere-se que sejam aplicadas, a todos os edifícios do MMT, medidas que assegurem que apenas pessoas autorizadas entram e circulam nas instalações.

Nem todos os equipamentos estão protegidos contra falhas de energia elétrica e alguns edifícios, mais antigos, não estão preparados para ter cablagem que permita uma proteção adequada contra intercetação, interferência ou danos.

As medidas de segurança para ativos que operem fora das dependências do MMT requerem melhorias.

A política mesa limpa e ecrã limpo ainda não foi interiorizada pelos recursos humanos do MMT, pelo que se recomenda uma maior consciencialização para a importância desta temática através da realização de ações de formação interna.

4.8.A.12 - Segurança nas Operações

No MMT esta é uma área em que, em média, os procedimentos de segurança são monitorizados, é mensurada a conformidade com os procedimentos instituídos e são efetuadas melhorias frequentes.

A Informática tem adotado como forma de atuação, sempre que surgem novos procedimentos ou a necessidade de alteração de procedimentos já existentes, a publicação, na intranet e em local de destaque, de manuais de utilização, garantindo assim que todos os utilizadores têm conhecimento imediato dos novos procedimentos.

O *backup* é feito ao longo do dia do servidor instalado no centro de dados do MMT para um servidor que está noutra localização. Ao fim de semana, este servidor cria uma réplica, das cópias de segurança alojadas, para banda magnética. No início da semana seguinte esta réplica é armazenada numa terceira localização segura. Desta forma, são seguidas as melhores práticas de *Disaster Recovery*. Caso ocorram situações de catástrofe ou desastre que tornem o centro de dados indisponível é possível garantir a recuperação dos dados.

4.9.A.13 - Segurança das Comunicações

No MMT existem procedimentos e controlos estabelecidos para manter a Segurança da Informação transferida dentro da organização e com entidades externas.

No entanto, recomenda-se que os acordos de confidencialidade e não divulgação sejam analisados criticamente de forma a que reflitam as necessidades de proteção das informações confidenciais nas relações do MMT com as partes externas e funcionários.

Os acordos de confidencialidade e não divulgação têm como objetivo proteger as informações do MMT e informam os signatários das suas responsabilidades, para proteger, usar e divulgar a informação de forma responsável e autorizada. Pode ser necessária a utilização de diferentes formas de acordos de confidencialidade ou de não divulgação, devendo ser considerados as diretrizes de implementação associada ao controlo A13.2.4.

4.10. A.14 - Aquisição, Desenvolvimento e Manutenção de Sistemas

Como pontos frágeis nesta secção destacam-se os controlos A.14.2.7, A.14.2.8 e A.14.2.9, verificando-se que os testes de segurança e de aceitação efetuados, de uma forma geral, resumem-se ao mínimo necessário para que se possa avançar com a sua utilização.

Relativamente ao desenvolvimento de sistemas por entidades externas (outsourcing) devem ser tidos em conta as diretrizes de implementação do controlo A.14.2.7

No que respeita aos testes de segurança do sistema (A14.2.8) convém que sejam realizados testes de funcionalidades de segurança durante o desenvolvimento de sistemas.

Novos sistemas ou atualizações requerem verificação e testes completos durante o processo de desenvolvimento, incluindo a preparação de um programa de atividade detalhado, com testes de entrada e de saída esperados sob determinadas condições. A abrangência do teste deve ser proporcional à importância e natureza do sistema.

Relativamente aos testes de aceitação de sistemas (A.14.2.9) devem ser efetuados para novos sistemas e novas versões. Devem incluir testes de requisitos de Segurança da Informação (A.14.1.1 e A.14.1.2) e adesão às práticas de desenvolvimento seguro de sistemas (A.14.2.1).

Os testes devem ser realizados em ambiente de teste realístico, de forma a assegurar que os testes são confiáveis e que o sistema não irá introduzir vulnerabilidades no ambiente do MMT.

4.11. A.15 - Relação com Fornecedores

Os controlos, o A.15.1.3 e o A.15.2.1 são os que apresentam maturidade mais baixa, merecendo assim especial atenção.

Relativamente ao controlo A.15.1.3 não existe um procedimento normalizado para aplicar ao fornecimento de produtos e serviços de Tecnologia de Informação e Comunicação. Existe uma preocupação a este nível, mas não havendo um procedimento documentado, que tenha de ser obrigatoriamente seguido, é provável que ocorram falhas.

Sugere-se que, na revisão dos acordos com os fornecedores, sejam tidos em consideração as diretrizes de implementação.

Relativamente à monitorização e análise critica dos serviços fornecidos, controlo A.15.2.1, apesar de existir uma preocupação com este controlo não existe um procedimento documentado e implementado, nem é efetuado em intervalos regulares.

A monitorização e análise crítica dos serviços fornecidos deve garantir que os termos e condições incluídos nos acordos de Segurança da Informação são cumpridos e que os incidentes e problemas de segurança são geridos de forma apropriada.

O relacionamento entre o MMT e os fornecedores devem obedecer a um processo de gestão que permita:

a. monitorizar os níveis de desempenho de serviço para verificar conformidade aos acordos;

b. analisar criticamente os relatórios de serviços produzidos por fornecedores e agendamento de reuniões de progresso conforme requerido pelos acordos;
c. realizar auditorias aos fornecedores, em conjunto com a análise crítica dos relatórios de auditoria independente, quando disponíveis, bem como o acompanhamento das questões identificadas;
d. fornecer informações sobre incidentes de segurança de informação e analisar criticamente tais informações, conforme requerido pelos acordos e por quaisquer procedimentos e diretrizes que os apoiem;
e. analisar criticamente os circuitos de auditoria do fornecedor e registos de eventos de Segurança da Informação, problemas operacionais, falhas, investigação de falhas e interrupções relativas ao serviço entregue;
f. resolver e gerir quaisquer problemas identificados;
g. analisar criticamente os aspetos de Segurança da Informação na relação dos fornecedores com seus próprios fornecedores;
h. garantir que o fornecedor mantém capacidade de serviço suficiente em conjunto com planos de trabalho desenhados para assegurar que os níveis de continuidade do serviço acordados são mantidos, no caso de um desastre ou falha dos serviços principais (A.17).

4.12. A.16 - Gestão de Incidentes de Segurança de Informação

A secção A.16 destaca-se, por ser a secção com classificação mais baixa, encontrando-se abaixo do nível médio de maturidade.

O MMT não possui um documento formal que estabeleça as responsabilidades e os procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas em caso de incidentes de Segurança da Informação. Os procedimentos existem, mas não estão normalizados.

O facto de não existir um documento formal faz com que os controlos incluídos na secção sejam classificados maioritariamente com o nível 2, o que significa que os procedimentos são realizados de forma repetitiva e geralmente sempre pela mesma pessoa, mas não há um processo normalizado.

O primeiro passo para melhorar o nível de maturidade desta secção é a implementação de um procedimento documentado e de seguimento obrigatório, que estabeleça as responsabilidades e os procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas em caso de incidentes de Segurança da Informação, devendo para isso ser consideradas as diretrizes de implementação associadas ao controlo A.16.1.1

4.13. A.17 - Aspetos da Segurança da Informação na Gestão da Continuidade do Negócio

Verifica-se que o MMT tem presente a preocupação de não permitir a interrupção das atividades e proteger os processos críticos contra as consequências de falhas ou desastres significativos, tendo como objetivo o desenvolvimento contínuo de processos com vista à melhoria da proteção dos processos críticos face aos riscos existentes.

Recomenda-se, no entanto, que o MMT defina, documente, implemente e mantenha processos, procedimentos e controlos para assegurar o nível requerido de continuidade para a Segurança da Informação, durante uma situação adversa, devendo para isso assegurar-se que:

a. está implementada uma estrutura de gestão adequada para mitigar e responder a um evento de interrupção, usando pessoal com a necessária autoridade, experiência e competência;
b. o pessoal designado para dar resposta em caso de incidente tem a necessária responsabilidade, autoridade e competência para gerir um incidente e garantir a Segurança da Informação;
c. estejam desenvolvidos e aprovados planos documentados, procedimentos de recuperação e resposta, detalhando como a organização irá gerir um evento de interrupção e como manterá a sua Segurança da Informação num nível pré-determinado, com base nos objetivos de continuidade da Segurança da Informação aprovado pela direção (A.17.1.1).

Em função dos requisitos de continuidade de Segurança da Informação, convém que a organização estabeleça, documente, implemente e mantenha:

a. controlos de Segurança da Informação dentro dos processos de recuperação de desastre ou de continuidade do negócio, procedimentos e ferramentas e sistemas de suporte;
b. processos, procedimentos e mudança de implementação para manter os controlos de Segurança da Informação existentes durante uma situação adversa;
c. controlos compensatórios para os controlos de Segurança da Informação que não possam ser mantidos durante uma situação adversa.

Tendo em conta o controlo A.17.1.3 o MMT deverá ainda verificar, em intervalos regulares, se os controlos definidos e implementados para a continuidade da Segurança da Informação, continuam válidos e eficazes em situações adversas.

4.14. A.18 - Conformidade

O objetivo da secção A.18 é evitar a violação de qualquer lei, estatuto, regulamento ou obrigação contratual relacionadas com a Segurança da Informação e de quaisquer requisitos de segurança.

Para garantir o cumprimento destes requisitos o MMT deverá efetuar a normalização dos processos referidos nas anteriores seções, de forma a que estes se tornem formalmente aceites e de seguimento obrigatório, evitando assim a violação de qualquer lei, estatuto, regulamento ou obrigação contratual relacionadas com a Segurança da Informação e de quaisquer requisitos de segurança.

5. Conclusões

A utilização da ISO/IEC 27002:2013 combinada com um modelo de maturidade constituem uma boa ferramenta de autoavaliação da segurança de Sistemas de Informação.

A análise dos resultados obtidos, demonstram que o MMT possui um nível de maturidade médio geral de 3 o que significa que, em média, os seus procedimentos de segurança estão normalizados, documentados, são divulgados em formação e têm de ser seguidos obrigatoriamente.

No entanto, apesar de os princípios e políticas inerentes à ISO/IEC 27002:2013 serem uma preocupação, verifica-se a falta de normalização de alguns processos, de forma a que estes se tornem formalmente aceites de seguimento obrigatório e divulgados em formação.

A utilização de uma escala de maturidade permitiu de forma simples e direta identificar as áreas que estão abaixo da média (áreas críticas) e que necessitam de melhoria, são elas, A.8 – Gestão de ativos (2,83), A.15 Relação com fornecedores (2,58) e A.16 Gestão de incidentes de Segurança da Informação (2,14). A classificação abaixo da média nestas secções deve-se fundamentalmente ao facto de não existirem procedimentos documentados nestas áreas. Apesar de existir uma preocupação e serem realizados procedimentos, não há um procedimento documentado, que seja de seguimento obrigatório, aumentando a probabilidade de ocorrência falhas.

Os processos informais dão lugar a que nem sempre sejam aplicados, pois não são obrigatórios nem existe um procedimento especifico a seguir, podendo também ocorrer que, para a mesma tarefa, dois funcionários executem procedimentos diferentes, por uma ordem diferente e/ou sem o mesmo rigor, podendo originar vulnerabilidades que podem ser exploradas por ameaças especificas.

A utilização deste método de avaliação proporciona uma visão abrangente de todo o Sistema de Informação, permitindo perceber se os controlos utilizados são os mais adequados e quais necessitam de ser melhorados.

A aplicação, de forma periódica, desta ferramenta permite a melhoria continua dos processos de segurança de informação através da identificação da necessidade de ajustamentos, sempre com o objetivo de melhorar a sua eficiência e eficácia e elevar o grau de maturidade dos Sistemas de Informação do Município.

Os resultados obtidos com esta avaliação podem também ser utilizados como suporte para a tomada de decisões relacionadas com melhorias e investimento necessários para assegurar a Segurança da Informação, bem essencial do Município.

Referências

Beal, A. (2005). *Segurança da Informação: principios e melhores práticas para a proteção dos ativos de informação nas organizações*. São Paulo: Atlas.

Carneiro, A. (2002). Introdução à Segurança dos Sistemas de Informação. Lisboa: FCA.

Carvalho, C. M. (2018). *Segurança e Auditoria em Sistemas de Informação e Comunicação - Implementação numa entidade pública*. Projeto de Mestrado, Universidade da Madeira.

Gouveia, L. B., & Ranito, J. (2004). *Sistemas de Informação de Apoio à Gestão*. Porto: SPI - Sociedade Portuguesa de Inovação.

ISO/IEC 27002:2013. (2013). ISO/IEC 27002 - Information Technology - Security Techniques - Code of Pratice for Information Security - Controls. Standardization, International Organization for Standardization.

Lopes, I. M. (2012). *Adopção de Políticas de segurança de Sistemas de Informação na administração Pública Local em Portugal*. Tese de Doutoramento, Universidade do Minho.

Pedro, J. M. (junho de 2010). *Livro Comemorativo dos 80 Anos da IGF-Autoridade de Auditoria - Sinais de inovação nas metodologias de controlo - Standards internacionais relacionados com o controlo interno na prespectiva dos sistemas de informção* (1.ª ed.). (I. G. Finanças, Ed.)

Trigacheiro, C. F. (02 de 2012). *O impacto das tecnologias de informação na avaliação dos sistemas de controlo interno das organizações*. Instituto Politécnico de Tomar, Escola Superior de Gestão.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 20/10/2021
Aceitação/Acceptance: 13/01/2022

O Código dos Contratos Públicos como instrumento potenciador da economia, eficiência e eficácia nas despesas públicas de segurança em Portugal

Cláudio Lopes[1], Luís Malheiro[2], José Silva[3], Pedro Pereira[4], Luís Ribeiro[5]

lopes.cmr@gnr.pt; malheiro.lcr@gnr.pt; silva.jptr@gnr.pt; pereira.pmc@gnr.pt; ribeiro.lmc@gnr.pt

[1] Guarda Nacional Republicana, Lisboa, Portugal

[2] Centro de Investigação Desenvolvimento e Inovação da Academia Militar, Academia Militar, Instituto Universitário Militar, Rua Gomes Freire, 1669-203, Lisboa, Portugal

[3] Guarda Nacional Republicana, Lisboa, Portugal

[4] Guarda Nacional Republicana, Lisboa, Portugal

[5] Guarda Nacional Republicana, Lisboa, Portugal

Pages: 17-27

Resumo: A gestão de recursos, sejam eles de que natureza forem, são talvez uma das tarefas mais críticas da administração pública, sendo cada vez mais necessário fazer a sua judiciosa administração cumprindo os normativos legais em vigor e observando as práticas de boa gestão. A presente investigação assenta num estudo de caso e consubstancia-se no estudo do Código de Contratação Pública (CCP), na medida em que se tenta perceber de que forma é que as suas disposições e mecanismos previstos, influenciam os princípios da economia, da eficiência e da eficácia na despesa pública na área da segurança. Além de se clarificar e correlacionar cada um dos conceitos referidos, através da análise documental, foram também efetuadas entrevistas a atores chave da função compras de um serviço integrado da área da segurança interna portuguesa, no sentido de colher a sua experiência profissional e os contributos práticos da aplicabilidade do diploma. Estudam-se também as principais vantagens da centralização da aquisição de bens e serviços através de meios eletrónicos de forma a perceber em que medida pode facilitar o procedimento de aquisição. Percebe-se que o mecanismo de gestão e aquisição de bens e serviços deve adotar características de flexibilidade, decorrentes da instituição de segurança e das suas especificidades, mas também decorrentes das especificidades e características do próprio bem ou serviço.

Palavras-chave: Economia; Eficiência; Eficácia; Despesa Pública; Código dos Contratos Públicos

The Public Contracts Code as a tool to enhance economy, efficiency, and effectiveness in public security spending in Portugal

Abstract: The management of resources is perhaps one of the most critical functions of the public administration, demanding a judicious approach that complies with the legal frameworks in place, and in line with management best practices. This investigation is based on a case study and focuses on understanding how the Portuguese Public Contract Code impacts the economy, as well as the efficiency and effectiveness of public expenditure on public safety. Besides clarifying and correlating all the previously referred concepts through documentary analysis, a set of interviews were also conducted with key players responsible for purchase management within the integrated Portuguese safety service, to tap into their professional experience and the practical effects of the diploma. The main advantages of centralizing the purchase of goods and services through electronic support were also objects of study, with the aim of gaining a better understanding of how impactful this could be in terms of facilitating the purchase process. Evidence suggests that the management mechanisms and practices adopted for the purchase of goods and services must be flexible and adaptable not only to the characteristics of the safety service in question but also to characteristics of the goods and services themselves.

Keywords: *Economy, Efficiency, Efficiency, Public expenditure, Public Contracts Code.*

1. Introdução

O estudo da Código dos Contratos Públicos (CCP) como instrumento potenciador da economia, eficiência e eficácia nas despesas públicas obriga em primeira instância a análise dos conceitos estruturantes envolvidos e as suas implicações, como é o caso da economia, eficiência e eficácia. Segundo o art.º 18 da Lei n.º 151/2015, de 11 de setembro, estes princípios são traduzidos em: usar o mínimo de recursos para assegurar os adequados padrões de qualidade do serviço público; fomentar o acréscimo de produtividade pelo alcance de resultados semelhantes com menor despesa e; uso dos recursos mais adequados para atingir o resultado que se pretende. Por outro lado, considerando a opção de se realizar um estudo de caso a uma Força de Segurança (FS) portuguesa, importa sublinhar que esta FS, como entidade adjudicante do Estado no âmbito do CCP, está obrigada a assegurar que tal normativo é cumprido sempre que realiza procedimentos que antecedem a alocação de recursos para suprir uma necessidade pública. Além disso, as necessidades públicas, quesito fundamental para a boa despesa pública, são delimitadas pelo legislador no âmbito do processo orçamental (Magalhães, 2011).

Assim, considerando que a aplicação do CCP e a garantia de economia, eficiência e eficácia são quesitos obrigatórios na realização de despesas públicas, e não opções, parece resultar como evidente que o tema fica limitado à análise do modo como tais quesitos são assegurados. Objetivamente, o tema fica reduzido ao estudo das opções e possibilidades de aplicação do instrumento legislativo (CCP), assegurando a legalidade, mas também maximizando a economia, eficiência e eficácia, sem fazer perigar a missão de uma instituição com características únicas - dimensão, atividade contínua e dispersão territorial.

Nestes termos e face aos conceitos estruturantes envolvidos, o objetivo geral da investigação prende-se com: analisar os principais contributos da aplicação do CCP

em uma FS para incrementar a economia, eficiência e eficácia na despesa pública. Os objetivos específicos são: analisar os principais contributos da aplicação do CCP em uma FS para incrementar a economia na despesa pública; analisar os principais contributos da aplicação do CCP em uma FS para incrementar a eficiência na despesa pública e; analisar os principais contributos da aplicação do CCP em uma FS para incrementar a eficácia na despesa pública.

Nestes termos, considerou-se pertinente delinear a seguinte questão central: quais os principais contributos da aplicação do CCP em uma FS para incrementar a economia, eficiência e eficácia na despesa pública?

Em face de tal problematização, surgem as seguintes questões derivadas: quais os principais contributos da aplicação do CCP em uma FS para incrementar a economia na despesa pública?; quais os principais contributos da aplicação do CCP em uma FS para incrementar a eficiência na despesa pública?; quais os principais contributos da aplicação do CCP em uma FS para incrementar a eficácia na despesa pública?

O estudo da aplicação do CCP em uma FS na atualidade (2019 a 2021), terá por base uma estratégia qualitativa, com um desenho de estudo de caso e recolha de dados com recurso a entrevistas semiestruturas a atores chave da estrutura das compras e áreas relacionadas (tabela 1), além da análise documental. Também no campo da delimitação do estudo, não se ignorando a existência da Lei n.º 30, de 21 de maio (medidas especiais de constatação pública) o foco do trabalho foi o Decreto-Lei n.º 111-B/2017, de 31 de agosto, com as diversas declarações de retificação.

Codificação	Área de funções dos entrevistados
E1	Departamento de Recursos Financeiros
E2	Direção de Recursos Logísticos
E3	Direção de Recursos Logísticos
E4	Departamento de Recursos Humanos

Tabela 1 – Definição de alguns estilos

A investigação organiza-se em quatro capítulos, além da introdução e da conclusão. O primeiro dos quatro diz respeito à abordagem conceptual e os seguintes tratam o debate das pistas existentes na literatura com a informação obtida das fontes primárias e desagregada conforme os objetivos específicos.

2. Abordagem Conceptual

Neste capítulo pretende efetuar-se uma breve abordagem aos conceitos que estão no cerne deste estudo, procurando descrevê-los de forma breve e resumida, com clareza, para, na sequência do trabalho de campo, poderem ser relacionados entre si.

Os princípios da economia, eficiência e eficácia vêm previstos na Lei n.º 151/2015 de 11 de setembro, que aprova a Lei de Enquadramento Orçamental, mais concretamente no art.º 18º do referido diploma. Efetivamente, o art.º 18º começa por determinar, no seu número primeiro, a obrigatoriedade de sujeição aos princípios da economia, eficiência e

eficácia à assunção de compromissos e realização de despesa pelos serviços e entidades pertencentes aos subsectores que constituem o sector das administrações públicas.

O número segundo do art.º 18º define em que se traduzem estes princípios, em três alíneas distintas: utilização do mínimo de recursos que assegurem os adequados padrões de qualidade do serviço público (princípio da economia), alínea a); promoção do acréscimo de produtividade pelo alcance de resultados semelhantes com menor despesa (princípio da eficiência), alínea b); utilização dos recursos mais adequados para atingir o resultado que se pretende alcançar (princípio da eficácia), alínea c).

Podemos inferir que, na realização da despesa pública, a Administração deve usar os mínimos recursos necessários para assegurar os adequados padrões de qualidade do seu serviço, que deve promover o máximo de produtividade da sua ação através da prossecução dos objetivos que competem aos seus diferentes subsectores com o mínimo de despesa possível e ainda a aplicação dos recursos mais aptos para atingir o resultado que é pretendido com a sua ação, em detrimento daqueles forem considerados menos adequados.

Por último, termina o artigo, no seu número terceiro, com a imposição da avaliação dos princípios enumerados nos investimentos públicos, quando os mesmos ultrapassem individualmente os cinco milhões de euros, através de estimativas de incidência orçamental e financeira líquidas ano a ano e globais, sempre que seja possível executar estas estimativas.

Na génese do CCP, estão algumas diretivas europeias anteriores, nomeadamente a diretiva 2004/17/CE do Parlamento Europeu e do Conselho de 31 de março de 2004 e a Diretiva 2004/18/CE do Parlamento Europeu e do Conselho de 31 de março de 2004, relativas, respetivamente, à coordenação dos processos de adjudicação de contratos nos sectores da água, energia, transportes e serviços postais, e à coordenação dos processos de adjudicação dos contratos de empreitada de obras públicas, dos contratos públicos de fornecimento e dos contratos públicos de serviço.

Nessas diretivas surgem pela primeira vez alguns dos princípios que mais tarde o Código de Contratação Pública vai regular e definir com precisão na legislação interna do estado Português, dos quais podemos destacar a necessidade dos estados membros de assegurarem uma abertura real do mercado no âmbito da contratação naqueles serviços específicos e um equilíbrio justo na aplicação das normas de adjudicação dos mesmos, assegurando que haja igualdade de tratamento das entidades adjudicantes que operam no sector público e privado e a obrigação dos estados membros em impedir distorções do mercado causadas pelas participações de proponentes que sejam organismos de direito público em detrimento de proponentes privados; a obrigação dos estados membros em evitar entraves à livre prestação de serviços, permitindo participação de todos os prestadores, quer sejam pessoas singulares ou coletivas; o recurso ao diálogo técnico; a abertura à utilização de técnicas eletrónicas de compras, por permitirem alargar a concorrência e melhorar a eficácia dos contratos, através do ganho de tempo e de economias advenientes da utilização destes sistemas; a necessidade de elaboração de um sistema de aquisição dinâmico (sistemas eletrónicos que possibilitam às entidades adjudicantes consultar um grande número de potenciais fornecedores cujas capacidades foram anteriormente verificadas) para compras de uso corrente e fixação das regras

específicas para a implementação e o funcionamento do mesmo sistema, com intuito de garantir um tratamento equitativo a todos os operadores económicos que dele desejem fazer parte; e a recomendação de serem previstas pelos estados membros disposições em matéria de subcontratação com o fim de favorecer o acesso das pequenas e médias empresas aos concursos públicos.

Os elementos anteriores permitem sublinhar a complexidade e a transversalidade da contratação pública, mas seguramente que saber-se que em 2019 o número de contratos celebrados e reportados foi de 144.226 a que corresponderam 8.860 milhões de euros (Instituto dos Mercados Públicos do Mobiliário e da Construção [IMPIC], 2019), seguramente que reforça o argumento anterior. Deste modo, considerando a preponderância e centralidade do tema, considera-se determinante aprofundar o modo como o código pode ser aplicado em uma FS, cumprindo a legalidade, assegurando a missão e fomentado a criação de valor - traduzido no reforço da economia, eficiência e eficácia.

3. Estudo de caso: a aplicação do CCP em uma FS

A gestão dos recursos financeiros é a atividade que engloba a obtenção de recursos financeiros e a sua aplicação com vista à consecução da missão da FS, com a maior economia, eficiência e eficácia. A gestão financeira da FS, rege-se pelo regime geral da contabilidade pública, que se traduz na disponibilização de créditos orçamentais inscritos no orçamento de Estado, e na competência do dirigente máximo da instituição para autorizar despesas e os seus pagamentos.

No âmbito de uma instituição ímpar como a FS em análise, pela sua dimensão, dispersão e em trabalho continuo, a gestão corrente impõe desconcentração através de delegações e subdelegações de competências, para permitir a prática de atos que integram a atividade financeira que nesta FS se desenvolvem para a prossecução das suas atribuições, conforme constante no Regulamento para a Gestão de Recursos Financeiros da GNR (Despacho n.º 121/11-OG, 2011).

A execução orçamental é a concretização, nos termos da legislação em vigor, dos planos e projetos inseridos no orçamento aprovado, para isso o princípio da prossecução do interesse público é o critério máximo na tomada de decisão.

Concretamente, o princípio da prossecução do interesse público concretiza-se na observância, nomeadamente, da economia, eficiência e eficácia, visando a obtenção do máximo rendimento com o mínimo dispêndio, tendo em conta a utilidade e prioridade da despesa, o acréscimo de produtividade daí decorrentes e o investimento realizado. Esse princípio tem um carácter impositivo nos termos do n.º 1 do art.º 55 do Regulamento Geral do Serviço da GNR, que refere que "o comandante tem em conta e faz sobressair a preocupação da defesa dos interesses da Fazenda Nacional (Despacho n.º 10393/2010, de 05 de maio, 2010).

Sendo o CCP a norma que estabelece a disciplina da contratação pública aplicável à realização dos procedimentos pré-contratuais para a realização de despesa pública, é crucial reforçar o conhecimento sobre as possibilidades, e restrições, de aplicação das diversas normas.

3.1. A aplicação do CCP em uma FS e a economia na despesa pública

No que tange ao princípio da economia, o E1 salienta como principais contributos para o mesmo, a exigência de planeamento prévio ao lançamento ao mercado dos procedimentos pré-contratuais, pois determina um planeamento e priorização das necessidades a suprir, fator essencial para o incremento da economia da despesa pública, o qual deve assentar num desenho das especificações técnicas e critérios de adjudicação mais adequados, para além do contributo associado ao cumprimento de outros princípios consignados no CCP, como são o da concorrência, publicidade e transparência, igualdade de tratamento e não descriminação.

Na opinião de E3 este é o princípio mais potenciado pelo atual CCP, concretamente através do procedimento de obtenção de três orçamentos distintos provenientes de diferentes proponentes, abrindo o processo de aquisição à concorrência do mercado.

A opinião de E4, ainda que num âmbito mais alargado, é semelhante, declarando que a abertura à concorrência, através da abrangência do processo de aquisição a vários operadores económicos, potencia o princípio da economia reduzindo os custos nas aquisições através de seleção do preponente que pratica o menor preço duma ampla variedade de operadores.

O E4 defende ainda que a aplicação correta do CCP, no âmbito procedimental, poupará o empenhamento de recursos no processo, resultando na amplificação do princípio da economia. No entanto, o E4 alerta para a subversão deste princípio quando os processos possuem deficiências técnicas, dando o exemplo do caso de processos que possuem deficientes parâmetros e, dessa forma, impedem o acesso de todo e qualquer operador económico por não conseguir o cumprimento dos mesmos, resultando num processo deserto em termos de propostas, o que obrigará à repetição do procedimento, com os custos decorrente da duplicação da mesma ação.

Relativamente ainda a este princípio, a opinião do E2 é de que é difícil identificar as características do CCP como fator potenciador de um princípio individual, analisado isoladamente, devendo existir uma leitura integrada dos três princípios no uso do CCP.

Nesse sentido, o E2 descreve o CCP como um código vocacionado para a prossecução de várias políticas públicas, enumerando as seguintes: inclusão social, contratação ecológica, fomento da criação de emprego por via da inclusão das pequenas e médias empresas no mercado de contratação pública, desmaterialização de processos e mercado único.

No âmbito do CCP, E2 refere que a análise do contributo do código através dos procedimentos pré-contratuais que o mesmo impõe (ajuste direto, consulta prévia, concurso público, concurso limitado por prévia qualificação, procedimento de negociação, diálogo negocial e parceria para a inovação) para a potencialização dos princípios da economia eficiência e eficácia só pode ser feita mediante análise do contrato em que se inserem e dos propósitos que se pretendem atingir com o mesmo contrato.

No entanto, alerta o E2 que a aptidão do CCP para potenciar os princípios referidos está dependente, em larga medida, do grau de assertividade do plano de necessidades elaborado pela FS, enquanto entidade adjudicante, estando, a montante, a capacidade

de efetuar esse plano condicionado pelas disponibilidades orçamentais atribuídas pelo Orçamento de Estado e pelos documentos que regulam a execução do mesmo.

Além disso, o E2 defende que é uma condicionante para a aplicação do CCP como fator de potenciação dos princípios da Economia, Eficiência e Eficácia, o grau de proficiência detido pelos recursos humanos da FS enquanto entidade adjudicante, na medida em que, enquanto decisores, condicionarão a escolha dos procedimentos pré-contratuais, promovendo a preferência por procedimentos de natureza fechada (ajuste direto/ consultas prévias) em detrimento dos procedimentos abertos à concorrência (concurso público) e de instrumentos procedimentais especiais (Sistemas de Aquisição Dinâmicos).

3.2. A aplicação do CCP em uma FS e a eficiência na despesa pública

A dimensão macroestrutural da FS em análise, impõe uma assertiva, uniforme e transversal capacidade de gestão dos vários recursos materiais que lhe estão confiados e, em especial, daqueles que permitem assegurar a manutenção da atividade operacional e administrativa diária.

Nesse desiderato, é fundamental um instrumento absolutamente dinâmico que garanta a fluidez das necessidades diárias e, em simultâneo, assegure um quadro de boa gestão dos orçamentos, em ordem à aplicação do princípio da boa gestão financeira, ponderando e concretizando operações de aquisição mais assertivas em matéria custo-benefício e legal procedimental, repugnando desperdícios e/ou fenómenos de corrupção financeira (Estorninho, 2013).

É nesta ótica, que o CCP garante a flexibilidade necessária à prossecução de um processo de gestão financeira rigoroso, mas flexível ao ponto de permitir aos decisores nos diferentes patamares, incrementar as melhores soluções caso a caso, com a fluidez e exigência necessárias, com a subjacente capacidade de criar o caminho onde subsista o mínimo de erros.

Entre a definição das necessidades e a efetiva aquisição, existe um percurso de eficiência que importa definir e onde concorrem fatores como a urgência, a disponibilidade orçamental, as necessidades pares (priorização), o volume/quantidade e oscilações dessas mesmas quantidades ao longo do tempo, a necessidade de fornecimento do produto e respetiva disponibilização no mercado a curto, médio ou longo prazo, a gestão dos materiais e opções de aprovisionamento, entre outros fatores que concorrem para este processo, como a própria formação dos elementos que conduzem os processos (Bernardino, 2012).

Se por um lado, tal como refere o E4, a centralização dos procedimentos de aquisição garante a abertura ao mercado dos procedimentos pré contratuais, o que resulta no acesso de mais operadores à satisfação da necessidade de aquisição, por outro lado a proximidade com os possíveis fornecedores garante um conhecimento da qualidade do produto e aumenta o comprometimento em manter essa mesma qualidade, pois fruto da maior proximidade com o órgão que sente a necessidade, conhecimento do mercado local e das soluções existentes, resulta a adoção de mecanismos para escolher a melhor solução.

Tal como aflorado anteriormente, a principal vantagem do CCP é permitir a ampla satisfação das necessidades das organizações públicas, garantindo o acesso à generalidade dos operadores económicos. No caso específico desta FS, se por um lado é fundamental aglutinar as necessidades de aquisições transversais a toda a organização potenciando uma economia de escala, condizente à redução dos custos do produto (ex: aquisição de fardamento, viaturas, armamento, etc); *ad contrário*, constata-se a necessidade de recorrer ao comércio local mediante ajustes diretos, regime geral ou simplificado, geralmente para bens e serviços de menor custo, de desgaste rápido e/ou de necessidade urgente, ou mesmo com especial especificidade, "gozando da liberdade, não apenas de escolher o número de participantes neste procedimento, mas igualmente a identidade desses mesmos participantes" (Pires, 2010, p. 6).

Este é, tal como elucida a E1, o verdadeiro espelho da eficiência do CCP, que mantém o objetivo de garantir o controlo procedimental, a flexibilidade na gestão dos recursos financeiros, a adaptação à disponibilidade do mercado, o respeito pelo princípio da concorrência, da transparência e publicidade, convergindo para a boa gestão dos recursos públicos.

3.3. A aplicação do CCP em uma FS e a eficácia na despesa pública

A eficácia permite conhecer em que razão os resultados conseguidos se aproximam, atingem ou excedem os objetivos programados, traduzindo-se no grau de alcance dos objetivos visados, segundo uma relação de custo/beneficio favorável.

Segundo E3, o CCP é potenciador de eficácia, contudo, indica que para que seja otimizada é necessário reunir os seguintes fatores: profissionalização das compras e a adequação da estrutura que assegura a sua execução, que considera não serem acautelados atualmente, propondo como solução um modelo misto com levantamento de necessidades descentralizado e as restantes etapas centralizadas, modelo que apresenta vantagens na redução de erros.

A opinião de E4 vem no mesmo sentido, mas considera que a aquisição realizada de forma direta, em detrimento de procedimentos pré contratuais previstos na Parte II do CCP, assegurada a legalidade, pode concorrer para atingir o objetivo de um modo mais célere.

No entanto, o E4 também considera que a eficácia enquanto uso dos recursos mais adequados para atingir o resultado que se pretende, é potenciada pela aplicação do CCP uma vez que assiste ao cumprimento de outros princípios como é o exemplo do princípio da transparência.

Relativamente ainda a este princípio, a opinião do E2 é de que é difícil analisar o CCP como fator potenciador de um princípio individual, analisado isoladamente, tendo que ser feita uma leitura integrada dos diversos princípios que resultará leituras diferentes em razão de diversos fatores.

Nomeadamente, qual o propósito que se pretende atingir com um procedimento pré contratual previsto no CCP, ou ainda aferido em razão do critério de adjudicação escolhido pelo órgão competente para a decisão de contratar, pelos aspetos não submetidos à concorrência pelo caderno de encargos, pelas especificações técnicas

constantes no mesmo caderno de encargos, pelo recurso à figura dos lotes, pelo período de vigência do contrato, pela impossibilidade de se renovar o contrato, pela realização, ou não, de consultas preliminares ao mercado.

O entrevistado E2 afirma ainda, e tal como já referido também por E3, que para além dos fatores indicados anteriormente, a assertividade no planeamento das necessidades por parte de uma entidade adjudicante como é o caso da FS em estudo, bem como, o grau de proficiência detido pelos recursos humanos da entidade adjudicante concorrem para potenciar os princípios.

Por seu lado, E1 apresenta uma opinião semelhante aos restantes entrevistados, e acrescenta que para além da proposta economicamente mais vantajosa, usando o critério custo-eficácia, os custos do ciclo de vida e a melhor relação qualidade/preço, deve ser avaliada com base em critérios que incluam aspetos qualitativos, ambientais e /ou sociais ligados ao objeto do contrato público em causa.

A título de exemplo de um planeamento antecipado e impacto na eficácia das aquisições foram identificadas duas aquisições da FS na plataforma de Gestão de Recursos Financeiros em modo Partilhado (GeRFiP) de gás de botija 45kg. A análise evidencia que uma aquisição foi feita de modo agregado ao abrigo de um concurso público (CP N.º 45/DRL/2020 - Aquisição o de gás de botija para a FS para o ano de 2021 - Distrito de Lisboa) permitiu obter um preço unitário de € 54. Este valor contrasta com o valor unitário de € 75,43 para o mesmo bem, a que acresceu o custo do transporte, conseguido com recurso a uma aquisição por ajuste direto em regime simplificado no mercado local. Não se ignorando as eventuais variações de preços que podem ocorrer na matéria prima, estamos perante aquisições de março e de maio de 2021, pelo que tais variações não justificam esta discrepância no custo unitário.

Assim, olhando para a eficácia apenas como garantir o fornecimento de gás para as instalações da FS, ambos os procedimentos atingem o *outcome*. No entanto, se integramos o cumprimento de outros princípios como a transparência e a ampla concorrência, parece resultar como evidente que apenas os procedimentos que não restringem concorrência asseguram a eficácia na sua plenitude.

4. Conclusões

O trabalho desenvolvido teve, essencialmente o objetivo de explicar de forma algo resumida, a forma como o CCP pode ser utilizado como um instrumento potenciador dos princípios da economia, eficiência e eficácia na despesa pública, critérios cuja observação e respeito é uma obrigação e não uma recomendação.

Para isso, foi realizado um breve enquadramento conceptual, com o objetivo de enquadrar e definir conceitos que serão essenciais à compreensão do conteúdo do trabalho, optando-se também por realizar entrevistas a atores chave no processo de compras da FS em análise que têm uma visão prática e muito voltada para o *saber fazer* no campo do tema em estudo.

Na investigação realizada, percebeu-se de forma clara que os procedimentos centralizados e em lote, contribuem de forma decisiva para a maximização da economia, eficácia e

eficiência, até porque maximizam a concorrência entre operadores e reduzem custos inerentes aos processos administrativos de aquisição.

Importa perceber que a FS é uma instituição com especificidades próprias e nem sempre é possível a aquisição centralizada de bens e serviços por motivo quer da dispersão territorial, quer da urgência de ter o bem ou serviço disponível, no entanto, também é possível concluir que os procedimentos não podem ser estanques e que, pese embora o procedimento centralizado seja na generalidade o mais económico e eficiente, nem sempre é o mais eficaz.

Desse ponto de vista, é percetível também que por vezes, contrariando os procedimentos centralizados, existe clara necessidade de recorrer a outros regimes, para suprir necessidades locais, como por exemplo os ajustes diretos (em regime geral ou simplificado), geralmente para aquisição de bens de baixo custo, de desgaste rápido ou cuja sua aquisição é urgente.

A principal vantagem do CCP, é permitir que sejam satisfeitas as necessidades das organizações públicas, estabelecendo critérios para que os processos aquisitivos garantam o acesso à generalidade dos operadores económicos, sendo fundamental para suprir as necessidades logísticas transversais a toda a organização.

Conclui-se que os princípios da economia, eficácia e eficiência são princípios orientadores na realização de qualquer despesa pública e assumem entre si um carácter complementar, sendo essencial respeitar a legislação vigente, nomeadamente o CCP, para que não aconteçam deficiências técnicas nos processos que prejudiquem a prossecução de qualquer um deles.

Cientes de que o tema não se esgota com a presente investigação, existe a convicção de que este estudo representa um primeiro passo no campo da investigação das compras nas FS em Portugal e que poderá ser complementada pela replicação do em outras instituições do espetro da segurança.

Referências

Decreto-Lei n.º 111-B/2017, de 31 de agosto (2017). Procede à nona alteração ao Código dos Contratos Públicos. *Diário da República n.º 168/2017, Série I de 2017-08-31*. Lisboa: Ministério do Planeamento e das Infraestruturas.

Despacho n.º 10393/2010, de 05 de maio. (2010). *Regulamento Geral do Serviço da GNR*. *Diário da República, 2.ª Série, 119, 33856-33891*, Lisboa: Assembleia da República.

Despacho n.º 121/11-OG. (13 de dezembro de 2011). R*egulamento para a Gestão de Recursos Financeiros da Guarda Nacional Republicana*. Lisboa: Guarda Nacional Republicana.

Estorninho, M. J. (2013). *Curso de Direito dos Contratos Públicos - Por Uma Contratação Pública Sustentável*. Almedina.

Gestão de Recursos Financeiros em modo Partilhado. (2015). *Pedido de Compra*. Retirado de https://www.gerfip.gerall.pt/Paginas/News.aspx?nid=45&newsType=1

Instituto dos Mercados Públicos do Mobiliário e da Construção. (2019). *Relatório Anual.* Retirado de https://www.impic.pt/impic/assets/misc/relatorios_dados_estatisticos/RelContratosPublicos_2019.pdf

Lei n.º 151/2015, de 11 de setembro. (2015). *A presente lei aprova a Lei de Enquadramento Orçamental. Diário da República n.º 178/2015, Série I de 2015-09-11*. Lisboa: Assembleia da República.

Magalhães, C. (2011). *Regime Jurídico da Despesa Pública: do direito da despesa*. Tese de Mestrado. Universidade do Minho.

Pires, M. L. (2010). *Âmbito de aplicação da limitação da liberdade de escolha das entidades a convidar para a participação no procedimento de Ajuste Direto*. Coimbra: Cedipre.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 23/12/2021
Aceitação/Acceptance: 15/02/2022

A Igualdade de Género na União Europeia: a implementação da agenda mulheres, paz e segurança

Luís Malheiro[1], Sofia Menezes[2], João Reis[3], Paulo Machado[4], Ana Romão[5], Fernando Bessa[6]

malheiro.lcr@gnr.pt; menezes.sofia@gmail.com; joao.reis@ulusofona.pt; paulo.machado@academiamilitar.pt; anaromao300@gmail.com; a15277@hotmail.com

[1] Centro de Investigação Desenvolvimento e Inovação da Academia Militar, Academia Militar, Instituto Universitário Militar, Rua Gomes Freire, 1669-203, Lisboa, Portugal

[2] Centro de Investigação Desenvolvimento e Inovação da Academia Militar, Academia Militar, Instituto Universitário Militar, Rua Gomes Freire, 1669-203, Lisboa, Portugal

[3] Industrial Engineering and Management, Faculty of Engineering, Lusófona University and EIGeS, Campo Grande, 1749-024 Lisbon, Portugal

[4] Centro de Investigação Desenvolvimento e Inovação da Academia Militar, Academia Militar, Instituto Universitário Militar, Rua Gomes Freire, 1669-203, Lisboa, Portugal

[5] Centro de Investigação Desenvolvimento e Inovação da Academia Militar, Academia Militar, Instituto Universitário Militar, Rua Gomes Freire, 1669-203, Lisboa, Portugal

[6] Centro de Investigação de Estudos de Sociologia, Avenida Forças Armadas 16 - s2, 1600-082 Lisboa, Portugal

Pages: 28-50

Resumo: A presente investigação versa sobre a promoção da igualdade de género nas organizações de segurança da União Europeia. Face à aprendizagem decorrente das ações dos vinte anos da implementação da agenda mulheres, paz e segurança que enfatizam os desafios que subsistem na sua adoção, surgiu a questão que guiou o presente estudo: que fatores influenciam a implementação da agenda mulheres, paz e segurança na União Europeia? O estudo foi materializado na análise dos conceitos estruturantes que permitiram desenhar o modelo analítico criado para dar resposta à lacuna identificada. Em seguida, o estudo foi reforçado pela comparação dos resultados da mensuração de fatores, recolhidos junto de organizações do espectro da segurança da União Europeia, que apresentam diversos níveis de implementação da agenda. A investigação permitiu sublinhar a importância da fase de implementação da agenda, ao nível institucional, para promoção da mudança sendo crucial: explicitar a igualdade nos documentos internos e nos objetivos para o dirigente máximo; estabelecer regras sobre o respeito pela dignidade das mulheres e dos homens no local de trabalho; incluir a perspetiva de género no orçamento e alocar verbas; estabelecer o princípio da não discriminação e a promoção da igualdade nos planos de formação, promovendo a realização de formações; divulgar os direitos e deveres dos trabalhadores sobre igualdade e não discriminação; fomentar políticas sectoriais que reforcem a igualdade; enfatizar a igualdade no planeamento estratégico; e delinear e levar a cabo um plano para implementar a agenda.

Palavras-chave: agenda mulheres, paz e segurança; União Europeia, igualdade de género; implementação; segurança.

Gender Equality in the European Union: the implementation of the women, peace, and security agenda

Abstract: This research focuses on the promotion of gender equality in the security institutions of the European Union. Given the objectives of the Guard's strategy and the learning from the activities of the twenty years of implementation of the women, peace and security agenda that emphasize the challenges that persist after its adoption, the question that guided this study arose: what factors influence the implementation of the women, peace, and security agenda in the European Union? The study was developed through the analysis of the structuring concepts that allowed the analytical model to be created as a response to the identified gap. This study was reinforced by the comparison of the results from data measurements, collected from institutions in the European Union's security spectrum, that commit to different levels of implementation of the agenda. The research has highlighted the importance of the implementation phase of the agenda, at the institutional level, promoting change crucial towards: making equality explicit in internal documents, and in the objectives for the top executive; establishing rules on respecting the dignity of women and men in the workplace; including the gender perspective in the budget and allocating funds; establishing the principle of non-discrimination and the promotion of equality in training plans, promoting training; disseminating the rights and duties of employees on equality and non-discrimination; fostering sectoral policies that reinforce equality; emphasizing equality in strategic planning and having a plan to implement the agenda.

Keywords: women, peace, and security agenda; European Union; Gender equality; implementation; security.

1. Introdução

A procura por um tema atual e relevante, no âmbito da estratégia institucional da Guarda Nacional Republicana em Portugal (GNR, 2021), revelou que um dos tópicos da oitava linha de orientação estratégica está ligada à agenda mulheres, paz e segurança (MPS) e ao impacto desproporcional que os conflitos têm sobre mulheres e crianças.

Face a experiências de investigação anteriores (Malheiro, 2020; Bessa & Malheiro, 2020; Carreiras, Silva, & Malheiro, 2021), tendo por base a experiência e conhecimento já adquiridos, bem como a convicção da pertinência, atualidade e centralidade do tema nas organizações ligadas à segurança, foram selecionados como objetivo central de estudo: avaliar os fatores que influenciam a implementação da agenda MPS na União Europeia (UE). Associado a este objetivo central, foram delineados quatro objetivos específicos com o intuito de analisar o comportamento das variáveis (1) motivação; (2) recursos/ obstáculos; (3) outras políticas; (4) ambiente externo, nos casos em análise.

Do mesmo modo, com o propósito de garantir que os objetivos são atingidos, foi redigida a seguinte questão central: que fatores influenciam a implementação da agenda mulheres, paz e segurança na União Europeia? Paralelamente a pergunta central

também desagregada, sendo identificadas quatro questões derivadas alinhadas com os objetivos específicos nos casos em análise: qual é o comportamento das variáveis (1) motivação; (2) recursos/obstáculos; (3) outras políticas; (4) ambiente externo, nos casos em análise?

Face à problematização, ao conhecimento adquirido na revisão da literatura e do modelo analítico identificado, a hipótese central sugere que: os fatores que influenciam a implementação da agenda MPS decorrem das diferenças existentes nas variáveis motivação, recursos/obstáculos, outras políticas e ambiente externo, dos casos em análise.

Assim, este estudo segue um raciocínio hipotético-dedutivo e uma estratégia mista, baseado num estudo de caso, recolhendo dados, num único momento, com recurso a entrevistas estruturadas (Saunders, Lewis, & Thornhill, 2019).

O estudo está delimitado ao exame da implementação da agenda MPS nas organizações do espectro da segurança dos países da UE, está organizado em duas partes (a ancoragem teórica e os resultados) e foram seguidas orientações metodológicas sugeridas por Santos e Lima (2019).

2. Ancoragem teórica e concetual

Nesta divisão do texto, será abordada toda a ancoragem teórica e concetual da agenda MPS. Inicia com o estudo da igualdade de género e os instrumentos de regulação internacional, segue com a análise no contexto da UE e termina com a explicação do caso nacional e a sua ligação à implementação da agenda pelas organizações.

2.1. A igualdade de género e os instrumentos de regulação internacional

A igualdade, enquanto princípio, consta na Constituição da República Portuguesa (art.º 13.º), desde a versão original de 1976. Desde então, a igualdade de oportunidades e de direitos entre homens e mulheres surge mencionada em diversos documentos que regem a vivência em sociedade, como é o caso da Resolução do Conselho de Ministros n.º 61/2018, de 21 maio. Este diploma, que define a estratégia para a igualdade, referencia muitos outros, desde a Agenda 2030 para o Desenvolvimento Sustentável, à Estratégia do Conselho da Europa para a Igualdade entre Mulheres e Homens 2018-2023, ou o Pacto Europeu para a Igualdade entre Homens e Mulheres 2011-2020.

Esta diversidade de instrumentos, sendo relevante e exemplificativa da importância do tema, também parece colocar em relevo as insuficiências de ações desenvolvidas nos vários domínios, com especial relevância para o da segurança. De facto, considerando que consolidar a igualdade de género nas áreas da segurança não significa eliminar a diferença, mas empoderar pessoas diferentes igualmente (Carreiras *et al.*, 2021), seguramente que ainda não se fez tudo.

Cientes desta realidade, em 2000, o Conselho de Segurança das Nações Unidas (CSNU, 2000) aprovou, por unanimidade, a Resolução 1325 sobre a agenda MPS, que materializa uma das primeiras ações para implementação da igualdade de género no campo da segurança. Este documento, representa o primeiro olhar da Organização das Nações

Unidas (ONU) sobre o impacto do conflito armado na vida de mulheres e crianças e sobre os contributos que as mulheres podem proporcionar para a resolução de conflitos e para a manutenção da paz. Além disso, é afirmada a sub-representação destas nos processos de paz e sublinhada a necessidade de uma participação igualitária, das ações de prevenção até às de pós-conflito. O diploma surge no seguimento de indicadores que relacionavam a igualdade com o desenvolvimento, e na sequência das Conferências Mundiais sobre as Mulheres organizadas pela ONU em Nairobi (1985) e em Pequim (1995), além de outros eventos como: os crimes contra mulheres na ex-Jugoslávia e no Ruanda. Esta Resolução, e as nove que se seguiram, moldaram, e moldam ainda, o pensamento sobre o género na segurança internacional (Barnes & Ikpe, 2011).

Após este primeiro passo, países e organizações de segurança internacionais e regionais desenvolveram esforços para implementar a agenda, criando um conjunto significativo de instrumentos de política (Davies & True, 2019). Uma parte significativa dos membros da ONU tem vindo a implementar Planos Nacionais de Ação (PNA) para fomentar a adoção da agenda MPS, sendo que, em setembro de 2021, noventa e oito países (51% dos membros da ONU) já possuíam um PNA.

Não obstante estas iniciativas, no vigésimo primeiro aniversário da RCSNU 1325, verificou-se que muito do entusiamo inicial não se encontrava traduzido em avanços consolidados. Não se contestando a importância da Resolução, o carácter inovador e o inegável avanço na sensibilização sobre o tema, as avaliações políticas e académicas de amplo espectro convergem e sublinham que o objetivo inicial ainda está longe da sua concretização: igualdade efetiva, e não normativa, entre homens e mulheres (Carreiras, 2006; Olsson & Tejpar, 2009; Organização das Nações Unidas [ONU], 2015).

Os principais desafios apontados prendem-se com: poucos recursos humanos e materiais alocados em exclusividade à implementação da agenda; falta de envolvimento dos dirigentes de topo; documentos de implementação ambíguos; e inexistência de mecanismos de responsabilização (Olsson & Sundström, 2013).

Ainda assim, quer ao nível da ONU, que ao nível de outras organizações como a UE ou a Organização do Tratado do Atlântico Norte (OTAN) surgiram, e continuam a surgir, diversas políticas públicas neste campo. Neste sentido, a próxima secção do texto é dedicada a aprofundar a agenda na UE.

2.2. A agenda Mulheres, Paz e Segurança na União Europeia

O artigo 22º da Carta dos Direitos Fundamentais da União Europeia estabelece que deve ser garantida a igualdade entre mulheres e homens e, tal como em outros domínios, o Tribunal de Justiça da União tem relembrado a necessidade de se respeitar os direitos fundamentais previstos na Carta (Gil, 2021).

Neste sentido, são vários os esforços que se têm vindo a desenvolver, nas mais diversas áreas, para implementar a agenda. Porém, continuam a existir limitações. As principais debilidades da implementação da agenda ao nível europeu foram sintetizadas por Barnes e Ikpe (2011) e por Olsson e Sundström (2013). Como corolário das suas investigações, estes autores sublinham as seguintes debilidades: o risco de a dimensão de proteção ser sobrevalorizada em detrimento da dimensão de participação; a marginalidade da

comprehensive approach e o facto de as preocupações com as questões de género na Política Comum de Segurança e Defesa ser traduzida nos parcos recursos e na ausência de mulheres em posições de destaque; défice de responsabilização pela não implementação; capacidade limitada de envolvimento com parceiros locais, designadamente grupos e redes de mulheres.

Não sendo estas limitações exclusivas da UE, mas os estudos anteriores a sublinham fragilidades requerem que se aprofunde a investigação e se identifique o que foi obtido após a publicação dos resultados.

No seguimento das conclusões do Conselho da União Europeia (2018), sobre a agenda MPS, foi adotada a Abordagem Estratégica da UE para a agenda MPS, sob a coordenação do Serviço Europeu para a Ação Externa. Esta abordagem pretende destacar o forte empenho e esforço da UE na implementação eficaz da Resolução 1325 e fornecer orientações sobre a operacionalização da igualdade de género e do empoderamento das mulheres nas ações externas da UE com base numa abordagem holística. A materialização desta estratégia preconiza quatro pilares: a participação (plena e igualitária, das mulheres em todos os níveis de representação e tomada de decisão); a prevenção (incorporação de uma perspetiva de género e participação das mulheres na prevenção do surgimento de conflitos); a proteção (direitos de proteção específicos para as mulheres e meninas em ambientes de conflito e pós-conflito); a recuperação (acesso a serviços de saúde e aconselhamento para traumas em situações de conflito e pós-conflito).

Neste sentido, dentro das mais variadas missões e operações militares e civis que têm sido implementadas, é evidente o esforço desenvolvido para a efetivação da agenda (Serviço Europeu para a Ação Externa, 2021). Esta procura de efetivação da integração de género em todas as ações e liderança pelo exemplo da promoção da igualdade de género é levada a cabo, por exemplo, na EULEX Kosovo (formação para investigadores da polícia sobre a violência de género e/ou campanhas de sensibilização para denunciar casos de violência sexual); EUCAP Sahel Mali (mulheres no setor de segurança, proteção contra violência e apoio às vítimas) e; EUMM Georgia (patrulhas mistas; recolha de dados desagregados por sexo, relatórios com perspetiva de género, acesso a serviços sobre a violência de género e mulheres em mecanismos de resolução de conflitos).

No entanto, conforme referiu a Gender/WPS Adviser Lina Andeer, da *Civilian Planning and Conduct Capability* do Serviço Europeu para a Ação Externa (2021), no âmbito dos 20 anos da agenda, apenas 24% dos funcionários internacionais são mulheres (em 2007 eram 13%), em operações são apenas 18% e só existe uma mulher a liderar uma missão no terreno.

Face a estes resultados, afigura-se como crucial continuar a monitorizar estas ações, mas importará sobretudo investigar o comportamento da política pública que se encontra em fase de implementação, ou seja, o Plano de Ação da UE sobre Mulheres, Paz e Segurança 2019-2024 (Conselho da União Europeia, 2019). Este plano de ação define um conjunto de iniciativas de curto prazo (até o final de 2020), iniciativas de médio prazo (as pontes entre as ações de curto e longo prazo e que devem ser alcançadas até 2022); e iniciativas de longo prazo que fornecem direção a seguir e definem as prioridades para o trabalho contínuo até 2024. As ações definidas estão alinhadas com os quatro pilares da estratégia da UE (participação, prevenção, proteção e recuperação), sendo ainda apresentados

os responsáveis pelo seu cumprimento. A responsabilidade pelo cumprimento de algumas ações é do Serviço Europeu para a Ação Externa. No entanto, na sua maioria, a responsabilidade recai nos Estados Membros.

Deste modo, sobressai a centralidade dos planos nacionais de ação para a prossecução dos objetivos nacionais, que devem estar alinhados com os objetivos mais globais das organizações de que fazem parte, como, por exemplo, a União Europeia. A próxima secção de texto é dedicada ao estudo do caso nacional que pretende ilustrar, não só o desenho dos planos nacionais de ação, mas também a interpretação que as organizações fazem desses planos e as fragilidades que persistem.

2.3. A adoção da agenda pelas organizações, o caso português

Portugal, não sendo exceção de todas estas dinâmicas, já publicou e implementou três PNA, através das Resoluções do Conselho de Ministros n.º 71/2009, de 25 de agosto; n.º 50/2014, de 26 agosto; e n.º 33/2019, de 15 fevereiro. No entanto, não sendo exceção das dinâmicas de implementação, também não o é no campo dos desafios que persistem à adoção da agenda ao nível institucional (Malheiro, 2020; Bessa & Malheiro, 2020).

Não obstante, continuam a verificar-se limitações em todas as organizações nacionais com responsabilidade pela implementação e a constatar que o nível de adoção da agenda difere entre organizações, sejam elas as Forças Armadas, as Forças e Serviços de Segurança ou outras. De facto, o conjunto de organizações que podem considerar-se centrais na adoção da agenda, apresenta níveis muito díspares nos indicadores relacionados com a tradução da agenda para a prática. Nomeadamente: taxa de feminização (global e dos dirigentes), participação de mulheres em missões no exterior, no âmbito da segurança; ou estruturas dedicadas em permanência a este tema (Meireles, 2018; Direção-Geral de Recursos da Defesa Nacional [DGRDN], 2020; Gabinete do Ministro da Administração Interna [GMAI], 2021).

Conhecem-se algumas variáveis que condicionam os indicadores anteriores, como sendo a entrada tardia das mulheres para as Forças Armadas e Forças de Segurança, bem como a necessidade de permanência de um tempo mínimo num posto hierárquico para ascender ao seguinte. Porém, estes circunstancialismos deveriam afetar de igual modo todas as organizações e tal não se verifica. Por exemplo, a percentagem de mulheres, em 2020, na Polícia de Segurança Pública (PSP) era de 10% (GMAI, 2021) e nas Forças Armadas, no final de 2019, de 12% (DGRDN, 2020), apesar de a PSP ter eliminado as barreiras à entrada vinte anos antes, 1971/72 e 1994/95, respetivamente (Ministério da Administração Interna [MAI], 2014). No entanto, a taxa de feminização da PSP é superior à da GNR, que se situava nos 9% em 2020 (GMAI, 2021). Por outro lado, no Ministério da Defesa Nacional (MDN, 2014; MDN, 2019) já foram criados dois planos para desagregar as medidas do PNA para as Forças Armadas, mas para as Forças de Segurança ainda não existem planos semelhantes. Apesar disso, é importante mencionar que antes da elaboração do primeiro PNA em Portugal, e antes dos respetivos planos setoriais dos ministérios, as Forças Armadas tinham uma taxa de feminização de 14,4% e, dez anos depois, com todas as políticas públicas adotadas, a taxa reduziu para 12% (DGRDN, 2020). Além disto, o Serviço de Estrangeiros e Fronteiras, no ano de 2020, tinha uma taxa de feminização global de 44% e não possuía uma estrutura específica para tratar esta área (GMAI, 2021).

Verifica-se que, mais de vinte anos após a aprovação da Resolução 1325, os desafios que a agenda enfrenta são reais e múltiplos e as respostas existentes não são completas, criando a necessidade de se reforçar o estudo das políticas nacionais, destinadas à sua implementação, para se entender a natureza desses mesmos desafios e adotar as modalidades mais pertinentes para os superar.

Um estudo recente, que dedica atenção às condições e contextos específicos de implementação da agenda a nível institucional (Malheiro, 2020), conclui que existe motivação para implementar a agenda, pese embora o seu estado embrionário. Este estudo ainda sublinha a importância da alocação de recursos em permanência para esta área, a necessidade de incorporar este assunto no planeamento estratégico institucional e a existência de políticas setoriais que fomentem a agenda.

Não obstante a existência do estudo anterior, sabe-se que a atenção dispensada a nível doméstico tem sido menor do que a dirigida ao nível da arena internacional. Muitos dos estudos conduzidos a nível interno centram os esforços de pesquisa na avaliação da implementação dos PNA, frequentemente adotados numa perspetiva burocrática e com base em indicadores quantitativos formais e não em estudos qualitativos aprofundados (Equipa de avaliação externa do II plano, 2018). Não contestando a necessidade da existência de indicadores quantitativos, afigura-se necessário ir mais além e integrar mais informação. Por exemplo, considera-se fundamental aliar o conhecimento sobre os conteúdos programáticos e/ou transferência de conhecimento à simples recolha do número de formandos presentes ou número de sessões sobre a agenda MPS.

Tendo em consideração as políticas fundamentais para promover a mudança, ainda que estas sejam mais motivadas por questões de legitimidade e pressão internacional do que por uma firme convicção de que tais mecanismos afetarão positivamente as organizações, é importante mencionar que são políticas que não se traduzem imediatamente em práticas (Barnes & Ikpe, 2011).

As explicações existentes na literatura sobre os fatores que influenciam a implementação (entrada tardia das mulheres nas organizações, falta de recursos ou inexistência de ligação a documentos estratégicos) não podem ser consideradas satisfatórias, pois não explicam todos os diferentes arranjos das variáveis que as organizações apresentam.

Em tal contexto, torna-se necessário recorrer a modelos analíticos que possibilitem a recolha de informação adicional, primária, com potencial para dirimir a lacuna de conhecimento existente e identificado na pergunta central do estudo. Concretamente, a factualidade de as políticas públicas serem transversais aos diversos países e organizações (Resolução, PNA, políticas setoriais e planos institucionais), obriga a incorporar neste estudo o conhecimento proveniente desta área do saber.

Deste modo, a ferramenta de análise terá de ser selecionada de entre as que permitem examinar as dinâmicas de implementação e avaliação como um todo, sem ignorar as potenciais tensões entre realidade e a narração das políticas públicas (Mota, 2020). Recorrendo à visão de Rocha (2010) sobre a diversidade de modelos, aos estudos sobre a avaliação de políticas públicas (Ferrão e Paixão, 2018) e aos autores mais clássicos (Cohen, March, & Olsen, 1972; Kingdon, 1995; Zahariadis, 1995; Matland, 1995; Fischer, Miller, & Sidney, 2007; Rodrigues & Silva, 2012), ressalta como modelo mais capaz

para a discussão da presente problemática o modelo unificado de inovação (Berry & Berry, 2007).

Berry e Berry (2007) afirmam que a probabilidade de uma medida ser adotada por um Estado (i), num determinado período (t), pode ser determinada pela equação:

$$Adoção_{i,t} = f\ (motivação_{i,t}\ recursos/obstáculos_{i,t}\ outras\ políticas_{i,t}\ ambiente\ externo_{i,t})$$

A variável motivação está associada ao comprometimento dos atores para implementar a medida. Os recursos/obstáculos estudam os impedimentos à inovação; as outras políticas analisam a diversidade de temas que o Estado está a tratar; o ambiente externo visa compreender o posicionamento dos restantes atores. Conforme descrito, apesar de o modelo possuir potencialidades, carece de melhorias, sobretudo por ter sido desenhado para a realidade dos governos estaduais dos Estados Unidos da América. No entanto, considerando que o modelo já foi testado na realidade nacional e no âmbito da política pública em estudo (Malheiro, 2020), afigura-se que também poderá ser replicado para os restantes países europeus, com as devidas adaptações.

Este modelo, depois de replicado, permitiu densificar as variáveis que decorrem do mesmo. No entanto, para obtenção de pistas de respostas consolidadas, será ainda necessário utilizar o método comparado (Oyen, 1990) para examinar os casos em análise: as organizações da área da segurança dos diversos países da UE que integraram o estudo. Assim, depois de se detalhar a metodologia e método na próxima divisão do texto, serão analisados os dados recolhidos.

3. Metodologia e método

O presente estudo, do ponto de vista axiológico é ético, ontologicamente enquadra-se no relativismo e epistemologicamente situa-se no interpretativismo, pois assenta numa determinada visão da sociedade (Easterby-Smith, Thorpe, & Jackson, 2015).

No que concerne ao raciocínio seguido, face à problematização e pistas existentes na literatura, a opção recaiu no método hipotético-dedutivo. De facto, utilizou-se a teoria para construir uma hipótese que foi testada para efetuar generalizações a partir das observações efetuadas (Mill, 1984; Santos & Lima, 2019).

Depois de se escolher e justificar o raciocínio, importa referir a estratégia metodológica. Assim, importa referir que a observação isolada do arranjo das variáveis (motivação, recursos/obstáculos, outras políticas e ambiente externo) de cada caso não permite validar, ou refutar, a hipótese delineada. Deste modo, foi crucial usar o método comparado (Oyen, 1990) para observar o arranjo das variáveis dos casos em análise: as organizações de segurança dos diversos países da UE que participaram no estudo. Objetivamente, utilizou-se o desenho denominado por *the most similar systems*, pois considera-se que os casos em estudo (organizações de segurança dos países da UE) são semelhantes em muitas características, mas diferem no elemento a analisar (implementação da agenda MPS) sendo que os fatores comuns não explicam as diferenças. Nestes termos, face às opções anteriores e à combinação de opções e de dados recolhidos, considera-se que uma estratégia mista é a mais apta para comparar as diferentes variáveis e os vários casos em estudo e garantir a resposta à questão central (Sartori & Morilo, 1991).

No que respeita ao desenho da pesquisa, estamos perante um estudo de caso, na medida que se está a estudar a implementação da agenda MPS, nas diversas organizações ligadas à segurança, nos países da UE (Saunders, Lewis, & Thornhill, 2019). Também é um estudo transversal, uma vez que apenas foram recolhidos dados sobre um determinado caso, num momento temporal único (Santos & Lima, 2019).

A recolha de dados teve por base entrevistas estruturadas, baseadas numa amostragem por caso múltiplo, por homogeneização, porque se está perante a utilização do desenho *the most similar systems*, mas também porque "nos estudos qualitativos de grupos relativamente homogéneos o ponto de saturação é alcançado ao fim de 15 a 20 entrevistas" (Santos & Lima, 2019, p. 71). A identificação dos níveis de implementação, em cada caso, foi efetuada com recurso a uma questão de autodiagnóstico e validada com todos os outros elementos recolhidos.

A utilização deste desenho tem a vantagem de ser modular e permitir a replicação mediante a necessidade do investigador. A aplicação das entrevistas permitiu identificar o estado da arte ao nível da implementação, sendo a comparação dos casos extremos (que ainda não implementaram a agenda / que implementaram a agenda na totalidade) o contributo mais relevante para validação da hipótese.

4. Resultados

Conforme decorre do debate efetuado sobre a ancoragem teórica e concetual, o estudo da igualdade de género na UE, especificamente a implementação da agenda MPS, só pode ser realizado através da recolha de informação junto das organizações com responsabilidades na sua adoção. As próximas divisões analisam os dados que foram recolhidos, com recurso a entrevistas estruturadas, junto de organizações de segurança da UE. Estes dados poderão facultar elementos para densificar o estudo da agenda e reforçar os seus níveis de adoção. A divisão inicia com a caracterização das organizações, seguindo-se o ponto de situação sobre a agenda e os fatores críticos de sucesso na sua adoção, sugeridos pelos entrevistados.

4.1. Caracterização

Foram recolhidos dados junto de vinte e seis organizações de doze países europeus, com uma característica comum: desempenharem missões no espectro da segurança, onde se incluem os três ramos das Forças Armadas, organizações civis e Forças de Segurança (civis e *gendarmeries*). A representação das organizações, por país, é variável e está ligada à capacidade de recolha dos dados (quadro 1).

País	Áustria	Bulgária	República Checa	França	Grécia	Itália	Letónia	Lituânia	Polónia	Portugal	Roménia	Eslováquia
Nº de instituições por país	1	3	1	1	3	1	1	1	6	5	2	1
"Respostas que caracterizam a sua entidade"	Exército	Marinha, instituição militar	Força de Segurança	Exército	Forças Armadas, Força Aérea	Força Aérea	Exército	Instituição militar	Exército, instituição civil, Força Aérea	Força de Segurança, Forças Armadas	Força Aérea, Marinha	Forças Armadas

Quadro 1 – Países e organizações

Através da análise do quadro 1, é possível verificar que a maioria das organizações, que participaram na entrevista são militares. Era expectável que tal acontecesse, devido aos canais que foram utilizados (gabinetes da igualdade de género e gabinetes Erasmus de instituições de ensino superior militar) para solicitar a participação no estudo às diferentes organizações.

Porém, é oportuno que se refira que a reduzida participação no presente estudo, considerando que foi enviado convite de entrevista a cerca de cem entidades, está em consonância com outras investigações que demonstram a falta de atenção para a implementação da agenda MPS, nomeadamente nas Forças de Segurança (Bessa & Malheiro, 2021). Contudo, olhando apenas para o campo das Forças de Segurança, foi possível recolher dados em três países diferentes (República Checa, Polónia e Portugal), os quais poderão ser utilizados em futuros estudos com o objetivo de identificar diferenças/semelhanças neste tipo de organizações de segurança.

Outra informação crucial, no campo da caracterização, prende-se com a autoavaliação do nível de implementação da agenda. O quadro 2 permite identificar que se conseguiu recolher dados em seis organizações onde a agenda se encontra totalmente implementada, em sete organizações que ainda não implementaram a agenda e em 13 onde a agenda foi implementada com limitações, características consideradas fundamentais para comparar e identificar padrões.

Como avalia a implementação da agenda MPS na sua	
Totalmente implementada	**6**
Implementada com limitações	**13**
Não implementada	**7**

Quadro 2 – Autoavaliação do nível de adoção da agenda MPS

Conforme demonstra o quadro 2, para a maioria das organizações, a agenda está "implementada com limitações," apenas seis organizações escolheram a opção "totalmente implementada." Esta implementação limitada, não se afigurando como um fator que afete a fiabilidade da recolha de dados e os resultados globais, obriga a referir que a autoavaliação do nível de execução da agenda pode ser influenciada por diferentes fatores (conhecimento da agenda e transparência nas respostas).

Relativamente ao retrato sociológico dos entrevistados, selecionados pelas organizações para responder à entrevista estruturada, verificou-se que a idade média é de 43 anos e que 58% dos respondentes são mulheres, 38% homens e que 4% respondeu "prefiro não divulgar." Os entrevistados ocupam lugares cimeiros nas organizações: 12% são Diretores-Gerais Adjuntos, 4% Administradores, 35% Chefes de Departamento e 12% Chefes de Unidade. O grau académico acompanha este padrão: 35% possuem o grau de doutor e 58% o grau de mestre. A caracterização dos respondentes (idade, qualificações e posição ocupadas no interior da instituição) permite-nos afirmar que são atores relevantes no processo de implementação da agenda nas suas organizações.

4.2. Realidade institucional

Após a caracterização social, era pedido aos entrevistados que respondessem a um conjunto de questões sobre a situação da instituição no que concerne à implementação da agenda do MPS (quadro 3).

Pela análise do quadro 3, pode-se afirmar que a implementação da agenda é um trabalho em curso, uma vez que alguns fatores básicos ligados à igualdade de género não se encontram completamente implementados nas diferentes organizações. De facto, para os dois últimos fatores, relacionados com a alocação de recursos, é evidente a necessidade de alguma atenção, estando este resultado alinhado com estudos anteriores (ONU, 2015) sobre a implementação da agenda. Por outro lado, apesar de existir um fator que é amplamente adotado nas organizações e que está ligado à formação, constatou-se o mesmo não é transversal a todas as organizações.

Realidade nas instituições	Sim	Não	Não sabe	Não resp.
Os planos de formação incluem o princípio da não discriminação entre mulheres e homens e a promoção da igualdade entre homens e mulheres.	77%	12%	8%	4%
A instituição promove a participação na formação em matéria de igualdade entre mulheres e homens.	65%	15%	15%	4%
A comunicação interna e externa considera o princípio da não discriminação baseada no sexo e na utilização de formas gramaticais neutras.	65%	19%	12%	4%
A promoção da igualdade entre mulheres e homens está incluída nos objetivos do dirigente da instituição.	62%	19%	15%	4%
A igualdade entre mulheres e homens é expressa nos documentos internos.	62%	12%	23%	4%
A instituição elaborou regras sobre o respeito pela dignidade das mulheres e dos homens no local de trabalho.	62%	31%	8%	0%
As políticas sectoriais reforçam o princípio da igualdade entre homens e mulheres.	62%	15%	19%	4%
A instituição incentiva o aumento de homens e mulheres em atividades em que estão sub-representados.	58%	19%	23%	0%
A instituição divulga informação sobre os direitos e deveres dos trabalhadores masculinos e femininos sobre igualdade e não discriminação com base no sexo.	58%	31%	12%	0%
O planeamento estratégico menciona explicitamente a igualdade entre mulheres e homens.	31%	27%	35%	8%
A instituição tem um plano para implementar a agenda MPS.	27%	27%	35%	12%
A instituição incluí a perspetiva de género na elaboração do orçamento.	12%	42%	42%	4%
A instituição aloca uma percentagem do orçamento para a execução de ações relacionadas com a agenda MPS.	8%	46%	38%	8%

Quadro 3 – Realidade organizacional sobre a implementação da agenda MPS

Além do que foi referido, o quadro 3 permite ainda sublinhar a falta de conhecimentos sobre a agenda e/ou os principais conceitos que lhe estão associados. Em 11 organizações (42%), não sabem se a "perspetiva de género na elaboração do orçamento" foi ou não utilizada. Não estando a discutir-se a importância *per se* deste fator específico, será evidente a relevância de se conhecer o estado da arte e os principais termos para se promover alguma mudança.

O quadro 4 ilustra o aprofundamento da análise, comparando-se as organizações que têm a agenda totalmente implementada com aquelas que ainda não a implementaram.

Os resultados demonstram que existe uma ligação entre estes fatores e o nível de implementação da agenda MPS, uma vez que a sua presença de tais fatores é mais

notória nas organizações com a agenda totalmente implementada. Além disso, também volta a sobressair a relevância dos recursos por serem uma realidade nas organizações com a agenda implementada e mais ausentes onde a agenda ainda não foi adotada.

Realidade nas instituições	Totalmente implementada				Não implementada			
	Sim	Não	Não Sabe	Não resp.	Sim	Não	Não Sabe	Não resp.
A Instituição aloca uma percentagem do orçamento para a execução de ações relacionadas com a agenda MPS.	83%	0%	0%	17%	29%	43%	29%	0%
O planeamento estratégico menciona explicitamente a igualdade entre mulheres e homens.	83%	17%	0%	0%	43%	43%	14%	0%
A instituição elaborou regras sobre o respeito pela dignidade das mulheres e dos homens no local de trabalho.	83%	0%	17%	0%	43%	29%	29%	0%
A instituição tem um plano para implementar a agenda do MPS.	67%	17%	17%	0%	29%	43%	29%	0%
A promoção da igualdade entre mulheres e homens está incluída nos objetivos do dirigente da instituição.	67%	0%	17%	17%	57%	43%	0%	0%
A igualdade entre mulheres e homens é expressa nos documentos internos.	67%	0%	17%	17%	43%	43%	14%	0%
As políticas sectoriais reforçam o princípio da igualdade entre homens e mulheres.	67%	17%	17%	0%	29%	57%	14%	0%
A instituição incluí a perspetiva de género na elaboração do orçamento.	50%	0%	33%	17%	29%	29%	43%	0%
A instituição promove a participação na formação em matéria de igualdade entre mulheres e homens.	50%	0%	33%	17%	29%	57%	14%	0%
A comunicação interna e externa considera o princípio da não discriminação baseada no sexo e na utilização de formas gramaticais neutras.	33%	0%	50%	17%	29%	43%	29%	0%
Os planos de formação incluem o princípio da não discriminação entre mulheres e homens e a promoção da igualdade entre homens e mulheres.	33%	0%	33%	33%	14%	43%	43%	0%
A instituição incentiva o aumento de homens e mulheres em atividades em que estão sub-representados.	17%	0%	67%	17%	0%	86%	14%	0%
A instituição divulga informações sobre os direitos e deveres dos trabalhadores masculinos e femininos em termos de igualdade e não discriminação com base no sexo.	0%	17%	67%	17%	14%	71%	14%	0%

Quadro 4 – Realidade das organizações - implementada / não implementada

Uma das questões que importa acompanhar no futuro, pelos impactos que pode vir a proporcionar, prende-se com os resultados relacionados com as opções “não sei” e “não respondo”, sendo a percentagem destas duas opções maior no grupo de organizações com a agenda consolidada.

Relativamente às percentagens globais, as mesmas revelam que a presença de mulheres nas organizações permanece abaixo dos 15%, estando em linha com os resultados de estudos anteriores, com algumas exceções: caso do Serviço de Estrangeiros e Fronteiras onde as mulheres representavam 45% do efetivo do Serviço (Malheiro, 2020). Analisando o desempenho de mulheres e homens com funções de Comandante ou Chefe, constatou-se que cinco organizações reportam menos de 1% de mulheres com estas funções e duas organizações reportam mesmo 0%.

No que diz respeito ao desempenho de tarefas operacionais por mulheres e homens, verificou-se que duas organizações reportam 100% das tarefas desempenhadas por homens, sendo evidente a tendência, neste sentido, nas restantes organizações. Apenas três organizações sublinham que não há discriminação neste domínio e que o equilíbrio é total.

Procurando o "número de participantes em eventos relacionados com a agenda MPS" constata-se que 13 organizações dizem não saber e que 10 indicam menos de oito participantes nestes eventos. Apenas três organizações reportam mais de mil participantes. Resultados semelhantes foram encontrados nas respostas relacionadas com os temas do número de formações sobre a agenda, nos últimos dois anos.

A grande maioria (23 respostas) à questão sobre a percentagem de mulheres candidatas a missões internacionais relacionadas com a prevenção de conflitos são inferiores a 5% ou "não sei". A mesma tendência foi identificada na percentagem de mulheres destacadas para missões internacionais (23 respostas são inferiores a 5% ou "não sei"), o que parece indicar que em algumas das organizações não há a preocupação de recolher dados sobre o tema.

Os principais elementos recolhidos na questão aberta sobre os desafios à implementação da agenda sublinham: a falta de interesse das lideranças, a falta de perceção da relevância do assunto, a falta de motivação, as abordagens erradas e os recursos limitados.

Por último, procurou-se identificar os principais fatores de diferença (superior a 20%) presentes nas organizações que implementaram totalmente a agenda e que não existem nas organizações que ainda não a implementaram na totalidade (quadro 5).

Principais diferenças existentes na realidade nas instituições	Totalmente impl.	Não impl.	Diferença
	Sim	Sim	
A Instituição aloca uma percentagem do orçamento para a execução de ações relacionadas com a agenda MPS.	83%	29%	**55%**
O planeamento estratégico menciona explicitamente a igualdade entre mulheres e homens.	83%	43%	**40%**
A instituição elaborou regras sobre o respeito pela dignidade das mulheres e dos homens no local de trabalho.	83%	43%	**40%**
A instituição tem um plano para implementar a agenda do MPS.	67%	29%	**38%**
As políticas sectoriais reforçam o princípio da igualdade entre homens e mulheres.	67%	29%	**38%**
A igualdade entre mulheres e homens é expressa nos documentos internos.	67%	43%	**24%**
A instituição incluí a perspetiva de género na elaboração do orçamento.	50%	29%	**21%**
A instituição promove a participação na formação em matéria de igualdade entre mulheres e homens.	50%	29%	**21%**

Quadro 5 – Principais fatores de diferença presentes nas organizações

Pela análise do quadro 5, verifica-se que os três fatores que apresentam as maiores diferenças em percentagens são: alocação de recursos orçamentais, inclusão do tema no planeamento estratégico e, elaboração de regras sobre dignidade de mulheres e homens no local de trabalho. No entanto, estas são diferenças que, caso sejam percecionadas pelas chefias das diferentes organizações com a agenda não implementada, poderão ser facilmente colmatadas com a sua inclusão nos planos de implementação da agenda.

4.3. Fatores-chave na implementação

Este subponto baseou-se num conjunto de questões para recolher a experiência das organizações sobre os fatores-chave ligados à implementação da agenda MPS (quadro 6).

Fatores-chave na implementação	Média	ó
Incluir o princípio da não discriminação entre mulheres e homens e a promoção da igualdade entre homens e mulheres nos planos de formação.	3,43	0,71
Mencionar explicitamente a igualdade entre mulheres e homens no planeamento estratégico.	3,35	0,73
Incluir a promoção da igualdade entre mulheres e homens nos objetivos para o dirigente da instituição.	3,35	0,70
Promover a participação na formação sobre a igualdade entre mulheres e homens.	3,29	0,61
Mencionar expressamente a igualdade entre mulheres e homens nos planos e relatórios internos.	3,26	0,61
Divulgar informações sobre os direitos e deveres dos trabalhadores masculinos e femininos em termos de igualdade e não discriminação com base no sexo.	3,26	0,74
Publicar regras escritas sobre respeito e dignidade de mulheres e homens no local de trabalho.	3,25	0,83
Encorajar o aumento de homens e mulheres para atividades em que estão sub-representados.	3,17	0,70
Políticas setoriais que promovam a agenda do MPS.	3,10	0,68
Incluir o princípio da não discriminação baseada no sexo e a utilização de formas gramaticais neutras na comunicação interna e externa.	3,00	0,82
Preparar e implementar um plano de promoção dos objetivos da agenda MPS.	3,00	0,69
Adotar a perspetiva de género da elaboração do orçamento.	2,82	0,78
Atribuir uma percentagem do orçamento para a execução de ações relacionadas com a agenda MPS.	2,79	0,83

Escala: 1= Não é importante; 2=Pouco importante; 3=Importante; 4=Muito importante.

Quadro 6 – Fatores-chave na implementação

A análise do quadro 6 permite identificar que o fator considerado mais relevante na implementação é "incluir o princípio da não discriminação entre mulheres e homens e a promoção da igualdade entre homens e mulheres nos planos de formação." Fatores como: "incluir a promoção da igualdade entre mulheres e homens nos objetivos para o dirigente da instituição" e "mencionar explicitamente a igualdade entre mulheres e homens no planeamento estratégico," também obtiveram pontuações elevadas.

No que concerne aos fatores menos relevantes constata-se que: "atribuir uma percentagem do orçamento para a execução de ações relacionadas com a agenda MPS" e "adotar a perspetiva de género da elaboração do orçamento" obtiveram pontuações baixas.

Saliente-se que nenhum dos fatores recebeu a classificação "não é importante," realidade que valida mais uma vez a ligação entre estas componentes e o nível de adoção da agenda. No entanto, pretende-se aprofundar a análise, de forma a poder contribuir para o desenvolvimento de sociedades mais pacíficas, justas e inclusivas. Tal motivação impulsionou a comparar as organizações com a agenda "totalmente implementada" com as organizações onde a agenda ainda não se encontra implementada (quadro 7).

O primeiro aspeto que sobressai é que os fatores menos importantes ("atribuir uma percentagem do orçamento para a execução de ações relacionadas com a agenda MPS" e "adotar a perspetiva de género da elaboração do orçamento") permanecem iguais nas organizações com a agenda "totalmente implementada" e difere no grupo das organizações com a agenda "não implementada" que apresentam fatores como: políticas setoriais que fomentem a agenda, e encorajar mulheres e homens a ocupar posições

onde estejam sub-representados. No campo dos recursos, é importante sublinhar que foi assinalado na divisão anterior como sendo uma diferença significativa entre estas duas tipologias de organizações e, talvez por isso, não seja tão valorizado pelas organizações onde já é uma realidade (onde as organizações já alocam recursos à implementação da agenda).

Fatores-chave na implementação	Totalmente implementada		Não implementada	
	Média	ó	Média	ó
Incluir o princípio da não discriminação entre mulheres e homens e a promoção da igualdade entre homens e mulheres nos planos de formação.	3,27	0,75	2,94	0,64
Mencionar explicitamente a igualdade entre mulheres e homens no planeamento estratégico.	3,09	0,79	3,24	0,73
Incluir a promoção da igualdade entre mulheres e homens nos objetivos para o dirigente da instituição.	3,08	0,64	2,94	0,64
Promover a participação na formação sobre a igualdade entre mulheres e homens.	3,08	0,76	3,11	0,74
Mencionar expressamente a igualdade entre mulheres e homens nos planos e relatórios internos.	3,00	0,60	3,16	0,59
Divulgar informações sobre os direitos e deveres dos trabalhadores masculinos e femininos em termos de igualdade e não discriminação com base no sexo.	3,00	0,74	2,88	0,83
Encorajar o aumento de homens e mulheres para atividades em que estão sub-representados.	2,91	0,79	2,64	0,72
Publicar regras escritas sobre respeito e dignidade de mulheres e homens no local de trabalho.	2,91	0,67	3,33	0,75
Preparar e implementar um plano de promoção dos objetivos da agenda MPS.	2,83	0,90	3,16	0,87
Políticas setoriais que promovam a agenda do MPS.	2,83	0,69	2,56	0,70
Incluir o princípio da não discriminação baseada no sexo e a utilização de formas gramaticais neutras na comunicação interna e externa.	2,64	0,77	3,06	0,70
Adotar a perspetiva de género da elaboração do orçamento.	2,50	0,67	3,11	0,57
Atribuir uma percentagem do orçamento para a execução de ações relacionadas com a agenda MPS.	2,45	0,66	3,22	0,71

Escala: 1= Não é importante; 2= Pouco importante; 3=Importante; 4=Muito importante.

Quadro 7 – Fatores-chave na implementação - implementada / não implementada

Para as organizações com a agenda "totalmente implementada" as opções e estratégias são bastante claras, uma vez que a média em sete fatores foi inferior a 3 (importante), no caso das organizações onde a agenda ainda não foi implementada existem mais fatores importantes, o que poderá indiciar uma falta de estratégia para a implementação da agenda.

Estes resultados e diferenças ajudam a compreender as consequências das opções a nível institucional, que, neste caso, afastam a agenda MPS das prioridades das organizações.

Seguindo o mesmo raciocínio do quadro 5, no quadro 8 foram identificados os fatores considerados importantes (média superior a 3) para as organizações com a agenda

totalmente implementada, e que não foram considerados importantes (média inferior a 3) para as organizações com a agenda por implementar.

Principais diferenças existentes nos fatores-chave na implementaçã	Totalmente impl.	Não impl.	Diferença
	Média	Média	
Divulgar informações sobre os direitos e deveres dos trabalhadores masculinos e femininos em termos de igualdade e não discriminação com base no sexo.	3,00	2,88	**-0,12**
Incluir a promoção da igualdade entre mulheres e homens nos objetivos para o dirigente da instituição.	3,08	2,94	**-0,14**
Incluir o princípio da não discriminação entre mulheres e homens e a promoção da igualdade entre homens e mulheres nos planos de formação.	3,27	2,94	**-0,33**

Escala: 1= Não é importante; 2= Pouco importante; 3=Importante; 4=Muito importante.

Quadro 8 – Principais diferenças nos fatores-chave na implementação

De modo a refinar a análise e retirar mais dados da experiência dos atores chave na implementação da agenda das organizações europeias, foram colocadas três questões abertas: as três últimas questões da entrevista. Face à diversidade, mas também à riqueza e amplitude de resposta, recorreu-se ao programa *Tree cloud* para gerar nuvens de árvores a partir do texto recolhido: nuvens de palavras que são organizadas em árvore, refletindo a sua proximidade semântica dentro do texto (figura 1).

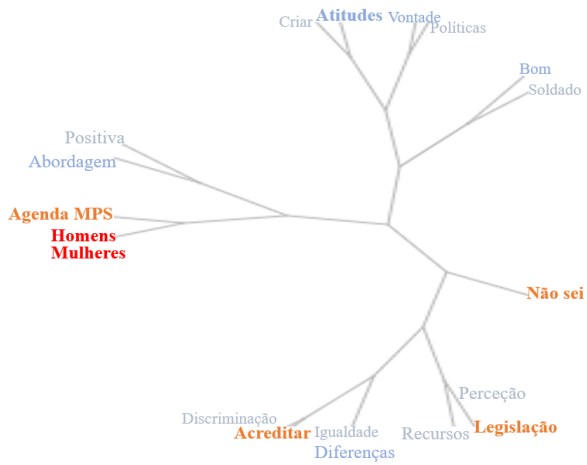


Figura 1 – Análise às questões abertas com recurso ao programa *Tree cloud*.

Esta análise permite identificar a repetição de palavras como acreditar (6 vezes), legislação (5 vezes), ou atitude (4 vezes), fazendo também sobressair o desconhecimento: "não sei"

foi repetido 6 vezes. Não obstante, considera-se que as principais sugestões prendem-se com: integração/alinhamento da agenda com a estratégia institucional; alocar recursos; sensibilização e formação, promover/ bons hábitos e/ou formação/divulgação da agenda; ensinar sobre as diferenças entre géneros e a sua complementaridade, ter uma abordagem positiva da agenda, incrementar a partilha de conhecimento sobre a importância da agenda MPS nas organizações.

As sugestões anteriores podem ajudar a adaptar as políticas ao contexto institucional e aumentar a probabilidade de sucesso (implementar efetivamente a agenda), constituindo-se como uma fonte de informação para quem pretender investigar o tema e contribuindo para uma resposta à questão central, a elaborar na próxima secção do texto.

5. Conclusão

A presente investigação teve como propósito principal dar resposta à questão: que fatores influenciam a implementação da agenda MPS na UE?

A relevância, pertinência e atualidade do tema derivou do seu alinhamento com o plano estratégico da Guarda e, sobretudo, dos testemunhos diários que demonstram a necessidade de existirem sociedades mais justas e mais igualitárias.

Para contribuir para o avanço da área da igualdade de género (crucial para as organizações do arco da segurança) e, simultaneamente, dar resposta à questão central, a investigação dividiu-se em três fases: identificação de lacunas no conhecimento, construção do modelo analítico, e recolha e análise de dados.

A identificação de lacunas no conhecimento baseou-se, sobretudo, em investigações anteriores que assinalavam, por um lado, a importância da fase da implementação em qualquer política pública e, por outro lado, a necessidade de se ampliarem estudos de nível nacional para uma dimensão europeia. Deste modo, a tão necessária e atrasada discussão sobre a articulação do nível da política nacional com o nível mais abaixo (adoção pelas organizações) foi o pano de fundo desta investigação, tendo sido delimitada à análise da implementação da agenda MPS nas organizações da área da segurança nos países da UE.

Considerando a inexistência de respostas cabais na literatura e as sugestões existentes em investigações anteriores, o segundo momento determinante do estudo prendeu-se com o desenho de um modelo analítico. Esta construção foi alicerçada na identificação dos instrumentos de regulação internacional da igualdade, desde as Resoluções do Conselho de Segurança das Nações Unidas, até às ações da UE e da OTAN. Após discussão das conclusões sobre os principais estudos da agenda MPS ao nível global, o foco centrou-se no estudo da agenda na UE, de onde sobressaem três elementos: um dos principais atores chave na coordenação do Plano de Ação da UE sobre MPS (2019-2024) é o Serviço Europeu para a Ação Externa; a estratégia europeia sobre a agenda MPS baseia-se num plano de ação (tal como em 98 países membros da ONU); e a responsabilidade da maioria das ações do plano de ação da UE recai nos Estados Membros. Esta factualidade determinou o detalhe do caso nacional como exemplo do alcance, mas também das limitações dos planos de ação e a importância da implementação a nível institucional. Nesta senda,

foi identificado um modelo de análise das políticas públicas como o mais apto para ser aplicado neste estudo e foram desenvolvidos dois instrumentos: o modelo de análise integrado com os casos e o modo como as variáveis em estudo seriam densificadas com a aplicação de uma entrevista estruturada. Decorrente da problematização, das pistas existentes na literatura e do modelo analítico, também foi avançada a hipótese de que: os fatores que influenciam a implementação da agenda MPS, decorrem das diferenças existentes nos casos em análise nas variáveis motivação, recursos/obstáculos, outras políticas e ambiente externo, dos casos em análise.

Após todo o desenho analítico, o esforço de pesquisa centrou-se na recolha de dados. Assim, foram obtidos dados junto de vinte e seis organizações de doze países europeus, com uma característica comum: desempenharem missões no espectro da segurança, onde se incluem os três ramos das Forças Armadas, organizações civis e Forças de Segurança (civis e *gendarmeries*).

Após o encerramento do período de recolha de dados iniciou-se a análise com o propósito de se caracterizar os respondentes e organizações, mas, sobretudo, recolher informação sobre as duas grandes dimensões da entrevista: realidade da implementação da agenda e visão sobre os fatores críticos de sucesso para a adoção. No que à caracterização dos entrevistados diz respeito, importa sublinhar o elevado nível funcional e as habilitações literárias, elementos que reforçam que os entrevistados, escolhidos pelas organizações, são atores chave no processo. Relativamente à caracterização das entidades, foram recolhidos dados de seis organizações com a agenda totalmente implementada, de sete organizações onde a agenda ainda não está implementada e de 13 organizações onde a agenda foi adotada com limitações.

Esta diversidade de níveis de implementação permitiu identificar as respostas às questões derivadas: (1) qual é o comportamento da variável motivação; (2) recursos/obstáculos; (3) outras políticas; (4) ambiente externo nos casos em análise?) e, ao mesmo tempo, testar a hipótese da investigação.

Neste sentido, os quadros 5 e 8 apresentam os principais fatores de diferença presentes nas organizações e ilustram os principais padrões, tendências e comportamentos das variáveis nos casos em análise que resultam da comparação entre as organizações que implementaram totalmente a agenda com as que ainda não a implementaram. Esta comparação contribuiu para dar resposta às questões derivadas. No entanto, não estando as questões agrupadas por variável, foi desenhado o quadro 9 que transporta a informação para o modelo analítico criado possibilitando responder à questão central do estudo.

Deste modo, os 26 fatores que resultaram das pistas existentes na literatura e que constituíram o modelo analítico, depois de testados, foram reduzidos a 11. Nestes termos, pode afirmar-se que os fatores que influenciam a implementação da agenda MPS na UE são: explicitar a igualdade nos documentos internos e nos objetivos para o dirigente máximo da instituição; estabelecer regras sobre o respeito pela dignidade das mulheres e dos homens no local de trabalho; incluir a perspetiva de género na elaboração do orçamento e alocar uma percentagem para a adoção da agenda; estabelecer o princípio da não discriminação e a promoção da igualdade nos planos de formação, promovendo a participação dos colaboradores neste tipo de formações; divulgar os direitos e deveres

dos trabalhadores sobre igualdade e não discriminação; fomentar a existência de políticas sectoriais que reforcem a igualdade; enfatizar a igualdade no planeamento estratégico; e ter um plano para implementar a agenda.

Realidade institucional	Importância atribuída aos fatores
Motivação	
b. A igualdade entre mulheres e homens é expressa nos documentos internos. d. A instituição elaborou regras sobre o respeito pela dignidade das mulheres e dos homens no local de trabalho.	a. Incluir a promoção da igualdade entre mulheres e homens nos objetivos para o dirigente da instituição.
Recursos/obstáculos	
e. A Instituição aloca uma percentagem do orçamento para a execução de ações relacionadas com a agenda MPS. f. A instituição incluí a perspetiva de género na elaboração do orçamento. h. A instituição promove a participação na formação em matéria de igualdade entre mulheres e homens.	g. Incluir o princípio da não discriminação entre mulheres e homens e a promoção da igualdade entre homens e mulheres nos planos de formação.
Outras políticas	
	j. Divulgar informações sobre os direitos e deveres dos trabalhadores masculinos e femininos em termos de igualdade e não discriminação com base no sexo.
Ambiente externo	
k. As políticas sectoriais reforçam o princípio da igualdade entre homens e mulheres. l. O planeamento estratégico menciona explicitamente a igualdade entre mulheres e homens. m. A instituição tem um plano para implementar a agenda do MPS.	

Quadro 9 – Resposta às questões derivadas

Os resultados obtidos com a presente investigação evidenciam a importância da implementação de políticas ao nível mais baixo (organizações), evidenciado a importância da interpretação institucional das prioridades das políticas de topo, bem como a complexidade de traduzir para a prática o escopo primário da política, *in casu*, a agenda MPS. Neste mesmo sentido, sabendo-se que as medidas de políticas públicas não se traduzem imediatamente em mudanças institucionais, sobretudo se não considerarem o contexto, este estudo evidencia que a existência de políticas concretas é crucial.

Com a convicção de que os principais objetivos da investigação foram alcançados, não se ignora a existência de desafios (*e.g.* limites para a recolha de dados e nível de densificação da análise), motivo pelo qual se reputa como crucial a replicação da investigação a outras organizações europeias, usando este estudo como ponto de partida.

Referências

Barnes, K., & Ikpe, E. (2011). *Women, Peace and Security: Translating Policy into Practice*. New York: Routledge.

Berry, F., & Berry, W. (2007). Innovation and Diffusion Models in Policy Reserarch. Em P. Sabatier, *Theories of the Policy Process* (pp. 223 - 261). Colorado: Westview Press.

Bessa, F., & Malheiro, L. (2020). A Agenda Mulheres, Paz e Segurança: um olhar sobre as Forças de Segurança. *Nação e Defesa, 156,* pp. 123-143.

Carreiras, H. (2006). *Gender and the Military, Women in the Armed Forces of Western Democracies*. London and New York: Routledge.

Carreiras, H., Silva, C., & Malheiro, L. (2021). The impact of UN Women, Peace, and Security agenda on national policies of gender integration in the military. The Portuguese case. *Travail, genre et sociétés*. Manuscrito por publicar.

Centro de Investigação e Desenvolvimento do Instituto Universitário Militar. (2021). *Domínio, Área e Subárea de Investigação*. Retirado de Centro de Investigação e Desenvolvimento do IUM: https://app.ium.pt/cisdi/index.php/pt/investigacao/dominios-areas-e-subareas-de-investigacao

Cohen, M., March, J., & Olsen, J. (1972). *A Garbage Can model of organizational choice*. Oxford: Administrative Science Quarterly.

Conselho da União Europeia. (2018). *Women, Peace and Security - Council conclusions (10 December 2018)* Retirado de: https://www.consilium.europa.eu/media/37412/st15086-en18.pdf

Conselho da União Europeia. (2019). Plano de Ação da UE sobre Mulheres, Paz e Segurança 2019-2024 Retirado de: https://data.consilium.europa.eu/doc/document/ST-11031-2019-INIT/en/pdf

Conselho de Segurança das Nações Unidas. (2000). *Resolution 1325*. Retirado de https://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1325%282000%29

Constituição da República Portuguesa. (1976). *Decreto de aprovação da Constituição*. Diário da República n.º 86/1976, Série I de 1976-04-10. Lisboa: Assembleia Constituinte.

Davies, S., & True, J. (2019). *Oxford Handbook of Women, Peace and Security*. Oxford: Oxford University Press.

Direção-Geral de Recursos da Defesa Nacional. (2020). *As Mulheres e as Forças Armadas: Alguns Desafios de Recrutamento e de Retenção*. Lisboa.

Easterby-Smith, M., Thorpe, R., & Jackson, P. (2015). *Management and Business Research 5th Edition*. London: Sage.

Equipa de avaliação externa do II plano. (2018). *Avaliação externa - II Plano Nacional de Acção para a implementação da RCSNU 1325*. Retirado de https://www.cig.gov.pt/wp-content/uploads/2019/06/Avalia%C3%A7%C3%A3o-PNA-II.pdf

Fischer, F., Miller, G., & Sidney, M. (2007). *Handbook of Public Policy*. USA: CRC Press.

Gabinete do Ministro da Administração Interna. (2021). *Mulheres MAI(S) (2011-2021)*. Retirado de https://www.sg.mai.gov.pt/Documents/MulheresMAI_VF_08_03_2021.pdf

Gil, A. R. (2021). *Estudos sobre Direito da Imigração e do Asilo*. Lisboa: Petrony.

Guarda Nacional Republicana. (2021). *Instrumentos de gestão - Estratégia da Guarda 2025*. Retirado de https://www.gnr.pt/InstrumentosGestao/estrategia_2025.pdf

Kingdon, J. W. (1995). *Alernatives and Public Policies*. London: Longman Classics.

Malheiro, L. (2020). *A questão do género e os instrumentos de regulação internacional: a agenda mulheres paz e segurança na Guarda Nacional Republicana*. Porto: Fronteira do Caos.

Matland, R. (1995). *Synthesizing the Implementation Literature: The Ambiguity-Conflict Model of Policy*. Retirado de file:///C:/Users/malhe/Downloads/JPART95.pdf

Meireles, J. M. (2018). *A integração da perspetiva do género – um modelo para as organizações militares*. Trabalho de Investigação Individual, Curso de Estado-Maior Conjunto. Instituto Universitário Militar, Lisboa.

Mill, J. S. (1984). *Sistema de lógica dedutiva e indutiva*. São Paulo: Abril Cultural.

Ministério da Administração Interna. (2014). *Plano para a Igualdade de Género do MAI (2014-2017)*. Retirado de https://www.cig.gov.pt/wp-content/uploads/2016/01/Plano-de-A%C3%A7%C3%A3o-Setorial-para-a-Igualdade-de-G%C3%A9nero-Minist%C3%A9rio-da-Administra%C3%A7%C3%A3o-Interna.pdf

Ministério da Defesa Nacional. (2014). *Plano de Ação Setorial para a Igualdade - Defesa Nacional e Forças Armadas*. Retirado de https://www.defesa.pt/institucional/ominister io/Documents/IgualdadedoGenero/20140314%20mdn%20PASI%202014_2017.pdf

Ministério da Defesa Nacional. (2019). *Plano Setorial para a Igualdade da Defesa Nacional 2019-2021*. Retirado de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=a654b649-aab0-4e93-8a7e-8105fe344c62

Mota, L. (2020). *Estudos de implementação de políticas públicas: uma revisão de literatura*. Retirado de https://journals.openedition.org/spp/7161

Olsson, L., & Sundström, K. (2013). *European Union's Gender Policy for CSDP Missions: Contents and Gaps*. Retirado de https://fba.se/contentassets/8ed4b9c1a27c4c1dbc20d51172d6e83e/policy-review_eu-gender-policy-for-csdp.pdf

Olsson, L., & Tejpar, J. (2009). O*perational effectiveness and UN Resolution 1325 - Practices and Lessons from Afghanistan. Retirado de* https://www.peacewomen.org/sites/default/files/1325_PracticeLessonsAfghanistan_SDRA_May2009_0.pdf

Organização das Nações Unidas. (2015). *Preventing Conflict, Transforming Justice, Securing the Peace: A Global Study on the Implementation of United Nations Security Council resolution 1325*. Retirado de https://www.peacewomen.org/sites/default/files/UNW-GLOBAL-STUDY-1325-2015%20(1).pdf

Oyen, E. (1990). *Comparative Methodology. Theory and practise in international social research*. London: Sage Publications.

Resolução do Conselho de Ministros n.º 33/2019, 15 de fevereiro. (2019). *III Plano Nacional de Ação para a Implementação da Resolução 1325*. Diário da República, 1.ª série — N.º 33 — 15. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 50/2014, 26 de agosto. (2014). *II Plano Nacional de Ação para a Implementação da Resolução 1325*. Diário da República, 1.ª série N.º 163 — 26. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 61/2018RCM, 21 de maio. (2018). *Estratégia Nacional para a Igualdade e a Não Discriminação 2018 -2030*. Diário da República, 1.ª série — N.º 97 — 21. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 71/2009, 25 de agosto. (2009). *I Plano Nacional de Acção para Implementação da RCSNU 1325*. Diário da República, 1.ª série — N.º 164 — 25. Lisboa: Presidência do Conselho de Ministros.

Rocha, O. J. (2010). *Gestão do Pocesso Político e Políticas Públicas* . Lisboa: Escolar Editora.

Rodrigues, M., & Silva, P. A. (2012). *Políticas Públicas em Portugal*. Lisboa: INCM & ISCTE-IUL.

Sabatier, P. (2007). *Theories of the Policy Process*. Colorado: Westview Press.

Santos, L., & Lima, J. (2019). *Orientaçõesesmetodológicas para a elaboração de trabalhos de investigação (2.ª ed., revista e atualizada)*. Cadernos do IUM. Lisboa: Instituto Universitário Militar.

Sartori, G., & Morilo, L. (1991). *La Comparación en las Ciencias Sociales*. Madrid: Alianza Editorial.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students 8th ed*. Harlow: Pearson Education.

Serviço Europeu para a Ação Externa. (2021). *Military and civilian missions and operations*. Retirado de: https://eeas.europa.eu/topics/military-and-civilian-missions-and-operations/430/military-and-civilian-missions-and-operations_en

Tavares, A. (2019). *Administração pública portuguesa*. Lisboa: Fundação Francisco Manuel dos Santos.

Women's International League of Peace and Freedom. (2021). *1325 National Action Plans (NAPs)*. Retirado de: http://1325naps.peacewomen.org/

Zahariadis, N. (1995). *Markets States and Public Policy*. USA: Michigan.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 11/10/2021
Aceitação/Acceptance: 03/01/2022

Os Diferentes Paradigmas da Administração Pública nas Forças Armadas Portuguesas

Ana Castanho[1], Tiago Gonçalves[2]

l43845@aln.iseg.ulisboa.pt; tiago@iseg.ulisboa.pt

[1] Centro de Investigação e Desenvolvimento do Instituto Universitário Militar (CIDIUM), Rua de Pedrouços, 1449-027, Lisboa, Portugal; ISEG - Lisbon School of Economics & Management, Universidade de Lisboa , Rua Miguel Lupi 20, 1249-078 Lisboa, Portugal

[2] Advance/ CSG; ISEG - Lisbon School of Economics & Management, Universidade de Lisboa, Rua Miguel Lupi 20, 1249-078 Lisboa, Portugal

Pages: 51-64

Resumo: As metodologias administrativas e de gestão públicas evoluíram com base nos três principais paradigmas da administração pública, objetivando uma maior eficiência e eficácia. As Forças Armadas estão sujeitas às reformas do Estado, no entanto, não existe conhecimento quanto ao nível de implementação das mesmas de forma a perceber se as organizações utilizam as novas metodologias. Este artigo visa a realização de um diagnóstico da implementação dos paradigmas *Old Public Administration*, *New Public Management* e *Public Governance* nas Forças Armadas portuguesas através de um questionário realizado aos militares. Primeiro, verifica-se a coexistência dos paradigmas com a predominância das metodologias antigas**,** o que demonstra uma gestão complexa e híbrida. Segundo, de acordo com as funções desempenhadas verificam-se diferentes perceções quanto aos paradigmas implementados. Estes resultados têm implicações ao nível da cidadania, ao nível político e ao nível da gestão.

Palavras-chave: Administração Pública; *Old Public Administration*; *New Public Management*; *Public Governance*; Forças Armadas.

The Different Paradigms of Public Administration in the Portuguese Armed Forces

Abstract: Public administrative and management methodologies evolved based on the three main paradigms of Public Administration aiming at greater efficiency and effectiveness. The Armed Forces are subject to State reforms, however, there is no knowledge as to the level of their implementation to understand whether organizations use the most efficient new methodologies. This article aims the Old Public Administration, New Public Management and Public Governance paradigms implementation diagnoses in the Armed Forces through a survey. Firstly, there is a coexistence of paradigms with a predominance of Old Public Administration methodologies, which demonstrates a complex and hybrid management. Secondly, military personnel with different functions present different perceptions of the

implemented paradigms. These results have implications at the level of citizenship, at the political level and at the management level.

Keywords: Public Administration; Old Public Administration; New Public Management; Public Governance; Armed Forces.

1. Introdução

À semelhança das restantes organizações públicas, as organizações militares estão sujeitas às reformas governamentais que contemplam metodologias distintas da AP (Norheim-Martinsen, 2016). Os desafios das Forças Armadas têm aumentado, mas os recursos disponíveis não acompanham esta tendência (Coutinho, 2021). O exemplo mais recente é o panorama atual da pandemia COVID-19 que levou as Forças Armadas a colaborar na logística de vacinação em Portugal (Coutinho, 2021). Atualmente, uma administração eficiente é crucial para o cumprimento da missão e, apesar do contexto contemporâneo, os estudos no setor da defesa negligenciam a área da gestão (Norheim-Martinsen, 2016).

A Administração Pública (AP) tem evoluído através de diferentes paradigmas administrativos que visam o aumento da eficiência das organizações públicas. Neste estudo são analisados os principais paradigmas da AP denominados *de Old Public Administration* (OPA) (final do século XIX até início dos anos oitenta), *New Public Management* (NPM) (final da década de oitenta até início do século XXI) e *Public Governance* (PG) (Osborne, 2006; Iacovino, Barsanti & Cinquini, 2017), modelo procedente, no âmbito das Forças Armadas portuguesas. Com base no argumento de que as perceções dos trabalhadores dos diferentes níveis de gestão organizacionais são distintas (Brewer & Walker, 2008) a análise é realizada a três níveis de gestão em simultâneo, ou seja, aos gestores de topo, aos gestores intermédios e aos operacionais. É assumido que a decisão dos trabalhadores é baseada na sua perceção, assim, estas podem ser utilizadas como fonte de dados (Mezias & Starbuck, 2003).

Com o intuito de obter um quadro real das práticas de administração e gestão aplicadas no setor da defesa, este artigo visa a realização de um diagnóstico da implementação dos paradigmas da AP nas Forças Armadas. Para concretizar o objetivo apresentado, são colocadas as seguintes questões de investigação: quais são os paradigmas da AP implementados nas Forças Armadas portuguesas? qual a perceção dos paradigmas implementados nos diferentes níveis de gestão?

Foi desenvolvido um questionário com base nas dimensões dos paradigmas apresentadas por Iacovino et al. (2017), e este foi submetido às Forças Armadas portuguesas. O questionário foi respondido por 880 militares.

Os principais resultados do estudo apresentam uma gestão híbrida e complexa nas Forças Armadas, composta pelos três paradigmas com predominância da OPA. Também se identificam diferenças entre as perceções dos militares relativamente aos paradigmas executados e salienta-se que os gestores de topo percecionam mais a utilização dos três paradigmas do que os outros grupos. Estes resultados têm implicações ao nível da cidadania, ao nível político, ao nível da gestão e organizacional.

O artigo apresenta, na secção seguinte a literatura dos três principais paradigmas da AP. Posteriormente, indica a metodologia da investigação e seguidamente, apresenta a análise dos resultados. Por fim, indica as conclusões.

2. Administração Pública

A AP tem evoluído nas últimas décadas através de diferentes paradigmas administrativos que visam o aumento da eficiência das organizações. Os três paradigmas contemplam características próprias de administração e de governação descritas nas seguintes subsecções.

2.1. Old Public Administration

De acordo com Osborne (2006), a Public Administration, ou OPA segundo Iacovino et al. (2017), atingiu o seu ponto alto no Reino Unido na era do estado de bem-estar social, pós 1945 (final do século XIX até início dos anos oitenta). Este seria o instrumento para que o Estado cumprisse com a cidadania e preenchesse as necessidades sociais. A OPA tem na sua génese as ciências políticas e a política pública (Osborne, 2006).

As principais características da OPA são o domínio do Estado de direito (*rule of law*), a administração de regras e diretrizes, a burocracia é fundamental na formulação e implementação de políticas, existe separação entre a política e a administração nas organizações públicas, subsiste o compromisso com o orçamento incremental e surge a hegemonia dos profissionais no âmbito do sistema de prestações de serviços (Osborne, 2006). De acordo com a matriz desenvolvida no estudo de Iacovino et al. (2017), a OPA é burocrática e constituída por regras e procedimentos predeterminados, é um sistema fechado e focado na dinâmica administrativa e na burocracia interna (inadequados ao ambiente externo e é orientada para as normas e procedimentos (a nível micro). Esta tem como dimensões relevantes a legitimidade e a conformidade administrativa com as normas (onde se concentram as atividades de gestão e a avaliação do desempenho), é constituída por relações hierárquicas, apresenta tomadas de decisão específicas e rigorosas. Neste paradigma o Estado é o único provedor dos serviços públicos, o cidadão é visto como um sujeito passivo, o planeamento e controlo são focados nos inputs (especialmente financeiros), a governação é baseada em protocolos e normas e existe confiança na supervisão e a expetativa de que as decisões e tarefas estão bem delineadas (*procedural governance*). No entanto, vários críticos da OPA surgiram, possibilitando o aparecimento e desenvolvimento da NPM. Hughes (1992) refere que os modelos burocráticos formais da OPA demonstram grandes ineficiências relativamente às formas de gestão mais flexíveis presentes na NPM.

2.2. New Public Management

A NPM surgiu na década de oitenta e foi desenvolvida por Hood (1991). Este é um modelo de gestão e administração muito disseminado originário no Reino Unido (quando há data a sua primeira ministra era Margaret Thatcher) e nos EUA, nomeadamente nos governos municipais de Sunnyvale e California, entre outros (Gruening, 2001. De acordo com a *Organisation for Economic Co-operation and Development* [OECD] (1994), a NPM é um esforço de tornar o setor público mais eficiente e competitivo, tornando

a AP mais sensível às necessidades dos cidadãos através da transparência, *value for money* e flexibilidade de escolha. À semelhança das organizações, os governos tiveram de se adaptar às mudanças ambientais e para isso foi necessário ser eficaz, existir uma descentralização, incluir uma orientação para o mercado, para a missão, para os resultados, para os clientes, entre outros (Pyun & Gamassou, 2018).

Osborne (2006) sumariza as características principais da NPM. Osborne refere que na NPM as organizações públicas vão retirar aprendizagens e metodologias ao setor privado, existe um crescimento da prática de gestão e de organizações onde os formuladores de políticas estão organizacionalmente distanciados da implementação de políticas, existe uma liderança empreendedora, enfatiza-se o controlo e avaliação dos inputs e outputs, surgem melhorias da gestão de desempenho e auditoria, dá-se a desagregação dos serviços públicos (até às unidades básicas) e respetiva gestão de custos, surge a utilização dos mercados, contratos e concorrência para prestação de serviços e alocação de recursos dentro dos serviços públicos. Este autor ainda refere que a base teórica da NPM é a teoria da escolha pública/racional e os estudos administrativos. Também Iaconivo et al. (2017) classificou a NPM como tendo uma lógica global focada na gestão e uma lógica de trabalho individualizada a cada AP, um sistema parcialmente fechado (organização orientada para os resultados) que enfatiza as características da gestão da AP (ao nível micro) e as dimensões relevantes centram-se na eficiência, eficácia e economia (três E´s) e no desempenho dos resultados na perspetiva económica e de gestão (onde se concentram as atividades de gestão e a avaliação do desempenho). Estes autores também referem que existe a separação entre o nível político e o nível administrativo, as tomadas de decisão têm em conta determinados critérios que avaliam a eficiência das decisões (existe mais flexibilidade relativamente à OPA), existe fragmentação do sistema da AP e concorrência entre organizações públicas e público-privadas, os clientes têm necessidades e interesses na AP, o planeamento e o controlo são orientados para o output (os sistemas de medição focam-se nos serviços e bens fornecidos ao contrário do foco nos recursos utilizados da OPA) e o modelo de governação (*corporate governance*) considera o reporte e a orçamentação, concentra-se nos outputs e foca-se nos cidadãos.

Apesar da evolução trazida pela NPM este paradigma é criticado. As maiores críticas têm sido realizadas a dois níveis. Por um lado, o facto da NPM num mundo pluralista ter um foco intragovernamental e, por outro, o argumento de que a NPM traz para o setor público técnicas ultrapassadas e inaplicáveis (Metcalfe e Richards (1991) citado por Osborne (2006)).

O modelo PG surge e Bryson, Crosby e Bloomberg (2014) referem que o novo movimento é consequente das ineficiências das abordagens da AP anteriores, mas também de novos desafios, como um mundo em rede onde globalmente existem várias fontes de poder e força.

2.3. Public Governance

Segundo Osborne (2006), no modelo PG as relações entre organizações são enfatizadas e duradouras, e este está ligado à sociologia organizacional e à teoria de rede. Este último paradigma, que surgiu no início do século XXI, contém um estado plural, vários atores interdependentes contribuem para a prestação dos serviços públicos, e um estado pluralista, múltiplos processos informam o sistema de elaboração de políticas

(Osborne, 2006). De acordo com Iacovino et al. (2017) a PG tem uma lógica de eficácia e eficiência focada nos serviços públicos, na formulação de políticas, na democracia e gestão, é um sistema parcialmente aberto (organizações orientadas para as relações e para o ambiente externo estratégico, através de processos de integração e coordenação), engloba a perspetiva micro (cada AP), a meso (AP e os sistemas da organização) e a macro (sistemas económico-sociais) com o foco no exterior, considera como dimensões relevantes os três E´s, a equidade, a transparência, a ética, o aumento da qualidade, a sustentabilidade social e do ambiente na implementação de políticas e a *accountability*, capacita os *stakeholders* internos e externos na elaboração de reportes (onde se concentram as atividades de gestão e a avaliação do desempenho). Este paradigma tenta superar a dicotomia político-gestor através do congraçamento de interesses ao nível administrativo, mantém a tomada de decisão semelhante à NPM (com maior flexibilidade), contém relações externas que têm na sua génese a cooperação entre organizações públicas e privadas, considera que os cidadãos são utilizadores, clientes e recetores ativos de políticas públicas, tem o planeamento e o controlo orientado para o output e o *outcome* (são mensurados objetivos como os outputs dos serviços, os *outcomes*, satisfação, legitimidade e confiança) e o modelo de governação (*Market/Network Governance*) é dirigido para o mercado, contratação externa e ofertas competitivas. No modelo de rede, as organizações públicas criam parcerias estratégicas e realizam ações conjuntas que substituem a concorrência e confidencialidade dos contratos. Bryson et al. (2014) refere que neste novo movimento os valores considerados ultrapassam a eficiência e a eficácia, destacando os valores democráticos, os cidadãos e a cidadania.

2.4. Coexistência dos Paradigmas da Administração Pública

Iacovino et al. (2017) analisa os paradigmas de administração na região italiana da Tuscania através de análise documental e de entrevistas aos gestores de topo e aos formuladores de políticas. Estes autores apresentam dez dimensões que diferenciam os três paradigmas. Iacovino et al. (2017) verifica a coexistência de diferentes lógicas de gestão no mesmo contexto e no mesmo período temporal e verifica que as novas reformas são adicionadas às reformas anteriores através de um processo de estratificação, e que estes três modelos distintos que coexistem no mesmo contexto e no mesmo período temporal fomentam uma gestão híbrida e complexa, onde os elementos dos diferentes modelos se complementam e suplementam (Christensen & Laegreid, 2011). O processo de estratificação é consequência da experiência diversificada dos gestores de topo, dos formuladores de políticas, dos valores presentes nas leis e nos atos regionais e da presença das três lógicas de gestão na mesma perspetiva e dimensão (Iacovino et al., 2017). Também Christensen e Laegreid (2011) analisam os paradigmas da AP através de análise documental e de entrevistas aos líderes políticos e a líderes da Organização Norueguesa do Trabalho e Bem-Estar Social, mas no contexto da reforma da Administração Norueguesa do Bem-Estar Social, e suportam a existência de um processo de estratificação que resulta numa organização híbrida e complexa. Na Nova Zelândia e no Japão a perceção dos cidadãos demonstra uma implementação híbrida dos três paradigmas principais da AP (Goldfinch & Yamamoto, 2018).

Com base na literatura constitui-se a hipótese um: Coexistência de diferentes perceções sobre os paradigmas de gestão executados na mesma AP.

Na análise documental Iacovino et al. (2017) demonstra que as leis e os documentos regionais estão direcionados para a NPM e para a PG (maioritariamente). Paralelamente, os autores analisam dois grupos de trabalhadores e verificam que as expectativas e experiência dos líderes políticos estão direcionados para a NPM e para a PG (maioritariamente) e que a experiência dos gestores de topo demonstra a existência maioritária da OPA e uma minoria de NPM e as suas expectativas são maioritariamente focadas na NPM e em minoria na PG. Existe evidência de que as reformas do Estado não estão totalmente implementadas e, de acordo com Ege (2019), as reformas do Estado nem sempre resultam em mudança e existem mudanças que ocorrem sem uma reforma precedente.

As diferenças encontradas nos grupos por Iacovino et al. (2017) tornam relevante a análise de diferentes grupos e consequentemente a análise por níveis de gestão organizacionais. Também Brewer e Walker (2008) relevam a importância de considerar diferentes grupos hierárquicos e analisam diferentes níveis de autoridade e responsabilidade nas organizações que têm diferentes interpretações do papel e do propósito da organização. No entanto, a maioria dos estudos de gestão foca-se nos níveis superiores da estrutura hierárquica (Brewer & Walker, 2008; Johansen & Hawes, 2016), contudo, existe evidência de que as tarefas dos gestores intermédios são essenciais para o bom desempenho das organizações (Johansen & Hawes, 2016). Os gestores de topo realizam funções de planeamento, de organização (Koontz e Weihrich, 2010) e tomam decisões estratégicas (Damanpour & Schneider, 2006), enquanto que os gestores intermédios empregam muito tempo na supervisão do grupo operacional (Koontz & Weirich, 2010) e tomam decisões operacionais (Damanpour & Schneider, 2006).

Com base na literatura apresentada é desenvolvida a hipótese dois: Coexistência de diferentes perceções sobre os paradigmas de gestão executados em função dos níveis de gestão.

3. Metodologia

De acordo com o artigo 6.º da Lei n.º 6/2014 (2014) a organização das Forças Armadas portuguesas é baseada numa estrutura vertical e hierarquizada, onde os órgãos se relacionam por diferentes níveis de autoridade: hierárquica; funcional, técnica e de coordenação. As Forças Armadas contemplam a Força Aérea, Marinha e Exército (artigo 10º da Lei n.º 6/2014 (2014)). Cada ramo ou organização tem a sua estrutura hierárquica militar, onde se encontram os militares que assumem funções de gestão de topo, funções de gestão intermédia ou funções operacionais.

É aplicado o método quantitativo através de um questionário constituído por questões fechadas às Forças Armadas portuguesas realizado entre dezembro de 2020 e janeiro de 2021. Paralelamente foi realizada análise documental que permitiu um melhor entendimento dos resultados obtidos. Numa primeira fase, o questionário foi construído com base nas dez dimensões dos três paradigmas da AP apresentados por Iacovino et al. (2017). Numa segunda fase, foram realizadas entrevistas semiestruturadas a militares de diferentes níveis de gestão para adaptar o questionário e as respetivas dimensões à amostra do estudo. No questionário é utilizada uma escala de tipo Likert de cinco pontos. As dimensões desenvolvidas no questionário foram sete e são as Relações Externas,

Responsabilização, Orientação dos Sistemas de Planeamento e Controlo (OSPC), Lógica Principal, Relações Internas, Dimensões Relevantes e Tomada de decisão.

O questionário foi difundido através do correio institucional a partir da aplicação Qualtrics, após autorização formal, e os dados recolhidos foram analisados estatisticamente através do programa *Statistical Package for the Social Sciences*, adotando as práticas de analise sugeridas por Pereira e Patrício (2016), e de forma anónima. A consistência interna do questionário é verificada através do Alpha de Cronbach onde se obtém o valor de 0,861, que permite garantir a validade interna boa do questionário, enquanto instrumento de investigação (Pereira & Patrício, 2016). Para a criação do índice de implementação das dimensões dos paradigmas da AP é realizada a análise das dimensões através de tabelas de frequências. Para a comparação das perceções dos militares com diferentes níveis de gestão relativamente às dimensões da AP utilizadas são realizadas tabelas de cruzamento e o teste não paramétrico Kruskal-Wallis (KW).

4. Análise de Resultados

Foram obtidas 880 respostas no questionário, das quais 23,3% da Força Aérea, 49,4% do Exército e 27,3% da Marinha. Dos respondentes, 83,5% são do sexo masculino, 80,9% tem idade entre os 31 e os 60 anos e, relativamente às habilitações literárias, 31,4% apresenta mestrado, 28,8% apresenta licenciatura e 35,1% o ensino secundário. Quanto ao nível de gestão, dos inquiridos 116 assumem funções de gestão de topo (inclui os que assumem funções de gestão de topo e intermédia), 276 assumem funções de gestão intermédia e 488 assumem outras funções, que representam as funções operacionais.

Face ao quantitativo das Forças Armadas, as respostas obtidas constatam uma representação significativa, superior a 20% de taxa de resposta, dos indivíduos em funções de gestão de topo e intermédia localizados em território nacional. Com base no Decreto-Lei n.º 4 de 2020 e na informação disponibilizada pelas organizações, os gestores de topo e os gestores intermédios totalizam aproximadamente 443 e 1237 militares respetivamente, o que corresponde a uma taxa de resposta de 26% e de 22%.

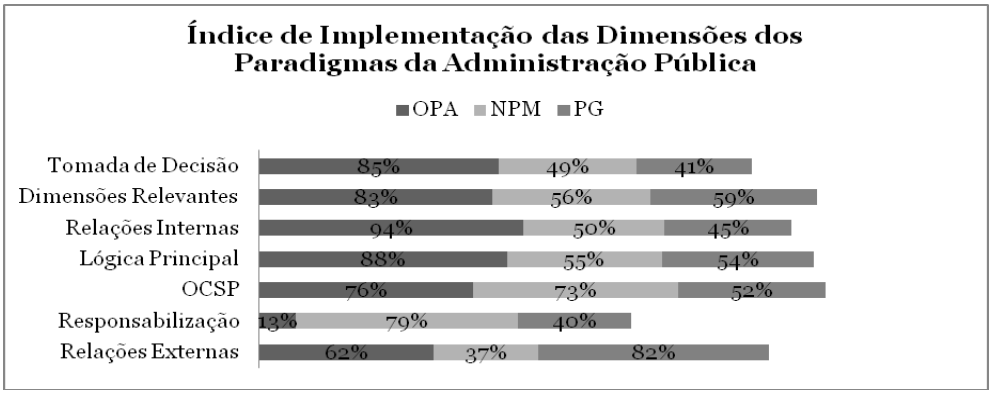


Figura 1 – Índice de implementação dos paradigmas da Administração Pública e respetivas dimensões

A partir da informação consolidada da percentagem de inquiridos das Forças Armadas que de acordo com a sua perceção concordam e concordam totalmente com a existência de determinada dimensão e paradigma na sua organização é desenvolvido o índice de implementação dos paradigmas da AP e respetivas dimensões apresentado na Figura 1. A análise dos paradigmas e respetivas dimensões realizada através de tabelas de frequências e percentagens pode ser disponibilizada pelos autores.

Relativamente aos paradigmas dominantes nas dimensões verifica-se que existe uma perceção generalizada de que as relações externas com organismos públicos e privados são maioritariamente de cooperação e não de concorrência. Maioritariamente, as organizações são responsáveis e têm em consideração a satisfação dos interesses e necessidades do cidadão público, e menos de metade dos inquiridos perceciona a existência de um diálogo entre a sua organização e o cidadão público que objetiva questionar, explicar e justificar. O controlo e planeamento incidem frequentemente nos recursos utilizados e nos outputs (menor incidência nos *outcomes*), a gestão é baseada principalmente na legislação, nos normativos e é burocrática (a eficiência interna organizacional e a eficiência e eficácia do sistema a que pertence a organização não é prioritária face à legislação). As relações internas são estritamente hierárquicas e aproximadamente metade dos inquiridos perceciona que existe a separação entre o nível político e administrativo, e uma parcela menor concorda com a existência de tentativa de conciliar os interesses ao nível do administrador. As atividades de gestão e a avaliação do desempenho têm como princípios maioritários a legitimidade e a conformidade administrativa com as regras (os três E´s e outros aspetos qualitativos como a ética, transparência e sustentabilidade não são prioritários face ao cumprimento das normas). A tomada de decisão parece ser estrita e específica a determinados intervenientes, e menos de metade dos inquiridos concorda com a existência de critérios definidos para avaliação da eficiência das decisões e com a tomada de decisão ser flexível e adaptável às intervenções da área administrativa.

Apesar do paradigma PG estar presente em todas as dimensões, e dado o índice de implementação obtido na Figura 1, pode-se afirmar que as antigas ideologias da AP estão fortemente enraizadas nas Forças Armadas portuguesas. Os valores do Alpha de Cronbach obtidos demonstram que a gestão híbrida e complexa verificada faz com que a consistência interna das respostas obtidas diminua com os paradigmas mais antigos, subterrados pelas novas ideologias, o que contribui para as distintas perceções. Deste modo, a hipótese um é verificada.

Estes resultados reforçam os estudos de Iacovino et al. (2017), de Christensen e Laegreid (2011) e de Goldfinch e Yamamoto (2018) ao demonstrar a coexistência de diferentes paradigmas de administração nas diferentes dimensões e no mesmo contexto e período temporal, resultando numa gestão híbrida e complexa, no entanto, estendem a literatura para o contexto das Forças Armadas. Acresce que este estudo, ao contrário de Iacovino et al. (2017) e de Christensen e Laegreid (2011), não contempla análise das reformas, e foca-se nas práticas e metodologias utilizadas nas organizações, dado que as reformas do Estado nem sempre resultam em mudança e existem mudanças que ocorrem sem uma reforma precedente (Ege, 2019). Estes resultados sugerem que a mudança de práticas de gestão menos modernas para práticas recentes nas Forças Armadas não é simples e consequentemente parece existir a utilização de diferentes métodos de gestão para âmbitos semelhantes. Os novos desafios das Forças Armadas

portuguesas, como o combate a incêndios com um número de militares insuficiente (Diário de Notícias, 2018) e mais recentemente o combate à COVID-19 (Coutinho, 2021), aumentam o consumo dos recursos disponíveis escassos (Coutinho, 2021). Este panorama pressupõe uma maior eficiência na gestão dos recursos e também um maior envolvimento com o cidadão público presentes nas metodologias NPM e PG (Iacovino et al., 2017; Bryson et al., 2014).

Os resultados obtidos e a realidade atual diversificada das Forças Armadas pode dificultar a utilização de práticas e metodologias de gestão mais recentes que contribuem para a eficiência, eficácia, democracia e cidadania. Os resultados trazem implicações para a cidadania, pois não existe participação do cidadão público na tomada de decisão das organizações militares. Salienta-se que a participação do cidadão é necessária para uma gestão inteligente, no entanto, a participação real do cidadão nem sempre é promovida e varia com a cultura administrativa do país (Bolívar, 2018).

Estes resultados também têm implicações ao nível político. É subentendido que não é suficiente normalizar as novas metodologias de gestão e administração pública para que as mesmas se apliquem. São necessárias sugestões, modelos e abordagens operacionais que permitam a correta implementação das normas. No entanto, independentemente das reformas políticas podem existir mudanças de gestão nas organizações (Ege, 2019) consequentes das normas internas ou da experiência dos gestores (Iacovino et al., 2017).

A Tabela 1 apresenta a % dos militares, por nível de gestão, que concordam e concordam totalmente com os paradigmas das sete dimensões, e apresenta o teste KW que indica as diferenças estatisticamente significativas das perceções dos paradigmas implementados, por dimensão, entre os três grupos.

Dimensão	**Nível de gestão e teste KW**	**Paradigmas**		
		OPA	**NPM**	**PG**
Relações Externas (1)	Gestores de topo	62%	40%	92%
	Gestores Intermédios	63%	41%	86%
	Operacionais	61%	34%	77%
	H de KW	1,163	5,097*; 0,505	19,440***
Responsabilização	Gestores de topo	10%	91%	47%
	Gestores Intermédios	12%	84%	43%
	Operacionais	15%	72%	37%
	H de KW	8,116**	21,945***	5,365*
OSPC	Gestores de topo	84%	83%	59%
	Gestores Intermédios	81%	76%	51%
	Operacionais	71%	68%	51%
	H de KW	33,331***	19,130***	2,687

Dimensão	Nível de gestão e teste KW	Paradigmas		
		OPA	NPM	PG
Lógica Principal	Gestores de topo	91%	64%	61%
	Gestores Intermédios	91%	62%	59%
	Operacionais	86%	49%	50%
	H de KW	4,379	9,303**	6,133**
Relações Internas	Gestores de topo	92%	62%	54%
	Gestores Intermédios	97%	55%	45%
	Operacionais	92%	44%	43%
	H de KW	6,020**	12,533***	2,567
Dimensões Relevantes	Gestores de topo	91%	64%	75%
	Gestores Intermédios	89%	59%	63%
	Operacionais	78%	52%	53%
	H de KW	28,073***	5,326*	25,329***
Tomada de Decisão	Gestores de topo	87%	55%	53%
	Gestores Intermédios	87%	51%	46%
	Operacionais	83%	47%	35%
	H de KW	0,45	2,491	14,938***

Teste KW: *** p < 0,01; ** p < 0,05; * p < 0,1
(1) A frequência da NPM é a média dos dois itens da dimensão relações externas e paradigma NPM.

Tabela 1 – Cruzamento entre o nível de gestão e as dimensões dos paradigmas da Administração Pública e o teste *Kruskal-Wallis*

Verifica-se através das % e do teste KW apresentados na Tabela 1 que as perceções dos militares com diferentes níveis de gestão sobre a execução dos paradigmas por dimensão nas Forças Armadas têm diferenças, e que em todas as dimensões existe pelo menos um paradigma onde existem diferenças significativas. A perceção dos militares com funções de gestão de topo é a de que o paradigma dominante por dimensão é a OPA seguindo-se maioritariamente a NPM, exceto nas dimensões Relações Externas e Responsabilização. Apesar das % serem diferentes, o paradigma dominante identificado por dimensão é igual para os três níveis de gestão. Também é identificada uma diminuição da perceção da utilização das práticas do paradigma PG ao longo da descida na hierarquia organizacional, exceto na dimensão OSCP. Dada a coexistência de diferentes perceções nos três níveis de gestão a hipótese dois é verificada.

Os dados da Tabela 1 reforçam os resultados identificados por Iacovino et al. (2017), ou seja, a perceção dos gestores de topo demonstra a existência maioritária da OPA e uma minoria de NPM e existem diferenças nas perceções dos grupos analisados. Estes dados também reforçam o argumento utilizado em Brewer e Walker (2008) de que diferentes

grupos hierárquicos têm diferentes atitudes e perceções sobre a organização, no entanto, ampliam a literatura para o contexto das Forças Armadas.

A gestão híbrida e complexa verificada, bem como as diferentes perceções dos militares identificadas, em função dos níveis de gestão, podem significar que existem dificuldades na adoção dos novos paradigmas da AP e, consequentemente, que existem problemas ou condicionantes ao nível da mudança organizacional na administração nas Forças Armadas. De acordo com os resultados, os diferentes níveis de gestão ou grupos hierárquicos não estão totalmente alinhados relativamente à perceção da utilização das práticas PG. Os gestores de topo percecionam mais a utilização das metodologias mais recentes, no entanto, os gestores intermédios e os operacionais não têm esta perceção. Este resultado pode evidenciar que existe uma mudança estratégica, relativamente às práticas de gestão utilizadas nas Forças Armadas, que não é percecionada nem executada pelos níveis hierárquicos inferiores e que pode ser consequente do nível de burocracia e da estrutura rígida e hierárquica identificada.

Salienta-se também que os gestores de topo são o grupo que percentualmente e maioritariamente perceciona mais a utilização dos três paradigmas. Este resultado demonstra que a perceção da utilização simultânea dos três paradigmas é mais complexa no nível hierárquico superior e que esta complexidade diminui com a descida na estrutura hierárquica. A visão complexa dos gestores de topo pode advir da sua experiência diversificada, dos formuladores de políticas, dos valores presentes nas leis e normas (Iacovino et al., 2017). Os gestores de topo nas Forças Armadas encontram-se maioritariamente no final de carreira e assumem posições de comando e liderança, de tomada de decisão estratégica e têm acesso à maioria da informação.

As diferentes perceções nos diferentes níveis de gestão sobre a utilização das práticas de gestão pode ser um constrangimento para a mudança de gestão nas Forças Armadas. O paradigma PG é mais percecionado pelos gestores de topo e tem um decréscimo à medida que se desce na estrutura hierárquica, o que pode trazer implicações ao nível da gestão da mudança de metodologias, como implicações na execução do alinhamento estratégico organizacional e nos regulamentos internos.

5. Conclusão

Este trabalho visa a criação de um quadro real das práticas de administração e gestão aplicadas no setor da defesa. Para cumprir este objetivo é desenvolvido um questionário para perceber quais os paradigmas da AP implementados nas Forças Armadas e qual a perceção dos paradigmas da AP implementados nos diferentes níveis de gestão. Foram obtidas 880 respostas do universo das Forças Armadas.

Conclui-se que as Forças Armadas apresentam uma gestão híbrida e complexa, todavia, o paradigma PG é o menos proeminente e o OPA é o predominante o que demonstra que as antigas ideologias da AP estão fortemente enraizadas. Salienta-se que as Forças Armadas têm relações externas maioritariamente de cooperação, preocupam-se com a satisfação dos interesses e necessidades do cidadão público, fazem um controlo e planeamento dos recursos utilizados e dos *outputs*, têm a legislação, os normativos e a burocracia como base de gestão, têm relações internas estritamente hierárquicas, têm os princípios da legitimidade e conformidade administrativa com as regras como

base das atividades de gestão e da avaliação de desempenho e a tomada de decisão é maioritariamente específica e estrita a determinados intervenientes. A base da gestão centrada nas normas e regulamentos, a burocracia e a tomada de decisão estrita são espelhadas na literatura como práticas ineficientes que não coadunam com os desafios atuais das Forças Armadas, no entanto, salienta-se a forte cooperação externa que pode ser inerente à missão militar.

Também é identificada a existência de diferentes perceções sobre os paradigmas de gestão executados entre os níveis de gestão. Contudo, todos os militares percecionam a dominância da OPA na maioria das dimensões o que demonstra a forte implementação das metodologias antigas. Salienta-se que os níveis hierárquicos superiores percecionam mais a utilização do paradigma PG e que esta perceção diminui à medida que se desce na estrutura hierárquica. Esta facto demonstra que a estrutura hierárquica não está alinhada relativamente às metodologias de gestão utilizadas o que pode contribuir para a gestão híbrida e complexa. Também se pode deduzir que as mudanças nas práticas de gestão provocadas pelos gestores de topo ou pelos normativos não estão bem implementadas, assim, o investimento na melhoria da gestão da mudança de metodologias seria pertinente. Evidencia-se também que os gestores de topo percecionam mais todos os paradigmas e esta complexidade diminui com a descida na estrutura hierárquica, o que se pode dever à elevada experiência no final de carreira dos militares.

Este trabalho contribui para a literatura em diversos aspetos. Primeiro, reforça a gestão híbrida e complexa identificada nos organismos públicos (Iacovino et al., 2017; Christensen & Laegreid, 2011; Goldfinch & Yamamoto, 2018).

Segundo, é o primeiro trabalho que analisa os três paradigmas da AP nas Forças Armadas que são distintas da restante função pública, essencialmente na sua estrutura (artigo 10º da Lei n.º 6/2014 (2014)) e valores, e são pouco estudadas na área da gestão (Norheim-Martinsen, 2016).

Terceiro, à semelhança de Brewer e Walker (2008) argumenta que diferentes níveis de gestão têm diferentes atitudes e perceções das organizações e estende a literatura existente através da análise dos paradigmas da AP realizada a três níveis de gestão organizacional em simultâneo.

Neste estudo são apresentadas possíveis condicionantes da implementação dos paradigmas da AP nas Forças Armadas. No entanto, as Forças Armadas podem conter diferentes condicionantes da implementação das metodologias dos paradigmas por explorar e identificar. Também as diferentes perceções necessitam de uma análise mais profunda, nomeadamente através de uma análise qualitativa.

Referências

Bolivar, M. P. R. (2018). Creative citizenship: the new wave for collaborative environments in smart cities. *Academia revista latinoamericana de administración*, 31(1), 277-302.

Brewer, G. A., & Walker, R. M. (2010). The impact of red tape on governmental performance: An empirical analysis. *Journal of Public Administration Research and Theory*, 20(1), 233-257.

Bryson, J. M., Crosby, B. C., & Bloomberg, L. (2014). Public value governance: Moving beyond traditional public administration and the new public management. *Public Administration Review,* 74(4), 445-456.

Christensen, T., & Lægreid, P. (2011). Complexity and hybrid public administration—theoretical and empirical challenges. *Public Organization Review*, 11(4), 407-423.

Coutinho, P. (2021). *A propósito da covid-19, repensar as Forças Armadas*. https://www.publico.pt/2021/02/05/opiniao/noticia/proposito-covid19-repensar-forcas-armadas-1949306

Decreto-Lei n.º 4/2020 (2020). Diário da República n.º 31, série I de 2020-02-13. https://dre.pt/dre/detalhe/decreto-lei/4-2020-129160712

Diário de Notícias (2018). *Força Aérea quer mais efetivos para nova missão de combate aos fogos*. https://www.dn.pt/portugal/forca-aerea-quer-mais-efetivos-para-nova-missao-de-combate-a-incendios-9026673.html#media-1

Goldfinch, S., & Yamamoto, K. (2019). Citizen perceptions of public management: Hybridisation and post-new public management in Japan and New Zealand. *Australian Journal of Public Administration*, 78(1), 79-94.

Hood, C. (1991). A public management for all seasons?. *Public Administration*, 69(1), 3-19.

Hughes, O. (1992). Public management or public administration?. *Australian journal of public administration*, 51(3), 286-296.

Iacovino, N. M., Barsanti, S., & Cinquini, L. (2017). Public organizations between old public administration, new public management and public governance: the case of the Tuscany region. *Public Organization Review*, 17(1), 61-82.

Johansen, M., & Hawes, D. P. (2016). The effect of the tasks middle managers perform on organizational performance. *Public Administration Quarterly*, 40(3), 589-616.

Koontz, H. & Weihrich, H. (2010). *Essentials of Management: An International Perspectiv*e (8ª ed.). New Delhi: Tata McGraw Hill Education Private Limited.

Lei n.º 6/2014 Lei Orgânica de Bases da Organização das Forças Armadas. (2014). Diário da República n.º 167, série I de 2014-09-01. https://dre.pt/application/conteudo/56384927

Metcalfe, L. & Richards, S. (1991). *Improving Public Management*. London: Sage.

Norheim-Martinsen, P. M. (2016). New sources of military change–armed forces as normal organizations. *Defence studies*, 16(3), 312-326.

Organisation for Economic Co-operation and Development (OECD) (1994). *Non-financial enterprises financial statistics 1993*. Paris: OECD Publications.

Osborne, S. P. (2006). The new public governance?. *Public Management Review*, 8(3), 377–387.

Pereira, P. & Patrício, T. (2016). *Guia Prático de Utilização do SPSS: Análise de Dados para Ciências Sociais e Psicologia* (8ª ed.). Lisboa: Edições Sílabo, Lda.

Pyun, H. O., & Gamassou, C. E. (2018). Looking for public administration theories?. *Public Organization Review*, 18(2), 245-261.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 12/10/2021
Aceitação/Acceptance: 30/01/2022

Integración de una microrred solar fotovoltaica al sistema eléctrico de un buque de apoyo logístico y cabotaje liviano BALC-L

M. P. Arrieta[1], A. M. Castaño[2], C. Marrugo[2], R. R. Mendoza[3]

mparrieta@cotecmar.com; amcastano@cotecmar.com; cmarrugo@cotecmar.com; rmendoza@cotecmar.com

[1] COTECMAR, Turbaco, 131001, Colombia.

[2] COTECMAR, Arjona, 131020, Colombia.

[3] COTECMAR, Cartagena, 130001, Colombia.

Pages: 65-79

Resumen: Actualmente, se presenta un aumento en la implementación de las energías renovables en los sistemas eléctricos convencionales por medio del uso de microrredes eléctricas. El desarrollo constante de estas tecnologías ha permitido avanzar hasta llegar a su integración en los buques. En este caso se realizó el diseño de una microrred solar fotovoltaica y su integración a la red eléctrica de un Buque de Apoyo Logístico y Cabotaje Liviano – BALC-L[1], extendiendo su cubierta superior con el propósito de disponer de un área para la instalación de módulos fotovoltaicos (PV), a partir de esto, se estimaron cargas a alimentar y se analizó su desempeño mediante herramientas de simulación, permitiendo de esta forma analizar su impacto en la reducción de costos de combustible y en las emisiones de carbono CO2 a lo largo del ciclo de vida.

Palabras-clave: Microrred solar fotovoltaica, Energías renovables, Simulación, Emisiones de carbono.

Integration of a solar photovoltaic microgrid to the electrical system of a Light Logistics Support vessel BALC-L[1]

Abstract: Nowadays, there is an increase in the application of renewable energies in conventional electric systems using microgrids. The constant development of these technologies has allowed progress towards integration on ships. In this study, the design of a solar photovoltaic microgrid and its integration to the electrical grid of a BALCL[1] (Light Logistic Support Vessel) was carried out through the extension of its upper deck to provide an area for the installation of PV modules. From this, the present investigation considered an estimation of the loads that the microgrid would supply, and their performance was analyzed through simulation tools,

[1] BALC-L: Buque de Apoyo Logístico y Cabotaje Liviano.

allowing to analyze their impact on reducing fuel costs and CO2 carbon emissions throughout the proper life cycle.

Keywords: Solar photovoltaic microgrid, Renewable energy, Simulation, Carbon emissions.

1. Introducción

En las últimas décadas la protección ambiental ha tomado un papel importante en el desarrollo industrial y en todos los sectores empresariales del mundo. Muestra de esto, es la implementación de tratados como "el Acuerdo de París", ratificado en el 2015 por los principales países emisores de gases de efecto invernadero, con el objetivo de reducir significativamente las emisiones de estos gases para limitar el aumento de la temperatura global (Organización de Naciones Unidas, 2015). De igual forma, en el 2015 los Estados miembros de las Naciones Unidas adoptaron diecisiete objetivos globales llamados Objetivos de Desarrollo Sostenible (ODS) dentro de los cuales se encuentran el fomento de la energía asequible y no contaminante y la acción por el clima, enfocados en erradicar la pobreza, proteger el planeta y asegurar la prosperidad para todos como parte de una nueva agenda de sostenibilidad mundial (ONU, 2015).

Esta tendencia de protección y prioridad ambiental se extiende a todos los sectores industriales, propendiendo por el desarrollo de estrategias y políticas institucionales para la satisfacción de estos objetivos y metas de protección ambiental; de todo esto, los sectores de la energía y el transporte se ven directamente comprometidos por su alta implicación en la afectación del ambiente.

Respecto al sector marítimo, se estima que contribuye aproximadamente en un 2,2% a las emisiones globales de dióxido de carbono; a pesar de que es el modo de transporte más eficiente desde el punto de vista energético, se ha identificado la necesidad de un control eficaz de las emisiones debido a su crecimiento en el comercio mundial (International Maritime Organization, 2020).

Debido a esta problemática a nivel mundial y en aras de afrontar los nuevos retos de energía renovable y sostenible, están surgiendo algunos conceptos en la esfera energética que, en conjunto con las nuevas tecnologías de generación, pueden aportar al cumplimiento de estos objetivos.

El presente artículo contribuye a la solución de esta problemática a partir de la implementación del concepto de microrredes en embarcaciones, las cuales son redes localizadas capaces de trabajar de forma autónoma a la red eléctrica tradicional (Hyland), compuestas por fuentes de generación, grupo de cargas, sistema de almacenamiento de energía y dispositivos de control para la gestión de la energía (Fusheng & et al, 2016). Para el Buque BALC-L[1] se integrará una microrred basada en un sistema de generación fotovoltaica, con el propósito de generar energía eléctrica aprovechable para alimentar cargas eléctricas, permitiendo de esta forma analizar la integración física de elementos en la plataforma, consumo de combustible de los generadores e impacto del sistema a lo largo del ciclo de vida del buque.

Así, se propone implementar a bordo de la embarcación un modelo de aplicación de tecnología para la generación de energía eléctrica adicional a la utilizada convencionalmente

(generadores Diesel), presentando propuestas y aportando estrategias prácticas dentro de la industria marítima para la reducción de la contaminación, a partir de la integración de una fuente de generación no convencional.

2. Antecedentes

Dentro del contexto colombiano, se establece el Plan de Desarrollo Naval 2042 el cual describe los roles y funciones de la Armada Nacional con las que aporta al desarrollo sostenible del territorio marítimo, insular, costero y fluvial, y proyecta el poder nacional desde el mar y los ríos. Dicho plan propone unos objetivos orientados hacia el Desarrollo Integral Social, Asistencia y Cooperación, Seguridad Integral Fluvial y Asistencia Humanitaria (Armada de Colombia, 2021).

Conforme a este último enfoque, surge la idea de diseñar un Buque de Apoyo Logístico y Cabotaje Liviano con el propósito de brindar soporte a la ejecución de operaciones encaminadas a la atención de desastres, apoyo logístico y ayuda humanitaria por medio del transporte de personal, carga líquida (combustible y agua potable) en tanques de transporte y carga adaptada a contenedores sobre cubierta (COTECMAR, 2021). A continuación, se puede observar el buque BALC-L[1].



Figura 1 – Buque de Apoyo Logístico y Cabotaje Liviano y características principales.

Este buque está destinado a ejecutar operaciones en ríos primarios y secundarios y un tránsito costero eventual entre deltas de los ríos en la región Pacífica Colombiana. Está diseñado con un bajo calado permitiendo a la Armada de Colombia ampliar su cobertura de acción, posibilitando las operaciones de asistencia humanitaria y atención de emergencias. El diseño del buque ha contemplado para su misión la implementación de soluciones innovadoras en cuanto a la modularidad, impacto ambiental y eficiencia energética (COTECMAR, 2021).

El buque dispondrá de un área en la cubierta de carga, una rampa de proa y una grúa para facilitar el transporte de hasta cuatro (04) contenedores con módulos de misión, carga rodada, vehículos y carga unitarizada, permitiendo alcanzar lugares en los cuales no se cuente con infraestructura portuaria (COTECMAR, 2021) y permitirá la instalación de tecnologías no convencionales a bordo para la generación de energía eléctrica, presentándose como un prototipo para los buques de su tipo y misión.

3. Dimensionamiento de un sistema solar fotovoltaico a bordo del buque BALC-L

Al llevar a cabo el dimensionamiento de un sistema fotovoltaico en el buque BALC-L[1], se afronta uno de los grandes retos, establecer un área extensa para la instalación de los módulos PV, puesto que un buque está proyectado para un aprovechamiento total del espacio (Fajardo Abenza, 2016). En los casos en los que no se consideren la implementación de sistemas PV en el diseño inicial de las formas del buque, se tiene una superficie limitada con las condiciones necesarias para la instalación de los módulos PV, razón por la cual en ocasiones es necesario la modificación de elementos (extensión de cubierta) o reubicación de sensores y/o sistemas; sin embargo, al ser un buque que operará en aguas someras y canales restringidos, presenta restricciones de peso, en la distribución de sus sistemas y en sus dimensiones principales.

Al realizar la planeación y diseño de la microrred solar fotovoltaica, se consideraron las recomendaciones prácticas brindadas por el estándar IEEE 2030.9-2019, en las cuales se establece que toda microrred debe atender los requerimientos del perfil de carga, la demanda energética y contar con fuentes de generación de energía eléctrica, de modo que sea lo suficientemente estable para satisfacer la demanda inmediata, así como escalable para un futuro crecimiento de la demanda teniendo en cuenta las condiciones de operación y el estado del sistema (IEEE, 2019).

Todo esto, basándose en los escenarios de aplicación, los requerimientos de eficiencia y un análisis costo beneficio; asumiendo que el objetivo se debe enfocar en cumplir con las tres áreas propuestas por la normativa, eficiencia económica, relevancia del sistema e impactos ambientales (IEEE, 2019).

Con base a todo lo anterior, se atienden las disposiciones del mencionado estándar, y se propone la integración de un sistema fotovoltaico a la red eléctrica de la embarcación BALC-L[1], posibilitando la alimentación de consumidores específicos y reduciendo los costos en consumo de combustible fósil.



Figura 2 – Diseño preliminar del buque BALC-L versus diseño final del buque BALC-L.

Para la integración de la microrred solar fotovoltaica en el BALC-L[1], se extendió la cubierta superior del buque lográndose proveer un área de $24\,m^2$ para la instalación de los módulos PV, de los cuales se dispuso un área de $13.6\,m^2$ distribuidos a los

alrededores de los arreglos de los módulos para el tránsito de la tripulación, la limpieza y mantenimiento de estos, delimitando de esta forma un área total para instalación de 10.4 m^2. En la Figura 2, se puede observar los cambios que se realizaron a nivel estructural en la cubierta superior, con el propósito de disponer un área para la instalación de los módulos PV.

Acorde al área de instalación, se procedió a evaluar tres tipos de tecnologías de módulos fotovoltaicos con el objetivo de estimar la potencia máxima de generación y seleccionar los consumidores a alimentar.

3.1. Cálculo y especificación de los componentes del sistema

En este contexto, se procede a dimensionar el sistema fotovoltaico teniendo en cuenta la cantidad de módulos acorde al área disponible y la potencia pico total producida por cada una de estas tecnologías. Ver Tabla 1.

Tecnología	Área del modulo (m2)	Potencia pico (Wp)	Cantidad de modulos	Potencia pico total (Wp)
Panel solar Monocristalino convencional	2.1	420	4	1,680
Panel solar flexible	1.65	175	6	1,050
Panel solar Bifacial monocristalino	2.3	445	4	1,780

Tabla 1 – Potencias pico de generación según tecnologías de módulos PV

Según lo indicado en la tabla anterior la capacidad de generación con las tecnologías de módulos PV evaluadas se encuentra en un rango de potencia pico entre 1.1kWp – 1.8kWp. De acuerdo con estos valores y las recomendaciones brindadas por el estándar IEEE 2030.9, y luego de analizar las cargas del buque en términos de demanda energética y de impacto en el cumplimiento de las misiones, se establece alimentar las luminarias de la cubierta 01 que tienen un consumo de potencia aproximado de 1kW incluyendo unos circuitos de reserva para un posible crecimiento futuro alrededor del 20%.

Se estima la energía total requerida durante un tiempo de operación específico teniendo en cuenta las cargas a alimentar, la potencia pico generada por los módulos y la radiación solar mínima de la región pacifica colombiana, zona establecida para la operación del buque conforme lo indicado en la formulación del proyecto ante Minciencias (COTECMAR, 2019). En la Tabla 2 se muestran cada uno de los consumidores del sistema, la potencia requerida y la energía necesaria total para un periodo de tiempo de operación de 08 horas.

Conforme con la energía total requerida, se establece una tensión nominal de 12VDC para el sistema. Para el dimensionamiento del sistema de almacenamiento de energía, se establecen unas baterías con una capacidad nominal de 200Ah y una profundidad máxima de descarga del 70%, que cuentan con un peso y tamaño adecuado para la integración en el buque. A partir de esto se obtiene la capacidad de almacenamiento total requerida de las baterías, la cual se define de acuerdo con la siguiente expresión:

Consumidores	Cubierta	Potencia (W)	Horas de uso al día (h)	Energía (Wh/ día)
Luminaria Camarote/Baño/ Cuarto de radio	01	394.4	08	3155
Luminaria Puente de gobierno	01	291.2	08	2330
Luminaria cubierta exterior winche de popa	01	60	08	480
Circuitos de reserva	01	200	08	1600
			$E_{TOTAL\ instalada}$ AC	7565
			E_{TOTAL} AC con un factor de utilización de 0.6	4539
			E_{TOTAL} AC (después del convertidor) = E_{TOTAL}AC /90%	**5043**

Tabla 2 – Energía estimada consumida por las cargas AC

$$Capacidad\ necesaria\ (Ah) = (E_{TOTAL}\ AC * días\ de\ autonomía)/Vnominal \quad (1)$$

Donde $E_{TOTAL}\ AC$ corresponde a la Energía total después del convertidor y *Vnominal* corresponde a 12VDC, de (2) se obtiene:

$$Capacidad\ necesaria\left(Ah\right) = \frac{5043 * 1.3}{12} = 546\ Ah \quad (2)$$

Teniendo en cuenta la capacidad nominal de 200Ah y la profundidad máxima de descarga del 70%, se calcula la cantidad de baterías requeridas para el almacenamiento de la energía, obteniendo una cantidad mínima de 4 baterías. Ver ecuación 3.

$$Cantidad\ de\ baterías = \frac{Capacidad\ necesaria\ de\ almacenamiento\left(Ah\right)}{Capacidad\ de\ almacenamiento\left(Ah\right)\ \ Profundidad\ máx\ descarga\left(SOC\right)} \left(\text{SEQ Ilustración \ * ARABIC 3} \right) \quad (3)$$

Obteniendo:

$$Cantidad\ de\ baterías\ = \frac{546}{200 * 0.7} = 4\ baterías \left(\text{SEQ Ilustración \ * ARABIC 4} \right) \quad (4)$$

Considerando el área para instalación se obtienen dos escenarios, en el primer escenario es posible disponer de 4 módulos PV convencionales o bifaciales con una potencia entre 420 - 445W, mientras que en el segundo escenario se pueden disponer de 6 módulos PV flexibles de 175W.

Para definir la tecnología de módulos PV, se procederá a realizar una serie de simulaciones con el propósito de evaluar la generación de energía teniendo en cuenta las condiciones meteorológicas del área de operación y las pérdidas producidas por las sombras de los elementos que se encuentran en esa cubierta del buque. Conforme a esto se evaluará cuál de estas tecnologías satisface los requerimientos del sistema.

4. Evaluación de tecnologías de módulos solares

Para seleccionar la tecnología a implementar en este buque, se realizaron simulaciones mediante el uso de HelioScope, en este software se tiene en cuenta, las condiciones meteorológicas donde navegará el buque (Rio Atrato, Chocó), las características comerciales de los módulos PV seleccionados, las sombras debido al mástil y los equipos que se encuentran dispuestos en cubierta externa y las pérdidas por la conversión DC/AC mediante el uso de inversores.

Al realizar las simulaciones se consideró la forma de instalación de los módulos PV de modo que la orientación e inclinación fuese la óptima, debido a que estos factores determinarán en parte cuanta radiación incidirá sobre ellos influyendo así, en la obtención de la potencia nominal. La orientación se realizó de acuerdo con la situación geográfica en función de la latitud, siendo en el ecuador donde la posición del sol alcanza el cenit, por lo tanto, entre más cerca se encuentre del ecuador, menor debe ser la inclinación de las placas (Fajardo Abenza, 2016).

La inclinación es un factor importante teniendo en cuenta que las placas se encontrarán instaladas en una embarcación que se encuentra en constate movimiento, por lo tanto, se necesita una forma de instalación que favorezca la generación de energía eléctrica la mayor parte del tiempo (Yigit & Acarkan, 2018). Otra opción de solventar los requerimientos de inclinación es mediante el uso de seguidores (Trackers). Este sistema se da generalmente en aplicaciones de alta concentración, son capaces de mantener los módulos fotovoltaicos perpendicularmente a los rayos solares durante el día alcanzando una eficiencia del 90% (Díaz & Garrido, 2016).

La orientación de los módulos en el buque está determinada por el rumbo, por lo tanto, aunque se establezca un ángulo para estos módulos, su orientación variará conforme a la navegación; sin embargo, al ser un sistema dinámico, la producción de energía puede verse afectada por los cambios de orientación y de la región estimada (Gaber, EL-banna, Hamad, & Eldabah, 2020). En la Figura 3 se puede observar el buque posicionado sobre el área de operación y los módulos en disposición.

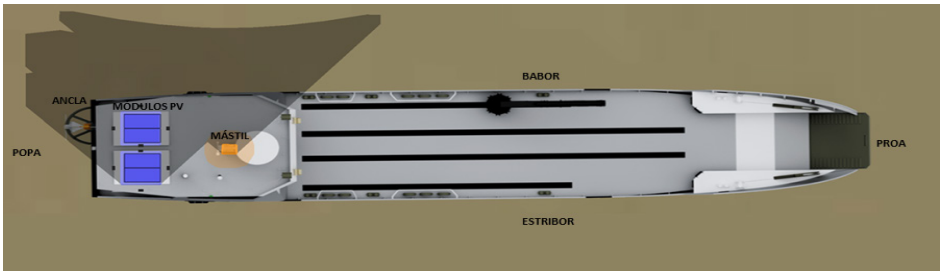


Figura 3 – Vista en planta de Buque de Apoyo Logístico y Cabotaje Liviano BALC-L. Adaptado de simulación en Helioscope (https://www.helioscope.com/projects).

4.1. Simulación de módulos solares

Basado en el área de instalación para la microrred solar fotovoltaica en la embarcación BALC-L[1], se realizaron simulaciones con cada tipo de tecnología de módulos PV

mediante el uso de la herramienta Helioscope. Las simulaciones fueron realizadas con las condiciones de irradiación directa normal, irradiación global horizontal y promedio de temperatura ambiente del Rio Atrato, Choco. El periodo de simulación fue de 4380 horas (un año), distinguiendo la producción mensual, las fuentes de pérdidas y el porcentaje de eficiencia del sistema, acorde a las referencias de los módulos PV e inversores con sus características comerciales.

Se realizaron tres simulaciones, cada una correspondió a un tipo de tecnología diferente y una forma de instalación:

- Panel convencional Monocristalino 420Wp instalado sobre riel, inclinación 10° y azimut 270°.
- Panel Bifacial Monocristalino 445Wp instalado sobre soporte, inclinación 15° y azimut 270°.
- Panel flexible 175Wp instalado sobre cubierta, inclinación 0° y azimut 270°.

4.2. Resultados obtenidos de las simulaciones

La producción de la energía mensual obtenida de los módulos PV se puede encontrar en la Tabla 3.

Mes del año	Energía Panel Monocristalino convencional (kWh)	Energía Panel flexible (kWh)	Energía Panel Bifacial monocristalino (kWh)
Enero	176.4	72.4	187.8
Febrero	159.1	64.9	176.5
Marzo	180.0	74.4	199.6
Abril	172.1	70.0	186.9
Mayo	175.7	71.4	192.4
Junio	165.4	67.5	177.9
Julio	183.0	74.7	201.7
Agosto	179.6	74.2	197.7
Septiembre	178.1	73.5	191.1
Octubre	168.4	69.8	180.0
Noviembre	162.1	65.8	174.6
Diciembre	178.9	73.3	193.5

Tabla 3 – Producción mensual de energía según tecnologías de módulos PV

De las simulaciones realizadas se determina lo siguiente:

- Los módulos PV rígidos convencionales generan la energía suficiente para alimentar las cargas, su instalación en riel es sencilla y no añade mucho peso a la cubierta.
- Los módulos PV de tipo bifacial generan la energía suficiente para los requerimientos del sistema, debido a su alta potencia pico, su eficiencia y

su característica particular de celdas en su parte trasera, lo que permite un aumento en su rendimiento; sin embargo, su forma de instalación requiere un soporte adicional, para obtener una altura suficiente para el aprovechamiento de la radiación incidente sobre la cubierta, aportando de esta forma un peso adicional sobre la cubierta.

- Los módulos PV flexibles se adaptan a la cubierta y no requieren una estructura adicional, sin embargo, requieren una gran área de instalación a causa de su baja potencia y eficiencia, debido a esto no logran generar la energía suficiente para alimentar las cargas.

4.3. Análisis de sombras

Conforme al análisis de producción de potencia realizado anteriormente, se seleccionaron para esta aplicación los módulos PV convencionales, considerando que a pesar de no ser la tecnología que permite generar la máxima potencia, presentan una practicidad en cuanto a instalación se refiere, debido a que este tipo de módulos se integran a la cubierta del buque mediante el uso de rieles, por lo cual, no generan un peso significativo.

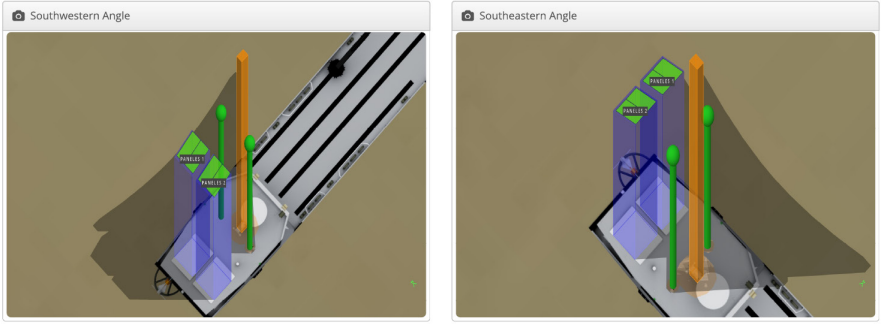


Figura 4 – Estudio de sombras que afecta la incidencia de rayos solares sobre los módulos PV. Adaptado de simulación en Helioscope (https://www.helioscope.com/projects).

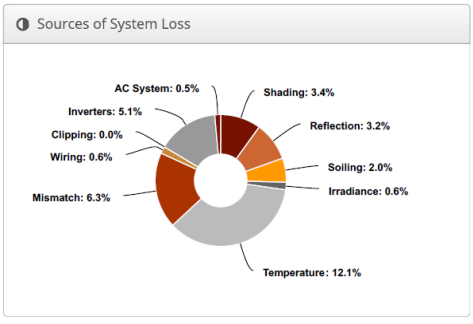


Figura 5 – Diagrama de fuentes de pérdidas del sistema solar fotovoltaico. Adaptado de simulación en Helioscope (https://www.helioscope.com/projects).

A estos módulos se les realizó un análisis de sombras teniendo en cuenta su altura con respecto a la línea base del buque, el mástil y los equipos principales que se encuentran dispuestos en la misma cubierta y los cuales se encuentran a mayor altura que los módulos PV, razón por la cual tienen un gran potencial para ocasionar sombras que generan pérdidas al sistema. En la Figura 4 se puede observar la simulación de las sombras.

De este estudio se obtuvo que las pérdidas generadas por sombra corresponden a un 3,4% de la producción del sistema, esto se encuentra entre los valores permisibles considerando que no afecta significativamente la energía producida, adicional se pueden observar en la Figura 5 otras fuentes de pérdidas del sistema.

5. Integración de la microrred solar fotovoltaica a la red eléctrica del buque BALC-L

La microrred solar fotovoltaica diseñada está compuesta por cuatro módulos PV, un controlador, un inversor y un arreglo de cuatro baterías. Durante el día los módulos PV producen energía eléctrica a partir de la radiación solar y la transmiten a las baterías mediante el uso de un controlador MPPT (Maximum Power Point Tracking), que disminuye la tensión de salida de los módulos de 44.9VDC a 12VDC con el propósito de cargar las baterías. Ver Figura 6.

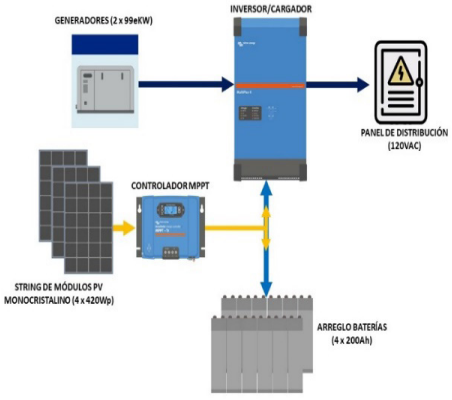


Figura 6 – Esquema representativo de la integración de microrred solar fotovoltaica a red eléctrica del buque. Adaptado de *SLD – MPPT MultiPlus-II- off-grid,* por Victron Energy, 2021, (https://www.victronenergy.com.es/inverters-chargers/multiplus-ii#system-schematics)

Por medio de un inversor/cargador se alimentan las cargas de las luminarias de la cubierta 01 que se encuentran en un panel de distribución a 120VAC. Este equipo tiene dos modos de uso, por un lado, se puede utilizar como un inversor, es decir, que realiza una conversión DC/AC y eleva la tensión para cumplir con el requerimiento de las cargas; por otra parte, trabaja como un cargador, recibe la potencia del generador y realiza una conversión AC/DC bajando la tensión con el propósito de cargar el arreglo de baterías. Adicional, mediante el uso de un sensor de tensión, este equipo ayuda a

prevenir la sobretensión, debido a que se ajusta un máximo de corriente admisible y cuando el generador lo supera, toma la restante para cargar las baterías.

En caso de presentarse alguna falla en el inversor, se alimenta el panel de distribución a 120VAC mediante el uso de un selector que permite cambiar la fuente de alimentación del inversor al generador, aportando de esta forma un sistema de respaldo a la microrred fotovoltaica.

Para la integración de la microrred solar fotovoltaica a la red eléctrica del buque se cuenta con disponibilidad de espacio para la instalación de los equipos que la conforman, asimismo en la cubierta inferior de la que se instalarán los módulos PV se encuentran bandejas para recolectar el cableado de los módulos y dirigirlos al gabinete de la microrred.

6. Impacto de la integración del sistema solar fotovoltaico al buque BALC-L a lo largo del ciclo de vida

Al definir el diseño y funcionamiento de la microrred solar fotovoltaica a bordo del buque BALC-L[1], podría considerarse que su impacto es muy limitado, si se asocia a la demanda eléctrica total requerida para la funcionalidad de este, sin embargo el esfuerzo por integrar esta microrred al sistema eléctrico convencional del buque permite ir abriendo camino en la industria marítima y fluvial Colombiana y ampliar cada vez más la inclusión de tecnologías a bordo que permitan una distribución flexible e inteligente en el que convergen favorablemente la generación distribuida, las fuentes de energías renovables y las cargas eléctricas locales como una entidad independiente y autosostenible, es decir, una microrred **(Jin & et al, 2016)**.

Para la valoración de la integración de la microrred al sistema eléctrico del buque se analiza también su impacto a lo largo de la vida útil de la embarcación, estimando el ahorro en costos de consumo de combustible Diesel y su aporte a la disminución de la huella de carbono, considerando sus 2500 horas de operación anual y su vida útil de 20 años.

Teniendo en cuenta la vida útil de la microrred solar fotovoltaica y del buque, se procede a realizar una estimación de los costos del consumo de combustible Diesel a lo largo de 20 años considerando el valor actual del combustible y un aumento por año del 9% asociado al promedio de incremento anual del diésel (Ministerio de minas y energías, 2022). En la Tabla 4 se puede observar el costo total del combustible diésel consumido durante cada año con la operación del sistema eléctrico convencional del buque alimentando toda la demanda (generador diésel instalado a bordo), el costo por el combustible consumido cada año con la integración de la microrred y por último el ahorro total en costos de combustible por año.

Año	Costo consumo combustible - convencional	Costo consumo combustible con microrred	Ahorro en consumo de combustible
01	$ 141'976.421	$ 140'290.526	$ 1'685.895
02	$ 154'754.298	$ 152'916.674	$ 1'837.625

Año	Costo consumo combustible - convencional	Costo consumo combustible con microrred	Ahorro en consumo de combustible
03	$ 168'682.185	$ 166'679.174	$ 2'003.012
04	$ 183'863.582	$ 181'680.300	$ 2'183.283
05	$ 200'411.305	$ 198'031.527	$ 2'379.778
06	$ 218'448.322	$ 215'854.364	$ 2'593.958
07	$ 238'108.671	$ 235'281.257	$ 2'827.414
08	$ 259'538.451	$ 256'456.570	$ 3'081.882
09	$ 282'896.912	$ 279'537.662	$ 3'359.251
10	$ 308'357.634	$ 304'696.051	$ 3'661.583
11	$ 336'109.821	$ 332'118.696	$ 3'991.126
12	$ 366'359.705	$ 362'009.379	$ 4'350.327
13	$ 399'332.079	$ 394'590.223	$ 4'741.857
14	$ 435'271.966	$ 430'103.343	$ 5'168.624
15	$ 474'446.443	$ 468'812.643	$ 5'633.800
16	$ 517'146.623	$ 511'005.781	$ 6'140.842
17	$ 563'689.819	$ 556'996.302	$ 6'693.518
18	$ 614'421.903	$ 607'125.969	$ 7'295.934
19	$ 669'719.875	$ 661'767.306	$ 7'952.568
20	$ 729'994.663	$ 721'326.364	$ 8'668.300
TOTAL	$ 7.263'530.687	$ 7.177'280.111	**$ 86'250.576**

Tabla 4 – Costo de consumo de combustible a lo largo de vida útil.

El análisis del costo en consumo de combustible se realizó teniendo en cuenta la potencia consumida en la maniobra de navegación que tiene un requerimiento de potencia de 80kW, lo que acorde a la ficha técnica del generador Caterpillar C4.4 – 99ekW equivale a un consumo de diésel de 6.21 gal/h (Caterpillar, 2011). Considerando lo anterior, se puede observar que al integrar la microrred solar fotovoltaica a la red eléctrica se puede producir un ahorro en costos de combustible de $86'250.576 COP a lo largo de la vida útil del buque.

Este ahorro sumado a las consideraciones de diseño y especificación de equipos y sistemas que apuntan a tener una embarcación con mayor eficiencia energética resulta como se ha analizado en un impacto también económico que permite una operación de la embarcación a un menor costo anual. El ahorro analizado de $86'250.576 COP es bastante significativo siendo que está asociado solo a la alimentación de la carga de iluminación de la cubierta 01 del buque, cuyo consumo es tan solo de 1kW de manera que el potencial de ahorro en costos de combustible fósil en las futuras generaciones del buque puede resultar considerable según la ampliación de esta microrred a bordo.

Con el sistema solar fotovoltaico se logra disminuir el consumo de combustible fósil, produciendo en el buque BALC-L[1] un ahorro de 184 galones al año debido a la carga asumida por la microrred y disminuyendo 2 toneladas de CO2 al año asociadas a la generación eléctrica del buque, de acuerdo con lo estimado mediante el uso de la herramienta para el cálculo de emisiones de UPME[2] (UPME, 2016). Una vez más este valor podría considerarse insignificante en comparación a la capacidad de emisión total que pueda tener la embarcación; sin embargo, representa un aporte positivo para el impacto medioambiental que se viene procurando a través de los tratados, acuerdos, normativas vigentes y plan de la Armada Nacional de Colombia.

7. Conclusiones y trabajo futuro

En este orden de ideas, este artículo permite presentar las siguientes conclusiones del proyecto:

- El uso de software como Helioscope, para el análisis del sistema solar fotovoltaico y el estudio de sombras, es de importancia para la validación de la implementación de microrredes solares fotovoltaicas a bordo de embarcaciones, considerando la variedad de elementos y equipos que normalmente se disponen en las cubiertas externas de los buques.
- Acorde a los análisis de producción de energía, estudio de sombras, y disponibilidad de espacios para la ubicación de componentes, se establece que la integración de la microrred a bordo del buque BALC-L es aprovechable para la alimentación de la carga asociada a la iluminación de la cubierta 01 y viable para su implementación.
- La implementación de esta microrred fotovoltaica al buque BALC-L representará un ahorro de combustible fósil estimado en $86'250.576 y una disminución de emisiones de CO2 estimada en 2 toneladas a lo largo del ciclo de vida de la embarcación.
- Para la integración de una microrred solar fotovoltaica se requiere disponer de un área de instalación para módulos PV, a mayor área se obtendrá una mayor potencia producida y como consecuencia una disminución en el consumo del combustible. Por lo que la integración de este tipo de microrredes se debe considerar desde la etapa de diseño conceptual para lograr la disposición de espacios a bordo de la embarcación.
- Basándose en la mejora continua de la tecnología, se espera que, en unos años, los módulos PV puedan producir mayor potencia y sean más eficientes, a partir de ahí, será un buen punto de partida para su implementación en buques. Así mismo en algunos años se podrá considerar la implementación de la tecnología de módulos PV flexibles, debido a su capacidad para instalación, amoldándose a las formas del buque y aportando poco peso a la plataforma.
- Con la integración de tecnologías de microrredes a bordo de un buque de la ARC se marca un precedente a nivel local en el sector naval, marítimo y fluvial para la continuación de desarrollos que contemplen el diseño de embarcaciones, considerando un perfil de operación, disposición general de espacios y

[2] UPME: Unidad de Planeación Minero-Energética.

especificación de sistemas y equipamiento que permitan la funcionalidad de diversas microrredes con un mayor alcance.

- Como potenciales trabajos futuros en el marco del diseño de este tipo de buques, resultaría conveniente evaluar diferentes tecnologías de generación renovable con capacidad para integración en estas plataformas, tales como turbinas eólicas verticales y celdas de combustible de hidrógeno.

Referencias

Armada de Colombia. (2021). *Plan de Desarrollo Naval 2042*. Bogóta: Armada de Colombia.

Caterpillar. (14 de diciembre de 2011). Marine Gen Set Engine Performance C4.4 DITA, 99ekW/60 Hz/1800 RPM. Caterpillar.

COTECMAR. (2019). *Presentación del proyecto BALC-L*. Cartagena.

COTECMAR. (2021). *Concepto Técnico, Resumen Diseño Contractual BALC-L*. Cartagena.

COTECMAR. (2022). *Documento de Necesidad Operativa*.

Díaz, A., & Garrido, R. (2016). Sistema de control en cascada aplicado a seguidores solares de alta concentración. *Memorias del Congreso Nacional de Control Automático*, (pp. 361-366). Querétaro, México.

Fajardo Abenza, H. (2016). *Análisis cualitativo de la aplicabilidad de instalaciones FV/T en los buques, unidades e instalaciones de la Armada Española*. Vigo.

Fusheng, L., & et al. (2016). *Microgrid Technology and Engineering Application*. China: ELSEVIER.

Gaber, M., EL-banna, S., Hamad, M., & Eldabah, M. (2020). Performance Enhancement of Ship Hybrid Power System Using Photovoltaic Arrays. *IEEE PES/IAS Power Africa*, 1-5.

Hyland, M. (s.d.). Microgrids: Back to the future? (p. 10). IEEE.

IEEE. (2019). IEEE Recommended Practice for the Planning and Design of the Microgrid. Em IEEE, *IEEE Std 2030.9* (pp. 1-46). IEEE.

International Maritime Organization. (2020). *Fourth IMO Greenhouse Gas Study*. London: IMO.

Jin, Z., & et al. (2016). Next-Generation Shipboard DC Power System: Introduction Smart Grid and DC Microgrid Technologies into Maritime Electrical Netowrks. *IEEE Electrification Magazine Volume 4*, 45-57.

Ministerio de minas y energías. (2022). *SICOM*. Obtido de https://www.sicom.gov.co/index.php/consulta-de-precios

ONU. (2015). Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible. *Asamblea General del 25 de septiembre de 2015* (pp. 15-30). Nueva York: ONU.

Organización de Naciones Unidas. (2015). *Acuerdo de París*. París: ONU.

UPME. (2016). *Calculadora de emisiones*. Obtido de http://www.upme.gov.co/calculadora_emisiones/aplicacion/calculadora.html

Victron Energy. (s.d.). *victronenergy.com.es*. Obtido de https://www.victronenergy.com.es/inverters-chargers/multiplus-ii#system-schematics

Yigit, K., & Acarkan, B. (2018). An examination of the photovoltaic, energy storage, and diesel hybrid power system fot he ship applications. *International Journal of Advances on Automotive and Technology*, 78-88.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 16/12/2021
Aceitação/Acceptance: 28/02/2022

Análisis OSINT aplicado a la investigación de Fraudes Financieros

Christian Vaca[1], David Martínez[2], Renato M. Toasa[1]

cvaca@uisrael.edu.ec; hector.martinezvi@ug.edu.ec; rtoasa@uisrael.edu.ec

[1] Universidad Tecnológica Israel. Quito - Ecuador

[2] Universidad de Guayaquil. Guayaquil-Ecuador

Pages: 80-91

Resumen: Las técnicas de Inteligencia de fuentes Abiertas (OSINT), permiten al investigador de fraude o al consultor de ciberseguridad obtener información de manera lícita con la finalidad de que esta pueda utilizarse para prevenir o detectar un esquema de fraude, considerando que las personas u organizaciones han migrado sus operaciones a entornos digitales sea por medio de redes sociales, plataformas de comercio electrónico, o pasarelas de pago donde puedan comercializar sus bienes y servicio o simplemente socializar, es aquí que el riesgo de fraude se incrementa al no contar con la presencialidad que permita asegurar que dicha persona u organización existe y no se trata de un fraude, estafa o mecanismo de ingeniería social para obtención de información que puede ser explotada más adelante. En este contexto, este trabajo resume el estado del arte respecto al uso de las técnicas OSINT en investigación de fraude y presenta como caso de estudio, el fraude generado por la plataforma Big Money en Ecuador.

Palabras-clave: OSINT, fraude, delito, big money, Ecuador

OSINT Analysis applied to Financial Fraud Investigation

Abstract: Open Source Intelligence Techniques (OSINT), allow the fraud investigator or cybersecurity consultant to obtain information in a lawful manner in order that it can be used to prevent or detect a fraud scheme, considering that people or organizations have migrated their operations to digital environments either through social networks, e-commerce platforms, or payment gateways where they can market their goods and services or simply socialize, E-commerce platforms, or payment gateways where they can market their goods and services or simply socialize, it is here that the risk of fraud is increased by not having the presence to ensure that the person or organization exists and it is not a fraud, scam or social engineering mechanism to obtain information that can be exploited later. In this context, this paper summarizes the state of the art regarding the use of OSINT techniques in fraud investigation and presents, as a case study, the fraud generated by the Big Money platform in Ecuador.

Keywords: OSINT, fraud, crime, big money, Ecuador

1. Introducción

Hoy en día existen distintos sistemas informáticos disponibles en internet que facilitan distintas gestiones a los usuarios, desde aplicaciones bancarias, gubernamentales, educativas, de diversión, personales, pero este gran auge de la tecnología trae consigo el potencial riesgo que dichos procesos sean manipulados por personas maliciosas, poniendo en peligro la integridad de los datos de los usuarios.

La pandemia ocasionada por el COVID-19, incrementó el número de fraudes a nivel mundial, según estimaciones presentadas por la ONU, los fraudes han crecido en más de un 600%, las modalidades más usadas son phishing (páginas falsas para robar datos) y malware (software malicioso), suplantación y falsedad documental (León C, 2020). Los fraudes informáticos y las nuevas formas de criminalidad implican una cierta incertidumbre sobre todas las posibilidades criminales que se pueden desarrollar, de ahí nace una creciente necesidad de tener sobre las aplicaciones y transacciones que se realizan en la red (Josefina & García-Cervigón, 2008) para prevenir posibles daños en los sistemas informáticos que se utilizan con regularidad en las actividades cotidianas.

En cuanto a los peligros que se generan, el fraude informático es uno de los más comunes, según Mayer Lux et al., 2020, se describen 3 definiciones de fraude informático, la primera: "el fraude informático se vincula con conductas que en realidad corresponden a etapas de ejecución imperfecta (delito tentado o frustrado)", la segunda "fraude informático en ocasiones es relacionado con comportamientos que corresponden a otros delitos informáticos o a otros ciberdelitos", finalmente "se lo relaciona con la estafa, al punto que en legislaciones como la alemana o la española se les regula sucesiva o conjuntamente, lo que ha contribuido a aclarar las diferencias entre ambos ilícitos."

Las teorías más sobresalientes sobre fraudes que pretenden explicar por qué las personas llegan a cometer un fraude hablan de tres factores principales que pueden incidir en las decisiones que toman los individuos. Estos son la motivación, la oportunidad y la racionalización (Cressey & Galtung, 1961).

En este sentido, este trabajo propone el uso de herramientas OSINT para obtener información licita de un caso de fraude financiero desarrollado en Ecuador en tiempos de pandemia, de esta manera identificar y analizar los aspectos más sobresalientes del caso y concientizar a las personas sobre los fraudes financieros para evitar que los afecten.

El documento se encuentra organizado de la siguiente manera, la sección describe la conceptualización y contextualización de términos y estudios relacionados, la sección 3 detalla el caso de estudio analizado, los resultados se muestran en la sección 4 y finalmente las conclusiones en la sección 5.

2. Conceptualización y Contextualización

2.1. Conceptualización

Según la ACFE (Association of Certified Fraud Examiners) el investigador de fraudes puede ocupar una serie de técnicas para obtener información valiosa ocupando OSINT,

y propone una metodología de 5 pasos (*ACFE Association of Certified Fraud Examiners Capítulo España*, n.d.):

1. Construir el perfil del sujeto
2. Buscar en Internet buscando un motor de búsqueda
3. Buscar en redes sociales
4. Identificar sospechosos potenciales
5. Seguir las pistas

Saccani, (2014), define 4 pasos para utilizar OSINT en una investigación que se muestran en la Tabla 1

No	Macroproceso	Actividad a realizar
1	Planificación	Pensar que buscar. Seleccionar el motor de búsqueda a utilizar. No creer todo lo que vemos.
2	Ejecución	Los motores de búsqueda no siempre son el mejor lugar para iniciar una búsqueda en línea. Probar con más de un motor de búsqueda. Buscar a profundidad, los primeros resultados no siempre son los mejores.
3	Evaluación de Resultados	Cuestionar si la fuente de origen es primaria. Validar quien creó el sitio web o escribe los artículos y por qué lo hace. Revisar cuando fue escrita la información o revisada por última vez.
4	Validación	Validar que los avisos del sitio están diferenciados de la información.

Tabla 1 – Pasos a seguir para Investigar utilizando OSINT

Sacanni, también propone que se debe documentar 6 aspectos del sospechoso cuando se utiliza OSINT en un proceso de investigación:

1. Vinculaciones societarias y Relaciones
2. Antecedentes legales
3. Antecedentes financieros y económicos
4. Identificación de activos
5. Búsqueda en medios
6. Trabajo de campo

Por otro lado Martínez, (2014), propone utilizar el método científico para investigar fraudes y lo esquematiza en 7 etapas:

1. Enunciar el problema.
2. Observación
3. Planteamiento de preguntas
4. Formulación de hipótesis
5. Verificación de la hipótesis
6. Exponer las conclusiones
7. Documentar adecuadamente

Otro enfoque que se aplica en otras áreas del conocimiento y que permite prevenir establecer la relación con una persona natural o jurídica (sea como cliente o proveedor) que tiene problemas legales, financieros, laborales, inmobiliarios, en sus procesos o fiscales, se conoce como due diligence o debida diligencia.

Este procedimiento se hace referencia en buenas prácticas, por ejemplo, para la gestión de proyectos (PMbok de PMI) así como para la prevención de lavado de activos (FELADE y ACAMS) y define las siguientes fases (Londoño, 2008):

1. Preliminar.
2. De investigación.
3. De confirmación de datos.
4. De emisión.

En base los enfoques citados, se propone el modelo de la Tabla 2, considerando un enfoque de investigación preventivo y el otro correctivo (post mortem):

No.	Enfoque Preventivo [EPR] (Antes de que ocurra el evento)	Enfoque Correctivo [ECO] (Una vez que el hecho ocurrió)
1	Definir el sujeto de análisis	Planteamiento de la Hipótesis
2	Definir el alcance de la revisión (legal, financiero, procedimientos, jurídico, laboral)	Definir los procedimientos a ejecutar para probar la o las hipótesis planteadas
3	Seleccionar las herramientas o fuentes de datos a utilizar	
4	Documentación de la información recolectada	
5	Validación y confirmación de la veracidad de la información recolectada	Emisión del Informe con los hallazgos más relevantes identificados
6	Emisión del Informe con los hallazgos más relevantes identificados	

Tabla 2 – Enfoques de investigación de fraudes

2.1. Contextualización

Las estafas son un problema social cuyo origen nace con el mismo ser humano y la satisfacción de sus necesidades (motivación, presión, racionalización) y que ha proliferado y crecido hoy en día con por el uso de plataformas digitales donde se ofrecen desde la compra-venta de bienes y servicios, así como también acceso a medios de financiamiento por medio de la emisión de líneas de crédito. Es así que, en el caso de Ecuador, los esquemas más utilizados son los esquemas Ponzi (Caso Notario Cabrera, es uno de los más icónicos) cuya forma de operar hace que sea insostenible en el tiempo, y uno de los más recientes es el caso "Big Money" que se analiza en esta investigación con el uso de herramientas OSINT.

En la literatura se identifica una serie de estudios que describen fraudes analizados, inicialmente Nguyen & Luong, (2020), describen una serie de fraudes informáticos con tarjetas bancarias y estafas telefónicas investigados por la policía vietnamita entre 2010 y 2018.

Por otro lado, la ciencia también se ha visto envuelta en fraudes Hernández-Chavarría, (2007), afirman que "el tipo de fraude científico más común es la autoría inmerecida, perpetrado con el objetivo de aumentar su número de publicaciones", donde se añaden

autores a trabajos científicos cuando no colaboraron en el desarrollo del artículo. (Oermann et al., 2019), mencionan que "existen revistas que cobran tarifas de publicación por adelantado al autor, estas son las llamadas revistas depredadoras que enmascaran las publicaciones existentes con el único propósito de obtener ganancias financieras".

Ecuador, al ser un país de tercer mundo, ha experimentado una serie de fraudes a lo largo de su historia, todas las acciones delictuosas en materia penal tributaria tienen que ver con engañar, ocultar, falsear, adulterar, simular, alterar, operaciones ficticias y en general cualquier hecho relacionado con el fraude (Saltos Orrala, 2017). El régimen tributario penal en Ecuador está mencionado en un solo elemento legal denominado Código Orgánico Integral Penal (COIP). Otro tipo de fraude común en Ecuador es el fraude aduanero, (Núñez Ortega, 2012), afirman que "examina el fenómeno del fraude aduanero, partiendo de una revisión global con la remisión a la normativa internacional y regional pertinente", donde se mencionan distintas formas de fraude aduanero. Se puede mencionar, además, fraudes en servicios electrónicos (Moscoso Mendoza, 2020), fraudes electorales (Córdova Bossano, 2017), fraude en el sistema penal (Guadamud Alay, 2021). Y distintos fraudes financieros, por medio de pirámides de estafa.

Por lo detallado anteriormente es necesario analizar los fraudes suscitados en el contexto ecuatoriano, se detalla en el resto de secciones un análisis de fraude financiero.

3. Caso de estudio

El 5 de junio del 2021 nace la empresa de inversiones "Big Money" en la provincia de Los Ríos en Ecuador, como una plataforma que solo tenía cinco empleados, sin embargo, la superintendencia de bancos informa que esta empresa no es financiera y que se trataría de una estafa piramidal.

Esta empresa ofrecía un retorno del 90% de interés en 8 días por depósitos a partir de los $300, por ejemplo, si entrega $1.000 en ocho días se recibían $900.

Esta entidad a simple vista, muestra un comportamiento inusual y se enmarca dentro de un esquema de estafa de tipo piramidal, así se puede mencionar los siguientes patrones:

- Ofrece ganancias con rendimientos exorbitantes y muy superiores a lo que ofrece el mercado financiero que opera bajo un marco regulado y legal.
- Carece de un mecanismo de transición claro, respecto a cómo se pagarán las ganancias fruto de la inversión que se realice.
- La magnitud de personas que desean participar del proceso de inversión sugiere la existencia de comisiones por ingreso de nuevos miembros.
- Múltiples perfiles en redes sociales
- Inconsistencia en su información

4. Resultados

Para el análisis del caso de estudio planteado se ocupará el enfoque preventivo denominado Antes de que ocurra el evento (EPR):

4.1. Identificar el sujeto de análisis

Big Money, Miguel Ángel Nazareno, Don Naza

4.2. Definir el alcance de la revisión (legal, financiero, procedimientos, jurídico, laboral)

Encontrar la huella digital de la Empresa Big Money y nombre, teléfono o email de su supuesto propietario.

4.3. Seleccionar las herramientas o fuentes de datos a utilizar

Las herramientas OSINT seleccionadas se detallan en la Tabla 3, estás permitirán recopilar información y analizar la legalidad de la cuenta o las cuentas que se tengan en la web la empresa Big Money o su propietario.

No.	Motor de Búsqueda	Herramienta a utilizar	Modo
1	Mozilla FireFox	Namecheckup	Incognito
2	Google Chrome	Phoneinfoga	Normal
3	Local	Maltego	Normal
4	Mozilla FireFox	Hunter	Incognito
5	Mozilla FireFox	Página de SRI	Normal
6	Google	Google	Normal

Tabla 3 – Herramientas Seleccionadas para el rastreo de huella digital del caso de estudio

4.4. Documentación de la información recolectada

Producto de la búsqueda de información en Google con las palabras clave %Big Money%recibos%fotos% se encontró el recibo de la Figura 1:



Figura 1 – Recibo de la Empresa Big Money

A partir de la información de este recibo se busca en la página del Servicio de Rentas Internas (SRI) el Registro Único de contribuyentes (RUC) 1205299058001, obteniendo los resultados detallados en la Figura 2:



Figura 2 – Consulta en el RUC

Con el número de cédula se realiza la búsqueda en la página https://sidehu.midena.gob.ec/certificados/nofa.action a fin de validar si el titular pertenece o perteneció a las Fuerzas Armadas, ver la Figura 3:

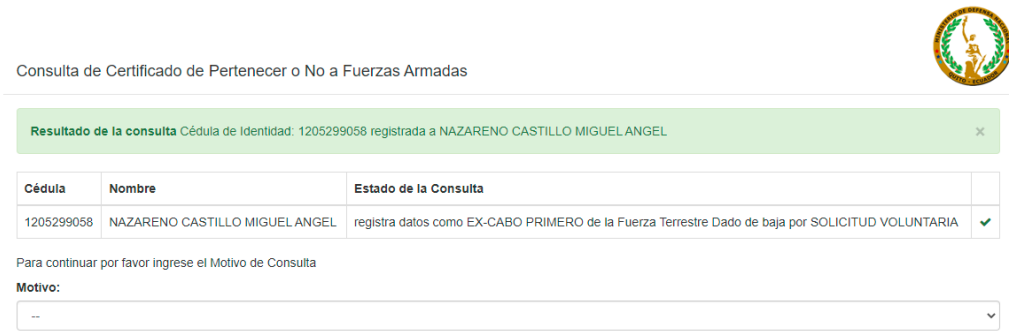


Figura 3 – Consulta Estado en las Fuerzas Armadas

Se realizó la búsqueda de Big Money y Don Naza con varias derivaciones de este nombre el Facebook, ver la Figura 4:



Figura 4 – Consulta Cuentas en Redes Sociales - Facebook

En la red Social LinkedIn, se identifica un perfil con los datos de Miguel Angel Nazareno Castillo, ver la Figura 5:

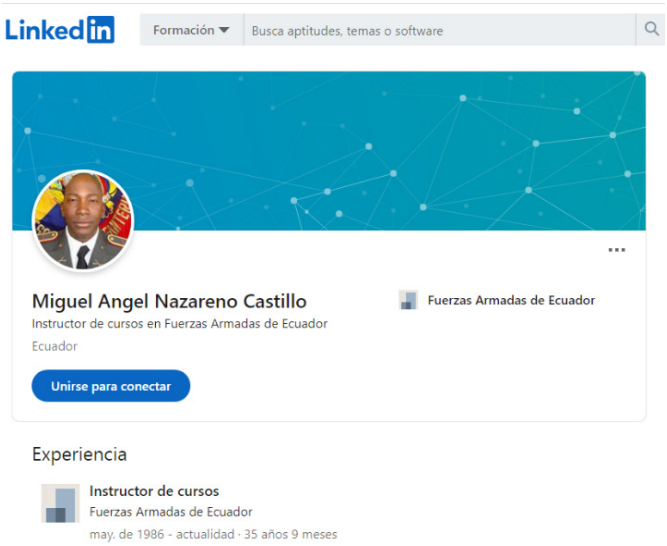


Figura 5 – Resultados consulta Redes Sociales - LinkedIn

Utilizando la herramienta Namecheck se identificó los siguientes resultados, ver Figura 6:

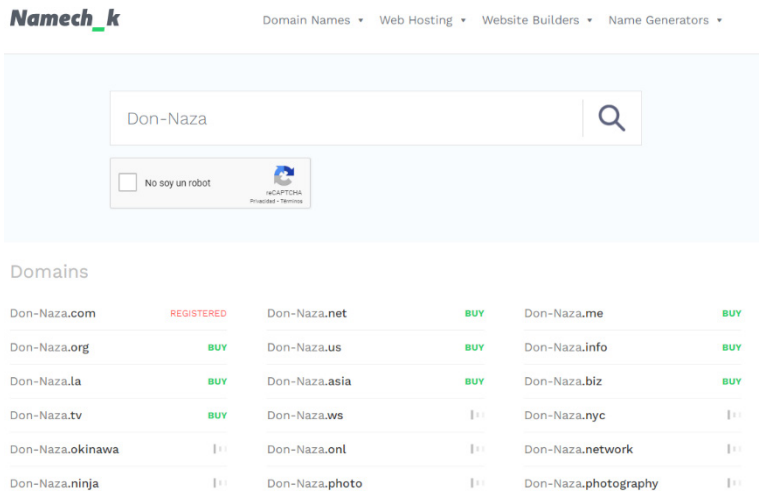
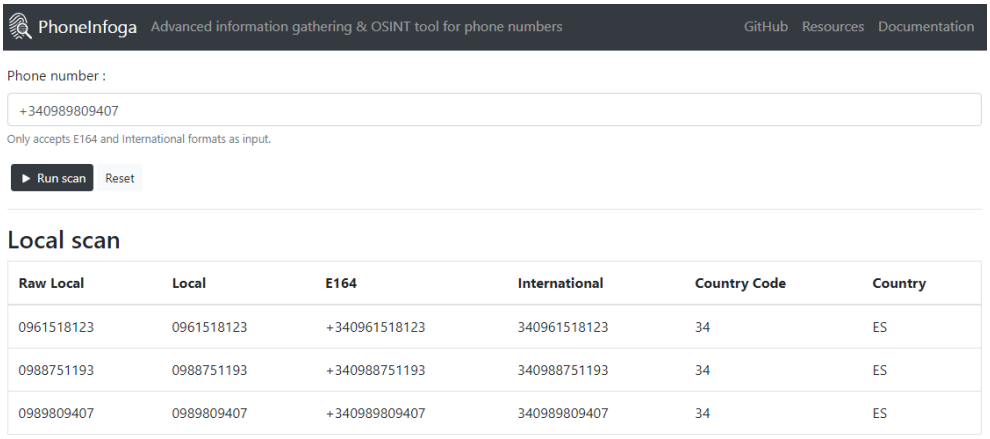


Figura 6 – Resultados consulta Namecheck

Con la herramienta PhoneInfoga se buscaron los teléfonos que el Sr. Nazareno utilizo para su esquema de fraude, ver Figura 7:



Raw Local	Local	E164	International	Country Code	Country
0961518123	0961518123	+340961518123	340961518123	34	ES
0988751193	0988751193	+340988751193	340988751193	34	ES
0989809407	0989809407	+340989809407	340989809407	34	ES

Figura 7 – Resultados consulta PhoneInfoga

4.5. Validación y confirmación de la veracidad de la información recolectada

Con la herramienta Maltego se identificó un resumen bastante completo del perfil del Sr. Nazareno que permite corroborar la información relevada en el punto 4, ver Figuras 8,9:



Figura 8 – Resultados consulta Maltego



Figura 9 – Resultados consulta Maltego

4.6. Emisión del Informe con los hallazgos más relevantes identificados

Miguel Nazareno Ángel Castillo portador de la cédula de identidad 1205299058, radica en el cantón Quevedo, provincia de Los Ríos, es de origen esmeraldeño. Vive desde hace 33 años en Quevedo y se autodenomina “empresario del pueblo”.

La actividad económica detallada en el RUC que mantiene no guarda relación con la actividad económica de préstamo de dinero, que en el caso de Ecuador es una actividad autorizada y regulada únicamente para Bancos, Mutualistas y Cooperativas de Ahorro y Crédito.

Perteneció a las Fuerzas Armadas del Ecuador específicamente al Ejército en el rango de cabo primero de infantería.

Un patrón normal de fraude es que una empresa o su representante tenga demasiadas cuentas en redes sociales o inconsistencia en la información que se publica en las mismas, este es un indicio de que no es una posible estafa.

5. Conclusiones

La metodología propuesta tiene como objetivo brindar al investigador de fraude o a una persona sin conocimiento previo un flujo bajo el cual documentar tanto la hipótesis que se plantea, las herramientas que se van a utilizar, así como un resumen de los hallazgos más importantes a fin de que facilite la toma de decisiones o la vinculación del individuo en análisis con un delito.

Las herramientas OSINT tienen un gran potencial para la investigación preventiva o detectiva de actos inusuales o fraudulentos, siempre y cuando esté basada en un flujo de proceso que permita documentar correctamente las evidencias identificadas.

La metodología propuesta sintetiza buenas prácticas sugeridas por la ACFE así como el método científico y el proceso de debida diligencia que se utiliza para prevención de lavado de activos en el sector financiero y para la validación de información previo a contraer relación comercial con una empresa o individuo.

Las herramientas OSINT, junto con un conocimiento de la Normativa General para las Instituciones del Sistema Financiero permite indagar y determinar que la empresa Inversiones Big Money presenta algunas inconsistencias que para un inversor genera dudas sobre la confianza del retorno de sus fondos, en tal sentido, con esta propuesta de metodología es fácil realizar un análisis previo a generar una relación contractual o de negocios con un tercero.

Referencias

ACFE Association of Certified Fraud Examiners Capítulo España. (n.d.). Retrieved March 20, 2022, from https://acfe-spain.com/

Córdova Bossano, F. (2017). Alegato contra la falsa acusación de fraude electoral en las elecciones presidenciales del Ecuador en 1940 | Córdova Bossano | Revista AFESE. *Revista Afese*, *65*(65). http://www.revistaafese.org/ojsAfese/index.php/afese/article/view/1166

Cressey, D. R., & Galtung, J. (1961). *The prison: Studies in institutional organization and change*. Holt, Rinehart and Winston New York.

Guadamud Alay, A. G. (2021). *El fraude procesal en el sistema penal ecuatoriano*. http://201.159.223.180/handle/3317/17538

Hernández-Chavarría, F. (2007). Fraude en la autoría de artículos científicos. *REVISTA BIOMÉDICA*, *18*(2), 127–140. https://doi.org/10.32776/REVBIOMED.V18I2.485

Josefina, D., & García-Cervigón, G. (2008). El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. *Icade. Revista de La Facultad de Derecho*, *74*, 289–308. https://revistas.comillas.edu/index.php/revistaicade/article/view/357

León C, C. E. (2020). El fraude en tiempos de pandemia . *Revista Fasecolda*, *178*, 64–67. https://revista.fasecolda.com/index.php/revfasecolda/article/view/635

Londoño, I. D. R. (2008). Puerta DUE Diligence Financiera, una forma para garantizar la toma eficiente de decisiones en la adquisición de empresas. *El Cuaderno Ciencias Estratégicas*, *2*(4), 263–278.

Martínez, J. M. (2014). *El método científico en las investigaciones de fraude e irregularidades*. https://www.auditool.org/blog/fraude/2864-el-metodo-cientifico-en-las-investigaciones-de-fraude-e-irregularidades

Mayer Lux, L., Oliver Calderón, G., Mayer Lux, L., & Oliver Calderón, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista Chilena de Derecho y Tecnología*, *9*(1), 151–184. https://doi.org/10.5354/0719-2584.2020.53447

Saltos Orrala, M. Á. (2017). EL DELITO TRIBUTARIO EN ECUADOR. *Revista Empresarial, ICE-FEE-UCSG*, *11*(1), 43–47.

Moscoso Mendoza, F. A. (2020). *Análisis de fraude en sistemas de pago electrónico en el sector empresarial de telecomunicaciones del Ecuador*. http://201.159.223.180/handle/3317/14277

Nguyen, T., & Luong, H. T. (2020). The structure of cybercrime networks: transnational computer fraud in Vietnam. *Https://Doi.Org/10.1080/0735648X.2020.1818605*, *44*(4), 419–440. https://doi.org/10.1080/0735648X.2020.1818605

Núñez Ortega, F. M. (2012). *Corrupción: tendencias globales y el fraude aduanero; caso ecuatoriano*. https://repositorio.uasb.edu.ec/handle/10644/3003

Oermann, M. H., Nicoll, L. H., Carter-Templeton, H., Woodward, A., Kidayi, P. L., Neal, L. B., Edie, A. H., Ashton, K. S., Chinn, P. L., & Amarasekara, S. (2019). Citations of articles in predatory nursing journals. *Nursing Outlook*. https://doi.org/10.1016/J.OUTLOOK.2019.05.001

Saccani, R. (2014). *OSINT E INVESTIGACIÓN EN REDES SOCIALES*.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 13/12/2021
Aceitação/Acceptance: 22/02/2022

Módulos de misión del Buque de Apoyo Logístico y Cabotaje Liviano (BALC-L) para operaciones humanitarias y atención de desastres en el Pacífico Colombiano

Farah Inés Vergara Chadid[1], José María Riola[1], Juan Carlos Martínez[2], Priscilla Areiza Frieri[2].

faritavch@gmail.com; chema.riola@rga-psi.es; jcmartinez@cotecmar.com; pareiza@cotecmar.com

[1]Escuela Naval de Cadetes "Almirante Padilla" – ENAP. Cartagena de Indias, Colombia.

[2]Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval Marítima y Fluvial – Cotecmar. Cartagena de Indias, Colombia.

Pages: 92-104

Resumen: La modularidad es una tendencia creciente en la industria astillera no solo en el diseño y la construcción naval, sino también en todo lo relacionado al desempeño operacional a través de módulos de misión, lo cual permite la configuración dinámica de los buques para cumplir las tareas asignadas sin requerir costosas modificaciones en sus plataformas. El presente artículo aborda las consideraciones, alcance, características y ampliación de las capacidades operacionales de una unidad tipo Buque de Apoyo Logístico y Cabotaje Liviano (BALC-L), con un enfoque en sus módulos de misión para operaciones en ríos primarios y secundarios de la región Pacífica colombiana, así como durante su eventual tránsito costero, con el objetivo de alcanzar una mayor capacidad de respuesta y soporte a las operaciones de la Flota Naval con el uso de contenedores para fines de ayuda humanitaria, atención de desastres y apoyo logístico de manera rápida, flexible y móvil en zonas de difícil acceso geográfico del territorio colombiano.

Palabras-clave: Modularidad, flexibilidad, soporte logístico y cabotaje, respuesta humanitaria ante desastres, embarcación fluvial.

Mission modules of the Light Cabotage and Logistics Support Vessel (BALC-L) for humanitarian operations and disaster response in the Colombian Pacific.

Abstract: Modularity is a growing trend in the shipyard industry not only in design and shipbuilding, but also in the concept associated with operational performance through mission modules, which allows the dynamic configuration of ships to fulfill the assigned tasks without requiring costly modifications to their platforms. This paper addresses the considerations, scope, characteristics and expansion of the

operational capabilities for a BALC-L light cabotage and logistical support vessel focused on its mission modules in operations (primary and secondary rivers and their eventual coastal transit) in the Colombian Pacific region. , with the objective of a greater response capacity and support to the operations of the Naval Fleet with the use of containers for humanitarian aid, disaster response and logistical support in a fast, flexible and mobile way in areas of difficult geographic access of the Colombian territory.

Keywords: Modularity, flexibility, logistical and cabotage support, humanitarian response to disasters, river vessels.

1. Introducción

La necesidad de construir buques adaptables y flexibles a las operaciones implica un esfuerzo en el complejo desarrollo de nuevas capacidades de construcción y diseño en la industria naval (Díaz-Reina et al, 2021), con la modularidad, enfocada no sólo al concepto de construcción sino al asociado al desempeño operacional a través de módulos de misión para la configuración dinámica de los espacios garantizando la interoperabilidad de los buques.

La Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial (COTECMAR) desde el 2014 viene construyendo buques de desembarco anfibio "BDA", los cuales se han unido a la flota de la Armada de Colombia, proporcionando soporte logístico a las misiones de atención desastres de las diversas poblaciones, especialmente aquellas con múltiples dificultades de comunicación. Con el diseño del Buque de Apoyo Logístico y Cabotaje Liviano (BALC-L), se pretende brindar soporte a las operaciones de la marina colombiana con fines de ayuda humanitaria, atención de desastres y apoyo logístico de manera rápida, flexible y móvil en zonas de difícil acceso geográfico, específicamente en el pacífico colombiano, mediante la disposición de una carga adaptada a cuatro contenedores (de 20 pies) sobre cubierta con acoplamiento a la superestructura y las conexiones necesarias a los diferentes sistemas y subsistemas del buque. Esta plataforma tendrá la capacidad de ser adaptada a diferentes roles operativos como, por ejemplo, centro de control de emergencias, centro de apoyo de asistencia médica, alojamiento de personal sanitario y técnico, buceo y salvamento, entre otros, aplicando el concepto de modularidad para cumplir las tareas asignadas.

En las últimas décadas, y a lo largo de todo el planeta, hemos sido testigos de numerosas catástrofes naturales que han dejado a cientos de miles de víctimas. Sólo por recordar algunos se pueden mencionar las inundaciones de Nueva Orleans en 2006 al paso del huracán Katrina, el terremoto de Haití en 2010 o el Tsunami de Indonesia en el 2018. Y si hablamos de Colombia podemos citar la tragedia de Armero en 1985, el terremoto del eje cafetero en 1999 o la tragedia de Mocoa en el año 2017. Ante estos hechos y de forma automática, la solidaridad nacional e internacional aparece con el envío de equipos de bomberos, médicos, víveres, etc., con la característica de llegar a la zona problemática cuanto antes y con la máxima carga posible. Y esta es una de las ventajas de los buques, pueden navegar con mucha carga y con la autonomía necesaria para llegar a su destino. Uno de los grandes retos de la Armada de Colombia tras el paso del huracán IOTA en 2020 (categoría 5 escala Saffir-Simpson) en el Archipiélago de San Andrés, Providencia, Santa Catalina, fue la respuesta oportuna en la atención de primeras necesidades de la

población local y el restablecimiento de las líneas de comunicación, tras los daños en el sistema eléctrico, pérdida total de las comunicaciones y deterioro de cerca del 98% de la infraestructura de la isla de Providencia, en el caso fluvial del país, necesitamos buques con muy poco calado para poder acceder muy arriba en el curso del río y la capacidad de llevar contenedores sobre su cubierta.

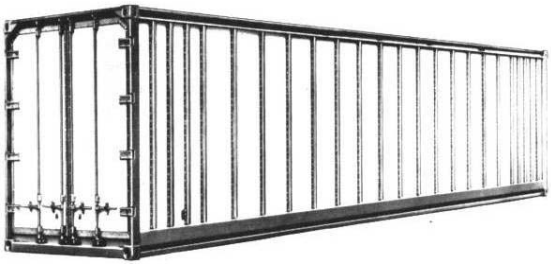


Figura 1 – Contenedor estándar. Fuente: ISO

Sin duda, el flujo de mercancías (Sanabria, 2008) es la principal herramienta que impulsa la economía del planeta, donde los contenedores (González-Laxe, 2007) juegan un rol fundamental. Se fabrican para evitar que la mercancía sufra cualquier daño y poder garantizar que llegue en óptimas condiciones a su destino (Chin el al, 2002). Su gran potencial se evidenció al ser usado entre los modos marítimo, ferroviario y terrestre, siendo el factor común utilizado en el transporte intermodal, particularmente cuando uno de los modos de transporte es un buque, y que conservan su forma actual (figura 1) desde hace más de 60 años.

La idea de llevar las mercancías en contenedores a bordo de los barcos fue de Malcom P. McLean "Qué fácil sería tomar la caja del camión y ponerla sobre la cubierta del buque" en Maxton, Carolina del Norte. Idea que, aunque parece sencilla, desafío en su momento a los mecanismos logísticos establecidos, los parámetros laborales, proporcionó el ambiente ideal para el auge de la globalización y que revolucionó en 1956 el comercio internacional al subir la primera carga a un buque mediante un contenedor, incrementando considerablemente la eficiencia del transporte, innovando en el desmontaje del camión y en la carga directamente al buque. Desde la década de los 60, su éxito radica en una gran fluidez de movimiento gracias a la estandarización de la carga al ofrecer la estructura, capacidad y dimensiones estandarizadas, por parte de la Organización Internacional de Estandarización (ISO).

Las dimensiones más comunes de los contenedores ISO son de 2,438 metros (8 pies) de ancho y alto con unas longitudes que pueden ser de 6,06 metros (20 pies) con un peso bruto máximo de unas 30,48 toneladas o del doble, 12,19 metros con un peso bruto máximo de 32,5 toneladas. Y aunque menos frecuentes, también podemos encontrar las longitudes de 13,716 metros, 14,63 metros y 16,154 metros. También la Unión Europea (CE, 2005) propone sus propias medidas adicionales con un contenedor de 15 metros de longitud y 40 toneladas de peso, justificándolo en la necesidad evidente del tamaño más grande posible.

La “contenerización” es el componente básico del transporte intermodal y un elemento crítico de las innovaciones en logística que revolucionaron el manejo de carga en la segunda mitad del siglo XX. En los años 80 su uso ya estaba generalizado y nos encontramos con unos crecimientos del comercio en contenedores del orden del 5% anual durante los últimos 15 años. El tráfico mundial de contenedores en millones de toneladas se presenta en la figura 2.

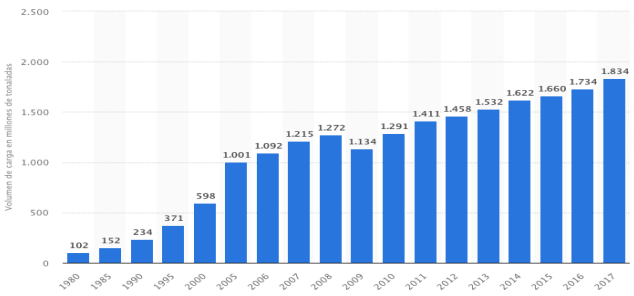


Figura 2 – Tráfico mundial de contenedores. Fuente: Statista

Los buques que transportan contenedores por las vías fluviales suelen tener unas capacidades más limitadas debido a la anchura, la profundidad y al propio trazado de los ríos, con unas capacidades que suelen oscilar entre las 800 y 1.500 toneladas. El diseño de estos buques se caracteriza por un alto coeficiente de bloque, mínimo calado y una optimización del equipo de carga (Georgijević et al, 2005) en su cubierta. A partir de los estrictos requerimientos de diseño para el buque BALC-L, basados en las restricciones de profundidad, ancho de canal y radios de giro propias de los ríos del pacífico colombiano, se realizó el dimensionamiento inicial del buque mediante un modelo de síntesis que al relacionar las variables de diseño se puede obtener un espacio de negociación que incluye las posibles opciones que cumplen con los requerimientos de diseño dentro de las restricciones impuestas al modelo. A partir de estas relaciones se puede tomar la decisión del concepto final (Parsons, 2004).

Un modelo de síntesis es una técnica de modelado para representar un sistema que depende de múltiples variables. Mediante esta técnica se simplifica el proceso de flujo aplicando una matriz de actividades independientes y dependientes y partir de condicionales para obtener un resultado. Un ejemplo de esta técnica es mostrado a continuación (Parsons, 2004).

Para el caso del BALCL el modelo consta de 4 bloques funcionales. El primer bloque contiene las dimensiones del buque parent que es el BDA, en el segundo bloque se presentan las restricciones de las dimensiones que dan las fronteras del espacio de diseño. A partir de estas, se ingresa al bloque de contadores. En el bloque de contadores se determina el paso de la variación de los parámetros para generar las posibles combinaciones. Finalmente, en el bloque para cálculos se ejecutan los módulos de potencia, capacidades, pesos, estabilidad y costos; de este módulo se descartan las combinaciones que no cumplen con los requisitos establecidos.

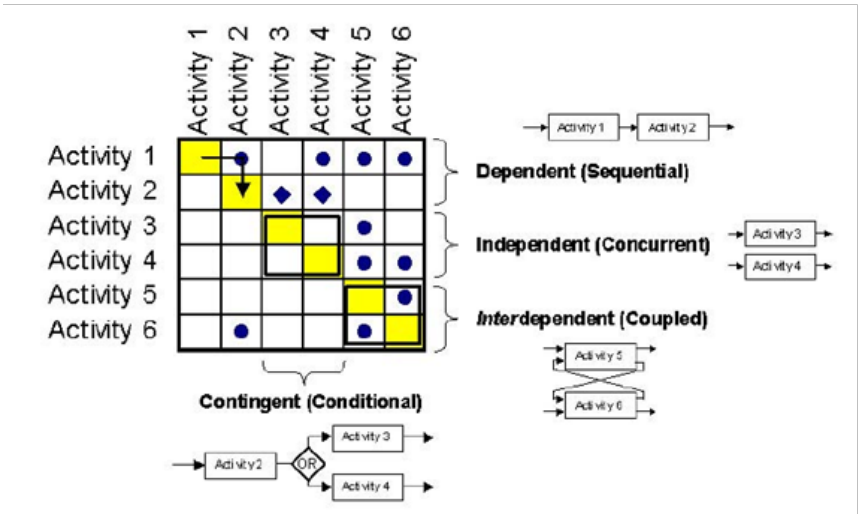


Figura 3 – Estructura de un modelo de síntesis

Mediante este proceso se lograron definir los siguientes rangos dimensionales relaciones geométricas:

Relación	Valor
L_{OA}/D	22,20 – 17,04
L_{OA}/B	5,85 – 4,50
B/T	10,38 – 7,54
C_B	0,8-0,9

Tabla 1 – Rango de las relaciones geométricas

Dimensión/ características	valor
Manga [m]	12,5 – 7,4
Eslora [m]	49- 33,3
Puntal [m]	2,9-1,1
Calado [m]	1,2-0,6
Velocidad [nudos]	9,0 -6,2

Tabla 2 – Dimensión y características limite

La mayoría de los buques de navegación fluvial se caracterizan por elevados valores en los coeficientes de bloque del casco con el fin de lograr un mayor desplazamiento a

bajo calado y disminuir su coste de construcción. Por lo tanto, para la mayoría de las embarcaciones de navegación de río el coeficiente de bloque puede variar entre 0,8 y 0,9 (Younis, 2011).

Para la definición del área de la cubierta de carga se determinó que un buque que cumpla con una manga máxima de 1,5 metros podrá navegar de forma segura sobre el canal sobre el rio Baudó, con un ancho de canal de navegación de 53 metros en el tramo cercano a Pie de Pató en temporada de lluvias. Respecto a la manga mínima, se toma como punto de partida la capacidad de llevar dos contenedores de 2,4 m de ancho con una separación entre sí de 0,7 m, mínimo necesario para el paso de una persona, y una separación de 1 m a cada uno de los costados. Se tiene como resultado una manga mínima de 7,4 m.

Para los buques cuya carga principal son contenedores, el principal componente es la carga útil (Payload) que corresponde al peso de los contenedores transportados. Para este análisis se consideró 10 toneladas como peso máximo para cada elemento de transporte modular. (Rawson, 2001). Este peso está sujeto a ajuste de acuerdo con las restricciones del calado de operación:

$$Payload{:}10{,}0{*}N_c$$

La cantidad de elementos de transporte modular (N_c), se determina en función del número de contenedores a lo largo de eslora del buque, número de contenedores a lo ancho de la manga y números de niveles de contenedores. El número de contenedores a lo largo de la eslora (*CNL*) del buque se determina en función de la eslora menos la longitud no asignada para carga (se asume 25 m) y de la longitud del contenedor de 20 ft (6.10 m) de la siguiente manera:

$$CNL = \frac{L_{oa} - 25{,}0}{6{,}1}$$

El número de contenedores a lo ancho de la manga (*CNB*) del buque se determina en función de la manga, espacio libre a los extremos para tránsito y ancho del contenedor (2.50 m) de la siguiente manera:

$$CNB = \frac{B + 2}{2.50}$$

Finalmente, el número de contenedores queda establecido de la siguiente manera:

$$N_c = CNL * CNB * N_{layer}$$

Además de la carga útil otros pesos son adicionados al peso muerto, tales como: combustible, agua transportada, pesos asociados a la tripulación, disposiciones, lastre que no sea permanente, provisiones o aceite lubricante. El peso muerto asociado a la

embarcación es cercano a 100 toneladas. Para este estudio se usa un margen de diseño y construcción del 5%.

DIMENSIONES PRINCIPALES	
Eslora total	43,5 m
Manga máxima	8,0 m
Calado de diseño	1,20 m
Alcance	1000 mn
Velocidad de diseño	8 kn
Desplazamiento	313 t
Tripulación	10 tripulantes

Tabla 3 – Características Buque de Apoyo Logístico y Cabotaje Liviano BALC-L

De acuerdo con estos planteamientos, el reto de diseño para el buque BALC-L (figura 4) contempla diversas tecnologías novedosas para alcanzar un mínimo impacto medioambiental debido a que operará en zonas con ecosistemas de alto valor a proteger. Por ello, contará con un sistema de pintura térmica basada en proyección de aluminio sobre el casco de acero (Riola y Garnica, 2021) que le permite evitar la corrosión, un sistema de "microrredes eléctricas" para conseguir la optimización de la energía de abordo y entre las distintas opciones del sistema de propulsión, se proyecta una propulsión totalmente eléctrica, basada en una pila de combustible de hidrógeno.



Figura 4 – Buque de Apoyo Logístico y Cabotaje Liviano (BALC-L). Fuente: Cotecmar

2. Módulos de misión

En la Organización del Tratado del Atlántico Norte (OTAN), han considerado los sistemas modulares o uso de contenedores como un medio para lograr la capacidad

en la interoperabilidad de buques, bajo el concepto de flexibilidad y adaptabilidad sin modificaciones en sus plataformas, de acuerdo con los estándares y orientación en diseño, operabilidad, logística, mantenimiento, dotación de buques y módulos del Equipo de Especialización en Modularidad de Misión (ST/MM) y el Grupo de Armamento Naval (NG/6) de la OTAN.

En este proyecto, se han definido tres principales módulos de misión para el BALC-L (figura 5), completamente funcionales, con acoplamientos a los sistemas y conexiones del buque, de acuerdo con las necesidades, antecedentes y requerimientos prioritarios en las operaciones enfocadas a la asistencia humanitaria y atención de desastres, considerando como base del sistema modular (Manley, 2018) el uso de contenedores ISO 20 pies, implementando una mejora de los modelos existentes para optimizar su capacidad en un entorno naval, manteniendo los estándares geométricos esenciales de este tipo de contenedores.



Figura 5 Módulos de misión (BALC-L). Fuente: Cotecmar

2.1. Módulo de mando y control para atención de desastres

El momento inmediatamente posterior a la catástrofe es clave para realizar la primera evaluación de necesidades, para esto, se plantea a lo largo de la investigación, un puesto de mando in situ capaz de realizar la valoración de la situación permitiendo optimizar y coordinar con prontitud el plan a desarrollar, y, asimismo, garantizar el restablecimiento de las comunicaciones y principalmente, la vida de las personas que sobrevivan al desastre, dotado con todos los sistemas, equipos de comunicación, herramientas y demás, que permitan la evaluación de daños y se garantice el continúo flujo de comunicación e información, con la posibilidad y bajo ciertas circunstancias, que este módulo se pueda dejar en tierra para la continuidad del centro de control de mando (figura 6 y 7).



Figura 6 – Criterios aplicables a los módulos de misión. Fuente: COTECMAR

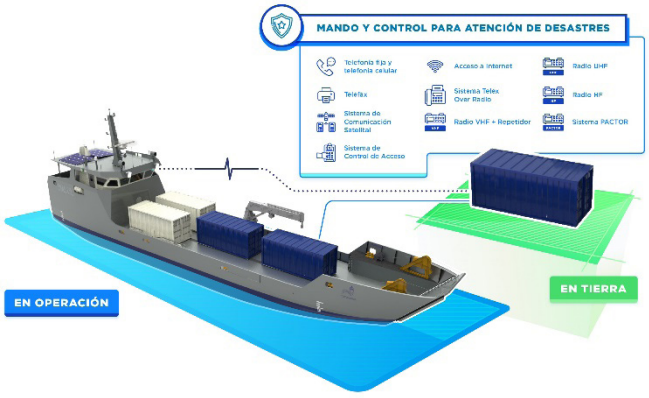


Figura 7 – Módulo de mando y control. Fuente: COTECMAR

2.2. Módulo de servicios médicos

Tanto los desastres naturales como los desastres denominados complejos, provocan un sinnúmero de víctimas que supera la capacidad del sistema de atención sanitaria local para atender y prestar los servicios necesarios (OPS, 2003), aunque muchos países optan por la utilización de hospitales de campaña móviles, desafortunadamente, la experiencia demuestra que estas instalaciones no cumplen con las expectativas de sus usuarios (figura 8).

Las primeras 48 horas son un requisito fundamental para la atención médica inicial de emergencia, porque se trata de una condición esencial para una intervención destinada a salvar vidas con la capacidad de funcionar de manera totalmente autosuficiente

(generación eléctrica, suministros médicos, equipos necesarios, suministro de agua y saneamiento). Las acciones de salud en el contexto humanitario están orientadas a facilitar una respuesta humanitaria rápida y eficaz, cumpliendo con los estándares mínimos humanitarios en salud, para proteger y salvar vidas (OCHA, 2019).

Cada módulo incluye personal, equipo, material y procedimientos cuyo resultado final es una capacidad funcional específica y una capacidad colectiva en prestación de servicios médicos, en el caso de operaciones que incluyan varias naciones, con la posibilidad de integrar contribuciones (especialmente de personal) de diferentes países en el propio módulo. De acuerdo con el estándar de la OTAN, se han identificado siete instalaciones principales de tratamientos médicos como: área de emergencia, cirugía, diagnóstico (incluyendo imágenes y pruebas de laboratorio), área de evacuación, área post operatoria, comunicación e información y área de suministros médicos (NATO, 2018).

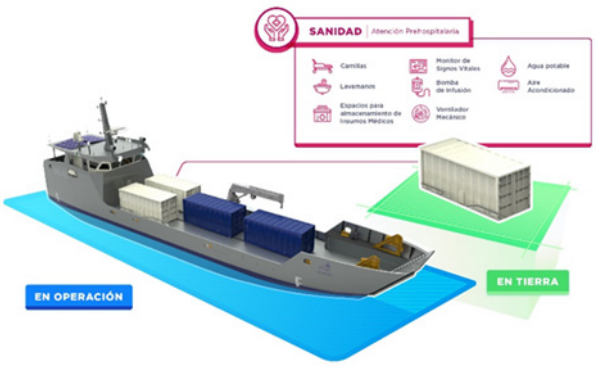


Figura 8 – Módulo de servicios médicos. Fuente: COTECMAR

2.3. Módulo de buceo y salvamento

El buceo en la Armada de Colombia es fundamental tanto en las operaciones de seguridad como de defensa de costas, bases e infraestructura crítica, incluye actividades de búsqueda, salvamento marítimo y fluvial, recuperación de material sumergido durante el desarrollo de operaciones, control de tráfico marítimo y fluvial (figura 9).

Los buzos también realizan operaciones de atención de desastres y emergencias, investigación oceanográfica e hidrográfica, entre otras, cumpliendo con las normas y reglamentos gubernamentales e internacionales para contribuir a la seguridad y bienestar de todos los que trabajan en la industria de buceo, incluyendo a los buzos comerciales, los tender/buzos, el personal de soporte en cubierta y los supervisores para las operaciones de buceo submarino (ADCI, 2020).

Dentro de sus capacidades se realizan operaciones de inmersiones con buzos en ríos donde la visibilidad es prácticamente nula, a gran profundidad y el uso de vehículos

submarinos no tripulados, así como los siguientes procedimientos operativos específicos que varían según la modalidad de buceo a realizar:

- Buceo autónomo con aire, mezcla de gases y aire enriquecido.
- Buceo semiautónomo.
- Mantenimiento submarino de buques y estructuras.
- Técnicas y ejecución de corte y soldadura submarina.
- Operaciones de salvamento y reflotamiento.
- Inspecciones técnicas y de seguridad.
- Asistencia médica hiperbárica para operaciones de buceo.

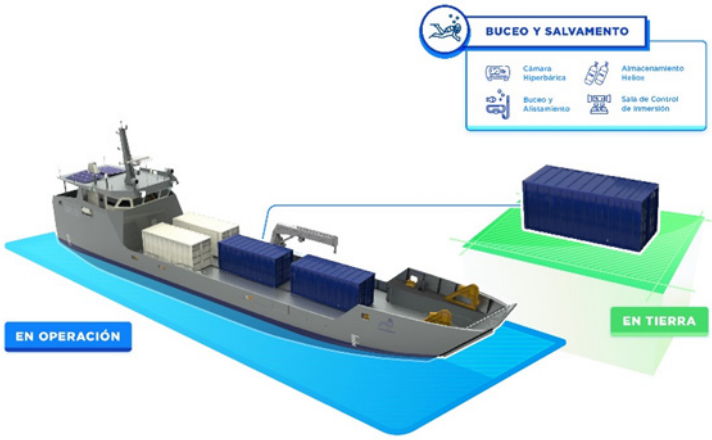


Figura 9 – Módulo de buceo y salvamento. Fuente: COTECMAR

3. Líneas futuras de módulos de misión

La búsqueda de nuevas tendencias y la renovación de sistemas serán los propósitos transcendentales en las construcciones y diseño de los buques militares (Torres Do Rego, 2018), por eso, es importante dejar plasmadas en el presente artículo científico las siguientes líneas para los futuros módulos de misión:

- **Contenedores autosostenibles**: Empleando energías renovables para su autoabastecimiento.
- **Contenedores NBQ** (Nuclear, Biológica y Química): Actualmente hay una amplia distribución de materiales radiactivos, biológicos y químicos, incrementando la posibilidad de emisión de estos materiales al medio ambiente, ocasionada por una negligencia, un desastre natural, una acción deliberada o un daño colateral en el curso de operaciones militares.
- **Contenedores para investigación fluvial**: Disponiendo de laboratorios secos y húmedos, acondicionados específicamente para los trabajos de investigación de las dinámicas geomorfológicas y las interacciones biofísicas

en los lechos de los ríos, aporta al conocimiento en la investigación científico-marina como oceanografía operacional, hidrografía, manejo integrado de zonas costeras y protección del medio ambiente marino, encaminado a fortalecer el poder marítimo en los mares y ríos nacionales.

4. Conclusiones

Los módulos de misión han sido utilizados por varias marinas que coinciden en su flexibilidad y adaptabilidad (Schank et al., 2016), sin requerir costosas modificaciones en sus plataformas para los diferentes roles operativos, mediante el estudio de antecedentes y desempeño en este tipo de operaciones, se abordan los problemas experimentados de la Armada de Colombia durante su labor de asistencia en catástrofes y se determinan las mejores prácticas que conducen a una mayor capacidad de respuesta con el uso de contenedores o módulos de misión.

Con el diseño de estos módulos de misión, aplicados al Buque de Apoyo Logístico y Cabotaje Liviano "BALC-L", la Armada de Colombia, dentro de las entidades públicas de carácter nacional involucradas en el Sistema Nacional de Gestión de Riesgo de Desastres "SNGRD" (Ministerio del Interior, 2012), dispondrá con la capacidad de respuesta para afrontar estas situaciones, porque las estadísticas prometen operaciones futuras de esta naturaleza más numerosas y complejas, específicamente, en áreas de difícil acceso como el pacífico colombiano.

Finalmente, debido a la continua evolución de los sistemas militares y para nuevos temas de investigación durante los próximos años, se ha dejado una explicación de las líneas futuras de los módulos de misión a bordo de un buque enfocado al área de operación fluvial tipo BALC-L.

Referencias

Automated container terminals. IEEE Transactions on Intelligent Transportation Systems. Vol. 3, Nº 1, pp. 12- 26.

Commission of the European Communities. (2006). Freight logistics in Europe – key to sustainable mobility, Bruselas, Bélgica.

D. Manley, (2018). The NATO drive to mission modularity, RINA, Royal Institute of Naval Architects. Warsh. 2018 Procure. Futur. Surf. Vessel. Pap., no. September.

Georgijević, M., Zrnić N., Arsenijević, A., Gašić, V. (2005). Machines for handling containers, are we ready for international competition. 5th International Conference Heavy Machinery, pp. 43 – 48, Kraljevo, Serbia.

González Laxe, F. (2007). El contenedor: la caja que cambió el mundo económico. Universidad de Coruña, Centro de Investigación Económica y Financiera. pp. 43-55. http://www.udc.es/iuem/documentos/monografias/2007-2.pdf

Grupo Tiba. (2016). Historia del Contenedor marítimo. México. https://www.tibagroup.com/mx/mclean-y-la-caja-que-cambio-la-historia-del-comercio. Descargado el 12 de noviembre de 2021.

Parsons, M. (2004) Applications of Optimization in Early-Stage Ship Design. Journal of Ship Research.

Rawson, K.J.. Basic ship theory (2001 a), Volume 1 Ship Dynamics and Design.

Reina, J. D., Fajardo-Toro, C. H., Torres, O. M., Riola, J. M., & López, M. A. G. (2020). Consideraciones para un modelo de simulación de procesos aplicado en construcción naval: Caso armada de Colombia. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 2020(E29), 553–569.

Riola, J.M., Garnica, M.A. (2021). Ensayos con aluminio en cámara de niebla salina bajo la norma ASTM B117. III Congreso de Ciencia, Tecnología e Innovación Naval (CTINAV), Barranquilla, Colombia.

Sanabria, S. (2008). El papel del transporte en el crecimiento económico colombiano en la segunda mitad del siglo XX. Apuntes del CENES. Vol. XXVII, Nº 46, pp. 141–182.

Younis, G.M., Gaafary, M.M., El-kilani, H., Moustafa, M.M.. (2011) "Techno-Economical Optimization for River Nile Container Ships, Brodograndnja, Vol. 62.

ADCI. (2020). International Consensus Standards for Commercial Diving and Underwater Operations (6.4). Houston, TX: Association of Diving Contractors International, Inc. Retrieved from www.adc-int.org

Ministerio del Interior. (2012). Ley Sistema Nacional de Gestión de Riesgos y Desastres (Abril 2012). Bogotá D.C. Retrieved from https://repositorio.gestiondelriesgo.gov.co/bitstream/handle/20.500.11762/20575/Ley_1523_2012.pdf?sequence=4&isAllowed=y

NATO. (2018). Modular approach for multinational medical treatment facilities (MTF) (Edition A).

OCHA. (2019). Guía para gobiernos Acción Humanitaria Internacional (Revisión 2). Oficina de Coordinación de Asuntos Humanitarios, ONU.

OPS. (2003). Guía de la OMS y la OPS para el uso de hospitales de Campaña extranjeros en caso de desastres. (Organización Panamericana de la Salud, Ed.). Washington D.C.

Schank, J., Savitz, S., Munson, K., Perkinson, B., McGee, J., & Sollinger, J. (2016). Designing Adaptable Ships: Modularity and Flexibility in Future Ship Designs. Designing Adaptable Ships: Modularity and Flexibility in Future Ship Designs (Vol. D). Santa Monica, California.: RAND Corporation. https://doi.org/10.7249/rr696

Torres Do Rego, J. M. (2018). Estudio de integración de opciones modulares sobre la plataforma multipropósito de un Buque Patrullero Oceánico (OPV). Universidad Politécnica de Cartagena.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 17/10/2021
Aceitação/Acceptance: 25/01/2022

Cloud Computing – Quem garante a segurança dos dados?

Nuno Miguel Carvalho Galego[1], Nelson Duarte[2], Domingos Martinho[3]

Nuno.galego@islasantarem.pt; Nelson.Duarte@islasantarem.pt

[1] ISLA – Instituto Superior de Gestão e Administração, Santarém, Portugal

[2] ISLA – Instituto Superior de Gestão e Administração, Santarém, Portugal

[3] ISLA – Instituto Superior de Gestão e Administração, Santarém, Portugal

Pages: 105-115

Resumo: Cloud computing elevou a realidade dos sistemas de informação para novos limites, oferecendo novos paradigmas tais como armazenamento e processamento de dados de forma flexível. Existe uma tendência crescente do uso de ambientes de Cloud para necessidades de armazenamento e processamento de dados, no entanto, a adoção de um paradigma de Cloud computing pode ter efeitos positivos e negativos sobre a segurança de dados dos utilizadores. Nos últimos anos, tem havido um progresso rápido no que toca a Cloud computing. Com o número crescente de empresas a recorrer aos recursos da nuvem, havendo a necessidade de proteger os dados dos vários utilizadores. Alguns dos grandes desafios que estão a ser enfrentados pela Cloud computing são para garantir, proteger e processar os dados. Este trabalho tem por finalidade destacar as questões de segurança importantes existentes nos ambientes de Cloud computing tal como as vantagens e desvantagens de um ambiente Cloud, tal como as estratégias de proteção de dados de forma a garantir a segurança dos dados.

Palavras-chave: Cloud computing; Informação; Segurança; Dados.

Cloud Computing – Who ensures data security?

Abstract: Cloud computing has elevated the reality of information systems to new boundaries, offering new paradigms such as storage and data processing flexibly. There is a growing tendency to use cloud environments for storage and data processing needs, however, the adoption of a cloud computing paradigm may have positive and negative effects on user data security. In recent years, there has been rapid progress in cloud computing, with the growing number of companies using cloud resources and the need to protect the data from various users. Some of the significant challenges cloud computing faces are ensuring, protecting, and processing the data. This work highlights the critical security issues in cloud computing environments, such as the advantages and disadvantages of a cloud environment, such as data protection strategies to ensure data security.

Keywords: Cloud Computing; Information; Security; Data.

1. Introdução

Cloud computing é a próxima geração da Internet que fornece serviços personalizáveis e fáceis para os utilizadores acederem ou trabalharem com várias aplicações na nuvem. *Cloud computing* fornece uma maneira de armazenar e aceder aos dados na nuvem de qualquer lugar a qualquer hora com recurso a uma ligação à Internet. Escolhendo os serviços da nuvem, os utilizadores são capazes de armazenar dados em servidores remotos. Os dados armazenados no *datacenter* remoto podem ser acedidos ou geridos através dos serviços de nuvem (*Cloud Services*) fornecidos pelos operadores de serviços de nuvem. Os dados armazenados num *datacenter* remoto onde ocorrem os processamentos de dados devem ser feitos com o máximo cuidado.

O ambiente de *cloud computing*, torna-se preocupante porque os dados estão localizados em lugares diferentes, podendo estar noutro pais ou outro continente, proteção, privacidade e segurança da informação são os principais fatores de preocupação dos utilizadores sobre esta nova tecnologia. Embora existam algumas investigações sobre o tema, proteção, privacidade e segurança estão a tornar-se importantes para o desenvolvimento desta tecnologia em todas as organizações.

Segurança da informação na nuvem refere-se a confidencialidade dos dados, integridade, disponibilidade e estes requisitos podem ser os grandes problemas para a *cloud computing*. Confidencialidade de dados requer que a informação esteja disponível e divulgada apenas a pessoas autorizadas.

Integridade de dados garante que os dados são mantidos no seu estado original e não foram intencionalmente ou acidentalmente alterados ou eliminados.

Disponibilidade dos dados garante o acesso contínuo aos dados no caso de um desastre natural ou sintético ou eventos, tais como incêndios ou perdas de energia.

Este estudo procura fazer uma revisão de segurança da proteção de dados na nuvem e visa reforçar a proteção da segurança e privacidade de dados num ambiente de nuvem.

2. Segurança da Informação em Cloud Computing

Cada vez mais o meio empresarial e os governos estão a migrar os seus dados para a nuvem, mas ainda há quem resista a essa mudança, devido a desconfiança e receios com a segurança das suas informações. Embora as preocupações sejam compreensíveis, a realidade hoje é que, se essa migração for executada correctamente, a segurança da informação na *Cloud* pode ser tão segura ou mais do que ter os dados em plataformas tradicionais locais (Akamai, 2017).

Na verdade, a segurança da informação na nuvem é potencialmente superior ao *datacenter* típico, isto porque os fornecedores de serviços na *Cloud* protegem a informação através da utilização de dados de vários centros com replicação entre as várias instalações.

Nos *datacenters*, onde estão alojados os dados da nuvem, os custos associados com a segurança dos dados são distribuídos entre um grande número de clientes, para que os operadores possam aplicar mais recursos para as medidas de segurança físicas, técnicas e operacionais, que a maioria das empresas ou governos não possuem, uma vez

que, ao contrario da maioria das empresas e órgãos públicos, a principal atividade dos operadores é a exploração e distribuição destes serviços.

No entanto, apesar das tecnologias e da experiência em segurança de informação na *Cloud* que os operadores possam ter, permanecem válidas as preocupações sobre a segurança.

Os operadores fornecem proteção contra as principais ameaças à segurança, como ataques de DDoS, injeções SQL e scripts entre *sites*, bem como formas mais opacas de ataques que existam na *Internet*

As soluções de segurança deste tipo de operadores que fornecem serviços na *Cloud* são altamente escaláveis e fornecem uma defesa distribuída, que deteta e bloqueia os ataques antes que eles atinjam o seu *datacenter*.

2.1. Prós e Contras da Cloud Computing

Tal como acontece com qualquer tecnologia nova, para ter uma ideia de todas as suas vantagens e desvantagens é necessária uma análise.

2.1.1. Vantagens da Cloud

Se for usada correctamente e na medida necessária, trabalhar os dados na *Cloud* pode beneficiar imensamente todos os tipos de empresas. Estas são, algumas das suas vantagens mais importantes (Linthicum, 2016):

Economia de custos

A *Cloud* é provavelmente o método mais eficiente ao nível do custo para usar, manter e atualizar. Com a *Cloud* é possível reduzir os custos de forma substancial, isto sem servidores físicos na infraestrutura local, o que também remove a energia, ar condicionado e os custos de administração. Já o *software* tradicional que tem um custo significativo para as empresas, somando-se as taxas de licenciamento para vários utilizadores que se pode revelar muito caro, também é eliminado. Além disso, existem soluções *pay-per-use* (pago por utilização) disponíveis.

Manutenções e atualizações na infraestrutura de IT são eliminados, passando essa tarefa ao operador.

A *Cloud*, por outro lado, está disponível a preços mais acessíveis e pode reduzir significativamente a despesa para a empresa. Desta forma, não são necessários investimentos iniciais caros com a incerteza de os conseguir pagar.

Armazenamento quase ilimitado

O armazenamento de informações na *Cloud* oferece a capacidade de armazenamento quase ilimitado, não existindo preocupação com falta de espaço, relativamente ao armazenamento atual.

Este é o principal fator que define a nuvem, é possivel aumentar a capacidade e reduzir, num curto espaço de tempo, conforme as necessidades.

Backup e recuperação

Desde que os dados estejam armazenados na *Cloud*, *backup* e restauros são relativamente mais simples do que noutros métodos tradicionais de armazenamento de dados.

Recuperação de desastres (disaster recovery) e continuidade do negócio (Business continuity)

Os utilizadores exigem que as suas operações e serviços continuem ativos no caso de calamidade ou no caso de acontecer algum incidente com o operador de serviços onde os dados estão alojados.

Acesso à informação

Uma vez na *Cloud,* é possível aceder às informações de qualquer lugar, desde que exista ligação à *Internet*. Este recurso permite avançar para além das questões de localização geográfica e fuso horário.

Disponibilidade

A *Cloud* só tem valor quando a rede e a largura de banda contratada estiver disponível, caso contrário não é possível aceder à informação, parecido com um ataque de negação de serviço (DoS) (Winkler , 2011)**.** A maioria dos operadores oferecem um nível de serviço que garante 24 horas por dia, 7 dias por semana, 365 por ano e 99,99% de disponibilidade. A organização pode beneficiar de uma redundância de recursos, bem como mecanismos de failover, i.e., se um servidor falhar, as aplicações e serviços podem ser facilmente transferidos para outro dos servidores disponíveis, sem impacto para o negócio.

O mecanismo da *Cloud* é distribuído de acordo com a necessidade de cada cliente, oferecendo uma incrível escalabilidade de recursos.

Em comparação com um servidor dedicado

A comparação é dificil, mas a melhor maneira de apreciar as vantagens da nuvem é compará-lo com o que sabemos de muitos anos atrás: um clássico com servidor dedicado. A **Figura 1** mostra-nos uma comparação das principais vantagensce desvantagens de um servidor Cloud e um servidor On-Premise.

Em primeiro lugar, com um servidor dedicado (uma máquina física), os recursos disponíveis são limitados, e não é possível expandir facilmente estes recursos, e muito menos sem interrupção do serviço, não esquecendo que esta máquina terá manutenções e períodos em que não estará disponível.

Em segundo lugar, é necessário ter uma equipa interna com o conhecimento necessário de administração deste tipo de servidores e o *software* associado a ele. Aqui existe um custo associado ao nível da equipa interna, ou contratada em regime de *outsourcing*.

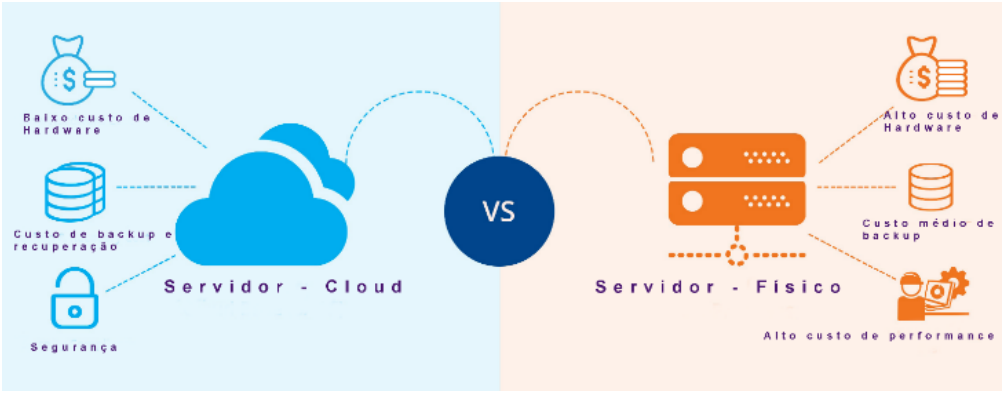


Figura 1 – Infraestrutura Cloud vs física (Adaptado de (Tahir, 2017)

Se forem avaliadas apenas as vantagens da *Cloud* acima mencionadas, está claro que a opção de um servidor dedicado é pior. Esta análise não está completa e para isso também foi feita uma análise das desvantagens de um sistema *Cloud*.

2.1.2. Desvantagens da Cloud

Apesar de seus muitos benefícios, como mencionado acima, *Cloud computing* tem muitas vantagens que vão fazer com que a sua introdução no mercado aumente nos próximos anos, mas também tem as suas desvantagens, as empresas, especialmente as pequenas, precisam estar cientes destes contras antes de adotar esta tecnologia. Quando acontece uma migração dos serviços para a *Cloud*, existem alguns problemas e perigos do seu uso, alguns deles estão listados abaixo (Seshachala, 2015).

Controlo limitado

Desde que a infraestrutura esteja totalmente na *Cloud*, a gestão e monitorização é feita em grande parte pelo operador, transferindo um controlo mínimo para o cliente. O cliente apenas controla e gere as aplicações, dados e serviços que funcionem em cima disso, não a infraestrutura de *back-end*.

É sempre difícil confiar num terceiro para guardar a nossa informação, especialmente quando não sabemos onde estão os nossos dados, nem onde é que as nossas aplicações estão a ser executadas.

As principais tarefas administrativas tais como, atualizações e *firmware* não são tarefas do cliente.

Existe algum medo, é preciso prudência para ultrapassar este primeiro problema, e ganhar confiança.

Confidencialidade e segurança dos dados

Apesar de existir um contracto assinado de confidencialidade muito detalhado, que obriga o operador a, sempre que existam problemas de segurança, manutenção inadequada, que possa causar danos à empresa, este tem de tomar medidas, mas nada garante que essas medidas não venham a ser ocultadas ou omitidas, uma vez que geralmente o cliente não tem essa perceção, além de possivelmente não ser do conhecimento do cliente onde os dados se encontram.

Um serviço de *Cloud computing* implementa os melhores padrões de segurança e certificações da indústria, armazenamento de dados e arquivos importantes, mas mesmo com todos estes cuidados existe sempre um risco.

Numa arquitetura com múltiplos clientes, onde vários estão hospedados no mesmo servidor, um *hacker* pode invadir os dados de outros clientes que armazenam informações no mesmo servidor e aceder às suas informações.

Antes de adotar esta tecnologia, é preciso saber que vão ser cedidas informações confidenciais da empresa a um operador de serviços de *Cloud*.

Disponibilidade do serviço

No caso de pequenas e médias empresas, que não têm um orçamento alto para investir em infraestrutura e técnicos qualificados, é estatisticamente mais seguro ter a informação e as suas aplicações na *Cloud*, que nos próprios servidores, mas ainda assim deve ser uma decisão ponderada. Podem vir a acontecer paragens técnicas, podendo ter um impacto brutal no negócio de qualquer organização, ficando em suspenso temporariamente. Além disso, se a ligação à *Internet* estiver *offline*, não é possível aceder a qualquer uma das suas aplicações, servidor ou dados que estejam na *Cloud*.

Questões técnicas

Embora seja verdade que as informações e dados na *Cloud* podem ser acedidas a qualquer hora e em qualquer lugar, de vez em quando este sistema pode ter alguma disfunção grave. É preciso estar consciente de que esta tecnologia está sempre propensa a falhas e outros problemas técnicos. Mesmo os melhores prestadores de serviços *Cloud* podem ter este tipo de problemas, apesar de manterem os elevados padrões de manutenção. É essencial ter uma boa ligação à *Internet* para obter um bom acesso aos servidores, em qualquer momento, e com qualquer nível de carga. Inevitavelmente, existirão sérios problemas caso haja um problema de rede ou ligação.

O armazenamento de informações na *Cloud* pode colocar qualquer empresa vulnerável a ameaças e ataques externos de *hacking*.

Existem conteúdos na Internet que não são seguros, existindo sempre a possibilidade de roubo de dados sensíveis. Em forma de conclusão, o *Cloud computing* também tem os seus prós e contras. Embora ainda existam algumas preocupações sobre a perspetiva da segurança da informação na nuvem, esta é essencialmente uma conclusão imprecisa. É fácil ver como as vantagens da *Cloud* facilmente superam as desvantagens, diminuição de custos, tempo de inatividade reduzida e menos esforço de gestão são benefícios que falam por si.

Com as suas qualidades inerentes, a *Cloud* tem um enorme potencial para as organizações melhorarem a segurança dos sistemas de informação.

3. Estratégias de protecção de dados

Até há alguns anos, a proteção de dados era uma tarefa secundária, onde não se dava a devida importância. Nos dias de hoje, é considerada uma atividade estratégica, que contribui para o sucesso do negócio, isto porque uma boa estratégia de proteção de dados pode evitar a interrupção dos serviços. Ainda assim a implementação de uma boa estratégia de proteção de dados requer alguns cuidados que devem ser tomados em atenção. Segundo Priya Viswanathan (Viswanathan, 2016) existem questões essenciais que devem ser tomadas para que a proteção de dados traga mais benefícios do que malefícios para a empresa.

Que estratégias uma empresa deve adotar para assegurar a proteção de dados?

Os ataques recentes no sector empresarial trazem questões muito importantes a este trabalho. Quão segura é a empresa? Quais são as políticas de segurança que uma empresa deve seguir para proteger as suas informações corporativas? Mais importante, que estratégias de proteção de dados o sector de empresas deve adotar? É essencial para qualquer empresa aplicar uma estratégia de proteção de dados eficaz, para assegurar a confidencialidade dos dados relativos a essa empresa. Considerando a importância deste aspeto da segurança na empresa, é mostrado abaixo uma secção de perguntas frequentes sobre as estratégias de proteção de dados que o sector empresarial deve seguir.

Porque é que uma estratégia de proteção de dados é importante?

Uma estratégia de proteção de dados eficaz tem de estar em conformidade com os requisitos de privacidade da empresa, tal como estipulado pela lei. A outra razão é que para manter uma política de proteção de dados eficaz, a empresa deve elaborar um inventário completo de todos os seus processos de dados e propriedade intelectual, ajudando também a criar uma estratégia abrangente de segurança. Todos os dados da empresa devem ser contabilizados neste processo, incluindo a propriedade intelectual tais como patentes, marcas comerciais e outro material protegido por direitos de autor, como funcionam os processos, códigos fonte de *software*, manuais, planos, relatórios e afins.

Como iniciar esta estratégia?

Existem vários departamentos numa empresa que gerem as informações confidenciais da empresa.

- O departamento de IT, por exemplo, lida com todas as informações que passam pelos servidores da empresa. Este processo pode ajudar a manter o inventário de dados e a implementar estratégias de segurança para o mesmo.
- O departamento jurídico, oficialmente, pode formular regras na empresa em relação ao uso desses arquivos e outros dados oficiais, confidenciais ou não. Esta secção é normalmente focada na criação e gestão das políticas de segurança da empresa.

- O departamento de recursos humanos pode trabalhar em conjunto com o departamento jurídico no rastreio dos funcionários para manter as informações pessoais identificáveis.

Que outras precauções que devem as empresas tomar?

Além de criar e manter uma política de segurança clara, a empresa deve gerir eficazmente toda a informação disponível. Isso inclui os seguintes aspetos:

- Uma política de segurança adequada e detalhada é uma necessidade absoluta para qualquer empresa. Os funcionários devem ser informados de todos os princípios e disposições incluídas na política de segurança, para que entendam que tipos de dados podem ou não podem aceder, e as informações que podem ou não divulgar a outras pessoas fora da empresa.
- Todos os dados e informações devem ser classificadas de acordo com o seu nível de sensibilidade. Podem dar alta prioridade somente para o que for considerado dados confidenciais. Muitas vezes, os dados que são vistos como menos importantes são completamente ignorados, criando assim uma possível fuga de informação.
- É muito importante atualizar constantemente todos os sistemas de segurança de dados, para que a empresa esteja preparada para lidar com as ameaças de segurança mais recentes. Embora seja quase impossível garantir uma segurança empresarial completa em todos os momentos, a empresa deve garantir a máxima segurança, mantendo os sistemas de segurança de dados o mais atualizados possível.

Os problemas mais importantes são os seguintes:

Abusos na Cloud computing

A infraestrutura de nuvem tem sido utilizada para fins menos claros como *botnet's* e redes de envio de *spam*. Isto acontece porque o acesso a esses recursos não é restrito. Qualquer pessoa que pague, pode ter recursos consideráveis para cometer um crime. E é preciso não esquecer que ao lado dessas aplicações "criminosas", na mesma *Cloud*, estão os dados das empresas.

Interfaces inseguras e APIs

Os serviços de *Cloud* fornecem uma interface, ou uma API para acesso a recursos, configuração, *status*, adicionar e remover recursos. Isso pode representar uma falha de segurança, já que não se controla quem está a aceder à *Cloud,* e assim, intencionalmente ou acidentalmente acontecer uma negação de serviço ou provocar algum mal ao serviço e, em caso extremo, a outros clientes do mesmo operador na *Cloud***.**

Perda de informação

Os problemas de informação são muitos e variados, perda de dados por exclusão acidental, acesso a dados fora da empresa, onde os recursos são partilhados com outros clientes, numa partilha, numa pasta alojada no operador de *Cloud*, onde pode existir

alguém mal-intencionado, que pode negligenciar os dados da empresa ou cometer um ato criminosos, ou até mesmo vender essas informações.

Roubo de sessão

Todos os controlos de acessos dos recursos da *Cloud* são efetuados usando credenciais (geralmente *username* e *password*), da mesma forma que acedemos ao *webmail*. Obviamente, se essas credenciais caírem nas mãos erradas, quem tiver esse acesso pode espiar e manipular dados, o que terá um impacto negativo no negócio.

Riscos devido à ignorância

Uma das vantagens da *Cloud* é precisamente de que não precisamos de saber os detalhes da infraestrutura. No entanto, é necessário ter um conhecimento mínimo das decisões a respeito da segurança e dimensionamento dos recursos. **Algumas recomendações importantes são:**

Conformidade normativa

Os clientes são responsáveis pela segurança e a integridade dos dados, mas os operadores devem permitir que sejam efetuadas auditorias, para mostrar que é possível confiar os dados confidenciais da empresa nessa infraestrutura.

Localização de dados

É importante conhecer a lei aplicável em matéria de proteção de dados, de preferência tem que existir um acordo, para aplicar as regras do país do cliente.

O isolamento de dados

O isolamento dos dados entre um cliente e outro deve existir, uma vez que vários clientes partilham os mesmos recursos. Se isso não for feito, existe o risco de fugas de informação confidencial.

Política de backup e recuperação

É muito importante exigir uma política de *backup* e recuperação de desastres. Vivemos num mundo digital, onde as regras da informação estão acima de tudo, portanto, desenvolver uma estratégia de proteção de dados eficaz torna-se imperativo para qualquer empresa. Esta estratégia de proteção de dados, tem de levar em consideração todos os dados da empresa, processos administrativos e políticas de segurança.

4. Conclusões

Apesar do *Cloud Computing* ter inúmeras vantagens, ainda existem muitos problemas que precisam de ser resolvidos. As vulnerabilidades existentes no modelo de *Cloud* vão aumentar as ameaças perpetuadas pelos *hackers*. De acordo com a investigação feita, as questões de proteção de segurança e privacidade dos dados são os problemas principais, que precisam ser resolvidos o mais rápido possível. Apesar do *Cloud Computing* ser uma

tecnologia emergente que apresenta um bom número de benefícios para as empresas, ainda enfrenta muitos desafios de segurança. Questões de segurança e privacidade de dados existem em todos os níveis e em todas as fases do ciclo de vida dos dados. Os desafios na proteção da privacidade estão na partilha dos dados e proteção de dados pessoais. Qualquer empresa que esteja a pensar em mudar para a nuvem, deve primeiro compreender o tipo de informação que vai armazenar, onde está e qual seria o impacto de uma falha no recebimento de dados. Um inventário das informações e a classificação das mesmas, são informaçãoes importantes para todos os ambientes de negócio, e é particularmente importante que as empresas compreendam a sensibilidade dos dados atualmente armazenados dentro da empresa, até que eles sejam migrados para um ambiente de *Cloud*.

Neste artigo foi abordado a segurança na *Cloud*, vantagens, desvantagens e vulnerabilidades que existem. Foi também abordada uma estratégia de proteção de dados proporcionando recomendações de como a informação deve ser tratada.

Para escolher a melhor forma de proteger a informação, é preciso ter noção da importância da informação a proteger. A primeira operação a concretizar, é definir o nível de privacidade necessária, e o nível de proteção pretendido. É preciso ter em atenção que nem todas as empresas estão dispostas a pagar para ter os dados na *Cloud*, contudo e após esta análise, conclui-se que é mais seguro ter os dados na *Cloud*.

Referências

Abbedi, I. M. (2014). *Cloud Management and Security*. Wiley.

Akamai. (09 de Outubro de 2017). *Data Security in Cloud Computing*. Obtido de https://www.akamai.com/uk/en/resources/data-security-in-cloud-computing.jsp

GFI. (Outubro de 2017). On-premise vs. cloud-based solutions.

Halpert, B. (2011). *Auditing Cloud Computing - A Security and Privacy Guide*. Wiley.

Huang, Z. (2015). *Cloud Computing and Security, First International Conference, ICCCS 2015*. Springer.

Kan Yang, X. J. (2014). *Security for Cloud Storage Systems*. Springer.

Linthicum, D. (18 de Maio de 2016). *The Benefits of Cloud Computing for the Enterprise*. Obtido de https://cloudacademy.com/blog/the-benefits-of-cloud-computing-for-the-enterprise/

Mather, T. (2009). *Cloud Security and Privacy*. O'Reilly.

Misra, S., Ajayi, O., & Odun-Ayo, I. (2018). Cloud Computing Security: Issues and Developments. *Proceedings of the World Congress on Engineering*. London: WCE .

Newcombe, L. (2012). *Securing Cloud Services: A pragmatic approach to security architecture in the Cloud*. IT Governance Publishing.

Osei-Opoku, E., Regaieg, R., & Koubaa, M. (2020). Review on Cloud Computing Security Challenges. *European Scientific Journal*.

Raghu Yeluri, E. C.-L. (2014). *Building the Infrastructure for Cloud Security - A Solutions View*. Apress Open.

Sen, A. (2018). *Security risk assessment in cloud computing domains*. Missouri: Missouri University of Science and Technology.

Seshachala, S. (Março de 2015). *Disadvantages of Cloud Computing*. Obtido de https://cloudacademy.com/blog/disadvantages-of-cloud-computing/

Tahir, R. (Abril de 2017). *Video Hosting Costs in Cloud vs. On-Premises Infrastructure*. Obtido de https://blog.vidizmo.com/cloud-vs.-on-premises-video-hosting-costs#gsc.tab=0

Viswanathan, P. (Outubro de 2016). *FAQ on Data Protection Strategies for Enterprise*. Obtido de https://www.lifewire.com/strategies-for-enterprises-to-ensure-data-protection-2373385

Winkler , V. (2011). Seguridad en la nube. Elsevier .

Zhu, S. Y. (2015). *Guide to Security Assurance for Cloud Computing*. Springer

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 29/12/2021
Aceitação/Acceptance: 19/02/2022

La informática y la ciencia de datos utilizando Deep learning

Javier Guaña-Moya[1], Nelson Salgado-Reyes[2], Charles Escobar-Terán[3]

eguana953@puce.edu.ec; nesalgado@puce.edu.ec; cescobar637@puce.edu.ec

[1] Pontificia Universidad Católica del Ecuador (PUCE), Quito, Ecuador.

[2] Pontificia Universidad Católica del Ecuador (PUCE), Quito, Ecuador.

[3] Pontificia Universidad Católica del Ecuador (PUCE), Quito, Ecuador.

Pages: 116-127

Resumen: La informática y la ciencia de datos, conjuntamente con la tecnología deep learning, perteneciente a machine learning, son ampliamente utilizados para identificar objetos en imágenes, transcribir el habla en texto, relacionar noticias, publicaciones o productos con los intereses de los usuarios y seleccionar resultados de búsqueda relevantes impulsando casi todos los aspectos de la sociedad moderna, especialmente el deep learning que ha logrado grandes avances en la resolución de problemas que han resistido los mejores intentos de la comunidad de inteligencia artificial durante muchos años, resultando muy efectivo para descubrir complicadas estructuras en una gran cantidad de datos de alta dimensión y, en consecuencia, aplicable a múltiples dominios de la ciencia, el gobierno y los negocios. El objetivo de la presente revisión bibliográfica es presentar una descripción general del deep learning, establecer una definición conceptual, revisar el origen de esta tecnología, entender la finalidad, la relación con la ciencia de datos, las maneras en que funciona y conocer la amplia variedad de aplicaciones en las distintas áreas de la vida cotidiana moderna.

Palabras-clave: Informática; ciencia de datos; deep learning; machine learning; inteligencia artificial.

Computing and data science using deep learning

Abstract: Computer science and data science, together with deep learning technology, belonging to machine learning, are widely used to identify objects in images, transcribe speech into text, relate news, publications or products with the interests of users and select results. relevant search engines powering almost every aspect of modern society, especially deep learning which has made great strides in solving problems that have withstood the best attempts of the AI community for many years, proving very effective in uncovering complicated structures in a large amount of high-dimensional data and, consequently, applicable to multiple domains of science, government and business. The objective of this bibliographic review is to present a general description of deep learning, establish a conceptual definition, review the origin of this technology, understand the purpose, the relationship with

data science, the ways in which it works and know the wide variety of applications in the different areas of modern daily life.

Keywords: Computing; data science; deep learning; machine learning; artificial intelligence.

1. Introducción

La ciencia de datos conjuntamente con la tecnología de machine learning impulsa muchos aspectos de la sociedad moderna, desde búsquedas online hasta filtrado de contenido en redes sociales y recomendaciones en sitios web de comercio electrónico, estando cada vez más presente en productos de consumo como cámaras y teléfonos inteligentes. Estos sistemas de machine learning se utilizan para identificar objetos en imágenes, transcribir el habla en texto, relacionar noticias, publicaciones o productos con los intereses de los usuarios y seleccionar resultados de búsqueda relevantes, usando cada vez con mayor frecuencia una clase de técnicas conocidas como "Deep Learning" (LeCun et al., 2015).

El deep learning permite que los modelos computacionales compuestos de variadas capas de procesamiento aprendan representaciones de datos con múltiples niveles de abstracción, mejorando drásticamente estos métodos el estado del arte en el reconocimiento de voz y de objetos visuales, detección de objetos y muchos otros dominios, como el descubrimiento de fármacos y la genómica. Asimismo, el deep learning descubre estructuras intrincadas en grandes conjuntos de datos mediante el uso del algoritmo de propagación hacia atrás para indicar cómo una máquina debe cambiar los parámetros internos usados para calcular la representación en cada capa a partir de la representación en la capa anterior, generando las redes convolucionales profundas avances en el procesamiento de imágenes, video, voz y audio, mientras que las redes recurrentes han arrojado luz sobre datos secuenciales como texto y voz (LeCun et al., 2015).

En consecuencia, el deep learning está logrando grandes avances en la resolución de problemas que han resistido los mejores intentos de la comunidad de inteligencia artificial durante muchos años, resultando muy efectivo para descubrir complicadas configuraciones en datos de gran extensión y, por lo tanto, es aplicable a múltiples dominios de la ciencia, el gobierno y los negocios, batiendo récords en reconocimiento de imágenes(Tompson et al., 2014), reconocimiento de voz(Sainath et al., 2013) y en otras técnicas de machine learning en la predicción de la actividad de posibles moléculas de fármacos (Ma et al., 2015), el análisis de datos de aceleradores de partículas (Ciodaro et al., 2012), la reconstrucción de circuitos cerebrales(Helmstaedter et al., 2013) y la predicción de los efectos de mutaciones en el ADN no codificante sobre la expresión génica y la enfermedad (Xiong et al., 2015) y, quizás lo más sorprendente, el deep learning ha arrojado resultados altamente prometedores para diversas tareas en la comprensión del lenguaje natural (Collobert et al., 2011), en particular, la clasificación de temas, el análisis de sentimientos, la respuesta a preguntas (Bordes et al., 2014) y la traducción de idiomas (Jean et al., 2015).

Es por lo anterior que la presente revisión bibliográfica extrae información relevante del deep learning revisando el origen de este método, estableciendo una definición

conceptual, la estrecha relación con la ciencia de datos, el objetivo que posee, la forma de funcionar y las diversas aplicaciones informáticas en variadas áreas de la vida moderna.

2. Ciencia de datos

Hace más de 50 años, se definió el análisis de datos como un esfuerzo amplio, mucho más amplio que las estadísticas matemáticas tradicionales, lo que en la actualidad ha derivado en el término "ciencia de datos", que ha llamado mucho la atención por la aplicación en diversos ámbitos, tal como los negocios, en el gobierno y en las áreas académicas de estadística e informática. Algunos autores señalan que la ciencia de datos se basa en la estadística y la informática, aplicando algunos de sus métodos y, principalmente, combinándolos, reenfocándolos y desarrollándolos para abordar el contexto y las necesidades del análisis de datos científicos modernos (Blei & Smyth, 2017).

La ciencia de datos suele ser un concepto que unifica estadísticas, análisis de datos y los métodos relacionados para comprender y analizar los fenómenos reales con datos. Por tanto, se define básicamente como el estudio de los datos, donde un producto de datos es un entregable de datos, habilitado o guiado por datos, lo cual puede ser un descubrimiento, predicción, servicio, sugerencia, conocimiento en la toma de decisiones, pensamiento, modelo, paradigma, herramienta o sistema (Cao, 2017).

El objetivo principal de la ciencia de datos es dar sentido a estos y obtener esta comprensión es un proceso de varios pasos que dependen de las especificaciones de un proyecto en particular, lo cual incluye la recopilación y el procesamiento de grandes cantidades de datos. Si, por otro lado, la carga de datos ya se ha completado, está directamente dentro del dominio de la ciencia de datos realizar los análisis predictivos utilizando herramientas como algoritmos de machine learning y redes neuronales de deep Learning (Variawa, 2019).

3. Definición de deep learning

Se conoce como deep learning al subcampo del machine learning relacionado con algoritmos inspirados en la estructura y función del cerebro llamados redes neuronales artificiales (Brownlee, 2019). Estas redes neuronales intentan simular el comportamiento del cerebro humano, lo que le permite aprender de grandes cantidades de datos y si una red neuronal con una sola capa puede realizar predicciones aproximadas, las capas ocultas adicionales pueden ayudar a optimizar y refinar la precisión (IBM Cloud Education, 2020b).

Otros autores señalan que el deep learning comprende el conjunto de métodos de representación-aprendizaje con múltiples niveles de representación, obtenidos mediante la composición de módulos simples pero no lineales, cada uno de los cuales transforma la representación en un nivel, comenzando con la entrada sin procesar, en una representación en un nivel superior, un poco más abstracto, siendo el aspecto clave el que estas capas de características no están diseñadas por ingenieros humanos: se aprenden de los datos mediante un procedimiento de aprendizaje de propósito general (Brownlee, 2019).

Por lo general, se emplean los términos de inteligencia artificial, machine learning y deep learning de manera indistinta, sin embargo, por definición no representan lo mismo debido que abarcan distintas áreas:

- **Inteligencia Artificial**: Es el término más general y se define como el trabajo por lograr la automatización de las labores intelectuales que son desarrolladas por los seres humanos normalmente. Abarca las áreas de machine learning y deep learning conjuntamente con otras técnicas como el razonamiento lógico y simbólico, la estadística y algoritmos de búsqueda. Comenzó en la década de los 50, cuando los especialistas en informática iniciaron estudios con el fin de determinar si era posible lograr que las computadoras razonaran por si mismas (López, 2017).
- **Machine Learning**: También conocido como aprendizaje automático, incluye al extenso grupo de técnicas informáticas que entregan a las computadoras la capacidad de aprender sin ser programadas de manera explícita. Existen variados modelos de algoritmos de machine learning, tal como los algoritmos genéticos y de agrupamiento, el aprendizaje por refuerzo y el basado en reglas de asociación, máquinas de vectores de soporte, árboles de decisión, redes neuronales y en la actualidad los algoritmos más conocidos dentro de esta área que son los de deep Learning (López, 2017).
- **Deep Learning:** Es un subcampo dentro del machine learning que emplea redes neuronales en esquemas diferentes para alcanzar el aprendizaje de capas sucesivas de representaciones de datos cada vez más relevantes; el término de deep o profundo distingue al número de capas de representaciones que son utilizadas en el modelo; por lo general son utilizadas grandes cantidades, decenas o centenares, de capas de representación, estás tienen la capacidad de aprender de manera automática en la proporción que el modelo es capacitado con los datos (López, 2017).

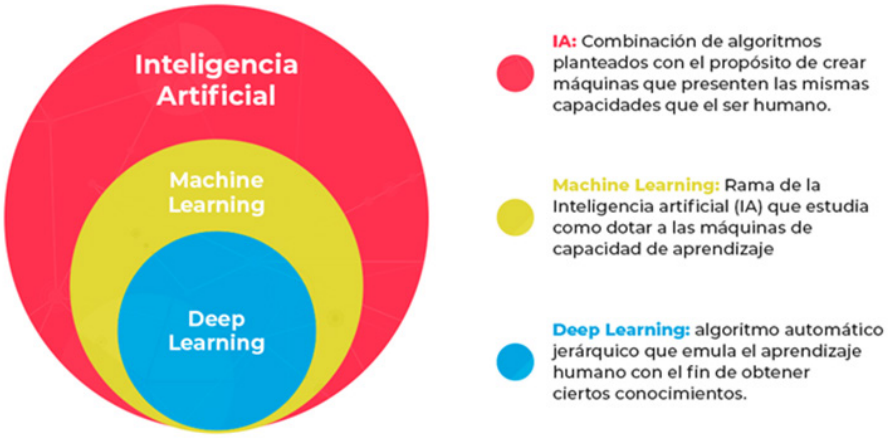


Figura 1 – Inteligencia artificial, Machine learning y Deep learning

Si bien la base teórica de deep learning surgió en la década de 1980, en la actualidad existen dos razones fundamentales por las que se ha maximizado la utilidad de este método:

1. Requiere grandes cantidades de datos etiquetados. Por ejemplo, el desarrollo de automóviles sin conductor requiere millones de imágenes y miles de horas de video.
2. Requiere una potencia informática sustancial y las GPUs de alto rendimiento tienen una arquitectura paralela que es eficiente para el deep learning, lo que permite que, al combinarse con clústeres o computación en la nube, los equipos de desarrollo reduzcan el tiempo de capacitación de semanas a horas o menos (MathWorks, 2022).

Por tanto, esta técnica de aprendizaje es una herramienta pionera para procesar grandes cantidades de datos, ya que el rendimiento de la máquina mejora a medida que analiza mayor cantidad de información, volviéndose más hábil para reconocer incluso patrones ocultos entre ellos. Además, debido a que la máquina también está aprendiendo de los datos procesados, puede realizar la extracción y abstracción de características automáticamente a partir de estos sin procesar, con poca o ninguna intervención humana (DeepAI, 2019).

En consecuencia, el deep learning facilita en gran medida la resolución de problemas, automatizando completamente lo que solía ser uno de los pasos más difíciles y cruciales en el flujo de trabajo de machine learning: la ingeniería de atributos. Previo al deep learning, para entrenar un modelo primero se debían refinar las entradas hasta adaptarlas al tipo de transformación del modelo, seleccionando cuidadosamente los atributos más representativos y desechando los poco informativos, por el contrario, este proceso se automatiza, aprendiendo todos los atributos de una sola pasada, encargándose de adaptarse y quedándose con lo más representativo (López, 2017).

4. Cómo funciona el deep learning

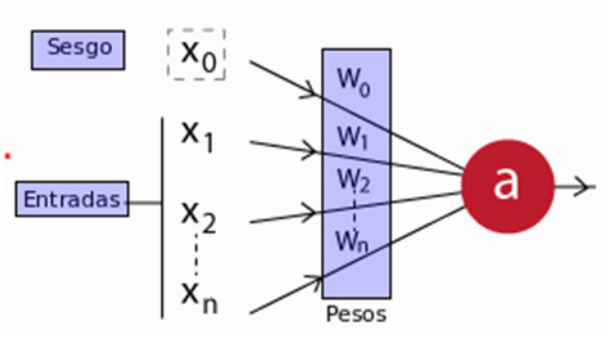
El deep learning es una función de la inteligencia artificial que imita el funcionamiento del cerebro humano al procesar datos y crear patrones que son usados en la toma de decisiones. Gracias a los avances de la neurociencia, al diagnóstico por imagen y los estudios de casos clínicos de daño cerebral sobrevenido se conoce que existen centros específicos del lenguaje, así como redes especializadas en detectar diversos aspectos de la visión, como bordes, inclinación de líneas, simetría e incluso áreas íntimamente relacionadas con el reconocimiento de rostros y la expresión emocional de los mismos (Arrabales, 2016).

Basado en lo anterior, el deep learning es un subconjunto de aprendizaje automático en inteligencia artificial que tiene redes neuronales capaces de aprender sin supervisión humana, a partir de datos no estructurados o sin etiquetar, considerando que los datos, los cuales normalmente no están estructurados, son tan vastos que a los humanos les puede llevar décadas entenderlos y extraer información relevante, por esta razón mayor cantidad de empresas se han dado cuenta del increíble potencial que puede surgir al revelar esta gran cantidad de información, adaptándose cada vez más a los sistemas de inteligencia artificial para el soporte automatizado. Por tanto, el deep learning desentraña

grandes cantidades de datos no estructurados que los humanos podrían tardar décadas en comprender y procesar (eCycle, 2020).

Estas redes neuronales o redes artificiales de deep learning realizan el intento de imitar el funcionamiento del cerebro a través de una combinación de entradas de datos, pesos y sesgos, elementos que trabajan conjuntamente para reconocer, clasificar y describir con precisión los objetos dentro de los datos; consistiendo estas redes neuronales profundas en múltiples capas de nodos interconectados, cada uno de los cuales se basa en la capa anterior para refinar y optimizar la predicción o categorización, conociendo esta progresión de cálculos a través de la red como propagación directa. Las capas de entrada y salida de una red neuronal profunda se denominan capas visibles, siendo la capa de entrada donde el modelo de aprendizaje profundo introduce los datos para el procesamiento y la capa de salida donde se realiza la predicción o clasificación final (IBM Cloud Education, 2020b).

De manera gráfica, cada una de estas neuronas posee una forma similar al siguiente esquema:



Aplicando la siguiente fórmula:

$$\propto = f\left(\sum_{i=0}^{n} W_i * X_i\right)$$

Donde:

$X_1, X_2 \ldots X_n$:	Representa los datos de entrada en la neurona, en ocasiones puede ser producto de otra neurona de la red.
X_o:	Es la unidad de sesgo, valor constante que se suma a la entrada de la función de activación de la neurona, generalmente es 1.
$W_o, W_1, W_2 \ldots W_n$:	Pesos relativos de cada entrada.
a:	Salida de la neurona.
f:	Función de activación de la neurona.

El proceso anterior describe el tipo más simple de red neuronal profunda en los términos más sencillos. Sin embargo, los algoritmos de aprendizaje profundo son increíblemente complejos y existen diferentes tipos de redes neuronales para abordar problemas o

conjuntos de datos específicos, entre los cuales se tienen las convolucionales (CNN) y las recurrentes (RNN)(IBM Cloud Education, 2020b).

Las redes neuronales convolucionales (CNN) se utilizan principalmente en aplicaciones de clasificación de imágenes y visión por computadora, pueden detectar características y patrones dentro de una imagen, lo que permite tareas, como la detección o el reconocimiento de objetos (IBM Cloud Education, 2020b). Este tipo de redes neuronales se distinguen de otras redes por el rendimiento superior con entradas de señales de imagen, voz o audio, y poseen tres tipos principales de capas, que son: la capa convolucional donde ocurren la mayoría de los cálculos; la capa de agrupación que reduce la dimensionalidad disminuyendo la cantidad de parámetros en la entrada; y la capa totalmente conectada donde cada nodo de la capa de salida se conecta directamente a un nodo de la capa anterior (IBM Cloud Education, 2021).

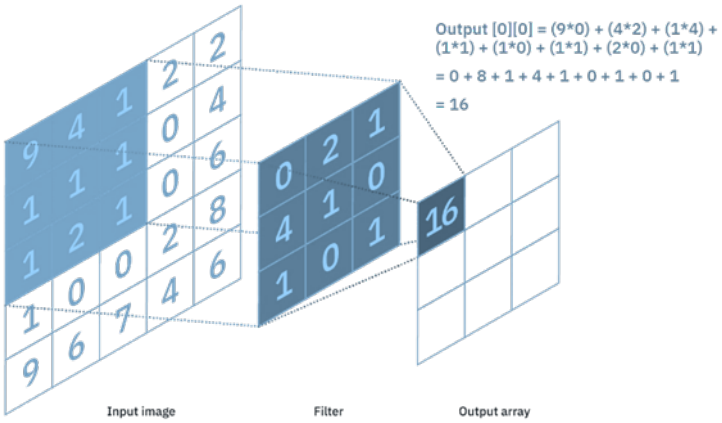


Figura 2 – Red neuronal convolucional

Las CNN eliminan la necesidad de extracción manual de características, por lo que no necesita identificar las características utilizadas para clasificar las imágenes, las sacan directamente de estas. Además, las características relevantes no están preentrenadas, estas se preparan en la medida que la red se entrena en un conjunto de imágenes, causando que a través de esta selección automatizada de características los modelos de aprendizaje profundo sean altamente exactos para labores de visión artificial como el ordenamiento de objetos (MathWorks, 2022).

Por otra parte, las redes neuronales recurrentes (RNN) normalmente son empleadas en aplicaciones de lenguaje natural y reconocimiento de voz, ya que aprovechan datos secuenciales o de series temporales (IBM Cloud Education, 2020b). Poseen la característica distintiva de compartir el mismo parámetro de peso dentro de cada capa de la red, ajustando los pesos por medio de los procesos de retropropagación y descenso de gradiente para facilitar el aprendizaje por refuerzo (IBM Cloud Education, 2020a).

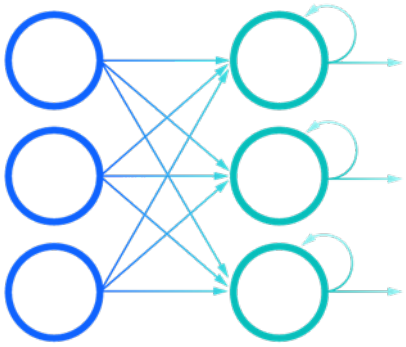


Figura 3 – Red neuronal recurrente

El proceso llamado retropropagación usa algoritmos, como el descenso de gradiente, para calcular los errores en las predicciones y luego ajusta los pesos y sesgos de la función moviéndose hacia atrás a través de las capas en un esfuerzo por entrenar el modelo, permitiendo el trabajo conjunto entre la propagación directa y la retropropagación que una red neuronal haga predicciones y corrija cualquier error en consecuencia, volviéndose el algoritmo más preciso con el paso del tiempo, permitiendo que las redes neuronales aprendan (IBM Cloud Education, 2020b; López, 2017).

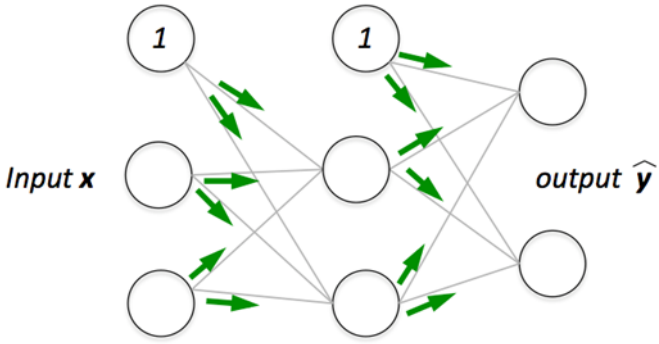


Figura 4 – Esquema de la propagación hacia atrás o retropropagación

5. Utilidades del deep learning

El deep learning constituye un elemento significativo gracias a la potencial utilidad en las diferentes aplicaciones disponibles en la vida real, debido que puede ser empleado con éxito en grandes cantidades de datos para el descubrimiento y aplicación de conocimientos, así como a la ejecución de predicciones a partir de estos datos,

especialmente por las altas tasas de éxito en entrenamientos no supervisados. Por ejemplo, las redes de deep learning aprenderían a identificar perros, aunque las imágenes no estuvieran identificadas con la etiqueta "perro" (García, 2020).

Los autos sin conductores, constituyen una de las aplicaciones más fascinantes del deep learning, las maquinas no aprenden a conducir por sí solas, lo hacen a partir del conocimiento y la experiencia de personas reales, alcanzando la capacidad de actuar en los distintos escenarios que el mundo real puede presentar, como señales de tráfico, obstrucciones en la vía y/o peatones cruzando la calle (eCycle, 2020).

Igualmente, los asistentes virtuales como Alexa, Cortana y Siri también son claros ejemplos de deep learning, debido que tienen la capacidad de reconocer el habla, comprender un comando y hacer una acción o tarea específica(da Silva, 2021). Skype traduce conversaciones habladas en tiempo real, muchas plataformas de correo electrónico pueden identificar el spam incluso antes de que llegue a la bandeja de entrada y PayPal ha implementado un deep learning para evitar pagos fraudulentos, entre otras aplicaciones (eCycle, 2020).

También se encuentran las herramientas de reconocimiento facial, ya sea en sistemas de vigilancia, filtros de Instagram o etiquetas de amigos de Facebook, considerando que las personas cambian de apariencia a lo largo de la vida y la máquina necesita adaptar la mirada para reconocer la identidad de las mismas. Además, la mayoría de las organizaciones ponen a disposición de los usuarios en línea los chatbots, que son programados con algoritmos sofisticados, capaces de ofrecer respuestas personalizadas con el fin de optimizar el servicio al cliente (da Silva, 2021).

Entre los principales problemas de la vida real donde las distintas empresas actualmente están aplicando deep learning se puede mencionar:

- Identificación de empresas mediante logotipos o marcas publicadas en fotos en las redes sociales.
- Uso de imágenes en sustitución de palabras clave para la búsqueda de productos o servicios de una empresa o elementos similares.
- Direccionamiento de la publicidad y pronóstico las preferencias de los usuarios.
- Seguimiento en tiempo real de las reacciones de los usuarios de canales en línea durante el lanzamiento de algún producto o servicio.
- Reconocimiento y seguimiento de los niveles de confianza de los clientes, opiniones y actitud en diferentes canales online y servicios de soporte automatizado al cliente.
- Descubrimiento de fraudes, recomendaciones a los clientes y gestión de atención con los mismos.
- Determinación de clientes potenciales.
- Mayor comprensión de diversas patologías, mutaciones de enfermedades y terapias en el área de la genética.
- Investigación del posible empleo de medicamentos y fármacos, ya conocidos y probados, en tratamientos de enfermedades novedosas.
- Incremento de la precisión diagnóstica en el análisis de resonancias magnéticas y radiografías, con reducción de tiempo y costos, en comparación con los métodos tradicionales.

- Análisis, pronóstico, detección y prevención en tiempo real de amenazas complejas en el área de la ciberseguridad.
- Identificación en textos de sentimientos positivos y negativos, temas y palabras clave.
- Reconocimiento de rostros y determinación de emociones mediante el análisis facial.
- Identificación de voces y sonidos.
- Catalogar vídeos (García, 2020).

A pesar de los innumerables y constantes desarrollos tecnológicos disponibles, el deep learning sigue siendo un amplio campo de la informática pendiente de exploración, por lo que con seguridad se continuarán recibiendo avances en áreas cada vez más novedosas mediante el empleo de estas técnicas, inclusive facilitando a los seres humanos el desarrollo de la ciencia, software y mucho más.

6. Conclusiones

El cada vez mayor volumen de datos necesarios para procesar información ha propiciado el desarrollo del machine learning, conjuntamente con los avances tecnológicos de GPUs de alto rendimiento que permiten reducir el tiempo de capacitación para una red de deep learning de semanas a horas o menos, con una amplia variedad de aplicaciones en diversas áreas como visión artificial, análisis predictivo, asistentes virtuales, chabots, robótica, salud, entretenimiento, noticias y publicidad, música y más.

Se define deep learning como el subcampo del machine learning que se relaciona con redes neuronales artificiales, algoritmos inspirados en la estructura y función del cerebro, con la finalidad de simular el comportamiento del mismo, lo que permite aprender de grandes cantidades de datos con una precisión cada vez más óptima y refinada, planteando a un futuro no muy lejano el paso del aprendizaje automático al aprendizaje no supervisado, donde los algoritmos posean la capacidad de aprender sin previa intervención humana, obteniendo por si mismos las conclusiones y resultados acerca de la semántica incorporada en los datos analizados.

La presente revisión bibliográfica permite concluir que el deep learning constituye un elemento significativo gracias a la utilidad potencial que posee al ser usado en las diversas aplicaciones disponibles en la vida moderna, demostrando ser altamente efectivo en el manejo de grandes cantidades de datos, para el descubrimiento y aplicación de conocimientos novedosos, así como para la ejecución de predicciones a partir de estos datos, especialmente por las altas tasas de éxito en entrenamientos no supervisados.

Referencias

Arrabales, R. (2016, marzo 29). *Deep Learning: Qué es y por qué va a ser una tecnología clave en el futuro de la inteligencia artificial*. Xataka. https://www.xataka.com/robotica-e-ia/deep-learning-que-es-y-por-que-va-a-ser-una-tecnologia-clave-en-el-futuro-de-la-inteligencia-artificial

Blei, D. M., & Smyth, P. (2017). Science and data science. *Proceedings of the National Academy of Sciences of the United States of America*, *114*(33), 8689-8692. https://doi.org/10.1073/pnas.1702076114

Bordes, A., Chopra, S., & Weston, J. (2014). Question Answering with Subgraph Embeddings. *arXiv:1406.3676 [cs]*. http://arxiv.org/abs/1406.3676

Brownlee, J. (2019, agosto 15). What is Deep Learning? *Machine Learning Mastery*. https://machinelearningmastery.com/what-is-deep-learning/

Cao, L. (2017). Data Science: A Comprehensive Overview. *ACM Computing Surveys*, *50*(3), 43:1-43:42. https://doi.org/10.1145/3076253

Ciodaro, T., Deva, D., Seixas, J. M. de, & Damazio, D. (2012). Online particle detection with Neural Networks based on topological calorimetry information. *Journal of Physics: Conference Series*, *368*, 012030. https://doi.org/10.1088/1742-6596/368/1/012030

Collobert, R., Weston, J., Bottou, L., Karlen, M., Kavukcuoglu, K., & Kuksa, P. (2011). Natural Language Processing (Almost) from Scratch. *NATURAL LANGUAGE PROCESSING*, *12*, 45.

da Silva, D. (2021, junio 15). *Deep learning vs Machine Learning*. Zendesk MX. https://www.zendesk.com.mx/blog/deep-learning-vs-machine-learning/

DeepAI. (2019, mayo 17). *Deep Learning*. DeepAI. https://deepai.org/machine-learning-glossary-and-terms/deep-learning

eCycle. (2020). *Aprendizagem profunda: Entenda a deep learning*. https://www.ecycle.com.br/aprendizagem-profunda/

García, C. (2020). *¿Qué es el Deep Learning y para qué sirve?* indra - Blog Neo. https://www.indracompany.com/es/blogneo/deep-learning-sirve

Helmstaedter, M., Briggman, K. L., Turaga, S. C., Jain, V., Seung, H. S., & Denk, W. (2013). Connectomic reconstruction of the inner plexiform layer in the mouse retina. *Nature*, *500*(7461), 168-174. https://doi.org/10.1038/nature12346

IBM Cloud Education. (2020a). *What are Recurrent Neural Networks?* https://www.ibm.com/cloud/learn/recurrent-neural-networks

IBM Cloud Education. (2020b). *What is Deep Learning?* https://www.ibm.com/cloud/learn/deep-learning

IBM Cloud Education. (2021, enero 6). *What are Convolutional Neural Networks?* https://www.ibm.com/cloud/learn/convolutional-neural-networks

Jean, S., Cho, K., Memisevic, R., & Bengio, Y. (2015). On Using Very Large Target Vocabulary for Neural Machine Translation. *arXiv:1412.2007 [cs]*. http://arxiv.org/abs/1412.2007

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436-444. https://doi.org/10.1038/nature14539

López, R. (2017). *Introducción al Deep Learning*. Matemáticas, análisis de datos y python. https://relopezbriega.github.io/blog/2017/06/13/introduccion-al-deep-learning/

Ma, J., Sheridan, R. P., Liaw, A., Dahl, G. E., & Svetnik, V. (2015). Deep Neural Nets as a Method for Quantitative Structure–Activity Relationships. *Journal of Chemical Information and Modeling*, *55*(2), 263-274. https://doi.org/10.1021/ci500747n

MathWorks. (2022). *What Is Deep Learning? | How It Works, Techniques & Applications*. https://www.mathworks.com/discovery/deep-learning.html

Sainath, T. N., Mohamed, A., Kingsbury, B., & Ramabhadran, B. (2013). Deep convolutional neural networks for LVCSR. *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 8614-8618. https://doi.org/10.1109/ICASSP.2013.6639347

Tompson, J., Jain, A., LeCun, Y., & Bregler, C. (2014). Joint Training of a Convolutional Network and a Graphical Model for Human Pose Estimation. *arXiv:1406.2984 [cs]*. http://arxiv.org/abs/1406.2984

Variawa, R. (2019, diciembre 6). *Machine Learning vs. Deep Learning vs. Data Science*. Medium. https://becominghuman.ai/machine-learning-vs-deep-learning-vs-data-science-484cfa520bf7

Xiong, H. Y., Alipanahi, B., Lee, L. J., Bretschneider, H., Merico, D., Yuen, R. K. C., Hua, Y., Gueroussov, S., Najafabadi, H. S., Hughes, T. R., Morris, Q., Barash, Y., Krainer, A. R., Jojic, N., Scherer, S. W., Blencowe, B. J., & Frey, B. J. (2015). The human splicing code reveals new insights into the genetic determinants of disease. *Science (New York, N.Y.)*, *347*(6218), 1254806. https://doi.org/10.1126/science.1254806

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 07/12/2021
Aceitação/Acceptance: 06/02/2022

Aplicación del Criterio de Minimización de Movimientos Totales en una Fábrica de armas y municiones

Ana Alvarez[1,2], David Andrés Guachamín[1], Alexis Suárez del Villar[1,2]

anaalvarez@indoamerica.edu.ec; dguachamin@indoamerica.edu.ec; asuarez@indoamerica.edu.ec

[1]Facultad de Ingeniería y Tecnologías de la Información y la Comunicación, Universidad Tecnológica Indoamérica, 170-301, Quito, Ecuador

[2] Grupo de Investigación en Sistemas Industriales, Software y Automatización SISAu, Universidad Tecnológica Indoamérica, 170-301, Quito, Ecuador

Pages: 128-138

Resumen: Al surgir la fábrica de armas y municiones en estudio, los seis puestos de trabajo analizados se fueron ubicando en correspondencia a su aparición o necesidad. Esta investigación presenta la aplicación del Método del Criterio de Minimización de Movimientos Totales con un estudio para optimizar el tiempo de producción. La agrupación de la serie de datos empleadas en el diagnóstico de la situación actual permitió determinar que la operación de Colocación de Fulminante en la bala tiene 768,89 TMU (unidad de medida de tiempo) correspondiendo a 27,68 segundos siendo los más altos de todo el proceso y el total recorrido es de 58811,1 metros. Con una nueva propuesta de reubicación de las estaciones de trabajo se obtienen 391,7 TMU (unidad de medida de tiempo) que transformados son 14,1 segundos, el resultado obtenido fue de 28178,3 metros de recorrido con una reducción en la distancia total de 30632,8 metros.

Palabras-clave: bimanual; minimización; movimientos; municiones; redistribución.

Application of the Total Movements Minimization Criterion in a Weapons and Ammunition Factory

Abstract: As the arms and ammunition factory under study came into being, the six workstations analyzed were positioned according to their appearance or need. This research presents the application of the Total Movements Minimization Criteria Method with a study to optimize production time. The grouping of the series of data used in the diagnosis of the current situation allowed to determine that the operation of Placement of Fulminant in the bullet, has 768.89 TMU (time measurement unit) corresponding to 27.68 seconds being the highest of the whole process and the total traveled is 58811.1 meters. With a new proposal for the relocation of the work stations, 391.7 TMU (time measurement unit) were obtained,

which transformed into 14.1 seconds, the result obtained was 28178.3 meters of travel with a reduction in the total distance of 30632.8 meters.

Keywords: two-handed; minimization; movements; ammunition; redistribution.

1. Introducción

La investigación y el desarrollo militar en el mundo moderno no solo es uno de los principales factores para construir el poder militar de un estado, fortalecer su independencia estratégica y garantizar ventajas tecnológicas significativas sobre un adversario potencial (Gilkova, 2022), sino también un factor importante que proporciona un impacto positivo tanto sobre el desarrollo del progreso científico y tecnológico en general, y sobre el desarrollo de la economía del Estado (Koç, 2022)

A lo largo del tiempo los pedidos de munición han aumentado de igual manera las cantidades y cada vez los tiempos de entrega son más cortos (Ameloot C., 2022), debido a esto la institución está en la obligación de mantener un producto de calidad (Kan, 2022), ya que la empresa es monopólica y es la única en el Ecuador certificada para la fabricación de munición, motivo por el cual es necesario realizar una reorganización de puestos de trabajo del área de municiones (McNeilly, 2022) y de esta manera facilitar el trabajo evitando movimientos innecesarios y optimizando al máximo los tiempos de movimientos entre áreas (Galarza, 2020).

Cuando el departamento de ventas recibe un pedido se procede de la siguiente manera (Skalny, 2021). Las órdenes de producción son evaluadas por el departamento de comercialización y los técnicos en armas y municiones (Wang, 2021), en base a esta evaluación se emiten las órdenes de trabajo y todas son tomadas de acuerdo a la cantidad y tiempo de entrega, que por lo general es muy corto. En la actualidad y puntualmente en el área de municiones, no cuenta con un estudio de movimientos en los diferentes puestos de trabajo (Hongzhi, 2021)

Uno de los puntos en los que la organización ha estado pendiente de cumplir es con los tiempos de entrega (Liu, 2021), y muchas veces lastimosamente no se han podido efectuar en el tiempo estimado ya que las áreas no están organizadas de forma óptima para poder realizar la producción de munición (Vu, 2021) (Carlos, 2016), motivo por el cual se procederá a iniciar esta mejora con el criterio de minimización de movimientos totales en el área de municiones (Xu, 2021).

2. Metodología

Con la observación directa se establece una relación concreta e intensiva entre los investigadores y el acontecimiento, de los cuales se obtienen datos que luego se sintetizan para desarrollar la investigación, mediante este método se puedo evidenciar datos esenciales para emplear los métodos de evaluación respectivos. Los therbligs pueden clasificarse en eficientes e ineficientes. Los Eficientes son los que contribuyen al avance productivo del trabajo los cuales pueden ser reducidos, pero no eliminados del todo por ser parte esencial del proceso; los Ineficientes no hacen avanzar el trabajo, por lo que deben ser eliminados en lo posible para mejorar la línea de producción; son los

componentes básicos del patrón de movimiento. En esencia se identifican las diferentes actividades de las dos manos. Para efectos del diagrama bimanual cada Therbligs tiene un símbolo, una designación cromática y una letra (Iván, 2017), al identificarse se aplican en el sistemas de tiempos predeterminados en el MTM (Medida de Tiempo de Método) para el cálculo de cada uno de los tiempos de ciclo del proceso en este estudio de operación de Colocación de Fulminante en la bala.

3. Análisis de los tiempos en los seis puestos de trabajo del Área de municiones

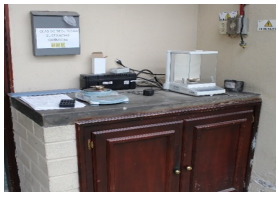
De acuerdo al estudio realizado en base a los datos recolectados en el área de producción de municiones y las actividades que se desempeñan en cada uno de los puestos de trabajo, se identificaron seis áreas de trabajo (Figura 1) y en cada una mediante el diagrama bimanual se detallaron todos los micromovimientos con sus respectivos tiempos en minutos y en TMU (unidad de medida de tiempo), tenemos como dato general que el puesto que más tiempo toma en realizar el trabajo es la Colocación de fulminante donde se registra un tiempo de 768.89 TMU y el puesto de trabajo 3 es la que menos tiempo tiene de ciclo con 200 TMU (unidad de medida de tiempo), el resumen por Puesto de Trabajo (PT) lo podemos ver en la Tabla 1.

PT_1	PT_2	PT_3	PT_4	PT_5	PT_6
768,89 TMU	658,33 TMU	200,00 TMU	455,56 TMU	475,00 TMU	394,44 TMU
27,68 seg	23,70 seg	7,2 seg	16,40 seg	17,1 seg	14,20 seg

Tabla 1 – Tiempo total por puesto de trabajo



PT_1. Colocación del fulminante



PT_2. Pesaje de la Pólvora



PT_3. Encapsulado de Pólvora



PT_4. Colocación de la bala



PT_5. Códificación



PT_6. Empacado

Figura 1 – Estaciones de trabajo del Área de municiones.

3.1. Distribución actual del Área de municiones

En la etapa de diagnóstico el área de Municiones estaba distribuida como se puede ver en el Layout de la Figura 2, para el estudio primero se identificaron los puestos de trabajo que se visualizaron en la Figura 1, seguido se analizaron los desplazamientos colocándose una línea verde que indica desde donde comienza en la Bodega y la finalización con el Empaque del producto terminado. Permitiendo a su vez determinar cuáles eran los PT que tenían una relación directa e indirecta. A continuación, obtuvimos la Tabla 2, en la cual se refleja los valores obtenidos del doble sentido de los movimientos entre todos los puestos de trabajo en unidad de medida de tiempo (TMU), existiendo PT que no tienen relación entre sí, es por ese motivo que en esos lugares tenemos un registro de cero movimientos.

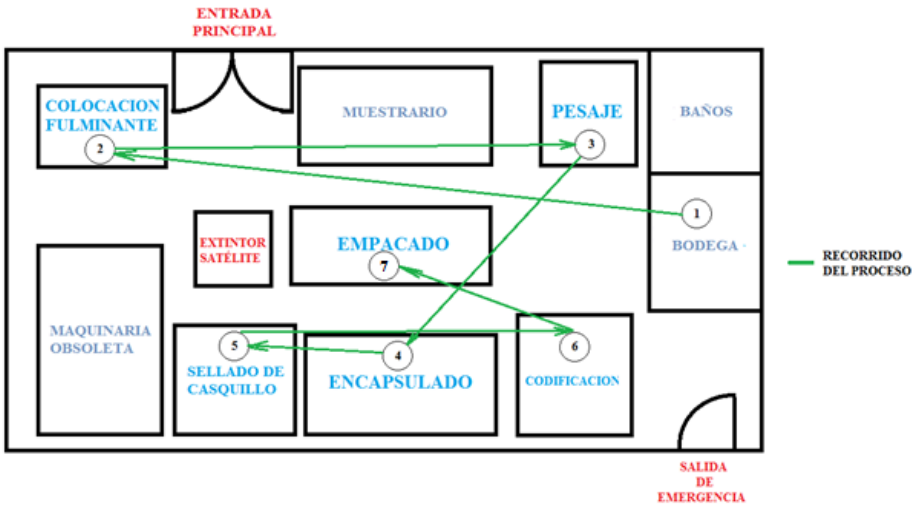


Figura 2 – Layout y recorrido actual del Área de municiones.

Movimientos entre áreas (TMU)	PT_1	PT_2	PT_3	PT_4	PT_5	PT_6	PT_7
PT_1	X	0	333,3	0	555,6	0	0
PT_2	0	X	0	338,9	433,3	0	0
PT_3	0	144,4	X	0	355,6	244,4	0
PT_4	0	0	0	X	222,2	0	155,6
PT_5	566,7	0	438,9	0	X	316,7	366,7
PT_6	0	0	300	0	250,0	X	0
PT_7	0	0	0	0	327,8	0	X

Tabla 2 – Sentido de los Movimientos entre Puestos de Trabajo en TMU.

3.2. Doble Sentido de los Movimientos entre Puestos de Trabajo

Se realizó un registro de los movimientos totales utilizando los resultados de la Tabla 2, con la aplicación del Criterio de Minimización de Movimientos Totales y valorando el doble sentido de los movimientos se resumen la tabla triangular número 3, que también incluye las distancias en metros de un puesto a otro.

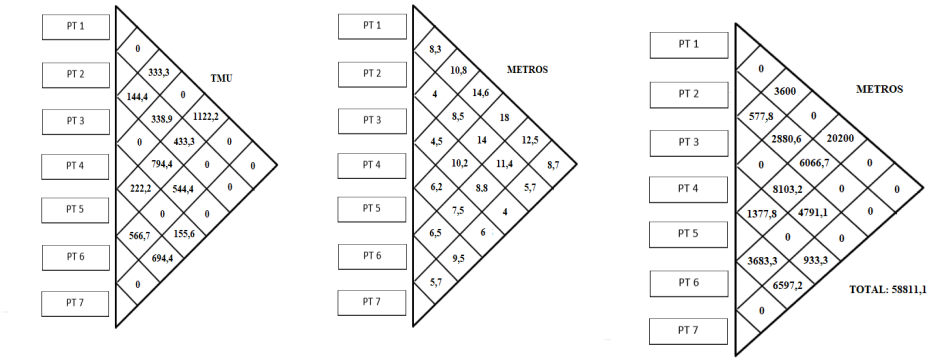


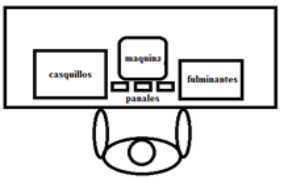
Tabla 3 – Movimientos Totales entre Puestos de Trabajo mediante tablas triangulares con el cálculo de las distancias.

Como principal limitación de la investigación tuvimos que al momento de la toma de datos los puestos de trabajo ya identificadas previamente no tenían un orden secuencial de producción, tampoco el personal operativo realizaba las tareas de su puesto de trabajo como está reglamentado, porque al existir déficit de mano de obra se realizaron contrataciones sin haber estado adiestrados en las tareas y actividades inherentes al cargo que ocupan, por lo que como investigadores trabajamos con los trabajadores que tienen un 100 % de ritmo de trabajo.

3.3. Propuesta de solución

Se propusieron nuevos diagramas bimanuales para cada PT, que contienen rediseños en las disposiciones del lugar de trabajo considerándose los principios de la economía de los movimientos y la minimización de movimientos totales por cada PT, se muestran en las Tablas 4 y 5 los diagramas de los PT_1-Pesaje de Pólvora con 14,1 segundos y PT_3 - Encapsulado de Pólvora con 6,2 segundos, por ser los que tenían mayor (27,68 segundos) y menor (7,2 segundos) tiempo en la etapa de diagnóstico.

DIAGRAMA BIMANUAL

Diagrama N°: 1 (ciclo1) Hoja N°: 1 de 6	**Disposición del lugar de trabajo**
Dibujo y Pieza:	**Propuesto** 
Operación: Colocación de Fulminante	
Investigadores	
Lugar: Área de municiones	

Ambas manos deben comenzar, así como completar sus movimientos a la vez
Ambas manos no deben estar inactivas a la vez, excepto durante los periodos de descanso
Los movimientos de los brazos deben hacerse en direcciones opuestas y simétricas y deben realizarse automáticamente
Los movimientos de las manos deben quedar confinados a la clasificación más baja con la que sea posible ejecutar satisfactoriamente el trabajo.
La clasificación más baja requiere por lo general el mínimo tiempo y esfuerzo
Clasificación general de los movimientos de las manos:
Movimientos de los dedos (clasificación más baja)
Movimientos que comprenden dedos, muñeca y antebrazo
Movimientos que comprenden dedos, muñeca, antebrazo y brazo
Movimientos que comprenden dedos, muñeca, antebrazo, brazo y hombro
Siempre que sea posible, debe emplearse la impulsión para ayudar al

COD	TIEMPO (SEG)	Descripción de Mano Izquierda	O	⇨	▽	D	O	⇨	▽	D	Descripción de Mano Derecha	TIEMPO (SEG)	COD
RC	1,3	alcanza casquillo									alcanzar fulminante	1,3	RC
G4A	0,4	toma casquillo									tomar fulminante	0,4	G4A
MC	0,9	mueve casquilo									mover fulminante	0,9	MB
P3	1,5	coloca casquillo									coloca fulminate en conte	1,5	PB
S	0,8	sostiene casquillo									alcanza palanca	0,8	RA
S	0,3	sostiene casquillo									toma palanca	0,3	G
S	1,8	sostiene casquillo									acciona palanca	1,8	AP
S	0,1	sostiene casquillo									soltar palanca	0,1	RL
S	1,6	sostiene casquillo									alcanza panal	1,6	RB
S	0,3	sostiene casquillo									toma panal	0,3	G
MC	1,7	mueve casquilo									mueve panal	1,7	MB
P2	1,4	colocar casquillo									sostiene panal	1,4	S
RL	1,5	soltar casquillo									sostiene panal	1,5	S
E	0,4	espera									mueve panal	0,4	MB
E	0,1	espera									soltar panal	0,1	RL
	14,1	**TOTAL**									**TOTAL**	14,1	
	391,7	**TOTAL TMU**									**TOTAL TMU**	391,7	

MÉTODO	Propuesto	Tiempo(seg)	TMU	Propuesto	Tiempo(seg)	TMU
	Izquierda			Derecha		
Operaciones	4	4,8	133,3	7	4,5	125,0
Transportes	3	3,9	108,3	6	6,7	186,1
Espera	2	0,5	13,9	0	0,0	0,0
Sostenimiento	6	4,9	136,1	2	2,9	80,6
Inspecciones	0	0,0	0,0	0	0,0	0,0
Totales	15	14,1	391,7	15	14,1	391,7

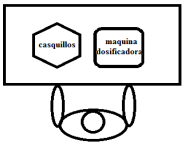
Tabla 4 – Diagrama Bimanual Colocación de Fulminante (Propuesto)

DIAGRAMA BIMANUAL

Diagrama N°: 3 (ciclo1) Hoja N°: 3 de 6

Disposición del lugar de trabajo

Propuesto



Dibujo y Pieza:

Operación: Encapsulado de pólvora

Investigadores

Lugar: Área de municiones

Ambas manos deben comenzar, así como completar sus movimientos a la vez
Ambas manos no deben estar inactivas a la vez, excepto durante los periodos de descanso
Los movimientos de los brazos deben hacerse en direcciones opuestas y simétricas y deben realizarse automáticamente
Los movimientos de las manos deben quedar confinados a la clasificación más baja con la que sea posible ejecutar satisfactoriamente el trabajo.
La clasificación más baja requiere por lo general el

COD	TIEMPO SEG	Descripción de Mano Izquierda	Descripción de Mano Derecha	TIEMPO SEG	COD
RC	1	alcanzar casquillo	espera	1	
G4A	0,4	toma casquillo	espera	0,4	
MC	1	mover casquillo	alcanza palanca	1	MC
P3	0,8	colocar casquillo	toma palanca	0,8	G
S	1,5	sostener casquillo	acciona palanca	1,5	AP
S	0,2	sostener casquillo	soltar palaca	0,2	RL
MC	0,8	mover casquillo	espera	0,8	E
P2	0,3	colocar casquillo	espera	0,3	E
RL	0,2	soltar caquillo	espera	0,2	E
6,2		**TOTAL**	**TOTAL**	6,2	
172,2		**TOTAL TMU**	**TOTAL TMU**	172,2	

MÉTODO	Propuesto	Tiempo(Seg)	TMU	Propuesto	Tiempo(Seg)	TMU
	Izquierda			Derecha		
Operaciones	4	1,7	47,2	3	2,5	69,4
Transportes	3	2,8	77,8	1	1,0	27,8
Espera	0	0,0	0,0	5	2,7	75,0
Sostenimiento	2	1,7	47,2	0	0,0	0,0
Inspecciones	0	0,0	0,0	0	0,0	0,0
Totales	9	6,2	172,2	9	6,2	172,2

Tabla 5 – Diagrama Bimanual Encapsulado de Pólvora (Propuesto)

Tenemos los resultados de los diagramas bimanuales con el tiempo final de cada puesto de trabajo en la Tabla 6.

PT_1	PT_2	PT_3	PT_4	PT_5	PT_6
391,70 TMU	580,60 TMU	172,2 TMU	294,40 TMU	358,00 TMU	319,40 TMU
14,10 min	20,90 min	6,20 min	10,60 min	12,89 min	11,50 min

Tabla 6 – Tiempo total por puesto de trabajo (propuesto)

3.4. Propuesta de Nueva Distribución de los puestos de trabajo

En la nueva distribución se consideró que los puestos de trabajo con una relación directa permanezcan los más cerca posible siguiendo un orden decreciente de movimientos (Tabla 7) entre puestos de trabajo evitando recorridos innecesarios, lo contrario con las de una relación indirecta. Debido a este argumento se tomó la alternativa de diseño donde estuvieran el puesto de trabajo 2 junto al 4, el 1 junto al 5, el 5 junto al 3, el 3 junto al 6 y así sucesivamente mientras el espacio disponible lo permita.

Luego se procede con el mismo mecanismo de cálculo antes ya desarrollado en la distancia de recorrido total inicial, pero ahora con la nueva distribución de distancia, ver en la Tabla 8.

Relaciones entre puestos de trabajo	Movimientos entre puestos de trabajo	Nuevas distancias (metros)
1-5	1122,2	4,0
3-5	794,4	4,0
5-7	694,4	4,5
5-6	566,7	5,7
3-6	544,4	5,7
2-5	433,3	6,0
2-4	338,9	6,2
1-3	333,3	6,5
4-5	222,2	7,5
4-7	155,6	8,3
2-3	144,4	8,5
3-7	0	8,7
3-4	0	8,8
2-7	0	9,5
6-7	0	10,2
4-6	0	10,8
1-2	0	11,4
1-7	0	12,5
2-6	0	14,0
1-6	0	14,6
1-4	0	18,0

Tabla 7 – Análisis de Relación Entre Puestos de Trabajo

En la Figura 3, se redistribuyeron las áreas de trabajo analizando cuales eran las que tenían relación directa e indirecta, tomando en cuenta que la bodega y sección de empaque no eran posible reubicarlas, en el caso de bodega (puestos de trabajo 5) no es posible trasponer debido a que esta adecuada especialmente para pólvora y material

balístico y es área de construcción fija y la zona de empaque (el puesto de trabajo 7) no se la puede reubicar debido a que la maquinaria de empaque está instalada en este lugar y es hasta dónde puede llegar el montacarga para realizar el traslado a bodega central.

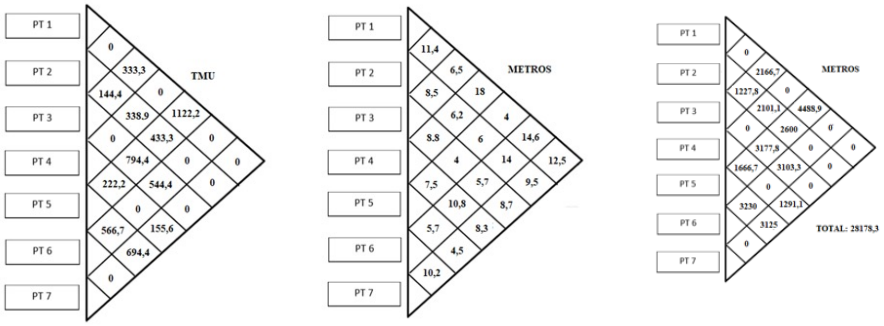


Tabla 8 – Triangular de Movimientos Totales Entre Estaciones de Trabajo.

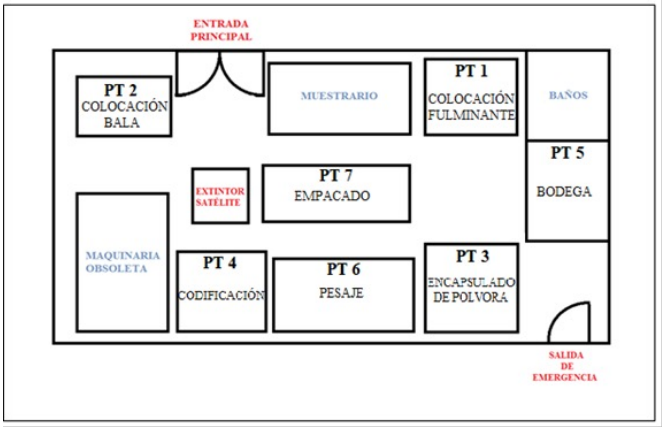


Figura 3 – Layout propuesto para el Área de municiones.

Tenemos el resultado del recorrido total de la distribución inicial que fue de 58811,1 metros en la etapa del diagnóstico en la Figura 2, y el resultado del recorrido total de la distribución propuestas que es de 28178.3 metros, de esta manera se obtuvo un ahorro en el recorrido total de 30632,8 metros con la nueva distribución, estudio que se realizo basado en el análisis de los movimientos.

4. Conclusiones

En el estudio de los Therbligs se identificaron como Efectivos: alcanzar, mover, tomar, soltar y posicionar por ser los que agregan valor a las operaciones en el Área de municiones y en cuanto a los Inefectivos que sólo agregan costos definimos : buscar,

seleccionar, sostener, retraso inevitable; mediante el análisis de la relación entre las dos manos y la utilización de los Diagramas bimanuales obtuvimos los tiempos de cada ciclo de los Puestos de trabajo, en el 1 (768,89 TMU) que representan 27,68 segundos, Puesto de trabajo 2 (658,33 TMU- 23,70 segundos), Puesto de trabajo 3 (200 TMU- 7,2 segundos), Puesto de trabajo 4 (455,56 TMU-16,40 segundos), Puesto de trabajo 5 (475 TMU-17,1 segundos) y Puesto de trabajo 6 (394,44 TMU-14,20 Segundos).

Mediante la aplicación del Criterio de Minimización de Movimientos Totales se evidencio que de inicio la cantidad de distancia total recorrida que se tenía entre los 6 puestos de trabajo y la bodega del Área de municiones era de 58811,1 metros, con la propuesta de mejora tomándose en consideración el cumplimiento de los principios de la economía de los movimientos y las nueva distribución de los puestos de trabajo se obtuvo un recorrido de 28178.3 metros, de esta manera se ahorraron en el recorrido total 30632,8 metros.

Referencias

Ameloot C., R. C. (2022). Modelado del comportamiento complejo del contador de proyectiles múltiples UAV calibre 12Munición. *Factores Humanos e Ingeniería Mecánica para la Defensa y la Seguridad*, Volumen 6, Edición 1, Artículo número 3.

Carlos, L. (11 de junion de 2016). *El estudio de tiempos y movimientos. Qué es, origen, objetivos y características*. Obtenido de https://www.gestiopolis.com/el-estudio-de-tiempos-y-movimientos/

Galarza, A. (2020). Diseño de la distribución de una planta extractora de leche en la ciudad de Cayambe. *Repositorio de la Universidad Tecnológica Indoamérica Facultad De Ingeniería Y Tecnología De La Información Y Comunicación Escuela De Ingeniería Industrial. Quito – Ecuador*.

Gilkova, O. (2022). La investigación y el desarrollo militar como motor de la economía del futuro. *Conferencia Internacional de Investigación Aplicada sobre Gestión de Operaciones y Proyectos: Estrategias y Tendencias y Conferencia Internacional de Investigación sobre la Gestión en la Economía Financiera*, 185-189.

Hongzhi, Z.,. (2021). Investigación sobre la aplicación del proceso de jerarquía analítica en la toma de decisiones de objetivos múltiples de municiones en red. *Journal of Physics: Serie de conferencias*.

Kan, W. C. (2022). Revisión de los dispositivos de seguridad y armado MEMS para el sistema de microiniciación. *Hanneng Cailiao/Journal chino de materiales energéticos*, 78-94.

Koç, M. (2022). Desarrollo de un Software Inteligente Basado en Sistemas de Inferencia Neural-Fuzzy Adaptativos para Predecir la Vibración de la Boca del Cañón de una Pistola. *Revista árabe de ciencia e ingeniería*.

Liu, M.,. (2021). Método de programación de municiones en un depósito de armas aerotransportado basado en un algoritmo genético mejorado. *Journal of Physics: Serie de conferencias*.

McNeilly, R.,. (2022). Caracterización integral de los subproductos de disparo generados por disparos de armas pequeñas de munición frangible sin plomo. *Revista de Higiene Ocupacional y Ambiental*, 169-184.

Skalny, A.,. (2021). Peligros ambientales y para la salud de la contaminación por metales militares. *Investigación Ambiental*.

Vu, T.,. (2021). Influencia del puerto de gas en las fuerzas y sus impulsos que actúan en un arma automática. *8ª Conferencia Internacional sobre Tecnologías Militares, ICMT 2021 - Actas*.

Wang, M.,. (2021). Investigación sobre el diseño de procesos MBD de armas ligeras basadas en UG. *Conferencia Internacional IEEE sobre Avances en Ingeniería Eléctrica y Aplicaciones Informáticas, AEECA*, 940-943.

Xu, Y.,. (2021). Investigación y desarrollo actuales de la tecnología de evaluación del efecto del daño de las municiones. *Beijing Ligong Daxue Xuebao/Transacción del Instituto de Tecnología de Beijing*, 569-578.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 18/10/2021
Aceitação/Acceptance: 11/01/2022

Detección y Seguimiento de Drones con Cámaras de Vigilancia Estáticas para Lugares Estratégicos

Rubén León[1], Alexis Tinoco-S[2], Álvaro Chisaguano[1], Héctor Tufiño[1], Héctor Moya, Fernando Lara[3].

rdleon@espe.edu.ec; alexis.tinoco@espoch.edu.ec; cachisaguano@espe.edu.ec; hatufino@espe.edu.ec; moya.unda@gmail.com; marco.lara@epn.edu.ec

[1] Departamento de Eléctrica, Electrónica y Telecomunicaciones, Centro de Investigación de Aplicaciones Militares (CICTE), Universidad de las Fuerzas Armadas ESPE, Sangolquí 171103, Ecuador.

[2] Facultad de Informática y Electrónica, Escuela Superior Politécnica del Chimborazo ESPOCH, Riobamba 060155, Ecuador.

[3] Departamento de Electrónica, Telecomunicaciones y Redes de la Información, Escuela Politécnica Nacional EPN, Quito 170517, Ecuador.

Pages: 139-151

Resumen: El incremento del vuelo de drones en determinadas áreas, sin conocer el objetivo de vuelo, motiva el desarrollo de un prototipo de detección, seguimiento e identificación de drones, a través de equipos disponibles en el mercado (OEM, *del inglés Original Equipment Manufacturer*) utilizando video cámaras para la detección. Con el objetivo de incrementar la capacidad de respuesta de la seguridad y vigilancia pública, se busca desarrollar un sistema capaz de adaptarse a equipos existentes, como son cámaras de video vigilancia estáticas, otro elemento importante es considerar que el desarrollo tenga un costo reducido para que pueda ser implementado de forma masiva en instalaciones militares y gubernamentales. Con eso en mente, la presente investigación presenta un prototipo basado en OpenCV, capaz de detectar drones a más de 90 metros de distancia.

Palabras-clave: Sobre vuelo, Detección de drones, OpenCV, Visión Artificial, Espacios Estratégicos

Detecting and tracking of drones with Static Surveillance Cameras for Strategic Sites

Abstract: The increase in the flight of drones in certain areas, without knowing the objective of the flight, motivates the development of a prototype for the detection, tracking and identification of drones, through original equipment manufacturer (OEM, English Original Equipment Manufacturer) using video cameras for detection. With the aim of increasing the response capacity of security and public surveillance, the aim is to develop a system capable of adapting to existing equipment, such as static video surveillance cameras, another important element is to consider that the development has a reduced cost so that can be massively

deployed in military and government installations. With that in mind, this research presents a prototype based on OpenCV, capable of detecting drones at more than 90 meters away.

Keywords: Over flight, Drone Detection, OpenCV, Artificial Vision, Strategic Sites

1. Introducción

En la actualidad, la presencia de vehículos aéreos no controlados (UAV*, del inglés unmanned aerial vehicles*) o también conocidos como drones, han generado problemas debido al mal uso de los mismos, a esto se suma el incremento de la manufactura y reducción de costos de fabricación de drones (Blázquez, Casamayón, & Burgos, 2018) (Peréz, 2015) (Ramos, 2017); esto facilita el acceso de drones a personas fuera del área militar y comercial, dificultando el control de UAV, por lo que, la investigación sobre técnicas de detección de drones es de suma importancia para proteger áreas protegidas, edificios entre otros.

Un ejemplo de esto se presenta en un reportaje del periódico británico *The Independent,* en el cual, se menciona que los llamados de emergencia debido al mal uso de drones pilotados por civiles, se han incrementado cuatro veces entre 2014 y 2015; en 2014 se tuvieron 94 llamados y en 2015 se presentaron 425 llamados, lo que nos muestra la importancia de investigar en temas de control de vuelo de drones así como en su regulación.

El incremento de drones hace necesario desarrollar e implementar dispositivos de detección, en edificaciones gubernamentales, espacios protegidos, entre otros (Pham & Nguyen, 2020); ya han existido incidentes en estas áreas a causa de UAV, por ejemplo, en 2019 un grupo de drones, mejor conocido como *drone swarm*, fue visto vigilando la Central Nuclear de Palo Verde en Arizona. En el reporte se indica que los drones fueron dos noches seguidas en septiembre de 2019, mientras el personal de seguridad se encontraba limitado a observar sin tener ningún tipo de defensa o poder alertar el incidente con anticipación, para dar tiempo a la llegada de un equipo de respuesta antes del arribo de los drones (Friedrich, 2021).

De forma similar, en Ecuador se presentaron incidentes con drones que pusieron la seguridad de la ciudadanía en riesgo, en el año 2021, en una de las cárceles del país, se registraron ataques con explosivos transportados en drones, estas son evidencias de que el incremento de drones, ha permitido que esta tecnología sea usada para realizar actos delictivos. Es por esto que, el diseño de sistemas de detección de drones de bajo costo son un tema de interés, se espera que estos sistemas tengan la capacidad de brindar control y seguridad al espacio aéreo que rodea a edificaciones.

Varias técnicas de detección de drones han sido exploradas por diferentes grupos, como: radar (De Quevedo , Urzaiz, Menoyo, & López, 2018), radar pasivo (Dan , Yi, Wan, Rao, & Wang, 2019), detección con arreglos de sensores electroópticos y arreglos de sensores de audio (Liu, y otros, 2017); de estas técnicas la detección a través de cámaras de video es la solución de menor costo, ya que, presenta la capacidad de usar elementos ya existentes como cámaras de seguridad instaladas en las edificaciones.

En la actualidad, no tener un sistema de detección y protección del espacio aéreo en áreas protegidas, para controlar la presencia de drones, representa un potencial riesgo para la sociedad, esto puede generar perdidas económicas a medio y largo plazo.

Con todo lo antes mencionado, esta investigación está enfocada en desarrollar un prototipo de seguimiento y detección de drones, basado en cámaras de video estáticas, por ejemplo las cámaras de seguridad existentes en edificaciones. El objetivo es usar cámaras existentes en las edificaciones gubernamentales o militares para tener un sistema de detección de drones de bajo costo, con un algoritmo que presente un reducido costo computacional manteniendo una alta probabilidad de detección de drones, lo que permite la implementación del sistema con equipos OEM; con el sistema propuesto se espera tener una primera alerta ante la presencia de drones en edificaciones gubernamentales, bases militares, entre otros.

En la Sección 2, se presenta el marco teórico necesario para el desarrollo del artículo, en la Sección 3, se presentan los detalles del sistema propuesto y una descripción del algoritmo implementado. Los resultados se presentan en la Sección 4, y en la Sección 5 se presenta la discusión y conclusiones.

2. Marco Teórico

2.1. Drones

En 2012, John Villaseñor profesor de Ingeniería Eléctrica en la Universidad de Los Ángeles California (UCLA, *del inglés University of California Los Angeles*), dijo que los drones son aeronaves no tripuladas que vuelan autónomamente, sin la necesidad de la presencia humana. Esta definición resulta curiosa, ya que, dar una definición de dron desde el punto de vista técnico y legal es complicado (Callegari & Goberna, 2015).

En otras palabras, los drones pueden ser definidos básicamente como un vehículo aéreo no tripulado, el cual, es controlado de forma remota o tiene almacenado un plan de vuelo; En principio, esto hacía referencia solo a las aplicaciones militares, pero con el paso del tiempo ya se aplican al ámbito civil (Ferrer, 2020).

Una definición tan amplia deja las puertas abiertas a un gran número de tamaños y geometrías de UAV como: easystar, wings, octocópteros, multicópteros, entre otros; este factor dificulta la tarea de detección y reconocimiento de drones.

2.2. Algoritmo de detección

El algoritmo de seguimiento puede ser definido de forma simple como un proceso de estimación de uno o múltiples objetivos en movimiento usando una cámara. Una de las técnicas más comunes en la actualidad es el seguimiento de blancos u objetivos cuadro a cuadro.

El objetivo del seguimiento de objetivos es determinar de forma aproximada la posición de uno o más objetivos o blancos importantes en una imagen o en un video y poder seguir su movimiento en el tiempo (Rico, 2016). Dependiendo de la aplicación a ser

desarrollada, existen diferentes tipos de seguimiento: *hand-tracking*, *fase-tracking*, *object-tracking* (ISOIN, 2016).

Object traking o seguimiento de objetos, es la categoría para detección de drones, pero como se menciona antes, la gran variedad de drones hace de esta una tarea compleja, para solucionar esto se han probado diferentes técnicas clásicas y de inteligencia artificial. En este trabajo se explora un algoritmo de bajo costo computacional, capaz de implementarse en sistemas de videovigilancia existentes.

2.3. Librerías para procesamiento de imágenes

Para esta investigación, se usó la librería OpenCV, esta es una librería de código abierto para visión por ordenador qué cuenta con la licencia BSD (del inglés, *Berkeley Software Distribution*); esta librería incluye una gran cantidad de algoritmos de visión por ordenador, y funciones que permiten la creación de nuevos algoritmos como es el caso de esta investigación (OpenCV, 2022) (Bradski & Kaehler, 2008).

2.3.1. Estructuras en OpenCV

En general, las estructuras de OpenCV contienen cinco componentes: CXCORE, CV, ML, HighGUI y CVCAM, estos componentes contienen funciones de entrada y salida, rutinas que almacenan y procesan videos e imágenes (Bradski & Kaehler, 2008).

- CXCORE: Contiene estructuras de datos, matrices algebraicas, transformación de datos, persistencia de objetos, administración de memoria, manejo de errores, funciones de dibujo y matemática básica.
- CV: Contiene funciones de procesamiento de imágenes, estructuras de imágenes, funciones de calibración para cámaras, algoritmos de seguimientos, reconocimientos de patrones.
- Machine Learning (ML): Contiene funciones de agrupamiento de datos, clasificaciones y análisis.
- HighGUI: Contiene herramientas para diseño de interfaces gráficas, almacena y recupera imágenes y videos.
- CVCAM: Contiene todo lo relacionado con la interfaz de la cámara.

2.3.2. Módulos OpenCV

Los módulos de OpenCV para procesamiento de imágenes y videos son:

- Core: Este módulo incluye estructuras básicas de datos y funciones para procesamiento de imágenes.
- Highgui: Este módulo permite crear la interfaz de usuario, contiene codecs de video, capturador de imágenes, entre otros.
- Imgproc: Contiene algoritmos para procesamiento de imágenes, filtros, entre otros.
- Video: Este módulo permite el análisis de videos usando algoritmos de seguimiento y detección en videos.
- Objdetect: Incluye objetivos de detección y reconocimiento de patrones.

3. Metodología

3.1. Prototipo de discriminación y seguimiento de drones

El prototipo de discriminación y seguimiento de drones está implementado con una arquitectura cliente-servidor; el sistema tiene una cámara IC Realtime EL8000IR que permite capturar video en tiempo real, el video se digitaliza con el dispositivo USB Driver Honestech VHS to DVD 3.0, la estructura general del proyecto se presenta en la Fig. 1.

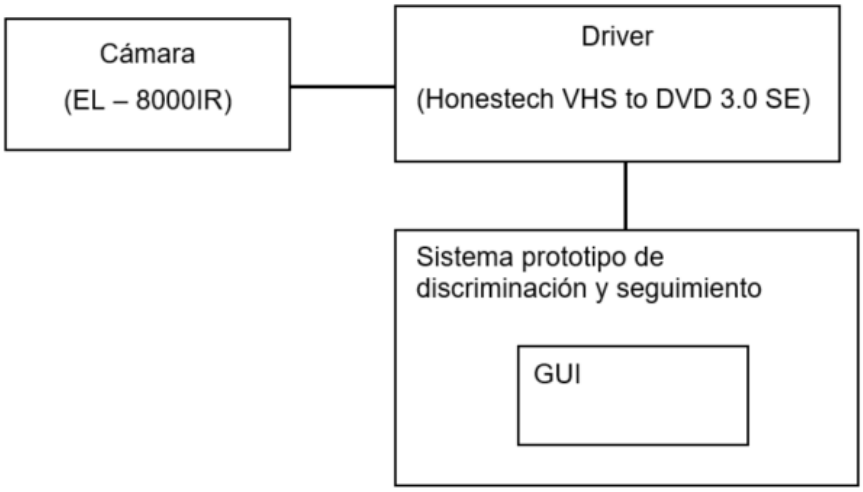


Figura 1 – Arquitectura del sistema

Para realizar el procesamiento de video de forma digital es necesario pasar del video analógico que nos entrega la cámara IC Realtime esto se hace con el equipo Honestech, una vez digitalizado el video se puede procesar con las funciones de OpenCV, representando la secuencia de imágenes como matrices dentro de los algoritmos, como parte del procedimiento se desarrolló una interfaz gráfica para presentar el video y la detección del dron, esto se detallara en siguientes párrafos.

La primera etapa consiste en adquirir los datos, es decir, pasar las imágenes a matrices como se mencionó, luego de esto se realizan modificaciones de color, para después, aplicar filtros esto puede ser considerado como aplicar funciones lógicas entre la imagen original y cuadros obtenidos de forma previa, con la intención de eliminar el fondo de las secuencias de imágenes obtenidas.

La idea del punto anterior es similar a tener un procesador MTI (del inglés, *moving target indicator*), donde a través de diferentes muestras suprime el clutter de objetos con velocidad cero, para esto adquiere diferentes giros completos del radar y los compara para eliminar el clutter (Reed, Gagliardi, & Stotts, 1990) (Mahafza, 2005), en nuestro

escenario se utilizan diferentes fotogramas del video para suprimir el fondo u objetos estáticos, resaltando objetos en movimiento como drones.

Finalmente, la etapa de detección y seguimiento marcan el contorno del dron siguiendo la ruta de vuelo, la condición es que el dron se encuentre dentro del campo visual de la cámara.

3.2. Aplicación de funciones OpenCV en el algoritmo

A continuación, se describen las principales funciones de OpenCV que serán usadas por el algoritmo.

- cap.read(frame)

  Esta función permite capturar el flujo de video desde la cámara conectada y almacenar el fotograma como una variable.

- cvtColor(frame,gray,COLOR_BGR2GRAY)

  El parámetro COLOR_BGR2GRAY y la función cvtColor permite cambiar el color original del video a un video en escala de grises, el resultado de esto se almacena en una nueva variable. Hacer esto permite preparar la imagen para pasos siguientes, en los que se aplica un umbral para la detección del dron y su siguiente contorneado.

- GaussianBlur(gray, gray, Size(21, 21), 0)

  Esta función es un filtro gaussiano, que tiene como objetivo eliminar el ruido gaussiano de la imagen.

- Absdiff(firstFrame, gray, frameDelta)

  Esta función calcula la diferencia entre el cuadro anterior y el cuadro actual.

- threshold(frameDelta, thresh, 20, 255, THRESH_BINARY)

  La función threshold permite aplicar el método de segmentación por regiones en una imagen, es decir, variar la intensidad de los píxeles de la imagen de interés de los píxeles del fondo de esa imagen, aplicando un umbral de nivel fijo a cada elemento de la matriz que almacena la imagen capturada.

  Los valores que los píxeles pueden tomar, están en el rango de 0 (negro) a 255 (blanco). Los píxeles que toman un valor de 0 son considerados fondo de la imagen.

- blur(thresh, thresh, Size(10, 10))

  Esta función permite implementar un filtro normalizado, donde, los parámetros thresh indican la imagen de origen y destino respectivamente, Size define el tamaño en píxeles del kernel a utilizar (ancho ancho, alto alto).

- findContours(temp, contornos, hierarchy, RETR_EXTERNAL, CHAIN_APPROX_TC89_KCOS)

  Como se ha notado, las funciones descritas hasta ahora sirven para capturar, filtrar, segmentar y colorear la imagen, ahora, la función findContours busca bordes y píxeles de similar intensidad para recuperar los contornos de la imagen. El parámetro temp corresponde a la imagen resultante al aplicar las funciones mencionadas anteriormente, el siguiente parámetro contours indica que sé que almacenará los contornos en un vector que puede variar su tamaño automáticamente, el parámetro hierarchy define el método de aproximación del contorno, el último parámetro CHAIN_APPROX_TC89_KCOS se refiere al método que identifica todos los puntos del contorno.

3.3. Algoritmo

El algoritmo implementado consiste en aplicar una serie de transformaciones a los fotogramas, los fotogramas se definen como γ (ver Fig 2a), la función bgr2gray es aplicada (φ, ver Fig. 2b), se encuentra γ'=φ(γ), con esto el fotograma γ' es un fotograma a blanco y negro, luego de esto se aplica la función gaussianblur (δ) para eliminar el ruido gaussiano presente en la imagen, se define como: γ''=δ (γ'). Desde esto, se obtiene un fotograma patrón γ0, con este fotograma se calcula la diferencia con los siguientes 30 fotogramas, el promedio de esta diferencia se obtiene con la expresión (el valor de 30 fotogramas fue probado, y es el valor que presenta mejor desempeño, este puede ser ajustado de acuerdo al entorno en el que se encuentre el sistema):

$$\theta = \frac{1}{N}\sum_{i=1}^{N}|\Upsilon_0'' - \Upsilon_i|$$

Donde: N es el número de fotogramas (N=30), luego de obtener el fotograma patrón obtiene la media de la diferencia, esto se ve en Fig. 2c. El valor de N, puede ser alterado de acuerdo al entorno, un entorno más estacionario o estático puede tomar un valor más pequeño.



a)



b)



c)

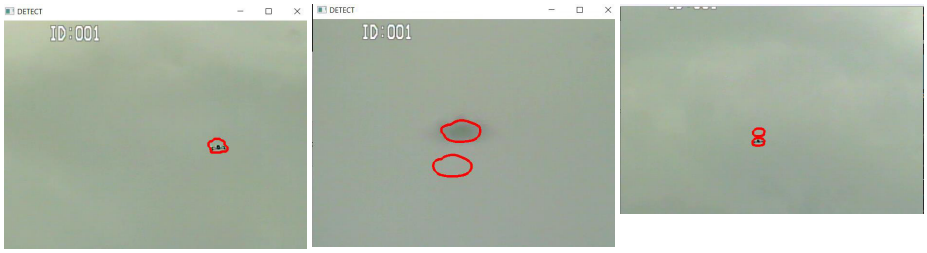
Figura 2 – Ejemplos de las etapas de procesamiento

4. Resultados

El desempeño del algoritmo es evaluado en diferentes escenarios, variando la distancia y apoyando la captura de imágenes con el acercamiento de la cámara.



a) b) c)



d) e) f)



g) h) i)

Figura 3 – Imágenes tomadas con el sistema propuesto: a) dron a 10 metros, b) dron a 20 metros, c) dron a 30 metros, d) dron a 40 metros, e) dron a 50 metros, f) dron a 60 metros, g) dron a 70 metros, h) dron a 80 metros y i) dron a 90 metros

Es importante mencionar que el zoom y enfoque de la cámara EL-8000IR se configuran de forma manual, pero soporta control por RS232, lo que hace ideal para control y vigilancia de edificios; se está trabajando en la integración del control automático de enfoque y zoom.

Para validar los resultados obtenidos los datos de la posición (distancia) se toman de la aplicación FreeFlight Pro, aplicación utilizada para controlar el dron.

Primera Prueba: Dentro de este marco , la prueba A se hizo teniendo como punto de inicio la posición de la cámara (casa ubicada en Quito), y como punto final, la posición del dron. En esta prueba se tuvo una separación de 10 metros, esto se presenta en la Fig. 3a. Adicional, en la Fig. 3a se observa un falso positivo en la parte superior de la imagen, estos falsos positivos son momentáneos mientras la presencia del objetivo se da de forma prolongada.

Segunda Prueba: En esta prueba el dron está localizado a una distancia de 20 metros desde el punto de referencia, en este caso al tener un fondo aún más estático (cielo) se tiene un mejor desempeño. Esta prueba se presenta en la Fig. 3b.

Tercera Prueba: Para la tercera prueba, el dron se ubica a 30 metros, esto es presentado en la Fig. 3c.

Cuarta Prueba: Según los resultados de la prueba cuatro, y teniendo en cuenta que a partir de este punto se empieza a utilizar el zoom (x6) de la cámara de vídeo, como resultado, la distancia aproximada establecida desde el punto de referencia hasta el dron es de 40 metros, en la Fig. 3d se puede determinar la detección y seguimiento del dron y por lo tanto, se verifica el funcionamiento del prototipo.

Quinta Prueba: Para esta prueba se configura el zoom en x13, con lo que se consigue tener detecciones exitosas a 50 metros (ver Fig. 3e).

Sexta Prueba: En la Fig. 3f se presenta un ejemplo a 60 metros, para esto se configura el zoom de la cámara a 60 metros, se valida un funcionamiento correcto, es importante resaltar que en esta prueba el dron fue contorneado con dos áreas distintas, esto se debe validar y mejorar en el algoritmo de contorneado.

Séptima Prueba: En el análisis de la séptima prueba se debe tener en cuenta que la configuración del zoom es (x25), con esto se alcanza una distancia de 70 metros entre el punto de referencia y el dron, como se puede apreciar en la Figura 3g, el algoritmo mantiene la detección y el seguimiento.

Octava Prueba: Para obtener resultados desde este punto se puede variar el zoom entre x27 y el zoom máximo de la cámara EL-8000IR de x37, todo depende del operador y de los resultados que se requieran del sistema, por lo tanto, la distancia entre el punto de referencia comprobada es de 80 metros, esto se evidencia en la Fig. 3h.

Novena Prueba: Finalmente, respecto a la novena prueba y con un zoom previamente configurado, se alcanza una distancia aproximada de 90 metros desde el punto de referencia hasta el dron.

En este escenario, aunque el dron es detectado, cabe señalar que el algoritmo genera otras detecciones dependiendo de varios factores externos como el clima, el posicionamiento y la estabilidad de la cámara, produciendo una mayor cantidad de falsos positivos. Pero estos falsos positivos están cortos instantes de tiempo, mientras el objetivo permanece por amplios periodos, por lo que, se pueden eliminar esos falsos positivos.

Como se presenta en los párrafos anteriores, la cámara debe estar estática para eliminar el fondo, y dadas las características del algoritmo utilizado puede presentar falsos positivos, mismo que por duración de tiempo se pueden eliminar.

Uno de los componentes importantes es mencionar que en las pruebas la distancia de detección está sujeta a la calidad del video y al zoom que pueda alcanzar la cámara (siendo mejor si la cámara tuviera mejores características).

Para evaluar el desempeño del algoritmo se realizó un sistema de votación evaluado en categorías de bueno, regular, limitado. Esto se obtuvo luego de realizar diversas pruebas de vuelo con drones y que registren las detecciones y la calidad de las mismas, considerando detección, falsos positivos, entre otros. Luego de esto se obtuvo la Tabla 1, donde se puede observar que el desempeño limitado a mayores distancias se debe a

falsos positivos ocasionados por objetos en movimiento como aves, aviones, entre otros esto se ve en las Fig. 3g, Fig. 3h y Fig. 3i.

Distancia [metros]	Zoom	Percepción
10	X0	Buena
20	X0	Buena
30	X4	Buena
40	X6	Buena
50	X13	Buena
60	X21	Regular
70	X25	Regular
80	X27-x37	Limitada
90	X27-x37	Limitada

Tabla 1 – Definición de algunos estilos

5. Conclusiones

El desarrollo de un prototipo basado en un algoritmo de bajo costo computacional, hace posible implementar la solución propuesta en sistemas de vigilancia existentes, tanto en el ámbito militar, gubernamental o civil.

El uso de librerías OpenCV, permite la implementación acelerada del algoritmo haciendo uso de procesamiento en paralelo con tarjetas CUDA, lo que permite en un solo ordenador realizar el procesamiento de varias cámaras de forma simultánea.

Luego de realizar las pruebas se verificó un correcto funcionamiento hasta distancias de 100 metros, como ya se ha mencionado, los falsos positivos se pueden descartar con el tiempo de permanencia en el espacio de cobertura de la cámara, por lo que, el sistema cumple con el objetivo de esta investigación, ser una primera alerta automática ante la presencia de drones en áreas restringidas.

Para incrementar la cobertura del sistema se puede reemplazar la cámara EL-8000IR, por una cámara de mayor alcance y mayor cobertura en elevación y azimut.

Si bien en el mercado existen sistemas que presentan una mayor robustez en el procesamiento de imágenes haciendo uso de técnicas avanzadas como: uso de aprendizaje de máquina, aprendizaje profundo, entre otros, el sistema propuesto por la reducción del coste computacional, reduce los costos de implementación, haciendo viable una implementación de forma masiva en áreas protegidas.

En un futuro se pretende integrar el sistema con técnicas de inteligencia computacional, teniendo como primer procesamiento el artículo descrito en este artículo, mismo que se encargara de procesar varias cámaras de forma simultánea, y solo los cuadros marcados con la presencia de un drone serán procesados por la inteligencia computacional, esta

solución permitiría tener un solo ordenador para procesar la información de todo un circuito de vigilancia.

Referencias

Blázquez García, R., Casamayón Antón, J., & Burgos García , M. (2018). Nuevo concepto de radares pasivos multiestáticos basados en LTE-R para vigilancia de líneas ferroviarias de alta velocidad. *Congreso Nacional GMR-SSR*.

Bradski, G., & Kaehler, A. (2008). *Learning OpenCV: Computer vision with the OpenCV library*. O'Reilly Media, Inc.

Callegari, A., & Goberna, A. (2015). El doble filo de los drones: regulación y resguardo de la privacidad en Argentina. *Simposio Argentino de Informática y Derecho (SID 2015)-JAIIO 44*.

Dan , Y., Yi, J., Wan, X., Rao, Y., & Wang, B. (2019). LTE-based passive radar for drone detection and its experimental results. *The Journal of Engineering*(20), 6910-6913.

De Quevedo , A., Urzaiz, F., Menoyo, J., & López, A. (2018). Drone detection with X-band ubiquitous radar. *2018 19th International Radar Symposium (IRS)*, 1-10.

Ferrer, G. (2020). Vehículos aéreos no tripulados (drones). Aspectos de interés e inscripción registral. *Revista de Derecho Notarial y Registral, Universidad Blas Pascal*(3), 206-221.

Friedrich, N. (2021). Drones Define New Combat Environment. New Developments in EW and Signals Intelligence. *Microwave Journal*, 18-20.

ISOIN. (2016). *Introducción en Técnicas de Tracking o Seguimiento*. Ingenieria y Soluciones Informaticas. Obtenido de https://www.isoin.es/introduccion-en-tecnicas-de-tracking-o-seguimiento/

Liu, H., Wei, Z., Chen , Y., Pan, J., Lin, L., & Ren, Y. (2017). Drone detection based on an audio-assisted camera array. *2017 IEEE Third International Conference on Multimedia Big Data (BigMM)*, 402-406.

Mahafza, B. (2005). *Radar systems analysis and design using MATLAB*. Chapman and Hall/CRC.

OpenCV. (2022). *Open source computer vision*. Intel. Obtenido de https://docs.OpenCV.org/3.3.0/d1/dfb/intro.html

Peréz, J. M. (2015). Prueba de concepto de un radar pasivo multiestático para aplicaciones. *Valencia: Universidad Politecnica de Valencia*.

Pham, G., & Nguyen, P. (2020). Drone Detection Experiment Based On Image Processing And Machine Learning. *International Journal of Scientific & Technology Research, 9*(2), 2965-2971.

Ramos, A. (2017). Sistema de navegación autónomo para drones. *Universidad Mayor de San Andres*.

Reed, I., Gagliardi, R., & Stotts, L. (1990). A recursive moving-target-indication algorithm for optical image sequences. (IEEE, Ed.) *IEEE transactions on aerospace and electronic systems, 26*(3), 434-440.

Rico, R. (2016). Seguimiento automático de objetivos con drones mediante algoritmos de tracking. *Universidad Autónoma de Madrid*.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 04/12/2021
Aceitação/Acceptance: 01/02/2022

Evolução do Nível de Proficiência das Competências de Liderança no Ensino Superior: Estudo de Caso dos Cadetes Alunos da Academia Militar Portuguesa

José Rouco[1], João Montez[2]

carlos.rouco@ulusofona.pt; montez.671@gmail.com

[1] Universidade Lusófona - TRIE, Campo Grande 376, 1749-024, Lisboa, Portugal

[2] Academia Militar, Avenida Conde Castro Guimarães, 2720-113, Amadora, Portugal

Pages: 152-168

Resumo: O desenvolvimento de competências de liderança na Academia Militar Portuguesa é uma área estratégica para a formação dos futuros comandantes e líderes. O objetivo desta investigação é avaliar a evolução do nível de proficiência das competências de liderança dos Cadetes alunos ao longo dos anos escolares. Para atingir os objetivos, os investigadores adotaram um método quantitativo utilizando um questionário de competências de liderança. O questionário foi aplicado a 117 Cadetes alunos da Academia Militar Portuguesa (estudo de caso) em dois momentos diferentes (estudo longitudinal). Dos resultados conclui-se que os programas curriculares da Academia Militar Portuguesa desenvolvem o nível de proficiência de todas as competências em estudo, com destaque para: aptidão técnica e profissional; autoconfiança; capacidade para resolver problemas; desenvolver os outros; liderança participativa; liderança por delegação; orientação para as relações humanas; reconhecimento e *feedback* positivo; tomada de decisão e transparência. Os alunos melhores classificados percecionam níveis de proficiência significativamente diferente na aptidão técnica e profissional, assertividade, autocontrolo, determinação e perseverança, e influência pelo exemplo.

Palavras-chave: Liderança; Competências; Cadetes alunos; Academia Militar

Evolution of the Level of Proficiency of Leadership Skills in Higher Education: Case Study of Cadets Students of the Portuguese Military Academy

Abstract: The leadership competence development in the Portuguese Military academy is a strategic area for the training of future commanders and leaders. The aim of this research is to evaluate the evolution of the level of proficiency of leadership skills on student cadets over the school years. To achieve the objectives, the researchers adopted a quantitative method using a questionnaire of leadership competences. The questionnaire was applied to 117 students of the Portuguese Military Academy (Case study) at two different times (longitudinal study). From the results it is concluded that the curricular programs of the Portuguese Military Academy develop the level of proficiency of all leadership skills under study, with

emphasis on: Technical and professional skills; Ability to solve problems; Develop others; Participatory leadership; Leadership by delegation; Recognition and positive feedback; Decision making; Orientation for human relations; Self-confidence; and transparency. The best ranked students see significantly different proficiency levels in the following competencies: Technical and professional skills; Assertiveness; Self-control; Determination and perseverance; Influence by example.

Keywords: Leadership; Competences; Students; Military Academy.

1. Introdução

Astin e Astin (2000, p. 17) à pergunta: Porque é que o desenvolvimento da liderança é importante para os alunos universitários? defendem que "o desenvolvimento de líderes mais eficientes e eficazes é essencial para a construção de uma sociedade e um mundo melhor", sugerem ainda que "o desenvolvimento da liderança deve ser uma parte crítica da experiência do ensino superior" e que "os alunos que já se veem como futuros líderes em áreas, como seja de serviço público, empresários, militares ou outros podem, legitimamente perguntar: Que relevância tem o desenvolvimento da liderança para nós?".

As instituições de ensino superior, em resposta a esta e outras questões, passaram a incluir nos seus currículos competências transversais, nas quais se incluem as associadas à liderança para melhor capacitar e enriquecer os seus alunos durante e após a sua educação e formação, com vista a uma melhor preparação e integração no mercado de trabalho. O desenvolvimento das competências de liderança em alunos universitários tem-se tornado fundamental para a sua integração no local de trabalho em todos os setores de atividades, em particular nos que têm uma forte componente operacional, elevados níveis de stress e o tempo disponível para a tomada de decisão é curto. No contexto militar, os futuros oficiais oriundos das Academias Militares podem desempenhar funções de Comandantes, quer no dia a dia das suas unidades militares em território nacional, quer em ambiente potencialmente hostil, como podem ser as missões no estrangeiro além-fronteiras, em teatros de operações em formações isoladas ou forças conjuntas se concentram, manobram e em casos mais extremos combatem em guerra declarada e aberta, na maioria das vezes em várias frentes, cuja exigência à liderança e desempenho é potenciada.

Neste contexto, os perfis e as competências dos quadros do Exército Português e da Guarda Nacional Republicana (GNR) de Portugal, são dos mais exigentes ao nível da sua educação e formação. Sendo o efetivo dos seus Oficiais "alimentado" pelos cadetes alunos que concluem com sucesso a sua educação e formação de base na Academia Militar Portuguesa, durante 5, 6 ou 7 anos consoante as especialidades das armas e serviços. Segundo o Estatuto dos Militares das Forças Armadas (EMFAR), "o ensino e a formação nas Forças Armadas visam a preparação dos militares para o desempenho de cargos e exercício de funções de cada categoria e quadro especial concretizando-se em percursos formativos estruturados e na aquisição e desenvolvimento de competências".

Em face do exposto, estudar a evolução do nível de proficiência das competências de liderança adquiridas ao longo da educação e formação dos Cadetes alunos na Academia Militar Portuguesa representa um pilar essencial para dotar os futuros comandantes das capacidades exigidas no exercício das suas funções. Assim, a presente investigação

tem como objetivo geral (OG) a avaliação da evolução do nível de proficiência das competências de liderança dos cadetes alunos da Academia Militar Portuguesa nos diferentes anos escolares. Para orientar esta investigação foi formulada a seguinte Pergunta de Partida (PP): **Será que o nível de proficiência das competências de liderança dos Cadetes alunos da Academia Militar Portuguesa têm uma evolução positiva ao longo dos anos escolares?**

2. Competências de liderança

2.1. Conceito de competência

David McClelland (psicólogo de nacionalidade americana) publicou um artigo "Testing Competence Rather Than Intelligence" onde, surge pela primeira vez o conceito de "competências" associado à qualificação profissional. O autor definiu as competências como características pessoais que podem levar a um desempenho superior. McClelland (1073) definiu as variáveis das competências associadas ao desempenho, como uma alternativa aos testes de inteligência que vigoravam na época. A metodologia por si utilizada pode ser sintetizada em dois pontos-chave: uso das amostras de critério e identificação de pensamentos específicos e comportamentos que apresentam uma relação causal com resultados de sucesso.

Boyatzis (1982, p. 21), definiu a competência como "uma característica subjacente de uma pessoa que pode ser um motivo, um traço, uma habilidade, um papel social ou conhecimentos que ela usa" e que potencia um desempenho superior. Prahalad e Hamel (1990) publicaram um estudo na revista Harvard Business Review sobre as competências essenciais da organização, que podem acrescentar vantagem competitiva aos produtos por serem de difícil imitação. Spencer e Spencer (1993, p. 9) identificam as "competências como uma característica intrínseca de um indivíduo que apresenta uma relação de causalidade com critérios de referência de efetiva performance, numa dada situação". Cruz (2001, p. 31) afirmou que a competência "é agir com eficiência, utilizando propriedade, conhecimentos e valores na ação que desenvolve e agindo com a mesma propriedade em situações diversas". Para Roldão (2003), a competência surge quando o sujeito, perante uma situação, é capaz de mobilizar adequadamente diversos conhecimentos prévios, selecioná-los e integrá-los de forma ajustada à situação em concreto. Ceitil (2007, p. 41), afirmou que: [...] as competências são consideradas como *outputs* de desempenho, quer dizer, são resultados específicos que as pessoas trazem para o exercício das suas atividades profissionais e são realidades suscetíveis de serem observadas, permitindo, pela sua constância e regularidade, sustentar avaliações relativamente objetivas e consistentes sobre a performance profissional dos seus detentores. Ao analisar as várias definições de competência e segundo diferentes autores pode-se afirmar que a competências é um conjunto de conhecimentos, aptidões, atitudes e comportamentos que segundo um critério padrão leva um indivíduo a ter desempenhos superiores num determinado contexto (Rouco, 2012).

Os comandantes e líderes militares perante as situações mais hostis ou quando sujeitos à enorme pressão da adversidade do campo de batalha, têm que tomar decisões e dar ordens aos seus subordinados, que em algumas situações, podem implicar o sacrifício da própria vida. É perante este contexto, que as competências de liderança dos

comandantes têm de eclodir no seu expoente máximo, de modo que, ele próprio e os seus subordinados, mantenham a moral em alta, se sintam motivados e com espírito guerreiro, gerando uma desmedida vontade de vencer.

2.2. Conceito de liderança

Para Bass (1990, p. 11), a liderança é a mais falada e o menos compreendido dos fenómenos humanos. Stogdill (1974, p. 259), no seu livro "Handbook of Leadership" concluiu que "existem tantas definições de liderança como os investigadores que a tentaram definir". Este mesmo autor, os líderes são agentes de mudança, pessoas cujos atos influenciam mais os outros do que são influenciados. Para Donnelly, Gibson e Ivancevich (2000, p. 272) a liderança é uma tentativa de usar a influência não coerciva para motivar os indivíduos a realizar algum objetivo. Para Rouco (2012) a liderança é a capacidade de influenciar uma ou mais pessoas para cumprir os objetivos organizações.

Muitas outras definições existem e os pontos de convergência e divergência são muitos. Dois aspetos parecem ser comuns à maioria das definições de liderança. Em primeiro lugar, elas conservam o denominador comum de que a liderança está ligada a um fenómeno grupal, isto é, envolve duas ou mais pessoas. Em segundo lugar, fica claro tratar-se de um processo de influência exercido de forma intencional por parte dos líderes sobre os seus seguidores, levando-os a cumprir os objetivos traçados (Barracho, 2012). Uma das maiores polémicas envolve a questão de se saber se a liderança é um processo coletivo partilhado por todos os membros do grupo ou se, pelo contrário, resulta de uma especialização de papéis (Rego, 1998).

Uma outra controvérsia sobre esta temática é a discussão sobre se a liderança é adquirida ou inata? É genericamente aceite que a liderança não é uma simples qualidade inata, "mas sim uma relação complexa entre algumas variáveis: as características do líder, as suas atitudes, as suas necessidades e as características pessoais dos elementos do grupo, características da organização e, por último, o ambiente económico, social e político (...)" (Barracho, 2012, p. 55). Também nesta linha de pensamento Motta (1999, p. 207), defende que para exercer liderança não é necessário conter habilidades raras, mas sim aprendê-las através do ensinamento e da experiência de vida e que os líderes são pessoas comuns que aprendem habilidades comuns, mas que no seu conjunto formam uma pessoa incomum. Contudo, o ato de liderar não está ao alcance de muitos, pese embora alguns desempenhem da melhor forma o seu cargo, não possuem competências extraordinárias, autoridade ou poder. Consequentemente liderar não é ordenar nem mandar, mas convencer os liderados no sentido de realizarem as ideias pré-concebidas por quem os lidera. A persuasão é feita de estímulos motivacionais que permitem aos subordinados, individualmente ou em trabalho de equipa, desempenhar as tarefas extraordinariamente bem.

Nunca se abordou tanto sobre a importância do trabalho em equipa como agora, cada vez mais se procura o indivíduo com capacidades de trabalhar em conjunto, tornando-se numa competência essencial aquando do recrutamento organizacional. O trabalho em equipa é essencial, tornando os subordinados "os óculos do líder", que lhe permitem "perceber melhor o que acontece à sua volta e prestar atenção aos sinais ténues, de forma a ter uma maior consciência da situação atual, o que o tende a ajudar a pensar nos problemas e projetos que estão para vir" de acordo com um estudo efetuado junto de

milhares de trabalhadores por James Kouzes e Barry Posner, para o seu livro "O desafio da liderança".

Segundo Kouzes e Posner (2007), existem padrões comuns à prática da liderança que podem ser aprendidos, não obstante de cada líder ser um indivíduo único. Afirmam também que "o fenómeno da liderança se encontra em todo o lado e não está reservada a só alguns" (Kouzes e Posner 2009, p. 45), na mesma lógica "a liderança é um conjunto identificável de capacidades e competências que estão disponíveis para todos" e "é uma relação entre aqueles que querem liderar e aqueles que escolhem seguir" (Kouzes & Posner, 2009, p. 46).

É de realçar que a liderança a nível das Forças Armadas apresenta-se como fator preponderante e essencial na organização, tendo o líder militar de ter capacidades muito desenvolvidas nesta área, por ter de lidar com o stress da batalha e com a gestão das emoções e expectativas das suas tropas, ou seja, não só tem de ser proficiente em termos táticos, como tem de saber lidar a nível emocional com a morte e de apresentar a resiliência e força mental para suprimir a pressão a que os subordinados ficam sujeitos numa situação de guerra aberta (Field Manual FM 6-22, Army Leadership, 2006).

Ser líder militar, apresenta-se como um desafio com dificuldades acrescidas e maiores responsabilidades. A defesa de uma Nação abarca muitas componentes com a conjugação de vários fatores, que fazem com que a liderança, neste ambiente, seja um trabalho particularmente de elevada complexidade. Para melhorar a sua proficiência, os líderes militares devem tirar proveito das mais variadas oportunidades para aprender e ganhar experiência para potenciar e otimizar as competências de um líder. Devem procurar novas oportunidades de aprendizagem, de formação, questionar e pedir críticas de desempenho.

Esta abordagem a favor da aprendizagem ao longo da vida garante líderes proficientes e não apenas Comandantes (FM 6-22, Army Leadership, 2006). Os Comandantes, têm de ter em atenção o facto de a desmotivação entre os militares ser cada vez mais notória, é necessário exercer o dever de tutela, acautelando o seu bem-estar, estimular a coesão e o trabalho de equipa, de modo a sentirem-se parte de algo superior - a instituição à qual pertencem, levando a um incremento da sua motivação, desempenho e, consequentemente aumento da sua produtividade.

2.3. Modelo de competências de liderança

Rouco (2012) apresentou um modelo com 26 competências de liderança para o contexto militar que resultou do estudo efetuado aos Oficiais do Exército Português na obtenção de desempenhos superiores e como indicam Oliveira, Rouco e Gladkikh (2016) foi acrescentado posteriormente a competência proatividade. O modelo de competências de liderança de Rouco está dividido em quatro dimensões e que são as seguintes: domínio de si próprio (competências pessoais-cognitivas); domínio das relações com os outros (competências sociais); domínio do trabalho, atividades e tarefas (competências funcionais); e domínio da gestão (competências organizacionais). O domínio de si próprio (competências pessoais-cognitivas) contempla as seguintes competências: coragem; auto-confiança; auto-controlo; flexibilidade e adaptabilidade; determinação e preserverança; otimismo e entusiasmo; consideração; integridade; transparência; e

proatividade. O domínio das relações com os outros (competências sociais) contempla as seguintes competências: carisma; liderança participativa e envolvimento; influencia pela referência; abertura à multilturalidade; reconhecimento, feedback positivo e valorização; comunicação e assertividade; coesão e trabalho de equipa; desenvolvimento dos outros; e orientação para as relações humanas. O domínio do trabalho, atividades e tarefas (competências funcionais) contempla as seguintes competências: tomada de decisão; capacidade para resolver problemas; e aptidão técnica e profissional. O domínio da gestão (competências organizacionais) contempla as seguintes competências: visão; gestão de conflitos; avaliação organizacional; orientação para a missão; e comando e direção. Para o presente estudo foi adotado o modelo de competências de liderança (Rouco, 2012) dado que é o que serve de referência nos couteúdos programaticos ministrados da Unidade Curricular de Ética e Liderança. Esta unidade curricular é ministrados as todos os cursos da Academia Militar Portuguesa.

Com base neste modelo foram realizados vários estudos. Rouco e Casademunt (2013), realizaram um estudo com Oficiais Subalternos e Capitães onde concluíram que a resiliência e o entusiasmo, a tomada de decisão e a aparência e a lealdade são as competências que mais promovem o desempenho superior e a eficácia da ação da liderança. Rouco, Vieira Borges, Lemos Pires, et al. (2013) verificaram que os comandantes na liderança direta (nível operacional da gestão) consideram como mais importantes para influenciar positivamente os seus seguidores a tomada de decisão, resiliência, entusiasmo, iniciativa, tato, exemplo e a aplicação da justiça (ser justo). Loureiro (2014) num estudo efetuado sobre o comando em operações em áreas edificadas verificou que os Oficiais Subalternos para promover elevados níveis de desempenho e satisfação, utilizavam com mais frequência a orientação para tarefa, tomar decisões, flexibilidade e adaptabilidade, autocontrolo, comunicação e promoção do desenvolvimento. Covelo (2014) confirmou que os subordinados percecionam que os seus comandantes (Oficias Subalternos) focam-se essencialmente na orientação para a tarefa através dos seguintes comportamentos: Orientação para a missão, ser o exemplo, ética, determinação e perseverança, e visão. Lopes (2015a) identificou que os comportamentos de liderança praticados pelos comandantes associados à visão do ambiente externo e interno, tomada de decisão, liderança participativa e coesão e trabalho de equipa estão positiva e fortemente correlacionados com a satisfação dos subordinados. Oliveira (2015) conclui que nas operações em áreas edificadas, os comandantes devem praticar, com elevados níveis de proficiência, os comportamentos de liderança associados à coragem, promoção desenvolvimento, liderança participativa, flexibilidade e adaptabilidade, ser um exemplo e tomar decisões. Pinto (2015) conduziu um estudo para verificar o impacto da ação da liderança no compromisso dos subordinados e confirmou que alguns comportamentos de liderança estão mais associados, tais como: orientação para a tarefa; tomada de decisão; visão do ambiente externo e interno; coesão, trabalho de equipa e cooperação; gestão de conflitos; e liderança participativa. Lopes (2015b) confirmou que os subordinados percecionam que os seus comandantes (Oficias Subalternos e Capitães) têm níveis mais elevados de proficiência nas seguintes competências: Comunicação assertiva; orientação para as tarefas; e reconhecimento, feedback positivo e valorização. Tavares, Rouco e Carvalho (2015) concluíram que os subordinados percecionam nos seus comandantes (Oficias Subalternos e Capitães) comportamentos de liderança relacionados significativamente de forma positiva com a orientação para as tarefas, comunicação assertiva e liderança participativa. Pinho (2016) num estudo efetuado

sobre a influência dos Instrutores nos graduados instruendos durante a realização de um curso de comandos concluiu que a coesão e trabalho de equipa, tomada de decisão, orientação para as tarefas, gestão de conflitos, liderança participativa e motivação são as competências que mais se relacionam com a satisfação e a eficácia da liderança para promover desempenhos superiores. Machado (2017) realizou um estudo no contexto da Guarda Nacional Republicana sobre o impacto dos estilos de liderança no afeto e concluiu que o estilo de liderança participativo está relacionado com o afeto positivo. Barbosa (2018) num estudo efetuado no contexto da Guarda Nacional Republicana (Grupo de Intervenção de Operações Especiais), concluiu que existem relações significativas entre a capacidade de resolver problemas, a tomada de decisão e o esforço extraordinário, e entre as relações interpessoais, comunicação assertiva, empatia e a satisfação da liderança.

Após a revisão de literatura foi desenhado o modelo concetual (Figura 1) e a relação entre as variáveis em estudo.

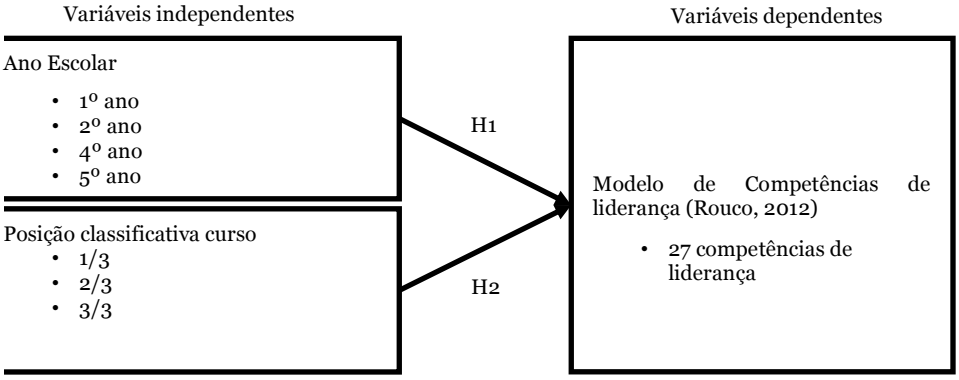


Figura 1 – Modelo Concetual do Estudo.

De acordo com a Figura 1 e tendo como referência a pergunta de partida apresentada no final da seção «Introdução», foi formulada a seguinte hipótese:

Hipótese 1: Existe uma evolução positiva significativa do nível de proficiência das competências de liderança dos Cadetes alunos da Academia Militar Portuguesa ao longo dos anos escolares.

Em contexto de uma Escola Militar, a posição que o Cadete aluno ocupa no curso durante e após a conclusão do mesmo é determinante para a escolha de cargos e da carreira. Por isso e face à curiosidade dos investigadores em verificar como se manifestam os níveis de proficiência das competências nos Cadetes alunos com diferentes classificações, foi formulada a seguinte hipótese:

Hipótese 2: Existem diferenças significativamente no nível de proficiência de competências de liderança entres os Cadetes alunos com diferentes posições no curso.

3. Materiais e Métodos

3.1. Contexto e Descrição dos Cursos

Os jovens cidadãos portugueses, voluntários, militares ou civis, de ambos os géneros, na sua opção de escolha da sua carreira profissional têm, de entre todos os estabelecimentos de ensino superior português, a Academia Militar como escolha. A Academia Militar Portuguesa, como escola de líderes, tem responsabilidade de formar os futuros oficiais nas áreas de conhecimento das ciências militares requeridas para o cumprimento das missões específicas das Forças Armadas Portuguesas e da GNR.

De acordo com a legislação que concerne ao ensino superior público universitário, depois de ultrapassadas todas as fases do concurso, os alunos considerados aptos e admitidos após seriação, ocupam as vagas a concurso e ingressam em ciclos de estudos de Mestrados Integrados das diferentes armas e serviços, agrupados em quatro áreas científicas a saber: Ciências Militares, Administração e Gestão, Engenharias e Saúde. O grau de mestre constitui a habilitação mínima exigida para a aquisição de competências adequadas para o exercício das funções de comando, direção e chefia para o início da profissão militar na categoria de oficiais quer para o Exército, quer para a GNR.

Para o efeito os alunos, em regime de internato e envergando uniforme, têm de frequentar os cursos até ao seu *terminus*, podendo ter a duração de 10 semestres (5 anos, com tirocínio incluído) ou de 12 semestres (6 anos) curriculares de trabalho, consoante a arma ou o serviço escolhido. A par de uma formação militar e comportamental, os alunos adquirem o grau referido após a obtenção de 300 a 360 ECTS correspondente ao 2º ciclo.

3.2. Metodologia de Investigação

Esta investigação é um estudo de caso sobre a avaliação da evolução do nível de proficiência das competências de liderança aos Cadetes alunos da Academia Militar Portuguesa. Para materializar os objetivos desta investigação seguiu-se o método quantitativo através da aplicação de um questionário aos Cadetes alunos da Academia Militar Portuguesa do Curso General Augusto Simas Machado (ano de entrada 2016/2017) e do Curso General Bernadim Freire de Andrade (ano de entrada 2013/2014). Para avaliar a evolução do nível de proficiência das competências de liderança dos Cadetes alunos realizou-se um estudo longitudinal através da aplicação do questionário em dois momentos destintos e em anos escolares diferentes. Esta investigação foi limitada aos alunos dos ciclos de estudo com a duração de 10 semestres (5 anos, com tirocínio incluído). Não tendo sido possível aplicar o questionário ao longo dos cinco anos (mestrado integrado) a um dos cursos mencionados, optou-se por aplicar o questionário aos Cadetes alunos do Curso General Augusto Simas Machado no início do ano escolar de 2016/2017 (1º ano) e 2017/2018 (2º ano), e ao Curso General Bernadim Freire de Andrade no final do ano escolar de 2016/ 2017 (4ºano) e 2017/2018 (5º ano).

3.3. Instrumento de Recolha de Dados

Para a recolha dos dados foi utilizado um questionário com perguntas fechadas. O questionário utilizado foi o de Rouco (2012), com seis perguntas sociodemográficas

(idade, ano escolar, posição no curso (1/3, 2/3 e 3/3), género, experiência profissional anterior e origem de recrutamento) e 81 perguntas para medir o nível de proficiência das competências de liderança. Para medir o nível de proficiência das competências em estudo, utilizou-se a escala de *Likert* com 5 níveis de resposta: 1 (discordo totalmente); 2 (discordo), 3 (nem discordo nem concordo); 4 (concordo); 5 (concordo totalmente).

O questionário foi aplicado presencialmente aos Cadetes alunos do Curso General Augusto Simas Machado no 1º e 2º momento. Ao Curso General Bernadim Freire de Andrade, o questionário foi aplicado presencialmente no 1º momento e via *Google Forms* no 2º momento dado que se encontravam em várias unidades militares a frequentar o 5º ano escolar (tirocínio/estágio).

3.4. Amostra

No ano letivo de 2016/2017 a população de Cadetes alunos na Academia Militar Portuguesa para os ciclos de estudo com 5 anos de duração era de 368. A amostra para este estudo é constituída por 117 cadetes alunos de todas as armas e serviços do Exército e da GNR, a frequentar o 1º ano escolar (66 - Curso General Augusto Simas Machado) e o 4º ano escolar (51 - Curso General Bernardim Freire de Andrade) da Academia Militar Portuguesa no ano letivo de 2016/17. Dos 117 Cadetes alunos, 18 são do género feminino e 99 do género masculino, com uma idade média de 21 anos.

3.5. Métodos Estatísticos

Os dados foram organizados e tratados no IBM Statically Packege for Social Sciences (SPSS – versão 22). Para verificar a consistência interna de cada competência usou-se o coeficiente de *Alpha de Cronbach* com valores entre os 0,72 e 0,93. Para confirmar ou infirmar as hipóteses 1 e 2 utilizou-se a significância estatística que é considerada um procedimento para verificar a discrepância de uma hipótese estatística em relação aos dados observados, utilizando uma medida de evidência (p-valor), e no qual o nível de significância é a probabilidade de rejeitar a hipótese nula quando esta é verdadeira. Para o efeito, foram utilizados testes paramétricos Teste-t (duas variáveis) e Post Hoc (3 variáveis). Nesta investigação para testar se a amostra segue ou não uma distribuição normal, utilizaram-se os testes Kolmogorov-Smirnov e *Shapiro-Wilk* e quanto à homogeneidade utilizou-se o teste *Levene*.

4. Resultados

4.1. Análise Descritiva

Da análise à Tabela 1 verifica-se que os valores da média do nível de proficiência das competências dos Cadetes alunos do Curso General Augusto Simas Machado no 1º ano, tendo em conta a categoria «ano escolar», variam entre ($\overline{x}$ = 3,86) e ($\overline{x}$ = 4,48). O valor da média mais baixo dentro deste curso ocorreu na competência «liderança por delegação» ao invés do valor mais elevado se verificar na competência «consideração». Em todas as competências o desvio padrão obtido foi sempre inferior a 1, com uma variância entre (S = 0,47) e (S = 0,74). Passado um ano e aplicado o mesmo questionário à mesma amostra, verificou-se que os valores da média do nível de proficiência das competências

dos Cadetes alunos agora a frequentar o 2º ano, tendo em conta a mesma categoria «ano escolar», variam na competência «autocontrolo» com o valor mais baixo ($\overline{x}$ = 4,04) mas com a maior dispersão nas respostas dadas (S = 0,57), seguida da «liderança por delegação» com média de ($\overline{x}$ = 4,05) e desvio padrão inferior (S = 0,46). De realçar que o valor das médias do nível de proficiência, no 2º momento da aplicação do questionário, foi superior em todas as competências de liderança, com exceção para «aptidão técnica e profissional».

No Curso General Bernardim Freire de Andrade, verifica-se que os valores da média do nível de proficiência das competências dos Cadetes alunos a frequentar o 4º ano, tendo em conta a categoria «ano escolar», assume uma variância entre ($\overline{x}$ = 3,80) e ($\overline{x}$ = 4,40). O valor da média mais baixo verifica-se na competência «liderança por delegação» ao invés do valor mais elevado se verificar na competência «consideração». Em todas as competências o desvio padrão obtido foi sempre inferior a 1, com uma variância entre (S = 0,47) e (S = 0,73) que, pese embora com valores diferentes, curiosamente ocorrem nas mesmas competências dos alunos do 1º ano. Após um ano escolar e aplicado o mesmo questionário ao referido Curso, verificou-se que os valores da média das competências dos cadetes alunos agora a frequentar o 5º ano, tendo em conta a mesma categoria «ano escolar», voltam os valores máximos e mínimos a recair na competência «liderança por delegação» com o valor mais baixo ($\overline{x}$ = 4,00) mas com a maior dispersão nas respostas dadas (S = 0,57). Ao invés e com o valor mais elevado na média a verificar-se na competência «consideração». De realçar que o valor das médias do nível de proficiência, no 2º momento da aplicação do questionário, foi superior em todas as competências de liderança.

Competências de liderança / Ano escolar	**Curso General Augusto Simas Machado**				**Curso General Bernardim Freire de Andrade**			
	1º ano 16/17 n = 66		**2ª ano 17/18 n = 66**		**4º ano 16/17 n = 51**		**5ª ano 17/18 n = 51**	
	($\overline{x}$)	**(S)**	**($\overline{x}$)**	**(S)**	**($\overline{x}$)**	(S)	**($\overline{x}$)**	(S)
Determinação e perseverança	4,32	0,47	4,34	0,48	4,22	0,51	4,34	0,44
Otimismo e entusiasmo	4,21	0,57	4,22	0,48	4,14	0,49	4,27	0,48
Abertura à multiculturalidade	4,21	0,74	4,26	0,56	4,06	0,65	4,24	0,50
Orientação para as relações humanas	4,25	0,48	4,34	0,44	4,13	0,48	4,32	0,40
Consideração	4,48	0,48	4,48	0,46	4,40	0,55	4,53	0,44
Aptidão técnica e profissional	4,41	0,48	4,19	0,50	4,33	0,47	4,35	0,43
Autoconfiança	4,13	0,51	4,18	0,47	4,08	0,51	4,29	0,45
Autocontrolo	3,90	0,66	4,04	0,57	3,97	0,73	4,15	0,53
Capacidade para resolver problemas	3,89	0,53	4,09	0,48	3,94	0,49	4,09	0,48
Comunicação	4,01	0,57	4,12	0,49	4,02	0,52	4,10	0,51
Assertividade	4,19	0,54	4,27	0,42	4,08	0,55	4,18	0,42
Coragem	4,15	0,55	4,21	0,48	3,98	0,54	4,15	0,45
Desenvolver os outros	4,02	0,47	4,17	0,47	4,05	0,53	4,17	0,41

Competências de liderança / Ano escolar	Curso General Augusto Simas Machado				Curso General Bernardim Freire de Andrade			
	1º ano 16/17 n = 66		2ª ano 17/18 n = 66		4º ano 16/17 n = 51		5ª ano 17/18 n = 51	
	$(\bar{\times})$	(S)	$(\bar{\times})$	(S)	$(\bar{\times})$	(S)	$(\bar{\times})$	(S)
Empatia	4,14	0,57	4,30	0,51	4,20	0,55	4,31	0,48
Liderança participativa	4,16	0,47	4,33	0,46	4,09	0,53	4,28	0,42
Liderança por delegação	3,86	0,57	4,05	0,46	3,80	0,61	4,00	0,57
Flexibilidade e adaptabilidade	4,11	0,53	4,15	0,45	4,20	0,50	4,34	0,45
Trabalho de equipa	4,30	0,56	4,37	0,45	4,26	0,50	4,33	0,43
Gestão de Conflitos	4,18	0,56	4,26	0,46	4,25	0,52	4,32	0,42
Influencia pelo exemplo	4,05	0,54	4,10	0,54	4,09	0,50	4,21	0,54
Orientação para a tarefa	4,06	0,56	4,16	0,47	4,02	0,54	4,20	0,45
Reconhecimento e feedback positivo	4,27	0,56	4,43	0,47	4,35	0,54	4,35	0,46
Relações interpessoais	4,28	0,52	4,34	0,46	4,16	0,51	4,33	0,41
Tomada de decisão	3,95	0,49	4,10	0,48	3,99	0,55	4,13	0,48
Transparência	4,25	0,58	4,38	0,50	4,03	0,67	4,31	0,50
Visão	4,02	0,50	4,12	0,43	3,95	0,53	4,09	0,44
Proatividade	4,06	0,47	4,12	0,52	4,05	0,51	4,20	0,46

Tabela 1 – Média e desvio padrão das competências de liderança por ano escolar (n=117).

4.2. Comparação das médias entre o 1º e 2º momento por anos escolares

A Tabela 2 apenas apresenta os resultados do Teste-t entre os pares do nível de proficiência das competências de liderança com um $\rho < 0,05$ das respostas dos alunos que frequentaram o 1º ano 16/17 e 2º ano 17/18 do Curso General Augusto Simas Machado e que são as seguintes: aptidão técnica e profissional; capacidade para resolver problemas; desenvolver os outros; liderança participativa; liderança por delegação; reconhecimento e *feedback* positivo; e tomada de decisão.

Pares de competências de liderança		Diferenças emparelhadas					t	Grau de liberdade df	Valor de ρ Sig. (2 extremidades)
		Média	Desvio Padrão	Erro padrão da média	95% Intervalo de Confiança da Diferença				
					Inferior	Superior			
Par 6	Aptidão técnica e profissional	0,22	0,53	0,07	0,09	0,35	3,38	65	0,00
Par 9	Capacidade para resolver problemas	-0,20	0,44	0,05	-0,31	-0,09	-3,63	65	0,00
Par 13	Desenvolver os outros	-0,16	0,48	0,06	-0,27	-0,04	-2,65	65	0,01

Pares de competências de liderança		Diferenças emparelhadas					t	Grau de liberdade df	Valor de ρ Sig. (2 extremidades)
		Média	Desvio Padrão	Erro padrão da média	95% Intervalo de Confiança da Diferença				
					Inferior	Superior			
Par 15	Liderança participativa	-0,18	0,52	0,06	-0,31	-0,05	-2,82	65	0,01
Par 16	Liderança por delegação	-0,19	0,56	0,07	-0,33	-0,05	-2,78	65	0,01
Par 22	Reconhecimento e feedback positivo	-0,17	0,50	0,06	-0,29	-0,04	-2,69	65	0,01
Par 24	Tomada de decisão	-0,16	0,49	0,06	-0,28	-0,04	-2,61	65	0,01

Tabela 2 – Teste-t entre os pares das médias das competências de liderança para os alunos que frequentaram o 1º ano 16/17 e 2º ano 17/18 do Curso General Augusto Simas Machado (n=66).

A Tabela 3 apenas apresenta os resultados do Teste-t entre os pares de competências de liderança com um ρ<0,05 das respostas dos alunos que frequentaram o 4º ano 16/17 e 5º ano 17/18 do Curso General Bernardim Freire de Andrade e que são as seguintes: orientação para as relações humanas; autoconfiança; liderança participativa; e transparência.

Pares de competências de liderança		Diferenças emparelhadas					t	Grau de liberdade df	Valor de ρ Sig. (2 extremidades)
		Média	Desvio Padrão	Erro padrão da média	95% Intervalo de Confiança da Diferença				
					Inferior	Superior			
Par 4	*Orientação para as relações humanas*	- 0,20	0,51	0,07	- 0,34	-0,05	- 2,73	50	0,01
Par 7	*Autoconfiança*	- 0,22	0,48	0,07	- 0,35	-0,08	- 3,18	50	0,00
Par 15	*Liderança participativa*	- 0,20	0,55	0,08	- 0,35	-0,04	- 2,56	50	0,01
Par 25	Transparência	- 0,28	0,66	0,09	- 0,47	- 0,09	- 3,02	50	0,00

Tabela 3 – Teste-t entre os pares das médias das competências de liderança para os alunos que frequentaram o 4º ano 16/17 e 5º ano 17/18 do Curso General Bernardim Freire de Andrade (n=51).

4.2. Comparação das médias por classificação (Posição no curso)

Para verificar se existem diferenças significativas entre o valor das médias das respostas dos Cadetes alunos que ocupam o primeiro terço, segundo terço e terceiro terço do curso foram consideradas as respostas do 2º momento da aplicação do questionário e a uma amostra total (n=117). De acordo com a Tabela 4, que apenas apresenta os resultados cujo ρ<0,05, verifica-se que o nível de proficiência da competência «determinação e perseverança» da subamostra «primeiro terço do curso» é significativamente diferente da subamostra «último terço do curso»; na competência «aptidão técnica e profissional» o nível de proficiência da subamostra «primeiro terço do curso» é significativamente diferente da do grupo «último terço do curso»; Na competência «autocontrolo» da subamostra «primeiro terço do curso» o nível de proficiência é significativamente diferente da subamostra «segundo terço do curso»; Na competência "assertividade" das subamostras "primeiro terço do curso» e «segundo terço do curso» o nível de proficiência é significativamente diferente da subamostra «último terço do curso»; Na competência «influência pelo exemplo» da subamostra «primeiro terço do curso» o nível de proficiência é significativamente diferente da subamostra «último terço do curso».

Variável dependente			Dif. média (I-J)	Erro Padrão	Sig.	Intervalo de Confiança 95%	
						Limite inferior	Limite superior
Determinação e perseverança	Primeiro terço do curso	Último terço do curso	0,31*	0,11	0,02	0,05	0,57
Aptidão técnica e profissional	Primeiro terço do curso	Último terço do curso	0,35*	0,11	0,01	0,08	0,62
Autocontrolo	Primeiro terço do curso	Segundo terço do curso	0,28*	0,11	0,04	0,01	0,55
Assertividade	Primeiro terço do curso	Último terço do curso	0,31*	0,10	0,01	0,07	0,55
	Segundo terço do curso	Último terço do curso	0,32*	0,10	0,01	0,08	0,57
Influencia pelo exemplo	Primeiro terço do curso	Último terço do curso	0,34*	0,13	0,03	0,03	0,65

Tabela 4 – Teste Post Hoc de Tukey HSD de comparações múltiplas (n=117).

5. Discussão

Considerando os resultados apresentados nas tabelas da seção anterior, nesta seção far-se-á uma interpretação dos mesmos tendo como referência os *curricula* e conteúdos programáticos da Academia Militar Portuguesa, bem como os resultados de outros estudos similares com amostras de Oficiais Subalternos e Capitães que utilizaram o mesmo modelo e questionário no contexto do Exército e da GNR. Durante a discussão dos resultados dar-se-á uma resposta às hipóteses e pergunta de partida deste estudo.

Hipótese 1: Existe uma evolução positiva significativa do nível de proficiência das competências de liderança dos Cadetes alunos da Academia Militar Portuguesa ao longo dos anos escolares. A hipótese 1 confirma-se. A Tabela 1 indica que todas as competências têm uma evolução positiva aos longo dos anos escolares em estudo. Ainda, as Tabelas 2 e 3 indicam que os Cadetes alunos desenvolvem significativamente as competências autoconfiança, aptidão técnica e profissional, capacidade para resolver problemas, desenvolver os outros, liderança participativa, liderança por delegação, orientação para as relações humanas, reconhecimento e *feedback* positivo, transparência, e tomada de decisão ao longo dos cinco anos escolares. No final dos 5 anos, os alunos estão mais capacitados para resolver problemas e tomar decisões que são duas competências essenciais e criticas no exercício das funções de comandante, em que estes são preparados para tomar decisões, em que esta é um «ato único e exclusivo do comandante» e que é reforçado pelas boas práticas dos Oficiais Subalternos e Capitães alcançados noutros estudos (Barbosa, 2018; Lopes, 2015b; Lopes, 2015c; Loureiro, 2014; Oliveira, 2015; Pinho; 2016; Pinto, 2015; Rouco & Casademunt, 2013; Rouco, Vieira Borges, Lemos Pires, et al., 2013). Associado à resolução de problemas e tomada de decisão, os resultados obtidos das respostas alunos confirmam que a formação e educação da AM quanto aos estilos de liderança, prepara-os para envolver os outros na tomada de decisão sobre o dia-a-dia das tarefas, e que também é reforçado pelos resultados obtidos noutros estudos (Lopes, 2015b; Machado; 2017; Oliveira, 2015; Pinho, 2016; Pinto, 2015; Tavares, Rouco & Carvalho, 2015). A orientação para as relações humanas e o reconhecimento e *feedback* positivo são competências que estão associadas à liderança na medida em que para influenciar os outros é necessário ter a capacidade para estabelecer relações interpessoais, e estas capacidades são reforçadas no dia-a-dia da vida académica dos alunos e assente na frase «primeiro a missão e pessoas sempre". A capacidade para desenvolver os outros é uma das funções principais de uma comandante na preparação dos seus subordinados para «agir» em tempo oportuno (Lopes, 2015b; Loureiro, 2014; Oliveira, 2015) em Teatros de Operações cada vez mais disperso. As competências autoconfiança e transparência vem validar e reforçar o ensino e prática dos valores Castrenses.

Hipótese 2: Existem diferenças significativamente no nível de proficiência de competências de liderança entre os Cadetes alunos com diferentes posições no curso. A hipótese 2 confirma-se. De acordo com a Tabela 4, que apenas apresenta os resultados cujo $\rho < 0{,}05$, verifica-se que o nível de proficiência das competências «aptidão técnica e profissional», «assertividade», «autocontrolo», «determinação e perseverança», «influência pelo exemplo» da subamostra «primeiro terço do curso» é significativamente diferente das outras subamostras. Com base nestes resultados, pode-se afirmar que os alunos melhor classificados desenvolvem com determinação e perseverança capacidades técnicas com elevados níveis de proficiência e controlo para obter desempenhos superiores, e mobilizando os outros através de uma comunicação assertiva e através do exemplo.

Pergunta de Partida (PP): Será que o nível de proficiência das competências de liderança tem uma evolução positiva ao longo dos anos escolares? De acordo com todos os resultados apresentados, pode-se afirmar que o programa e conteúdos curriculares da Academia Militar desenvolvem o nível de proficiência de todas as competências de liderança do modelo Rouco (2012).

Limitações: A não aplicação do questionário ao longo dos 5 anos escolares a um curso não permitiu fazer uma avaliação completa da evolução do nível de proficiência de competências de liderança.

Futuras investigações: Aplicar o questionário de competências de liderança a todos os anos escolares (5 anos) de um curso de entrada na Academia Militar e continuar o estudo sobre estes indivíduos enquanto Oficiais e até ao Curso de Promoção a Capitão.

6. Conclusões

Este estudo confirma que os programas e os conteúdos curriculares da Academia Militar Portuguesa desenvolvem o nível de proficiência de todas as competências de liderança do Modelo (Rouco, 2012).

Os Cadetes alunos desenvolvem significativamente as competências autoconfiança, aptidão técnica e profissional, capacidade para resolver problemas, desenvolver os outros, liderança participativa, liderança por delegação, orientação para as relações humanas, reconhecimento e *feedback* positivo, transparência, e tomada de decisão ao longo dos cinco anos escolares.

Os alunos melhor classificados desenvolvem com determinação e perseverança capacidades técnicas com elevados níveis de proficiência e controlo para obter desempenhos superiores, e mobilizando os outros através de uma comunicação assertiva e através do exemplo.

Referências

Astin, A. W., & Astin, H. S. (2000). *Leadership reconsidered: Engaging higher education in social change*. Battle Creek, MI: W. K. Kellogg Foundation.

Barracho, C. (2012). *Liderança em contexto organizacional*. Lisboa: Escolar Editora.

Barbosa, J. M. (2018). *O Big-Five e a liderança no Grupo de Intervenção de Operações Especiais*. Trabalho Individual Aplicado para o Mestrado Integrado na Especialidade de Segurança. Lisboa: Academia Militar.

Bass, B. M. (1990). *Bass and Stodgill´s handbook of leadership* (3rd ed.). New York: Free Press.

Boyatzis, R. E. (1982). *The competence manager: A model for effective performance*. New York: John Wiley & Sons Inc.

Ceitil, M. (2007). Gestão e desenvolvimento de competências (2. Ed.). Lisboa: Edições Sílabo.

Covelo, J. (2014). *Caraterização dos comportamentos de liderança e a sua influência no clima organizacional das Unidades de Infantaria*. Trabalho Individual Aplicado para o Mestrado Integrado na Especialidade de Infantaria. Lisboa: Academia Militar.

Cruz, C. (2001). *Competências e habilidades: Da proposta à prática*. São Paulo: Edições Loyola.

Donnelly, J. H., Gibson, J. L., & Ivancevich, J. M. (2000). *Administração – Princípios de gestão empresarial*. Lisboa, McGraw-Hill.

FM 6-22 (2006). *Field manual: Army leadership: Competent, confident, and agile*. Washington, DC: Headquarters Department of the Army.

Kouzes, J. M., & Posner, B. Z. (2007). *The leadership challenge* (4. ed.). San Francisco: Jossey-Bass.

Lopes, F. (2015a). *Caraterização dos comportamentos de liderança e estilos de comunicação dos Oficiais Subalternos do quadro permanente da Arma de Cavalaria e a sua influência no esforço extraordinário, satisfação e eficácia*. Trabalho Individual Aplicado para o Mestrado Integrado na Especialidade de Cavalaria. Lisboa: Academia Militar.

Lopes, L. (2015b). *Identificação das competências de liderança associadas ao comando dos Oficiais Subalternos e Capitães de Infantaria: Uma meta-análise*. Trabalho Individual Aplicado para o Mestrado Integrado na Especialidade de Infantaria. Lisboa: Academia Militar.

Loureiro, N. (2014). *O Combate em áreas edificadas e a sua implicação no desenvolvimento de competências de comando e liderança*. Trabalho Individual Aplicado para o Mestrado Integrado na Especialidade de Infantaria. Lisboa: Academia Militar.

Machado, J.V. (2017). *Os estilos de liderança do comandante de Posto Territorial da Guarda Nacional Republicana e as emoções dos subordinados: Estudo de caso do Comando Territorial de Braga*. Trabalho Individual Aplicado para o Mestrado Integrado na Especialidade de Segurança. Lisboa: Academia Militar.

McClelland, D. (1973). Testing for competence rather than for "intelligence". *American Psychologist*, 1-14.

Motta, P. R. (1999). *Gestão contemporânea: A ciência e a arte de se ser dirigente* (10. ed.). Rio de Janeiro: Record.

Oliveiro, T. (2015). *As Operações em áreas edificadas e a sua implicação no desenvolvimento da competência de comando e liderança. Estudo de caso: Kosovo*. Trabalho Individual Aplicado para o Mestrado Integrado na Especialidade de Infantaria. Lisboa: Academia Militar.

Oliveira, F., Rouco, J. C., & Gladkikh, T. (2016). Riding as a way of developing soft skills in higher education. *Scientific Journal Proelium*, VII (11), 269-283.

Pinho, R.F. (2016). *Liderança e coesão dos graduados instruendos no curso de comandos*. Trabalho Individual Aplicado para o Mestrado Integrado na Especialidade de Infantaria. Lisboa: Academia Militar.

Pinto, J. (2015). *A influência das competências de liderança dos Oficiais Subalternos de Cavalaria no compromisso dos subordinados*. Trabalho Individual Aplicado para o Mestrado Integrado na Especialidade de Cavalaria. Lisboa: Academia Militar.

Prahalad, C. K., & Hamel, G. (1990). The core competence of the corporation. Boston: Harvard Business Review, 68 (3), 79-91.

Rego, A. (1998). *Liderança nas organizações – teoria e prática*. Aveiro: Universidade de Aveiro.

Roldão, M. (2003). *Gestão do currículo e avaliação de competências – as questões dos professores*. Lisboa: Editorial Presença.

Rouco, J. C. D. (2012). *Modelo de gestão de desenvolvimento de competências de liderança em contexto militar*. Tese de Doutoramento em Gestão, Universidade Lusíada de Lisboa: Faculdade de Ciências da Economia e da Empresa, Lisboa.

Rouco, C., & Casademunt, A. L. (2013). O conhecimento tácito às competências de liderança. In Actas do XXVII Congresso *Anual de European Academy of Management and Business Economics* - AEDEM, Islantilla (Spain).

Rouco, C., Vieira Borges, J., Lemos Pires, N., Freire, M., Borges. J., & Casademunt, A. L. (2013). Organisational learning model in leadership based on best practices. In actas da *Conferência Internacional Managing Services in the Knowledge Economy* - MSKE 2013 da Universidade Lusíada de Famalicão. Famalicão (Portugal).

Spencer, L., & Spencer, S. (1993). *Competence at Work: Models for superior performance*. New York: John-Wiley & Sons Inc.

Stogdill, R. M. (1974). *Handbook of leadership*. New York: McMillan Free Press.

Tavares, M., Rouco, C., & Carvalho, A. (2015). Dos comportamentos de liderança aos estilos de gestão conflitos: estudo de caso de uma Grande Unidade Militar Portuguesa. In Actas do *XXV Jornadas HisponoLusas de Gestão Científica*. Universidade de Vigo, Ourense (Spain).

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 31/10/2021
Aceitação/Acceptance: 25/01/2022

Um diagnóstico sobre o processo de comunicação sigilosa entre os órgãos do Sistema Brasileiro de Inteligência

Cileno de Magalhães Ribeiro[1], Rafael Rabelo Nunes[1, 2],
Robson de Oliveira Albuquerque[1]

cilenomag@gmail.com; rafaelrabelo@unb.br; robson@redes.unb.br

[1] Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, Brasil - Zipcode 70910-900.

[2] Centro Universitário UniAtenas, Paracatu-MG, Brasil – Zipcode 38602-108 .

Pages: 169-183

Resumo: O Sistema Brasileiro de Inteligência (Sisbin) é fundamental para o assessoramento em informações ao chefe do poder executivo brasileiro. O objetivo deste trabalho é diagnosticar os desafios e oportunidades no processo de comunicação sigilosa não classificada entre os órgãos do Sisbin. Para isso, foi desenvolvido e aplicado um questionário para 137 pessoas de 13 órgãos do sistema para valorar as informações, obter apreciações sobre a Lei de Acesso à Informação e Segurança da Informação. Os dados foram analisados com base na Doutrina de Inteligência e legislações específicas que tratam sobre a Segurança da Informação. Os resultados demonstram a necessidade de atualização da ferramenta para troca de informações, além do tratamento de alguns fatores críticos. Dessa forma, esse trabalho estabelece uma diretriz para uma nova ferramenta que deve: utilizar nuvem privada, definir e implementar seus processos, possibilitar a construção conjunta de documentos e prover suporte centralizado.

Palavras-chave: Sisbin; comunicação sigilosa; nuvem privada.

A diagnosis on the secret communication process among the agencies of the Brazilian Intelligence System

Abstract: The Brazilian Intelligence System (Sisbin) is fundamental for the provision of intelligence advice to the head of the Brazilian executive branch. The objective of this paper is to diagnose the difficulties and opportunities in the process of unclassified secret communication among the agencies of the Sisbin. For this, a questionnaire was developed and applied to 137 people from 13 organs of the system to value the information, obtain appreciations about the Access to Information Law and Information Security. The data were analyzed based on the Intelligence Doctrine and specific legislation dealing with Information Security. The results show the need to update the tool for information exchange, besides the

treatment of some critical factors. Thus, this work establishes a guideline for a new tool that should: use private cloud, define and implement its processes, enable the joint construction of documents and provide centralized support.

Keywords: Sisbin; secret communication; private cloud.

1. Introdução

A importância de trocar conhecimentos entre as estruturas de Inteligência com objetivos similares é um consenso entre aqueles que se dedicam a identificar, gerir e analisar informações de interesse do Estado em todo o mundo. No Brasil, o assunto está previsto na Política Nacional de Inteligência (PNI) (Brasil, 2016), e na instituição do Sistema Brasileiro de Inteligência (Sisbin) e criação da Agência Brasileira de Inteligência (Abin), nos seus 1º, 2º e 3º artigos (Brasil, 1999).

O Sisbin foi criado para integrar ações de planejamento e execução das atividades de inteligência do Brasil. Sua função é realizar a troca de informações relevantes, facilitando a tomada de decisão pelo governo brasileiro. Logo após sua implantação em 2002, com 22 órgãos, passou-se a avaliar a adesão de novos órgãos federais por meio do Conselho Consultivo do Sisbin. A relevância da atividade ocasionou uma expansão gradativa, chegando a alcançar 48 órgãos em 2021.

O fomento do governo federal na integração de esforços e na atuação de forma conjunta também foi enfatizado na PNI (Brasil, 2016) e na Estratégia Nacional de Inteligência (Enint) (Brasil, 2017), documentos que regulamentam os aspectos de cooperação entre órgãos, atuação em rede, compartilhamento e intercâmbio de informações e do trabalho coordenado e integrado.

O processo de troca de informações de inteligência ocorre por meio de tramitação de documentos no Sisbin por dois canais: o hierárquico, que obedece à subordinação baseada na precedência funcional e o técnico, que se caracteriza por ligações de cooperação, em função da necessidade de conhecer. Esses canais devem possibilitar pronta e eficaz comunicação entre si e entre os diferentes níveis de decisão de um mesmo órgão, subsidiando o Chefe do Poder Executivo na tomada de decisão.

Os conhecimentos obtidos pelo Sisbin são concentrados na Abin, órgão central do sistema, transmitindo ao Presidente da República por meio do órgão a que estiver subordinada. Porém, no âmbito dos demais integrantes do sistema, as frações de inteligência também devem obedecer à cadeia hierárquica própria, conforme o artigo 5º da lei nº 9883 de criação da Abin (Brasil, 1999).

No contexto atual, as mídias sociais têm impulsionado o fluxo de informações por aplicativos e *"chats online",* como exemplo: *WhatsApp, Telegram, Signal, Facebook, Instagram*, dentre outros. Contudo, muitas vezes esses meios desinformam e publicam *fake news*, o que demanda agilidade no trâmite informacional, com a finalidade de melhor assessorar o chefe do poder executivo do Estado brasileiro. Assim, mesmo cercados por informação, nem sempre é possível contar com dados reais. Desta forma, esses meios de comunicação informais potencializam a necessidade de uma estruturação organizada, com rápida capacidade de processamento e checagem dos dados por meio de fontes confirmadas, aumentando ainda mais a importância do Sisbin atuar conjuntamente.

Considerando a breve contextualização apresentada, o objetivo deste trabalho é diagnosticar os desafios e oportunidades no processo de comunicação sigilosa não classificada entre os órgãos do Sisbin, buscando opiniões para agilizar, garantir e assegurar a troca de informações, tomando documentos basilares como a Lei de Acesso à Informação, A Lei Federal nº 12.527/2011 (LAI) (Brasil, 2011), a PNI, a ENINT e normativos do Departamento de Segurança da Informação que tratam sobre o assunto para assegurar o cumprimento a legislação vigente e ainda agilizar o fluxo de informações por canais seguros e padronizados para o Sisbin, visando reduzir o tempo de tramitação de dados e ainda permitir avanços nos trabalhos colaborativos de inteligência entre os órgãos de interesse.

O trabalho está organizado da seguinte forma: além da introdução, a seção 2 trata de referencial teórico onde serão discorridos sobre o Sisbin, Segurança da Informação e uma pequena revisão sobre Nuvem Privada. Em seguida, na seção 3, apresenta-se o detalhamento da metodologia utilizada no trabalho. A seção 4 apresenta os resultados e sua análise; e por fim, apresenta-se a conclusão na seção 5.

2. Referencial Teórico

A LAI do Brasil estabelece que informação são todos os dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato, sendo essa definição adotada nos orgãos nacionais (Brasil, 2011).

Informação sigilosa é aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, ou ainda, aquelas abrangidas pelas demais hipóteses legais de sigilo, nos termos do Art. 4º da LAI, e nos termos do Art 3º do Decreto sobre acesso as informações (Brasil, 2011; Brasil, 2012). Vale destacar que hipóteses legais de sigilo contemplam as informações que não precisam ser classificadas, pois já tem seu sigilo garantido por outras legislações específicas (Brasil, 2011).

Informação classificada é regida como aquela submetida temporariamente à restrição de acesso público em razão do seu teor e da sua imprescindibilidade para a segurança da sociedade e do Estado, possuindo 3 graus de restrições: ultrassecreta, cujo tempo de restrição dura 25 anos; secreta, cujo tempo de restrição dura 15 anos; e reservada, cujo tempo de restrição dura 5 anos (Brasil, 2011). Assim, toda a informação classificada é sigilosa, porém nem toda a informação sigilosa é classificada. Esse ponto gera inúmeros conflitos de organização, difusão, controle e acesso à informação, já que para determinados tipos de controle, a informação classificada no executivo federal deve usar premissas próprias de criptografia de Estado e não deve ser realizada de qualquer maneira.

2.1. Sisbin

A Atividade de Inteligência utiliza dispositivos legais que abrangem hipóteses de sigilo para garantir o fluxo de informações confidenciais em diferentes níveis. De acordo com a PNI, o Sisbin e a Abin preveem o uso de técnicas e meios sigilosos como forma de preservar a ação, os métodos e processos, a obtenção de dados negados por meio de

operações de Inteligência, a doutrina comum e os valores profissionais. Desta forma, a combinação do sigilo, dado negado e métodos próprios e flexíveis dentro de um sistema integrado que se adaptem as necessidades garantem um produto que atinge o estado da arte, pois aumentam seu viés de confirmação e consequentemente sua confiabilidade.

Por agirem de forma autônoma, as agências aportam ao centro informações por ela obtidas ou produzidas, mediante livre conveniência. Nesse ponto, localizamos limitadores a uma integração para além da acepção de coordenação que vem se reproduzindo até hoje (Ferreira, 2020).

No âmbito do Sisbin, muito se fala sobre compartilhamento de dados e informações, bem como de ações coordenadas, sobretudo no campo da segurança pública (Ferreira, 2020). Porém, os dados ou conhecimentos compartilhados, raramente são processados de maneira conjunta. Ainda que contenham alguma colaboração de outras instituições, o produto final geralmente é resultado do trabalho de análise de um único órgão, fortalecendo a necessidade de modernização tecnológica para facilitar as trocas de informações e trabalhos conjuntos. Tal compartilhamento de conhecimentos e dados ainda é realizado via Plataforma Criptográfica Portátil (PCP), tecnologia proprietária de segurança composta por um hardware criptográfico e respectivos módulos, que cifra/decifra qualquer tipo de documento digital, de modo a não torná-los protegidos contra interpretação do conteúdo por quem não de direito. Esse equipamento, desenvolvido pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC) da Abin, começou a ser usado no fim de 2007 em organizações estratégicas do governo (IDg New, 2008).

Assim, como Ferreira (2020) relata a necessidade de maior integração no compartilhamento de dados e informações, Clark (2019) reforça também a importância do trabalho conjunto em todos os projetos de análise, como esforços de equipe, já que a colaboração é vista como o único futuro prático para uma inteligência relevante e bem sucedida. Desta maneira, a união de esforços de forma colaborativa e a integração são reforçadas por ambos os autores.

Nesse contexto, a atividade de inteligência vem demonstrando muitas experiências de integração de sistemas e comunidades de inteligência como uma forma relevante e bem-sucedida para se antepor as complexidades atuais. Os conhecimentos oriundos de uma única fonte, muitas vezes não são capazes de responder a contento, assim equipes multidisciplinares para produção de conhecimento oportuno e integrado tem fortalecido o emprego do Sisbin (Ferreira, 2020).

2.2. Segurança da Informação e Nuvem privada

Segurança da Informação (SI) pode ser compreendida como ações e medidas que visam à "proteção da confidencialidade, da integridade e da disponibilidade das informações" (International Organization for Standardization, 2018, p. 4). Somando-se a esses princípios também é comum se encontrar outras propriedades relacionadas à segurança da informação, tais como confiabilidade, não-repúdio, responsabilidade e autenticidade. Essa última, que está relacionada com a "propriedade de que uma entidade seja o que ela afirma ser" (International Organization for Standardization, 2018, p. 2), se junta àquelas três primeiras para compor os requisitos mínimos de segurança da informação

que são considerados pelo Departamento de Segurança da Informação e Comunicação, do Gabinete de Segurança Institucional da Presidência da República do Brasil, segundo a Política Nacional de Segurança da Informação (Brasil, 2021).

Diversos padrões internacionais procuram traçar diretrizes sobre como essa disciplina deve ser gerenciada pelas organizações. Entre eles pode-se citar a série de normas ABNT/ ISO 27000; o CiberSecurity Framework publicado pelo National Institute of Standards and Technology (NIST); o CIS Controls v8, publicado pelo Center for Internet Security (CIS). Em todos esses padrões é consenso de que riscos de SI surgem e são mitigados por tecnologias, processos e pessoas.

Nesse sentido, após a apreciação das normatizações de gerenciamento de riscos de SI, observa-se que preservados os requisitos mínimos de SI a computação em nuvem proporciona, por suas características essenciais, tais como acesso amplo pela rede, rápida elasticidade, serviços medidos por utilização, auto provisionamento sob demanda, compartilhamento através de pool de recursos (Alves *et al,* 2021).

Além das vantagens expostas, segundo Alves *et al* (2021) os modelos de implantação em nuvem possibilitam ampla flexibilidade na sua utilização, dividindo-se em nuvem privada, como a infraestrutura que está disponível para uso exclusivo de uma única organização; nuvem comunitária: como uma infraestrutura que está disponível para uso exclusivo de uma comunidade específica, formada por organizações que possuem interesses e preocupações comuns; nuvem pública, como uma infraestrurtura disponível para uso aberto do público em geral; e nuvem híbrida: como uma infraestrutura de nuvem composta de duas ou mais infraestruturas de nuvem (privada, comunitária ou pública).

Segundo Moreira *et al* (2021) as atualizações de normativas recentes sobre o uso de nuvem foram um reflexo da necessidade do uso da nuvem frente a pandemia do coronavírus, onde ocorreu a migração de centenas de órgãos públicos e privados para o modelo home office, aumentando a demanda por serviços em nuvem de forma exponencial. A transformação digital foi acelerada em meses o que aconteceria ao longo dos anos, e dentre as mudanças está a alta adesão à nuvem.

Diante disso, a normatização recente da instrução normativa nº 5/2021 do Gabinete de Segurança Institucional da Presidência da República (Brasil, 2021), dispôs sobre os requisitos mínimos de segurança de informação para utilização de soluções de computação em nuvem, visando uma adequação na sua utilização em organismos públicos e privados.

Em meio a alta adesão de serviços de nuvem, Alves *et al* (2021) sugerem a necessidade de enfrentar riscos de transposição complexa, fato que funciona como incentivo para postergar a implementação dessa tecnologia por entidades governamentais brasileiras, principalmente quando se refere a questionamentos acerca dos riscos que estão atrelados ao seu uso, com atenção ao tratamento de dados sensíveis.

No que tange a segurança em nuvem nos diferentes modelos de serviços entregues são considerados por Sen & Tiware (2017, pp. 67-72) e Ahmed (2019, pp. 2812-2817) como mais efetivos quando há um nível de segurança maior em serviços que empregam diversos níveis de abstração.

De forma similar Dos Santos *et al* (2020) indicam um nível de segurança maior como Ahmed (2019, pp. 2812-2817), mas também acrescenta uma avaliação de desempenho de três servidores privados em nuvem, apresentando diferentes cenários de teste para avaliar o desempenho de CPU, memória e disco, para ilustrar a aplicabilidade destes softwares numa nuvem privada de baixo custo com fácil gestão e alta capacidade de desempenho, facilitando a compreensão e comparação do software NextCloud, dando ampla vantagem de utilização nessa ferramenta de código aberto se comparada aos outros servidores.

Por outro lado, Alves *et al* (2020) demonstram uma aplicação de um modelo de requisitos de segurança de computação em nuvem que de forma conceitual trata de quatro componentes – segurança de dados; avaliação de risco; requisitos técnicos, legais e de negócios e de conformidade, com um escopo mais amplo e complexo, baseado na participação de 480 funcionários de tecnologia de informação (TI) do governo australiano, promovendo uma percepção mais abrangente sobre o uso da segurança em nuvem.

3. Metodologia

Trata-se de uma pesquisa de natureza aplicada, com objetivos exploratórios e descritivos. Ela é descritiva pois "tem como principal objetivo descrever características de determinada população, fenômeno ou estabelecimento de relações entre variáveis" (Gil, 2002, p. 42). Ela é exploratória pois tem a intenção de se ter maior familiaridade com o problema estudado, compreendendo os desafios e oportunidades em se utilizar ferramentas computação em nuvem privada no processo de comunicação sigilosa não classificada entre os órgãos do Sisbin. Dessa forma, "torna-se possível construir hipóteses, que são características de uma pesquisa exploratória" (Bardin *et al*, 2010, p. 27).

A pesquisa utilizou abordagem essencialmente qualitativa pois trabalhou com "universos de significados, motivos, aspirações, crenças, valores, atitudes, o que corresponde a um espaço mais profundo de relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis" (Minayo, 1996, p. 21).

Utilizou-se um questionário como forma de coleta de dados. Ele foi construído utilizando as informações da literatura de segurança da informação e computação em nuvem e, também, de legislações específicas sobre a lei de acesso à informação e de inteligência. O uso do questionário teve como objetivo abranger maior público do Sisbin, que não seria possível com outra forma de coleta de dados. O questionário continha questões fechadas, que se utilizaram de uma escala do tipo-likert de 5 pontos, cujas opções foram: discordo totalmente, discordo, não concordo/não discordo, concordo e concordo totalmente, segundo (Monteiro Feijó, 2020). Também foi facultada a opção para o respondente informar o desconhecimento sobre o assunto, com a opção: não sei/não quero responder. Aproveitou-se também para realizar algumas perguntas abertas no final do questionário, com o objetivo de entender melhor necessidades específicas e o entendimento dos respondentes sobre a temática do levantamento de dados.

A análise dos dados do questionário foi realizada utilizando estatística descritiva para as questões fechadas, somando-se as marcações de discordo totalmente e discordo,

onde essas duas opções compuseram a “discordância” com o item questionado; e concordo e concordo totalmente, sintetizaram a concordância com o assunto abordado. Os respondentes que não opinaram ou não concordaram/ não discordaram, foram descartados do percentual que concordou ou discordou. O questionário contou com a participação de 137 servidores de 13 órgãos do Sisbin e foi aplicado de 18 de outubro a 18 de dezembro de 2021 . A amostra foi não probabilística por conveniência direcionada a servidores que lidam com informações sigilosas no seu dia-a-dia.

4. Resultados e Discussões

Nesta seção serão apresentados os resultados e discussões da pesquisa. Os assuntos serão segmentados da seguinte forma: na primeira parte, serão apresentados os resultados e análise sobre questões relacionadas especificamente ao processo de troca de informações de inteligência; na segunda parte, foram discorridas questões relacionadas à Lei de Acesso à Informação; na terceira parte serão abordadas questões inter-relacionadas. Na última parte, serão apresentados os principais pontos levantados pelos respondentes nas questões abertas. Salienta-se que foram delimitadas na pesquisa a utilização de informações não classificadas como meio inicial de implementação e testagem, podendo ser utilizada posteriormente em informações classificadas.

4.1. Resultados sobre o processo de troca de informações

Os resultados sobre o processo de troca de informações de inteligência estão dispostos na Tabela 1. É praticamente unânime a concordância dos respondentes da necessidade de controle da segurança e da gestão do conhecimento, nesse processo (questão 2.6). Também é possível verificar que a maioria dos respondentes entendem que a solução atual atende aos critérios de integridade, confidencialidade e autenticidade exigidos para troca de informações de inteligência (questões 2.1 a, b e c). Contudo, aproximadamente metade dos respondentes entendem que a solução atual não atende aos critérios de disponibilidade (questão 2.1a).

Ademais, observa-se que a maioria relata que a solução atual não atende ao critério de oportunidade (questão 2.5), o que permite concluir que há uma percepção de que a solução atual não é efetiva para compartilhamento de informações, apesar de que quando ela consiga estabelecer o fluxo informacional, faça atendendo à critérios de sigilo.

Ao questionar sobre possível solução utilizando nuvem privada, 74% responderam que concordam que essa solução atenderia à confidencialidade, integridade, autenticidade e disponibilidade. Isso reforça a importância do uso dessa ferramenta, porém também demonstra a indicação dos discordantes com a segurança dos conhecimentos e dados na nuvem, fortalecendo o gerenciamento de riscos e a adequação a normatização de requisitos mínimos para implementação da nuvem estabelecida pelo Departamento de Segurança da Informação.

Importante destacar que o uso dessa solução, viabilizaria a produção de trabalhos conjuntos interórgãos, e a edição conjunta de relatórios. Esses dois pontos tiveram concordância de mais de 90% dos respondentes (questões 2.3 e 2.4).

O processo de troca atual de informações do SISBIN em contraste com trabalhos correlatos dos autores Ferreira (2020) e Clark (2019) fortaleceram a ideia de que é necessário trabalhar em conjunto e em ambiente interagências. Tal fato favorece o emprego de uma tecnologia que viabilize a elaboração e edição de relatórios conjuntos, confirmados nas questões constante na Tabela 1.

Em relação ao uso da computação em nuvem os autores por Sen & Tiware (2017, pp. 67-72) e Ahmed (2019, pp. 2812-2817) ressaltam a importância da implementação de um meio seguro para trânsito de informações. Ainda foram reforçados aspectos de transposição complexa por Alves *et al* (2021) e o aumento exponencial da transformação digital por Moreira *et al* (2021) respaldando o emprego de softwares que garantam a segurança no fluxo informacional tanto no armazenamento como no transporte de dados.

Afirmativas avaliadas sobre a comunicação sigilosa	**Concordam**	**Discordam**	**Não opinaram**	**Não concordo / Não discordo**
2.1 a) A troca de informações entre os órgãos vinculados ao SISBIN ocorre com rapidez, atendendo aos critérios de Disponibilidade.	51% (51)	49% (49)	10% (14)	17% (23)
2.1b) A troca de informações entre os órgãos vinculados ao SISBIN ocorre com rapidez, atendendo aos critérios de Integridade	85% (92)	15% (16)	12% (17)	9% (12)
2.1c) A troca de informações entre os órgãos vinculados ao SISBIN ocorre com rapidez, atendendo aos critérios de Confidencialidade	81% (88)	19% (21)	8% (11)	12% (17)
2.1d) A troca de informações entre os órgãos vinculados ao SISBIN ocorre com rapidez, atendendo aos critérios de Autenticidade.	87% (92)	13% (14)	11% (15)	12% (16)
2.2) A criação de uma nuvem privada no SISBIN atenderia à disponibilidade, a integridade, à confidencialidade, e a autenticidade.	74% (80)	26% (28)	4% (6)	17% (23)
2.3) A capacidade de produzir trabalhos conjuntos agilizaria a produção de documentos	91% (118)	9% (12)	1% (1)	4% (6)
2.4) A troca de informações com edição conjunta de relatórios traz vantagens ao SISBIN.	92% (117)	8% (10)	2% (3)	5% (7)
2.5 a) A plataforma atual atende ao critério de oportunidade.	38% (33)	63% (55)	24% (33)	12% (16)
2.5 b) A plataforma atual atende ao critério de imparcialidade.	76% (63)	24% (20)	28% (38)	12% (16)
2.6 O controle da segurança e a gestão dos conhecimentos são fundamentais para a comunicação.	98% (131)	2% (2)	0% (0)	3% (4)
2.7 A plataforma atual atende aos critérios de possível auditoria.	65% (35)	35% (19)	42% (57)	19% (26)

Afirmativas avaliadas sobre a comunicação sigilosa	Concordam	Discordam	Não opinaram	Não concordo / Não discordo
2.8 A nuvem privada produz trilhas de auditoria na comunicação de conhecimentos e dados.	93% (113)	7% (8)	6% (8)	6% (8)
2.9 A adoção de nuvem privada de fácil acesso fomentaria o aumento da integração no SISBIN.	91% (116)	9% (12)	1% (2)	5% (7)
2.10 A antecipação de fatos ao Presidente da República por meio da nuvem privada condiz um valor.	88% (105)	12% (14)	2% (3)	11% (15)
2.11 A nuvem privada capaz de automatizar o registro de conhecimentos fortalece o SISBIN.	93% (112)	7% (9)	2% (3)	2% (3)
2.12 O suporte tecnológico centralizado pela Abin no SISBIN gera continuidade na comunicação.	89% (91)	11% (11)	11% (3)	15% (13)

Tabela 1 – Questões sobre o processo de troca de informações de inteligência

Ainda de acordo com os respondentes, uma solução de nuvem privada fortalece o Sisbin (questões 2.9 e 2.11), permitindo gerar valor ao Presidente da República (questão 2.10) e ainda, eles reconhecem a percepção de liderança da Abin como importante na condução desse processo (questão 2.12).

4.2. Questionamentos baseadas na Lei de Informação

A Tabela 2 demonstra o resultado das questões relacionadas à LAI, tais como a informações sigilosas não classificadas, o uso da criptografia de estado e a importância dos postos de controle para tratamento das informações sigilosas.

Afirmativas avaliadas sobre a Lei de Acesso à Informação	Concordam	Discordam	Não opinaram	Não concordo/ Não discordo
3.1 A proteção no fluxo das informações sigilosas não classificadas, mesmo sem possuírem amparo legal previsto na LAI, são fundamentais.	98% (130)	2% (2)	2% (1)	3% (4)
3.2 As ferramentas utilizadas para a troca de conhecimentos sigilosos não classificados atendem as necessidades de agilidade atual.	47% (36)	53% (40)	25% (34)	20% (27)
3.3 O uso de criptografia de estado somente para informações classificadas conforme a LAI atende aos critérios de segurança no SISBIN.	51% (49)	49% (47)	9% (28)	20% (13)
3.4. a) A criação de postos de controle no tratamento das informações sigilosas potencializa o uso da nuvem privada, gerando agilidade.	85% (99)	15% (17)	5% (7)	10% (14)

Afirmativas avaliadas sobre a Lei de Acesso à Informação	Concordam	Discordam	Não opinaram	Não concordo/ Não discordo
3.4 b) A criação de postos de controle no tratamento das informações sigilosas potencializa o uso da nuvem privada, gerando segurança.	83% (88)	17% (18)	6% (23)	17% (8)
3.4 c) A criação de postos de controle no tratamento das informações sigilosas potencializa o uso da nuvem privada, gerando oportunidade.	89% (104)	11% (13)	7% (7)	8% (15)

Tabela 2 – Questões relacionadas sobre a Lei de Acesso à Informação

Mesmo sem possuírem amparo legal previsto na LAI, a proteção no fluxo das informações sigilosas, não classificadas, se materializaram como fundamental para a maioria dos entrevistados no processo de segurança no fluxo de informações (questão 3.1). Importante ressaltar que as informações sigilosas, que não possuírem hipótese de sigilo fundamentada em lei, tem sua confidencialidade baseada no princípio da razoabilidade, gerando grande vulnerabilidade na divulgação da informação sensível, conforme o Art. 31 da LAI.

Merecendo igual destaque a informação sobre as ferramentas utilizadas para a troca de conhecimentos sigilosos não classificados, onde visualizam-se em grande parte um equilíbrio de opiniões (questões 3.2 e 3.3), fortalecendo a ideia da falta de sensibilização de usuários e formação de opinião. De forma semelhante, a questão sobre o aumento da sensibilização, habilitação e criação de postos de controle no tratamento das informações sigilosas foi apreciada como meio de potencializar o uso da nuvem privada, ratificando a importância desse modelo.

Também foi mensurada a importância da criação de postos de controle no tratamento de informações sigilosas, onde os resultados (questões 3.4 a, b e c) demonstraram que a maioria dos respondentes concordam que as fiscalizações do fluxo de informações promovem agilidade, segurança e oportunidade.

Os principais aspectos a serem discutidos relacionados a LAI neste trabalho, permitem avaliar como fundamental a previsão de amparo legal para proteger as informações sigilosas, conforme a Tabela 2 apresenta, e a adoção de tecnologias que garantam a segurança e proteção dos dados trafegados e armazenados, onde destaca-se os trabalhos dos autores Moreira *et al*(2021) e Dos Santos *et al*(2020) que possibilitam softwares de código aberto que podem ser implementados em testes como uma solução disponível.

4.3. Questionamentos inter-relacionados

A Tabela 3 apresenta perguntas inter-relacionadas sobre a nuvem privada, lei de acesso à informação (Brasil, 2011) e Norma Complementar Nr 14 - R01 - Segurança da Informação em Nuvem (Brasil, 2018). Os resultados confirmam que a manutenção do fluxo de troca de conhecimentos e dados entre os órgãos do sistema são fundamentais

ao assessoramento baseado em inteligência, (questão 4.1), e a liderança da Abin na condução do processo (questão 4.3). Também há concordância de que é necessário que a alta administração dos órgãos do Sisbin se aproprie da Gestão de Riscos de Segurança da Informação e Comunicações para definir o emprego da tecnologia da nuvem (questão 4.2).

Afirmativas avaliadas sobre questões inter-relacionadas	**Concordam**	**Discordam**	**Não opinaram**	**Não concordo/ Não discordo**
4.1) O fluxo de troca de conhecimentos e dados entre os órgãos do sistema são fundamentais ao assessoramento baseado em inteligência.	97% (131)	3% (2)	0% (0)	3% (4)
4.2) A alta administração deve considerar a Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) para usar a nuvem.	98% (129)	2% (2)	1% (1)	4% (5)
4.3) A Abin, como órgão central do Sisbin, deve ser a provedora da nuvem privada, baseando o servidor em área sob sua responsabilidade.	90% (104)	10% (11)	5% (15)	11% (17)

Tabela 3 – Questões inter-relacionadas

Esses pontos permitem uma análise em conjunto dos normativos já disponíveis e suas adequações necessárias no âmbito legal, assim como no campo tecnológico, favorecendo o assessoramento em alto nível por meio de uma ferramenta adequada. Uma síntese das perguntas consta na Figura 1.

4.4. Perguntas abertas

Os respondentes tiveram a possibilidade de opinar em duas questões abertas: na primeira, foi perguntado se os respondentes teriam sugestões quanto ao modelo de uso de nuvem privada na troca de informações de inteligência; e a segunda, com relação às sugestões que pudessem fortalecer o processo, a interação e a troca conhecimentos entre os órgãos do Sisbin. Foram recebidas 33 respostas para a primeira questão, e 23 para a segunda.

Quanto à primeira pergunta, a maioria dos respondentes, da amostra das 33 respostas, ressaltou que a nuvem privada é uma alternativa viável desde que sejam garantidas a segurança da informação. Além disso, foi reforçada a importância do cumprimento dos normativos brasileiros, como a LAI, a Instrução Normativa nº 5 (Brasil, 2021), e que caso sejam necessárias readequações essas sejam analisadas pelos órgãos competentes.

Outros aspectos também foram citados, tais como: mobilidade do pessoal de tecnologia de informação, auditoria, controle da difusão, capacidade da nuvem privada de se adaptar a novas tecnologias, gestão de riscos e o envolvimento da governança na adoção de nova tecnologia.

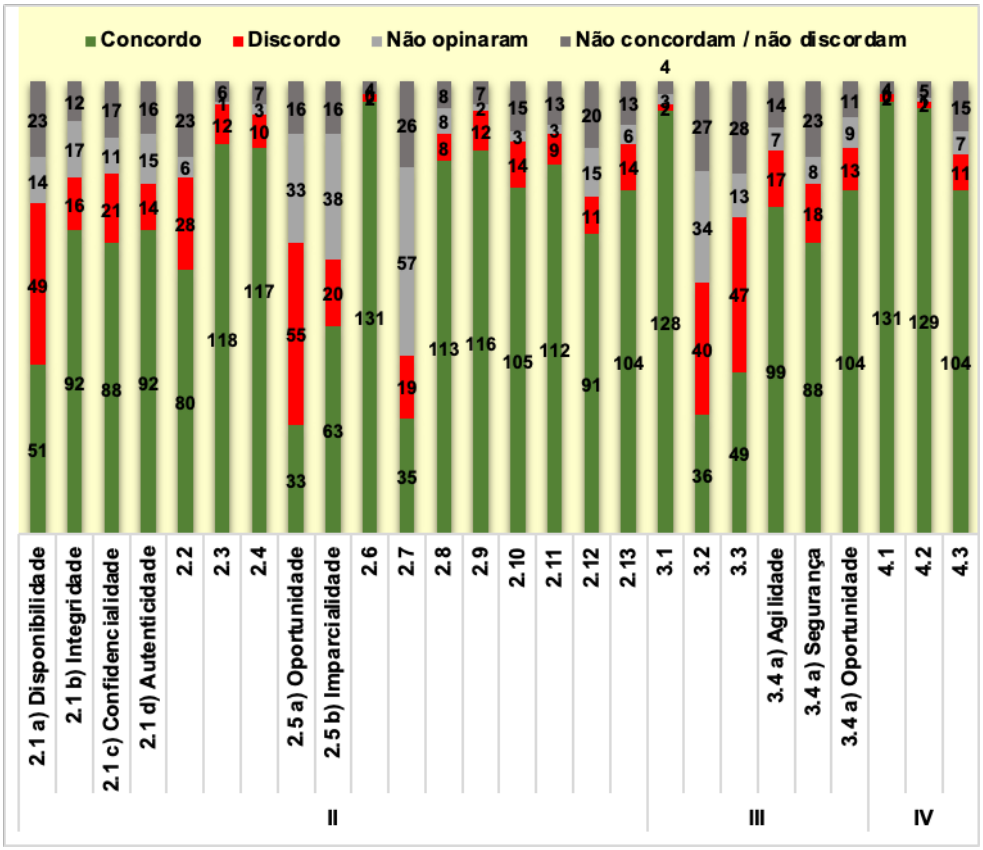


Figura 1 – Síntese das respostas

Quanto à segunda pergunta, destacou-se: o incentivo a adoção de novas ferramentas para fomentar a integração, a reformulação de legislações, importância do trabalho em conjunto, sensibilização entre os integrantes do sistema de inteligência, treinamento, formação de equipes integradas, nivelamento de conhecimentos no Sisbin, o credenciamento no acesso ao Sisbin e a constante necessidade de especialistas capacitados em tecnologia da informação.

As ideias apresentadas potencializam a adoção de uma ferramenta que possibilite trabalhos coordenados, criando embasamento para argumentos já estudados durante o desenvolvimento do trabalho, desde que a implementação da ferramenta tecnológica seja segura e possibilite a impulsão do processo de comunicação sigilosa não classificada de forma eficaz entre órgãos.

5. Conclusão

Este artigo teve por objetivo diagnosticar os desafios e oportunidades no processo de comunicação sigilosa não classificada entre os órgãos Sisbin. Em síntese, esse trabalho

indicou a necessidade de atualização de uma ferramenta para troca de informações entre os órgãos, com a possibilidade de realizar documentos, apreciações e estimativas de forma conjunta. Também trouxe a computação em nuvem privada como uma solução, fortalecendo critérios fundamentais de segurança cibernética, como os servidores estarem sob a guarda do órgão central do sistema, assim como o suporte tecnológico também ser fornecido Abin, como fatores de risco de grande impacto na segurança dos dados no ambiente da computação em nuvem.

A criação de uma fundamentação legal para tratar a informação sensível de inteligência foi apresentada como um desafio, pois atualmente não há previsões jurídicas objetivas na LAI que abordem essa questão.

O desenvolvimento de protocolos para fluxo de informações sigilosas não classificadas, o treinamento e formação de equipes integradas, com pontos focais dos órgãos integrados ao Departamento de Segurança da Informação também foram fortalecidas como oportunidades significativas no processo.

Em relação aos trabalhos futuros, uma série de soluções de *Software as a Service* (SaaS) e *Platform as a Service* (PaaS) podem ser estruturados e implantadas em órgãos do Sisbin que participem de uma mesma configuração ministerial, como por exemplo, o GSIPR e a Abin, possibilitando a implementação de testes e validações.

Por fim, o diagnóstico demonstrou a necessidade de uma tecnologia eficaz, onde a nuvem privada aparece como uma solução a ser estudada e implementada em trabalho futuro no âmbito do Sisbin.

Agradecimentos

Os autores agradecem o suporte da ABIN TED 08/2019. O autor Rafael Rabelo Nunes agradece o suporte do Centro Universitário Atenas e da Universidade de Brasília, por meio do Edital DPI/DPG 02/2022.

Referências

Alves, A. de A., Alves, C. A. de M., Tabosa, F. G. F., & Nunes, R. R. (2021). Riscos da computação em nuvem: estudo na ótica dos gestores de órgãos públicos federais no Brasil. *Navus - Revista de Gestão e Tecnologia*, 11, 01–18. doi: https://doi.org/10.22279/navus.2021.v11.p01-18.1513

Ahmed, I. (2019). A brief review: Security issues in cloud computing and their solutions. Telkomnika (Telecommunication Computing Electronics and Control), 17(6), 2812–2817.

Bardin, L., Cavignac, J., Lins, C., Maux, A., de Lima, I. B., de Souza, G. I. R., ... & Virginio, D. F. GIL, AC Métodos e técnicas de pesquisa social. São Paulo: Atlas, 2010. *Programação Geral*, 69.

Brasil (1999), Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - Abin, e dá outras providências. 7 dez. 1999. https://bit.ly/3wWb46L

Brasil (2011) Lei Nº 12.527 – Lei de Acesso a informação, De 18 De Novembro De 2011. https://bit.ly/3Q0fItk Brasil (2021) Instrução Normativa 5 de 30 de agosto de 2021 – Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal. Diário Oficial da União nº 165: seção 1, Brasília; DF p.2, 18 dez. 2021. https://bit.ly/3N1Eqrl

Brasil (2012) Coletânea 2012 – Atividade de Inteligência no Brasil. https://bit.ly/3avhzpG

Brasil (2016) Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. Diário Oficial da União nº 124: seção 1, Brasília; DF, p. 5, 30 jun. 2016. https://bit.ly/3z7GXMA

Brasil (2016) Doutrina Nacional de Inteligência: fundamentos doutrinários. Aprovada pela Portaria nº 244 – Abin/GSI/PR, de 23 de agosto de 2016. https://bit.ly/3GsDI3V

Brasil (2017) Decreto 4.376 de 15 de dezembro de 2017 – Institui a Estratégia Nacional de Inteligência. Diário Oficial da União nº 241: seção 1, Brasília; DF p.36, 18 dez. 2017. https://bit.ly/3NFWKG9

Brasil (2018) Norma Complementar 14/GSI/PR, de 13 de março de 2018. https://bit.ly/3z6F9n0

Clark, R. M. (2019). Intelligence analysis: a target-centric approach. CQ Press.

Cruz, A. (2020). Aprimoramento da Capacidade Analítica e Avanço na Atividade de Inteligência. *Revista Brasileira de Inteligência*, (15), 25-40. https://rbi.enap.gov.br/index.php/RBI/article/view/178

Dos Santos, D. M. L., Vale, K. M. A. C., & de Alencar, F. M. R. (2020). Avaliação de desempenho de nuvens privadas: um comparativo entre Owncloud, Nextcloud e Pydio. *Brazilian Journal of Development*, *6*, 40549-40566.

Ferreira, G. (2020). Perspectivas e desafios para o trabalho integrado em centros de inteligência. Monografia de fim de Curso de Aperfeiçoamento em Inteligência.

Gil, A. C. (2002). Como classificar as pesquisas. *Como elaborar projetos de pesquisa*, *4*(1), 44-45.

Gil, A. C. (2008). Métodos e Técnicas de Pesquisa Social. Escalas Sociais, *6*(1), 143-144.

IDG New, itforum. (2008). *Abin anuncia sistema de criptografia de dados para proteger Petrobras*. https://itforum.com.br/noticias/depois-de-seis-anos-nec-troca-a-presidencia-no-brasil/

International Organization for Standardization (2018). *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. Geneva. ISO

Minayo, M. C. D. S. (1996). Pesquisa Social: Teoria, Método e Criatividade. 6ª Edição. *Petrópolis: Editora Vozes*.

Moreira, C. V., Monteiro, R. M., de Caldas Filho, F. L., Lucas, M. C., de Oliveira Albuquerque, R., & de Sousa Júnior, R. T. (2021). Compartilhamento de arquivos em Home Office: uma solução de armazenamento de arquivos segura e altamente disponível em um ambiente de nuvem privada. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E42), 409-424.

Monteiro Feijó, A., Rodrigues Vicente, E. F., & Murilo Petri, S. (2020). O Uso Das Escalas Likert Nas Pesquisas De Contabilidade. The Use of Likert Scales in Accounting Resreangelearch., 13(1), 27–41. doi: https://doi.org/10.22277/rgo.v13i1.5112

Sen, A. K., & Tiwari, P. K. (2017). Security issues and solutions in cloud computing. *IOSR Journal of Computer Engineering*, 19(2), 67-72.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 05/12/2021
Aceitação/Acceptance: 19/02/2022

Proceso de desarrollo de vehículos de superficie no tripulados en instituciones Navales Colombianas

José María Riola[1], Shamir Sánchez[1], Enrique Sierra[1], Carlos Hernán Fajardo-Toro[2]

Chema.riola@rga-psi.es; shasp1111@gmail.com; enriquesb1@gmail.com; carlosh.fajardo@esap.edu.co

[1] Escuela Naval de Cadetes "Almirante Padilla", Barrio el Bosque - Isla Manzanillo, 130001, Cartagena, Colombia.

[2] Escuela Superior de Administración Pública - ESAP, 760046, Cali, Colombia

Pages: 184-196

Resumen: En la última década, la Armada de Colombia (ARC) ha estado llevando a cabo diversos programas de I+D+i para desarrollar tecnologías en torno a los vehículos de superficie sin tripular (USV). La razón de estos desarrollos es la necesidad de tener operativas estas plataformas navales para hacer operaciones de vigilancia, salvamento, operaciones de infantería de marina, tareas ISTAR, escuchas con sónares remolcados, contra la piratería, relé de comunicaciones, etc. El uso de estos vehículos permitirá una mayor capacidad y un menor coste al poder realizar las tareas que actualmente lo están haciendo buques de mucho mayor tamaño. Objetivos como el control de la plataforma, sus comunicaciones, el posicionamiento dinámico, la navegación en enjambres, desarrollo de formas de cascos no convencionales, planificación de misiones, evitar colisiones y obstáculos, mejora en los sistemas de recogida y lanzamiento, interoperabilidad, optimización de la propulsión, mayor autonomía o desarrollo de sensórica son ejemplos de algunos de los programas de I+D necesarios para tener unos USV para plena operatividad en la ARC.

Palabras-clave: USV; I+D; Control; Hidrodinámica; Comunicaciones.

ARC R&D on Unmanned Surface Vehicles

Abstract: In the last decade, the Colombian Navy (ARC) has been carrying out some R&D programs to develop technologies around unmanned surface vehicles (USV). The reasons for these developments are the need to have these naval platforms operational to carry out surveillance operations, rescue operations, marine infantry operations, ISTAR tasks, towed sonars, anti-piracy, communications relay, etc. The use of these vehicles will allow a greater capacity and a lower cost by being able to carry out the tasks that are currently being carried out by longer ships. Objectives such as platform control, communications relay, dynamic positioning, swarm navigation, development of unconventional hull shapes, mission planning, collision and obstacle avoidance, improved pickup and launch systems, interoperability, propulsion, optimization greater autonomy or sensors development are examples of some R+D necessary projects to have USVs fully operational into the ARC.

Keywords: USV; R&D; control; hydrodynamics; communications.

1. Introducción

El desarrollo de los USVs y su avance tecnológico han experimentado una notable transformación en las últimas dos décadas, con un incremento en el interés en el uso comercial de este tipo de embarcaciones sobre las convencionales o las totalmente tripuladas (Zhu et al., 2020a). Han pasado de ser considerados simplemente como un equipo pesado y costoso, a un instrumento viable para muchas aplicaciones científicas y comerciales (Munim, 2019; Zaghi et al., 2016), como la cartografía de los fondos marinos (Gil, 2021; Hsieh et al., 2022), la inspección de las infraestructuras o sus aplicaciones militares (US DEPARMENT OF DEFENSE, 2016)(Langebrake et al., n.d.) así como también en muchos desarrollos encaminados hacia la seguridad marítima como evitar colisiones (Murray & Perera, 2021; Shaobo et al., 2020; Zhang et al., 2021) Esto se ha debido fundamentalmente a las capacidades computacionales, desarrollos de sensores, aumento de su autonomía e inteligencia que han favorecido su capacidad de atender las necesidades de las misiones requeridas (Im et al., 2018; Lee et al., 2020; Zhu et al., 2020b)

La necesaria adaptación de la ARC a posibles circunstancias imprevistas es necesariamente un elemento para considerar, en especial cuando se habla de seguridad y defensa. Y con esta idea, los vehículos de superficie no tripulados (USV) tienen mucho que aportar; pueden ir más lejos, más rápidos o asumir más riesgos, lo que les hace imprescindibles en los buques de las próximas décadas (Munim, 2019). De hecho, El Plan 2042 de la Armada Colombiana expresa (ARC, 2021): "la necesidad de aparición de barcos totalmente automatizados, que no necesitan tripulación humana a bordo, y cuyo control se realiza de forma remota en tierra". Actualmente, la mayoría de las tecnologías asociadas a estos vehículos se desarrollan en el campo civil, dadas las necesidades de tener vigilancia en las infraestructuras críticas, estructuras sobre el fondo, plataformas offshore, tuberías de gas, cables eléctricos, cables de fibra óptica, etc.

Este trabajo presentará el prototipo de un USV construidos por la Armada Colombiana como parte de un proyecto de I+D desarrollado en la Escuela Naval Almirante Padilla-ENAP, mostrando los elementos a tener en cuenta en la construcción, así como los conceptos y ecuaciones requeridas y aplicadas en lo referente a control, hidrodinámica y estabilidad, para relacionarlo finalmente con lo que ha sido el proceso de I+D para su construcción.

2. Elementos para la construcción de USVs

Dependiendo de las aplicaciones y funcionalidades que se persiguen, los USV pueden tener una apariencia muy diferente. Sin embargo, se puede concretar (Liu, 2018), en la figura 1, cuales son los elementos básicos que suelen incluirse en un USV:

- Casco y sus apéndices
- Sistema de propulsión
- Sistema de guiado, navegación y control
- Sistema de comunicaciones

– Sistema de recogida de datos
– Estación en tierra

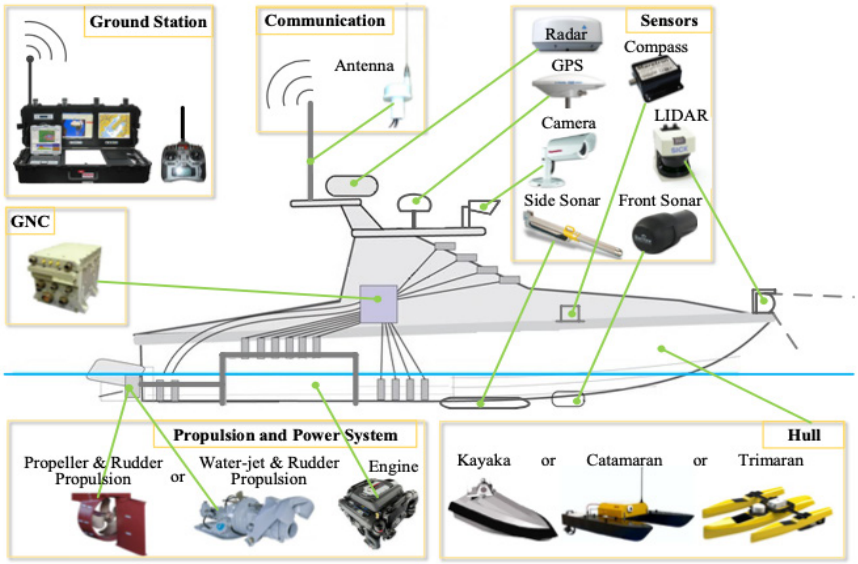


Figura 1 – Arquitectura naval de un USV. (Fuente: Liu et al)

Las principales zonas de operación que se prevén en una primera etapa de funcionamiento de los prototipos desarrollados en la Escuela Naval Almirante Padilla - ENAP (figura 2), quedan limitadas a la costa así como aguas interiores por lo que su eslora no necesita tener más de 2 metros ni calificar su comportamiento ante elevadas alturas significativas de ola.

De ello, se desprende la utilización de un sistema de propulsión mediante hidrojets, evitando así cualquier apéndice por debajo del casco que pudiese interferir con el fondo o que pudiera ver su operación diezmada por interferencia con objetos en suspensión. Por lo tanto, con codillos y exento de apéndices, el contacto del dron con el agua se limita a la superficie mojada de sus formas. Estas formas están optimizadas hidrodinámicamente para operar en un rango de operación de entre 5 y 25 nudos.

Así, desde el punto de vista de la plataforma, el requerimiento más crítico es la velocidad, pudiendo llegar a valores más altos, aunque si se pretenden alcanzar los 40 o 45 nudos, se debe tener en cuenta desarrollos previos para evitar el fenómeno de la cavitación (González-Adalid, 2005).

El sistema propulsivo de la embarcación son dos waterjets instalados en el espejo de popa, alimentados mediante un rack de baterías. La elección de los waterjets viene dada, casi de manera obligatoria, por el entorno en el que va a operar el USV, donde además la presencia de objetos en suspensión suele ser mayor que en zonas más profundas. Ambas características de entorno (González, 2019) supondrían un problema para una propulsión convencional mediante hélice. Además, al no contar el casco con ningún

apéndice por debajo del fondo, operarlo en zonas como pantalanes o ríos resulta más sencillo, al igual que su estiba. La geometría típica del waterjet se muestra en la siguiente figura 3:



Figura 2 – Bote “Sábalo”. (Fuente: ENAP)

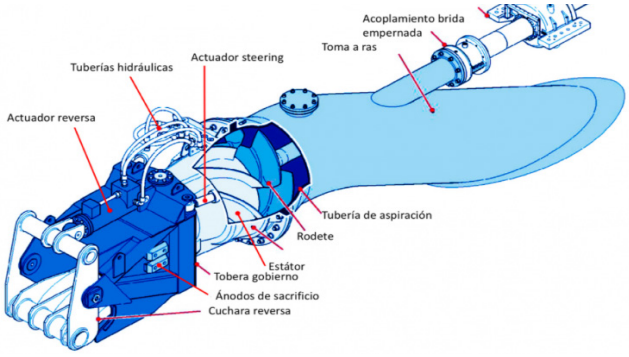


Figura 3 – Esquema de waterjet comercial. (Fuente: González, 2019)

La turbo-bomba es el elemento más crítico del waterjet y transmite la potencia del motor al fluido. Su funcionamiento se basa en la ecuación de Euler que expresa los cambios de las diferentes componentes de la velocidad del fluido al atravesar y hacer girar el rodete con álabes que crean una diferencia de presiones en ambas caras de los mismos. A nivel estructural, el prototipo no presenta una gran complicación, y podría ser definido como un casco de fibra de vidrio vacío, sin ningún tipo de refuerzo interno a lo largo de toda su estructura. Como dificultad añadida, mencionar que no existe dentro de las normativas de las Sociedades de Clasificación un conjunto de normas o reglas que guíen en cálculo de los escantillones de estructuras de este tipo.

3. Hidrodinámica y control

Desde el punto de vista hidrodinámico, para definir el casco de un USV, se utilizaron las ecuaciones propuestas por Gutiérrez et al (2014), que presenta f y M como las variables

de fuerza y momento de un sólido rígido en movimiento en un fluido sin fricción, considerando sus velocidades lineal y angular respecto a un sistema inercial y en el que T representa su energía cinética. Las ecuaciones que presentan la dinámica del USV presentadas en forma vectorial:

$$\boldsymbol{f} = \frac{\boldsymbol{d}}{\boldsymbol{dt}} \frac{\boldsymbol{\partial T}}{\boldsymbol{\partial v}} + \boldsymbol{w} \frac{\boldsymbol{\partial T}}{\boldsymbol{\partial w}}$$

$$M = \frac{d}{dt} \frac{\partial T}{\partial w} + w \frac{\partial T}{\partial w} + v \frac{\partial T}{\partial v}$$

Donde la energía cinética se representa como:

$$T(v, w) = \frac{1}{2} v^I M v$$

Y las ecuaciones de la dinámica son:

$$M v + C(v) v = \tau$$

Donde, de acuerdo con Fossen (2002), M puede ser presentada como una matriz simétrica y C incluye las aceleraciones centrípetas y de Coriolis. Puede escribirse como una matriz asimétrica con su centro de referencia en el centro de gravedad del USV, considerando su masa e inercia respecto a su centro de gravedad:

$$M = \left[\begin{bmatrix} mI_{3x3} & 0_{3x3} \\ 0_{3x3} & J_g \end{bmatrix} \right]$$

Al comenzar a navegar el USV se presentan varias olas a lo largo de su eslora, cuyo número va disminuyendo a medida que aumenta su velocidad. Y al llegar esta a un determinado valor, fácilmente relacionada con el número de Froude, la ola tendrá suficiente energía para que su longitud sea igual a la eslora de flotación del barco (Riola et al, 2017) . En este momento la dinámica del USV hace que la popa se asiente sobre esa ola, ayudada por el nacimiento de la ola de popa y que, debido a la combinación de ambas olas, no le permite subirla o dejarla atrás. Si se trata de aumentar la velocidad para salirse de esa ola, se refuerza este efecto sin conseguir un efecto favorable. La velocidad teórica máxima suele expresarse en función de la aceleración de la gravedad y la eslora en la flotación mediante la fórmula:

$$v_{max} = \sqrt{\frac{g\, L_{flot}}{2\pi}}$$

Básicamente, el control del USV se compone de 3 sistemas complementarios, los de guiado, navegación y control. El sistema de guiado proporciona de modo continuo al sistema de

control las referencias necesarias para poder realizar una determinada ruta, teniendo en cuenta las características de maniobrabilidad y limitaciones del bote. Este sistema recibe la información del sistema de navegación y de las variables influyentes como deriva, oleaje, datos de geolocalización, puntos de referencia, etc. El sistema de control, a su vez, también suele estar formado por 3 subsistemas, un controlador central, el observador del estado en cada momento y el sistema de distribución de fuerzas en los actuadores.

El piloto automático se encarga de conseguir definir la ruta establecida en un plano y de dar las señales de control a los hidrojets orientables para conseguir tanto el rumbo como las revoluciones del motor que ofrecen la velocidad que se necesita. Así, los pilotos automáticos controlan el rumbo del USV, debe cambiar el ángulo del vector de velocidad se le ordena mantener, o para alcanzar unos puntos de referencia o seguir una determinada ruta y además, lograr la velocidad adecuada para llegar en el momento adecuado, según la conveniencia de la operación.

El autopiloto debe seguir sus trayectorias basándose en puntos de referencia y utilizar la estrategia de guiado de línea de visión o desarrollar controladores no lineales multi-variables para la posición y así realizar un seguimiento de la trayectoria prefijada como entrada al sistema, empleando modelos de maniobra no lineales. Se necesita saber en cada instante la localización y orientación del USV, por lo que para la navegación se necesita la captura de datos con los doppler sonar, los girocompases ópticos o los sistemas de medida inercial.

Los primeros pasos de control se realizan con los PID que suelen tener sensores que reportan rumbo, velocidad y aceleración, incluyen el observador de estado, el filtro de movimiento inducido por el oleaje y la retroalimentación de rumbo mientras el viento funciona como mecanismo de adaptación al medio. Además, suelen tener una acción proporcional a la aceleración del ángulo de rumbo para aumentar la inercia del vehículo y minimizar las perturbaciones. Mencionar además del obligado Fossen (2002) con sus modelos no lineales, a Girón et al (2010, 2011) con sus métodos iterativos para una disminución de los movimientos y aceleraciones en el USV (figura 4) y a Velasco et al (2010) que trabajan la hidrodinámica de UUV y USV y en el control de evitación de obstáculos para su aplicación en la academia.

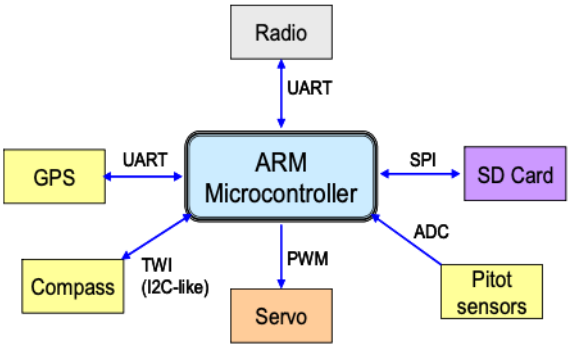


Figura 4 – Subsistemas hardware e interfaces. (Fuente: Girón 2010, 2011)

Las operaciones autónomas de USVs por períodos prolongados precisa de interfaces de comunicación avanzadas, basadas en la módems acústicos y enlaces con satélites, para evitar las limitaciones del procesamiento de gran cantidad de datos. El control en tierra sirve para la monitorización remota y planificación de operaciones.

4. Estabilidad

Un aspecto crítico en estos buques es su estabilidad, ya que debido a su pequeño francobordo suelen acumular cierta cantidad de agua en su cubierta durante sus operaciones. Para el cálculo de su altura metacéntrica (GM) (figura 5), se procedió al traslado del bote hasta una pesa industrial, en la que se le realizó un pesaje al buque con el fin de obtener su desplazamiento Δ, y con el que se tendrá un elemento movible de peso P para la realización de una prueba de traslado de pesos. El procedimiento consiste en comprobar el equilibrio y simetría del USV para posteriormente trasladar el peso movible a un costado, una distancia d y registrar el ángulo de escora θ que coge el USV tras dicho traslado de peso. El procedimiento se repite hasta su confirmación.

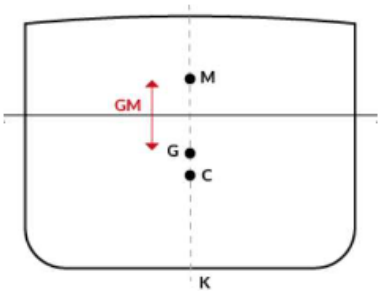


Figura 5 – Centros de referencia en los cálculos. (Fuente: Elaboración propia)

Después de realizada la prueba de estabilidad en el buque con lo que se procede a realizar los cálculos de la altura metacéntrica:

$$GM = \frac{P\ d}{\Delta\ tg\theta}$$

Para posteriormente pasar a calcular el brazo adrizante (figura 6), que para pequeños ángulos se utiliza la fórmula:

$$GZ = GM\ sen\ \theta$$

Se procedió al cálculo de los valores de los brazos adrizantes hasta 10º, dado que es lo máximo que se suele aplicar, con un error asumible, mediante la simplificación de tomar el valor de la tangente del ángulo por el del propio ángulo. La gráfica de la figura 7 presenta los valores de brazos adrizantes GZ:

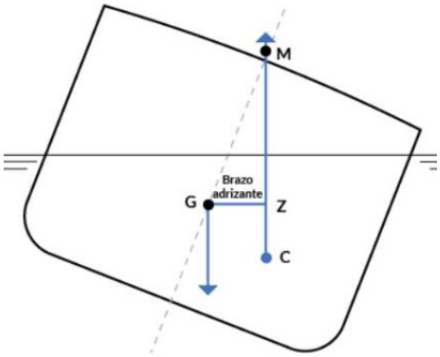


Figura 6 – Brazo adrizante. (Fuente: Elaboración propia)

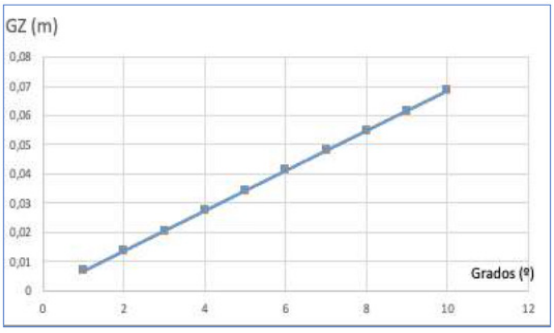


Figura 7 – Brazos adrizantes. (Fuente: Elaboración propia)

5. Programas de I+D

Ejemplos del interés de la ARC y del Ministerio de Ciencia, Tecnología e Innovación (Minciencias) en esta tecnología, son los programas de I+D llevados a cabo a través de los programas Francisco José de Caldas como: "Desarrollo del sistema de control de navegación de los vehículos de superficie no tripulados "SABALO" para su implementación en operaciones de patrullaje marítimo y fluvial" en el año 2018 y el proyecto "Desarrollo de un demostrador de tecnología (TRL5) para el vehículo de superficie no tripulado para la Plataforma Estratégica de Superficie (PES), enfocado en el sistema de comunicaciones y su integración con el control de navegación desarrollado por la ENAP para su futura implementación en el USV de la PES" en el año 2019.

Este segundo proyecto (figura 9), se enfoca en el sistema de comunicaciones y su integración con el control de navegación desarrollado por la ENAP. Actualmente, el sistema contiene la red táctica naval LINK-CO y un sistema de comunicaciones encriptadas que permite la transmisión de datos e información desde diferentes plataformas a la red con el fin de crear un panorama táctico común que permita realizar las operaciones de una manera más eficiente.



Figura 8 – USV "Sábalo" en pruebas. (Fuente: Propia)

Estos programas cuentan con amplios desarrollos académicos, mediante los cuales se adquieren capacidades de vehículos no tripulados de superficie, y difundir el conocimiento en el sector de investigación nacional. Un ejemplo de evidencias de lo desarrollado se presenta en la figura 9 con el esquema electrónico general de USV.

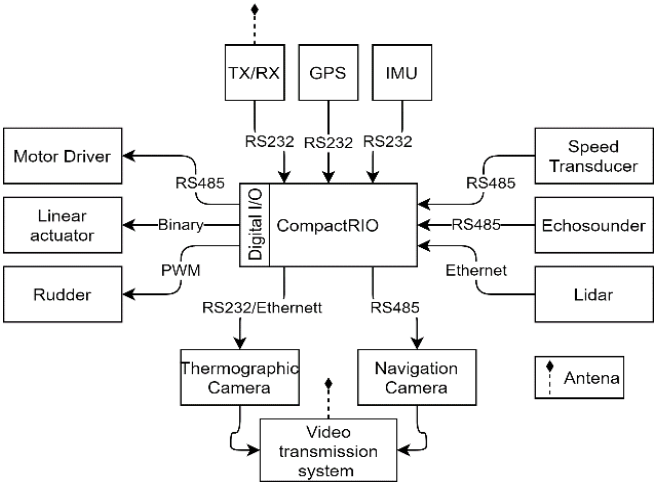


Figura 9 – Esquema general del "Sábalo". (Fuente: Propia)

El siguiente paso a seguir se asocia al desarrollo de algoritmos que permitan evitar obstáculos durante su navegación, teniendo como referencia a lo publicado por Revestido et al, (2017). La complicación se debe a que un planificador de rutas en escenarios con obstáculos puede resultar demasiado lento si estos tienen mucha presencia. Si además, se le suman las restricciones cinemáticas y dinámicas el problema se vuelve complejo, fundamentalmente a que los obstáculos pueden estar cambiando su posición con mayor o menor velocidad, se necesita una rápida y continua adaptación de las trayectoria previamente calculadas.

También se está diseñando y planeando llevar a cabo programas de I+D para el desarrollo de nuevos sistemas de generación y almacenamiento de energía que proporcionen una mayor autonomía de los USV. Se pretende reducir el coste del ciclo de vida (Fernández-Jove et al, 2019) y conseguir una mayor disponibilidad del combustible, lo que lleva a una mayor disponibilidad. Así, la tecnología del hidrógeno es considerada una de las más prometedoras para los USV (ABS, 2021), principalmente basada en pilas de combustible; estas presentan ventajas como la no utilización de piezas móviles, bajo nivel de ruido y vibraciones y bajas emisiones.

El uso del hidrógeno, y sus derivados como el amoniaco, tienen una mayor probabilidad de ser usado en los grandes buques al necesitar un menor volumen de almacenamiento, lo que implica importantes beneficios ambientales y económicos, una vez que se han reducido sus costes de producción, almacenamiento, transporte, distribución y uso (figura 10).

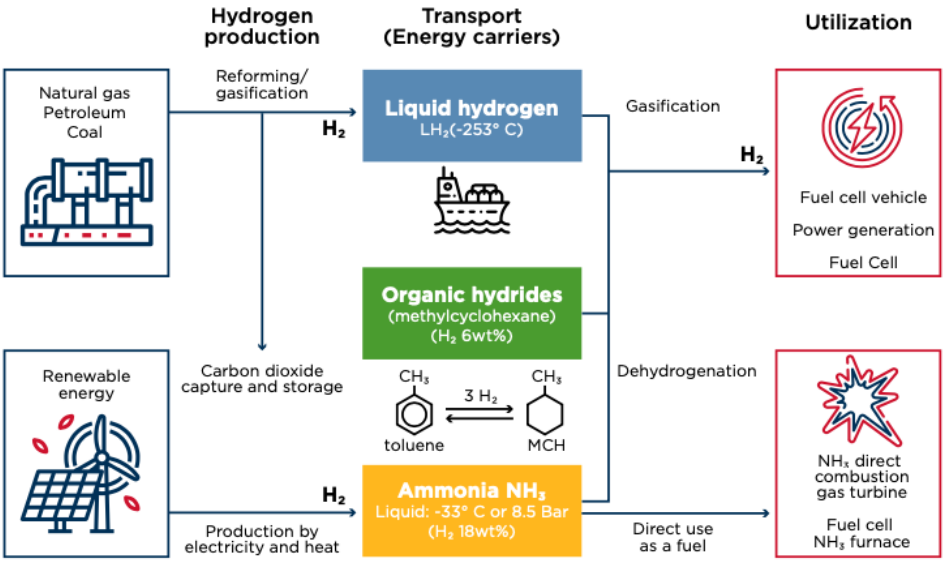


Figura 10 – Producción y uso del hidrógeno y del amoniaco. (Fuente: ABS)

El hidrógeno tiene una mayor energía específica que otro tipo de baterias y produce mayores niveles de potencia para los USVs, y además ofrece la ventaja de su mayor disponibilidad debido al elevado tiempo que se tarda en la carga de las baterías. De los tipos de celdas de combustible de hidrógeno se han identificado las pilas de combustible alcalinas (AFCs) y las celdas de combustible de membrana de electrolito polimérico (PEMFCs) y se ha evaluado su eficiencia y la necesidad de oxígeno puro para su funcionamiento. La pila de combustible deberá ser monitorizada y controlada para su optimización energética.

6. Conclusiones

Se evidencia la importancia en inversión en I+D, en especial por las instituciones relacionadas con la seguridad nacional, preferiblemente en colaboración con la industria y la academia, para así lograr el desarrollo de tecnologías y productos propios, lo que permite tanto la apropiación y desarrollo de capacidades tecnológicas, así como ahorros y agregación de valor en el sistema industrial nacional.

Respecto al desarrollo, los prototipos USV "Sábalo" desarrollados presentan los requisitos de las necesidades de la ARC para operaciones fluviales y cerca de costa. Para operaciones en mar abierto se debe de diseñar unos cascos de mayores esloras y desplazamiento. Su rendimiento sigue mejorando con los diferentes proyectos de I+D+i en marcha. ENAP y COTECMAR tienen una fuerte alianza para continuar en esta línea de investigación.

El desarrollo de las tecnologías en desarrollo permitirá que los USV tenga una mayor autonomía, reconocimiento automático de objetivos, prevención de obstáculos y colisiones, mayor carga útil y mejoras hidrodinámicas, lo cual contribuirá llevara cab desde operaciones científicas hasta de seguridad y vigilancia.

Por otra parte, y dentro del trabajo desarrollado, se puede afirmar que el hidrógeno parece ser el combustible perfecto para este tipo de buques. Y el hecho de que su uso como vector energético reduce las emisiones de sustancias contaminantes, presenta una solución correcta a la propulsión de las USV en zonas de alto valor medioambiental.

Referencias

ABS. (2021). Hydrogen as marine fuel. American Bureau of Shipping.

ARC. (2021). Plan 2042. Armada de la República de Colombia. www.armada.mil.co Recuperado el 24 de febrero del 2022.

Fernández-Jove, A., McKinlay, A. & Riola, J.M. (2019). Optimization of the Life Cycle in the warships: maintenance plan and monitoring for cost reduction. Proceeding of the International Ship Design & Naval Engineering Congress (CIDIN) and XXVI Pan-American Congress of Naval Engineering, Maritime Transportation and Port Engineering (COPINAVAL). Singapore: Springer.

Fossen, T. (2002). Marine Control Systems Guidance, Navigation and Control of Ships, Rigs and Underwater Vehicles. Marine Cybernetics AS, Trondheim, Noruega.

Gil, M. (2021). A concept of critical safety area applicable for an obstacle-avoidance process for manned and autonomous ships. Reliability Engineering and System Safety, 214. https://doi.org/10.1016/j.ress.2021.107806

Girón, J.M. (2010). Developing an Autonomous Surface Ship for Sea Demining: First Steps. IFAC Proceedings Volumes. https://doi.org/10.3182/20100915-3-DE-3008.00008

Girón, J.M., Recas, J., Esteban, S. (2011). Iterative method based on cfd data for the assessment of seakeeping control effects, considering amplitude and rate saturation. International Journal of Robust and Nonlinear Control, vol. 21, nº 13.

González, V. (2019). Diseño y selección de materiales para un USV de control medioambiental. Universidad Politécnica de Barcelona, España.

González-Adalid, J. (2005). Propeller cavitation. Escuela Técnica Superior de Ingenieros Navales. Universidad Politécnica de Madrid, España.

Gutiérrez, A., Ortega, J., Parra, V. & Pérez, Á. (2014). Circuitos eléctricos. Madrid: Universidad Nacional de Educación a Distancia, España.

Hsieh, T.-H., Li, B., Wang, S., & Liu, W. (2022). Application of Radar Image Fusion Method to Near-Field Sea Ice Warning for Autonomous Ships in the Polar Region. Journal of Marine Science and Engineering, 10(3), 421. https://doi.org/10.3390/jmse10030421

Im, I., Shin, D., & Jeong, J. (2018). Components for Smart Autonomous Ship Architecture Based on Intelligent Information Technology. Procedia Computer Science, 134, 91–98. https://doi.org/10.1016/j.procs.2018.07.148

Langebrake, L., Betzer, P., & Tripp, S. T. (n.d.). Autonomous Underwater Vehicle for Homeland Defense.

Lee, E. J., Ruy, W. S., & Seo, J. (2020). Application of reinforcement learning to fire suppression system of an autonomous ship in irregular waves. International Journal of Naval Architecture and Ocean Engineering, 12, 910–917. https://doi.org/10.1016/j.ijnaoe.2020.11.001

Munim, Z. H. (2019). Autonomous ships: a review, innovative applications and future maritime business models. In Supply Chain Forum (Vol. 20, Issue 4, pp. 266–279). Taylor and Francis Ltd. https://doi.org/10.1080/16258312.2019.1631714

Murray, B., & Perera, L. P. (2021). Proactive collision avoidance for autonomous ships: Leveraging machine learning to emulate situation awareness. IFAC-PapersOnLine, 54(16), 16–23. https://doi.org/10.1016/j.ifacol.2021.10.067

Revestido, E., Lastra, F., Velasco, F.J., Riola, J.M., Díaz, J.J. & Vega, L. (2021). Estimación de parámetros de un modelo de maniobra no lineal de un UUV teleoperado mediante ensayos en canal. XLII Jornadas de Automática. Castellón, España. https://doi.org/10.17979/spudc.9788497498043.001

Riola, J.M., Velasco, F. & Revestido, E. (2017). Estudio de maniobrabilidad de un UUV. Revista Derrotero. Escuela Naval Almirante Padilla, Cartagena de indias, Colombia.

Shaobo, W., Yingjun, Z., & Lianbo, L. (2020). A collision avoidance decision-making system for autonomous ship based on modified velocity obstacle method. Ocean Engineering, 215, 107910. https://doi.org/10.1016/j.oceaneng.2020.107910

US DEPARMENT OF DEFENSE. (2016). Report of the Defense Science Board Summer Study on AutonomyJune 2016.

Velasco, F.J., Revestido, E., López, E. & Moyano, E. (2010). Remote laboratory for marine vehicles experimentation. Computer Applications in Engineering Education. doi:10.1002/cae.20444.

Zaghi, S., Dubbioso, G., Broglia, R., & Muscari, R. (2016). Hydrodynamic Characterization of USV Vessels with Innovative SWATH Configuration for Coastal Monitoring and Low Environmental Impact. Transportation Research Procedia, 14, 1562–1570. https://doi.org/10.1016/j.trpro.2016.05.121

Zhang, X., Wang, C., Jiang, L., An, L., & Yang, R. (2021). Collision-avoidance navigation systems for Maritime Autonomous Surface Ships: A state of the art survey. In Ocean Engineering (Vol. 235). Elsevier Ltd. https://doi.org/10.1016/j.oceaneng.2021.109380

Zhu, M., Sun, W., Hahn, A., Wen, Y., Xiao, C., & Tao, W. (2020). Adaptive modeling of maritime autonomous surface ships with uncertainty using a weighted LS-SVR robust to outliers. Ocean Engineering, 200. https://doi.org/10.1016/j.oceaneng.2020.107053

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 02/10/2021
Aceitação/Acceptance: 12/01/2022

Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990 – 2021

Diego Edison Cabuya Padilla[1], Carlos Fabián Alvarado Carvajal[1], Ramiro Alfonso Carrascal Ortiz[1], Stefany Patricia Escandón Bernal[1], José María Riola[1], Carlos Hernán Fajardo-Toro[2,3].

diego.cabuya@enap.edu.co; carlos.alvarado@armada.mil.co; ramiro.carrascal@armada.mil.co; stefany.escandon@enap.edu.co; Chema.riola@rga-psi.es; carlosh.fajardo@esap.edu.co

[1,] Escuela Naval de Cadetes "Almirante Padilla", Barrio el Bosque - Isla Manzanillo, 130001, Cartagena, Colombia.

[2] Universidad el Bosque, 110121, Bogotá, Colombia

[2] Escuela Superior de Administración Pública - ESAP, Bogotá, Colombia

Pages: 197-210

Resumen: El artículo muestra los resultados del análisis bibliométrico del tema de ciberseguridad y ciberdefensa marítima, del periodo de 1990 a 2021, utilizando modelos estadísticos y cálculo de valores cuantificables en la producción y el consumo de información científica. La metodología consta de una fase que abarcó de la captura y procesamiento de datos utilizando el metabuscador Scopus y el software R, librería bibliometrix, y la segunda fase el análisis bibliométrico de la información recogida. Como resultado se presenta el análisis de diferentes indicadores bibliométricos como: línea de tiempo, localización, análisis de autores, acoplamiento bibliográfico, colaboración científica internacional, áreas de investigación y temática. Finalmente, la investigación presenta el estado actual de la actividad científica sobre ciberseguridad y ciberdefensa marítima.

Palabras-clave: Bibliometría; Bibliometrix; Ciberseguridad; Ciberdefensa; Marítimo; Naval.

Maritime cyberdefense and Cybersecurity: bibliometric analysis years 1990 – 2021

Abstract: The article shows the results of the bibliometric analysis of maritime cybersecurity and cyberdefense, from the period from 1990 to 2021, using statistical models and calculation of quantifiable values in the production and consumption of scientific information. The methodology consists in two phases, the first phase that included the capture and processing of data using the Scopus metasearch engine and the R software, bibliometrix library, and the second phase, the bibliometric analysis of the information collected. As a result, the analysis of different bibliometric indicators is presented, such as: timeline, location, analysis of authors, bibliographic coupling, international scientific collaboration, research and

theme areas. Finally, the research presents the current state of scientific activity on maritime cybersecurity and cyberdefense.

Keywords: Bibliometrics; Bibliometrix; Cybersecurity; Cyberdefense; Maritime; Naval.

1. Introducción

Cada vez que inicia una revolución industrial se afecta a gran velocidad la industria, la economía y la sociedad, aunque no siempre de manera fácil o directa, siendo un reto en sí mismo comprender la amplitud y celeridad de dicha revolución. En este sentido, muchas de las tecnologías que se plantearon años atrás están llegando a un punto de madurez en su desarrollo, en el que su implementación se aplica a las industrias, para mantener, igualar o superar las ventajas competitivas en cada uno de los sectores. La inteligencia artificial, la robótica, el internet de las cosas, la impresión 3D, la biotecnología, ciberseguridad y la computación en la nube son muestras claras de ello (Cabuya Padilla, 2018). En este sentido, la ciberseguridad se ha convertido en una preocupación particular en todas las organizaciones y entidades; ya que cada vez se almacena más información en el ciberespacio, aumentando así la propagación de eventos como fugas de información y ataques informáticos.

Es de interés para la comunidad científica abordar académicamente la ciberseguridad y ciberdefensa marítima al estar enfocadas en un sector que mueve más del 90% de la carga económica, además del fuerte componente tecnológico que lo enlaza con los demás sectores productivos (Cabuya Padilla, 2021; Conferencia de las Naciones Unidas sobre Comercio y Desarrollo - UNCTAD, 2020), lo que lo consolida como un sector vital para la economía global que debe ser protegido de las amenazas en el ciberespacio, teniendo en cuenta que los ciberataques a este sector han aumentado un 900% en los últimos 3 años (Alcaide & Llave, 2020; Cabuya Padilla, 2021; Hellenic Shipping News Worlwide, 2020). Los ataques dirigidos tanto a tecnologías de información como de operación son una de las principales preocupaciones del sector marítimo ya que pueden provocar pérdida de vidas, pérdida de control sobre los buques o los datos confidenciales, así como el secuestro de barcos y/o carga (Cabuya Padilla, 2021; Cabuya Padilla & Castaneda-marroquin, 2021; Mraković & Vojinović, 2019, pp. 132, 135–136). Adicionalmente, la investigación aportó al desarrollo del estado del arte de la investigación titulada "Marco de Referencia para el Modelamiento y Simulación de la Ciberdefensa Marítima a Nivel Estratégico – MARCIM" (Cabuya Padilla, 2021).

Así las cosas, el presente artículo muestra el panorama de la actividad científica alrededor de la ciberseguridad y ciberdefensa marítima, a través de un análisis bibliométrico con información extraída del metabuscador Scopus, procesando la información con el software R y la librería Bibliometrix. Se analizaron un total de 153 registros entre los años 1990 y 2021, analizando diferentes indicadores bibliométricos como: línea de tiempo, localización, análisis de autores, acoplamiento bibliográfico, colaboración científica internacional, áreas de investigación y temática. Finalmente, se presentan las principales conclusiones del proceso de investigación.

2. Metodología

Para el desarrollo de la investigación se establecieron dos fases. La primera que trató de la captura y procesamiento de datos utilizando el metabuscador Scopus y el software R (*Project for Statistical Computing*), con la librería Bibliometrix, siguiendo los siguientes pasos: definición de palabras clave y motor de búsqueda, captura de datos en Scopus y procesamiento de datos en R Project. La segunda fase abarca el análisis bibliométrico de la información recogida, utilizando diferentes indicadores bibliométricos como línea de tiempo, localización, análisis de autores, acoplamiento bibliográfico, colaboración científica internacional, áreas de investigación y temática. Finalmente, se presentan las principales conclusiones del proceso de investigación.

3. Captura y procesamiento de datos

3.1. Definición de palabras clave y sentencia de búsqueda

La definición de las palabras clave de búsqueda y sus diferentes combinaciones se da por la combinación de tres factores: experticia de los investigadores en el tema, pruebas sobre el metabuscador Scopus y consulta a expertos. El resultado de las palabras clave se presenta en la Tabla 1, la cual se depuró mediante pruebas de ensayo y error sobre Scopus para determinar resultados con palabras compuestas, variaciones ortográficas, eliminar los términos que no aportaban a la recuperación de información, así como aquellos que recuperaban resultados diferentes a lo requerido.

TEMÁTICA A	TEMÁTICA B
cyber security	maritime
cybersecurity	marine
cyber-security	sea
cyber defense	nautical
cyberdefense	naval
cyber-defense	navy
cyber defence	warship
cyberdefence	shipping
cyber-defence	ship
cyber	vessel
Information assurance	seafaring
Information security	seagoing
	ocean-going
	OMI IMO

Fuente: Elaboración propia.

Tabla 1 – Palabras clave.

Teniendo en cuenta la definición de palabras anterior, se estableció el siguiente motor de búsqueda para Scopus:

(TITLE (cyber OR cybersecurity OR {cyber security} OR "cyber-security" OR cyberdefense OR {cyber defense} OR "cyber-defense" OR cyberdefence OR {cyber defence} OR "cyber-defence" OR {information assurance} OR {information security}) AND TITLE (maritime OR marine OR sea OR seafaring OR seagoing OR "ocean-going" OR nautical OR naval OR navy OR warship OR shipping OR ship OR vessel OR "OMI" OR "IMO")

3.2. Captura de los Datos en SCOPUS

Con el motor de búsqueda definido, se procedió a capturar la información bibliográfica en el metabuscador Scopus, seleccionado por su calidad científica y número de fuentes de información. Web of Science es otro metabuscador reconocido de características similares a Scopus, que reúne información de múltiples bases de datos internacionales, pero difiere con el primero en que para Web of Science los indicadores como factor de impacto e índice h tienen una correlación de 0.17, mientras que para SCOPUS corresponden a 0.79, por lo cual es más útil para realizar análisis bibliométricos (Hernández-González et al., 2016).

La fecha de corte para la búsqueda se hizo el día 31 de diciembre de 2021. La fecha de inicio de la búsqueda se estableció en 1999, año en que se publica el documento más antiguo que arrojó SCOPUS con el motor de búsqueda utilizado, finalizando con los documentos del 2021 en donde se desarrolló el proceso de localización documental.

La descarga de los datos se realizó en formato .bib, acorde con la compatibilidad del formato de la herramienta tecnológica utilizada para el estudio Bibliométrico, que es R Project, con la librería Bibliometrix. El registro documental en SCOPUS se construyó con todas las variables de búsqueda disponibles como: Información de citación (Autores, Titulo del documento, Año, EID, Titulo de fuente, Tipo de documento, Etapa publicación, Recuento de citas), Información bibliográfica (Afiliación, Editor, Editorial, Identificador de serie, Lenguaje de documento), resumen y palabras claves, datos de información y otras.

3.3. Procesamiento de los Datos en R

Una vez realizada la captura de los datos se procedió a cargar el archivo generado en SCOPUS en el programa R, Project for Statistical Computing, implementando la librería Bibliometrix, la cual fue propuesta por sus autores (Aria & Cuccurullo, 2017, p. 959) como herramienta única de código abierto diseñada para el análisis exhaustivo del mundo científico en determinado tema, siendo una herramienta flexible y de fácil actualización, útil en una ciencia de constante cambio como la bibliometría. Utilizando los algoritmos de Bibliometrix se dio paso al análisis bibliométrico, que se presenta en el siguiente punto.

4. Resultados y Discusión

Se encontraron 120 registros para el tema de ciberseguridad y ciberdefensa marítima en la información recolectada en Scopus. Esta información fue procesada en R utilizando

la librería Bibliometrix, y a continuación se presentan los principales resultados del análisis bibliométrico:

4.1. Línea de Tiempo

Entre los años 1999 y 2021, de los 153 documentos existentes sobre Ciberseguridad y Ciberdefensa Marítima, 93 de ellos correspondientes al 60.78%, fueron escritos entre el año 2019 y el 2020 (Figura 1). Además, el porcentaje de crecimiento anual en promedio fue del 3.2%, observándose el limitado crecimiento e interés que el tema ha tenido en el campo científico en los primeros años, sin embargo, en los últimos años su crecimiento aumentó exponencialmente.

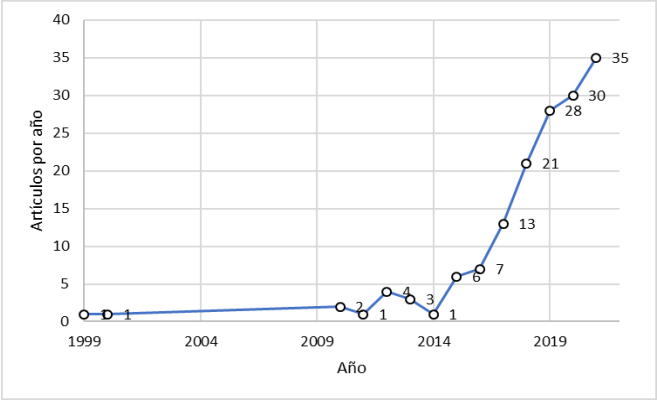


Figura 1 – Porcentaje de producción de documentos por año. Fuente: Elaboración propia.

4.2. Localización

El país más productivo en ciberseguridad y ciberdefensa marítima es China, con una producción de 13 artículos, seguido de Reino Unido con 9 publicaciones y de otros países como Estados Unidos y Noruega (Figura 2).

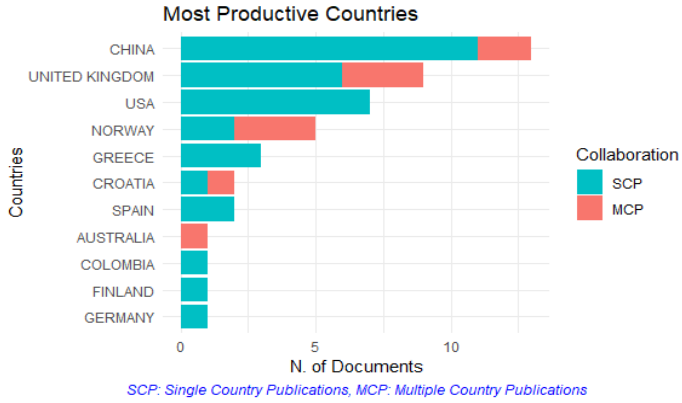


Figura 2 – Países más productivos. Fuente: Elaboración propia.

4.3. Autores

Se identificaron 315 autores del tema, con un promedio de 2,5 citas por documento y 760 palabras claves mostradas. Los 10 autores más productivos se muestran en la Figura 3.

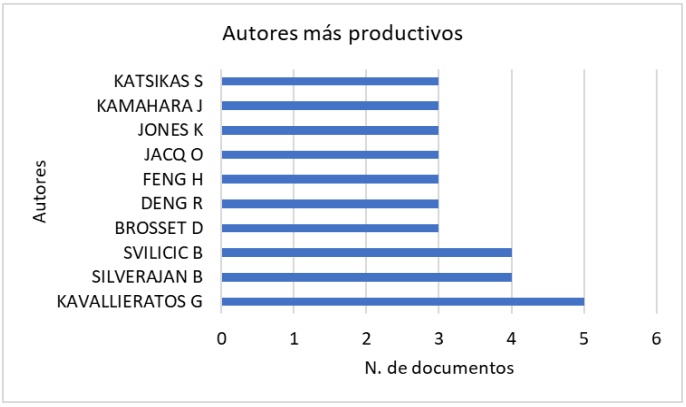


Figura 3 – Autores más productivos. Fuente: Elaboración propia.

Las principales revistas donde se están publicando los productos científicos del tema se relacionan en la Tabla 2, mostrando que las series de libros de ciencias de la computación son los que más contribuyen en el tema de investigación sobre Ciberseguridad y Ciberdefensa Marítima, en comparación con revistas, asambleas y conferencias.

Revista/Publicación	Ranking Scimago	Número de publicaciones
Lecture Notes in Computer Science	Q3	4
18th Annual General Assembly of the International Association Of Maritime Universities - Global Perspectives in Met: Towards Sustainable Green and Integrated Maritime Transport Iamu 2017	No aplica	2
Advances in Intelligent Systems and Computing	Q3	2
Automatic Control and Computer Sciences	Q3	2
Communications in Computer and Information Science	Q4	2
European Conference on Information Warfare and Security Eccws	No aplica	2
International Journal of Distributed Sensor Networks	Q2	2
Journal of Marine Science and Engineering	Q2	2
Journal of Navigation	Q2	2
Marine Technology Society Journal	Q3	2
Smart Innovation Systems and Technologies	Q4	2

Fuente: Elaboración propia.

Tabla 2 – Principales publicaciones académicas.

Ranking de dominancia de los autores

El factor de dominancia se refiere a la proporción que indica el número de artículos de varios autores en los que aparece un investigador como primer autor en las publicaciones respecto al número total de estas (Elango & Rajendran, 2012, p. 165). Para este análisis, Svilicic encabeza el nivel más alto de dominancia ya que de 4 artículos publicados aparece como primer autor en los mismos 4; el segundo es Tam ya que, de 3 artículos publicados, aparece en los 3 mismos como primer autor, al igual que Yang. Es de resaltar que Kavallieratos a pesar de tener un factor de dominancia de 0,8, es el autor que ha participado en el mayor número de publicaciones. Los demás autores pueden verse en la Tabla 3.

Autor	Factor de dominancia	Total de artículos	Un solo autor	Múltiples autores	Primer autor
Svilicic B	1	4	0	4	4
Tam K	1	3	0	3	3
Yang T	1	3	0	3	3
BolboT V	1	2	0	2	2
Brown C	1	2	0	2	2
Csorba MJ	1	2	1	1	1
Kavallieratos	0.8	5	0	5	4
Jacq O	0.66	3	0	3	2

Fuente: Elaboración propia.

Tabla 3 – Ranking de dominancia de los autores.

Índice h, g y m de los autores

El índice h es indicador de impacto que tienen las revistas y las publicaciones; en este índice se relacionan las publicaciones de una revista o autor con las citas que se han obtenido, es aquí donde un número h de publicaciones han recibido un número mínimo h de citas (Tuñez & De Pablos, 2013, p. 135).

Por otro lado, el índice g, calcula la productividad científica, la cual es determinada por medio del historial de publicaciones de los autores. Para obtener este cálculo, son listadas las publicaciones de un autor de forma descendente de acuerdo con el número de citas recibidas por cada uno de ellos, para posteriormente elevar este último número al cuadrado (Tuñez & De Pablos, 2013).

Por último, el índice m es calculado a través de la división h/n, donde n es el número de años de carrera como investigador, lo cual representa la mediana de las citas recibidas por el índice h (Gutiérrez-Salcedo et al., 2018, p. 4).

Para este caso en particular, se demostró que los autores con mayor índice h (3) son Kavallieratos, Svilicic y Kamahara; de la misma forma, se evidencia que los autores con mejor índice g (4) son Kavallieratos y Svilicic; por otra parte, los autores con mejor índice m son Svilicic y Kamahara (0.75), mostrando que estos últimos publican artículos más frecuentemente que los demás autores (Tabla 4).

Autor	Índice H	Índice G	Índice M
Kavallieratos	3	4	1
Silverajan B	1	2	0.25
Svilicic B	3	4	0.75
Brosset D	1	2	0.25
Deng R	1	2	0.16
Feng H	1	2	0.16
Jacq O	1	2	0.25
Jones K	2	3	0.50
Kamahara J	3	3	0.75
Katsikas S	2	3	0.66

Fuente: Elaboración propia.

Tabla 4 – Índice h, g y m de los primeros 10 autores.

Estimación del coeficiente de la ley de Lotka

La ley de Lotka describe la frecuencia de publicación de los autores en cualquier campo de estudio y en un determinado tiempo, evidenciando que la producción científica sobre el tema específico se concentra en cierto número de autores que publican y mantienen mayor producción científica en contraste con el número de autores que sostienen menos producción (Urbizagastegui, 1999, p. 126).

En el presente análisis, al aplicar la ley de Lotka (Figura 4), se observa que existen 261 autores que han publicado un solo artículo sobre el tema de ciberseguridad y ciberdefensa marítima, el total de autores que han escrito dos artículos son 40; tres artículos, 11; cuatro artículos, 2 y cinco artículos, 1. Al comparar la estimación teórica de la Ley de Lotka y el comportamiento de la muestra estudiada, se espera que no haya diferencias significativas entre las dos muestras.

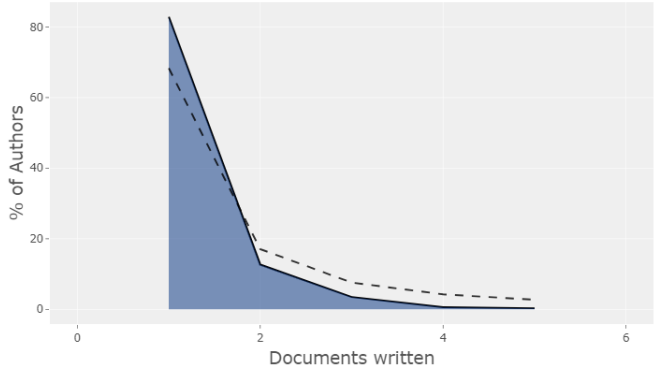


Figura 4 – Ley de Lotka. Fuente: Elaboración propia utilizando el software R.

El coeficiente Beta estimado es 3.50, constante 1.08 con una bondad de ajuste igual a 0.98. La prueba de dos muestras de Kolmogorov-Smirnoff proporciona un valor de p = 0.32, es decir, sí existe diferencia significativa entre las distribuciones observadas y teóricas (Figura 5).

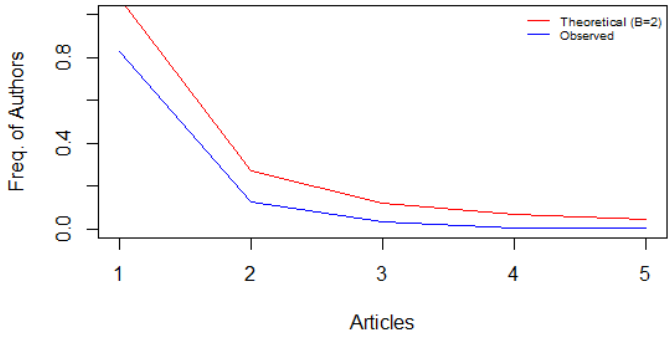


Figura 5 – Comparación de la beta teórica con la observada de las distribuciones Lotka.
Fuente: Elaboración propia utilizando el software R.

4.4.Acoplamiento bibliográfico

Para establecer la existencia de acoplamiento bibliográfico, al menos una fuente citada debe encontrarse en la lista de referencias de dos artículos más. La fuerza del acoplamiento de los dos artículos se calcula a partir del número de referencias compartidas en común por estos mismos, además de introducir el acoplamiento entre la co-cita, la co-ocurrencia de palabras clave y la cooperación entre países (Aria & Cuccurullo, 2017, p. 968), que se analizan a continuación:

Co-citas

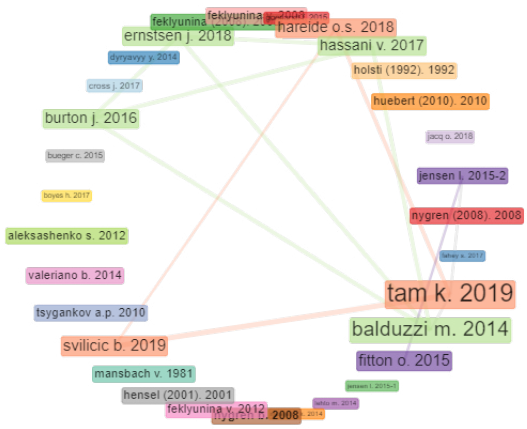


Figura 6 – Red de co-citación. Fuente: Elaboración propia utilizando el software R.

La red de co-citación se puede observar cuando dos artículos son citados en un tercer artículo (Aria & Cuccurullo, 2017). En la figura 6 se muestra el nodo de artículos de autores destacados, siendo para este caso los artículos de Tam (2019) y Balduzzi (2014), los que presentan un nodo más grande y están espacialmente más cerca entre sí, en comparación con otros artículos menos populares como los de Cross (2017) y Jacq (2018).

Co-ocurrencia de palabras clave

Se identifican cuatro conglomerados de nodos: el primero, encabezado por las palabras ciber seguridad y evaluación de riesgos, acompañado de otras palabras menos concurrentes como gestión de riesgos, seguridad de datos, industria marina, prevención de accidentes, percepción de riesgos, planes de estudios y producción de pozos de petróleo en alta mar; el segundo está encabezado por las palabras sistemas integrados y sistemas físicos cibernéticos, acompañado de palabras como ciber-sistema-físico (cps), gestión de la información, sistemas ciberfísicos (cpss), ingeniería de seguridad, entre otras; en el tercer nodo se encuentran palabras compuestas como barcos, organizaciones marítimas internacionales, automatización, inteligencia artificial, control de inteligencia, ciber amenazas, ciberataques, etc.; por último, en el cuarto nodo se hayan palabras como seguridad de la red, transporte fluvial, delincuencia, delitos informáticos, protocolos de red y seguridad marítima. Con lo anterior, se evidencia que uno de los nodos muestra cuál es el contexto de investigación más relevante en la Ciberseguridad y Ciberdefensa Marítima (nodo azul), mientras que el nodo color rojo, muestra el modo de estudio y aplicación de los conceptos, y los nodos de color morado y verde muestran temas emergentes en diferentes categorías para este tipo de investigaciones.

4.5. Colaboración Científica Internacional

Una red de colaboración científica es aquella que se estimula por medio de políticas de promoción de la investigación mediante la financiación y tienen como objetivo la cooperación internacional para generar producción científica (Carvalho et al., 2014, p. 225); esto permite identificar a los nodos como autores y a los enlaces como coautorías entre estos, si el nodo es de mayor tamaño, quiere decir que hay más cantidad de autores de ese país en coautoría con otros. En el caso del presente análisis, se evidencia que los países que más cooperación de coautorías tiene en relación con la Ciberseguridad y Ciberdefensa Marítima son Japón y Noruega, unidos con Croacia-Suecia y Chipre-Grecia respectivamente; así mismo, se destacan redes de colaboración como la que mantiene China con Canadá y por su parte, Reino Unido con Alemania.

4.6. Áreas de investigación

Las áreas de investigación que están relacionadas en torno a la Ciberseguridad y Ciberdefensa Marítima se identificaron a través de un análisis de correspondencias múltiples (ACM), el cual analiza la homogeneidad de la matriz de indicadores para obtener una representación euclidiana de baja dimensión de los datos originales (Abdi & Valentin, 2007, p. 1). En el presente caso, la figura 7 muestra 4 grandes campos de investigación al mapear las co-ocurrencias de palabras en la colección bibliográfica; en el campo rojo se observan investigaciones relacionadas con ciberseguridad, barcos, ciber

amenazas, navegación, sistemas de control, percepción de riesgo, control inteligente, entre otros; en el campo azul se muestran estudios de sistema físico cibernético, robótica, ingeniería de seguridad, gestión de la información, etc.; en el nodo verde se observan investigaciones relacionadas con seguridad marítima, análisis de riesgos, delincuencia, delitos informáticos e investigación industrial; por último, en el morado hay investigaciones orientadas a los sistema de seguridad y la criptografía.

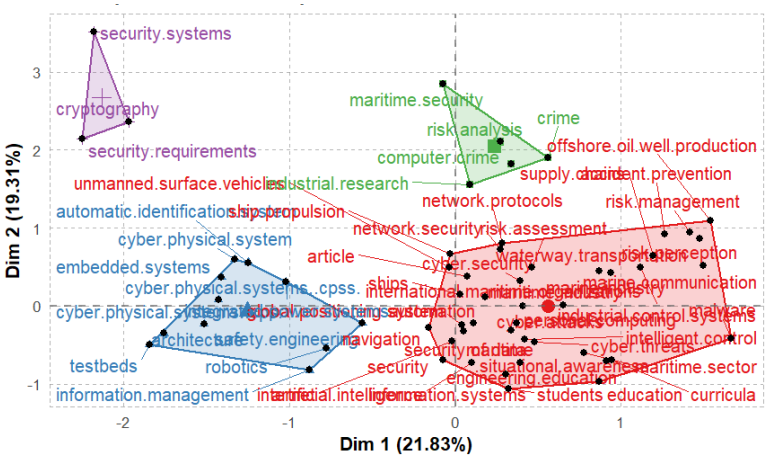


Figura 7 – Estructura conceptual del campo de estudio MCA.
Fuente: Elaboración propia utilizando el software R.

4.7. Temáticas

Finalmente, en la figura 8 se observa la estructura general de la tendencia temática a lo largo de los últimos años, la cual se centra en ciberseguridad, barcos, evaluación de riesgos, seguridad de redes, sistemas integrados, gestión de riesgos, delitos informáticos, sistemas de información, ingeniería de seguridad, entre otros.

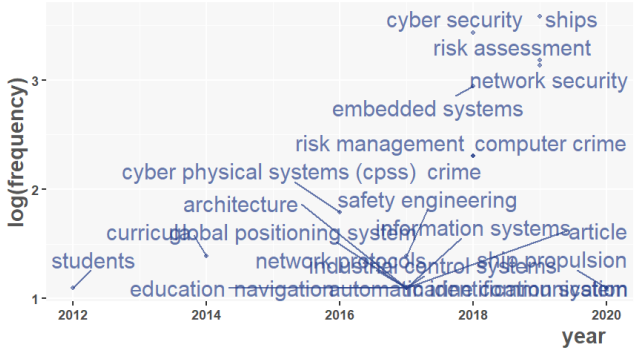


Figura 8 – Dendrograma temático. Fuente: Elaboración propia utilizando el software R.

La co-ocurrencia de palabras claves, el análisis de correspondencias múltiples y el dendrograma temático ilustra los principales temas en los que se han centrado la documentación científica sobre Ciberseguridad y Ciberdefensa Marítima, sobresaliendo las palabras: ciberseguridad, barcos, evaluación de riesgos, seguridad de redes, ciber amenazas y sistemas integrados; además se puede apreciar que la palabra ciberdefensa no aparece con frecuencia en los términos claves de los artículos publicados en SCOPUS, infiriendo que es una de las razones por la cual hay un bajo número de publicaciones científicas sobre el tema.

5. Conclusiones

La bibliometría arrojó un total de 153 documentos relacionados con el tema, escritos entre 1999 y 2021 con un porcentaje de crecimiento anual del 3.2%, que indica un limitado crecimiento e interés científico del tema a pesar de que en los últimos años su investigación va en aumento. El país más productivo en el tema es China, evidenciado en la producción de 13 artículos, seguido de Reino Unido (9) y de otros países como Estados Unidos (7) y Noruega (5). Los autores más productivos son Kavallieratos G., Silverajan B., Svilicic B., Brosset D. y Deng R; el más alto nivel de dominancia lo tienen Svilicic B., Tam K. y Yang T.; el mayor índice h es para Kavallieratos, Svilicic y Kamahara; el mejor índice g es para Kavallieratos y Svilicic; y el mejor índice m son Svilicic y Kamahara. Los países que más cooperación de coautorías tienen en relación con la ciberseguridad y ciberdefensa marítima son Reino Unido y Noruega, que están unidos hasta con tres países diferentes. También se destacan redes de colaboración como las que mantienen China con Canadá, Estados Unidos con Nueva Zelanda y Japón con Croacia y Suecia.

A través de un análisis de correspondencias múltiples (ACM) de las co-ocurrencias de palabras en la colección bibliográfica se establecieron cuatro áreas de investigación para la temática: la primera relacionada con criptografía y sistemas de seguridad de la información, la segunda relacionada con los sistemas de control industrial y sistemas ciberfísicos, la tercera relacionada con gestión de riesgos cibernéticos, seguridad marítima y crimen cibernético, y la cuarta relacionada con sistemas de control marítimo, ciencia de datos, actividades y conciencia marítima.

Se evidenció que la ciberdefensa no es una palabra muy mencionada en las publicaciones, por lo cual es interesante que se desarrollen un poco más la ciberdefensa en el campo académico. Estos análisis demuestran que el presente trabajo puede servir como complemento durante el desarrollo de nuevos estudios que aborden las áreas de investigación de Ciberseguridad y Ciberdefensa Marítima.

La colaboración es una particularidad que se repite también con los autores, quienes en la mayoría de sus investigaciones lo han aplicado. Esta contribución en la investigación académica de la Ciberseguridad y Ciberdefensa Marítima en materia de autores podría inferirse como una necesidad por la complejidad del tema y entre países su interés nacería por la afectación transnacional que presentan los ciberdelitos y ciberataques.

Las investigaciones en torno al tema de estudio crecen exponencialmente de acuerdo con el análisis realizado de la línea de tiempo, relacionándose como una respuesta al aumento significativo del uso del ciberespacio en el campo marítimo, siendo los libros

de ciencia de la computación, como el *Lecture notes in computer science,* en donde se ha desarrollado mayormente el tema en la academia.

Es importante continuar realizando investigaciones sobre el tema, por la relación con la integralidad de la seguridad de aquellas actividades globalizadas y digitalizadas realizadas en el mar. Al utilizar el ciberespacio en las actividades marítimas que explotan los Intereses Marítimos Nacionales, se convierte en una infraestructura estratégica a ser protegida a través del uso del Poder Naval, que utiliza la Ciberseguridad y Ciberdefensa como uno de sus instrumentos. En esa línea, esta investigación contribuye al conocimiento de la seguridad y la defensa marítima en el ciberespacio, creando conciencia para proteger y potencializar el Poder Marítimo en Colombia.

Para terminar, se recomienda replicar este estudio utilizando el Metabuscador *Web of Science* para contrastar los resultados y refinar las conclusiones sobre la actividad científica frente al tema.

Referencias

Abdi, H., & Valentin, D. (2007). Multiple correspondence analysis. In *Encyclopedia of measurement and statistics* (Vol. 2, Issue 4).

Alcaide, J. I., & Llave, R. G. (2020). Critical Infrastructures Cybersecurity and the Maritime Sector. *Transportation Research Procedia*, *45*, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959–975. https://doi.org/10.1016/j.joi.2017.08.007

Cabuya Padilla, D. E. (2018). Relación de la Industria 4.0 con la competitividad industrial. *Revista El Derrotero*, *12*, 143–174. https://www.escuelanaval.edu.co/es/file-download/download/public/4882#:~:text=Es la integración de las,y volver a la industria

Cabuya Padilla, D. E. (2021). *Marco de Referencia para el Modelamiento y Simulación de la Ciberdefensa Marítima a Nivel Estratégico - MARCIM [Tesis de doctorado no publicada]*. Escuela Naval de Cadetes "Almirante Padilla."

Cabuya Padilla, D. E., & Castaneda-marroquin, C. (2021). Maritime Cyberdefense Actors Taxonomy for Command and Control. *Smart Innovation Systems and Technologies*, *181*.

Carvalho, M. S., Travassos, C., & Coeli, C. M. (2014). Collaborative scientific research networks. *Cadernos de Saude Publica*, *30*(2), 225–227. https://doi.org/10.1590/0102-311XED010214

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo - UNCTAD. (2020). Review of Maritime Transport 2020. In *United Nations Conference on Trade and Development*. https://unctad.org/system/files/official-document/rmt2020_en.pdf

Elango, B., & Rajendran, P. (2012). Authorship trends and collaboration pattern in the marine sciences literature: a scientometric study. *International Journal of Information Dissemination and Technology*, *2*(3), 166–169.

Gutiérrez-Salcedo, M., Martínez, M. Á., Moral-Munoz, J. A., Herrera-Viedma, E., & Cobo, M. J. (2018). Some bibliometric procedures for analyzing and evaluating research fields. *Applied Intelligence*, *48*(5), 1275–1287. https://doi.org/10.1007/s10489-017-1105-y

Hellenic Shipping News Worlwide. (2020). *Maritime Cyber Attacks Increase By 900% In Three Years*. Marine Insight. https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/#

Hernández-González, V., Sans-Rosell, ;, Jové-Deltell, ;, & Reverter-Masia, &. (2016). Comparación entre Web of Science y Scopus, Estudio Bibliométrico de las Revistas de Anatomía y Morfología Comparison between Web of Science and Scopus, Bibliometric Study of Anatomy and Morphology Journals. In *Int. J. Morphol* (Vol. 34, Issue 4). http://ip-science.thomsonreuters.com

Mraković, I., & Vojinović, R. (2019). Maritime Cyber Security Analysis – How to Reduce Threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Tuñez, M., & De Pablos, J. (2013). El 'índice h' en las estrategias de visibilidad, posicionamiento y medición de impacto de artículos y revistas de investigación. *Actas Del 2º Congreso Nacional Sobre Metodología de La Investigación En Comunicación*, 133–150.

Urbizagastegui, R. (1999). La ley de Lotka y la literatura de bibliometría. *Investigación Bibliotecológica: Archivonomía, Bibliotecología e Información*, *13*(27), 125–141. https://doi.org/10.22201/iibi.0187358xp.1999.27.3913

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 17/10/2021
Aceitação/Acceptance: 05/01/2022

Modelo conceptual del Sistema del Poder Marítimo a nivel estratégico en Colombia

Diego Andrés Alba Rocha[1], Juan Ricardo Ortegón Vega[1], Diego Edison Cabuya Padilla[1], José María Riola[1], Carlos Hernán Fajardo-Toro[2].

diego.alba@armada.mil.co; juan.ortegon@enap.edu.co; diego.cabuya@enap.edu.co; Chema.riola@rga-psi.es; carlosh.fajardo@esap.edu.co

[1] Escuela Naval de Cadetes "Almirante Padilla", Barrio el Bosque - Isla Manzanillo, 130001, Cartagena, Colombia.

[5] Escuela Superior de Administración Pública - ESAP, 760046, Cali, Colombia

Pages: 211-221

Resumen: el artículo presenta una propuesta de modelo conceptual del Sistema del Poder Marítimo a nivel estratégico en Colombia, para identificar sus diferentes elementos, acciones e interacciones, entendiendo la complejidad del fenómeno y facilitando la protección y defensa de este poder en términos de toma de decisiones y administración de recursos. Para el desarrollo del modelo se establecieron tres fases. La primera, buscó identificar los actores y elementos que hacen parte del sistema del poder marítimo en Colombia. La segunda fase se enfocó en caracterizar las relaciones e interacciones que existen entre los elementos del poder marítimo. En la tercera fase se desarrolló el modelo conceptual del sistema del poder marítimo en Colombia utilizando la norma ISO 19450, bajo la metodología OPM y el software OPCAT OPM. Finalmente, se resaltan las principales características del modelo y su importancia para la Armada de Colombia.

Palabras-clave: Intereses Marítimos; Modelo Conceptual; Poder Marítimo; Poder Naval.

Conceptual model of the Maritime Power System at a strategic level in Colombia

Abstract: the article presents a proposal for a conceptual model of the Maritime Power System at a strategic level in Colombia, to identify its different elements, actions and interactions, understanding the complexity of the phenomenon and facilitating the protection and defense of this power in terms of decision-making and resource management. Three phases were established for the development of the model. The first sought to identify the actors and elements that are part of the maritime power system in Colombia. The second phase focused on characterizing the relationships and interactions that exist between the elements of maritime power. In the third phase, the conceptual model of the maritime power system in Colombia was developed using the ISO 19450 standard, under the OPM methodology and the OPCAT OPM software. Finally, the main characteristics of the model and its importance for the Colombian Navy are highlighted.

Keywords: Bibliometrics; Bibliometrix; Cybersecurity; Cyberdefense; Maritime; Naval.

1. Introducción

La condición bioceánica y posición estratégica de Colombia representa un factor básico para su desarrollo económico y social lo que genera para el Estado la necesidad de preservar, proteger y explotar los intereses marítimos de la nación, apoyado de un poder naval flexible con la capacidad de proteger y defender los intereses marítimos de las diferentes amenazas, propias de la dinámica del poder marítimo, de manera efectiva y con las capacidades operacionales adecuadas.

Para ello es esencial identificar las diferentes elementos, acciones e interacciones entre los componentes del poder marítimo estratégico que contribuyan a entender la complejidad del fenómeno, faciliten su protección y defensa y favorezcan el proceso de toma de decisiones y la administración de recursos. El desarrollo de un modelo conceptual del poder marítimo se plantea como una vía que da respuesta a la situación planteada.

Entender cómo es la dinámica entre el poder marítimo, el poder naval y los intereses marítimos con un modelo que facilite su comprensión y dinamismo, se enmarca en la estrategia pentagonal de la Armada de Colombia (Armada República de Colombia, 2020), aportando a la toma de decisiones en concordancia con la necesidad institucional de estar preparada para desplegar toda su capacidad con elevados niveles de dinamismo y de flexibilidad, adaptándose a múltiples escenarios y situaciones en el cumplimiento de su misión , la política Colombia bioceánica (Departamento Nacional de Planeación, 2020) y la política nacional de los océanos y espacios costeros (Comisión Colombiana del Oceano, 2017). Adicionalmente, la investigación aportó al desarrollo de los objetivos de la investigación titulada “Marco de Referencia para el Modelamiento y Simulación de la Ciberdefensa Marítima a Nivel Estratégico – MARCIM” (Cabuya Padilla, 2021).

Para el desarrollo del modelo se establecieron tres fases. La primera fase buscó identificar los actores y elementos que hacen parte del sistema del Poder Marítimo en Colombia. La segunda, se enfocó en caracterizar las relaciones e interacciones que existen entre los elementos del poder marítimo. Finalmente, la tercera fase buscó modelar el sistema del poder marítimo en Colombia utilizando la norma ISO 19450, bajo la metodología OPM (*Object Process Methodology*) y el software OPCAT OPM, representando así el fenómeno estudiado mediante un modelo conceptual.

Como conclusiones se resalta que la sistematización de un modelo conceptual del poder marítimo no solo aporta resultados para toma de decisiones referente a temas presupuestales y adquisición de unidades, también contribuye de forma indirecta a la educación, investigación y doctrina naval, temas sustanciales para la Armada de Colombia.

2. Metodología

El objetivo de la investigación fue caracterizar el modelo conceptual del sistema del poder marítimo a nivel estratégico en Colombia. Para su desarrollo se establecieron

tres fases. La primera, buscó identificar los actores y elementos que hacen parte del sistema del Poder Marítimo en Colombia, para ello se caracterizaron los ejes temáticos de la investigación: poder marítimo, poder naval e intereses marítimos; y se realizó una entrevista a un experto en el tema, señor Almirante de la Armada de Colombia Juan Manuel Soltau Ospina, profesional en oceanografía física, hidrógrafo, magíster en relaciones internacionales, especialista en seguridad y defensa y experto en temas marítimos y fluviales.

La segunda fase se enfocó en caracterizar las relaciones e interacciones que existen entre los elementos del poder marítimo, para ello se realizó un análisis bibliográfico, apoyado de los resultados de la primera fase que arrojó como resultado una matriz en la que se caracterizaron las relaciones e interrelaciones entre estos elementos.

Finalmente, la tercera fase buscó modelar el sistema del poder marítimo en Colombia utilizando la norma ISO 19450 (ISO, 2015). Para ello se utilizó la metodología OPM (*Object Process Methodology*) (Dori, 2002, 2016) y el software OPCAT OPM (Enterprise System Modeling Laboratory, 2021), ambos alineados con la norma ISO 19450, y se hizo la representación del fenómeno estudiado mediante un modelo conceptual.

3. Identificación de los actores y elementos que hacen parte del sistema del poder marítimo en Colombia

Colombia por su ubicación bioceánica se convierte en eje fundamental de desarrollo gracias a los beneficios derivados del acceso al mar que la proyectan como un país marítimo en el que los Intereses Marítimos Nacionales (IMN) crean condiciones de desarrollo económico sostenible, inclusivo y estable que impactan su desarrollo en materia de ingresos, progreso y bienestar, teniendo como eje central el recurso humano y la comunidad (Ramírez-Cabrales et al., 2021), y a nivel competitivo afectan la productividad, la I+D+i y la tecnología (Cabuya Padilla, 2018).

La Comisión Colombiana del Océano – CCO (2015) indica que Colombia cuenta una extensión territorial aproximada de 2070 km2, del cual el 55,15% corresponde a tierras emergidas, continentales e insulares y el 44,85% a territorio marítimo (aproximadamente 589.560 km2 en el Caribe y 339.100 km2 en el Pacifico). La zona costera de Colombia se extiende a lo largo de 12 de los 32 departamentos del país (47 municipios), de los cuales, ocho tienen costas en el Caribe y cuatro en el Pacifico. Además, el país cuenta, aproximadamente, con 100 islas, 17 cayos, 42 bahías, 5 golfos, múltiples áreas coralinas, arrecifes coralinos y manglares (Comisión Colombiana del Oceano, 2015), tres Reservas de Biosfera, 35 Áreas marinas protegidas, una Zona Marina Especialmente Sensible y 9 Zonas Portuarias (Ramírez-Cabrales et al., 2021).

Son diversos los actores que tienen relación directa con el desarrollo y gestión del poder marítimo, tales como (Cabuya Padilla & Castaneda-marroquin, 2021) autoridades marítimas, puertos, buques y su carga, industria marítima, proveedores de servicios de información y comunicaciones marítimas, operadores de transporte marítimo, proveedores de servicios marítimos e instituciones de seguridad y defensa, como la Armada de Colombia. A nivel estratégico estos se pueden agrupar para entender la dinámica propia de este fenómeno, para esta investigación se entenderá la dinámica general del poder marítimo como se representa en la Figura 1.



Figura 1 – Poder Marítimo. Fuente: (Uribe, 2016).

El Poder Marítimo Nacional está definido como la capacidad de crear, desarrollar, explotar y defender los intereses marítimos de un país, tanto en la paz como en la guerra, pudiendo tener la habilidad de utilizar el mar en provecho propio, incorporando el medio marítimo, su entorno, artefactos que actúan, y la voluntad de poder ejercer ese poder (Uribe Caceres, 2017).

El Poder Naval, a su vez, se compone de la Fuerza (los buques de guerra) y de la posición que estos tengan en el espacio marítimo bajo su responsabilidad. Su agente dinamizador es la Voluntad Estratégica que debe tener la alta dirigencia política del Estado para utilizarlo cuando sea requerido. Sin lugar a duda, las poderosas talasocracias de la Edad Media hicieron uso de ese Poder Marítimo para garantizar la supremacía en el mar que ejercieron durante siglos (Uribe, 2016). Los Intereses Marítimos son el conjunto de beneficios de carácter político, económico, social, ambiental y militar que logra el país mediante el desarrollo de las actividades relacionadas con el uso y explotación del mar y los espacios costeros. Suponen una visión estratégica con amplia proyección de desarrollo y seguridad (Ramírez-Cabrales et al., 2021).

La voluntad política ejerce un papel fundamental como estrategia para influir sobre el desarrollo del poder marítimo, esta incluye dos componentes, la conciencia marítima y la voluntad estratégica, esta última se define como la voluntad y estrategia para usar el poder naval (Alba Rocha & Ortegon Vega, 2021). La Escuela Superior de Guerra de Colombia (Uribe, 2016) define el poder marítimo a partir de la ecuación chilena, poder marítimo igual a poder naval más intereses marítimos, pero añade como factor dinamizador a la conciencia marítima, y como elemento estimulador del poder naval a la voluntad estratégica (Figura 1).

Ahora bien, identificados los componentes o actores principales del poder marítimo, se especifican ciertas particularidades para el caso colombiano(Alba Rocha & Ortegon Vega, 2021):

- La voluntad política requiere un proceso de seguimiento para desarrollarse, ya que no tiene un lineamiento o ruta a seguir en la (PNOEC) Política Nacional de los Océanos y Espacios Costeros, que es la carta magna para el desarrollo del poder marítimo en Colombia.
- La Armada de Colombia por su conformación y relacionamiento a través de la historia, no ha sido exitosa en temas de influencia en los tomadores de decisiones a nivel estratégico.

- Para poder inculcar la voluntad política del poder marítimo se debe hacer un trabajo de mediano y largo plazo para que se logre interiorizar el fenómeno y que sea incluido en los planes de desarrollo nacionales.
- La conciencia marítima no es exclusiva de la Armada de Colombia o de aquellos actores que están explotando sus beneficios, es un tema nacional que apoya el desarrollo del país así no se esté en contacto directo con el medio.
- La voluntad estratégica en Colombia debe ser una interacción democrática en beneficio del Estado, que usa el poder naval más allá de las capacidades disuasivas, por ejemplo, medios navales de ayudas humanitarias y plataformas navales de apoyo al desarrollo.
- La voluntad estratégica en un Estado democrático para los efectos de desarrollo debe contar con un grupo de asesores en los diferentes niveles de las ramas del poder ejecutivo, legislativo y judicial que servirán como canalizadores en la voluntad del Estado.

Para finalizar, la Tabla 1 resume la identificación y definición de los principales actores dentro del poder marítimo.

ACTOR	DEFINICIÓN	FUENTE
Poder Nacional	Es la capacidad que tiene un estado para alcanzar sus fines, está integrado por los diferentes campos del poder económico, social, militar y político, está definido por la estrategia y la política nacional diseñada para alcanzar los objetivos político-estratégicos nacionales, estos se desarrollan en condiciones de seguridad nacional que debe garantizar el poder militar.	(Uribe, 2016)
Poder Militar	Uno de los campos del poder nacional, es una fuerza de disponibilidad permanente y empleo inmediato, sus funciones son velar por la integridad territorial, ejercer soberanía, aplicar la política exterior del Estado, defender y proteger sus intereses y contribuir a establecer las condiciones de seguridad para su desarrollo.	(Uribe, 2016)
Poder Marítimo	Es la capacidad que tiene el Estado para crear, desarrollar, mantener, explotar y proteger los intereses marítimos del país tanto en tiempo de paz como en guerra. Está compuesto por los Intereses Marítimos (IM) que este posee y explota y por un Poder Naval (PN).	(Uribe, 2016)
Poder Naval	Es el componente militar del poder marítimo. En función de su aplicación ejerce un importante papel en la contribución al logro de los objetivos nacionales, tanto del ámbito marítimo como de ciertas áreas terrestres de interés para las operaciones navales. Su función principal es el mantenimiento de la situación de seguridad requeridas para asegurar el desarrollo económico y los intereses marítimos.	(Uribe Caceres, 2017)
Conciencia Marítima	Constituye el conocimiento cabal y reflexivo del mar y de sus proximidades, tanto sobre su real naturaleza como de sus posibilidades políticas, económicas, sociales y militares. Cuando la geografía lo permite, la conciencia marítima facilita la labor de orientar al país hacia un destino oceánico y convertirlo en una potencia marítima próspera y poderosa.	(Uribe, 2016)
Voluntad estratégica	Es la preparación de los dirigentes del Estado en asuntos marítimos y navales, y su decisión de emplear el Poder Naval para contribuir al logro de los fines y objetivos del Estado.	(Uribe, 2016)

ACTOR	DEFINICIÓN	FUENTE
Posición Estratégica	La Posición Estratégica consiste en un factor geográfico y como tal inerte, lo que le infunde vida es la Fuerza apoyada en ella. Pero la Fuerza necesita actuar para ejercer su efecto.	(Uribe, 2016)
Intereses Marítimos	Es el conjunto de beneficios de carácter político, económico, social, ambiental y militar que logra el país mediante el desarrollo de las actividades relacionadas con el uso y explotación del mar y los espacios costeros.	(Ramírez-Cabrales et al., 2021)

Fuente: Elaboración propia.

Tabla 1 – Actores principales.

4. Caracterización de las relaciones e interacciones que existen entre los elementos del poder marítimo

A partir de los resultados anteriores y con soporte bibliográfico adicional, se construyó la matriz de actores, acciones e interacciones del poder marítimo en Colombia a nivel estratégico. En las columnas se ubica la siguiente información: identificación del actor, definición del actor, fuente de los datos de definición, tipo de relación del actor con otro actor (entidad, organización, corporación, etc.), e identificación del actor con el que se da la relación. Sobre el tipo de relación se proporcionan tres opciones: "CONSISTE", determina los actores que componen o caracterizan al actor base; "AFECTA", actores que se afectan por las acciones o decisiones que toma el actor base, está relación puede ser reciproca; "REQUIERE", actores que son necesarios para la función u operación del actor base. En total se identificaron y caracterizaron 34 actores, y la Tabla 2 presenta un ejemplo de la operacionalización de dos actores.

ACTOR	DEFINICIÓN	FUENTE	RELACIÓN	ACTOR
Soberanía e Integridad del Territorio Marítimo Nacional.	Se entiende como el ejercicio del poder absoluto y permanente del Estado sobre el territorio marítimo colombiano	(Ramírez-Cabrales et al., 2021)	CONSISTE	CCO (Comisión Colombiana del Océano)
				DIMAR (Dirección General Marítima)
			AFECTA	Poder Marítimo
			REQUIERE	Comando General FFMM
Industria Naval y Marítima	Confección de bienes de larga duración que integran el equipamiento de las múltiples actividades que constituyen los denominados Intereses Marítimos (Guzmán, 2008).	(Ramírez-Cabrales et al., 2021)	CONSISTE	COTECMAR (Corporación de ciencia y tecnología para el desarrollo de la industria naval marítima y fluvial)
				Puertos - Astilleros
			AFECTA	Poder Marítimo
			REQUIERE	Ministerio de trabajo

Fuente: Elaboración propia.

Tabla 2 – Ejemplos de definición de relaciones e interacciones de un actor

5. Modelamiento del Poder Marítimo a nivel Estratégico en Colombia

Para representar los resultados de las dos fases anteriores y formular el modelo conceptual del poder marítimo a nivel estratégico, se utilizó la Metodología de Proceso de Objetos OPM, en inglés *Object Process Methodology,* bajo la norma ISO 19450 de 2015. En este sentido, se presentan tres diagramas de objetos y procesos (OPD) que en su conjunto representan el modelo conceptual. El primer diagrama (Figura 2) es el modelo conceptual a nivel general, que representa la dinámica de alto nivel entre los actores del poder marítimo en Colombia, donde:

- La voluntad política está integrada por la voluntad estratégica y la conciencia marítima.
- La voluntad estratégica es un agente operador del poder naval.
- La conciencia marítima aporta al desarrollo del poder naval y de los intereses marítimos.
- El poder naval y los intereses marítimos integran el poder marítimo.
- El desarrollo del poder marítimo afecta al Estado transformándolo de un país marítimo a una potencia media oceánica.

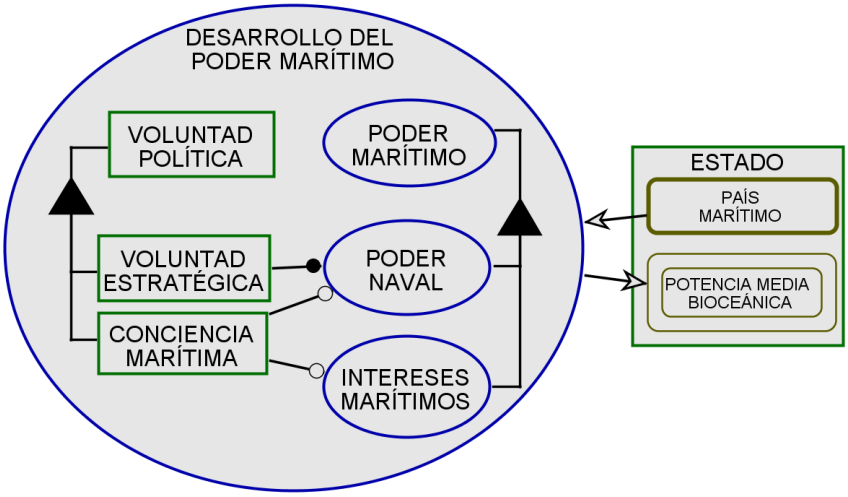


Figura 2 – Modelo conceptual general. Fuente: Elaboración propia.
Fuente: Elaboración propia utilizando OPCAT OPM.

El segundo diagrama (Figura 3), representa el poder naval como subproceso del poder marítimo, donde la Fuerza Pública, la Fiscalía y la Dirección General Marítima integran las entidades de coordinación con las que interactúa el poder naval. La fuerza naval y las bases navales constituyen los medios navales que proporcionan una posición estratégica orientada por la voluntad estratégica y la naturaleza de las operaciones navales que se desarrollan.

Finalmente, el tercer diagrama (Figura 4) representa los intereses marítimos aplicables a un modelo conceptual como el planteado, representando la complejidad de las relaciones e interacciones desde una mirada estratégica y holística.

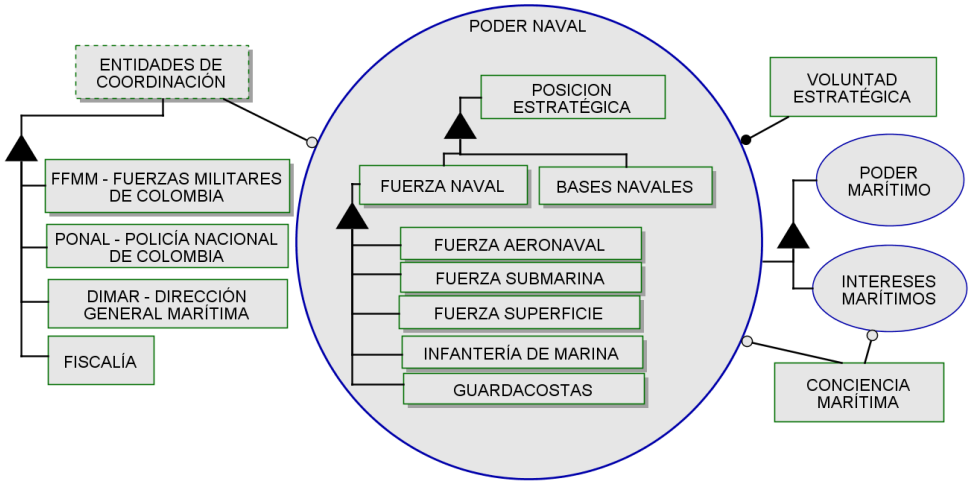


Figura 3 – Modelo conceptual poder naval.
Fuente: Elaboración propia utilizando OPCAT OPM.

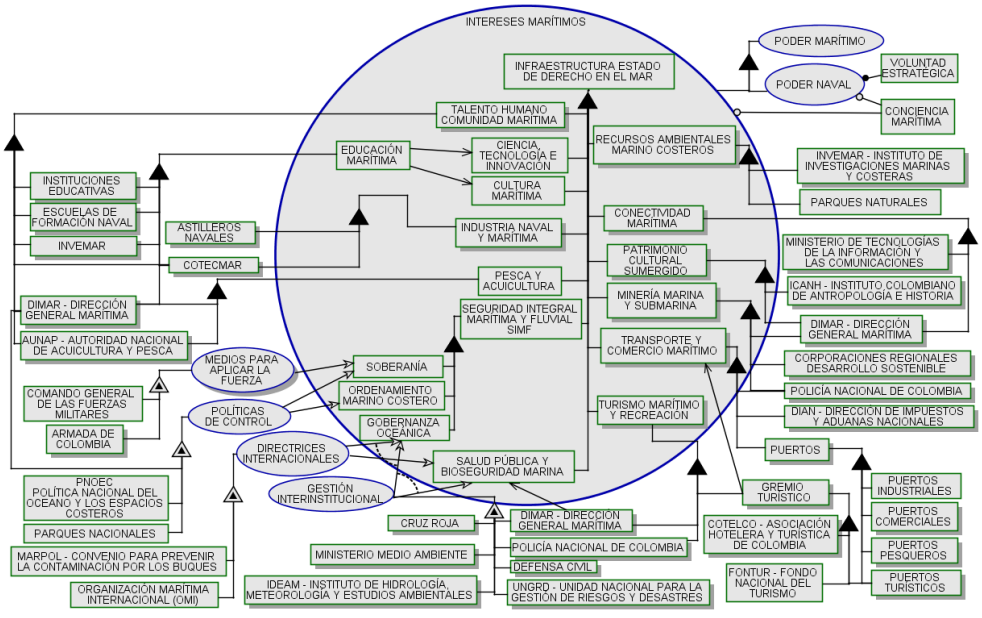


Figura 4 – Modelo conceptual intereses marítimos.
Fuente: Elaboración propia utilizando OPCAT OPM.

6. Conclusiones

Se identificaron actores, acciones e interacciones a nivel estratégico del poder marítimo en Colombia y se representaron gráficamente en un modelo conceptual bajo la metodología OPM (Dori, 2002, 2016) y la norma ISO 19450 (ISO, 2015), concluyendo lo siguiente:

- La voluntad política se divide en dos componentes, la voluntad estratégica y la conciencia marítima. La voluntad estratégica incide directamente en el poder naval, dándole una intención y objetivo estratégico.
- El aporte del poder naval al poder marítimo va más allá del ámbito bélico, consolidándose como un componente de apoyo y coordinación necesario para desarrollar los demás intereses marítimos, diferentes a la soberanía, contribuyendo al desarrollo del país hacia una potencia media bioceánica.
- La conciencia marítima no es exclusivamente y solo del dominio de la gente de mar (políticos, militares y área científica), sino que cualquier persona que considere y tenga la conciencia sobre la importancia del mar como medio para alcanzar el desarrollo contribuye al colectivo de conciencia a marítima en el país.
- La política nacional de los océanos y de los espacios costeros (PNOEC), no fomenta la conciencia marítima en la esfera política, por lo tanto, es vital generar una estrategia que impulse el pensamiento marítimo, acorde a la realidad del país y de los objetivos estratégicos de la Armada de Colombia, vinculados a ser una marina AMPRE - Armada Mediana de Proyección Regional; y los de la PNOEC, ser una potencia mediana bioceánica.
- La cooperación interinstitucional es la vital para mantener la dinámica del sistema del poder marítimo, teniendo en cuenta las múltiples relaciones identificadas a nivel estratégico.
- El eje principal de los intereses marítimos es la "Infraestructura para el aseguramiento, la integridad, el orden marítimo y el estado de derecho en el mar" y que los demás se pueden agrupar en tres ejes más: seguridad, desarrollo y explotación.
    - Eje seguridad: la infraestructura y medios para el aseguramiento, protección, defensa e integridad del orden marítimo y el estado de derecho en el mar:
        - Seguridad Integral Marítima y Fluvial
        - Soberanía e integridad del territorio marítimo nacional
        - Gobernanza oceánica
    - Eje desarrollo: conectar y desarrollar el espacio marítimo, es decir facilitar las condiciones para la explotación:
        - Conectividad marítima
        - Industria Naval y Marítima
        - Investigación científica, tecnológica e innovación
        - Educación marítima
        - Cultura marítima
        - Ordenamiento marino costero
        - Salud pública y bioseguridad marina
        - Talento humano y comunidad marítima
    - Eje explotación: una vez dadas las condiciones de seguridad y el desarrollo del espacio marítimo es posible realizar una explotación eficiente y sostenible:

- Patrimonio cultural sumergido
- Recursos ambientales marino costeros
- Minería marina y submarina
- Pesca y acuicultura
- Turismo marítimo y recreación
- Transporte y comercio marítimo

Para finalizar, el modelo conceptual del poder marítimo en Colombia facilita al investigador y tomador de decisiones el entendimiento de la dinámica del fenómeno estudiado en los correspondiente a actores, acciones e interacciones, y se enmarca como una herramienta de trabajo para la toma de decisiones a nivel estratégico, con miras al cumplimiento de los objetivos de ese nivel.

Referencias

Alba Rocha, D. A., & Ortegon Vega, J. R. (2021). *Entrevista Almirante Juan Manuel Soltau Ospina - Modelo Conceptual del Poder Marítimo*.

Armada República de Colombia. (2020). *Plan de Desarrollo Naval 2042* (Jefatura de Planeación Naval & Dirección de Planeación Estratégica (eds.)). ARC. https://www.escuelanaval.edu.co/es/file-download/download/public/14011

Cabuya Padilla, D. E. (2018). Relación de la Industria 4.0 con la competitividad industrial. *Revista El Derrotero*, *12*, 143–174. https://www.escuelanaval.edu.co/es/file-download/download/public/4882#:~:text=Es la integración de las,y volver a la industria

Cabuya Padilla, D. E. (2021). *Marco de Referencia para el Modelamiento y Simulación de la Ciberdefensa Marítima a Nivel Estratégico - MARCIM [Tesis de doctorado no publicada]*. Escuela Naval de Cadetes "Almirante Padilla."

Cabuya Padilla, D. E., & Castaneda-marroquin, C. (2021). Maritime Cyberdefense Actors Taxonomy for Command and Control. *Smart Innovation Systems and Technologies*, *181*.

Comisión Colombiana del Oceano. (2015). *Mapa Esquemático de Colombia*. https://cco.gov.co/component/content/article.html?id=102:mapa-

Comisión Colombiana del Oceano. (2017). *Política Nacional del Océano y los Espacios Costeros*. 96. http://www.cco.gov.co/docs/publicaciones/pnoec-2018-09.pdf

Departamento Nacional de Planeación. (2020). *Documento CONPES 3990 - Colombia Potencia Bioceánica*. Consejo Nacional de Política Económica y Social.

Dori, D. (2002). *Object-Process Methodology: A Holistic Systems Paradigm*.

Dori, D. (2016). Model-based systems engineering with OPM and SysML. In *Model-Based Systems Engineering with OPM and SysML*. https://doi.org/10.1007/978-1-4939-3295-5

Enterprise System Modeling Laboratory. (2021). *OPM - OPCAT*. https://esml.technion.ac.il/opm/opcat-installation/

ISO. (2015). *Object-Process Methodology - ISO/PAS 19450:2015*. https://www.iso.org/standard/62274.html

Ramírez-Cabrales, F., Pedroza Nieto, W. T., & Forero Hauzeur, J. C. (2021). *Intereses Marítimos Colombianos* (Vicepresidencia de la República (ed.)). Vicepresidencia de la República-Comisión Colombiana del Océano-Armada de Colombia.

Uribe Caceres, S. (2017). El Estado y el Mar: Relaciones con el Poder Marítimo, Nacional, el Poder Naval y el desarrollo. In *Página Institucional*. file:///Users/jonathancortes/Downloads/29-Manuscrito de libro-430-1-10-20180517.pdf

Uribe, S. (2016). De la Estrategia y sus Niveles. In *Estrategia Marítima, Evolución y Prospectiva* (pp. 29–40). https://doi.org/https://doi.org/10.25062/9789585737693

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 09/12/2021
Aceitação/Acceptance: 10/02/2022

Sistema Inteligente para Control y Monitorización de una Estación Robótica usando Motion Control y Visión Artificial

Lesly Tarira Montalvan[1], Edisson Jordan[2], Edith Tubón[2], Sandra Carrillo[2], Eduardo Heredia[3], Franklin Salazar[4]

ltarira3535@uta.edu.ec; edissonpjordan@uta.edu.ec; ee.tubon@uta.edu.ec; sandralcarrillor@uta.edu.ec; heheredia@espe.edu.ec; franklin.salazar@uam.edu.es

[1, 2] Universidad Técnica de Ambato, 180103, Ambato, Ecuador.

[3] Universidad de las Fuerzas Armadas ESPEL, 050150, Latacunga, Ecuador.

[4] Universidad Autónoma de Madrid, 28049, Madrid, España.

Pages: 222-236

Resumen: Las tecnologías actuales permiten que las operaciones industriales sean más eficientes con el objetivo de lograr una mayor productividad y seguridad en situaciones de riesgo. Debido a la complejidad y precisión requeridas en estas operaciones, los operarios han sido sustituidos por la inteligencia artificial y otras mejoras tecnológicas. Así, el objetivo de este proyecto es diseñar y poner en marcha un robot cartesiano paletizador didáctico de bajo coste que permita el aprendizaje de estas nuevas técnicas de control inteligente aplicados a procesos industriales. Para ello se han integrado plataformas de programación y arquitectura como Motion Control, PLC, software de control Labview, interfaz HMI, visión artificial. El sistema comienza distinguiendo las cajas por su color, lo que active el robot cartesiano para posicionarlas en la cinta transportadora. Posteriormente, éstas se dirigen a la zona de paletizado, la banda se activa mediante una señal enviada por el PLC a través de una conexión Profinet. El proceso de paletizado puede ser controlado a distancia, se incorpora visión artificial para la clasificación de cajas de forma automática. El procesamiento de datos del software LabVIEW y el TIA PORTAL están vinculados través de una conexión OPC. El sistema robotizado es operado por vía inalámbrica y logrando ejecutar correctamente la secuencia programada de manera que se evitaron colisiones. Para comprobar la funcionalidad de las cadenas cinemáticas de los robots industriales se realizó la simulación en el software tía portal (siemens) haciendo uso de las herramientas tecnológicas que nos ofrece la gama de PLC versiones avanzadas. Tras realizar varias pruebas con el sistema completo, se comprobó el correcto funcionamiento de los componentes, indicando que se realizaban en tiempo real y con una gran efectividad ofreciendo una Plataforma flexible, robusta y de bajo coste.

Palabras clave: brazo robótico; visión artificial; sistema inteligente.

Smart Control and Monitoring System of a Robotic Station Operating with Motion Control and Artificial Vision

Abstract: Today's technologies allow industrial operations to be more efficient with the aim of achieve higher productivity and safety during hazardous situations. Due to the complexity and precision required in these operations, the operators have been replaced by artificial intelligence. Thus, the purpose of this project is to design and start up a didactic palletizer cartesian robot. In this design, programing, and architecture platforms such as LabVIEW, Motion Control, s-7-1200 PLC, HMI interface, artificial vision and a robotic arm were integrated. The system begins with the distinguishing of boxes by color, which activates the cartesian robot to position them on the conveyor belt. Subsequently, these are directed to the palletizing area, the band is activated through a signal sent by the PLC through a Profinet connection. The palletizing process can be remotely controlled, and artificial vision is incorporated for the box classification. LabVIEW and TIA PORTAL software data processing are linked via an OPC connection. The robot operated via wireless was successfully used by properly executing the programmed sequence in such manner preventing any collisions. To check the functionality of the kinematic chains of the industrial robots, the simulation was carried out in the aunt portal software (siemens) using the technological tools offered by the advanced version PLC range. After performing several tests with the complete system, the correct operation of the components was verified, indicating that they were performed in real time and with great effectiveness, offering a flexible, robust and low cost platform.

Keywords: robotic arm; artificial visión; intelligent system.

1. Introducción

La automatización industrial de procesos consigue sustituir el trabajo manual de los operarios en situaciones repetitivas o de mayores niveles de complejidad y/o exactitud, logrando mejorar la eficiencia de los procesos y el incremento de la productividad en conjunto con la mejora de la calidad de los productos (Radityo Wibisono, 2018). Bajo este mismo enfoque los sistemas automatizados se han desarrollado para dotar a las máquinas de habilidades humanas con el fin de que ejecuten una determinada acción (Detez L, Sep 3-2019). Inicialmente las máquinas solo ejecutaban operaciones simples y lineales como cortar, empujar, levantar entre otras (Jonathan Talahua, 2021) (Zoran Salcic, 2019). Con el avance tecnológico la robótica industrial ha ido tomando gran importancia en todos los sectores manufactureros (Štefan. Kozák, 2018). Los robots industriales son máquinas complejas que están constituidos por tres elementos esenciales: un elemento operativo para ejecutar las acciones, una unidad de procesamiento (CPU) para ejecutar y almacenar la información y programación del control y una fuente de poder para la alimentación del sistema (Gassert, 2018). Por otra parte, la visión artificial intenta emular las características de los seres vivos para ver una imagen, entenderla y actuar en consecuencia. En la actualidad, la automatización industrial a través de la robótica y la visión artificial han demostrado un sin número de aplicaciones (Matthew Johnson, 2017).

Finalmente, gran variedad de industrias han optado por utilizar mecanismos basados en técnicas, herramientas y métodos visuales ejecutados por operarios para el control de los procesos industriales (Marcin Szuster, 2016). Por esta razón, nace la necesidad de implementar un sistema inteligente para el control y monitorización de una aplicación robotizada de bajo coste que sirvan de apoyo en la formación de los estudiantes en esta etapa de clases virtuales y presenciales. Estas herramientas son muy útiles en el proceso formativo de los futuros profesionales que podrán mostrar estos conocimientos

en la industrial. En el campo empresarial se pueden reducir riesgos, incrementar la producción y una mejor toma de decisiones.

Esta investigación se divide en 4 secciones, incluyendo la introducción en la sección 1, la sección 2 se expone el caso de estudio, en la sección 3 se presentan los resultados obtenidos al implementar el sistema propuesto. Finalmente, las conclusiones y trabajos futuros del proyecto se plasman en la sección 4.

2. Hardware

El sistema de control y monitorización de un robot cartesiano (Franklin Salazar, 2019) está diseñado de acuerdo con la arquitectura mostrada en la Figura 1.

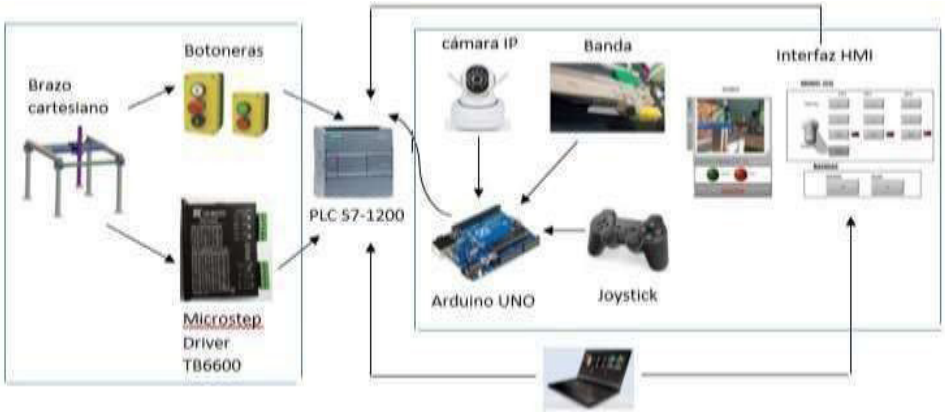


Figura 1 – Arquitectura del Ambiente de Control

El proceso de clasificación y paletizado de las cajas puede ser controlado y monitorizado a distancia mediante protocolos de comunicación industrial y basados en IoT. La programación realizada permite detectar diferentes tipos de cajas en función del proceso seleccionado por el operador. A su vez el sistema cuenta con implementaciones de seguridad que permiten la correcta operación del sistema sin provocar dañar a los equipos o la integridad del personal que ejecuta el proceso (Jorge Aroca, 2018).

2.1. Interfaz de Control Electrónico

El sistema cuenta con 2 etapas como se pude apreciar en la Figura 1. En la etapa 1 se realiza la configuración y programación para el control y monitorización del robot cartesiano y todos los elementos complementarios. Para el correcto funcionamiento se utiliza una comunicación entre una variedad de plataformas, mediante la integración de PLC'S S7-1200, un robot cartesiano de 3 ejes, el software LabVIEW, Motion Control, TIA Portal y visión artificial. En la etapa 2 se establece un proceso industrial de clasificado y paletizado de forma manual y automática. Éste se encuentra basado en la cadena cinemática de todo el sistema, teniendo en cuenta las posiciones iniciales de cada eje robot, del lugar de recepción de las cajas y de la zona de paletizado. Para la comprobación el sistema y del posicionamiento de los ejes.

El proceso propuesto consiste en la detección de las cajas mediante visión artificial a través de una cámara vinculada a la programación en el software LabVIEW para el procesamiento de imágenes. Una vez que se reconocen las cajas se envía un pulso eléctrico que activa un sistema robótico de 3 ejes para que ejecute una serie de secuencias programadas previamente, de acuerdo con el color de las cajas que se detecte. Este sistema emplea una comunicación OPC-DA para la integración de todos sus componentes. Los movimientos del robot son proporcionados desde dos zonas remotas; la primera a través de un joystick para su control y la segunda opción desde una interfaz HMI para su control y monitorización en tiempo real.

2.2. Configuración de entradas y salidas del Sistema

A continuación, se detallan las entradas y salidas físicas que van a ser empleadas para la conexión de los diferentes equipos. El proyecto cuenta con un PLC S7-1200 DC/ DC/DC físico que controla la maqueta del robot y además una pantalla HMI simulada para controlar cada uno de los ejes. Este debe ser configurado tomando en cuenta los finales de carrera, longitudes y referencias. Así se provee la información adecuada para el dimensionamiento de la maqueta y su área de trabajo, mediante Motion Control. Las conexiones se presentan de la siguiente manera: las salidas Q0.0 y Q0.1 del dispositivo PLC S7-1214 se acoplan a las señales de entrada de velocidad (PUL+) y dirección (DIR+) del primer driver TB6600, para ejecutar los movimientos en el eje X. Posterior- mente, las salidas Q0.2 y Q0.3 se ajustan a las señales de velocidad y dirección del segundo driver, para controlar el movimiento del motor en el eje Y. Finalmente, las salidas Q0.4 y Q0.5 se conectan a las señales de entrada de un tercer driver que controla el eje Z. La salida Q1.0 va a ser utilizada para el elemento encargado de las piezas seleccionadas para su recolección y posicionamiento en la banda y luego para dejar en la zona de paletizado previamente programada. En la tabla 1 se detallan estas especificaciones.

Entrada	Descripción	Salida	Descripción
I0.0	Home eje X	Q0.0	Velocidad eje X
I0.1	Final de carrerainicial eje X	Q0.1	Dirección eje X
I0.2	Final de carrera finaleje X	Q0.2	Velocidad eje Y
I0.3	Habilitar eje X	Q0.3	Dirección eje Y
I0.4	Reset	Q0.4	Velocidad eje Z
I0.5	Home	Q0.5	Dirección eje Z
I0.6	Secuencia	Q1.0	Electroiman
I0.7	Final de carrera inicial eje y derecha		
I1.0	Final de carrera final eje e izquierda		
I1.1	Home eje Y		
I1.2	Final de carrera inicial eje Z superior		

Tabla 1 – Especificación de entradas y salidas del PLC S7-1200 DC/DC/DC

2.3. Control de movimiento

Los controladores de movimiento son la unidad central de los sistemas que generan movimiento de una forma controlada y precisa. Mediante motion control se puede controlar la posición, la velocidad de avance o el par motor de máquinas y robots. Para este caso de estudio del sistema motion control consiste en un controlador de movimiento para cada eje del robot y realizar secuencias determinadas por el operador. Por cada uno de los ejes existe un driver, un servomotor y un encoder de alimentación. En la Figura 2 se muestra el sistema para un eje del robot en el que se detallan las conexiones y configuraciones necesarias de todos los equipos para el correcto funcionamiento. Todo el sistema debe ser previamente configurado en el software de tia portal y verificado en la simulación de las cadenas cinemáticas incorporadas en el mismo.

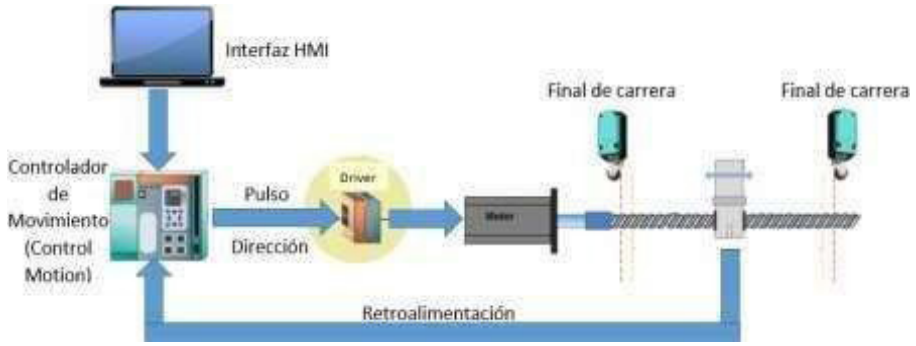


Figura 2 – Sistema de Control Motion

Para el control y accionamiento de cada uno de los ejes del autómata de la estación propuesta, se emplea Control Motion de TIA Portal V15. El accionamiento y control de los ejes del robot se lo podrá hacer de forma manual o automática. Por una parte, para instanciar los ejes de movimiento X, Y, Z; se emplea el objeto "TO_PositioningAxis" que permite la integración y configuración de los ejes que intervienen en el sistema del robot cartesiano.

Para el accionamiento de los ejes es fundamental que se determine el tipo de señal y se definan las salidas del PLC que se utilizarán en el sentido de giro y para la velocidad de los ejes, como se muestra en la siguiente Figura 3 (a). Mientras que, para caracterizar y limitar los movimientos de cada uno de los ejes del robot, es necesario delimitar su trayectoria (véase la Figura 3(b)), mediante finales de carrera (hardware) y su respectiva programación en Control de Movimiento.

Para que no se genera ninguna anormalidad o inconveniente en los movimientos del robot, se inicializa los parámetros de aceleración, desaceleración, rampas de arranque, rampas de parada y la velocidad de los motores de los ejes. Así se evitan colisiones entre sus eslabonamientos y daños en los demás elementos del prototipo (véase Figura 4). Además se realiza la configuración y simulación de la cadena cinemática en control de movimiento (véase Figura 5).

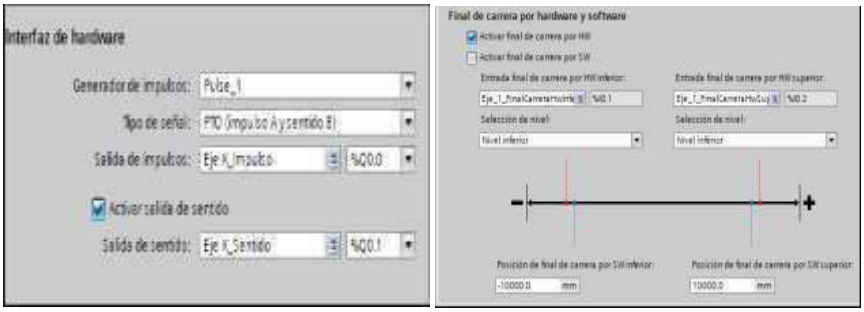


Figura 3 – (a) Configuración de señal y salidas, (b) Asignación límites y entradas

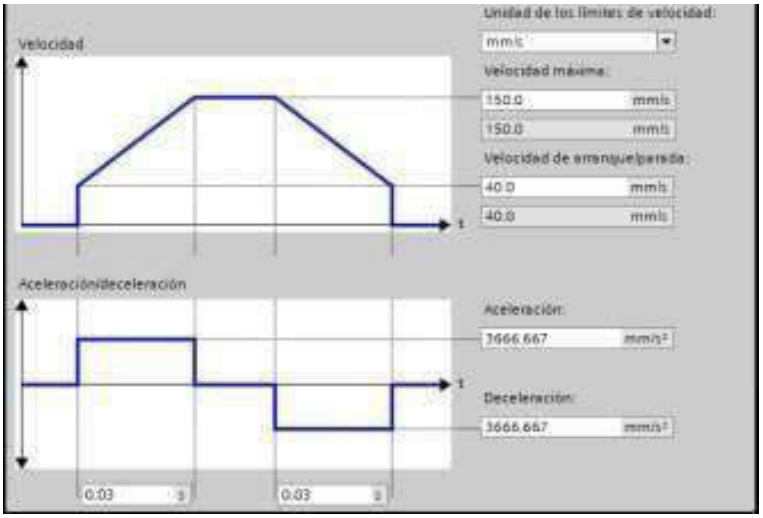


Figura 4 – Configuración de velocidad y aceleración/desaceleración

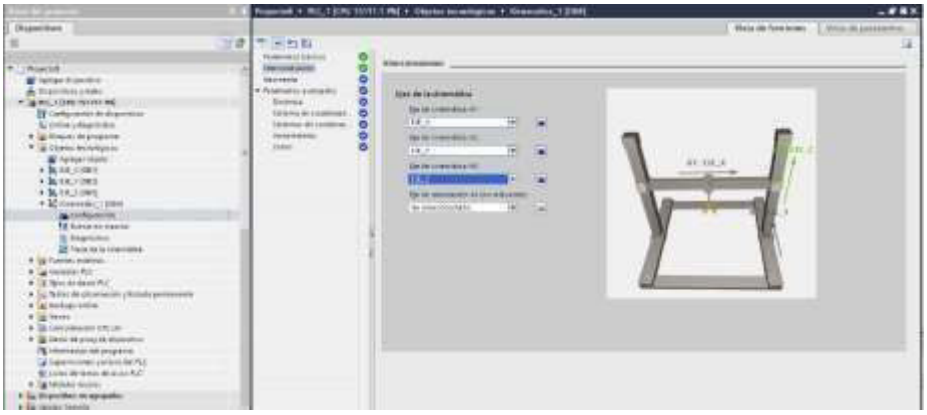


Figura 5 – Simulación cadena cinemática tia portal

2.4. Control del robot en TIA PORTAL

Para poder realizar los posicionamientos de los ejes tales como home, reset, posiciones fijas o secuencias se necesita de bloques de programación en el PLC. Una vez programadas podrán ejecutarse de forma manual o automática desde los controles de la estación o de forma virtual. Lo bloques MC_Power, MC_Reset, MC_Home permiten realizar la programación y configuración del control de los ejes mediante Motion Control a través del PLC. Es necesario configurar estos tres bloques para cada uno de los ejes denominados X, Y, Z, como se puede apreciar en la Figura 6.

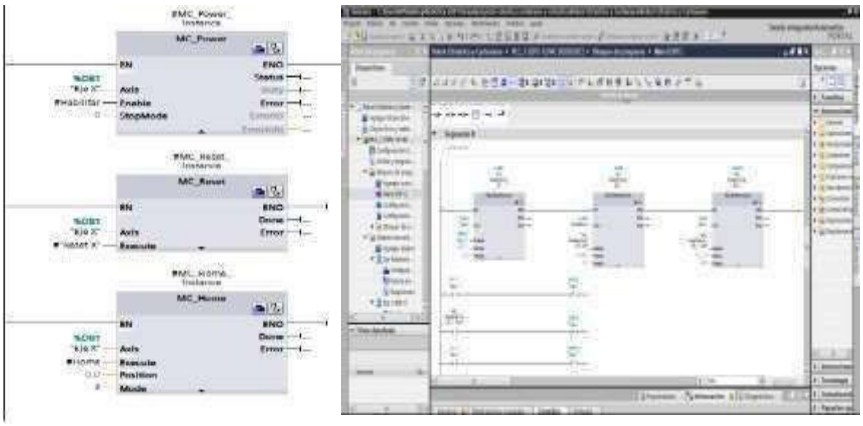


Figura 6 – Control de las funciones tecnológicas Motion Control

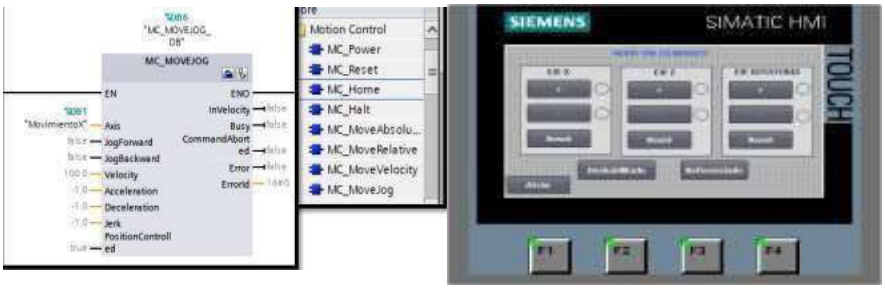


Figura 7 – Movimiento mediante JOG en TIA PORTAL

Ya declarados los bloques FB necesarios se procede a adaptarlos en el bloque principal o main con la finalidad de que estos sean ejecutados en el programa cuando se inicie. Además, hemos realizado la programación para dotar al sistema de un control automático y manual para lo cual es necesario declarar los objetos haciendo uso del bloque JOG, en este caso se utiliza MC_MOVEJOG para cada uno de los ejes, estos objetos se asignan con los movimientos mediante la declaración de variables X, Y, Z con el AXIS. Una vez realizada la declaración de los ejes es posible realizar programas para el control tanto

manual es decir movimiento eje a eje una determinada distancia y con un sentido o mediante secuencias automáticas que permiten al sistema robotizado desplazarse a posiciones previamente definidas y calculadas. Para la comprobar la programación se utiliza el HMI del programa TIA PORTAL (véase Figura 7).

3. Software

3.1. Interfaz de Comunicación

En el diagrama de flujo de la Figura 8 se detalla la aplicación para el control del sistema robotizado en sus dos modalidades.

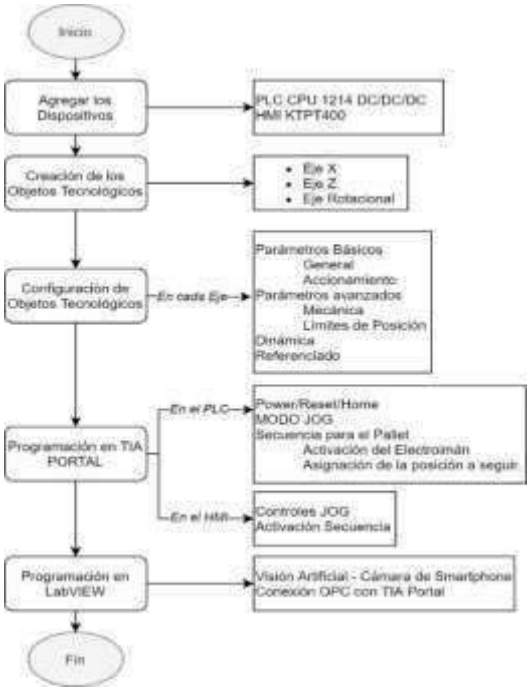


Figura 8 – Flujograma de la lógica de programación utilizada

Para la forma manual existen dos vías de accionamiento; por una parte, la vía virtual mediante una interfaz HMI y por otra parte, a través de un control joystick. La comunicación entre la interfaz HMI, el control joystick y el robot cartesiano se lo realiza mediante OPC-DA y los drivers TB6600 son controladores de motores paso a paso. Estas conexiones son compatibles con microcontroladores que pueden emitir una señal de pulso digital de 5V. Estos drivers cuentan con una fuente de alimentación de gran alcance (9 a 24VDC), que genera 4A como corriente máxima, siendo suficiente para la mayoría de los motores paso a paso.

3.2. Comunicación del sistema de visión artificial y el sistema robótico

Para este sistema se realizará el procesamiento de imágenes mediante el software LabVIEW. Se declara la inicialización de un dispositivo de visualización (cámara y/o videocámara) mediante el comando "Session In" y posteriormente se active la cámara mediante el comando "IMAQdex Open Camera VI". Una vez se tiene el área de la imagen que se desea analizar con "IMAQdx Configure Grab VI", se utiliza el comando "IMAQdx Grab2 VI" que se encarga de realizar una captura de la misma. Para el procesamiento de las imágenes se empleará el comando "IMAQ ColorLearn VI" para obtener las características del color de las cajas (obsérvese Figura 9). Para el procesa- miento de las imágenes, se obtienen sus características a través del comando "In Range and Coerce Function", que arroja un valor numérico que representa a un determinado color y se obtiene mediante el comando "Index Array". Para este caso de estudio el color numérico para el reconocimiento de colores está comprendido entre el rango de valores de 0,4 hasta el valor 1,1 (obsérvese la Figura 10). Este valor se traslada a la programación de TIA Portal para indicar la presencia de la pieza a paletizar e iniciar la secuencia. La comunicación efectuada se desarrolla con un servidor OPC, en este caso se hace uso de KEPServerEx, con ellos se transfiere el valor booleano desde LabVIEW a TIA portal.

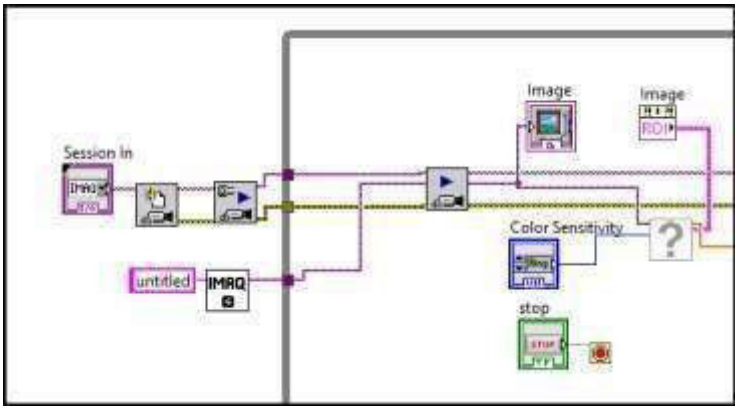


Figura 9 – Algoritmo desarrollado para la detección de colores

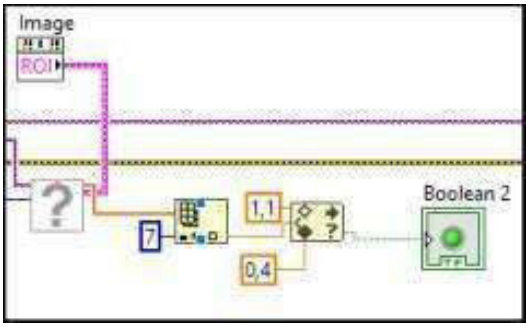


Figura 10 – Activación de colores

Cuando esta señal es recibida, el PLC active la banda transportadora, y al mismo tiempo cualquiera de los dos contadores, dependiendo si el objeto es verde o rojo. A continuación, mediante comparadores lógicos, se activa el sistema robótico y la secuencia adecuada para ubicar el objeto en las coordenadas configuradas realizando un paletizado dividiéndolos por colores. Para el accionamiento virtual, por medio de la interfaz HMI se emplean 6 botones con el propósito de controlar el sentido de giro y el eje correspondiente (eje X, Y, Z) obsérvese Figura 11 (a). Por otro lado, para el control físico (joystick), se realize su programación en LabVIEW, mediante el comando "device index" para seleccionar el dispositivo de mando que se utilizará en el sistema. Este dispositivo de control se activa mediante el comando "Initialize Joystick VI" y sus datos son almacenados en un array mediante el comando "Acquire Input Data VI" para la activación del movimiento deseado por el usuario obsérvese Figura 11 (b). En esta interfaz el usuario determina si desea realizar un proceso automático o manual y de la misma manera monitorea el estado del proceso de clasificado de cajas mediante el reconocimiento de imágenes desde una zona remota (véase Figura 12).

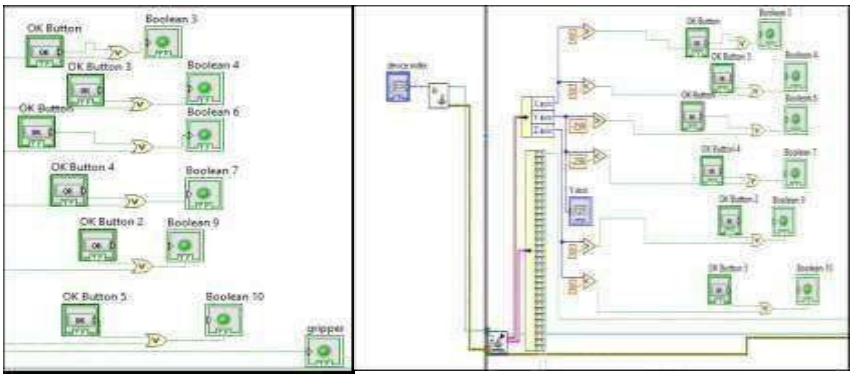


Figura 11 – (a) Programación del control virtual, (b) Programación del control físico

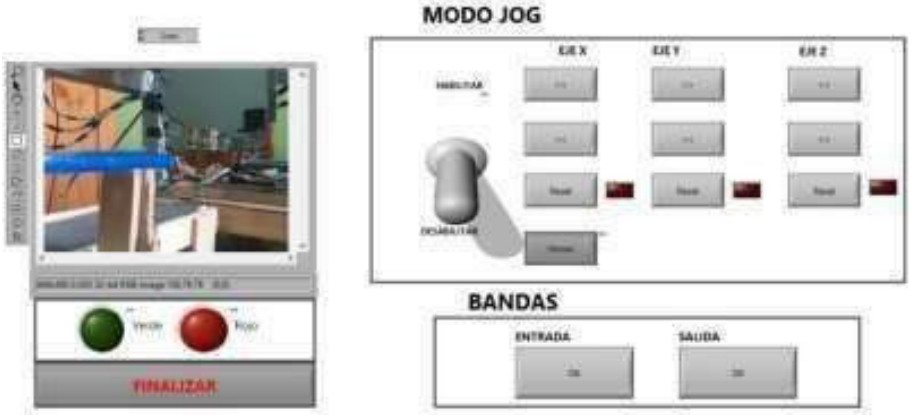


Figura 12 – Interfaz de control y monitorización desarrollada en LabVIEW

4. Resultados Experimentales

El resultado del sistema implementado y los ejes del sistema se puede observar en la Figura 13 (a). En la Figura 13 (b) se puede apreciar la interfaz gráfica que controla la identificación de piezas y mediante el sistema de visión artificial es capaz de detectar el color de cajas que ingresan al proceso.



Figura 13 – (a) Robot cartesiano; (b) Programación gráfico visual en LabVIEW

Posteriormente en base a la programación realizada se ejecuta un proceso de paletizado a zonas previamente configuradas, analizadas y comprobadas. La comunicación realizada hace uso de diferentes protocolos para el control de la estación robotizada y su aplicación con visión artificial. El sistema completo que se aprecia en la zona izquierda de la figura, comprobando que cuando una caja es ubicada en el lugar de recogida, activa la secuencia de arranque de todo el sistema de paletizado, en este caso el robot comienza la ejecución de su secuencia programado.

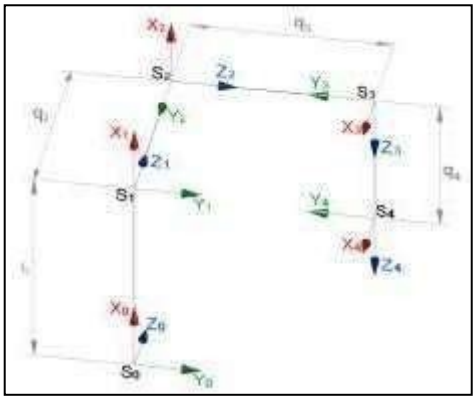


Figura 14 – Detalle de sistemas de referencia - robot cartesiano

Con la ayuda del análisis cinemático se pueden determinar las trayectorias que debe realizar el robot cartesiano. Para un mejor entendimiento de la cadena cinemática que tiene el robot, se traza un sistema de referencia en cada eslabón del robot y demás parámetros geométricos con el fin de conocer la orientación y posición final del extremo final del robot.

Se toma los valores de las distancias y ángulos existentes entre los sistemas referenciales para así obtener la posición y orientación de la herramienta final mediante cinemática directa. En la Figura 14 se hace detalles del sistema de referencia del robot cartesiano y en la Tabla 2 se especifica los datos antes mencionados para el cálculo de la posición final mediante matrices de transformación homogénea DH de cada articulación.

Sistema	Z		X		Referencia
	Theta (°)	d (mm)	a (mm)	Alpha (°)	
${}^{0}A_{1}$	0	0	l_1	0	
${}^{1}A_{2}$	0	q_2	0	-90	
${}^{2}A_{3}$	90	q_3	0	-90	
${}^{3}A_{4}$	0	q_4	0	0	

Tabla 2 – Parámetros DH - robot cartesiano

4.1. Cinemática Directa

Matrices de transformación homogénea DH de cada articulación

$$ {}^{0}A_{1} = \begin{vmatrix} 1 \to 0 \to 0 \to l_1 \\ 0 \to 1 \to 0 \to 0 \\ 0 \to 0 \to 1 \to 0 \\ 0 \quad 0 \quad 0 \quad 1 \end{vmatrix} \qquad {}^{2}A_{3} = \begin{vmatrix} 0 \quad 0 \to 1 \to 0 \\ 1 \quad 0 \to 0 \to 0 \\ 0 \quad 1 \to 0 \to q_3 \end{vmatrix} $$

$$ 1 \quad 0 \quad 0 \quad 0 \qquad\qquad 1 \quad 0 \quad 0 \quad 0 $$

$$ {}^{1}A_{2} = \begin{matrix} 0 \to 0 \to 1 \to 0 \\ 0 \to -1 \to 0 \to q_2 \\ 0 \to 0 \to 0 \to 1 \end{matrix} \qquad {}^{3}A_{4} = \begin{matrix} 0 \to 1 \to 0 \to 0 \\ 0 \to 0 \to 1 \to q_4 \\ 0 \to 0 \to 0 \to 1 \end{matrix} $$

Matriz de transformación homogénea final

$$ T = {}^{0}A_{6} = {}^{0}A_{1} * {}^{1}A_{2} * {}^{2}A_{3} * {}^{3}A_{4} $$

$$T = \begin{matrix} 0 & 0 & -1 & l_1 - q_4 \\ 0 & -1 & 0 & q_3 \\ -1 & 0 & 0 & q_2 \\ 0 & 0 & 0 & 1 \end{matrix}$$

A partir de la obtención de los parámetros de Denavit Hartenberg de la cadena cinemática que tiene el robot, posicionamos cada eslabón y demás parámetros geométricos en Home, con el fin de calcular la orientación y posición final del extremo final del robot.

Matrices de transformación homogénea DH de cada articulación en Home

$$^{0}A_{1} = \begin{vmatrix} 1 & 0 & 0 & 210 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} \quad ^{2}A_{3} = \begin{vmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 210 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

$$^{1}A_{2} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 300 \\ 0 & 0 & 0 & 1 \end{vmatrix} \quad ^{3}A_{4} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 150 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

Con la información obtenida se procede a realizar los análisis del sistema implementado basados en los parámetros de Denavit–Hartenberg (D-H) para comprobar que las posiciones asignadas desde el programa fueron las correctas. Además, se realiza la comparación de los valores obtenidos con la herramienta ARTE de MATLAB. Teniendo los valores de los parámetros D-H y los resultados de las columnas de la submatriz de transformación homogénea, un observador localizado en el origen del sistema puede ver cómo están orientados los ejes x, y, z del sistema. Así mismo se corrobora el desplazamiento en coordenadas cartesianas de la posición de la herramienta final del sistema respecto a la referencia de la base del robot, para realizar un movimiento específico a un punto determinado de la zona de paletizado de cajas como se puede ver en la Tabla 3.

1 Cálculo					**Comprobación mediante softwareMatlab**
	0	0	-1	60	
T	0	-1	0	210	
=	-1	0	0	300	
	0	0	0	1	

Tabla 3 – Matriz Final de transformación homogénea DH del robot

Bajo el funcionamiento y aplicación de una encuesta basada en la facilidad de uso y dinámica de programación a estudiantes de 8vo semestre de la cátedra automatización y robótica, se obtuvo como resultado un porcentaje mayor a 95% satisfactoriamente comprobando la flexibilidad y robustez del Sistema, además del rápido entendimiento de los estudiantes.

5. Conclusiones

El sistema robotizado es una alternativa de estudio durante el proceso de formación de los estudiantes de las carreras de automatización y robótica, debido a que es un sistema similar a los reales y con equipos que forman parte del equipamiento de las diferentes empresas del sector industrial. Al ser un sistema de bajo coste ayuda en gran medida a la factibilidad de uso de los estudiantes. La configuración del robot cartesiano no representa alto grado de complejidad para determinar la cinemática directa, simplemente se necesita conocer las medidas de los eslabones, coordenadas en el sistema de referencia trazado desde la ubicación Home del robot, y con estos valores se determina qué distancia se debe desplazar cada uno de los eslabones. La implementación de sistemas de monitorización permite comprobar la ejecución de los procesos y la implementación de sistemas HMI tanto en tia portal como en labview permite al estudiante controlar el proceso de diferentes maneras sean estás directamente en el proceso o manejar a distancia. La simulación de las cadenas cinemáticas que ofrecen estás nuevas plataformas de programación como es el caso de siemens fortalece el aprendizaje y entendimiento. La inserción de nuevas tecnologías como la inteligencia artificial permiten que los procesos industriales puedan mejorar y optimizar su producción que hace pocos años era tarea del ser humano. Los múltiples avances en técnicas de detección permiten mejorar habilidades de los estudiantes que realizarán tareas dentro de las empresas y de la vida cotidiana industrial. Como trabajos futuros, se continuará realizando aplicaciones mediante diferentes tipos de inteligencia artificial y redes neuronales para el mejor entendimiento de los estudiantes.

Referencias

Detez L, G. L. (Sep 3-2019). A Psychophysiological and Behavioural Study of Slot Machine Near-Misses Using Immer-sive Virtual Reality. J Gambl Stud, 929-944. https://doi.org/10.1007/s10899-018-09822-z.

Franklin Salazar, J. B. (2019). Teleoperation and Remote Monitoring of a ScorBot ER-4U Robotic Arm in an Academic Environment. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 40-45.

Gassert, R. D. (2018). Rehabilitation robots for the treatment of sensorimotor deficits: a neurophysiological perspective. J NeuroEngineering Rehabil 15, 46. https://doi.org/10.1186/s12984-018-0383-x.

Jonathan Talahua, J. B. (2021). Facial Recognition System for People with and without FaceMask in Times of the COVID-19 Pandemic. Sustainability 2021,13,6900. https://doi.org/10.3390/su13126900.

Jorge Aroca, R. R. (2018). Kinematic Model of the Scorbot 4PC ManipulatorImplemented in Matlab's Guide. Contemporary Engineering Sciences,11, 183-199. https://doi.org/10.12988/ces.2018.8112.

Marcin Szuster, P. G. (2016). Approximate Dynamic Programming in Tracking Control of a Robotic Manipulator. International Journal of Advanced Robotic Systems 13. https://doi.org/10.5772/62129.

Matthew Johnson, M. B. (2017). High-Resolution Underwater Robotic Vision-Based Mapping and Three-Dimensional Reconstruction for Archaeology. Journal of Fields Robotics. https://doi.org/10.1002/rob.21658.

Radityo Wibisono, N. S. (2018). Automation Canal Intake Control System Using Fuzzy Logic and Internet of Things (IoT). 6th International Conference on Information and Communication Technology (ICoICT), 233-238. https://doi.org/10.1109/ICoICT.2018.8528756.

Štefan. Kozák, E. R. (2018). Research and education for industry 4.0: Present development. 2018 Cybernetics & Informatics (K&I), 1-8. https://doi.org/10.1109/CYBERI.2018.8337556.

Zoran Salcic, U. D.-Y.-k. (2019). Designing Dynamic and Collaborative Automation and Robotics Software Systems. IEEE Transactions on Industrial Informatics, 540- 549. https://doi.org/10.1109/TII.2017.2786280.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 08/10/2021
Aceitação/Acceptance: 06/01/2022

Perfil Psicológico del Líder: Un Estudio Exploratorio con Estudiantes de la Carrera de Administración de Negocios Internacionales

Ivan Iraola-Real[1], Alonso Iraola-Arroyo[2], Daniel Iraola[3], Keita Nakamine[4]

iiraola@uch.edu.pe; air_2025@outlook.com; diraolamiranda@gmail.com; keitanakamine@gmail.com

[1] Universidad de Ciencias y Humanidades, Los Olivos, Lima 15314, Lima, Perú.

[2] Universidad Tecnológica del Perú, Ate, Lima 15487, Lima, Perú.

[3] Universidad del Pacífico, Jesús María, Lima 15072, Lima, Perú.

[4] Pontificia Universidad Católica del Perú, San Miguel, Lima 15088, Lima, Perú.

Pages: 237-248

Resumen: El liderazgo es una competencia gerencial asociada a otras competencias que resultan ser necesarias para el desarrollo económico en la pos pandemia. De acuerdo a ello, el estudio presente tiene como objetivo analizar las competencias gerenciales de la iniciativa, el análisis situacional, la toma de decisiones y la planificación y su relación predictiva con el liderazgo en estudiantes de administración de negocios internacionales de una universidad privada de Lima – Perú. La muestra fue de 152 estudiantes, 70 eran mujeres (46.1%) y 82 varones (53.9%) quienes oscilaban entre 16 a 36 años (M_{edad} = *18.86, DE = 3.70*). Los resultados muestran que los estudiantes no sienten seguridad del desarrollo de sus competencias gerenciales. Además, la iniciativa, el análisis contextual, la planificación y la toma de decisiones se relacionan significativamente con el liderazgo, pero solo la iniciativa y la toma de decisiones predicen el desarrollo de la competencia del liderazgo.

Palabras-clave: Liderazgo, planificación, toma de decisiones, competencia profesional.

Psychological Profiles of Leaders: An Exploratory Study with Students of the International Business Administration Career

Abstract: Leadership is a managerial skill associated with other skills that turn out to be necessary for post-pandemic economic development. Accordingly, the present study aims to analyze the managerial competencies of the initiative, situational analysis, decision making and planning and their predictive relationship with leadership in international business administration students from a private university in Lima. - Peru. The sample consisted of 152 students, 70 were women (46.1%) and 82 men (53.9%) who ranged from 16 to 36 years old (Mage = 18.86, SD = 3.70). The results show that students do not feel secure in the development

of their managerial skills. Furthermore, initiative, contextual analysis, planning, and decision-making are significantly related to leadership, but only initiative and decision-making predict the development of leadership competency.

Keywords: Leadership, planning, decision-making, occupational qualifications.

1. Introducción

La pandemia a nivel mundial no debió ser una situación sorpresiva, la sociedad debió estar prevenida para evitar las pérdidas de vidas y del impacto económico en las diversas instituciones porque no fue ni es la única amenaza que el mundo enfrenta (Blandford & Thome, 2020). Es así que desde el 2020, diversas empresas a nivel mundial se fueron preparando para atender a las necesidades humanas para la fase pos pandémica. Para lograr ello, analizaron el riesgo de reactivar sus propuestas de negocios y de garantizar su éxito apelando al talento de sus trabajadores (Joly, 2020). De forma similar, a nivel de los líderes, en el actual contexto pos pandémico exige que se den soluciones organizacionales eficientes de acuerdo a la nueva normalidad; siendo necesario desarrollar y practicar un liderazgo más holístico que contemplen aspectos axiológicos, relacionales, la toma de decisiones de acuerdo al contexto y la capacidad de análisis desde ópticas diferentes (Bleich & Bowles, 2021). Prácticas basadas en la integridad, colaboración y bienestar personal (Ryan & Goldingay, 2022). Así, desarrollar competencias enfocadas en el desarrollo de los trabajadores que garanticen el crecimiento atendiendo las demandas del cliente (Anderson, Bieck & Marshall, 2021).

Este trabajo en equipo, resulta ser esencial porque debido a la pandemia Covid-19, se necesita descentralizar el liderazgo compartiendo la dirigencia con el equipo (Edge, 2022). Tradicionalmente, el liderazgo ha sido enfocado como la capacidad de dirigir a un equipo u organización para posicionar de manera eficiente a una empresa (Tripathi & Agrawal, 2014). Pero, en contextos actuales se requiere transformar la visión individual del líder por una visión colaborativa (Ryan & Goldingay, 2022). Lo cual, se sustenta en la necesidad que el líder se enfoque en actividades cada vez más demandantes como, potenciar sus propias competencias como su iniciativa, enfocarse más en el análisis del contexto nacional e internacional, en tomar decisiones objetivas y en la planificación. Competencias que se pueden desarrollar desde las universidades de forma equitativa, garantizando futuros líderes eficientes desde el plano académico y orientados al servicio social (Allen, Butler-Henderson, Reupert, Longmuir & Finefter-Rosenblud, 2021).

2. Marco conceptual

2.1. Desarrollando el liderazgo en las universidades

Es evidente que la pandemia dejó tres imperativos en la sociedad, uno de ellos es hacer transformaciones en la política, reconstruir la economía y garantizar la equidad social; demandas en las que la educación universitaria debe responder con sus respectivas adecuaciones en la que la labor docente se asocia creativamente a la industria (Blandford & Thome, 2020). Además, desde las universidades se debe lograr un liderazgo inclusivo, un liderazgo holístico que valora las experiencias, el capital intelectual y las motivaciones de los integrantes del equipo, con la finalidad de compartir la dirigencia, migrando

del enfoque predominante del líder como individuo a un liderazgo colaborativo como práctica pedagógica (Ryan & Goldingay, 2022).

Estos cambios en el liderazgo son coherentes en el contexto pos pandémico en el que es un riesgo individualizar el liderazgo (Edge, 2022). Y ante este contexto, las universidades han respondido desarrollando programas educativos orientados a la formación de competencias desde la Declaración de Bolonia en el que se acordó educar profesionales para el campo laboral y para la internacionalización (Beneitone, Esquetini, González, Marty, Siufi & Wagenaar, 2007). Estos programas educativos universitarios desarrollan las habilidades procedimentales y cognitivas de los futuros profesionales, específicamente en los administradores, quienes se educan para ser competentes en su función gerencial en un ambiente económico dinámico (Lombana, Cabeza, Castrillón & Zapata, 2014).

Y de forma particular, las universidades peruanas desarrollan una educación por competencias que garanticen la calidad educativa (British Council, 2016). De esta manera son organizadas y monitoreadas por el Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa (SINEACE, 2016) quien propone gestionar los perfiles profesionales de egreso basados en aprendizajes y evaluaciones por competencias que sean verificables al culminar los estudios universitarios. Así, las universidades han desarrollado programas curriculares orientadas al desarrollo de competencias gerenciales implementando asignaturas de planificación, toma de decisiones, investigación, realidad social y liderazgo, las que se acompañan de foros, congresos, jornadas, etc. En las que el estudiante puede poner en práctica lo aprendido.

2.2. Competencias gerenciales y el liderazgo

Las competencias gerenciales son aquellas habilidades que desarrollan las personas para aplicar sus destrezas cognitivas en labores organizacionales en diversos contextos (Lombana, et al., 2014). Tradicionalmente, estas competencias demandan el saber hacer, el saber conocer, saber ser éticamente y el saber conocerse (Bédard, 2003). De esta manera, las competencias gerenciales involucran los conocimientos, los comportamientos y las actitudes que una persona posee para desempeñarse con efectividad en una empresa (Sánchez-Valbuena, Sánchez-González & Pinedo-Frías, 2020). Es así que entre las competencias gerenciales se encuentran la iniciativa, la capacidad de investigar para aprender y actualizarse constantemente (Lombana, et al., 2014), de tomar decisiones (Saaty, 2018), la capacidad de planificar (Tripathi & Agrawal, 2014), y el liderazgo como la competencia para dirigir una empresa y auto dirigirse con perspectivas de futuro (Steyn & Van Staden, 2018).

Entre estas competencias, la iniciativa se refiere al comportamiento emprendedor asociado a la motivación intrínseca para iniciar labores y prevenir problemas, por lo que resulta esencial para el logro de objetivos en el campo empresarial (Frese & Fay, 2001). Luego, la competencia del análisis situacional, permite investigar lo que acontece en el contexto porque permite tener una ventaja ante los competidores con una perspectiva de futuro (Tripathi & Agrawal, 2014). Por otro lado, la competencia de la planificación consiste en organizar las actividades para optimizar el desempeño empresarial direccionando proyectos de acuerdo a los objetivos institucionales (Steyn & Van Staden, 2018). Además, la toma de decisiones es la competencia que se caracteriza por la

habilidad de elegir de acuerdo a las prioridades empresariales (Saaty, 2018). Finalmente, el liderazgo es la competencia caracterizada por la habilidad de dirigir una organización con una perspectiva futura para garantizar su posicionamiento. El liderazgo se asocia a la planificación eficiente y al análisis del contexto para lograr ventajas competitivas (Tripathi & Agrawal, 2014). Al mismo tiempo, el líder debe saber tomar decisiones de acuerdo a los objetivos estratégicos (Saaty, 2018). Por estos motivos, es importante desarrollar estas competencias gerenciales en los futuros profesionales y líderes. Por ejemplo: la iniciativa favorece la ejecución acciones sin esperar alguna orden (Frese & Fay, 2001). De esta manera investigar el contexto que favorecerá a la actualización profesional y conocimiento del entorno empresarial (Lombana, et al., 2014). En función a esto planificar acciones tácticas para optimizar el desempeño organizacional (Tripathi & Agrawal, 2014). Y desde luego, en las universidades se deben diseñar estrategias que garanticen que los profesionales poseen un adecuado juicio para tomar decisiones (Bazerman & Moore, 2013).

De acuerdo a lo analizado, la investigación presente se orienta según el siguiente objetivo: analizar las competencias gerenciales de la iniciativa, el análisis situacional, la toma de decisiones y la planificación y su relación predictiva con el liderazgo en estudiantes de administración de negocios internacionales de una universidad privada de Lima – Perú.

3. Metodología

Según la temática propuesta, el equipo investigador decidió abordar el estudio de acuerdo a un enfoque cuantitativo. Debido a que son estudios que permiten analizar la realidad con instrumentos estandarizados y obtener resultados que se puedan generalizar (Leavy, 2017). Del mismo modo, para obtener información más exacta, el estudio es de tipo correlacional predictivo (Bingham & Fry, 2010). De esta manera, identificar los factores psicológicos asociados a las competencias gerenciales que anticipen el desarrollo del liderazgo en los participantes.

3.1. Muestra

Se tuvo acceso a los estudiantes de los cursos lectivos virtuales de una universidad privada de Lima – Perú. Por estos motivos, la selección de los participantes fue mediante un muestreo no probabilístico por conveniencia, debido a que permiten realizar estudios con informantes de fácil acceso (Saumure & Given, 2008). Así, se pudo contar con el apoyo voluntario de 152 estudiantes universitarios de la carrera profesional de administración de negocios internacionales. Todos los participantes eran peruanos, de la misma universidad, cursaban del séptimo al décimo ciclo de estudios y de los cuales 70 eran mujeres (46.1%) y 82 varones (53.9%). De ellos, 112 participantes (75.7%) eran de Lima (ciudad capital del Perú) y 36 (24.3%) procedían de las provincias peruanas. Respecto a la edad, oscilaban entre 16 a 36 años ($M_{edad} = 18.86, DE = 3.70$).

3.2. Instrumentos

Escala de Aptitudes para el Liderazgo (elaboración propia). Es un instrumento unidimensional que permite que el evaluado responda afirmaciones que le indican si posee aptitudes personales como líder. Esta escala tiene un total de tres ítems con siete opciones de

respuesta en escala de Likert (1 "Totalmente en desacuerdo" – 7 "totalmente de acuerdo"). Por ejemplo, el segundo ítem plantea lo siguiente: "*Se me hace fácil ser el que organiza un equipo de trabajo*". Esta escala se diseñó con una cantidad mínima de ítems para no agotar a los encuestados. Pero al mismo tiempo, el número de ítems se respalda en los criterios de Streiner (1994) quien plantea que una escala debe contener un mínimo de tres ítems para lograr óptimos niveles de confiabilidad del coeficiente de consistencia interna del Alfa de Cronbach. En la Tabla 1 se puede apreciar que la escala pasó satisfactoriamente la prueba de ajuste muestral de Kaiser-Meyer-Olkin (KMO) con una puntuación de .69 y el Test de Esfericidad de Bartlett fue significativo ($\chi^2 = 119{,}028$, $gl = 3$, $p < .001$), demostrando así que la escala es válida (Field, 2009). Y de acuerdo a los análisis de confiabilidad, el coeficiente del Alfa de Cronbach fue de .77, demostrando adecuados niveles de confiabilidad para continuar con los análisis del estudio (Aiken, 2002).

Escala de Competencias Gerenciales (elaboración propia). Es un instrumento multifactorial que evalúa el nivel de desarrollo de cuatro competencias gerenciales: análisis situacional, iniciativa, planificación y toma de decisiones. Esta escala tiene un total de 12 ítems con siete opciones de respuesta en escala de Likert (1 "Totalmente en desacuerdo" – 7 "totalmente de acuerdo"). Por ejemplo, el séptimo ítem plantea lo siguiente: "*Prefiero organizarme estableciendo metas para lograr*". Cada una de las competencias gerenciales posee tres ítems, establecidos de acuerdo a los criterios de Streiner (1994) como cantidad mínima confiable. De forma similar a la primera escala, en la Tabla 1 se puede apreciar que la escala pasó satisfactoriamente la prueba del KMO con una puntuación de .85 y el Test de Esfericidad de Bartlett fue significativo ($\chi^2 = 591{,}219$, $gl = 66$, $p < .001$), demostrando un adecuado nivel de validez (Field, 2009). Y el coeficiente del Alfa de Cronbach fue de .85, evidenciando ser confiable para el estudio (Aiken, 2002).

Escala	Prueba de Kaiser Meyer y Olkin (Validez)	Coeficiente Alfa de Cronbach
Escala de Aptitudes para el Liderazgo	.69 (p<.000)	.77
Escala de Competencias Gerenciales	.85 (p<.000)	.85

Tabla 1 – Análisis de Validez y Confiabilidad de la Escala

La aplicación de ambos instrumentos se realizó de acuerdo a los criterios éticos de investigación mediante la participación voluntaria y al mismo tiempo conservando el anonimato de los encuestados (Goodwin, 2010). De esta forma, se procedió según la Ley Peruana de Protección de Datos Personales Nro. 29733 (Congreso de la República del Perú, 2013).

4. Resultados

Una vez confirmado los niveles óptimos de validez y confiabilidad de los instrumentos; a continuación, se proceden a realizar los estudios de los estadísticos descriptivos, los análisis exploratorios y los análisis de correlaciones predictivas.

4.1. Análisis de Estadísticos Descriptivos

Se analizaron de los estadísticos descriptivos para identificar el nivel de las medias alcanzado en las variables de estudio. Así, en la Tabla 2 se observa que todas las variables poseen un valor redondeado de cinco (5) oscilando entre las medias de 4.88 para la variable análisis situacional y 5.31 para la variable iniciativa. De esta manera, la variable liderazgo obtuvo una media de 5.24. Esto indica que los estudiantes encuestados se perciben en "relativo acuerdo" respecto al logro personal de las variables analizadas. Demostrando cierto grado de inseguridad sobre el logro de las competencias gerenciales y de liderazgo.

Variables	N	Mínimo	Máximo	Media	D. E.
Iniciativa	152	2	7	5,31	,955
Análisis Situacional	152	2	7	4,88	1,071
Planificación	151	1	7	5,34	1,069
Toma de Decisiones	150	1	7	4,94	1,045
Liderazgo	151	2	7	5,24	1,125

Tabla 2 – Análisis de Estadísticos Descriptivos (Medias)

4.2. Análisis Exploratorios con los Boxplot

Al obtener el nivel de las medias a nivel general de toda la muestra, surgió la necesidad de explorar la base de datos para identificar casos particulares con avances significativos o déficit en el desarrollo del liderazgo. Así, se decidió emplear los análisis con los diagramas de cajas (Helsel, 2011).

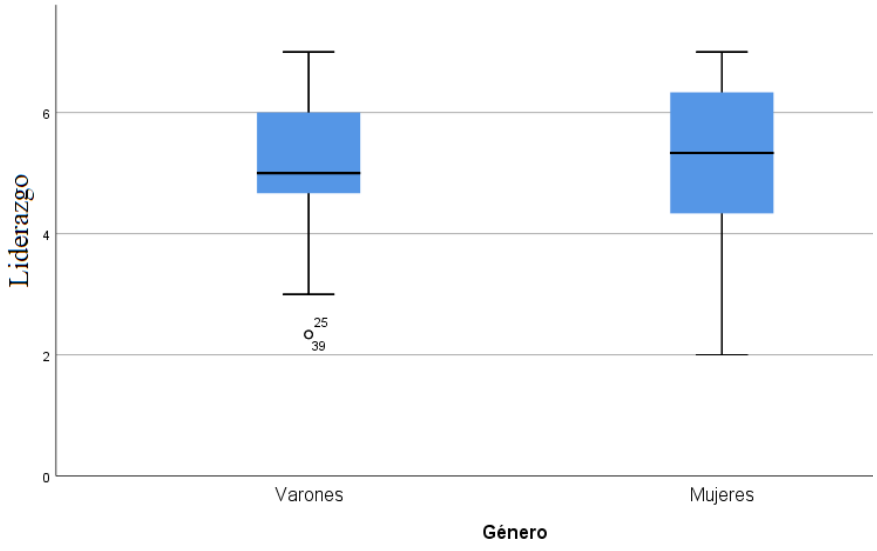


Figura 1 – Diagrama de Cajas para el análisis exploratorio de casos atípicos o extremos.

En el caso de los varones, este estadístico evidenció que los casos centrales (la caja); es decir un total de 41 (50%) varones se ubican entre los valores 4 y 6, equivalentes al "ni de acuerdo ni desacuerdo" y "de acuerdo". Luego, 25% de ellos, aproximadamente 20 varones se ubicaron entre el nivel 6 y 7, equivalentes al "de acuerdo" y "totalmente de acuerdo", siendo los que presentaron los niveles más altos de liderazgo. Particularmente, se identificaron 2 casos a típicos (25 y 39) próximos al nivel 2 equivalente al "desacuerdo" en haber desarrollado la competencia del liderazgo. En el caso de las mujeres, en el diagrama de cajas se observa que los casos centrales (la caja); es decir un total de 35 (50%) mujeres se ubican entre los valores 4 y superando el valor 6, equivalentes al "ni de acuerdo ni desacuerdo" y "de acuerdo". Luego, 25% de ellas, aproximadamente 17 mujeres se ubicaron entre el nivel 6 y 7, equivalentes al "de acuerdo" y "totalmente de acuerdo", siendo los que presentaron los niveles más altos de liderazgo. Y, el 25% de ellas, aproximadamente 17 mujeres se ubicaron entre ligeramente cercanas al nivel 4 y 2, equivalentes al "ni de acuerdo ni desacuerdo" y "desacuerdo", siendo las que presentaron los niveles más bajos de liderazgo. En las mujeres no se evidencias casos atípicos (ver Figura 1).

4.3. Análisis de Relaciones entre Variables

A continuación, como parte de los análisis principales, se estudiaron las correlaciones con el *r* de Pearson; de esta manera, identificar el nivel de la correlación aplicando los criterios de Cohen (1992) que son idóneos para analizar ciencias sociales. Estos criterios consideran una relación leve si el coeficiente *r =.10 a .23*; moderada, si *r = .24 a .36*; y fuerte, si *r = .37 a más*. De acuerdo a estos criterios, en la Tabla 3 se observa que: la variable iniciativa, análisis situacional, planificación y toma de decisiones poseen una relación positiva, fuerte y significativa con el liderazgo. Es decir, todas las variables se relacionan de forma directamente proporcional, indicando que, a mayores niveles de iniciativa, de análisis situacional, de planificación y de toma de decisiones, habrá mayores niveles de desarrollo del liderazgo. Pero, por el contrario, los débiles niveles de iniciativa, de análisis situacional, de planificación y de toma de decisiones, se asociarán a menores niveles del liderazgo.

Variables		1	2	3	4	5
1	**Iniciativa**	1				
	Sig. (bilateral)					
	N	152				
2	**Análisis Situacional**	,41***	1			
	Sig. (bilateral)	,000				
	N	152	152			
3	**Planificación**	,58***	,45***	1		
	Sig. (bilateral)	,000	,000			
	N	151	151	151		
4	**Toma de Decisiones**	,51***	,34***	,46***	1	
	Sig. (bilateral)	,000	,000	,000		
	N	150	150	150	150	

Variables		1	2	3	4	5
5	**Liderazgo**	,57***	,39***	,42***	,48***	1
	Sig. (bilateral)	,000	,000	,000	,000	
	N	151	151	151	150	151

Nota: Las correlaciones son significativas si *** <.001, ** <.01, * <.05.

Tabla 3 – Análisis de relación entre variables

4.4. Análisis Predictivos (Regresiones Lineales Múltiples)

Una vez confirmadas las relaciones predictivas entre las variables se procedió a analizar el nivel predictivo (Bingham & Fry, 2010). De esta forma, en la Tabla 4 se aprecia que mediante el método introducir se ingresaron como variables predictoras a la iniciativa, el análisis situacional, la planificación y la toma de decisiones; y como variable dependiente al liderazgo. De esta manera se identificó que, de las cuatro competencias gerenciales, dos de ellas predicen positivamente al liderazgo. Se observa que la iniciativa (β = .37; p < .001) y la toma de decisiones (β = .22; p < .01) predicen de manera positiva al liderazgo. Sin embargo, el análisis situacional (β = *.14, p> .05*) y la planificación (β = *.05, p> .05*) no predicen al liderazgo.

Las variables explican el 37% de la varianza (R^2 = *.37*). Anova$^{Variable\ Dependiente:\ Liderazgo}$ (*Suma de cuadrados = 73.608, gl =4, f = 23.038, p <.001*$^{Variables\ Predictoras:\ Iniciativa,\ Análisis\ Situacional,\ Planificación,\ Toma\ de\ Decisiones}$).

Coeficientes[a]						
Modelo (Variables Predictoras)		**Coeficientes no estandarizados**		**Coeficientes estandarizados**	**t**	**Sig.**
		B	**Desv. Error**	**Beta**		
1	(Constante)	,784	,478		1,641	,103
	Iniciativa	,435	,101	,370	4,316	,000
	Análisis Situacional	,144	,079	,137	1,832	,069
	Planificación	,055	,090	,052	,612	,542
	Toma de Decisiones	,234	,084	,217	2,783	,006

a. Variable dependiente: Liderazgo

Tabla 4 – Análisis de regresión lineal múltiple

5. Discusión

La presente investigación analiza la relación predictiva entre las competencias gerenciales de la iniciativa, el análisis situacional, la planificación y la toma de decisiones con el liderazgo en una muestra de estudiantes de la carrera profesional de administración de negocios internacionales. El estudio se sustenta en la necesidad que las universidades presten atención al desarrollo de las competencias gerenciales y diseñen estrategias para lograrlas es los futuros profesionales (Bazerman & Moore, 2013).

Sabiendo que las competencias gerenciales requieren de la aplicación de destrezas en las actividades organizacionales (Lombana, et al., 2014); resulta esencial hacer un respectivo diagnóstico de las mismas en la muestra de estudiantes investigados. Por lo que, resulta preocupante que los participantes presenten niveles medios y estén en relativo acuerdo sobre el logro de su iniciativa, análisis contextual, planificación, toma de decisiones y de liderazgo. Siendo esta última en la que identificaron estudiantes con débiles niveles de logro. El motivo de la preocupación es que si los estudiantes no muestran seguridad y un adecuado logro de estas competencias no lograrán desempeñarse efectivamente en las empresas (Sánchez-Valbuena, et al., 2020), porque no se actualizarían según las demandas contextuales (Lombana, et al., 2014), no tomarían las decisiones objetivamente (Saaty, 2018), planificarían con dificultades (Tripathi & Agrawal, 2014), y no podrían liderar las organizaciones de manera eficiente (Steyn & Van Staden, 2018). Situación que debe ser resulta desde el interior de la universidad adecuando actividades curriculares y extracurriculares (Lombana, et al., 2014; SINEACE, 2016).

Además, se observa que, en los estudiantes de administración de negocios internacionales, las cuatro competencias gerenciales se relacionan con el liderazgo. Confirmando así los estudios de Tripathi y Agrawal (2014) quienes identificaron que el liderazgo está vinculado al análisis situacional y a la planificación, lo cual es adecuado para lograr ventajas competitivas. Que se observe este resultado permite reflexionar en la necesidad de desarrollar la toma de decisiones de acuerdo a los objetivos estratégicos (Saaty, 2018) y promover la iniciativa para emprender proyectos (Frese & Fay, 2001), porque así se favorecería al desarrollo del liderazgo. Pero, según los resultados de los análisis predictivos, es importante priorizar el desarrollo de la iniciativa y de la toma de decisiones. Es decir, desde la universidad se debe promover actividades que desarrollen en los estudiantes un objetivo juicio para tomar decisiones (Bazerman & Moore, 2013), porque de los futuros profesionales elegirán de acuerdo a las prioridades empresariales (Saaty, 2018). Además de, desarrollar la iniciativa como comportamiento emprendedor y preventivo para el logro de objetivos (Frese & Fay, 2001). De esta manera garantizar el perfil de líderes en los estudiantes de administración de negocios internacionales; desde luego, sin descuidar las actividades para incrementar el nivel de desarrollo de las competencias gerenciales en general para obtener resultados óptimos.

6. Conclusiones y trabajos futuros

El estudio permite concluir que los estudiantes de la carrera de administración de negocios internacionales han desarrollado cierto grado de competencias gerenciales como la iniciativa, el análisis contextual, la planificación, la toma de decisiones y el liderazgo. Sin embargo, ellos se auto perciben con cierto grado de inseguridad respecto al logro de las mismas. Luego, los análisis evidencian que las competencias gerenciales se vinculan con el liderazgo, pero al momento de definir cuáles de ellas predicen al liderazgo, solo la iniciativa y la toma de decisiones logran ser la base que anticipa el desarrollo de la competencia del liderazgo. Estos hallazgos permiten orientar las siguientes actividades: primero, a nivel educativo, desarrollar estrategias curriculares para incrementar el nivel de las competencias gerenciales en los estudiantes de la carrera de administración de negocios internacionales. Segundo, realizar una intervención psicopedagógica con los estudiantes que han reportado los niveles más débiles de liderazgo. Tercero, a nivel

investigativo, realizar estudios con muestras más amplias de estudiantes y docentes, estudiar otras muestras de otras carreras profesionales e incorporar metodologías de investigación cualitativas o mixtas para lograr resultados más completos en cuanto a las necesidades y condiciones para desarrollar el liderazgo.

Referencias

Aiken, R. (2002). *Psychological testing and assessment* (11th Ed.).Boston: Allyn & Bacon.

Allen, A., Butler-Henderson, K., Reupert, A., Longmuir, F., & Finefter-Rosenbluh , I. (2021). Work like a girl: Redressing gender inequity in academia through systemic solutions. *Journal of University Teaching & Learning Practice, 18*(3), 1-15. https://doi.org/10.53761/1.18.3.3

Anderson, C., Bieck, Ch. & Marshall, A. (2021). How business is adapting to Covid-19: Executive insights reveal post-pandemic opportunities. *Strategy & Leadership, 49*(1), 38 – 47. https://doi.org/10.1108/SL-11-2020-0140

Bazerman, M. & Moore, D. (2013). *Judgment in managerial decision making*. 8th ed. John Wiley & Sons.

Bédard, R. (2003). Los fundamentos del pensamiento y las prácticas administrativas. *AD-MINISTER*, (3), 68–88.

Beneitone, P., Esquetini, E., González, J., Marty, M., Siufi, G. & Wagenaar, R. (2007). Reflexiones y perspectivas de la Educación Superior en América Latina: Informe Final – Proyecto Tuning – América Latina 2004 – 2007. Recuperado de http://www.sg.inter.edu/uploads/UIPRSG/documentos/asuntos_academicos/RevisionPEG/Proyecto%20Tuning%20America%20Latina_Informe%20Final_Espanol_2007.pdf

Blandford, R. & Thome, K. (2020). Post – Pandemic science and education. *American Journal of Physics, 88*(7), 518 – 520. https://authors.library.caltech.edu/104005/1/10.0001390.pdf

Bleich, M. & Bowles, J. (2021). A model for holistic leadership in Post – Pandemic Recovery. Nurse Leader, 19(5), 479 – 482. https://doi.org/10.1016/j.mnl.2021.06.002

Bingham, N. & Fry, J. (2010). *Regression: Linear models in statistics*. New York: Springer.

British Council. (2016). *The Reform of the Peruvian University System: Internationalization, progress, challenges and opportunities*. https://www.britishcouncil.pe/sites/default/files/the_reform_of_the_peruvian_university_system_interactive_version_23_02_2017_fg.pdf

Cohen, J. (1992). A power primer, *Psychological Bulletin*., *112*(1), 155–159. https://doi.apa.org/doi/10.1037/0033-2909.112.1.155

Congreso de la República del Perú. (2013). Ley de Protección de datos personales. Ley N°. 29733. Lima. Perú. https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf

Edge, K. (2022). A tale of two leaders: Reflecting on senior co-leadership in higher education. In D. Netolicky (Ed.) Future alternatives for educational leadership. Diversity, inclusion, equity and democracy (1st ed., pp.135-140). Routledge. https://doi.org/10.4324/9781003131496-13

Field, A. (2009). *Discovering statistics using SPSS* (3era Ed.). Lóndres: Sage Publications.

Frese, M. & Fay, D. (2001). Personal initiative: An active performance concept for work in the 21st century, *Research in Organizational Behavior*., 23,133–187.

Goodwin, J. (2010). Research in psychology: methods and design. Córdova, Brujas.

Helsel, D. (2011). Statistics for cosored environmental data using Minitab and R (2th Ed). Denver: Wiley.

Joly, H. (2020). Lead your team into a post-pandemic world, *Harvard Business Review*, 1–5. https://www.harvardbusiness.org/wp-content/uploads/2020/05/HBR-Lead-Your-Team-Into-a-Post-Pandemic-World.pdf

Leavy, P. (2017). *Research Design: Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches*. London: The Guilford Press.

Lombana, J., Cabeza, L., Castrillón, J., & Zapata, Á. (2014). Formación en competencias gerenciales. Una mirada desde los fundamentos filosóficos de la administración. *Estudios Gerenciales, 30*(132), 301–313. doi:10.1016/j.estger.2014.01.017

Ryan, J., & Goldingay, S. (2022). University leadership as engaged pedagogy: A call for governance reform. *Journal of University Teaching & Learning Practice, 19*(1), 122-139. https://doi.org/10.53761/1.19.1.08

Saaty, T. (2018). Decision making with the analytic hierarchy process. *Int. Services Sciences., 1*, 83–394.

Sánchez-Valbuena, I., Sánchez-González, J., & Pinedo-Frías, A. (2020). Competencias Gerenciales Factor de Éxito en Empresas de Servicios Públicos. Saber, Ciencia y Libertad, 15(2), 74–90. https://doi.org/10.18041/2382- 3240/saber.2020v15n2.6716

Saumure, K. & Given, L. (2008). *Convenience Sample*. In The SAGE Encyclopedia of Qualitative Research Methods. Thousand Oaks, CA: Sage.

Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa. (2016). Modelo de Acreditación para Programas de Estudios de Educación Superior Universitaria. Lima. Perú, SINEACE.

Steyn, Z. & Van Staden, L. (2018). Investigating selected self-management competencies of managers. *Acta Commercii-Independet Research Journal in the Management Sciences, 18*(1), 1–10.

Streiner, D. (1994). Figuring out factors: the use and misuse of factor analysis, *Can Journal Psychiatry*, *39*, 135-40.

Tripathi, K. & Agrawal, M. (2014). Competency based management in organizational context: A literature review. *Global Journal of Finance and Management.,* *6*(4), 349–356.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 23/10/2021
Aceitação/Acceptance: 28/01/2022

Evaluación de la Gestión Virtual Educativa en Ingeniería Industrial: Una Experiencia en el Contexto de Enseñanza Remota de Emergencia

Ivan Iraola-Real[1], Alonso Iraola-Arroyo[2]

Ivanir701@hotmail.com; air_2025@outlook.com

[1] Universidad de Ciencias y Humanidades, Los Olivos, Lima 15314, Lima, Perú.

[2] Universidad Tecnológica del Perú, Ate, Lima 15487, Lima, Perú.

Pages: 249-261

Resumen: Durante la pandemia Covid-19 las universidades adaptaron la gestión pedagógica y administrativa a la virtualidad. Sin embargo, países como Perú, que no habían avanzado mucho en educación virtual; esto fue una experiencia novedosa con aciertos y limitaciones. Según este análisis, el presente estudio tiene como propósito evaluar la eficiencia de la gestión educativa virtual de la carrera de ingeniería industrial de una universidad privada peruana en el contexto de educación remota de emergencia. Participaron 414 estudiantes de ingeniería industrial desde el primer al décimo ciclo de estudios entre 16 y 43 años (M_{edad} = *23.65, DE = 5.92*). Los resultados demostraron que los estudiantes evalúan como relativamente eficiente a la gestión virtual educativa y las dimensiones de recursos educativos virtuales, enseñanza virtual universitaria, gestión para la continuidad estudiantil, gestión administrativa, tutoría virtual e investigación. Pero, algunos ciclos de estudios calificaron a la gestión como relativamente eficiente y ni eficiente ni deficiente.

Palabras-clave: Evaluación de la educación, Gestión educacional, Educación superior, Aprendizaje en línea.

Evaluation of Virtual Educational Management in Industrial Engineering: An Experience in the Context of Emergency Remote Teaching

Abstract: During the Covid-19 pandemic, universities adapted pedagogical and administrative management to virtuality. However, countries like Peru, which had not advanced much in virtual education; this was a new experience with successes and limitations. According to this analysis, the purpose of this study is to evaluate the efficiency of the virtual educational management of the industrial engineering career of a private Peruvian university in the context of remote emergency education. 414 industrial engineering students participated from the first to the tenth cycle of studies between 16 and 43 years old (Mage = 23.65, SD = 5.92). The results show that students evaluate virtual educational management and the dimensions of virtual educational resources, virtual university teaching, and management for

student continuity, administrative management, virtual tutoring and research as relatively efficient. However, some cycles of studies qualified management as relatively efficient and neither efficient nor deficient.

Keywords: Educational evaluation, Educational management, Higher education, Electronic learning.

1. Introducción

La pandemia Covid-19 resultó ser el mayor de los retos educativos que a nivel mundial se enfrentó en cuanto a implementación de nuevas estrategias de aprendizaje virtual en el contexto de la Enseñanza Remota de Emergencia (ERE); específicamente en cuanto a las adecuaciones de la gestión educativa (Anthony & Noel, 2021). Estas medidas se tomaron debido al aislamiento social en el cual, desde la educación se buscó reducir la mortalidad (Bozkurt & Sharma, 2020), que terminó afectando a 1.500 millones de estudiantes de un total de 165 países (Osman, 2020). Así, los países adoptaron diversas alternativas de solución mediante la enseñanza virtual durante la pandemia y constituyéndose como una alternativa convencional para la post pandemia (Lederman, 2020).

En este contexto, las competencias digitales pasaron a ser habilidades más valoradas quedando como obsoletas las competencias clásicas, principalmente en el contexto educacional (Lévano-Francia, et al., 2019). Incluso, se evidenciaron situaciones en las que los estudiantes demostraron mejor desarrollo de las competencias digitales a diferencia de los docentes (Osman, 2020). A nivel de educación básica, en las escuelas fueron más evidentes las dificultades en cuanto a las competencias digitales docentes, y en las universidades estas limitaciones no estuvieron ausentes (Allen, et al., 2020). A pesar de estas limitaciones, los docentes tuvieron que adaptar las estrategias de enseñanza, los materiales educativos y los procedimientos evaluativos a la virtualidad considerando las características de las materias y de los estudiantes (Lepp, et al., 2021).

Como se puede apreciar, la educación virtual demanda una reestructuración significativa en las formas de comunicarse en las comunidades educativas, en los procesos pedagógicos, en los contenidos a enseñar y en las relaciones entre docentes y educandos; todos estos fueron cambios mediados por las herramientas tecnológicas (Huerta, et al., 2020). Por estos motivos, se debe comprender que la modalidad virtual debe ser enfocada como un proceso formativo que emplea las herramientas tecnológicas como un medio y no como un fin (Cocunubo, et al., 2018). Así, brindar un adecuado servicio educativo no solo atendiendo los aspectos académicos sino también brindando atención a la orientación tutorial.

2. Marco conceptual

2.1. Gestión educativa virtual en las universidades peruanas

Al inicio de la pandemia, en marzo del 2020 en el Perú, la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU, 2020) estableció las normativas para el desarrollo de la educación virtual en universidades y en escuelas de postgrado, proporcionando criterios para el desarrollo de las sesiones de aprendizaje virtuales

incluyendo los servicios educativos no presenciales. Así se establecieron orientaciones para la adecuación educativa, para las inducciones de docentes y estudiantes, para la implementación de servicios educativos como plataformas y bibliotecas virtuales, servicios de administrativos y orientación tutorial remota. Permitiendo así, integrar los servicios educativos y la enseñanza con las Tecnologías de la Información y la Comunicación (TIC) (Tretyakova, et al., 2020).

En la educación virtual universitaria es relevante que los docentes prioricen los esfuerzos para garantizar la calidad de la enseñanza en la que se adecuen metodologías activas para el aprendizaje (Guzzetti, 2020). Para lograrlo, el uso de las TIC fue necesario para interactuar con los estudiantes (Prada, et al., 2019). Desde luego, en estos procesos pedagógicos de enseñanza y aprendizaje, la labor docente es esencial (Gálvez & Milla, 2018). De esta manera, orientar el uso de las TIC con fines pedagógicos y no técnicos. Y en el contexto peruano, en concordancia con el Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa (SINEACE) en el Plan de supervisión anual del 2021 (SINEACE, 2021), se planteó la necesidad de evaluar el desempeño docente con la finalidad de identificar los aspectos educativos a mejorar en el área pedagógica y de gestión administrativa (Quezada, et al., 2020).

2.2. Adaptación para la gestión educativa virtual en la carrera de ingeniería industrial

En la universidad investigada, se realizaron las adaptaciones pertinentes para dar continuidad al servicio educativo. Como muchas universidades que lograron intensificar el uso de las herramientas digitales (Anderson, et al., 2020), y así responder a la ERE. En esta universidad, la gestión educativa virtual se logró mediante el uso de plataformas digitales (Anthony & Noel, 2021). Así, aplicar estrategias de enseñanza virtual (Lederman, 2020). Como la gestión administrativa es importante para el adecuado desempeño académico estudiantil (Vela, 2021), se priorizó el uso de plataformas virtuales, la web universitaria y el correo electrónico institucional. Pero, como es evidente, la educación virtual deja ver diversas desigualdades educativas como dificultades de acceso o disposición de medios tecnológicos y al mismo tiempo falencias en cuanto a las capacidades para el manejo de lo digital (Alcántara, 2020).

Por estas razones, se adecuaron mecanismos de apoyo para la continuidad de los estudios, así como la tutoría virtual. Se logró realizar el préstamo de equipos tecnológicos y servicio de internet (Figallo, González & Diestra, 2021) a los estudiantes destacados. Así como tutoría psicológica para brindar acompañamiento personal y emocional para favorecer la formación estudiantil (Rojo & Rojas, 2021). Además, la orientación en cuanto al uso de herramientas digitales para docentes y estudiantes. Así, los docentes estuvieron en condiciones de adaptar sus metodologías de enseñanza y sus recursos didácticos (Lepp, et al., 2021). Por ejemplo, intensificaron el uso de la plataforma Moodle (2021) en la que implementaron las sesiones de aprendizaje, materiales educativos digitales como diapositivas, lecturas, vídeos, etc. Para las sesiones sincrónicas se empleó el Zoom (2020) permitiendo la participación activa de los estudiantes y docentes. Y mediante una metodología de Aula Invertida (Flipped Classroom) se desarrolló la enseñanza de modo sincrónico y asincrónico (Beregman, 2014). Finalmente, para la investigación universitaria se adaptó la enseñanza por competencias evaluada en el proceso y en el

producto de trabajos académicos. Además, ya se contaba con la biblioteca virtual y se diagnosticaron las coincidencias de la redacción con el software Turnitin (2018).

Según lo expuesto, resulta necesario evaluar los niveles de eficiencia de la gestión educativa virtual de la carrera de ingeniería industrial de una universidad privada peruana en el contexto de educación remota de emergencia. Por ello, se pretende evaluar la gestión educativa virtual en la carrera de ingeniería industrial de una universidad privada de Lima – Perú.

3. Metodología

El estudio se orienta bajo una orientación de evaluación sumativa (Ngan, 2020) en el contexto de la virtualidad. Por estas razones, al emplearse un instrumento validado y resultados analizados estadísticamente, el estudio es coherente con el enfoque cuantitativo (Appelbaum, et al., 2018), acorde con el tipo de investigación evaluativa (Kushner, 2017).

3.1. Muestra

Mediante un cálculo del 95% de nivel de confianza y con un margen de error del 5% se definió la muestra a partir de la población (Badii, et al., 2011). De esta manera, para el primer ciclo, se calculó encuestar a 28 estudiantes de una población de 30, para el segundo ciclo 54 encuestados de 62, para el tercer ciclo 56 encuestados de 65, para el cuarto ciclo 60 de 70, para el quinto ciclo 44 de 49, para el sexto ciclo 42 de 47, en el séptimo ciclo fueron 33 de 36, para el octavo ciclo 35 de 39, en el noveno ciclo fueron 31 de 33, y finalmente, el décimo ciclo se seleccionaron 31 de 33. Así se contó con una muestra total de 414 estudiantes de ingeniería industrial de una universidad privada peruana. Del primer ciclo fueron el 6.8%, del segundo ciclo 13%, del tercer ciclo 13.5%, del cuarto ciclo 14.5%, del quinto ciclo 10.6%, en el sexto ciclo 10.1%, del séptimo ciclo 8%, del octavo 8.5%, del noveno 7.5% y del décimo 7.5%. Todos los participantes tenían entre 16 y 43 años ($M_{edad} = 23.65, DE = 5.92$).

3.2. Instrumentos

Escala de Evaluación de la Gestión Virtual Educativa (elaboración propia). La escala es multifactorial y evalúa la calidad de la educación virtual en gestión pedagógica y administrativa. Consta de seis dimensiones: recursos educativos virtuales, enseñanza virtual universitaria, gestión para la continuidad de los estudios, gestión administrativa, tutoría virtual e investigación universitaria. Cada dimensión cuenta con un mínimo de tres ítems para lograr intervalos de confianza óptimos (Streiner, 1994). La escala consta de 18 ítems con siete opciones de respuesta en escala de Likert (1 "Totalmente deficiente" – 7 "Totalmente eficiente"). Por ejemplo, el ítem 1 *"las condiciones de la gestión virtual administrativa de la universidad son óptimas"*. En la Tabla 1 se puede apreciar que la escala pasó satisfactoriamente la prueba de ajuste muestral de Kaiser-Meyer-Olkin (KMO) con una puntuación de .75 y el Test de Esfericidad de Bartlett fue significativo ($\chi^2 = 743{,}919, gl = 21, p < .001$), demostrando así que la escala es válida (Field, 2009). Y de acuerdo a los análisis de confiabilidad, el coeficiente del Alfa de Cronbach fue de .65, evidenciando niveles óptimos de confiabilidad (Aiken, 2002).

Escala	Prueba de Kaiser Meyer y Olkin (Validez)	Coeficiente Alfa de Cronbach
Escala de Evaluación de la Gestión Virtual Educativa	.75 (p<.000)	.65

Tabla 1 – Análisis de Validez y Confiabilidad de la Escala

4. Resultados

Confirmada la confiabilidad de la escala de evaluación, a continuación de analizan los resultados. Por ser una investigación evaluativa (Kushner, 2017) de tipo sumativa (Ngan, 2020), se realizaron análisis de medias generales con los estadísticos descriptivos, luego por ciclos y finalmente análisis exploratorios.

4.1. Análisis de Medias de la Gestión Educativa Virtual

En la Tabla 2 se puede apreciar que de acuerdo a los estadísticos descriptivos la media de la variable gestión educativa virtual fue de 5.2; lo que, según las opciones de respuesta de la escala de Likert (1 "Totalmente deficiente" – 7 "Totalmente eficiente"), es equivalente a la evaluación de "relativamente eficiente". Luego, en el análisis por dimensiones se aprecia que las medias oscilan desde 4.65 para la dimensión de la gestión administrativa virtual y 5.30 para la dimensión de recursos educativos virtuales. Las medias redondeadas de las seis dimensiones corresponden a la evaluación cinco en la escala de Likert, indicando que consideran que todas las dimensiones han sido "relativamente eficientes".

Variable General / Dimensiones	N	Mínimo	Máximo	Media	D.E
Gestión de la Educación Virtual (General)	414	3	7	5,21	1,018
Recursos Educativos Virtuales	414	3	7	5,30	1,018
Enseñanza Virtual Universitaria	414	1	7	5,29	1,015
Gestión para Continuidad de Estudios	414	2	7	5,29	1,280
Gestión Administrativa virtual	414	2	6	4,65	1,304
Tutoría Virtual	414	1	7	5,29	1,264
Investigación Universitaria	414	1	7	5,16	1,250
N válido (por lista)	414				

Tabla 2 – Análisis de Estadísticos Descriptivos (Medias)

4.2. Análisis Exploratorios con Gráfico de Áreas Diferenciadas

Para obtener un análisis de las medias y su evolución por ciclo se emplearon los gráficos de áreas diferenciadas. En los ejes se ingresaron los valores máximos y mínimos de las medias por cada uno de los diez ciclos de estudios. Así se puede apreciar que para la dimensión recursos educativos virtuales y enseñanza universitaria virtual, las medias predominantemente oscilan entre el valor cinco y seis de la escala, reflejando nuevamente encontrarse en la evaluación "relativamente eficiente". Solo para la muestra del octavo ciclo la valoración desciende levemente menos del cinco (ver Figura 1).

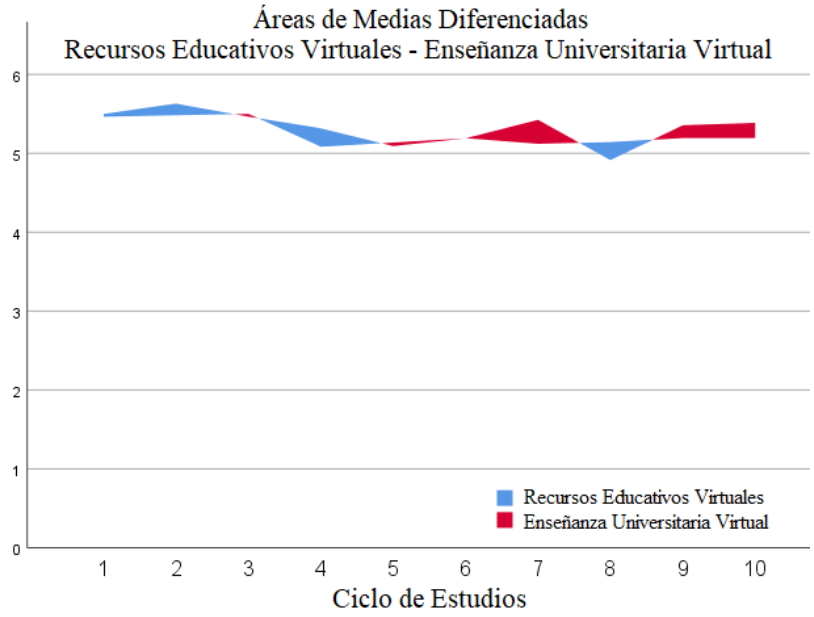


Figura 1 – Se aprecian las medias desde el primer y décimo ciclo de estudios respecto a la eficiencia de los recursos educativos virtuales y la eficiencia de la enseñanza virtual.

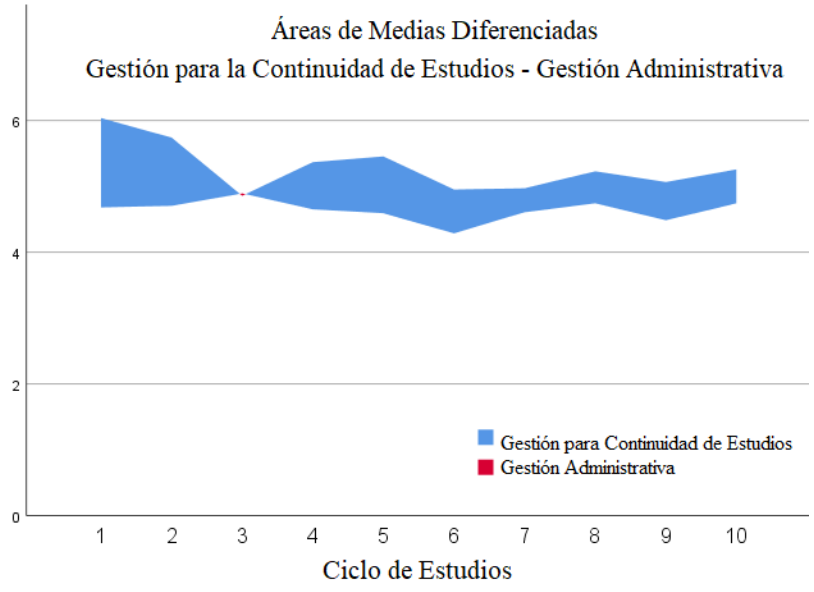


Figura 2 – Se aprecian las medias desde el primer y décimo ciclo de estudios respecto a la eficiencia de la gestión para la continuidad de los estudios y la eficiencia de la gestión administrativa virtual.

Luego, se analizaron las dimensiones de gestión para la continuidad de estudios y gestión administrativa virtual; en el cual se observan los valores máximos y mínimos para cada una de los diez ciclos de estudios. A diferencia de los resultados previos se observó que las medias predominantemente oscilan entre el valor cuatro y seis de la escala, reflejando encontrarse entre la evaluación "eficiente" y "ni eficiente y ni deficiente". En el sexto ciclo se aprecian las valoraciones más bajas de la evaluación (ver Figura 2).

Para el análisis de las dimensiones de la tutoría virtual y la investigación universitaria; se observan los valores máximos y mínimos para cada una de los diez ciclos de estudios. En este análisis, las medias predominantemente oscilan entre el valor cinco y seis de la escala, reflejando encontrarse entre la evaluación "eficiente" y "relativamente deficiente". En este análisis queda la preocupación por el segundo ciclo con la evaluación más baja (ver Figura 3).

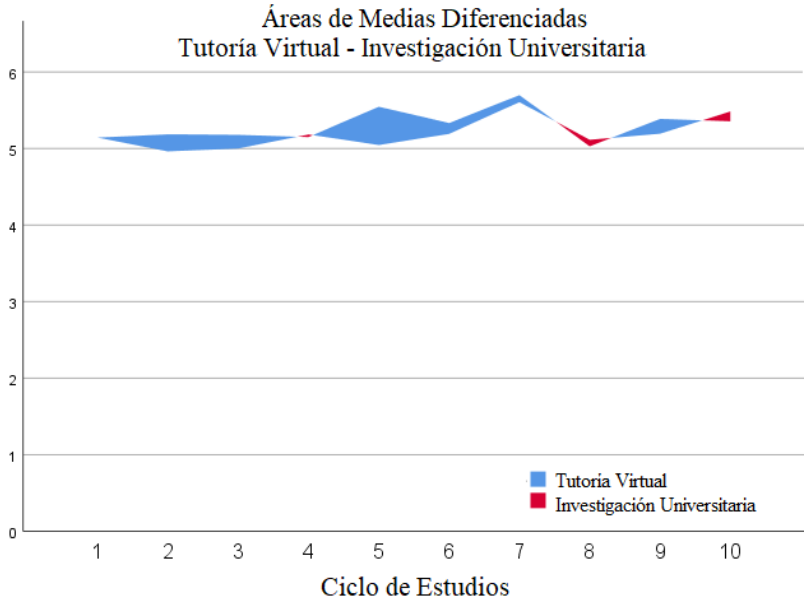


Figura 3 – Se aprecian las medias desde el primer y décimo ciclo de estudios respecto a la eficiencia de la gestión para la continuidad de los estudios y la eficiencia de la gestión administrativa virtual.

4.3. Análisis Exploratorios con Diagramas de Cajas

Una vez estudiadas las medias de las dimensiones de la gestión educativa virtual se exploraron los datos para encontrar casos específicos que brinden una alta o baja evaluación. Este análisis se realizó mediante los diagramas de cajas.

En el análisis de los diagramas de cajas (boxplot) se observa que en los primeros tres ciclos las medianas, la mitad de los casos centrales y el valor más alto se ubican sobre el valor seis. Es decir, 14 estudiantes del primer ciclo, 27 del segundo y 28 del tercero califican

la gestión educativa virtual como “eficiente” y “totalmente eficiente”. Sin embargo, en el primer ciclo se aprecia que el 25% de los estudiantes de primer ciclo (7 estudiantes) y dos casos atípicos del tercer ciclo (101 y 308) se ubican entre el valor cuatro y 2 de la escala, correspondiendo a las evaluaciones “ni eficiente ni deficiente” y “deficiente”. Luego, para en el cuarto ciclo, el 25% de sus encuestados (15 estudiantes), el 25% del séptimo ciclo (aproximadamente 8 estudiantes), el 25% del octavo ciclo (aproximadamente 8 estudiantes) y el 25% del décimo ciclo (aproximadamente 7 estudiantes) están sobre la calificación seis. Es decir, califican la gestión educativa virtual como “eficiente” y “totalmente eficiente”. También se aprecia que desde el cuarto al décimo ciclo, las cajas con el 50% de los participantes por cada ciclo se ubican entre los valores cuatro y seis. Lo que indica que 30 encuestados del cuarto ciclo, 22 del quinto, 21 del sexto, 17 del séptimo, 18 del octavo, 16 del noveno y 16 del décimo califican a la gestión como “eficiente” y “ni eficiente ni deficiente”. En los casos del quinto, sexto, séptimo, octavo y décimo ciclo se aprecia que aproximadamente el 25% de los encuestados alcanzan calificaciones de tres, evidenciando una calificación de “relativamente deficiente” (ver Figura 4).

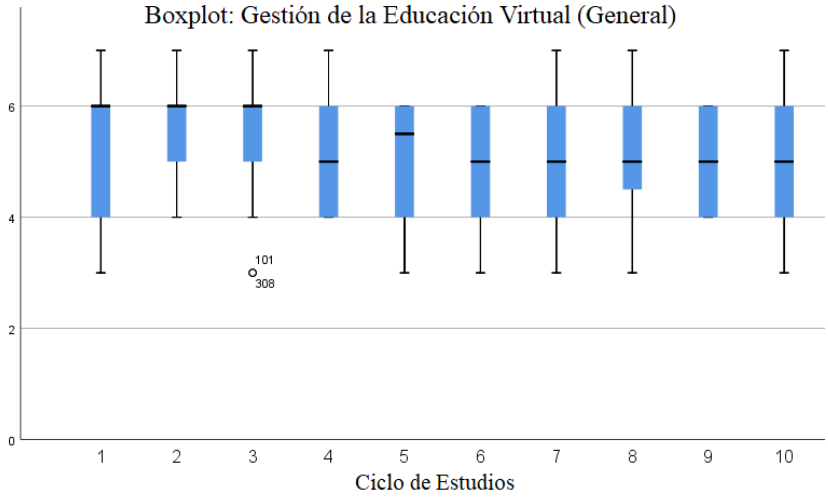


Figura 4 – Análisis de la eficiencia de la Gestión de la Educación Virtual.

4.4. Análisis de Relaciones entre Variables

Adicionalmente, se pretende identificar si las variables se asociaban con el desempeño académico. Así, se aplicaron los criterios de Cohen (1992) que clasifican relaciones leves (*r =.10 - .23*), moderadas (*r = .24 - .36*) y fuertes (*r = .37 - más*). Según estos criterios, en la Tabla 3 se identificaron dos relaciones significativas. Ambos casos, se observó que la gestión administrativa virtual y la tutoría virtual poseen relaciones positivas, leves y significativas con el desempeño académico. Es decir que, si la gestión administrativa es eficiente y la tutoría también, entonces el desempeño académico será mayor.

Variable General / Dimensiones	Desempeño Académico	
	r	*p*
Gestión de la Educación Virtual (General)	0.04	.39
Recursos Educativos Virtuales	0.30	.53
Enseñanza Virtual Universitaria	0.37	.45
Gestión para Continuidad de Estudios	0.02	.63
Gestión Administrativa	0.11*	.03
Tutoría Virtual	0.12*	.02
Investigación Universitaria	0.32	.52
Nota: Las correlaciones son significativas si *** <.001, ** <.01, * <.05.		

Tabla 3 – Relación entre variables (Medias)

5. Discusión

Este estudio tuvo como propósito evaluar los niveles de eficiencia de la gestión educativa virtual de la carrera de ingeniería industrial de una universidad privada peruana en el contexto de educación remota de emergencia. La relevancia del estudio se fundamenta en que las universidades a nivel mundial se adaptaron a la gestión educativa virtual empleando diversas plataformas tecnológicas (Anthony & Noel, 2021). Pero, específicamente en el contexto peruano, como en todo contexto educativo, surgió la necesidad de evaluar la educación virtual para optimizar la gestión pedagógica (Quezada, et al., 2020). Necesidad respaldada en el Plan de supervisión anual del 2021 del SINEACE (2021) en el que se evaluó la calidad del servicio educativo universitario de modo virtual.

De acuerdo a este objetivo, se observó que los estudiantes evaluadores consideran a la gestión educativa virtual como relativamente eficiente. Este resultado resulta preocupante debido a que en la educación virtual universitaria es prioritario optimizar la calidad educativa (Guzzetti, 2020). Además, según los estándares peruanos del SINEACE (2021), no se ha logrado cumplir totalmente con lo establecido. Resultando ser un motivo de reflexión y a la vez una prioridad para resolver las falencias educativas universitarias para garantizar un adecuado servicio.

Al realizar los análisis exploratorios, se observó que en algunos ciclos de estudios hay deficiencias calificando a la gestión como relativamente eficiente o ni eficiente ni deficiente. Sumándose un número menor de encuestados que consideran que la gestión educativa virtual es ni eficiente ni deficiente y relativamente deficiente. Si bien la gestión educativa virtual en Perú se intensificó en la pandemia con las normativas de la SUNEDU (2020); estos resultados evidencian que se dio el servicio, pero no se ha garantizado la calidad educativa. Si bien, se establecieron orientaciones para la adecuación educativa de los servicios educativos con las TIC (Tretyakova, et al., 2020). Al analizar cada ciclo en particular, se observa que en algunos la evaluación es cada vez menor.

Además, la gestión administrativa y la tutoría favorecen al adecuado desempeño académico. Este hallazgo coincide con los estudios de Vela (2021) quien al investigar una

muestra de estudiantes de educación superior tecnológica demostró que la gestión influye significativamente en el rendimiento académico de los estudiantes, así como también en el autoconcepto, en la metodología didáctica y en las relaciones interpersonales. Este resultado confirmó los estudios de Rojo y Rojas (2021) quienes a pesar de fundamentar que la tutoría influye en el desempeño académico, también es una labor preventiva de los problemas de aprendizaje, de ansiedad, emocionales y actitudes hacia la profesión. Motivos por los cuales, estos hallazgos son relevantes en este estudio, porque evidencian la necesidad de incrementar la calidad en toda la gestión educativa virtual en todas las dimensiones estudiadas para la mejora del servicio.

6. Conclusiones y trabajos futuros

Concluyendo el estudio se puede afirmar que los estudiantes evalúan como relativamente eficiente a la gestión virtual educativa y a las dimensiones de recursos educativos virtuales, enseñanza virtual universitaria, gestión para la continuidad de los estudios, gestión administrativa, tutoría virtual e investigación universitaria. Si bien se evidencia que para algunos ciclos de estudios hay deficiencias calificando a la gestión como relativamente eficiente; y ni eficiente ni deficiente; esto sumado a los análisis exploratorios, se aprecia que por cada ciclo existe un menor número de encuestados que consideran que la gestión educativa virtual es ni eficiente ni deficiente y relativamente deficiente. Además, la gestión administrativa y la tutoría favorecen al adecuado desempeño académico. Ante estos hallazgos, se requiere optimizar las dimensiones estudiadas para mejorar la calidad educativa, se pretende realizar capacitaciones del personal docente y administrativo para brindar un mejor servicio. También, se sugiere ampliar los diagnósticos solicitando la evaluación de los docentes, de los trabajadores, de los padres de los estudiantes y de especialistas para la mejora del servicio en el futuro contexto de la semi presencialidad.

Referencias

Aiken, R. (2002). *Psychological testing and assessment* (11th Ed.).Boston: Allyn & Bacon.

Allen, J., Rowan, L. & Singh, P. (2020). Teaching and teacher education in the time of COVID-19, *Asia-Pacific Journal of Teacher Education, 48*(3), 233-236. doi: 10.1080/1359866X.2020.1752051

Alcántara, A. (2020). Educación superior y Covid-19: Una perspectiva comparada. En H. Casanova (Comp.). *Educación y pandemia. Una visión académica*. (pp. 75-82). Universidad de Nacional Autónoma de México: Instituto de Investigaciones sobre la Universidad y la Educación, 2020.

Andersen, G., Rambaut, A., Lipkin, I., Holmes, C., & Garry, F. (2020). The proximal origin of SARS-CoV-2, *Nature Medicine, 26*(4), 450-452.

Anthony, B. & Noel, S. (2021). Examining the adoption of emergency remote teaching and virtual learning during and after Covid-19 pandemic. *International Journal of Educational Management,* 1-18 https://doi.org/10.1108/IJEM-08-2020-0370

Appelbaum, M., Cooper, H., Kline, R., Mayo-Wilson, E., Nezu, A. & Rao, S. (2018). Journal Article Reporting Standards for Quantitative Research in Psychology: The APA Publications and Communications Board Task Force Report. *American Psychological Association, 73*(1), 3 – 25. 2018.

Badii, M., Guillen, A., Cerna, E. & Valenzuela, J. (2011). Introductory notions of statistical sampling. *Daena: International Journal of Good Conscience, 6*(1), 89-105.

Bergmann, J., Sams, A., Cols, S. (2014). What is Flipped Learning? Flipped Learning Network (FLN). http://www.flippedlearning.org/cms/lib07/VA01923112/Centricity/Domain/46/FLIP_handout_FNL_Web.pdf

Bozkurt, A., & Sharma, R. C. (2020), "Emergency remote teaching in a time of global crisis due to CoronaVirus pandemic", *Asian Journal of Distance Education, 15*(1), 1-5.

Cocunubo, S., Parra, V. & Otálora, L. (2018). Propuesta para la evaluación de Entornos Virtuales de Enseñanza Aprendizaje con base en estándares de Usabilidad. *TecnoLógicas, 21*(41), 135-147. https://dialnet.unirioja.es/servlet/articulo?codigo=6289039

Cohen, J. (1992). A power primer, *Psychological Bulletin.*, *112*(1), 155–159. https://doi.apa.org/doi/10.1037/0033-2909.112.1.155

Field, A. (2009). *Discovering statistics using SPSS* (3era Ed.). Lóndres: Sage Publications.

Figallo, F., González, M. & Diestra, V. (2021), Perú: Educación Superior en el contexto de la pandemia por el Covid-19. ESAL – Revista de Educación Superior en América Latina: Educación Superior y Covid-19: Disrupción y Adaptabilidad. https://rcientificas.uninorte.edu.co/index.php/esal/article/view/13404/214421444832

Gálvez, E. & Milla, R. (2018). Teaching performance evaluation model: Preparation for Student Learning within the framework for teacher good performance. *Propósitos y Representaciones, 6*(2), 431-452. http://www.scielo.org.pe/pdf/pyr/v6n2/en_a09v6n2.pdf

Guzzetti, P. (2020). Plataforma virtual: una herramienta didáctica para el proceso de enseñanza aprendizaje. *Ciencia Latina Revista Multidisciplinar, 4*(2). https://ciencialatina.org/index.php/cienciala/article/view/122

Huerta, G., Torres, C. & Lagunes, A. (2020). Evaluación del Desempeño Docente en la Modalidad virtual. En: *Tecnología Innovación y Práctica Educativa*, pp. 436-445, 2020. https://www.researchgate.net/publication/343040982_Tecnologia_Innovacion_y_Practica_Educativa

Kushner, S. (2017). *Evaluative Research Methods: Managing the Complexities of Judgment in the Field*. New York: Information Age Publishing.

Lederman, D. (2020). Preparing for a Fall without In-person Classes. https://www.insidehighered.com/digital-learning/article/2020/04/01/preparingquietly-fall-semester-without-person-instruction

Lepp, L., Aaviku, T., Leijen, L., Pedaste, M. & Saks, K. (2021). Teaching during COVID-19: The Decisions Made in Teaching. *Education Science, 11*(47). https://doi.org/10.3390/ educsci11020047

Levano-Francia, L., Sanchez, S., Guillén-Aparicio, P., Tello-Cabello, S., Herrera-Paico, N. & Collantes-Inga, Z. (2019). Digital Competences and Education. *Propósitos y Representaciones, 7*(2), 569-588. http://dx.doi.org/10.20511/pyr2019.v7n2.329

Moodle. (2021). Start building your online learning site in minutes. https://moodle.com/getstarted/

Ngan, J. (2020). Implications of summative and formative assessment in Japan: A review of the current literature, *International Journal of Education & Literacy Studies*, *8*(2), 28-35. http://dx.doi.org/10.7575/aiac.ijels.v.8n.2p.28

Osman, M. (2020). Global impact of COVID-19 on education systems: the emergency remote teaching at Sultan Qaboos University, *Journal of Education for Teaching, 46*(4), 463-471. doi: 10.1080/02607476.2020.1802583

Prada, R., Hernández, C. & Aloiso, A. (2019). Usos y efectos de la implementación de una plataforma digital en el proceso de enseñanza de futuros docentes en matemáticas. *Revista Virtual Universidad Católica del Norte*, 57, 137-156. https://revistavirtual.ucn.edu.co/index.php/RevistaUCN/article/view/1059/0

Quezada, M., Castro, M., Oliva, J., Gallo, C. & Quezada, G. (2020). Características del docente peruano virtual: retos de la universidad peruana en el contexto de una pandemia, *Revista Inclusiones, 7*, 119-136. https://revistainclusiones.org/index.php/inclu/article/view/1272

Rojas, D. & Rojas, A. (2021). La acción tutorial en el CUSur, prácticas durante la pandemia: Prácticas efectivas en la actividad tutorial. En L. Aceves y M. Ureña (Comp.). *Compendio de buenas prácticas de la tutoría en el CUSur 2020*. (pp. 08-21). Universidad de Guadalajara: Centro Universitario del Sur, 2021.

Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa. (2021). Plan anual de supervisión 2021 del SINEACE. Ministerio de Educación del Perú. https://cdn.www.gob.pe/uploads/document/file/1693108/Modificaci%C3%B3n%20de%20la%20Directiva%20N%C2%B0002-2018-SINEACEP-ST.pdf.pdf

Streiner, D. (1994). Figuring out factors: the use and misuse of factor analysis, *Can Journal Psychiatry*, *39*, 135-40.

Superintendencia Nacional de Educación Superior Universitaria. (2020). Resolución del Consejo Directivo N° 039-2020. https://busquedas.elperuano.pe/normaslegales/aprueban-los-criterios-para-la-supervision-de-la-adaptacion-resolucion-n-039-2020-sunedu-cd-1865206-1/

Tretyakova, V., Prokopiev, S., Goncharova, V., Karpova, A., & Ilina, S. (2020). Distance pedagogical education in the conditions of the coronavirus. *Propósitos y Representaciones, 8,*SPE(3), e718 http://dx.doi.org/10.20511/pyr2020.v8nSPE3.718

Turnitin. (2022). Empower students to do their best, original work. https://www.turnitin.com

Vela, L. (2021). Gestión educativa en el rendimiento académico de los estudiantes de electrotecnia industrial IESTP Mariscal Ramón Castilla, Loreto, 2021. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/71675/Castro_VL-SD.pdf?sequence=8

Zoom. (2020). Comprehensive Guide to Educating Through Zoom. https://www.zoom.us/docs/en-us/childrens-privacy.html, last accessed 2021/01/15.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 17/12/2022
Aceitação/Acceptance: 13/02/2022

Análisis de ataques DoS en redes de datos basadas en hardware y software

Anthony Albarracín-Estrada[1], Darío Enrique Soto-Duran[2],
Juliver Gil-Herrera[3] , Fabio Alberto Vargas-Agudelo[4]

ajalbarra@tdea.edu.co; dsoto@tdea.edu.co; julivergil@itm.edu.co; fvargas@tdea.edu.co

[1] Tecnológico de Antioquia (TdeA), Cl. 78B #72A-220, 050034, Medellín, Colombia.

[2] Tecnológico de Antioquia (TdeA), Cl. 78B #72A-220, 050034, Medellín, Colombia.

[3] Instituto Tecnológico Metropolitano (ITM), Cl 54ª #30-01, 050012, Medellín, Colombia.

[4] Tecnológico de Antioquia (TdeA), Cl. 78B #72A-220, 050034, Medellín, Colombia.

Pages: 262-275

Resumen: Las redes basadas en tecnologías SDN (Software Defined Networking) también pueden ser objeto de ataques de denegación de servicio (DoS). El ataque DoS intenta dañar la arquitectura de la red al debilitar el controlador SDN. Actualmente, no existen soluciones efectivas para la prevención de este ataque, lo que comúnmente se hace es detectar cada paquete de datos entrante y bloquear temporalmente el host atacante, esto hace que las redes SDN sean vulnerables a este tipo de ataque. Además, las soluciones propuestas no pueden adaptarse a la frecuencia y tipo de ataque. Esta investigación busca comprender y comprobar el grado de afectación que producen los ataques DoS a las redes SDN en comparación a los que se producen en las redes HDN a través de un entorno virtualizado en la nube. Los resultados permiten concluir que las afectaciones en la red SDN son 20% mayores a las sufridas en la red HDN y a su vez evitar que la propia red SDN se convierta en víctima de ataques DoS.

Palabras-clave: vulnerabilidades de redes de datos; seguridad cibernética; ataque de denegación de servicio; redes basadas en software y hardware.

Analysis of DoS attacks on hardware and software-based data networks

Abstract: Networks based on SDN (Software Defined Networking) technologies can also be the target of Denial of Service (DoS) attacks. DoS attack tries to damage the network architecture by weakening the SDN controller. Currenly, there are not effective solutions to the prevention of this attack, what is commonly done is to detect every incoming data packet and temporarily block the attacking host, this makes SDN networks vulnerable to this type of attack. This research seeks to understand and verify the degree of impact that DoS attacks produce on SDN networks compared to those that occur in HDN networks through a virtualized environment in the cloud. The results allow us to conclude that the effects on the

SDN network are 20% greater than those suffered on the HDN network and in turn prevent the SDN network itself from becoming a victim of DoS attacks.

Keywords: data network vulnerabilities; cybersecurity; denial of service attack (DoS); software and hardware based networking

1. Introducción

Las redes de datos son la columna vertebral y la base funcional y operacional de los sistemas de telecomunicaciones. A través de ellas viajan todos los datos que se utilizan en los diferentes sistemas que soportan las tecnologías actuales.

En sus inicios, la proliferación de las redes de datos se ejecutó a través de una base física de interconexión, es decir usando el hardware con el factor principal. Pero en los últimos años se ha venido realizando un cambio vertiginoso provocado por la incorporación de tecnologías de virtualización y automatización en las redes, lo que genera actualmente dos grandes tipos de redes de datos: las redes definidas por hardware (HDN) y las redes definidas por software (SDN), por sus siglas en ingles respectivamente. Estos tipos de redes presentan su principal diferencia en que la red definida por software requiere de un controlador que gestiona las decisiones de los dispositivos de red (Maziku et al., 2019) (Herrera & Botero, 2021). Por el contrario, en las redes definidas por hardware las decisiones se centran en el administrador de la red. Esta diferencia en el funcionamiento permite establecer una nueva forma en la que el plano de control automatiza la red.

El primer aporte de este trabajo es una revisión de la literatura en torno a las diferentes afectaciones documentadas de los ataques de DoS en las redes HDN y SDN. Un segundo aporte es la construcción de un entorno de simulación donde se configuran los dos escenarios de interés en un mismo sistema operativo de fácil escalamiento, que permita la instalación de la herramienta Mininet y los componentes adicionales de medición; así como la ejecución de un controlador externo para el escenario en el que se utiliza el protocolo OpenFlow. El entorno de simulación se despliega en una plataforma virtualizada en la nube y desde esta se genera un ataque DoS, suficientemente dañino para afectar tanto la red HDN como la red SDN y de esta manera generar la data que permita evaluar en función del desempeño, las afectaciones sufridas en los dos tipos de red. En tercera instancia, se realiza un análisis de los datos obtenidos en cada escenario evaluado, que permite establecer las conclusiones para clasificar las diferencias y caracterizar de manera cuantitativa las afectaciones.

2. Metodología

La estrategia metodológica se sustenta en el estudio de caso, dado que aborda el estudio de fenómenos reales, desde un enfoque basado en la exploración y descripción del comportamiento en condiciones controladas. Siendo desarrollado en tres fases: Aproximación Teórica, Experimental y Analítica, ejecutadas de manera secuencial teniendo en cuenta los siguientes argumentos:

Fase 1. Aproximación Teórica: se analizan experiencias similares para establecer condiciones del análisis o comparación que sirvan de insumo en el estudio exploratorio.

Fase 2. Experimental: Se recrea el ambiente para la ejecución de la simulación del ataque DoS en las redes de datos de hardware y software. Igualmente, se establecen los atributos a ser evaluados para su posterior análisis.

Fase 3. Análisis: Una vez ejecutada la simulación del ataque, se realiza la interpretación de los datos obtenidos.

2.1. Fase 1: Aproximación Teórica

Esta sección presenta la revisión de literatura sobre las experiencias y estudios más relevantes que soportan las afectaciones que derivan bajo ataque DoS en las redes HDN y SDN. Para ello, se instancio el protocolo de revisión sistemática de Kitchenham y Charters (2007), el cual establece pautas para una revisión bibliográfica clara y objetiva.

La revisión de literatura se sustenta en criterios de búsqueda y selección que permiten dar respuesta a las necesidades y problemática planteada en el dominio de las redes HDN y SDN bajo ataque DoS. De igual manera establecer criterios para un escenario de validación para la comprobación de las principales afectaciones y sus respectivas causas.

A partir de la revisión de literatura se obtiene la taxonomía de las afectaciones en las redes HDN y SDN bajo ataque DoS; teniendo en cuenta que la gran mayoría de los estudios se enfocan a las redes SDN y las redes HDN son referentes de comparación para su análisis. De este modo, se categorizaron las afectaciones que impactan las redes HDN y los estudios que las describen en la siguiente tabla.

Categoria	Descripción	Autores
Alto consumo de recursos de computación	Se presenta una saturación en las capas de control y datos de los switches dado que no existe independencia entre estos planos.	(Deng et al., 2019), (Siregar et al., 2018), (Yan et al., 2015), (Tatang et al., 2017), (Chen et al., 2016) y (Prakash & Priyadarshini, 2018)
Alta saturación de tráfico	Los autores atribuyen esta afectación a la saturación progresiva de los canales de transmisión de datos, incluso en los switches interconectados.	(Lawal & Nuray, 2018b), (Wang et al., 2015), (Wang et al., 2018), (Behal & Kumar, 2016), (Anithaashri et al., 2019), (Cui et al., 2016), (Townsley Chris, 2018), (Singh et al., 2019),
Lentitud en la detección del origen	Esta afectación se presenta debido a que se deben recorrer todos los posibles puntos de falla para encontrar el agente malicioso y así encontrar el origen	(Maziku et al., 2019), (Lawal & Nuray, 2018), (Joshi et al., 2018), (Chen et al., 2016), (Prakash & Priyadarshini, 2018), (Cui et al., 2019), (Imran et al., 2019), (Cui et al., 2016)

Tabla 1 – Afectaciones de una red HDN ante un ataque DoS

De igual manera, se establece que las afectaciones que sufre una red SDN son: la rápida saturación de tráfico, la baja escalabilidad dentro del plano de control y la falta de disponibilidad del servicio por la dependencia con el controlador. En La Tabla 2, se presentan las categorías con su respectiva descripción y los autores que hacen mención de dicha afectación.

Categoria	Descripcion	Autores
Rápida Saturación del tráfico	Hace referencia a la obstaculización provocada por el flujo de grandes cantidades de transacciones, que de manera rápida generan una inundación que ralentiza los procesos de transmisión	(Birkinshaw et al., 2019), (Siregar et al., 2018), (Yan et al., 2015), (Lawal & Nuray, 2018a), (Keti & Askar, 2015), (Tatang et al., 2017) y (Chen et al., 2016)
Baja escalabilidad del plano de control	La centralización de la capa de control agrega una escalabilidad limitada en ese ámbito, lo que facilita al atacante la inundación de tráfico	(Maziku et al., 2019), (Lawal & Nuray, 2018a), (Lawal & Nuray, 2018b), (Chen et al., 2016), (Prakash & Priyadarshini, 2018) y (Dao et al., 2015)
Indisponibilidad del plano de control	Hace referencia a la dependencia de la existencia de un controlador para toda la infraestructura, un ataque de DoS.	(Siregar et al., 2018), (Zhang et al., 2018), (Joshi et al., 2018), (Wang et al., 2018)y (Behal & Kumar, 2016).

Tabla 2 – Afectaciones de una red SDN ante un ataque DoS

Asimismo, en la revisión desarrollada se encuentran 12 estudios que implementan un controlador para la red SDN que permite soportar los escenarios de simulación y validación de resultados. En la Tabla 3, se listan los estudios que mencionan los controladores.

Controlador	Autores
POX en Python	(Siregar et al., 2018), (Keti & Askar, 2015) y (Wang et al., 2015)
FloodLight en java	(Siregar et al., 2018), (Zhang et al., 2018), (Tatang et al., 2017) y (Wang et al., 2018)
HPVAN de HP	(Tatang et al., 2017)
RYU en Python	(Tatang et al., 2017), (Jantila & Chaipah, 2016) y (Cui et al., 2016)
GENI-based	(Maziku et al., 2019)

Tabla 3 – Controladores Usados para los escenarios de validación

Igualmente, en la literatura se mencionan herramientas de emulación como: Mininet, OpNet y GENI. Teniendo mayor preferencia la herramienta Mininet, dado que se reporta facilidad de uso y compatibilidad en las redes HDN y SDN.

De acuerdo con los autores (Deng et al., 2019), la transmisión de datos en una red HDN está enmarcada bajo los patrones de emisión y control que desde el datagrama se condicionan en la mayoría de los casos a resolver rutas y vecinos cercanos. Pero este escenario es totalmente distinto en las redes SDN.

En las redes SDN, se presenta la separación de los planos de control y de datos agregan un nuevo componente a la red llamado controlador, el cual se introduce a la topología con el fin de llevar a cabo la toma decisiones en transmisión de información de manera centralizada, favoreciendo la dinámica de crecimiento automatizada mediante programación y evita la configuración exhaustiva de dispositivos y rutas. Sin embargo, introduce un nuevo foco de ataques (Birkinshaw et al., 2019)(Siregar et al., 2018).

El tiempo que un administrador requiere para la implementación y puesta en producción de una red HDN configurada por defecto, puede llegar a ser muy superior al tiempo requerido para implementar y poner en producción la misma red en una arquitectura SDN. Estas configuraciones por defecto son las que en muchos casos acompañan los escenarios productivos de empresas y corporaciones. De tal manera que se hace necesario comparar las afectaciones entre el desempeño de una red SDN y una red HDN cuando están bajo un ataque DoS.

2.2. Fase 2: Experimental

Esta sección presenta los aspectos necesarios para la definición del ambiente de validación y la ejecución del ataque DoS para los escenarios previstos en las redes SDN y HDN. La simulación se desarrolla así: en la primera instancia se recrea un ambiente homologado y controlado, así como los argumentos que sustenta los criterios a usar y los elementos a desplegar. Después se describe el procedimiento que permite la construcción del escenario y la ejecución de la simulación de los escenarios bajo ataque. Por último, se realiza un análisis comparativo de los resultados obtenidos.

Diseño e Implementación del entorno de prueba

Los escenarios desplegados son homologados entre sí, de manera tal que la comparación sea viable. La homologación de estos ambientes se realizó construyendo la misma arquitectura, compuesta por una configuración tipo estrella, la cual es la configuración de apilamiento de Switches más común en los ambientes empresariales (Yan et al., 2015). En esta topología los equipos de cómputo están conectadas a un punto central, que para el escenario propuesto se establece en S1. Para ambos ambientes se usaron 8 estaciones de trabajo, enumeradas desde h1 hasta h8. Para los Switches, independientemente de su tipo, se identifican desde S1 hasta S7. Lo anterior se controló mediante un emulador de red.

El estudio adopta el emulador Mininet, porque soporta la implementación de los ambientes SDN y HDN simultáneamente. Lo que permite el uso de controladores SDN y, además, no requiere la adquisición de una licencia dado que es software libre.

Para el ambiente que emula la red HDN se usa el esquema propuesto en la Figura 1. En el cual, todos los switches están configurados con los parámetros “Legacy”, lo cual significa que no dependerán de un controlador, y su funcionamiento se limita a comportarse como un conmutador tradicional de capa 2.

Igualmente, para el ambiente que emula la red SDN se usa el esquema propuesto en la Figura 2. En el cual, todos los switches están configurados para soportar el protocolo OpenFlow y dependen de un controlador.

Para los ambientes o escenarios donde se configura la red SDN, se realizan los cuatro pasos que se describen a continuación: instalación del sistema operativo, ejecución del ambiente de simulación, despliegue del controlador SDN y despliegue del monitor de flujos.

Paso 1. Instalación del sistema operativo: para el ambiente de simulación controlado se requiere de un modelo que permita la flexibilidad y escalabilidad idónea (Lawal

& Nuray, 2018a); y así homologar los escenarios y poder replicar las evidencias que a través de estos ambientes se extraigan. La anterior fue resuelto por medio del despliegue de una arquitectura en la nube, que permite la creación de los escenarios sin depender de manera directa de experimentados administradores de TI que configuren e instalen servidores, estaciones de trabajo y elementos de red. Por tal motivo, se elige la construcción del ambiente de simulación Google Compute Engine como plataforma en la nube que provee la instalación inmediata de un sistema operativo para desplegar las redes SDN y HDN. Google Compute Engine suministra máquinas virtuales ubicadas en centros de datos de Google, que hacen posible el escalamiento de instancias únicas a una red global de procesamiento en la nube, resultando conveniente dado que simular un ataque DoS consume un volumen significativo de recursos computacionales.

Paso 2. Ejecución del ambiente de simulación: Las redes SDN centran su operación en 4 diferentes factores, el primero de ellos es la separación entre el plano de datos y el plano de control; el segundo es la necesidad de la existencia de un controlador SDN centralizado que por medio de un protocolo como OpenFlow pueda tener una vista general de la red; el tercero tiene que ver con la facilidad en el despliegue de interfaces abiertas y de fácil interconexión, y por último, la existencia de una aplicación externa que permita la programación de dichas redes (Jamali, 2019)(Ravi & Shalinie, 2021).

Contrario a lo descrito anteriormente, las redes HDN no separan el plano de datos del plano de control, no necesitan un controlador centralizado ni de un protocolo como OpenFlow, y el despliegue de sus interfaces no necesariamente debe ser dinámico. Además, la configuración de estas redes no depende siempre de la intervención de una aplicación externa, por el contrario, en muchos casos requiere el despliegue de configuraciones y adaptaciones de infraestructura costosas y que demandan muchos recursos (Keti & Askar, 2015). Por lo tanto, se utiliza Mininet para configurar los dos escenarios de evolución. Mininet es un emulador que permite el despliegue de redes SDN, y también permite la configuración personalizada de una red HDN, manteniendo el ambiente de pruebas totalmente homologado para los dos escenarios en cuestión (Varghese & Muniyal, 2021)(Lawal & Nuray, 2018b). Mininet provee la capacidad de emular múltiples tipos de elementos de red como: estaciones finales, switches capa 2 y capa 3, routers y enlaces; así como el montaje completo de una red SDN conectada a un controlador externo, usando Switches Openflow a través de una arquitectura de fácil creación y gestión (Thomas & James, 2017).

Paso 3. Despliegue del controlador SDN: se utiliza el controlador FloodLight dado que soporta el protocolo OpenFlow y realiza la orquestación de los flujos de tráfico en una red SDN (Wang et al., 2015). El despliegue del controlador solo requiere la última versión de java (java –jar target/floodflight.jar). Se aclara que los parámetros de seguridad que ofrece FloodLight se han dejado por defecto y que estos pueden ser mejorados usando metodologías de control adicionales que las redes SDN no ofrecen en primera instancia como lo plantean Zhang y sus colegas (2018).

Paso 4. Despliegue del monitor de flujos RMON: Parte importante de la correcta medida de las comparaciones depende de tener control en tiempo real del tráfico que está circulando por cada uno de los escenarios, motivo por el cual se instaló en el sistema operativo un software de monitoreo llamado RMON y se le asoció un flujo de muestreo para las redes del mismo, que grafique el comportamiento de la red. RMON

también provee de un mecanismo para monitorear los cambios o afectaciones en el comportamiento de una red de datos (Tatang et al., 2017).

Ejecución del escenario bajo ataque

Para ambos escenarios se plantea un protocolo que permita desplegar de manera homogénea el ataque DoS, permitiendo una comparación confiable de los datos. De ese modo el escenario inicia las variables de control sin ningún tipo de alteración. Para el escenario de una red HDN mostrado en la figura 1, el atacante envía paquetes de comportamiento no anómalo desde h1 hacia h5, sin provocar ningún ataque DoS, y las víctimas indirectas h3 y h7 también se interconectan de manera normal a la red HDN.

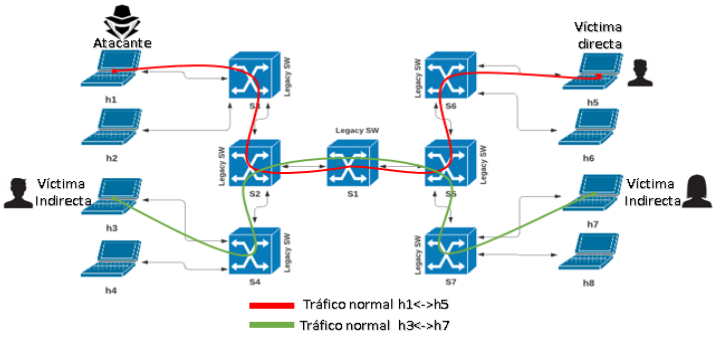


Figura 1 – Escenario de una red HDN sin ejecución de ataque

Para el escenario de una red SDN mostrado en la Figura 2, el atacante también envía paquetes de comportamiento no anómalo desde h1 hacia h5, sin provocar ningún ataque de denegación de servicio, y las víctimas indirectas h3 y h7 se interconectan de manera normal a la red SDN.

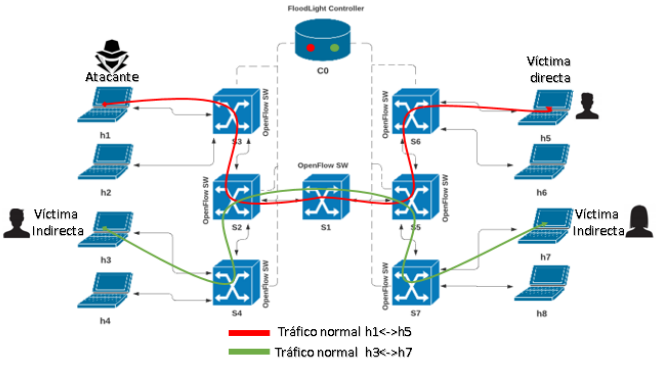


Figura 2 – Escenario de una red SDN sin ejecución de ataque

Para medir el rendimiento de los escenarios planteados en las Figuras 1 y 2 se realizó el siguiente procedimiento: En un instante t0 desde el equipo h1 se ejecuta el siguiente comando: "h1 ping -w 60 h5" lo cual envía una petición ping desde h1 hacia h5 durante 60 segundos; se utiliza una configuración por defecto del comando y no se activa el modo "flood". En un instante t0+n siendo n el número entre 5 y 10 segundos, se ejecuta desde el equipo h3 el siguiente comando: "h3 ping "c 20 h7", por medio del cual se envían 20 paquetes desde el instante t0+n. Con esto, se asegura que la medición de transmisión entre h3 y h7 está contenida dentro de la transmisión que existe entre h1 y h5. La Figura 3 muestra de manera gráfica el procedimiento.

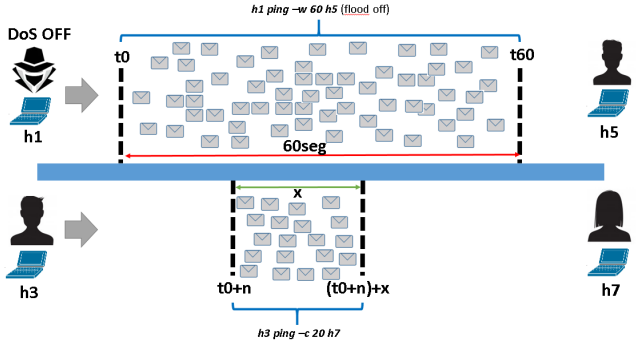


Figura 3 – Esquema para el envío de paquetes previo a la medición.

Escenarios de ejecución

- Escenario 1. Red SDN con Openflow: En primera instancia se ejecuta Mininet, con los parámetros requeridos para desplegar la topología previamente ilustrada en la Figura 2.
- Escenario 2. Red HDN sin Openflow: En primera instancia se ejecuta Mininet con los parámetros requeridos para desplegar la topología previamente ilustrada en la Figura 1. Es importante destacar que para este escenario se desactiva el controlador.

2.3. Fase 3: Análisis

El análisis se realiza a partir de cuatro escenarios para tener un acercamiento porcentual del nivel de afectación sustentado en el valor promedio de las mediciones (RTT), debido a que esta medida es la más representativa en el desempeño de una red cuando se expone a un ataque de DoS (Joshi et al., 2018).

Comparación 1: Valor promedio RTT medido desde el equipo del atacante (h1) en una red tradicional sin efectuar un DoS, versus el valor promedio RTT medido desde el equipo del atacante (h1) en una red HDN bajo ataque DoS.

Comparación 2: Valor promedio RTT medido desde el equipo de la víctima (h3) en una red tradicional que no está siendo afectada por un DoS, versus el valor promedio

RTT medido desde el equipo de la víctima (h3) en una red HDN sobre la que el atacante está efectuando un DoS.

Comparación 3: Valor promedio RTT medido desde el equipo del atacante (h1) en una red SDN con OpenFlow sin efectuar un DoS, versus el valor promedio RTT medido desde el equipo del atacante (h1) en una red SDN con OpenFlow sobre la que está efectuando un DoS.

Comparación 4: Valor promedio RTT medido desde el equipo de la víctima (h3) en una red SDN con OpenFlow que no está siendo afectada por un DoS versus el valor promedio RTT medido desde el equipo de la víctima (h3) en una red SDN con OpenFlow sobre la que el atacante está efectuando un DoS.

Resultados por escenario

A partir de los resultados, se realiza un análisis para identificar las diferencias y obtener argumentos válidos que permitan alcanzar el propósito de esta investigación. Para ello, se tienen en cuenta las métricas de cantidad de paquetes enviados, y los datos del RTT mínimo, RTT promedio, RTT máximo y la desviación estándar. Para el escenario de la red HDN la cantidad de paquetes enviados en el ataque DoS fue de 765231 y para el escenario de la red SDN el total de paquetes enviados fue de 764751, una diferencia de 480 paquetes, esto es un 0.063% de variación entre escenarios.

Se recolectaron datos en dos hosts, el primer host fue h1, desde donde se generaron todos los ataques DoS y además se tomaron datos de control para cada uno de los escenarios. De acuerdo con los datos resumidos en la Figura 4, se evidencia que para todos los casos en los que el escenario fue la red SDN, los tiempos RTT fueron mayores, incluso en los casos en los que no existía un ataque DoS sobre la red.

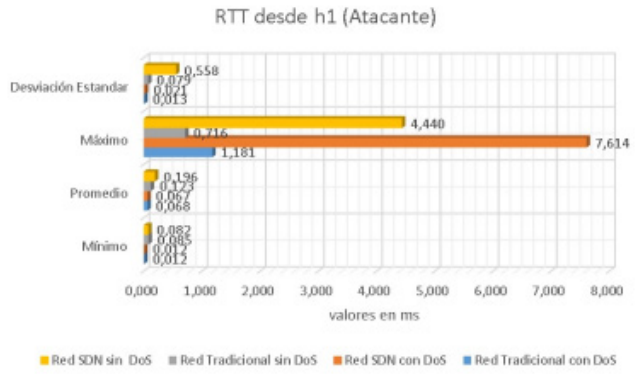


Figura 4 – Ponderación de datos RTT recolectados desde h1

El segundo host desde donde también se recolectaron datos fue h3, desde allí no se generó ningún ataque DoS, y por el contrario el objetivo de las mediciones realizadas desde este host tenía como propósito verificar el nivel de afectación en cada uno de los

casos. La Figura 5, muestra el panorama general de comparación, en ella se observa que para todos los casos en los que el escenario fue la red SDN, como ya se había descrito en el análisis de datos desde h1, los tiempos RTT fueron mayores, incluso en los casos en los que no existía un ataque DoS.

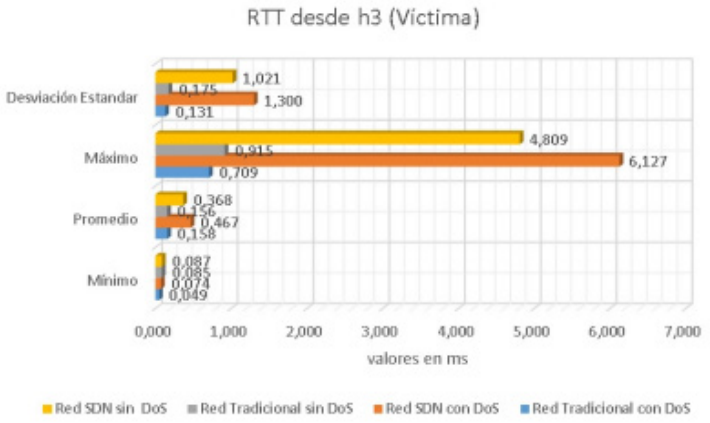


Figura 5 – Ponderación de datos RTT recolectados desde h3

Comparación 1: El valor promedio RTT en el escenario sin DoS fue de 0,123ms, mientras que el valor medido para el escenario con DoS fue de 0,068ms. Lo cual arroja un porcentaje de la variación de RTT de 81% aproximadamente; esto evidencia que para el equipo del atacante h1 se reduce el RTT cuando efectúa el DoS. Lo cual es un comportamiento esperado debido a que la red dispone de todos sus recursos posible para atender la solicitud expresa de h1, que no es más que una inundación de datos. La expresión para realizar este cálculo porcentual de las comparaciones se describe en la Ecuación 1.

$$Variacion\ del\ RTT = \left| \frac{Valor\ \ RTT\ \ promedio\ con\ DoS - Valor\ \ RTT\ \ promedio\ \text{sin}\ DoS}{Valor\ RTT\ \ promedio\ con\ DoS} \right|$$

Ecuación 1. Cálculo de la variación del RTT.

Comparación 2: El valor promedio RTT en el escenario sin DoS fue de 0,156ms, mientras que el valor medido para el escenario con DoS fue de 0,158ms. Esto arroja un porcentaje de la variación de RTT de 1% aproximadamente. Por lo tanto, se evidencia que para el equipo de la víctima h3 no se reduce de manera significativa el RTT cuando la red está sufriendo un DoS.

Comparación 3: El valor promedio RTT en el escenario sin DoS fue de 1,96ms, mientras que para el escenario con DoS fue de 0,67ms. Esto arroja un porcentaje de la variación de RTT de 193% aproximadamente. Al obtener este valor en la variación del RTT se evidencia que para el equipo de la víctima h3 se aumenta mucho el RTT cuando la red está sufriendo un DoS. Un comportamiento esperado debido a que la red dispone

de todos sus recursos posibles para atender la solicitud expresa de h1, que no es más que una saturación prolongada de tráfico hacia y desde el controlador.

Comparación 4: El valor promedio RTT en el escenario sin DoS fue de 0,368ms, mientras que el valor para el escenario con DoS fue de 0,467ms. Esto arroja un porcentaje de la variación de RTT de 21% aproximadamente; al obtener este valor en la variación del RTT se evidencia que para el equipo de la víctima h3 si se reduce de manera significativa el RTT cuando la red está sufriendo un ataque DoS persistente.

3. Conclusiones

De acuerdo a la revisión de literatura se identifican las afectaciones más comunes que un ataque de DoS puede provocar sobre las redes SDN y HDN que son: la rápida saturación de tráfico, la baja escalabilidad dentro del plano de control y la potencial indisponibilidad que puede generar la dependencia de un controlador central, esto sumado con el alto consumo de recursos.

Basados en los resultados experimentales, se pudo validar que una estación de trabajo (host) de una red SDN que está siendo afectada por un ataque DoS, tiene un aumento en el tiempo promedio RTT del 21% en comparación con el comportamiento de ese mismo host en una red SDN que no está siendo afectada por el ataque DoS. Lo cual, coincide con la revisión de literatura frente a la rápida saturación de tráfico y generación de cuellos de botella como principales desventajas.

Una estación de trabajo (host) presente en una red HDN que está siendo afectada por un ataque DoS tiene un aumento en el tiempo promedio RTT (tiempo de ida y regreso) del 1% en comparación con el comportamiento de ese mismo host en una red HDN que no está siendo afectada por un ataque DoS. Este aumento no es significativo, porque la saturación de tráfico es progresiva en el tiempo y al no existir una dependencia directa con un controlador central, hace que la saturación no afecte de manera significativa el flujo de datos.

Las ventajas de la virtualización y automatización de la red, facilitan la detección del ataque más no permite su contención. Además, hay limitaciones para mitigar ataques DoS en las redes SDN, como son la sobrecarga del controlador centralizado en presencia de gran cantidad de tráfico a procesar. Otra limitación es que la información del tráfico que se puede extraer desde el plano de datos es muy limitada, lo que restringe el uso de contramedidas eficaces que logren mitigar o detener el ataque.

Los argumentos validados empíricamente son coherentes frente a los resultados obtenidos en la revisión de literatura, siendo relevante concluir que existe mayor vulnerabilidad en la red SDN ante un ataque de DoS, dada las afectaciones producidas en el rendimiento de la red, cuantificables aproximadamente en un 20% superior a las que se presentan en una red HDN. Por lo tanto, un ataque DoS en el escenario HDN debe ser 80% menor para alcanzar resultados similares en una red SDN.

Referencias

Anithaashri, T. P., Ravichandran, G., & Baskaran, R. (2019). Software Defined Network Security enhancement using Game Theory. Elsivere COMNET, vol157, 112-121.

Behal, S., & Kumar, K. (2016). Trends in validation of DDoS research. Procedia Computer Science, 85, 7-15.

Birkinshaw, C., Rouka, E., & Vassilakis, V. G. (2019). Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. Journal of Network and Computer Applications, 136, 71-85.

Chen, K. Y., Junuthula, A. R., Siddhrau, I. K., Xu, Y., & Chao, H. J. (2016, October). SDNShield: Towards more comprehensive defense against DDoS attacks on SDN control plane. In 2016 IEEE Conference on Communications and Network Security (CNS) (pp. 28-36). IEEE.

Cui, J., Wang, M., Luo, Y., & Zhong, H. (2019). DDoS detection and defense mechanism based on cognitive-inspired computing in SDN. Future generation computer systems, 97, 275-283.

Cui, Y., Yan, L., Li, S., Xing, H., Pan, W., Zhu, J., & Zheng, X. (2016). SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks. Journal of Network and Computer Applications, 68, 65-79.

Dao, N. N., Park, J., Park, M., & Cho, S. (2015, January). A feasible method to combat against DDoS attack in SDN network. In 2015 International Conference on Information Networking (ICOIN) (pp. 309-311). IEEE.

Deng, S., Gao, X., Lu, Z., Li, Z., & Gao, X. (2019). DoS vulnerabilities and mitigation strategies in software-defined networks. Journal of Network and Computer Applications, 125, 209-219.

J. Gil Herrera and J. F. Botero, "Tabu Search For Service Function Chain Composition In NFV," in IEEE Latin America Transactions, vol. 19, no. 01, pp. 17-25, January 2021, doi: 10.1109/TLA.2021.9423822..

Imran, M., Durad, M. H., Khan, F. A., & Derhab, A. (2019). Toward an optimal solution against denial of service attacks in software defined networks. Future Generation Computer Systems, 92, 444-453.

Jamali, S., Badirzadeh, A., & Siapoush, M. S. (2019). On the use of the genetic programming for balanced load distribution in software-defined networks. Digital Communications and Networks, 5(4), 288-296.

Jantila, S., & Chaipah, K. (2016). A security analysis of a hybrid mechanism to defend DDoS attacks in SDN. Procedia Computer Science, 86, 437-440.

Joshi, B. K., Joshi, N., & Joshi, M. C. (2018, August). Early detection of distributed denial of service attack in era of software-defined network. In 2018 Eleventh International Conference on Contemporary Computing (IC3) (pp. 1-3). IEEE.

Keti, F., & Askar, S. (2015, February). Emulation of software defined networks using mininet in different simulation environments. In 2015 6th International Conference on Intelligent Systems, Modelling and Simulation (pp. 205-210). IEEE.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering version 2.3. Engineering, 45(4ve), 1051.

Lawal, B. H., & Nuray, A. T. (2018a). Improving Software Defined Network Security via sFLow and IPSec Protocol. Anadolu University Journal of Science and Technology A-Applied Sciences and Engineering, 19(3), 555-564.

Lawal, B. H., & Nuray, A. T. (2018b, May). Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN). In 2018 26th Signal Processing and Communications Applications Conference (SIU) (pp. 1-4). IEEE.

Maziku, H., Shetty, S., & Nicol, D. M. (2019). Security risk assessment for SDN-enabled smart grids. Computer Communications, 133, 1-11.

Prakash, A., & Priyadarshini, R. (2018, April). An intelligent software defined network controller for preventing distributed denial of service attack. In 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 585-589). IEEE.

Ravi, N., & Shalinie, S. M. (2021). Self-Corrected Belief-Propagation Decoder for Source Coding With Unknown Source Statistics. IEEE COMMUNICATIONS LETTERS, 25(7), 2146-2150.

Singh, D., Ng, B., Lai, Y. C., Lin, Y. D., & Seah, W. K. (2019). Analytical modelling of software and hardware switches with internal buffer in software-defined networks. Journal of Network and Computer Applications, 136, 22-37.

Siregar, B., Purba, R. F. D., & Fahmi, F. (2018, November). Intrusion Prevention System Against Denial of Service Attacks Using Genetic Algorithm. In 2018 IEEE International Conference on Communication, Networks and Satellite (Comnetsat) (pp. 55-59). IEEE.

Tatang, D., Quinkert, F., Frank, J., Röpke, C., & Holz, T. (2017, November). SDN-Guard: Protecting SDN controllers against SDN rootkits. In 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) (pp. 297-302). IEEE.

Thomas, R. M., & James, D. (2017, August). DDOS detection and denial using third party application in SDN. In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (pp. 3892-3897). IEEE.

Townsley, C. (2018). Are businesses getting complacent when it comes to DDoS mitigation?. Network Security, 2018(6), 6-9.

Varghese, J. E., & Muniyal, B. (2021). An efficient ids framework for ddos attacks in sdn environment. IEEE Access, 9, 69680-69699.

Wang, H., Xu, L., & Gu, G. (2015, June). Floodguard: A dos attack prevention extension in software-defined networks. In 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (pp. 239-250). IEEE.

Wang, T., Guo, Z., Chen, H., & Liu, W. (2018). BWManager: Mitigating denial of service attacks in software-defined networks through bandwidth prediction. IEEE Transactions on Network and Service Management, 15(4), 1235-1248.

Wieringa, R., Maiden, N., Mead, N., & Rolland, C. (2006). Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. Requirements engineering, 11(1), 102-107.

Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2015). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE communications surveys & tutorials, 18(1), 602-622.

Zhang, M., Bi, J., Bai, J., & Li, G. (2018, August). Floodshield: Securing the sdn infrastructure against denial-of-service attacks. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 687-698). IEEE.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 01/12/2021
Aceitação/Acceptance: 08/02/2022

Análisis previo para la implementación de un plan de instrucción y entrenamiento estándar NATO en el sistema remotamente pilotado Scaneagle

Capitán Tiria Contreras Christian Mauricio

christian.tiria@fac.mil.co

[1] Vinculación del primer autor, Comando Aéreo de Combate N°3, 083021, Malambo-Atlántico, Colombia.

Pages: 276-287

Resumen: De acuerdo al cumplimiento de la misión, visión y alineado a la Estrategia para el desarrollo aéreo y espacial de la FAC, en los cuales el entrenamiento y la interoperabilidad son unos de los puntos clave en el del desarrollo de las operaciones aéreas; se proyecta la necesidad de integrar los estándares NATO a la operación del Sistema Remotamente Pilotado ScanEagle, por ello este artículo muestra la comparación realizada de las habilidades establecidas por el STANAG 4670 y el manual-fac-7.2.1-c-scaneagle-restringido- programa de instrucción y entrenamiento, décimo quinta edición, septiembre de 2021, así mismo conocer el estado actual de la población objetivo a través de un elemento primario de investigación y el análisis de los datos del programa Fligth Data Analysis (FDA) con el fin de ajustar el Programa de Instrucción y Entrenamiento y estructurar el plan de capacitación, que permita llevar a cabo el Diplomado UAS Clase I bajo standard NATO. Para ello se utilizó como población objetivo de investigación el personal de pilotos operadores de la FAC.

Palabras-clave: Remotely Piloted Aircraft(RPA); NATO; estándar; Fligth Data Analysis(FDA); interoperabilidad.

Analysis for the implementation of a NATO standard instruction and training plan in the Scaneagle remotely piloted system.

Abstract: According to the fulfillment of the mission, vision and aligned with the Strategy for Air and Space development of the FAC, in which training and interoperability is one of the key points in the development of air operations, it generates the need to integrate the NATO standards to the operation of the ScanEagle Remotely Piloted System, for this reason this article shows the comparison made of the skills established by the STANAG 4670 and the manual-fac-7.2.1-c-scaneagle-restricted- training program and training, fifteenth edition, September 2021, as well as knowing the current status of the target population through a primary element of research and the analysis of data from the Flight Data Analysis (FDA) program in order to adjust the Program of Instruction and Training and structure the training plan, which allows carrying out the Class I UAS Diploma under NATO standard. To this end, the FAC operator pilot staff was increased as the target research population.

Keywords: Remotely Piloted Aircraft(RPA); BORN; standard; Flight Data Analysis(FDA); interoperability.

1. Introducción

La Fuerza Aérea Colombiana (FAC) enfrenta grandes desafíos en el desarrollo de las actividades que le permiten cumplir la misión y visión institucional. La evolución del conflicto armado interno, que ha migrado en un contexto de guerra de 5 generación, la combinación de múltiples formas de lucha por parte de los enemigos del estado colombiano, así como las crecientes amenazas internacionales, la integración de Colombia como socio global de la NATO, la participación y desarrollo de ejercicios conjuntos en los cuales la interoperabilidad con otras fuerzas y países aliados es el objetivo principal a desarrollar; la escuadrilla de vuelo básico de la Escuela de Aeronaves Remotamente Tripuladas, se ve en la necesidad de plantear la hoja de ruta a seguir para alinear la instrucción y entrenamiento de las tripulaciones del sistema ScanEagle, acorde a los estándares NATO y así garantizar el concepto de interoperabilidad en estos escuadrones de la fuerza.

Tanto ha sido su auge que el uso de estas herramientas tecnológicas que permiten mantener el comando y control de las operaciones en tiempo real, y/o que permitan ser el primer respondiente en una situación adversa se han convertido hoy en día en los ojos del comandante en un teatro operacional.

Es por ello que el desarrollo del presente artículo analiza el contexto actual de instrucción y entrenamiento utilizado por los pilotos operadores del sistema ART -ScanEagle de la FAC, en comparativa con los estándares de la NATO, dejando ver las necesidades presentes y planteando la base para la modificación de la doctrina acorde a las necesidades de la Fuerza en pro del cumplimiento de los objetivos definidos.

2. Interoperabilidad

Para Farrow (2016), durante la guerra de Vietnam el uso de las aeronaves sin piloto por parte de la Fuerza Aérea de los Estados Unidos [USAF] se catapultó en el desarrollo de misiones de inteligencia, pero fue hasta el año de 1994 cuando la primera aeronave con despegue automático fue puesta en funcionamiento. Acorde a lo estípulado por Santino(2020) psoterior al año 2001 y luego de los ataques del 11-S la inversión en herramientas tecnológicas y desarrollo de medios que protegieran la vida de las tropas en tierra, el programa de gobiernos de George Bush y posterior la administración Obama catapultaron el desarrollo de sistemas tales como los MQ-1 y MQ-9, los cuales fueron probados e iniciaron sus operaciones en la denominada guerra del terror, atacando las amenazas terroristas de oriente medio, con lo que se hizo visible el uso de estos sistemas en la integración de las fuerzas aliadas para el desarrollo de misiones de ataque e ISR.

La visión de la FAC (Disp. 026 2019), tiene inmersa en sus propósitos ser innovadora, polivalente, interoperable, líder y preferente regional, por ende, desde febrero de 2011 con la aceptación por parte de la USAF del escuadrón KFIR en RED FLAG 2012, la FAC logró llegar a la cima de la aviación militar, teniendo que adaptarse y modificar sus

procesos para poder participar en un ejercicio internacional. Este ejercicio fue el primero en el cual las tripulaciones y aeronaves abanderadas del país dejaron en alto el nombre de Colombia y la institución, desencadenando una serie de invitaciones y entrenamientos que han hecho de la FAC un referente regional en el desarrollo y participación de este tipo de entrenamientos como Ángel de los Andes, Relámpago, Green Flag, Cruxez entre otros, en los cuales las diferentes capacidades operacionales han sido puestas en práctica con los más altos estándares.

En 2018 con la formalización de Colombia como socio global NATO, el desarrollo de entrenamientos bajo estos estándares ha obligado al ajuste en el planeamiento y desarrollo de operaciones de los diferentes escuadrones de la FAC para garantizar la interoperabilidad, generando así una doctrina de operación global y estandarizada, acorde a las necesidades del entorno.

Desde la llegada de los sistemas ScanEagle a la institución en el año 2006, las capacidades de los sistemas remotamente pilotados en el teatro de operaciones han sido aprovechadas en nivel medio, sin explotar al máximo las mismas, y es solo hasta el año 2018 en la participación del ejercicio internacional Angel de los Andes, cuando se integro por primera vez el sistema a un ejercicio conjunto, resaltando la experiencia con la que contaban en ese momento sus tripulaciones, hasta hoy en día cuando el crecimiento exponencial del uso de estas aeronaves, persuadió a la Entidad Aeronautica de Aviación de Estado, regular su uso en el uso militar y definir unas habilidades mínimas para el uso de estos componentes en las diferentes situaciones operacionales.

En razón a lo anterior y despues 16 años de operación de los mismos en Colombia, y cuando el Ministerio de Defensa [MDN] cuenta con proyectos de desarrollo tecnológico en esta área del conocimiento, la planta operativa de los RPA ScanEagle es la más amplia de la Fuerza Aérea, ya que cuenta con 308 tripulantes, de los cuales 112 corresponden al cargo de CMA, 69 se encuentran formados como OPR, 69 técnicos tripulantes y 67 analistas de video, los cuales son formados y entrenado anualmente en el Escuela Básica de Aeronave Remotamente Tripuladas.

La definición de Doctrina Básica Aérea Espacial y ciberespacial[DBAEC] interpreta la aplicación del Poder Aéreo Espacial y Ciberespacial[PAEC] en los diferentes ámbitos y dominios, buscando alinearse a las organizaciones conjuntas e internacionales, con el fin de potenciar la interoperabilidad local, regional y global. Proyecta que todos los componentes de la fuerza se enfoquen en buscar la unidad ideológica que permita la participación de la FAC en coaliciones internacionales (DBAEC, 2020, p viii); y nos permite ubicar los sistemas remotamente pilotados dentro del poder aéreo con una necesidad latente de garantizar su interoperabilidad.

Acorde a lo mencionado con anterioridad y la iniciativa de la Escuadrilla de Vuelo Básica, y sentando como presente el documento ESDAES 2042, en conjunto con misión y visión de la FAC; se planteó la idea de integrar los estandares internacionales de instrucción y entrenamiento NATO, al Programa de Instrucción y Entrenamiento del Sistema ART ScanEagle como primer paso para la profesionalización de las tripulaciones y el acople del sistema como herramienta primordial en el desarrollo de operaciones que implique garantizar el comando, control y toma de decisiones en tiempo real.

3. Comparación de requisitos en instrucción y entrenamiento NATO vs FAC

La revisión previa de la documentación que pudiese llegar a tener injerencia en la instrucción, entrenamiento y operación del sistema remotamente pilotado ScanEagle por parte de la fuerza fue definida con anterioridad, y se encuentra alineada a la doctrina de la FAC para mencionados procesos. En el sector internacional, se realizó una amplia búsqueda en las diferentes regiones, con referencia a manuales y documentación de análisis para el empleo de sistemas remotos en entornos operacionales conjuntos, razón por la cual se seleccionó el documento NATO STANDARD ATP-3.3.7 GUIDANCE FOR THE TRAINING OF UNMANNED AIRCRAFT SYSTEMS (UAS) OPERATORS, Edition B Version 1, APRIL 2014, como documento regente en el estándar internacional, teniendo en cuenta que se encuentra desclasificado y permite efectuar una comparativa acorde con el MANUAL-FAC-7.2.1-C-SCANEAGLE-RESTRINGIDO- PROGRAMA DE INSTRUCCIÓN Y ENTRENAMIENTO, Décimo quinta edición, septiembre de 2021.

El primer ítem de referencia del presente análisis es definir la clasificación del sistema a estandarizar, y para ello podemos traer a colación la referencia NATO basada en la calificación del STANAG 4670 establecida en la siguiente figura:

NATO UAS CLASSIFICATION

Class	Category	Normal Employment	Normal Operating Altitude	Normal Mission Radius	Primary Supported Commander	Example Platform
Class III (> 600 kg)	Strike/ Combat*	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre	Reaper
	HALE	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre	Global Hawk
	MALE	Operational/Theatre	Up to 45,000 ft MSL	Unlimited (BLOS)	JTF	Heron
Class II (150 kg - 600 kg)	Tactical	Tactical Formation	Up to 18,000 ft AGL	200 km (LOS)	Brigade	Hermes 450
Class I (< 150 kg)	Small (>15 kg)	Tactical Unit	Up to 5,000 ft AGL	50 km (LOS)	Battalion, Regiment	Scan Eagle
	Mini (<15 kg)	Tactical Subunit (manual or hand launch)	Up to 3,000 ft AGL	Up to 25 km (LOS)	Company, Platoon, Squad	Skylark
	Micro ** (<66 J)	Tactical Subunit (manual or hand launch)	Up to 200 ft AGL	Up to 5 km (LOS)	Platoon, Squad	Black Widow

Figura 1 – Clasificación de los UAS acorde a la NATO

Se efectúo un análisis por parte de los instructores de vuelo del sistema y el director de la escuela de aeronaves remotamente tripuladas, en el que efectuaron el análisis y comparación de los requisitos establecidos en el ATP-3.3.7 y el PIE, dentro de los cuales se establece cuáles son los conocimientos generales de aviación con los que un operador debe garantizar las condiciones de seguridad de manera única en reglas visuales de vuelo (VFR), teniendo en cuenta que en ningún momento se operará un sistema RPA en reglas de vuelo instrumentos(IFR)de manera intencional, por lo cual se hace necesario definir los temas contemplados por el estándar y compararlos así como lo establecido en el documento guía para la formación de operadores de la FAC.

ÍTEM	STANAG	PIE FAC	OBSERVACIONES
Estructura y operacion del espacio aéreo	X	X	Establecido en el curso CAAOR requisito para ser operador RPA FAC. Se refuerza en el curso de tierra
Procedimientos del ATC y reaglas del aire	X	X	Establecido en el curso CAAOR requisito para ser operador RPA FAC. Se refuerza en el curso de tierra
Aerodinámica	X	X	Establecido en el curso CAAOR requisito para ser operador RPA FAC. Se refuerza en el curso de tierra
Sistemas de la aeronave	X	X	Se define en el curso de tierra de la aeronave
Rendimiento	X	X	Se define acorde a la aeronave en el curso de tierra
Navegacion	X	X	Establecido en el curso CAAOR requisito para ser operador RPA FAC. Se refuerza en el curso de tierra
Meteorologia	X	X	Establecido en el curso CAAOR requisito para ser operador RPA FAC. Se refuerza en el curso de tierra
Procedimientos de comunicaciones, incluyendo competencias en el ICAO 4	X		Se tiene un nivel requerido acorde a la directiva de idiomas extranjeros, pero no alineada al ICAO 4
Preparación de la misión	X	X	Establecido en el curso CAAOR requisito para ser operador RPA FAC. Se refuerza en el curso de tierra

Tabla 1 – Conocimientos generales de aviación

De lo anterior se pudo definir que los conocimientos aeronáuticos establecidos por la FAC, se encuentran acorde a los definidos por el estándar internacional, observando una opción de mejora en el nivel de inglés establecido para la operación de los sistemas en un ambiente conjunto, por lo cual se deberá verificar con el ente de regulación académica de la fuerza, una paso a paso para garantizar que el personal de operadores cuente con un nivel de inglés ICAO 4, así mismo deja ver que el nivel académico con el cual se instruye al personal de operadores de la FAC es alto, y que ciertos temas de vital importancia como las regulaciones aéreas y las comunicaciones aeronáuticas, se ven enseñan en

un curso requisito para su formación como operadores y luego de ello se refuerzan los conceptos durante su curso de tierra.

Teniendo en cuenta las habilidades nombradas con anterioridad, se deberá garantizar unas habilidades básicas, las cuales mediante una escala nos permite clasificar el conocimiento del operador acorde a la necesidad de la operación. El standard define para la aeronave ScanEagle un nivel básico de calificación nivel 2:

BUQ Level II: Knowledge and skills required to operate under VFR in ICAO Class D, E, F, and G, and Restricted/combat airspace below 5000 ft (1500 m) AGL. NATO Class I, Small UAS operators are to be trained to BUQ Level II.

Pero, teniendo en cuenta las circunstancias de operación del sistema en Colombia a través de los años, y las áreas de vuelo que normalmente se encuentran establecidas mediante as diferentes cartas de acuerdo, se debe adoptar como calificación mínima requerida el nivel de habilidades, definido de la siguiente manera:

BUQ Level III: Knowledge and skills required to operate under VFR in all ICAO airspace except Class A below 18,000 ft (5500 m) AGL or FL180. NATO Class II, Tactical UAS operators are to be trained to BUQ Level III.

Teniendo como precedente las capacidades básicas de entrenamiento se realizó la analogía entre los niveles de competencias específicas acorde a la siguiente tabla:

ÍTEM	STANAG	PIE FAC	OBSERVACIONES
Nivel de conocimeinto del tema	X	X	Establecido en el PIE como el SABER
Nivel de conocimiento de la tarea	X	X	Establecido en el pie como el SABER
Nivel de rendimiento al ejecutar la tarea	X	X	Establecido en el PIE como el SER
Convivir		X	En el stanag nos e encuentra definida esta habilidad blanda que permita medir su integración a la tripulación.

Tabla 2 – Habilidades de acuerdo a las capacidades

Acorde a la comparativa anterior y rigiéndose al standard, un operador de UAS, deberá tener las siguientes habilidades:

Nivel de conocimiento del tema C: de tal manera que pueda analizar los factores y principios que le permitan concluir a cerca del tema.

Nivel de conocimiento de la tarea C: de tal manera que pueda identificar por qué y cuando la tarea debe ser realizada, y por qué cada paso es necesario.

Nivel de rendimiento al ejecutar la tarea 3: de tal manera que pueda ejecutar todas las fases de la tarea, solo deberá verificar ser chequeada la tarea ejecutada.

Estos niveles de pericia en la ejecución de las tareas y la verificación de los procedimientos, se encuentran definidas para la FAC en el cuadro de misiones acorde a las fases del curso

de vuelo, de tal manera que se puedan evaluar y garantizar las siguientes estructuras: tareas de planeamiento de la misión, categoría de contacto, categoría de navegación, categoría de emergencias y categoría post vuelo.

Con lo anterior se evidencia en la estructura de enseñanza, que la forma de enseñanza y exigencia al personal de operadores de la FAC, es bastante riguroso, acorde a lo establecido en el PIE, y para alinearse al standard, el esquema de notas y niveles de evaluación, deberán homologarse y ajustarse acorde a cada competencia, teniendo en cuenta que el standard identifica el nivel de conocimiento del tema y conocimiento de la tarea en niveles de la A hasta la D donde la D es la más alta, y el nivel de ejecución de la tarea en una escala de 1 a 4, donde 4 es el nivel más alto; mientras que en la FAC, las tres habilidades se califican en un solo ítem con clasificación de A hasta C, donde la C es la calificación más baja, teniendo como referencia una calificación de N para definir que el alumno no tiene la competencia.

Por tal motivo estaría pendiente efectuar la propuesta para el ajuste en la forma de calificar un alumno en el proceso de formación.

4. Análisis de estado actual de la planta de operadores ScanEagle de la FAC

Una vez teniendo como referencia la comparación de la guía de instrucción y entrenamiento de la NATO, se procedió a elaborar un medio primario de investigación que permitiera identificar el estado actual del conocimiento general de conocimiento en cuanto a operación de la aeronave, en procedimientos normales, ejecución de técnicas de reconocimiento y conocimiento de normatividad internacional en la ejecución de operaciones conjuntas, de la siguiente manera:

La población total de OPR en la FAC es de 69 oficiales del cuerpo de vuelo, logístico, mantenimiento o seguridad y defensa de bases, los cuales se encuentran asignados al CACOM-1-3-5-6-7, Grupo Aéreo del Casanare y Componente Aéreo FTC-Omega, y cumplen con las disponibilidades en los 16 puntos de operación que se encuentran desplegados por toda Colombia, de los cuales se seleccionó una muestra de 28 operadores para la aplicación de la herramienta.

ACTOR	VALORES
Tamaño muestra (n)	28.4229 OPR
Tamaño población (N)	69 OPR
Nivel de confianza (Z)	0.95
Probabilidad de éxito (P)	0.95
Probabilidad de fracaso (Q)	0.05
Precisión (D)	0.03

Tabla 3 – Selección de la muestra

En cuanto a los resultados del medio aplicado, podemos definir que el puntaje máximo de calificación eran 1000 puntos, de los cuales los resultados esperados, eran un promedio por encima de 800 puntos como media, teniendo en cuenta el tiempo de operación del sistema en la fuerza, y la anualidad con la que se evalúa el desempeño de cada operador y el nivel de complejidad del entrenamiento. En la estadística de campo se identifican no conformidades acordes al desempeño de los operadores en los procedimientos y modo de empleo del sistema.

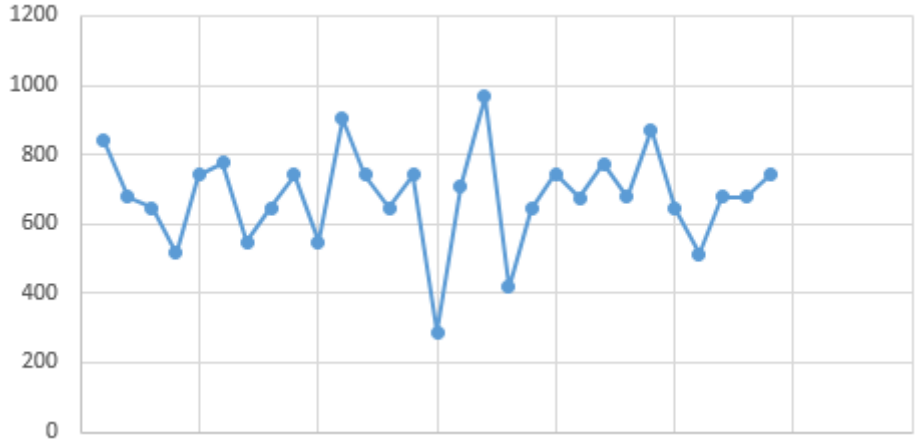


Figura 2 – Media de resultados acorde a la encuesta

La muestra de la investigación tiene oficiales del grado ST al grado MY, quienes pueden tener entre 1 y 10 años de experiencia en operaciones de ISR, por tal motivo se genera la preocupación por el resultado por debajo de lo esperado, lo cual genera una incertidumbre, teniendo en cuenta que el medio fue desarrollado en el idioma inglés, dado que el standard está dado en mencionado idioma, y en los conceptos de interoperabilidad la NATO, tiene como idiomas de comunicación el inglés y el francés, lo cual genera esa brecha en el resultado, sin embargo teniendo como precedente mencionados resultados, se planteó revisar el programa de análisis de datos de vuelo, que tiene establecida la Escuela de aeronaves remotamente tripuladas y a cargo de una oficial perteneciente a la escuadrilla de vuelo, conllevando al siguiente análisis.

Se parte de los datos de vuelo analizados por el personal de supervisores de vuelo de las diferentes unidades militares aéreas, donde opera el sistema ScanEagle, identificando los siguientes factores:

En mencionado análisis de los datos de vuelo, se observa como los operadores presentan falencias en los procedimientos de calentamiento del motor, incrementando el riesgo de sufrir una apagada de motor en vuelo y colocar en riesgo la misión y la aeronave, así como otro factor de las rutas utilizadas para el despegue.

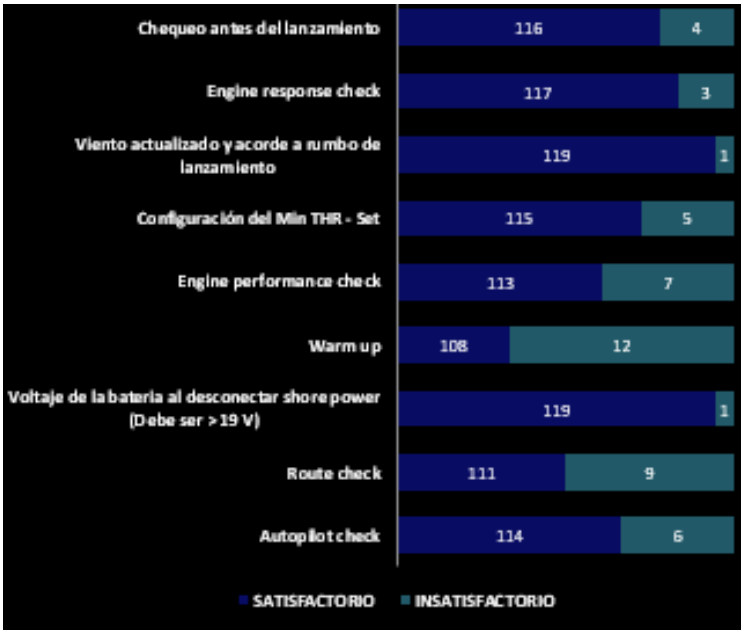


Figura 3 – Procedimientos críticos en el despegue y desviaciones

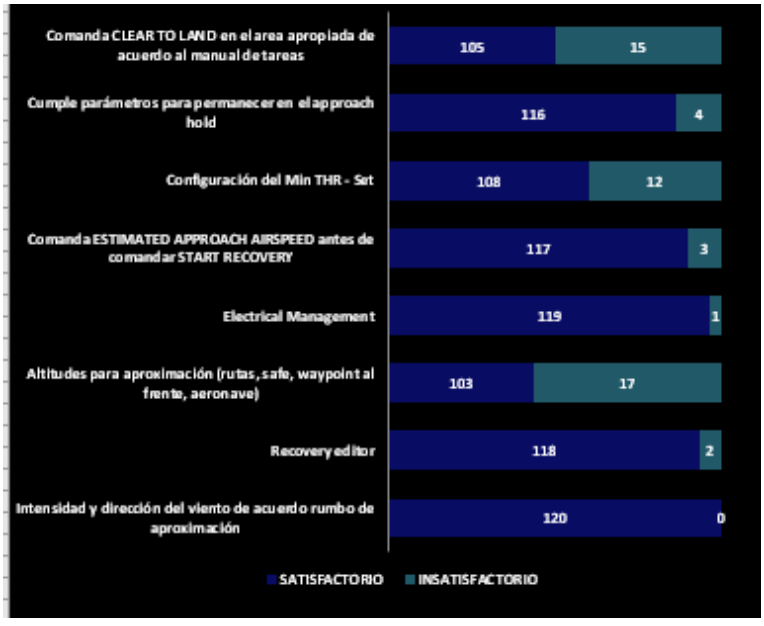


Figura 4 – Procedimientos críticos en el aterrizaje y sus desviaciones

En cuanto a la fase de aterrizaje se observa una desviación bastante alta al momento de comandar la aeronave a final, incrementando el riesgo de sufrir un accidente al mantener la aeronave orbitando a bajo nivel durante el momento antes de aterrizar, así como las altitudes configuradas para la aproximación, dadas las diferencias y malas configuraciones, que pudieran causar un CFIT.

Con estos tres análisis y la información recolectada se puede llegar a paso a las siguientes conclusiones en cuanto al análisis para la implementación del STANAG 4670 ATP-3.3.7 al programa de instrucción y entrenamiento de Scaneagle en la FAC.

5. Conclusiones

El PIE de ScanEagle en la FAC, es un programa robusto y establecido con factores que pueden conllevar un ajuste a las necesidades que permitan alinearse al NATO STANDARD ATP-3.3.7 GUIDANCE FOR THE TRAINING OF UNMANNED AIRCRAFT SYSTEMS (UAS) OPERATORS, Edition B Version 1, APRIL 2014, teniendo en cuenta las matrices de comparación que fueron realizadas, que permitirán determinadas opciones de mejora del programa de instrucción y entrenamiento de los actuales y futuros pilotos operadores del sistema en la FAC, entre ellos la estandarización de los factores de evaluación, los modos y escalas de calificación y demás tópicos relevantes en los procesos educativos.

El programa de Instrucción y Entrenamiento ScanEagle, se encuentra enfocado a la forma en como realizamos los procedimientos de vuelo, garantizando los procesos de seguridad, generando la necesidad de fortalecer el proceso de explotación de la herramienta y el desarrollo de técnicas para su empleo, que se encuentran definidas, pero que se identifican opciones de mejora que facilitarán el cumplimiento de la misión. Es por ello que acorde a las mesas de trabajo realizadas, los análisis de proyección de la presente investigación y los lineamientos de la Escuela Básica de aeronaves Remotamente Tripuladas, se deberá proyectar la estructuración de un Diplomado en el uso y explotación de los sistemas UAS en la FAC con estándares NATO.

El enlace de los tres puntos de análisis del presente documento, nos deja ver que tenemos una estructura académica fuerte, con las necesidades de fortalecimiento del idioma inglés, identificado en la estructura de la formación que es redundante en el elemento primario de investigación. Así mismo en las opciones de mejora identificadas en cuanto a procedimientos normales tanto en el análisis del programa de datos de vuelo y la herramienta primaria aplicada, generan la necesidad de efectuar una revisión a la forma de entrenamiento anual de los operadores, con el fin de fortalecer el proceso de formación, y por último el presente documento nos deja ver la importancia de concatenar los diferentes puntos de vista en el desarrollo de una investigación, con el propósito de estructurar o modificar un proceso formativo que permita la evolución de la doctrina institucional acorde a las necesidades de la fuerza.

Referencias

Acuña Lizarazo, M. E. (2016). Drones, nuevos panoramas para la aviación: análisis comparativo de la normatividad internacional frente a la normatividad colombiana. Ciencia Y Poder Aéreo, 11(1). https://doi.org/10.18667/cienciaypoderaereo.524

Anderson, Dagvin R M, USAF.Air & Space Power Journal; Maxwell AFB Tomo 25, N.º 4, (Winter 2011): 54-64,1.

Aponte Castro, Diana Del Pilar, Andres Mauricio Palacios Silva, and Manuel Alexander Santamaría Álvarez. Líneas De Acción Como Estrategía En La Toma De Decisiones Para La Mitigación Y Reducción De La Accidentalidad A.R.T. Scaneagle a Partir De La Identificación Y Análisis De Los Eventos Entre Los Años 2013 Al 2016. 2018. Print.

Bejarano Parra, Autor, and Buitrago Benítez. Procedimiento Para La Instalación De Una Base De Lanzamiento De Aeronaves Remotamente Tripuladas En La Fuerza Aérea. 2019. Print.

Cárdenas Velandia, Oscar Javier, Jorge Andrés Correa Orejuela, Julián López Ramírez, and Charlie Solarte Ríos. La Necesidad Del Empleo De UAV En Seguridad Fronteriza. 2019. Print.

Echeverri Restrepo, Luis Eduardo, and Manuel Alexander Santamaría Álvarez. Diseño, Creación Y Propuesta De La Doctrina Para El Sistema De Aeronaves Remotamente Tripuladas Táctico Adquirido Por La Fuerza Aérea Colombiana. 2017. Print.

Farrow, A. (2016). La guerra con drones como instrumento militar de la estrategia antiterrorista. Air & Space Power. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-28_Issue-4/2016_4_02_farrow_s.pdf

López Aragón, Daisy Nathalie, and Diego L. Malpica. Análisis Y Clasificación De Factores Humanos En Eventos No Deseados De Seguridad Operacional (EVESOS) De Aeronaves Remotamente Tripuladas (ART) De La Fuerza Aérea Colombiana En El 2012. 2014. Print.

Páez López, G. A., Corzo Zamora, M. A., Díaz Ariza, A., & Rodríguez Guerrero, N. I. (2020). Herramienta de entrenamiento neuropsicológico para operadores de Aeronaves Remotamente Tripuladas ScanEagle. Ciencia Y Poder Aéreo, 15(1), 39-52. https://doi.org/10.18667/cienciaypoderaereo.658

Rodríguez, L. R. (2019). Colombia y la Organización del Tratado del Atlántico Norte: Aproximaciones de análisis desde la academia, 5. Análisis económico de la interoperabilidad de las Fuerzas Militares de Colombia con la Organización del Tratado del Atlántico Norte (NATO) (pp. 155-203). Escuela Superior de Guerra.

Sánchez Camelo, César Augusto, and Adriana Guzmán Pérez. Integración Del Sistema De Aeronaves Remotamente Tripuladas ART (scaneagle) Al Proceso Logístico De La Fuerza Aérea Colombiana. 2015. Print.

Sandoval Murillo, Rodriguez Beltran, Sánchez Quemba, Sánchez Muñoz, Martínez Rubiano, Vanegas Montoya, Martínez, Rodríguez Nelson, and Martínez, Alicia.

Szabolcsi, r. (2016). Uav operator training – beyond minimum standards. Scientific research and education in the air force, 18(1), 193–198. Https://doi.org/10.19062/2247-3173.2016.18.1.25

Zieliński T, (2017). Unmanned aircraft systems in support of the land forces. Selected issues. Zeszyty Naukowe Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. Tadeusza Kościuszki Journal of Science of the gen. Tadeusz Kosciuszko Military Academy of Land Forces, 49 (2), p. 195-210, DOI: 10.5604/01.3001.0010.4909

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 22/12/2021
Aceitação/Acceptance: 24/02/2022

Política de língua como vetor de projeção de poder: o caso de Timor-Leste

Rui Pereira[1], Luís Malheiro[2]

pereira.rms1@gnr.pt; malheiro.lcr@gnr.pt

[1] Centro de Estudos Globais da Universidade Aberta, Lisboa, Portugal

[2] Centro de Investigação Desenvolvimento e Inovação da Academia Militar, Academia Militar, Instituto Universitário Militar, Rua Gomes Freire, 1669-203, Lisboa, Portugal

Pages: 288-300

Resumo: A história demonstra que a estratégia na utilização de políticas da língua pelos estados tem impacto transversal em diversas em áreas, nomeadamente na segurança. Timor-Leste foi o primeiro país a surgir no século XXI e é detentor de uma diversidade linguística ímpar, motivo pelo qual foi escolhido para o presente estudo de caso sobre a estratégia seguida na política de língua. Assente em metodologia qualitativa, a investigação visou: compreender a importância da história no desenvolvimento linguístico e a opção pelas línguas oficiais e; analisar as tendências da política de língua em Timor-Leste. A análise dos dados recolhidos sugere que Timor-Leste é um exemplo onde as mudanças sociais influenciaram as políticas de língua. Objetivamente, a influencia da língua foi incontestável e transversal à política do estado no campo da manutenção da paz, da ordem e garantia do poder e dos direitos humanos. Apesar de tal, é notório que a efetivação da capacitação da população está depende da renovação geracional.

Palavras-chave: Timor-Leste; Política de língua; Estratégia; Segurança.

Language policy as a vector of power projection: the case of Timor-Leste

Abstract: History shows that the strategy in the use of language policies by states has a transversal impact in several areas, namely in security. Timor-Leste was the first country to emerge in the 21st century and has a unique linguistic diversity, which is why it was chosen for the present case study on the strategy followed in language policy. Based on qualitative methodology, the research aimed to understand the importance of history in linguistic development and the option for official languages and analyze trends in language policy in Timor-Leste. Analysis of the data collected suggests that Timor-Leste is an example where social changes have influenced language policies. Objectively, the influence of the language was indisputable and transversal to the state policy in the field of maintaining peace, order and guaranteeing power and human rights. Despite this, the effectiveness of the training of the population depends on generational renewal.

Keywords: Timor-Leste; Language policy; Strategy; Safety.

1. Introdução

O território de Timor-Leste é para a generalidade dos portugueses um país que suscita afetividade recíproca entre as duas nações e retratada num misto de sentimentos, que vão desde a nostalgia, de pertença e até de impotência. Este último caso é motivado pela memória muito recente da sua história e do sofrimento a que o seu povo foi sujeito, especificamente a luta pela independência e a criação daquele que foi o primeiro país do século XXI.

No campo da observação participante recordam-se as memórias "massacre do Cemitério de Santa Cruz", as movimentações de apoio da sociedade civil em Portugal e a celebração da independência de Timor-Leste. Objetivamente, foram desempenhadas missões pela Guarda Nacional Republicana (GNR), ao serviço das Nações Unidas, contribuir no apoio à estabilidade, segurança e desenvolvimento de Timor-Leste. Durante esse período de intervenção, o foco foi maioritariamente a manutenção da ordem pública e a segurança das populações. A comunicação diária com as populações locais era geralmente em português. Existindo, porém, timorenses que não dominavam a língua portuguesa e tendo a GNR esse conhecimento prévio, a comunicação era estendida ao Tétum-praça, recorrendo a intérpretes locais e através do uso diário e comum. Contudo, mesmo com a utilização do intérprete como intermediário na comunicação com o povo timorense, por vezes a transmissão da informação e a compreensão da mensagem era dificultada na ação, nos diferentes distritos de Timor-Leste.

Esta diversidade linguística do território motivou a realização da presente investigação sob o escopo de se aprofundar os conhecimentos relativos à diversidade linguística e à política de língua em Timor-Leste, procurando fundamentalmente alcançar dois objetivos: compreender a importância da história no desenvolvimento linguístico do seu povo e a opção pelas línguas oficiais, português e Tétum-praça; perspetivar quais as tendências da Política de Língua em Timor-Leste.

Para se atingir tal intento, recorreu-se a uma metodologia essencialmente qualitativa, baseada na revisão de literatura científica, alem das posições institucionais pela consulta de endereços eletrónicos de organizações e documentos oficiais e bem assim com recurso ao método de observação participante no caso do trabalho de campo para o estudo de caso em análise: Timor-Leste.

O trabalho é estruturado em quatro capítulos, além da introdução e da conclusão. No primeiro capítulo analisa-se a política de língua, que servirá de guia no estudo das línguas timorenses. No segundo capítulo é feita a análise necessária da história de Timor-Leste, para que se possibilite uma melhor compreensão da cultura e da evolução linguística timorense. No terceiro capítulo é efetuado o estudo da evolução da língua em Timor-Leste até à atualidade. O quarto capítulo refere-se uma abordagem às políticas de língua desenvolvidas e uma perspetiva de futuro linguístico em Timor-Leste.

2. Política de língua

A globalização é de facto algo incontornável e inegável no nosso mundo. O debate e os diversos estudos que têm surgido em torno deste fenómeno, revelam análises díspares

quanto à sua origem e conceptualização, mas concordantes quanto à necessidade de se analisar através de um prisma multidisciplinar.

A análise da política de língua e o planeamento linguístico são uma área de estudo recente. Porém, sem que tal fosse percecionado, as atividades ligadas a esta área já são utilizadas há muito tempo e estão diretamente ligadas ao próprio uso das línguas. Segundo Maria Mateus (2009), qualquer reflexão sobre política linguística se insere obrigatoriamente num cenário internacional de rede de interesses e de solidariedades institucional, sendo fundamental uma análise vasta e abrangente entre todos os intervenientes. Como realça R. Salomão (2007), o termo Planeamento Linguístico e, sobretudo, a diferença e a interação entre os conceitos de Planeamento e de Política têm sido menos evidentes, parecendo mesmo não existir a nível mais alargado, a consciência de que as políticas se consubstanciam num leque de múltiplas atividades, processos, métodos, agentes, etc. e que o seu Planeamento constitui a prossecução das Políticas".

Como grande referência desta área surge o trabalho desenvolvido por Robert L. Cooper, que na sua obra de *Language Planning and Social Change*, refere que para se compreender o planeamento da língua é necessário interpretar as alterações sociais. Nos anos oitenta, este autor constata que à época não existia uma definição clara de política de língua. Reconhece, porém, que o termo política de língua não foi o primeiro a surgir na literatura, tendo sido introduzido em 1959 por Haugen como "*the activity of preparing a normative orthography, grammar, and dictionary for the guidance of writers and speakers in a non-homogeneous speech community*" (Cooper, 1989, 29). Nesse sentido, Cooper reúne e apresenta doze conceptualizações, que surgiram após a de Haugen, de diferentes autores de referência que estudaram o planeamento linguístico. Utilizando estas definições, Cooper efetua uma análise assente em quatro questões: "Quem planeia?" – considera que a maioria das definições eram muito restritivas excluindo algumas iniciativas; "O que planeia?" – questiona-se sobre o foco e apresenta três tipos de planeamento, o *corpus*, o *status* e o *acquisition planning*; "Para quem?" – considera que algumas definições não mencionam os comportamentos de pessoas que se pretende influenciar e a que nível; "Como?" – considera que algumas definições ficam apenas pela gestão do processo e não integram outras interferências que não as planeadas. Com a análise efetuada às definições, Cooper conclui que a definição de planeamento linguístico deveria de ser mais aberta e não limitar quem planeia, para quem, nem o tipo de planeamento, devendo focar-se na influência de comportamentos e não na resolução de problemas. Assim, o autor apresenta uma décima terceira definição, que é a sua: "*Language planning refers to deliberate efforts to influence the behavior of others with respect to the acquisition, structure, or functional allocation of their language codes*" (Cooper, 1989, p.45).

Conforme referido no parágrafo anterior, Cooper considera três tipos de planeamento: o *status planning*, o *corpus planning* e o *acquisition planning*. O *status planning* refere-se aos esforços desenvolvidos para influenciar várias funções numa comunidade; está relacionado com a oficialização de uma língua, a sua definição e normalização, para Cooper (1989, p.110) "*a statutory official language is necessarily the outcome of status planning, a government's use of given languages for given activities need not be the outcome of deliberate planning*". Citando Steward (1968), Cooper menciona as funções do *status planning, "official, provincial, wider comunication, international,*

capital, group, educational, school subject, literary, religious"; acrescenta duas outras: comunicação social e de trabalho; conclui que o *status planning* está geralmente relacionado com alterações desejadas na função da língua, mas influenciado pelas elites e contra elites. Para Cooper, o *corpus planning* está relacionado com o desenvolvimento, manutenção e modernização da língua para o seu uso, tendo como funções tradicionais a "*graphization, standardization and modernization*", às quais sugere que seja acrescentado uma nova, "*renovation*". Segundo o autor, o *corpus planning* tem a responsabilidade de manter o sentimento de união com o passado, com a tradição e representar as redes de solidariedade entre a sociedade. "*If it serves elites, it serves the mass as well*" (Cooper, 1989, p.164). O *acquisition planning* refere-se à promoção da língua e pode ser distinguido quanto a metas e a métodos. Quanto a metas, Cooper considera que se podem dividir em três: aquisição como segunda língua ou línguas estrangeiras; reaquisição da língua; manutenção da língua. Quanto a métodos, pode ser por métodos diretos ou indiretos, considerando que pode ser por uma questão de oportunidade, por incentivo, ou simultaneamente os dois. É de salientar que Cooper considera que o planeamento linguístico está relacionado com as mudanças sociais pois, como afirma, "*the social change accompanies language planning is scarcely urprising, inasmuch as language planning, concerned with the management of change, is itself an instance of social change*" (Cooper, 1989, p.172). A mudança social está relacionada com diversos fatores complexos de analisar e relacionados entre si, como a população, o ambiente, as descobertas e invenções, a cultura, as crenças e tomada de decisão. O planeamento linguístico é muito complexo e difícil de teorizar, considerando Cooper que para uma se chegar a uma teoria, primeiramente é necessário chegar-se a uma teoria de mudança social, pois "*to plan language is to plan society*" (Cooper, 1989, p.190).

Percebendo a dificuldade de chegar a uma teoria única, os académicos foram desenvolvendo várias teorias mais restritas para problemas específicos. O planeamento linguístico não é algo novo e tem de ser entendido no seu contexto social, como parte da continuidade e da mudança social. Pode ser motivado por interesses materiais e não materiais, usualmente relacionados com o poder, ou mesmo como condição necessária para o desenvolvimento económico. A política de língua é influenciada pelas elites, mas serve as elites, as contra elites e também a comunidade em geral.

Mais recentemente, e no âmbito do Encontro da Associação Portuguesa de Linguística, abordando a temática de uma política de língua para o português, Maria Mateus (2009) define a política linguística como um conjunto de ações definidas e levadas e afeito pelas autoridades governativas de uma comunidade, que tendem em última análise ao benefício individual e coletivo dos cidadãos que utilizam a língua.

3. Breve história de Timor

A República Democrática de Timor-Leste localiza-se no sudeste asiático e faz fronteira terrestre com a Indonésia, relativamente próximo da Austrália. É constituída pelo lado oriental da ilha de Timor, pela ilha de Ataúro, ilha de Jaco e pelo enclave de Oecusse no lado Oeste da ilha de Timor; tem aproximadamente 15.000 km2 e cerca de 1 milhão de habitantes. Apesar de ser um país recente, tendo-se tornado independente apenas em 2002, a sua ligação ao mundo e a sua história global é muito antiga.

Estudos e descobertas arqueológicas demonstram que os povos locais tiveram as suas origens nas migrações provenientes numa primeira fase da Melanésia e posteriormente da Austronésia. De entre as descobertas que evidenciam as migrações da Melanésia há cerca de 40.000 a 60.000 anos, encontram-se algumas ferramentas em pedra, pinturas rupestres e destacam-se evidências da influência de línguas papuásicas, como fataluku, makalero, makasae e bunak. As migrações mais recentes, com cerca de 4500 anos da Austronésia, influenciaram as culturas locais com a introdução da agropecuária e de novas técnicas de cerâmica, sendo que ao nível das línguas faladas influenciaram o Tétum, Mambae e Kemak (Ramos, 2019, p.188-189).

Para se compreender a cultura timorense é necessário não só conhecer as influências referidas, mas também a história recente, com o impacto da ocupação por parte de Portugal e da Indonésia. Para a sua compreensão, refere-se António Soares (2015), que considerou três períodos para efetuar o enquadramento histórico-geográfico de Timor-Leste: o Período de Contacto (1511-1891); o Período Colonial (1891-1974) e o Período de Ocupação Indonésia (1975-1999).

3.1. Período de Contacto (1511-1891)

Os primeiros contactos que os portugueses estabeleceram com Timor ocorreram provavelmente em 1515, com a sua entrada na rede de comércio mais ampla de Sândalo, que já existia por essa altura. A partir do ano de 1576, com a chegada dos Padres Dominicanos, a presença portuguesa ganhou maior influência com a construção de várias igrejas. Quando em 1636 os portugueses foram expulsos pelos Holandeses de Solo, antiga base portuguesa para controlo da rede de comércio de Sândalo, e se fixaram em Kupang, atual região da indonésia, é que efetivamente houve presença oficial de Portugal no território e o aumento do prestígio dos Portugueses, da religião Católica e da língua portuguesa, que passou a ser ensinada e usada para além das relações comerciais. Os Padres procuravam catequisar e ensinar a língua portuguesa principalmente aos nativos mais influentes e ligados a lideranças, ganhando um status social de prestígio. Mas a língua portuguesa era apenas usada por uma parte da população, nomeadamente para a administração oficial, instrução, comércio, religião e interação com portugueses (Ramos, 2019, p.189). A presença de Portugal neste território não era muito estável neste período, pelo que era necessário recorrer a alianças com os diversos reinos, que iam alternando as suas posições com as influências exercidas pelos Portugueses e Holandeses. Devido às pressões e ataques provocados pelos holandeses, em 1769 a capital é transferida para Dili que "fomentou assim o cimentar da influência da Coroa Portuguesa e uma maior difusão do português, caracterizado pela abertura de escolas, seminários e igrejas em diversas localidades do atual país Timor-Leste" (Soares, 2015, p.17).

3.2. Período Colonial (1891-1974)

Este período é marcado pela transformação político-administrativa e económica, com influência nas relações entre timorenses e portugueses. Como refere André Ramos (2019, p.190) o objetivo desta época era manter alianças através de administração militar e judicial baseada nos direitos tradicionais, mas com a prevalência da autoridade portuguesa. A influência portuguesa mantinha-se restrita a uma pequena franja da população, sendo que a restante não era recetiva, o que deu origem a vários desacordos.

Houve a necessidade de reforçar a cultura de identidade portuguesa, que ocorreu por influência da generalização da língua, mas principalmente pela influência da religião católica. Com a II Guerra Mundial e apesar de Portugal ter adotado uma posição neutra, os timorenses foram afetados por ataques de japoneses e mesmo australianos, tendo morrido cerca de 50.000 mil timorenses, deixando marcas no território, que ainda nos dias de hoje tem efeitos com o aparecimento de munições desse período, maioritariamente na época das chuvas. Após a II Guerra Mundial, começaram a surgir os partidos timorenses, constituídos maioritariamente por elites locais e que se tornaram o embrião dos movimentos anticoloniais, que com a colaboração da igreja, nomeadamente a Diocese de Dili, divulgavam mensagens nacionalistas. A estes movimentos juntaram-se as pressões internacionais por parte da Organização Mundial das Nações Unidas (ONU) na promoção da descolonização. Assim, com as alterações provocadas pelo 25 de abril de 1974 e a consequente mudança de regime, foram autorizados a criação de partidos políticos para efetuar a transição do território, desancando-se na altura três: União Democrática Timorense (UDT) – favorável a um processo gradual; Associação Social Democrática Timorense (ASDT) que deu origem à Frente Revolucionária de Timor-Leste Independente (FRETILIN) – defensora da transferência imediata; Associação Popular Democrática Timorense (Apodeti) – que pretendia uma integração no território da indonésia (Ramos. André, 2019, p.191).

3.3. Período de Ocupação indonésia (1975-1999)

Com o desentendimento entre os principais novos atores políticos e o despoletar de um conflito armado entre eles, levou a que os portugueses se tenham retirado para a ilha de Ataúro, e que a Indonésia (já independente da Holanda), e solicitado por alguns membros da UDT, tenham invadido o País com as suas forças armadas no dia 07 de dezembro de 1975, depois de em 28 de novembro ter sido declarada a de independência unilateral de Timor-Leste. A intervenção das forças indonésias pretendia eliminar a oposição e cultura timorense, mas tiveram uma forte oposição apesar das disparidades de capacidades humanas e militares existentes em comparação com as Forças Armadas de Libertação e Independência de Timor-Leste (FALINTIL), braço armado da FRETILIN. Como resultado da ocupação as FALINTIL continuaram a usar a língua portuguesa e preservaram os símbolos de identidade e cultura timorense, o que permitiu ainda o reforço do espírito de sacrifício e de identidade do povo timorense. Graças a esse enquadramento e após o Presidente indonésio ter permitido a abertura parcial do território, o Papa João Paulo II fez questão de visitar o território e de chamar a atenção da comunidade internacional para o problema do domínio indonésio sobre o povo timorense. Seguiram-se uma série de acontecimentos marcantes na história de Timor-Leste, como o Massacre de Santa Cruz em 1991, a detenção de Xanana Gusmão em 1992, a atribuição do Prémio Nobel da Paz a José Ramos Horta em 1996, os movimentos internacionais do Bispo Dom Ximenes Belo, a autorização para a realização de um plebiscito de autodeterminação perante o qual o "SIM" da independência ganhou e que culminou com semanas de elevada violência. Perante esta situação de instabilidade, houve finalmente a necessidade de intervenção da ONU, com a International Force East Timor (Interfer) e a missão *United Nation Transitional Administration in East Timor* (UNTAET), para preparar Timor-Leste para a sua independência com poderes legislativos, regulamentares e executivos.

Assim, surge o período mais recente, o da independência, iniciado em agosto de 2001 com as eleições para a assembleia constituinte, ganha por Xanana Gusmão. Em dezembro seguinte, é feita pela Assembleia a declaração das duas línguas oficiais: o tétum e o português. A independência é oficialmente declarada em 20 de maio de 2002 e inicia-se o decréscimo da presença dos elementos das Nações Unidas no País. Contudo, a existência de conflitos sociais mantinha-se. Em maio de 2006 ocorre uma nova crise, que despoleta novamente a necessidade de apoio internacional para a estabilização de Timor-Leste, tendo Portugal enviado no imediato e através de acordo bilateral uma força da GNR, enquanto se preparava uma nova missão da ONU, a *United Nations Mission* in Timor-Leste (UNMIT). Como refere António Soares (2015), apesar da cooperação internacional e da identidade do povo timorense, num contexto de difícil situação política-económica-social, surgiram alguns conflitos sociais maioritariamente de ordem étnica, nomeadamente entre os *Loromonu* (população de oeste) e *Lorosae* (população de este), que se estende à própria questão das línguas e do estatuto que cada uma delas ocupava.

4. Evolução linguística em Timor

A questão das línguas em Timor-Leste é de extrema importância pois permite recolher informação sobre a história da origem do povo timorense, mas também pela importância que tem para o futuro da população e do país, assim como na sua inserção no mundo global.

Pela análise histórica já efetuada por alguns autores, e por não se conseguir identificar a existência de escritos, pode-se concluir que os povos que habitavam primeiramente em Timor eram ágrafos. Assim, e recorrendo à análise linguística, é possível verificar que as atuais línguas existentes em Timor-Leste são resultantes de dois grandes movimentos migratórios como referido no capítulo anterior, que deram origem às línguas faladas de proveniência Austronesia e Papusianas que acabaram por sofrer um processo de adaptação e crioulização local.

Segundo Davi Albuquerque (2010) as línguas existentes em Timor-Leste podem ser divididas em três grupos:

1. Grupo Fabrônico:
    a. Tétum – esta língua ao lado do português tem o status de língua oficial e é falada pela grande maioria da população, estando conotada com a identidade nacional pois foi a língua que se manteve em utilização após o português ter sido proibido durante o período de ocupação indonésio (era apenas utilizado na clandestinidade pela resistência), sendo também a língua selecionada pela igreja para a catequese e a melhor documentada entre as restantes, possuindo uma gramática;
    b. Habun – é considerada uma versão mais arcaica do Tétum e possui um número reduzido de falantes;
    c. Galolen – língua utilizada no distrito de Manatuto, possuindo uma gramática e um dicionário de galolen-português;
    d. Werarês – língua utilizada na ilha de Ataúro e possui três subdialetos: Resuk, Raklungu e Rahesuk;

e. Kawaimina – Trata-se de uma mistura dos dialetos Kairui, Midiki, Naueti e Waimoa, que são falados na zona leste de Timor-Leste, convivendo com línguas de origem Papuásicas;
f. Bekais – é utilizada na zona de Balibó, perto da fronteira com a Indonésia;
g. Dawan – é a língua utilizada através do dialeto Baikenu no enclave de Oecussi, o qual foi a capital até que em 1769 os Portugueses transferiram para Dili. Por esse motivo, é possível identificar alguma influência da língua portuguesa neste dialeto;
h. Makuva – língua sobre a qual não existe muita informação, pressupondo-se que é usada em rituais e não é atualmente transmitida às novas gerações.

2. Grupo Ramelaico:

a. Mambae – é uma língua que possui muitos falantes e alguns dialetos, sendo de uma morfologia simples e com influência Papuásica;
b. Tokodede – língua utilizada no distrito de Liquiçã e zonas envolventes, com uma morfologia isolante e com influência Papuásica;
c. Kemak – língua utilizada junto da fronteira com a Indonésia, com dialexico Papuásico e com influência do malaio;
d. Idalaka – formado pelos dialetos Idaté, Lakalei, Isni e Kawaimina; partilham características com as línguas do grupo anterior, considerada como proto-lingua do grupo Mamelaico.

3. Línguas papuásicas:

a. Fataluku – língua utilizada no distrito de Lautém e que apresenta uma variação dialetal. Como realça David Albuquerque (2010) o povo que fala esta língua é culturalmente diferente dos restantes povos de Timor-Leste;
b. Makasae – língua utilizada no distrito de Baucau, sendo uma das mais faladas em Timor-Leste;
c. Makalero – é uma língua muito semelhante ao Makasae e Fataluku, sendo uma língua intermédia entre as duas, utilizada na zona leste do país;
d. Bunak – Língua utilizada na região de Kemak, sendo a mais divergente das línguas Papuásicas.

Segundo Hull (2001, cit Albuquerque, Davi, 2010) "as línguas Timóricas são descendentes de uma única língua, o Proto-Timórico e os processos que geraram as diversas línguas timóricas modernas e suas respetivas crioulizações aconteceram num período da história mais recente". Segundo Davi Albuquerque (2010) o status de língua franca atribuída ao Tétum deve de ter acontecido antes da chegada dos Portugueses, por apresentar uma distribuição geográfica descontinua e três dialetos, o Tétum-praça, Tétum-Terik e Tétum-Belo, com variações mínimas entre eles.

Às línguas existentes em Timor-Leste acresce a língua portuguesa, que foi sendo implementada, mas sem colocar de lado as línguas nativas, pois constatamos que apesar dos séculos de presença dos portugueses, ainda nos dias de hoje se verifica a existência das línguas referidas no território de Timor-Leste. Este facto talvez se justifique por a existência de portugueses em Timor nunca ter sido muito elevada em número e por se ter considerado que o ensino e o estudo das línguas nativas iriam facilitar a difusão escolar e proporcionar uma maior aproximação com o povo nativo.

Perante um cenário multilinguístico, aquando da escolha da língua oficial para o País, foi gerada alguma discussão, tendo sido colocado com opções o Tétum-praça, a língua indonésia, a língua inglesa e a língua portuguesa. Um importante linguista australiano, Geofrey Hull, durante o 1º Congresso do Conselho Nacional de Resistência Timorense em 2000, defendeu que as línguas a adotar deveriam ser o Tétum-Praça e o português. A primeira por ser a língua Franca e a segunda pelas relações entre os dois países, nomeadamente por o português nunca ter obstruído as línguas maternas ao contrário da indonésia, e pela existência de harmonia e contribuições entre as duas línguas. Davi Albuquerque (2010) fez uma análise ao status e corpus, numa escala de 0-100, das línguas portuguesa e Tétum-praça, concluindo que durante o período colonial português (até 1974) a língua portuguesa tinha um status de 80 e corpus de 20, já o Tétum-praça tinha um status de 14 e um corpus de 75, situação típica de época colonial. No período de domínio Indonésio (1975-1999) a língua portuguesa tinha um status de 10 e um corpus de 15, o Tétum-praça tinha um status de 20 e um corpus de 68, isto porque durante o período de ocupação a indonésia afastou estas línguas para implementar a sua.

Com a aprovação da Constituição da Républica Democrática de Timor-Leste foi formalmente definida a existência de duas línguas com o status de Língua Oficial: o português e o Tétum-praça. Neste novo período o status da língua portuguesa voltou a subir para os 72 e o corpus ficou pelos 15, já o status do Tétum-praça aumentou para os 65 e o corpus para os 90. As línguas de trabalho, como previsto na Constituição da República Democrática de Timor-Leste, são o inglês e o bahasa indonésio, que seriam apenas de carácter temporário, mas que se têm mantido e ganho algum relevo na política e na sociedade timorense, especialmente o inglês.

5. Políticas de língua e perspetivas de desenvolvimento

O atual cenário linguístico requer a atenção por parte do Governo de Timor-Leste para o estudo do passado linguístico, da atualidade e das políticas a implementar na educação, para que exista uma clara orientação no caminho a seguir e não se corra o risco de sobrevivência e manutenção das suas línguas nativas e do português e Tétum-praça como línguas oficiais.

Após definidas as línguas oficiais, é necessário elaborar a descrição gramatical da língua, o referencial teórico a ser usado para que exista uma independência linguística em todas as áreas do conhecimento minimizando a utilização de outras línguas. "A elaboração da gramática da língua, sua publicação e distribuição, servem como base para a comunidade começar a pensar o ensino da sua língua paralelamente ao ensino das línguas oficiais nas escolas. Dessa forma, a língua nativa quando começar a ser ensinada nas escolas: estará protegida da ameaça de redução do número de falantes, servirá como um instrumento para a comunidade manter e eternizar as suas tradições e formas de pensamento, terá o seu registo social aumentado e estará devidamente documentada (...) esse processo servirá como um instrumento para a revitalização das línguas nativas timorenses que estão ameaçadas" (Albuquerque, 2010, p.50).

O I Governo Constitucional apresentou o Plano de Desenvolvimento Nacional em 2002, que tinha como um dos pilares mais importantes a educação para reduzir a pobreza, referindo-se nos objetivos à necessidade de facilitar a transição para as línguas oficiais

no âmbito da educação escolar, apesar de a grande maioria das escolas ter sido destruída pela ocupação indonésia e de terem um grande trabalho pela frente.

O Ministério da Educação e Cultura Timorense foi criado em 2006 já durante o II Governo Constitucional. acompanhado de dois importantes documentos, a Lei Orgânica do Ministério da Educação e a Política Nacional de Educação e Cultura 2006-2010. Ambos reforçavam a necessidade de acelerar a educação das línguas oficiais nas escolas, prevendo o português como língua de instrução e que os materiais de ensino primário deveriam ser em português.

Durante o curto período do III Governo Constitucional foi elaborado um estudo para avaliar as políticas educativas, que apresentou como resultados a necessidade de aumentar a taxa de retenção nas escolas, melhoria do desempenho dos alunos, necessidade de um quadro de professores, melhoria das condições das escolas e a necessidade de se ultrapassar as dificuldades no uso das línguas de instrução.

Já com o IV Governo Constitucional é feita uma revisão da Política Nacional de Educação e aprovada uma nova Lei de Bases da Educação que estabeleceu o ensino obrigatório e gratuito até ao 9.º ano e medidas para que o ensino pudesse chegar efetivamente a todos. Esta Lei mantém o português e o Tétum-praça como línguas de instrução, mas abre a oportunidade para que no ensino básico pudesse ser ensinada outra língua e o reforço das línguas e cultura timorenses.

Em 2011 com a apresentação do Plano Estratégico Nacional da Educação (2011-2030) surge a iniciativa de se poderem utilizar as línguas maternas no início da escolaridade como línguas base, como resultado de alguns estudos que comprovam que o seu uso no início do ensino facilita a aprendizagem e potencia a aquisição de competências. Assim, surge o projeto teste de Educação Multilingue Baseada na Língua Materna (EMBLI), iniciado em 2013, usado em "apenas três línguas maternas, faladas em três distritos diferentes: o Fataluku, em Lautém; o Galolen, em Manatuto; e o Baikeno em Oecussi" (Ramos, 2019, p.200). Esta iniciativa gerou alguma controvérsia no Parlamento timorense pela preocupação com a questão da cultura, coesão e identidade timorense.

Com o V Governo Constitucional foi assumida a possibilidade de ensino Multilingue com base nas línguas maternas timorenses como línguas de instrução no ensino básico e pré-escolar, colocadas em ação através do Plano do Ministério da Educação 2013-2019.

Foi durante o VI Governo Constitucional que foram apresentados os resultados do projeto EMBLI iniciado em 2013, referindo que essa metodologia permitiu aumentar o desempenho escolar, nomeadamente nas áreas mais rurais e que costumavam apresentar priores resultados. Perante estes dados, em 2018 o VIII Governo Constitucional manteve o programa e alargou até ao final do 6.º ano do ensino básico, destacando ainda assim o importante papel das línguas oficiais, tendo sugerido que no ensino superior o primeiro ano fosse para reforçar as competências linguísticas das línguas oficiais e outras competências básicas.

António Soares (2015, p.77) salienta que "O facto do atual Governo intervir sobre a função social das línguas presentes em Timor-Leste, representa uma intervenção do próprio Estado numa área que não é do teor da Política de Línguas, mas sim no que poderemos considerar de Planeamento Linguístico. O Estado é que decide aqui se as línguas devem

ou não continuar a existir, se estas devem ou não continuar a ser usadas pelos seus falantes, em que contexto estas devem ser usadas." Fruto da sua investigação, considera que a continuidade das línguas oficiais dependerá da intenção dos falantes, pela função e utilidade que lhes dão, assim com as línguas maternas também dependerão da vontade dos falantes e não de legislação governamental".

Timor-Leste é um país recente e está a ganhar maturidade democrática, o que lhe permite consolidar políticas e seguir estratégias nacionais, nomeadamente no que diz respeito à educação, perspetivando-se uma cada vez maior implementação de um sistema de educação com qualidade e sucesso no desempenho dos alunos e no reforço das competências linguísticas e culturais timorenses.

6. Conclusões

A análise da evolução histórica de um país é fundamental para que se possa compreender a formação da sua cultura, da sua sociedade e da sua língua. No caso de Timor-Leste, apesar de ser o primeiro país do seculo XXI, é igualmente importante.

Os primeiros registos da história de Timor-Leste remetem-nos para dois grandes movimentos migratórios com proveniência Austronesia e Papusiana, que ainda nos dias de hoje tem impacto, nomeadamente ao nível linguístico. Essa influência sobre o Proto-Timórico permitiu que se emancipassem dezasseis diferentes línguas que podem ser agrupas em três grandes grupos, consoante a influência que receberam: Grupo Fabrônico (Tétum, Habun, Galolen, Werarês, Kawaimina, Bekais, Dawan, Makuva); Grupo Ramelaico (Mambae, Tokodede, Kemak, Idalaka); Línguas Papuásicas (Fataluku, Makasae, Makalero, Bunak). Estas línguas foram capazes de sobreviver ao Período de Contacto com o Português (1511-1891), ao Período Colonial Português (1891-1974) e ao Período de Ocupação Indonésia (1975-1999), que antecederam o atual período da independência.

Com a independência de Timor-Leste, existiu a necessidade de definir quais as línguas a adotar. Nesse momento, estes períodos recentes da história foram determinantes para a eleição do Tétum-praça e do português como línguas oficiais e o Bahasa Indonésio e o inglês como línguas de trabalho. Para estas escolhas foi determinante o facto de o Tétum-praça ser a língua franca e mais bem documentada em Timor-Leste, e o português pelas relações entre os dois países designadamente por nunca se ter obstruído as línguas maternas e pela existência de harmonia e contribuições entre as duas línguas. Sendo que, atualmente, o Tétum-praça comparativamente com o português ganhou relevo quanto ao status e ao corpus, e as línguas de trabalho têm ganho algum relevo na política e na sociedade timorense.

Timor-Leste, enquanto democracia, tem vindo a ganhar maturidade, apesar dos anos de agitações populares que teve. Essa maturidade permite gerar alguma serenidade para seguir estratégias e políticas de educação, que têm vindo a ser implementadas ao longo dos diferentes governos constitucionais e que foram surgindo em busca de uma educação de qualidade e de sucesso escolar. Ao nível do ensino da língua é de realçar a possibilidade de ensino multilingue. Este tipo de ensino permite que os alunos no ensino pré-primário e primário possam utilizar as suas línguas maternas, tendo já como

provas dadas a melhoria da aquisição de competências e de aprendizagem, mas que gerou também alguma controvérsia por poder colocar em causa a questão da identidade e da coesão nacional de Timor-Leste.

Interpretando os dados materiais publicados pelos diferentes governos e também pelos vários resultados apresentados, a perspetiva é que este tipo de ensino se continue a manter, salvaguardando-se a importância dada às línguas oficiais e com a continuidade da utilização das línguas de trabalho pela população. O prosseguimento da língua portuguesa continua a ser um elo entre a cultura Portuguesa e Timorense, potenciando o trabalho em conjunto que tem sido desenvolvido quer através de acordos bilaterais e multilaterais, quer através da Comunidade de Países de Língua Portuguesa, para facilitar de forma conjunta um desenvolvimento sustentável e humano, assente numa ligação cultural e linguística no atual mundo global.

Assim, afigura-se que a política linguística em Timor-Leste tem sido materializada por um conjunto de iniciativas e ações levadas a cabo maioritariamente pelos Governos Constitucionais na busca de uma maior capacitação da sua população ao nível linguístico, de aquisição de competências e de desenvolvimento. Sem dúvida que o caso de Timor-Leste é um exemplo concreto em que as mudanças sociais que ocorreram no território influenciaram as políticas de língua seguidas. Ou seja, tal como aconteceu noutros períodos da história mundial, referindo-se ao contexto social, à manutenção da paz, da ordem e garantia do poder e de direitos, a importância do poder da língua é incontestável e transversal às políticas dos estados. Ao longo dos tempos a língua surge aliada à unidade nacional e ao fortalecimento de autonomias. Tal como se prevê em relação a Timor-Leste, a implementação de políticas de língua é refém dos processos de renovação geracional, isto é, não terá resultados imediatos e poderá levar gerações a produzir efeitos de implementação efetiva.

Referências

Albuquerque, Davi. (2010). As línguas de Timor-Leste: perspetivas e prospetivas. *Revista de Língua e Literatura*. v.27, p. 313-335

Albuquerque, Davi; Taylor-Leech, Kerry. (2012). Política linguística para as línguas oficiais em Timor-Leste: o português e o tétum-praça. *Niterói nº32*. p.153-169

Bernardino, L. Leal, J. S. (2011). A arquitetura de segurança e defesa da comunidade dos países de língua portuguesa, *IDN Cadernos n.º 6* ed. Lisboa: Instituto Defesa Nacional.

Cooper, Robert L. (1989). *Language Planning and social change*. Cambridge, Cambridge University Press

Mateus, Maria. (2009). Uma política de língua para o português. *Encontro da Associação Portuguesa de Linguista*. FLUL. Lisboa

Ramos, André Gonçalves. (2019). Língua Portuguesa em Timor-Leste: percurso Histórico e Políticas atuais para a manutenção da língua. *Línguas & Letras*. n. º46 v.20. p. 187-206

Salomão, R. (2007). *Línguas e Culturas nas Comunicações de Exportações: Para uma Política de Línguas Estrangeiras ao Serviço da Internacionalização da Economia Portuguesa*. Universidade Aberta. Lisboa

Soares, António José de Oliveira. (2015). *Políticas de línguas e Planeamento Linguístico em Timor-Leste: Língua Portuguesa e Línguas Locais no sistema de Ensino Timorense*. Universidade Aberta

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 30/10/2021
Aceitação/Acceptance: 20/01/2022

Avaliação da Rotina Operacional do Operador Nacional do Sistema Elétrico Brasileiro (ONS) em Relação às Ações de Gerenciamento de Riscos Associados à Segurança Cibernética

Eduardo De Oliveira Lima[1], Fernando Rocha Moreira[1], Flávio Elias Gomes de Deus[1], Georges Daniel Amvame Nze[1], Rafael Timóteo de Sousa Júnior[1], Rafael Rabelo Nunes[1,2,3]

oliveira-eduardo.eo@aluno.unb.br; fernando.moreira@aluno.unb.br; flavioelias@unb.br; georges@unb.br; desousa@unb.br; rafaelrabelo@unb.br

[1] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP 70910-900 Brasília-DF Brasil

[2] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Administração, CEP 70910-900 Brasília-DF Brasil

[3] Centro Universitário Atenas, Rua Euridamas Avelino de Barros, nº 1400, Prado, CEP 38602-002 Paracatu-MG Brasil

Pages: 301-312

Resumo: Este trabalho tem por objetivo comparar os controles mínimos de segurança cibernética definidos pelo Operador Nacional do Sistema Elétrico Brasileiro (ONS) com aqueles recomendados pelo Center for Internet Security (CIS) para avaliar se a Rotina Operacional do ONS inclui controles suficientes para lidar com os riscos cibernéticos do setor elétrico. Foi utilizada uma escala de cinco níveis contidas no CIS CSC para realizar a comparação. Os resultados mostram que um dos dezoito grupos de controle que o ONS recomenda excede as exigências do Framework. Em contraponto, cinco outros grupos de controle não são mencionados pelas recomendações do ONS, e, para os outros grupos, os requisitos do ONS ficam aquém da estrutura do CIS CSC. Este trabalho contribui para o debate de risco cibernético relacionado à infraestrutura operacional do Sistema Elétrico Brasileiro (SEB), que, de acordo com os resultados, ainda necessita de melhorias em sua maturidade de gestão e operacional.

Palavras-chave: CIS CSC, Segurança Cibernética, Setor Elétrico, ONS, Gestão de Riscos

Assessment of the Brazilian National Electrical System Operator (ONS) Operational Routine regarding actions to manage the cybersecurity risks

Abstract: This paper aims to compare the minimum cybersecurity controls set by the Brazilian National Electric System Operator (ONS) with those recommended

by the 'includes sufficient controls to address cyber risks in the electricity sector. The Scale used in the CIS CSC contain five-level to perform the comparison. The results show that one of the eighteen control groups that ONS recommends exceeds the requirements of the Framework. In contrast, the ONS recommendation did not mention five other control groups, and for the other groups, the ONS requirements fall short of the CIS CSC Framework. This work contributes to the cyber risk debate related to the operational infrastructure of the Brazilian Electric System (SEB), which, according to the results, still needs improvements in its management and operational maturity.

Keywords: *CIS CSC, Cybersecurity, Electric Field Supplier Sector, ONS, Risk Management*

1. Introdução

As vulnerabilidades cibernéticas dos Sistemas de Controle Industrial (ICS) têm sido alvos de constante e crescente interesse de grupos *hackers*. Por exemplo, em 2010, o *malware Stuxnet* causou danos significativos ao Sistema de Supervisão e Aquisição de Dados (SCADA) das centrífugas no Irã (Baezner et al, 2017). Nos anos seguintes, vários casos também foram relatados: em 2014, a campanha de ataque *Havex* (Pixel, 2014) e a campanha *Sandworm* usando uma vulnerabilidade de dia zero para atingir o sistema SCADA da *General Electric* (GE) (Muncaster, 2014), e nos anos de 2015 a 2017, as ações destrutivas do *malware* Killdisk (Zetter, 2016) e Industroyer (Greenberg, 2017) causaram o desligamento da rede elétrica ucraniana. Eventos como estes levaram o Departamento de Segurança Nacional dos EUA (DHS) e o *Federal Bureau of Investigation* (FBI) a emitir um alerta em 2018 sobre ataques direcionados a energia e outros setores industriais críticos, quase todos eles direcionados aos sistemas de supervisão e aquisição de dados - SCADA (USCERT, 2018).

A este respeito, o ONS, considerando os riscos cibernéticos a que são submetidas as instalações do Sistema Elétrico de Potência - SEP, essencialmente aquelas sob influência do Sistema de Supervisão e Aquisição de Dados - SCADA, publicou em 09 de julho de 2021, uma Rotina Operacional (RO) que tem o objetivo de determinar aos agentes do Setor Elétrico Brasileiro - SEB a implantação de controles mínimos de segurança cibernética no Ambiente Regulamentado denominado ARCiber (ONS, 2021). Até o momento, não existem registros de outras rotinas operacionais do ONS, pertencentes ao Manual de Procedimentos Operacionais - MPO, que abordam a gestão da segurança cibernética no setor elétrico brasileiro.

O escopo do ARCiber é o ambiente operacional composto pelo conjunto de redes e equipamentos considerados no domínio da RO, a saber: os centros de operação dos agentes; os equipamentos participantes da infraestrutura de envio ou recebimento de dados e voz para os ambientes operacionais do ONS; os centros de operação de outros agentes; e, também, o ambiente operacional do ONS.

Neste contexto, surge uma pergunta: a implementação destes controles mínimos seria suficiente para enfrentar os riscos cibernéticos no setor elétrico? Como resposta, este trabalho se propôs avaliar a rotina publicada pelo ONS, e compará-la com a estrutura de segurança cibernética do CIS CSC V 8.0 (CIS, 2021).

A escolha do CIS CSC V 8.0 como parâmetro de comparação foi baseada no fato de ser ele um *Framework* otimizado, pois foi construído a partir de uma simplificação das estruturas NIST_SP_800_53 (NIST SP, 2020) e NIST_CSF (NIST CSF, 2018), que podem representar custos de implementação muito altos (DRTNS, 2016). Este *framework* selecionou os controles que oferecem a melhor relação risco/retorno em sua implementação. Com isto em mente, pretende-se avaliar se a proposta feita pela ONS é compatível com um padrão aceito como mínimo pela comunidade de segurança cibernética.

Este documento está organizado da seguinte forma: a Seção 2 abordará as referências teóricas, caracterizando o ambiente de estudo, tecnologias e padrões aplicáveis à segurança cibernética de infraestruturas críticas; a Seção 3 apresentará a metodologia adotada para o desenvolvimento do trabalho; a Seção 4 apresentará a análise dos resultados obtidos e uma breve discussão; e a Seção 5 mostrará as conclusões deste estudo.

2. Referencial Teórico

O SEP consiste em um complexo sistema de engenharia no qual o centro de controle concentra a responsabilidade pelo monitoramento, controle e tomada de decisões operacionais em tempo real (Sridhar & Hahn, 2012). Além disso, os sistemas cibernéticos que consistem em dispositivos eletrônicos de campo, como vistos em redes de comunicação, sistemas de automação de subestações e centros de controle, são incorporados em toda a rede física e envolvem os segmentos de geração, transmissão e distribuição de energia (Laprie et al, 2008). Assim, esta infraestrutura representa uma tecnologia muito diversificada com vários graus de conectividade. Além disso, como um desafio clássico, manter o equilíbrio dinâmico entre oferta e demanda de eletricidade é um aspecto fundamental que precisa ser mantido e garantido em tempo real (Arghandeh et al, 2016).

Nos últimos anos, o uso de dispositivos eletrônicos inteligentes (IEDs) tem sido disseminado para enfrentar estes desafios. Estes dispositivos permitem o gerenciamento do equilíbrio energético, uma vez que operam sistemas de proteção, supervisão, comando e controle do sistema elétrico (Huang et al, 2009). Entretanto, o intercâmbio de dados realizado por estes componentes tem como consequência o aumento das vulnerabilidades da superfície de exploração nos IEDs (Laprie et al, 2008) (Arghandeh et al, 2016). Os sistemas elétricos de comando e controle de potência são compostos por uma série de laços responsáveis pela identificação dos sinais de comunicação, protocolos, máquinas/dispositivos, processamento e ações de controle, associados a cada classificação funcional. Os impactos potenciais dos ataques cibernéticos estão concentrados principalmente nestes processos (Huang et al, 2009).

Os processos de avaliação dos riscos cibernéticos, associados à segurança das redes de energia elétrica, devem ser continuamente reavaliados, visando garantir uma operação com um nível adequado de segurança (Parks, 2007). Entretanto, a complexidade do SEP, a longa vida útil de seus componentes e a constante evolução das ameaças cibernéticas começaram a apresentar um novo vetor de ataque. A detecção e remoção dos problemas de segurança cibernética começaram a indicar a necessidade de abordagens específicas,

tanto para os sistemas e aplicações de energia (SPCS) como também para os sistemas e aplicações associados ao suporte da infraestrutura de Tecnologia da Informação (TI) (Permann & Rohde, 2005). Considerando o cenário de riscos cibernéticos apresentado para o SEP, entende-se que é de grande importância tratar a questão a partir de uma abordagem de gerenciamento de risco. Neste sentido, o apoio às normas e diretrizes de segurança, difundidas e aceitas pela comunidade internacional, torna-se um fator de grande importância. Portanto, o desafio é definir um bom instrumento para gerenciar redes de energia elétrica, considerando a melhor relação risco/retorno para o ambiente cibernético.

2.1. Padrões clássicos para o gerenciamento da segurança cibernética

O Guia de Segurança Cibernética das Redes Elétricas Inteligentes, NISTIR-7628 (US Department of Commerce, 2014), publicado pelo *National Institute of Standards and Technology* (NIST), propôs um conjunto de requisitos de segurança cibernética abrangente para garantir a adequação do mecanismo de proteção cibernética. Portanto, trata-se de um guia de grande importância para os sistemas que integram a infraestrutura de processos críticos, tais como os Sistemas Elétricos de Potência.

Devido a sua evolução, o NIST publicou as estruturas NIST_SP_800_53 e NIST_CSF, que apresentam uma vasta lista de controles que precisam ser gerenciados para garantir um nível adequado de segurança cibernética para as interfaces do SEP identificadas.

Além das estruturas publicadas pelo NIST, a Organização Internacional de Normalização (ISO) disponibilizou normas para a segurança da informação e gerenciamento de riscos, entre as quais a série ISO/IEC 27000 (ISO, 2022) e a série ISO/IEC 31000 (ISO, 2018), respectivamente, podem ser destacadas.

Entretanto, o NIST procurou harmonizar as normas internacionais e americanas, possibilitando um sistema de gerenciamento de segurança da informação e um processo de gerenciamento de risco baseado nas melhores práticas das normas ISO/IEC e COBIT 5 (ISACA, 2013). Portanto, o *Council on Cybersecurity* (CCS) *Top 20 Critical Security Controls* (CSC), ANSI/ISA-62443-2-1 (ISA, 2009), e ANSI/ISA-62443-3-3 (ISA, 2013) fornecem uma forma de facilitar a conformidade com base nas normas internacionais, bem como nas normas e diretrizes do NIST.

2.2. Controles do CIS CSC Versão 8

O padrão proposto pela NIST para a gestão da segurança cibernética é bastante abrangente, consistindo em cinco funções que incluem vinte e três categorias e cento e oito controles (subcategorias). O NIST reforça a tendência de custos elevados para sua implementação completa (DRTNS, 2016).

Este aspecto motivou o CIS a construir uma estrutura mais otimizada, consistindo em dezoito grupos de controles obtidos a partir do CSF da NIST. Estes controles destinam-se a atender às exigências das infraestruturas críticas com a melhor relação risco/retorno, com base no Princípio de Pareto, que define que 20% das causas são responsáveis por cerca de 80% dos efeitos, portanto, cerca de 20% dos controles do NIST podem representar 80% de melhoria no nível de segurança cibernética (McClain & Sagerand, 2018)

Além disso, os controles são estruturados em Grupos de Implementação (IGs), que consideram os recursos e o perfil de risco de cada organização. Assim, a implementação dos controles do CIS CSC começa com o grupo IG1, que é obrigatório para todas as organizações (incluindo aquelas com recursos limitados), seguido pelo grupo IG2, que considera organizações com recursos moderados, e finalmente, o grupo IG3, para organizações com exposição a alto risco. Portanto, o número de controles do IG3 é maior que o IG2, e o IG2 é maior que o IG1, como mostra a Tabela 1, a seguir.

Observe que os grupos 13, 16 e 18 não têm controles IG1, mas IG2 e IG3. Portanto, estes controles são implementados em organizações com maior disponibilidade de recursos.

Grupos de Controles CIS CSC	**IG1**	**IG2**	**IG3**
1- Inventário e Controle de Dispositivos de *Hardware*	2	4	5
2- Inventário e Controle de Ativos de *Software*	3	6	7
3- Proteção de Dados	6	12	14
4- Configuração Segura dos Softwares e Ativos Empresariais	7	11	12
5- Grenciamento de Contas	4	6	6
6- Gerenciamento do Controle de Acesso	5	7	8
7- Gerenciamento Contínuo de Vulnerabilidades	4	7	7
8- Gerenciamento dos Logs de Auditoria	3	11	12
9- Proteção de *e-mails* e Navegadores WEB	2	6	7
10- Proteção contra aplicações maliciosas	3	7	7
11- Recuperação de Dados	4	5	5
12- Gerenciamento da Infraestrutura de Rede	1	7	8
13- Defesa e monitoramento da Rede	0	6	11
14- Treinamento de Conscientização e Habilidades de Segurança	8	9	9
15- Gerenciamento de Provedor de Serviços	1	4	7
16- Segurança de Softwares e Aplicativos	0	11	14
17- Gerenciamento de Resposta a Incidentes	3	8	9
18- Teste de Penetração	0	3	5

Tabela 1 – Grupos de controle do CIS CSC e o número de subcontroles (salvaguardas) em cada grupo de implementação

2.3. Rotina Operacional do ONS

Em 09 de julho de 2021, o ONS, entidade responsável pela coordenação e controle das instalações de geração e operação de transmissão de eletricidade no Sistema Interligado Nacional - SIN, emitiu o RO-CB.BR.01 R00, pertencente ao Módulo 5 - Submódulo 5.13 do Manual de Procedimentos Operacionais - MPO, com o objetivo de orientar os Agentes do Setor Elétrico a adotarem controles mínimos de Segurança Cibernética para o Ambiente Regulamentado de Segurança Cibernética (ARCiber).

A Tabela 2 mostra os Grupos de Segurança definidos na Rotina Operacional (RO) e seus níveis de proteção. Os Agentes do Setor Elétrico Brasileiro devem direcionar seus esforços de controle e gestão, visando o cumprimento da RO em vinte e sete meses, após a publicação da norma, ou seja, em setembro de 2023.

Grupo de Segurança ARCiber	Macro Controles ARCiber
1- Arquitetura Tecnológica para o Ambiente do ARCiber	Redes Segregadas ARCiber isolado da Internet Existência de soluções *anti-malware* implantadas e atualizadas no ARCiber
2- Governança de Segurança da Informação	Existência de Processo Formal de Gestão da Segurança Cibernética no ARCiber
3- Inventários de Ativos	Realização de Inventário físico periódico de ativos de *hardware*, *software* e Dados conectados ao ARCiber Armazenamento Seguro do Inventário Físico
4- Gestão de Vulnerabilidades	Gestão da Implantação de Pacotes de Correção de Segurança Conexão de Novos Ativos ao ARCiber
5- Gestão de Acessos	Política de Gestão de Identidade e Acesso
6- Monitoramento e Resposta a Incidentes	Política de Monitoramento Plano de Resposta a Incidentes
7- Exceções	Tratamento de Exceções

Tabela 2 – Processo de Segurança Cibernética para o ARCiber (RO-CB.BR.01)

3. Metodologia

O presente trabalho representa uma pesquisa aplicada com objetivos exploratórios que teve como principal característica a captação de informações visando o entendimento de uma realidade, utilizando-se de investigações realizadas no contexto da pesquisa (Vergara, 2006). Trata-se de um trabalho qualitativo, uma vez que se valeu da análise de material documental como um dos principais métodos adotados (Prodanov & Freitas, 2013).

Para responder à pergunta proposta no objetivo deste trabalho, ou seja: "A Rotina Operacional do ONS é suficiente para lidar com os riscos cibernéticos do setor elétrico?", comparamos os controles da Rotina Operacional RO-CB.BR.0 com os controles estruturais do CIS CSC. Dessa forma, os resultados obtidos são considerados secundários, cuja pesquisa associada está correlacionada a diversas fontes de documentos como livros, normas, padrões, revistas, periódicos, revisões sistemáticas da literatura (Marconi, 2003).

A avaliação da relação entre os pares de controle CIS CSC e ARCiber considerou a intensidade da semelhança ou diferença entre os controles existentes em ambos, avaliando a relação da esquerda para a direita, ou seja, partindo da relação dos controles da estrutura CIS CSC para os itens de segurança propostos pelo ONS para o ARCiber.

Esta comparação utilizou os mesmos critérios de classificação que a estrutura do CIS CSC utiliza para se comparar com outras estruturas (CIS, 2021). A Tabela 3 mostrada a seguir apresenta estes critérios, destacando as avaliações qualitativas graduadas em cinco níveis: *Equivalent; Superset; Subset; Intersection; e None.*

Relação CIS x ARCiber	**Atenuação Defensiva**
Equivalent	O controle CIS contém o mesmo conceito de Segurança Cibernética do controle ARCiber.
Superset	O Controle CIS possui um conceito mais amplo de Segurança Cibernética e contém o controle ARCiber.
Subset	O Controle CIS possui um conceito mais restrito de Segurança Cibernética e está contido no controle ARCiber.
Intersections	Há muitas semelhanças entre os dois, porém nenhum dos dois está contido dentro do outro. Não pode ser usado para atender aos requisitos do outro.
None	Não há nenhum controle ARCiber que se relacione com o Controle do *framework* CIS.

Tabela 3 – Relação entre os controles CIS CSC e os controles ARCiber

Assim, considerando cada Grupo de Implementação IG, os dezoito macrocontroles CIS CSC, e seus respectivos subcontroles (salvaguardas) foram realizadas as comparações com os controles definidos no ambiente regulado ARCiber. Esta análise permitiu a construção de um mapeamento que mostra os 18 grupos de controle CIS CSC e como o ambiente regulado ARCiber se relaciona com cada Grupo de Implementação IG1, IG2 e IG3, de acordo com a classificação qualitativa exposta acima.

4. Resultados e Discussão

A Tabela 4 mostra os resultados da comparação realizada. Nos resultados, é possível observar que dos 18 grupos de controle do CIS CSC, apenas o grupo 9 do CIS CSC é um *subset* dos controles ARCiber, ou seja, o *framework* ARCiber é mais restritivo nesse grupo de controles. Isso é explicado por dois motivos: alguns dos controles não se aplicam ao cenário do ARCiber, e em outros, há superação das exigências do CIS CSC visto que o ARCiber determina a segregação absoluta da arquitetura da rede de operação e a corporativa, vedando acesso à internet pelos dispositivos IEDs.

CIS CSC x ARCiber				**Grupos de Controle ARCiber**
Grupo CIS CSC	**IG1**	**IG2**	**IG3**	
1	*Equivalent*	*Superset / None*	*None*	*Groups 3 e 6*
2	*Equivalent*	*Superset / None*	*None*	*Groups 3 e 6*
3	*None*	*None*	*None*	-
4	*Equivalent / None*	*None*	*None*	*Groups 1, 3, 4, 5 e 6*

CIS CSC x ARCiber				**Grupos de Controle ARCiber**
Grupo CIS CSC	**IG1**	**IG2**	**IG3**	
5	*Equivalent / Superset*	*None*	*None*	*Groups 3 e 5*
6	*Equivalent / Superset*	*None*	*None*	*Groups 3 e 5*
7	*Equivalent / Superset*	*None*	*None*	*Groups 3, 4 e 6*
8	*Equivalent*	*Equivalent / None*	*None*	*Groups 6*
9	*Subset*	*Subset*	*Equivalent*	*Groups 1*
10	*Equivalent*	*Equivalent / Superset*	*Equivalent / Superset*	*Groups 1*
11	*None*	*None*	*None*	-
12	*Equivalent*	*Equivalent / None*	*None*	*Groups 1, 3, 4 e 5*
13	-	*Equivalent*	*Equivalent*	-
14	*None*	*None*	*None*	-
15	*None*	*None*	*None*	-
16	-	*None*	*None*	-
17	*Equivalent*	*Equivalent*	*None*	*Groups 2 e 6*
18	-	*None*	*None*	-

Tabela 4 – Comparação entre os Controles do *Framework* CIS CSC x Controles ARCiber da Rotina Operacional RO-CB.BR.01, Rev. 00

No outro extremo, tem-se que 6 dos 18 grupos de controles do CIS não tem nenhuma menção no ARCiber em nenhum dos níveis de implementação IG1, IG2 e IG3. Nesses grupos há identificação de "None" nos resultados da Tabela 4. São eles: 3 (Proteção de dados), 11 (Recuperação de Dados), 14 (Treinamento de Conscientização e Habilidades de Segurança), 15 (Gerenciamento de Provedor de Serviços), 16 (Segurança de Softwares e Aplicativos) e 18 (Testes de penetração). Isso significa que a aplicação desses controles por agentes do setor elétrico pode ser considerada opcional. Apesar de a não aplicação de controles do Grupo 3 ser justificável, já que os agentes não tratarão dados pessoais em sua maioria, a não previsão de controles dos grupos 11, 14, 15, 16 e 18 demonstra um baixo nível de maturidade na segurança cibernética do setor elétrico brasileiro. Nesse quesito, é importante registrar dois pontos: a falta desses controles pode dificultar no sucesso na implantação de programas de segurança cibernética (Muflihah & Subriadi, 2018) (Al-Daeef et al, 2017)(Feng et al, 2019) (Thomas et al, 2018) (Khera et al, 2019) e ainda, potencializar o impacto de riscos que porventura comprometam os discos rígidos dos equipamentos, pois não se menciona em nenhum momento da RO, a obrigatoriedade de rotinas de backup e recuperação de dados (Grupo 11).

Quando se considera o grupo de implementação IG2, os grupos de controle 1, 2, 8, 10, 12, 13 e 17 possuem equivalência relativa, sendo que em alguns casos, os controles do CIS são mais abrangentes do que o do ARCiber. Além disso, registra-se que os grupos de controle 3, 4, 5, 6, 7, 11, 14, 15, 16 e 18 não tem correspondência com o ARCiber.

Considerando o grupo de implementação IG3, o ARCiber não possui equivalência com a maioria dos controles, tendo alguma relação apenas nos controles dos grupos 9, 10 e 13, o que expõe muitas lacunas quando se consideram os controles que deveriam ser aplicados em ambientes com alto risco e criticidade, que é o caso do SEB.

Esses resultados demostram que o nível de controle que será exigido para o ARCiber se aproxima mais ao do grupo de implantação IG1, que conforme descrito, se aplicaria às organizações com restrições de recursos, o que não deveria ser o caso.

5. Conclusões e Trabalhos Futuros

Esse trabalho teve como principal objetivo responder à pergunta: a RO-CB.BR.01 Rev. 00 do Operador Nacional do Sistema Elétrico é suficiente para enfrentar riscos cibernéticos no setor?

Para isso, o trabalho comparou a RO com o *framework* CIS CSC que é amplamente utilizado na área de segurança cibernética e já é uma simplificação de outros *frameworks*.

A comparação foi realizada utilizando avaliações qualitativas graduadas nos 18 grupos de controle, sendo que apenas um grupo de controle do ARCiber superou as exigências do *framework* CIS, se posicionando aquém nos demais. Dessa forma, chega-se a conclusão que a RO elenca um conjunto de controles significativamente menor do que os mínimos necessários para que os principais aspectos da segurança cibernética possam ser monitorados, gerenciados e tratados pelos Agentes do Setor Elétrico.

Considerando a criticidade do setor elétrico para o país e o volume de recursos destinado a ele, entende-se que o nível de maturidade exigido para os controles do ARCiber, quando se verifica apenas a RO-CB.BR.01 Rev. 00, ainda é muito baixo, o que demonstra que a situação não estará confortável mesmo se todos os controles previstos para os agentes do setor elétrico sejam implantados até o final de setembro de 2023.

Destaca-se a falta de menção no ARCiber a controles de Recuperação de Dados; de Treinamento de Conscientização e Habilidades de Segurança; de Gerenciamento de Provedor de Serviços; de Segurança de Softwares e Aplicativos; e de Testes de penetração, que podem ter impactos significativos no resultado da implantação do programa de segurança cibernética dentro do setor.

Uma limitação do trabalho foi o grau de subjetividade que foi exigido para escolher um dos cinco níveis ao se fazer a comparação. Apesar disso, entende-se que essa limitação não compromete o resultado geral do trabalho, deixando aberta a discussão sobre segurança cibernética no setor elétrico brasileiro.

Sugere-se como trabalhos futuros, que se acompanhe a implantação desses controles, e que se compare as ações realizadas no ARCiber, com outros *frameworks* que se julgarem pertinentes para se realizar avaliação de possíveis gaps que porventura possam existir.

Agradecimentos

O autor Eduardo de Oliveira Lima agradece o suporte da Universidade de Brasília, por meio do DPG, Edital 01/2022; da ENBPar – Empresa Brasileira de Participações em Energia Nuclear e Binacional S/A. O autor Rafael Rabelo Nunes agradece o suporte do Centro Universitário Atenas e da Universidade de Brasília, por meio do Edital DPI/DPG 02/2022. Os autores Flávio Elias Gomes de Deus, Fernando Rocha Moreira e Rafael Rabelo Nunes agradecem o suporte do Ministério da Justiça e Segurança Pública representado pela Diretoria de Tecnologia da Informação e Comunicação (TED DTIC/SE/MJSP 01/2019). O autor Fernando Rocha Moreira agradece o suporte da FAP/DF, por meio do Edital 07/2022. O autor Rafael Timóteo de Sousa Júnior agradece o apoio do CNPq outorgas 465741/2014-2 e 312180/2019-5, da Advocacia Geral da União outorga 697.935/2019, do Departamento Nacional de Auditoria do SUS outorga 23106.118410/2020-85, da Procuradoria Geral da Fazenda Nacional outorga 23106.148934/2019-67, e do Conselho Administrativo de Defesa Econômica outorga 08700.000047/2019-14. O autor Georges Daniel agradece o suporte do laboratório LATITUDE / UnB por meio da outorga 23106.099441/2016-43 SDN.

Referências

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). "Security Awareness Training: A Review," in World Congress on Engineering.

Arghandeh, R., Meier, A. V., Mehrmanesh, L. & Mili, L. (2016). "On the definition of cyber-physical resilience in power systems," vol. 58, pp. 1060-1069. https://doi.org/10.1016/j.rser.2015.12.193.

Baezner M., & Robin, P. (2017). "Stuxnet," *Cyber Defense Project (CDP) and Center for Security Studies (CSS)*.

CIS, Center for Internet Security. (2021). "CIS Controls v8 Mapping to NIST_CSF_06_11_21".

CIS, Center for Internet Security. (2021). "Simplified & Prioritized Cyber Defense Guidance – CIS Critical Security Controls - CSC, Version 8.0".

DRTNS, Dimentional Research and Tenable Network Security, (2016). "Trends in Security Framework Adoption – A Survey of it and security professionals".

Feng, N., Wang, M., Li, M., & Li, D. (2019). "Effect of Security Investment Strategy on the Business Value of Managed Security Service Providers," *Journal Electronic Commerce Research and Applications,* vol. 35. https://doi.org/10.1016/j.elerap.2019.100843.

Greenberg, A. (2017). "Crash Override: The Malware That Took Down a Power Grid".

Huang, Y. L. & Cardenas, A. A. & Amin, S. & Z. S. Lin & H.-Y. Tsai & Sastry, S. (2009). "Understanding the physical and economic consequences of attacks on control systems," *International Journal of Critical Infrastructure Protect,* p. 73–83. https://doi.org/10.1016/j.ijcip.2009.06.001.

ISA, International Society of Automation, (2009). "ANSI/ISA–62443-2- 1 (99.02.01)-Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program".

ISA, International Society of Automation, (2013). "ANSI/ISA-62443-3-3 (99.03.03) - Security for industrial automation and control systems Part 3-3: System security requirements and security levels".

ISACA, Information Systems Audit and Control Association, (2013). "Transforming Cybersecurity: Using COBIT 5".

ISO, International Organization for Standardization, (2022). "ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements".

ISO, International Organization for Standardization, (2018). "ISO/IEC 31000 - Risk Management".

Khera, Y., Kumar, D., Sujay & Garg, N. (2019). "Analysis and Impact of Vulnerability Assessment and Penetration Testing," in *International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con).* https://doi.org/10.1109/COMITCon.2019.8862224.

Laprie, J. C., Kanoun, K. & Kaaniche, M. (2008). "Modelling interdependencies between the electricity and information infrastructures," *Computer Safety, Reliability, and Security,* pp. 54-67. https://doi.org/10.1007/978-3-540-75101-4_5.

Marconi, M. L. (2003). "E. F. da M. Científica", 5ª edição, Editora Atas S.A. São Paulo

McClain, S. & Sagerand, T. (2018). "Auditing, Assessing, Analyzing: A Prioritized Approach using the Pareto Principle".

Muflihah, Y. & Subriadi, A. P., (2018). "A Basic Element of IT Business Continuity Plan: Systematic Review," *Jurnal Informatika,* vol. 12, no. 1, pp. 17-23. https://doi.org;10.26555/JIFO.V12I1.A8370.

Muncaster, P. (2014). "Microsoft Zero Day Traced to Russian 'Sandworm' Hackers," *Infosecurity Magazine.*

NIST Special Publication (SP) 800-53, Revision 5, (2020). "Security and Privacy Controls for Federal Information Systems and Organizations".

NIST_CSF, Cybersecurity Framework, Version 1.1, (2018). "Framework for Improving Critical Infrastructure Cybersecurity".

ONS, Operador Nacional do Sistema Elétrico, (2021). "Manual de Procedimentos da Operação Módulo 5 - Submódulo 5.13, Número RO-CB.BR.01, Revisão 00, Item 4.1.11".

Parks, R. C. (2007). “BSAND2007-7328: Guide to critical infrastructure protection cyber vulnerability assessment,” *Sandia National Laboratories*.

Permann, M. R. & Rohde, K. (2005). “Cyber Assessment Methods for SCADA Security,” in *15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference*.

Pixel, A. (2014). “HAVEX Targets Industrrial Control Systems,” *Trend Micro Threat Encyclopedia*.

Prodanov C. C., & Freitas, E. C. D. (2013). “Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico”, 2ª Edição. [S.l.]: Editora Feevale

Sridhar, S., Hahn, A. & Govindarasu, M. (2012). “Cyber–physical system security for the electric power grid,” *Proceedings of the IEEE,* vol. 100, pp. 210-224. https://doi.org/10.1109/JPROC.2011.2165269.

Thomas, T. W. & Tabassum, M. & Chu, B. & Lipford, H. (2018). “Security During Application Development: an Application Security Expert Perspective,” University of North Carolina at Charlotte - Department of Software and Information Systems.

United States Computer Emergency Readiness Team, (2018). “Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors”.

US Department of Commerce, National Institute of Standards and Technology, (2014). “NISTIR 7628 Revision 1 - Guidelines for Smart Grid Cybersecurity”.

Vergara, S. C. (2006). “Projetos e relatórios de pesquisa”. São Paulo: Atlas.

Zetter, K. (2016). “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 12/10/2021
Aceitação/Acceptance: 07/01/2022

Gestão de Riscos Cibernéticos no Ambiente Operacional do Sistema Elétrico Brasileiro (ARCiber ONS): uma avaliação do processo de recuperação de dados pelo sistema SCADA

Eduardo de Oliveira Lima[1], Fernando Rocha Moreira[1], Carlos André de Melo Alves[2], Rafael Rabelo Nunes[1,2,3]

oliveira-eduardo.eo@aluno.unb.br; fernando.moreira@aluno.unb.br; carlosandre@unb.br; rafaelrabelo@unb.br

[1] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP 70910-900 Brasília-DF Brasil

[2] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Administração, CEP 70910-900 Brasília-DF Brasil

[3] Centro Universitário Atenas, Rua Euridamas Avelino de Barros, nº 1400, Prado, CEP 38602-002 Paracatu-MG Brasil

Pages: 313-325

Resumo: Com o aumento dos ataques cibernéticos ao setor elétrico, cada vez torna-se mais relevante proteger esse setor de riscos cibernéticos, além de se tornar resiliente para recuperar o ambiente em caso de ataques catastróficos. Esse artigo tem como objetivo avaliar a abrangência dos procedimentos de backup e recuperação de dados do sistema SCADA, visando identificar sua conformidade com os controles do Framework CIS que versam sobre o assunto. Para isso, foi analisado um manual operacional do sistema utilizando técnicas de análise de conteúdo. Verificou-se que há conformidade dos aspectos tecnológicos com o framework CIS, apesar de não ser possível garantir que empresas do setor elétrico brasileiro executem as rotinas de recuperação de forma sistemática. A relevância desse trabalho está na possibilidade da construção de um debate acerca do tema, diante das recentes ações do ONS para enfrentar riscos cibernéticos.

Palavras-chave: Setor Elétrico; SCADA, Backup e Recuperação de Dados; CIS; ONS; Segurança Cibernética; Riscos Cibernéticos.

Cyber Risk Management in the Brazilian Electric System Operational Environment (ARCiber ONS): Data Recovery Process Assessment by the SCADA System

Abstract: With the increase in cyber-attacks on the electric sector, it is becoming increasingly important to protect this sector from cyber-risks, in addition to becoming resilient to recover the environment in case of catastrophic attacks. This article aims to evaluate the backup and data recovery comprehensiveness of SCADA

system procedures, in order to identify its compliance with the CIS Framework controls that address the subject. To this end, this work analyzed a system operational manual using content analysis techniques. The research verified that there is conformity of the technological aspects with the CIS framework, although it is not possible to guarantee that companies from the Brazilian electric power sector execute the recovery routines in a systematic way. The relevance of this work lies in the possibility of building a debate about the topic, given the ONS' recent actions to address cyber risks.

Keywords: Electric Sector; SCADA; Data Backup Recovery; CIS; ONS; Cybersecurity; Cyber Risks.

1. Introdução

Os ataques cibernéticos em Sistemas de Infraestruturas Críticas (Industrial Control Systems – ICS) têm sido de interesse constante e crescente de grupos de Hackers. Mais especificamente, ataques cibernéticos provocaram um aumento significativo de ocorrências de violações na segurança dos Sistemas de Supervisão e Aquisição de Dados (SCADA), aumentando em 11% entre os anos de 2017 e 2018 e um acréscimo de 67% se for levado em consideração o período considerado entre os anos de 2013 e 2018 (Accenture Security, 2019). A campanha Sandworm atingiu o sistema SCADA da GE causando diversos tipos de danos, onde utilizou-se de uma vulnerabilidade de zero-day (Muncaster, 2014). Eventos como esses levaram o Department of Homeland Security - DHS dos EUA e o Federal Bureau of Investigation - FBI a emitirem um alerta, em 2018, de ataques direcionados à energia e outros setores industriais críticos, quase todos direcionados aos Sistemas SCADA (USCERT, 2018).

De forma similar, no Brasil, o Operador Nacional do Sistema - ONS publicou em 09 de julho de 2021 uma Rotina Operacional - RO, a qual tem por finalidade determinar aos agentes do Setor Elétrico Brasileiro – SEB a implantação de controles mínimos de segurança cibernética no Ambiente Regulado Cibernético - ARCiber (ONS, 2021).

O ARCiber tem como abrangência o ambiente operacional constituido pelo conjunto de redes e equipamentos que estão considerados no escopo da RO, quais sejam: os centros de operação dos agentes; os equipamentos que participam da infraestrutura de envio ou recebimento de dados e voz para ambientes operacionais do ONS; ou para centros de operação de outros agentes; e, ainda, o próprio ambiente operativo do ONS.

Essa RO apresenta sete dimensões de controles de segurança cibernética: Arquitetura Tecnológica para o Ambiente do ARCiber; Governança de Segurança da Informação; Inventários de Ativos; Gestão de Vulnerabilidades; Gestão de Acessos; Monitoramento e Resposta a Incidentes; e Exceções.

Além de se protegerem preventivamente de ataques cibernéticos, um elemento fundamental com o qual as empresas do setor elétrico devem fomentar para o aumento de suas resiliências é a execução sistemática de um processo de *backup* e recuperação de dados. No entanto, verifica-se que muitas empresas desse segmento ainda não padronizaram suas métricas associadas ao processo de gestão de riscos cibernéticos, deixando de conhecer e gerenciar adequadamente os seus parâmetros operacionais, tornando ainda mais vital a presença de uma gestão de riscos que contemple o processo

de recuperação de dados de forma clara e controlada (Plèta, 2021). Outro fato que corrobora com isso é que a lista de controles da RO não faz menção sobre procedimentos específicos sobre a gestão de recuperação de dados do ambiente ARCiber (ONS, 2021).

Nesse sentido, coloca-se a seguinte questão: os manuais de operação dos sistemas SCADA já abrangem rotinas suficientes de forma que a previsão de controles para essa dimensão fosse prescindível de auditoria pelo ONS? Dessa forma, esse trabalho tem como objetivo avaliar a abrangência dos procedimentos de backup e recuperação de dados do sistema SCADA, visando identificar sua conformidade com os controles do Framework CIS que versam sobre o assunto. Dessa forma, será possível verificar a disponibilidade de controles previamente existentes para uso do processo de gestão de riscos cibernéticos o que poderia justificar a dispensa da inserção obrigatória no ambiente regulado ARCiber, definido pela Rotina Operacional.

Esse trabalho está organizado da seguinte forma: além desta introdução, na seção 2 serão abordadas referências teóricas, caracterizando o ambiente de estudo, tecnologias e normas aplicáveis à segurança cibernética de infraestruturas críticas; na Seção 3 será apresentada a metodologia adotada para o desenvolvimento do trabalho; na Seção 4 será apresentada a análise dos resultados obtidos e uma discussão sobre o tema abordado; e, na Seção 5, serão mostradas as conclusões do presente estudo.

2. Referencial Teórico

Nessa seção, serão descritos os principais tópicos para compreensão desse artigo. Na seção 2.1, são tratados os aspectos do processo de Gestão de Riscos cibernéticos em Sistemas Eletricos de Potências. Na seção 2.2, abordamos o *framework* CIS CSC V8. Na seção 2.3, detalhamos a Rotina Operacional publicada pelo Operador Nacional do Sistema elétrico brasileiro, e por fim, na seção 2.4, abordamos os sistemas SCADA e seus processos de *backup* e recuperação de dados.

2.1. O processo de Gestão de Riscos Cibernéticos em Sistemas Elétricos de Potência

O processo de gestão de riscos cibernéticos passa, inicialmente, pela análise de vulnerabilidades a que está submetida a infraestrutura de um sistema elétrico em geral. As vulnerabilidades associadas aos sistemas de supervisão e aquisição de dados (SCADA) são umas das mais importantes a serem avaliadas em um processo de gestão de riscos cibernéticos (Stouffer et al, 2015). Nesses ambientes, as principais vulnerabilidades podem ser identificadas nos produtos de terceiros e softwares embarcados, assim como aquelas encontradas em configurações e fragilidades associadas à rede de comunicação (DHS CSSP, 2011).

Após a identificação de vulnerabilidades e riscos cibernéticos, a etapa de análise de impacto deve ser realizada para determinar as possíveis consequências nos aplicativos suportados pela infraestrutura elétrica (Sridhar et al, 2012). As atividades subsequentes têm por objetivo mitigar e minimizar os níveis de risco inaceitáveis (Laprie et al, 2007).

O processo de gestão de riscos cibernéticos exige, então, a definição de procedimentos e controles que irão permitir não apenas o monitoramento da execução das ações de

segurança e de mitigação de riscos, como também o acompanhamento sistemático da rotina e dos respectivos controles associados.

No entanto, é importante destacar que a manutenção da disponibilidade, da confidencialidade e da integridade das informações associadas aos controles só é possível caso eles sejam suportados sob três dimensões: tecnologia, processos, e pessoas (Nakamura, 2007), considerando o contexto de um processo de gestão de riscos cibernéticos.

2.2. CIS CSC Critical Security Controls Version 8

Os Controles apresentados no framework CIS Critical Security Controls constituem um conjunto prioritário de ações (salvaguardas) recomendadas para a defesa cibernética, que oferecem formas específicas e acionáveis de se impedir e mitigar os ataques cibernéticos mais usuais contra sistemas e redes. Esse framework é gerenciado pelo Center for Internet Security – CIS, e seus controles foram aprimorados para acompanhar os sistemas e softwares modernos (nuvem, virtualização, mobilidade, terceirização, trabalho remoto, evolução das táticas de ataque, etc.) (CIS, 2021).

O CIS CSC (CIS, 2021) foi escolhido para este trabalho por ser um *framework* otimizado, constituído de dezoito Macrocontroles obtidos a partir do Framework NIST_CSF - Cyber Security Framework (NIST, 2018).

Este framework estrutura os controles por meio de uma classificação de Implementation Groups - IGs, que levam em consideração os recursos e perfis de risco de cada organização. Dessa forma, a implantação dos controles CIS CSC começam pelos controles IG1, que são obrigatórios a todas as organizações (inclusive as com recursos limitados); seguindo com a implantação dos controles IG2, onde se considera organizações com recursos moderados, e por fim, os controles IG3, para organizações com alta exposição a riscos (Ibrahim, 2021).

O Macrocontrole 11 trata especificamente dos aspectos sobre Recuperação de Dados do Framework CIS CSC e tem por objetivo disponibilizar condições para se estabelecer e manter práticas de recuperação de dados que sejam suficientes para garantir a recuperação dos ativos empresariais para uma situação igual àquela identificada antes do incidente, de forma confiável e segura.

Esse Macrocontrole 11 é composto de cinco subcontroles, cuja abrangência atende às funções de segurança associadas à recuperação e proteção dos dados. São eles:

- Subcontrole 11.1 – Tem como objetivo estabelecer e manter um processo de recuperação de dados. No processo, deve ser abordado o escopo das atividades de recuperação de dados, a priorização da recuperação e a segurança dos dados de backup. Revisar e atualizar a documentação anualmente, ou quando ocorrerem mudanças significativas na empresa que possam impactar este Subcontrole (Salvaguarda);
- Subcontrole 11.2 – Realizar backups automatizados de ativos empresariais no escopo. Executar backups semanalmente, ou com maior freqüência, com base na importância dos dados;
- Subcontrole 11.3 – Proteger os dados de recuperação com controles equivalentes aos dados originais. Dependendo dos requisitos, pode ser utilizada criptografia ou separação de dados;

- Subcontrole 11.4 – Estabelecer e manter uma instância isolada de dados de recuperação. Exemplos de implementações incluem versão controlando destinos de backup através de sistemas ou serviços off-line, em nuvem ou fora do local;
- Subcontrole 11.5 – Testar a recuperação do backup trimestralmente, ou mais freqüentemente, para uma amostragem dos ativos da empresa no escopo.

Esses subcontroles atingem as três categorias de IGs, independentemente dos recursos e do perfil de risco de cada organização, exceto o Subcontrole 11.5, para o qual o CIS dispensa a sua adoção para o Grupo de Implantação IG1 (CIS, 2021).

No entanto, para as empresas de geração, transmissão e distribuição de energia elétrica, todos os subcontroles (salvaguardas), são importantes: "Para essas empresas, os processos são dotados de uma elevada criticidade, em especial aqueles monitorados pelo Sistema SCADA. As avaliações de segurança devem ser incluídas como parte da governança de um sistema crítico e seu gerenciamento de segurança" (Alcaraz & Zeadally, 2015).

2.3. Rotina Operacional do ONS

Em 09 de julho de 2021 o ONS, órgão responsável pela coordenação e controle da operação das instalações de geração e transmissão de energia elétrica no Sistema Interligado Nacional – SIN, emitiu a RO-CB.BR.01 R0, pertencente ao MPO Módulo 5 – Submódulo 5.13, que teve como objetivo definir e orientar os Agentes do Setor Elétrico quanto aos controles mínimos de segurança cibernética a serem adotados para o Ambiente Regulado Cibernético, o qual passou a ser chamado de ARCiber (ONS, 2021).

A Tabela 1 consolida os Grupos de Segurança definidos na RO, assim como os seus respectivos níveis de proteção, para os quais os agentes do Setor Elétrico Brasileiro deverão direcionar seus esforços de gestão e controle, visando à constituição de um ambiente minimamente seguro para as instalações operacionais (ONS, 2021).

Por meio da Tabela 1 é possível perceber a ausência, dentre outros, de macrocontroles ARCiber associados ao Macrocontrole 11 do Framework CIS CSC – Recuperação de Dados, o qual deve ser considerado, segundo o CIS CSC, por todas as empresas que tenham por objetivo implantar um processo de gestão de riscos cibernéticos, independentemente do tamanho e capacidade financeira.

Grupo ARCiber	Subcontroles ARCiber
1 – Arquitetura tecnológica para o ambiente do ARCiber	Redes segregadas
	ARCiber isolado da internet
	Existência de soluções anti-malware implantadas e atualizadas no ARCiber
2 – Governança de segurança da informação	Existência de processo formal de gestão da segurança cibernética no ARCiber
3 – Inventários de ativos	Realização de inventário físico periódico de ativos de hardware, software e dados conectados ao ARCiber
	Armazenamento seguro do inventário físico

Grupo ARCiber	Subcontroles ARCiber
4 – Gestão de vulnerabilidades	Gestão da implantação de pacotes de correção da segurança
	Conexão de novos ativos ao ARCiber
5 – Gestão de acessos	Política de gestão de identidade e acesso
6 – Monitoramento e resposta a incidentes	Política de monitoramento
	Plano de resposta a incidentes
7 – Exceções	Tratamento de exceções

Fonte: os autores a partir do conteúdo da RO-CB.BR.01 R0

Tabela 1 – Processo de Segurança Cibernética para o ARCiber (RO-CB.BR.01)

2.4. Sistemas SCADA e os seus processos de recuperação de dados

O Sistema SCADA tem uma função crucial para os processos industriais: é ele que assume a responsabilidade pelo acompanhamento e supervisão dos processos produtivos, cujo principal objetivo é garantir a sua correta execução, de conformidade com os padrões de projeto. Ele ainda oferece os subsídios para a atuação de sistemas auxiliares de proteção, comando e controle por exemplo.

Ele é projetado para que seja possível a implementação de configurações específicas para cada tipo de processo, armazenar dados e disponibilizar recursos para intervir manualmente ou automaticamente no processo, quando necessário. Além de atuar preponderantemente em processos industriais, o SCADA também tem sido muito utilizado em processos experimentais (Daneels,1999).

Além de coletar os dados, o SCADA, também chamado de sistema supervisório, permite ainda a visualização e supervisão dessas informações. Essa visualização normalmente são apresentadas de forma amigável em telas sinópticas, se valendo de gráficos de tendências, evolução histórica e sinalização de alarmes e falhas

A infraestrutura associada aos Sistemas SCADA é constituída de servidores, drivers de comunicação, sensores e atuadores conectados ao processo. Com isso é possível a sua atuação em tempo real (Daneels,1999).

Uma variedade de sistemas SCADA está em operação nas subestações transformadoras de energia elétrica, providos por vários fabricantes diferentes.

O Sistema SCADA da Siemens, WinCC V7.5 SP2 possui um grande número de funcionalidades associadas aos procedimentos de arquivamento de dados do processo, assim como de arquivos de usuários (SCADA, 2020).

Para a execução desse trabalho, foi utilizada uma versão moderna do sistema SCADA, com escopo de funcionalidades abrangentes, em especial aquelas associadas aos processos de Backup/Recovery. Buscou-se utilizar um sistema SCADA que apresentasse um bom nível de automação e com alta tecnologia embarcada (SCADA, 2020).

O SCADA da Siemens apresenta os principais grupos de funcionalidades associadas ao Backup/Recovery, quais sejam:

- Archiving Fast e Slow;
- Backup de Arquivos de Processo;
- Configurações Gerais de Origem e Destino de Arquivos de Processo e de Usuários;
- Configurações de Infraestrutura de Rede e Servidores de Backup/Recovery;
- Links de Conexão com Servidores de Backup/Recovery;
- LOG de Monitoramento;
- Criptografia.

A partir desses grupos de funcionalidades é de se esperar que os subsídios necessários para a construção, alimentação e monitoramento dos subcontroles definidos no Macrocontrole 11 do CIS CSC estejam disponíveis, independentemente dos Grupos de Implantação (IG1, IG2 e IG3) a que pertencem.

O processo de análise de conteúdo realizado permitiu a identificação das principais funcionalidades do Sistema SCADA da Siemens, associadas à recuperação de dados, conforme descrito a seguir:

- Archieving fast e slow de dados de processo;
- Backup de arquivos de processo;
- Sistemas redundantes
- Ativação do backup
- Definição de caminhos de rede para dados de processo;
- Idem para dados de usuários;
- Servidor de Backup;
- Desconexão de arquivos;
- Gravação e Recuperação de Dados;
- Backup específico;
- Arquivos de usuários;
- Redundância em arquivos de usuários;
- Backup manual dos arquivos de usuário.

3. Metodologia

O presente trabalho representa uma pesquisa aplicada com objetivos exploratórios que teve como principal característica a captação de informações visando o entendimento de uma realidade, utilizando-se de investigações realizadas no contexto da pesquisa (Vergara, 2006). Trata-se de um trabalho qualitativo, uma vez que se valeu da análise de material documental como um dos principais métodos adotados (Prodanov, 2013).

Para se atingir o objetivo desejado, foram analisados os Capítulos 7 e 8 do Manual do Sistema SCADA Siemens WinCC V7.5 SP2. Dessa forma, os resultados obtidos são considerados secundários. Resultados nessa natureza são obtidos quando a pesquisa associada está correlacionada a fontes diversas, isoladas ou associadas, tais como documentos, livros, normas, padrões, revistas, periódicos e revisões sistemáticas da literatura (Marconi, 2003).

Os dados secundários obtidos foram analisados utilizando as técnicas de análise de conteúdo (Bardin, 2011), cujos passos estão descritos a seguir:

- Pré-análise: onde são feitos a leitura flutuante; escolha dos documentos; reformulações de objetivos e hipóteses e a formulação de indicadores (Bardin, 2011);
- Construção das Categorias: na qual a descrição analítica contribui fortemente para o estudo detalhado e consistente. Esse processo deve basear-se nas hipóteses e nos referenciais teóricos adotados (Mozzato & Grzyboviski, 2011). Na definição dessas categorias é realizada a classificação, quando se realiza o desmembramento e posterior agrupamento ou reagrupamento das unidades de registro do texto. Assim, a repetição de palavras e/ou termos foi a estratégia adotada no processo de codificação para serem criadas as unidades de registro e, posteriormente, as categorias de análise usadas inicialmente (Bardin, 2011);
- Tratamento dos resultados, inferências e interpretações: nesse momento devem ser realizadas as reflexões e críticas, as quais devem ser capazes de viabilizar os conteúdos de interesse existentes no material identificado, utilizando-se as ferramentas disponibilizadas durante o processo de análise de conteúdo. Trata-se de uma fase lógica, cujos resultados são obtidos a partir da conexões existentes entre proposições inferidas e outras já tidas como verdadeiras (Fossá, 2003).

Desse modo, foram realizadas as análises dos resultados obtidos a partir da comparação entre os Macrocontrole No. 11 do Framework CIS CSC e o ambiente regulado ARCiber definido pela RO do ONS.

4. Resultados

A Tabela 2 apresenta o número de ocorrências de palavras/termos de interesse nos Capítulos 7 e 8 do manual SCADA, obtidas por meio do software *Word Counter (*Countwordsfree*,* 2022*)*. Essa estratégia foi a adotada no processo de codificação para criar as unidades de registro (Bardin, 2011). Com isso, foram obtidas as unidades de registro mais representativas para a análise de conteúdo. Pelo resultado, verifica-se que o Sistema SCADA apresenta, em ordem decrescente, os termos 'Configuração', 'Arquivamento', 'Backup', 'Exportar dados', 'Importar', 'Gravar', 'Redundância', 'Restaurar', 'Recuperar'. Isso permite inferir que o foco principal do processo de Recuperação de Dados para o Sistema SCADA baseia-se em primeiro lugar na Configuração do Sistema, já que como pode ser observado, o número de ocorrências desse termo é quase o dobro do segundo. Em seguida, aparecem aspectos associados ao 'Backup', 'Exportação' e 'Importação' de Dados.

Por meio das unidades de registro apresentadas na Tabela 3, foi possível a definição das categorias iniciais. A Tabela 3 a seguir mostra a distribuição dessas categorias, baseando-se na significância das palavras e termos oriundos da leitura dos documentos.

Unidades de Registro	Número de ocorrências das Palavras
Configuração	641
Arquivamento	315
Backup	57
Exportar dados	34
Importar	22

Unidades de Registro	Número de ocorrências das Palavras
Gravar	13
Redundância	13
Restaurar	10
Recuperar	1

Fonte: os autores a partir de dados da pesquisa

Tabela 2 – Unidades de registro da documentação

Número	Categorias iniciais
1	Exportar registro de dados para backup de segurança
2	Arquivamento de valores de processo
3	Arquivamento de registros de usuários e configurações
4	Backup de valores de processo
5	Backup de registros de usuário
6	Recuperar e importar dados de processo para base de produção
7	Recuperar dados de configuração do SCADA
8	Recuperar dados do usuário
9	Ciclo de arquivamento em runtime
10	Configurações de arquivamento de valores de processo “archiving”
11	Arquivamento sob demanda
12	Arquivamento em Inicialização e desligamento do sistema
13	Ciclo de arquivamento processo ciclico e aciclico
14	Armazenamento de dados em memória

Fonte: os autores a partir de dados da pesquisa

Tabela 3 – Categorias iniciais

As categorias inciais, apresentadas na Tabela 3, foram definidas a partir das unidades de registro. Nesse sentido, tanto o Sistema SCADA, como a RO do ONS, sugeriram segmentos de atividades classificados pela sua importância no processo.

A partir das categorias iniciais, descritas na Tabela 4, foram definidas três categorias intermediárias, todas associadas ao objeto do Macrocontrole No. 11 do CIS CSC. Essas categorias intermediárias representam, respectivamente, um processo interno e externo de geração de backups, a geração dos arquivos internos de *runtime*, a partir dos quais os backups são gerados e, por último, o processo de recuperação de dados de processo e de usuários existentes em backup. Pelo exposto, é possível verificar que para os Subcontroles do Macrocontrole 11 do Framework CIS CSC, os subsídios para a sua efetiva construção e gerenciamento de recuperação de dados podem ser identificados no sistema SCADA, independentemente de o agente definir e operar um processo formal e estruturado de

backup e restauração de dados, que esteja vinculado a um processo de gestão de riscos. A Tabela 4 a seguir ilustra as categorias intermediárias identificadas e seus respectivos conceitos norteadores.

Categoria Intermediária	Conceito Norteador	Categoria Inicial
Geração de Backup externo ao SCADA **Atende: CIS CSC 11.1 e 11.4**	O Sistema SCADA é dotado de ferramentas responsáveis pela geração de cópias de arquivos de segurança externos ao runtime, os quais são armazenados em diretórios específicos informados por caminho a ser utilizado, podendo ser em Servidores da Rede de Comunicação de Dados ou armazenamento externo. Além da possibilidade de alta disponibilidade oferecida por um sistema com redundância (Cluster), o sistema também oferece outra via de recuperação de dados de processos e geração de backup, os quais são configurados no runtime ou gerados a partir de procedimentos manuais de exportação para arquivos externos.	[1][2][3]
Geração de arquivos internos ao SCADA com dados de processo e de usuários **Atende: CIS CSC 11.2**	Para a geração de backups de segurança, o sistema SCADA é configurado para a geração de arquivos em tempo real de informações do processo supervisionado ou arquivos de usuários que são utilizados para interfaces com sistemas de proteção, comando e controle, assim como informações de interface com plataformas externas. A geração das informações de processos obedecem configurações específicas que definem os ciclos a serem utilizados automaticamente ou arquivamento por demanda operacional e local de armazenamento.	[4][5][9][10] [11][12][13] [14]
Recuperação de arquivos Backup externo ao SCADA **Atende: CIS CSC 11.3 e 11.5**	A recuperação de dados armazenados em arquivos externos (backups) também é uma função customizável do Sistema SCADA e é realizada por comando interno manual configurável. Essa operação pode ser realizada por meio do método de recuperação do WinCC ou ação de importação, de forma segura e integra, utilizando arquivos gerados pelos métodos de backup internos (runtime em arquivos de processo e arquivos de usuário) ou externos (exportação), respectivamente.	[6][7][8]

Fonte: os autores a partir de dados da pesquisa

Tabela 4 – Categorias intermediárias

A partir das informações obtidas e organizadas nas Tabelas 2, 3 e 4 pôde-se verificar que os subsídios necessários para a geração dos controles previstos no Macrocontrole 11 do CIS CSC estão disponíveis, qualquer que seja o Grupo de Implantação (IG1, IG2 e IG3). Contudo, a construção dos respectivos controles deve ser considerada e formalizada pelo processo de gestão de riscos associado, tendo como suporte os pilares definidos pelas três dimensões básicas: tecnologia, processos e pessoas. Com isso, será possível manter a disponibilidade, a confidencialidade e a integridade das informações que serão tratadas por esses controles (Nakamura, 2007).

A análise realizada nesta seção permitiu verificar que de fato, os aspectos sobre backup e recuperação de dados relacionados à dimensão "tecnologia" estão cobertos pelos manuais dos sistemas SCADA. Contudo, há de se ressaltar que a implementação de um processo de backup e recuperação de dados que utilize e valide essas funcionalidades depende do planejamento e operação de cada organização. Isso inclui garantir que as pessoas

consigam executar o processo de acordo com o que foi definido e que estejam preparadas em operar as funcionalidades de restauração de dados em caso de materialização de algum risco.

5. Conclusões

Esse trabalho teve como objetivo avaliar a abrangência dos procedimentos de backup e recuperação de dados disponíveis no sistema SCADA, verificando sua conformidade com os controles do grupo 11 do *framework* CIS CSC, que versam sobre backup e recuperação de dados. O trabalho foi conduzido analisando o manual de referência do Sistema SCADA da Siemens WinCC V7.5 SP2, sistema muito utilizado no ambiente do setor elétrico brasileiro.

Por meio de técnicas de análise de conteúdo foi possível verificar que, apesar de o sistema possuir as funcionalidades necessárias para a realização dos procedimentos, não é possível garantir que eles são devidamente executados pelas empresas de geração, transmissão e distribuição de energia elétrica já que é necessário que as funcionalidades existentes nesses manuais sejam suportadas por processos de backup e recuperação de dados, e por sua execução e/ou monitoração efetiva de pessoas capacitadas.

Das 14 categorias iniciais identificadas, pôde-se perceber que 11 delas estavam associadas ao processo de geração de backup (externo ou interno) e as outras 03 associadas à recuperação de dados. Isso mostra que o sistema SCADA tem as funcionalidades necessárias para se garantir o processo de recuperação de dados definido no Macrocontrole 11 do CIS CSC, no entanto os instrumentos para a realização da gestão dessas funcionalidades não se apresenta de forma prática por meio de controles específicos.

Isto posto, a ausência de controles de backup e recuperação de dados no ARCiber sugere uma lacuna que precisa ser enfrentada pelas empresas Geradoras, Transmissoras e Distribuidoras de Energia Elétrica, sob supervisão e auditoria do ONS. Espera-se que uma próxima versão do ARCiber normatize esse ponto.

A perda definitiva das informações de usuários e de processsos do Sistema SCADA, em tempo real, podem provocar interrupções no fornecimento de energia elétrica e um tempo de recomposição demasiadamente grande, causando grandes prejuízos aos consumidores e às empresas concessionárias.

A relevância desse trabalho está em suscitar, portanto, o debate sobre a necessidade de revisão da RO-CB.BR.01, uma vez que a ausência de controles de Recuperação de Dados no ambiente regulado ARCiber, apesar do sistema SCADA possuir capacidade de atender aos subsídios definidos pelos Subcontroles do Macrocontrole Nº. 11 do Framework CIS CSC, eles não são evidenciados, levando a uma grande fragilidade ao processo de gestão de riscos cibernéticos do sistema elétrico de potência.

Por fim, esse trabalho oferece uma contribuição ao processo de avaliação dos riscos cibernéticos a que está submetida a infraestrutura operacional do Sistema Elétrico Brasileiro - SEB, diante das recentes ações do ONS.

Uma evolução do presente estudo pode ser sugerida como trabalho futuro, no sentido de se avaliar outros Macrocontroles do Framework CIS CSC, para os quais o ARCiber do ONS também não tenha previsto controles em seu processo de gestão de riscos cibernéticos, proposto por meio da Rotina Operacional RO-CB.BR.01 Revisão 00.

Agradecimentos

O autor Eduardo de Oliveira Lima agradece o suporte da Universidade de Brasília, por meio do DPG, Edital 01/2022; da ENBPar – Empresa Brasileira de Participações em Energia Nuclear e Binacional S/A. O autor Rafael Rabelo Nunes agradece o suporte do Centro Universitário Atenas; da Universidade de Brasília, por meio do Edital DPI/DPG 02/2022. Os autores Fernando Rocha Moreira e Rafael Rabelo Nunes agradecem o suporte do Ministério da Justiça e Segurança Pública representado pela Diretoria de Tecnologia da Informação e Comunicação (TED DTIC/SE/MJSP 01/2019). O autor Fernando Rocha Moreira agradece o suporte da FAP/DF, por meio do Edital 07/2022.

Referências

Accenture Security, (2019). The Cost of Cybercrime, Traverse City, Michigan: Ponemon Institute, from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Alcaraz, C; & Zeadally, S., (2015). “Critical infrastructure protection: Requirements and challenges for the 21st century”. International Journal of Critical Infrastructure Protection, Vol. 8, Pages 53-66. DOI: 10.1016/j.ijcip.2014.12.002

Bardin, L., (2011). Análise de Conteúdo. São Paulo: Edições 70.

CIS CSC - Center for Internet Security, (2021). “Simplified & Prioritized Cyber Defense Guidance”, CIS CSC Critical Security Controls Version 8.

Cooper, D. R.; Schindler, P. S. (2016). “Métodos de Pesquisa em Administração”, 12ª Edição. [S.l.]: McGraw Hill Brasil.

Countwordsfree, (2022). “Text Processing Tools”, from https://countwordsfree.com/

DHS CSSP - Common Cybersecurity Vulnerabilities in Industrial Control Systems, Department of Homeland Security, 92011). “Control Systems Security Program”.

Daneels, A., Salter. W., (1999). “What is Scada?”, International Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, Italy.

Fossà, M. I. T., (2003). “Proposição de um constructo para análise da cultura de devoção nas empresas familiares e visionárias”. Tese (Doutorado em Administração). Universidade Federal do Rio Grande do Sul, Porto Alegre.

Ibrahim, A. I. G., (2021). “Cybersecurity: Panorama and Implementation in 2021”, Safety and Security Engineering IX, WIT Transaction on the Built Envinonment, Vol. 206, WIT Press. DOI: 10.2495/SAFE210041

Plèta, T., Tvaronavičienė, M., Casa, S., Agafonov, K., (2021). “Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases”. HAL Open Science. HAL: hal-03271856

Laprie, J. C., Kanoun, K., Kaanishe, M. (2007). “Modelling interdependencies between the electricity and information infrastructures”, in Computer Safety, Reliability, and Security, ed: Springer, pp. 54-67, DOI:10.1007/978-3-540-75101-4_5.

Marconi, M. L.; Cientifica, E. F. da M. , (2003). 5ª edição, editora atas sa. São Paulo.

Mozzato, A. R; & Grzyboviski, D., (2011). “Análise de Conteúdo como Técnica de Análise de Dados Qualitativos no Campo da Administração: Potencial e Desafios”. Revista de Administração Contemporânea, Curitiba, v. 15, n. 4.

Muncaster, P., (2014). “Microsoft Zero Day Traced to Russian ‘Sandworm’ Hackers,” Infosecurity Magazine.

Nakamura, E.; de Geus, P. L. (2007). “Segurança de Redes em Ambientes Cooperativos”. São Paulo: Novatec.

NIST, (2018). “Framework for Improving Critical Infrastructure Cybersecurity”, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Operador Nacional do Sistema Elétrico – ONS, (2021). “Manual de Procedimentos da Operação Módulo 5 - Submódulo 5.13, Número RO-CB.BR.01, Rev. 00, Item 4.1.11”.

Prodanov, C. C.; Freitas, E. C. D. (2013). “Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico”, 2ª Edição. [S.l.]: Editora Feevale

Scada System Siemens WinCC V7.5 SP2, (2020). SCADA WinCC: Working with WinCC, ASE50503017-AA.

Souza, J. R., Santos, S. C. M., (2020). “Análise de conteúdo em pesquisa qualitativa: modo de pensar e de fazer”, Pesquisa e Debate em Educação, Juiz de Fora: U FJF, v. 10, n. 2.

Sridhar, S., Hahn, A., Govindarasu, M., (2012). “Cyber–physical system security for the electric power grid”, Proceedings of the IEEE, vol. 100, pp. 210-224. DOI**:** 10.1109/JPROC.2011.2165269

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A., (2015). “Guide to industrial control systems (ICS) security”, NIST Special Publication, vol. 800-82. DOI**:** 10.6028/NIST.SP.800-82r2

USCERT - United States Computer Emergency Readiness Team, (2018). Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, from https://www.us-cert.gov/ncas/alerts/TA18-074A

Vergara, S. C., (2006). “Projetos e relatórios de pesquisa”. São Paulo: Atlas

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 16/12/2021
Aceitação/Acceptance: 08/02/2022

El gran juego interminable: estudio de caso afgano

Rui Pereira[1], Luís Malheiro[2]

pereira.rms1@gnr.pt; malheiro.lcr@gnr.pt

[1] Centro de Estudos Globais da Universidade Aberta, Lisboa, Portugal

[2] Centro de Investigação Desenvolvimento e Inovação da Academia Militar, Academia Militar, Instituto Universitário Militar, Rua Gomes Freire, 1669-203, Lisboa, Portugal

Pages: 326-334

Resumen: Afganistán es un país del Medio Oriente, caracterizado por sus montañas, planicies y diversidad cultural. Es conocido por ser el cementerio de los imperios y donde tiene lugar el Gran Juego entre Rusia y Reino Unido. Más recientemente, es un país conocido por la producción de drogas, el terrorismo, las violaciones de los derechos humanos y la guerra que se desarrolla después del 11-S. El principal objetivo de esta investigación es analizar el origen del conflicto y el papel de los aliados y los talibanes. Siguiendo un enfoque cualitativo de este estudio de caso, utilizamos la revisión y el análisis de la literatura para inferir nuestra respuesta. La principal conclusión es que el conflicto tiene causas profundas, basadas en la ética, la religión, la lingüística y la falta de pertenencia nacional. A esto se suman los problemas de organización interna, crisis económica y política que permiten el desarrollo de la corrupción y el desprestigio en los gobiernos.

Palabras clave: Afganistán; causas del conflicto; instrumentos de poder; naturaleza del conflicto

The big never-ending game: Afghan case study

Abstract: Afghanistan it´s a country in Middle East, characterized by their mountains, highlands, and cultural diversity. It´s known by the graveyard of empires and where takes place the Big Game between Russia and United Kingdom. More recently it's a country now known by the drugs production, terrorism, human rights violations, and war that takes place after 11-S. The main objective of this research is to analyses the origin of the conflict and the role of the allies and Taliban's. Following a qualitative approach to this case study, we use the literature review and analysis to infer our answer. The main conclusion is that the conflict has root causes, based on the ethics, religious, linguistics and lack of national belonging. To this we can add the problems of internal organization, economic and political crisis which allow the development of corruption and discredit in governments.

Keywords: *Afghanistan; conflict causes; power tolls; Conflict nature.*

1. Introducción

Afganistán es un país ubicado en la región de Medio Oriente que se caracteriza por una morfología montañosa con planicies al norte y suroeste. Es un país único por la complejidad de etnias, religiones, culturas, idiomas y organización.

Afganistán ya fue un país donde la gente vivía en paz y donde incluso había turismo. Sin embargo, hoy en día la información que nos llega sobre el país es principalmente por razones negativas, desde la producción de estupefacientes hasta el desarrollo de conflictos. Este ha sido el caso principalmente desde los conflictos que tuvieron lugar en el período del gran juego entre los imperios ruso e inglés, que fueron seguidos por conflictos internos.

Pero el gran cuadro histórico de los conflictos está marcado principalmente por el 11-S y el posterior uso de diversos instrumentos, incluido el vector militar, materializado con una intervención militar en Afganistán. Fue la primera intervención en la que un miembro de la Organización del Tratado del Atlántico Norte (OTAN) invocó el artículo 5 (sobre defensa mutua) para justificar tal intervención.

Así, la presente investigación tiene como objetivo central el análisis de las causas del conflicto en Afganistán.

Para lograr este objetivo, nos proponemos desarrollar un estudio ético, posicionándose ontológicamente en el relativismo y epistemológicamente en el interpretativismo, basado en el razonamiento deductivo, con una estrategia mixta basada en un estudio de caso. El estudio será transversal, recurriendo principalmente al análisis documental.

La investigación está organizada y estará delimitada por el estudio de las causas del conflicto, los instrumentos de poder utilizados por los Aliados y la naturaleza del conflicto, al que seguirán las conclusiones.

2. Causas del conflicto

Como referencia y delimitación del análisis vamos a utilizar como inicio del marco temporal el momento del “Gran Juego”. Periodo histórico marcado por los conflictos y competición entre dos imperios, el ruso y el inglés. Este mismo periodo contribuye como referencia y delimitación del espacio, permitiendo definir las actuales fronteras del territorio afgano y su constitución ética, cultural y social.

Para el análisis de las causes de conflictos se tiene como referencia el pensamiento de Gaston Bouthoul y del Instituto Español de Estudios Estratégicos, que los clasifican en tres niveles de grandeza: profundo o estructural; medio o coyuntural; superficial o litigioso (IEEE, 1994, pp. 28,29).

2.1. Causas profundas

Desde el punto de vista interno del país, las causas de conflicto más recurrentes son influenciadas por la geografía e historia.

Afganistán es un territorio muy marcado pela diversidad étnica, lingüística, cultural y religiosa (López-Zuazo, 2021; Murphy, 2010). En consecuencia, no existe una conciencia común de identidad nacional.

El país ha sido marcado por el dominio de los Pashtu, que son adversos a la modernización y se asumen como el pueblo genuino de Afganistán. Es la etnia que más destaca, rivalizando con las restantes, y donde tiente origen los talibanes. Que perderán el poder con la intervención de los Aliados y que ahora retoman y controlan el país (López-Zuazo, 2021).

2.2. Causas conyunturales

Estas causas son más delimitadas en lo tiempo y espacio.

Las causas geopolíticas son marcadas por tres periodos distintos: el periodo en que Afganistán fue usado como zona de conflicto entre rusos y el Imperio Británico; el periodo de la ocupación rusa en que los afganos jihadistas (principalmente etnia pashtu) recibieron apoyo de otros países como Estados Unidos de América (USA), China e irán; el periodo siguiente marcado por la hegemonía de la etnia pashtu e imposición de la sharía por los talibanes, hasta el 11 de septiembre de 2001. Estés periodos contribuirán a la degradación de escasas las infraestructuras políticas, económicas, sociales, militares, sanitarias.

En la historia de militar Afganistán siempre se verifico el déficit de fuerzas armadas. Para el enfrentamiento de las amenazas, internas y externas, eran desarrolladas alianzas entre tribus. Con la intervención de la alianza su ejército fue desarrollado y equipado a semejanza al de los americanos. Sin embargo, no fue capaz de detener el avanzó de los Talibanes con la salida de los aliados, pues fueran preparados para trabajar solos sin toda la tecnología y apoyo de los aliados (Servert, 2021).

Gran parte de las infraestructuras son débiles y la economía no es sustentable y la inversión externa es limitada. Se basa en agricultura de subsistencia y en la larga producción de opio (Murphy, 2010) que además sirve para financiar a los Talibanes (Moreno, 2010; Sopko, 2021 p. 63). En cambio, tiene varios recursos naturales como el gas y otros recursos naturales como los minerales. Aunque no los consigue explorar, motivo por lo cual China tiene demostrado interés y abertura de dialogo con los talibanes con intención de garantizar su acceso a los recursos.

2.3. Causas superficiales

Como ya fue referido, durante el periodo del “gran juego” fue posible observar e identificar los distintos comportamientos e intereses de los imperios, materializándose con el envío de misiones diplomáticas, relaciones de apoyo a determinados lideres y tentativas de expansión. Además de los imperios referidos también EUA e Irán varias veces influencian la política interna y juegos de poder internos de Afganistán.

Al mismo tiempo también fue y continua a ser fuertemente marcado por distintitos intereses y alianzas que son constituidas momentáneamente en luchas de poder internas.

Más recientemente, se destacó la corrupción existente por varios funcionarios del estado y políticos en los órganos estatales, en las fuerzas del país y otras organizaciones (Sopko, 2021; Murphy, 2010; López-Zuazo, 2021).

Verificamos así que el origen del conflicto en Afganistán tiene distintas causas. Algunas de las causas tienen origen en un espacio temporal lejano como el propio origen se su población y territorio. Finalmente, una intervención en Afganistán exige un abordaje integral de los distintos instrumentos de poder.

3. Utilización de los instrumentos de poder dime por los aliados en su intervención tras el 11-s

El Estado, según la perspectiva de Hobbes es la entidad a quien el ciudadano delega su poder para usarlo en su nombre. Los poderes delegados al estado son: el legislativo, el ejecutivo y el judicial. Además, en situaciones de conflictos pueden recurrir a otros no estatales, los cuales se quedan a su disposición y contribuyen para sus instrumentos de poder.

Los instrumentos de poder del estado en los conflictos son: diplomático, información, militar y económico (DIME) (Ministerio Defensa, 2018). Su uso es una constante en las relaciones internacionales y cuando utilizados de forma sincronizada se denomina de guerra hibrida (López-Zuazo, 2021).

Así vamos a analizar la intervención de los EUA y aliados según los instrumentos de poder referidos tras los atentados de 11- S. Los cuales marcarán al mundo cuando en directo se presenciaba como la mayor potencia mundial era atacada por un actor no estatal. En consecuencia, invocando la legitima defensa, los EUA y aliados en coligación inician la operación *Enduring Freedom* (OEF), la operación de la *NATO Eagle Asssit y la International Security Assistance Force* (ISAF).

3.1. Diplomático

Inmediatamente tras los atentados de 11-S, los EUA realizaran negociaciones con los Talibanes, gobierno de Afganistán, para que estos entregasen a Osama Bin Laden para que respondiese por los atentados. No obstante, la diplomacia, los Talibanes se niegan a entregarlo, provocando la intervención militar referida (López-Zuazo, 2021).

El esfuerzo diplomático paralelamente también fue desarrollado con sus aliados y en las organizaciones internacionales como la OTAN y la Organización de las Naciones Unidas (ONU). Además, antes de la intervención militar, la diplomacia de los Estados Unidos tuvo que procurar el apoyo de otros aliados y de organizaciones internacionales.

La intervención militar inicial permitió retirar los Talibanes del poder, localizar y eliminar a Bin Laden. Con los Talibanes fuera del poder, y muchos de ellos huidos a Pakistán, la Alianza del norte se disuelve y retoman sus tribus. La fuga para el Pakistán creó un problema a los Aliados, pues este ha rechazado colaborar y entregar a los Talibanes. La esencia de la cuestión es que los Aliados no pretendían hostilizar Pakistán para evitar su aproximación a China. Así los talibanes conquistaran un lugar seguro para los Talibanes (Frías, 2021 p. 11).

Mas recientemente durante la gestión del proceso de retirada de los militares aliados, la diplomacia no fue capaz recuperar al gobernó afgano y los Talibán para una resolución pacífica del conflicto.

3.2. Información

El poder de información de las fuerzas aliadas estaba muy desarrollado especialmente a nivel tecnológico y fue aplicado a nivel operacional y táctico (Pinto, 2020 p.50), culminado con identificación de Bin Laden. Pero su estrategia incremento el sentimiento antioccidental propagado por los Talibán.

En respuesta los Aliados cambiarán su estrategia de información y comunicación. Tenían que obtener la confianza de la población en oposición a los Talibán. Pero fueron ineficaces y derrotados en esa disputa ideológica (Pinto, 2020 p.50).

Además, no fueran capaces de identificar las reales necesidades, problemas y sus soluciones para el desarrollo de la sociedad y país.

Igualmente fueran incapaces de prever la rápida recuperación del poder por los Talibanes.

3.3. Militar

El instrumento militar de los aliados era muy superior en recursos a sus oponentes y fue muy eficaz de inicio. Pero los Talibán no se retiran por completo y efectuarán lucha tipo guerrilla y contrainsurgencia atacando a la Alianza.

Los medios militares disponibles no eran suficientes para la resolución del conflicto. No obstante, el poder político no asignó medios suficientes para que la intervención militar pudiera cumplir su misión.

Esa opción política quedó clara por las palabras de Dom Rumsfeld, afirmando que se va para guerra con los medios que se tiene y no con los que se debería o querría (Stavridis, 2021). No hubo empeño total (Frías, 2021). Parte de las fuerzas que deberían garantizar la seguridad de la población y territorio estaban garantizando la seguridad de las instalaciones (Moreno, 2010; Alberto, 2021).

Además, la influencia cultural occidental, poco adaptada a guerra de contrainsurgencia, condicionó su intervención (Frías, 2021 p. 11). Uno de los reflejos fué que formaran un ejército afgano a su imagen y no adaptado su realidad local (Stavridis, 2021). Además, condicionados por los medios disponibles fueran incapaces de garantir la seguridad de la población en los campos de opio contra los talibanes.

3.4. Económico

A nivel económico Afganistán estaba muy débil, pero la producción de opio era creciente. Durante la ocupación de los Aliados, los Talibanes sacaron todo el dinero que podían del banco. Esa reacción provocó una ruptura del sistema financiero.

La intervención de la Alianza permitió una positiva recuperación económica del país. Fueron efectuados varias inversiones en infraestructuras y se formaron trabajadores locales. Pero el desarrollo del sistema financiero era complejo por no existir confianza y

si una fuerte corrupción a todos los niveles. Además, algunos trabajos e infraestructuras desarrolladas no les eran usada para su fin, generando un sentimiento de fracaso de los aliados (Sopko, 2021).

La intervención en Afganistán por los aliados utilizó los cuatro instrumentos de poder. Su utilización en mayor o menor grado fue distinta en el desarrollo de la intervención, provocando distintos efectos que conducirán a la actual situación. Así, es importante analizar la naturaleza del conflicto para una mejor reflexión.

4. Interpretación de la naturaleza del conflicto de acuerdo con los postulados de tratadistas

El estudio de la estrategia después de la guerra fría se cambió y quedo más difuso con los nuevos conflictos modernos de la complejidad del entorno (Baylis, et al., 2019). No obstante, las condiciones materiales y la lógica del conflicto se mantienen las mismas del siglo XIX, motivo por el cual es importante continuar estudiando las obras clásicas relevantes como de Carl Von Clausewits y de SunTzu (González, 2009).

Después del ataque del 11-S los EUA no tuvieron la capacidad de influir para que el régimen Talibán (Gobierno de Afganistán) entregase a Bin Laden (Líder de Al-qaeda) y avanzaron para la guerra "un acto de fuerza que se lleva a cabo para obligar al adversario a acatar nuestra voluntad" (Clausewitz, 2020 p. 23).

SunTzu refería que Los maestros del Arte de la Guerra son aquellos que "consiguen que se rindan impotentes los ejércitos ajenos sin luchar" (Tzu, 2021 p. 06), pero los EUA optaron por avanzar la confrontación. Estaban heridos y toda la sociedad quería justicia, juntando así los dos elementos intervinientes en las luchas entre hombres según Clausewitz "el sentimiento y la intención hostiles" (Clausewitz, 2020 p. 24).

Como ya fue posible referir la intervención militar es apenas uno de los instrumentos de poder disponibles que el Estado tiene para la guerra. Según Clausewitz (2020) la guerra es un camaleón. La guerra puede cambiar de clases de acuerdo con la naturaleza de las emociones y circunstancias, estableciendo una "trinidad" entre: violencia y pasión (de lo pueblo); valor y competencia (de los ejércitos); subordinación y razón (del gobierno).

En Afganistán se destaca la superioridad a largo plazo de la pasión de los Talibanes que fueron capaces de mantener sus objetivos y pasión para alcanzar superioridad cuando eran militarmente inferiores y a largo de los 20 años de ocupación de los aliados. Su voluntad de vencer enfrentándose a un adversario superior también demostraron su coraje y espirito de sacrificio.

Además, las elites y la población afgana fueran perdiendo su pasión y en la solución que los aliados presentaban y constataron que no eran tan fuertes y generosos como hacían creer (Alberto, 2021), especialmente después de la anuncia retirada.

Por otro lado, con la limitada atribución de medios desde inicio, los aliados demostraran poco interés en la guerra. Situación que se ve agravada con los costosos costes humanos y económicos resultantes (Alberto, 2021). Sobre la duración de las batallas Sun Tzu refería que cuando es larga "desanimará a tus tropas y embotará tu espada… tus suministros se

agotarán….no es beneficioso para un país dejar que una operación militar se prolongue por mucho tiempo" (Tzu, 2021 p. 06)

Además, a lo largo de los años el apoyo de población fue bajando, hasta que, "hoy en día, más de dos tercios de la población considera que las trobas americanas deberían volver a casa" (López-Zuazo, 2021). Al mismo tiempo "la idea de que la OTAN había fracasado en el teatro afgano estaba muy extendida desde hace mucho tiempo" (Frías, 2021 p. 01)

Basados en lo concepto de Clausewitz de los Centros de Gravedad (CoG), adopta una estrategia de intervención usando toda su superioridad tecnológica en los CoG del adversario, obteniendo un gran éxito en la fase inicial (González, 2009). Pero no recorrer del conflicto tuvieran que realizar operaciones de contrainsurgencia que ejecutas del punto de vista occidental no obtuvieran éxito, pero por lo contrario fueran exploradas por los Talibanes. Hecho que nos lleva al pensamiento de Sun Tzu "Si conoces a los demás y te conoces a ti mismo, ni en cien batallas correrás peligro; si no conoces a los demás, pero te conoces a ti mismo, perderás una batalla y ganarás otra; si no conoces a los demás ni te conoces a ti mismo, correrás peligro en cada batalla" (Tzu, 2021).

En oposición los Talibanes utilizarán la estrategia indirecta delante un adversario más fuerte utilizando técnicas de guerra irregular. Su actividad refleja en gran parte el pensamiento de Sun Tzu (Tzu, 2021 p. 04) "El arte de la guerra se basa en el engaño… Golpear al enemigo cuando esta desordenado…intenta irritarle…fomenta su egoísmo… ataca el enemigo cuando no está preparado y aparece cuando no te espera". Además, cuando se supo que los aliados se iban a retirar y empezaron las negociaciones, solo tuvieron que esperar para volver a ocupar y asaltar el poder. "Consolida la energía… ahorra las fuerzas … mantén en secreto tus formaciones y tus planes, … y espera a que se produzca un punto vulnerable para avanzar" (Tzu, 2021 p. 40).

Así, pasados 20 años de conflictos, millones de dólares gastados y millares de vidas perdidas, la resiliencia de los Talibanes permitió que su portavoz afirmase el día 16 agosto de 2021 "*Thanks to God, the war is over in the coutry*" (Rasheed, et al., 2021).

5. Conclusiones

El estudio de la estrategia y de los conflictos que estudian los fines políticos, empleo del instrumento de poder y efectos producidos, es un conocimiento complejo y difuso, siendo necesario hacer análisis integral de distintos dominios. Sin embargo, la lógica de la guerra permanece casi la misma, así que continúa siendo importante analizar autores clásicos.

Afganistán durante grande parte de su historia estuvo envuelto en conflictos, siendo que en parte fue utilizado como un campo de imperios que se confrontaban, constituyendo también una zona tapón.

Siendo un país marcado por dificultades económicas, por diferencias étnicas, religiosas y lingüísticas, muchas das veces sus habitantes se aprovechan la intervención externa para satisfacer sus necesidades de poder internas. Además, su debilidad económica, social y política, permitió el desarrollo de la corrupción y descredito en su gobierno y prosperidad. Siendo que ahora grande parte de su riqueza es proveniente del cultivo

de opio y de recursos naturales como el gas y minerales. Pero las causas de conflicto más complejas son las profundas asociadas a las diferencias entre su pueblo y falta de sentimiento de nacionalidad.

Los actuales conflictos exigen que todos los instrumentos DIME sean utilizados en situación de guerra – guerra hibrida. Durante la intervención es necesaria una mayor coordinación para que sea más eficaz, principalmente el Diplomático e el Militar.

Cuando se analiza la naturaleza del conflicto actual de Afganistán permite verificarse que la intervención de los aliados se identifica más con el pensamiento de Clausewitz. Por el contrario, la intervención de los Talibanes se identifica más con la de Sun Tzu. Lo que más se destaca fue la utilización de la guerra no convencional y la voluntad de vencer de los Talibán, identificada por Clausewitz como el elemento irracional de la trinidad, siendo esta la clave para el regreso del poder de Afganistán de los Talibán.

Referencias

Libros y capítulos de libros

Baylis, John, J. Wirts, James e S. Gray, Colin. (2019) *Strategy in te contemporary worl*d. 4ªed.

Clausewitz, Carl Von. (2020) *Da guerra*. Clássica editora. Forte da Casa.

Murphy, Thomas Joseph. (2010) *Afghan culture, observations, insights, and lessons*. *US Army combined center*. Disponible en: https://cgsc.contentdm.oclc.org/digital/collection/p15040coll4/id/26

[Consulta: 10 de ocutbre de 2021]

Tzu, Sun. (2021) *El Arte de la guerra*. 2021. Elejandria.com. Disponible en: https://www.elejandria.com/libro/el-arte-de-la-guerra/sun-tzu/847

[Consulta: 10 de ocutbre de 2021]

Articulos de revistas científicas

IEEE. (1994). Analisis factorial. Analisis factorial de las causas que originan conflictos bélicos. *Cuadernos de Estratégia*. 1994, Vol. 69, pp. 27-45.

Pereira, C. (2011) "Dez Anos de Guerra no Afeganistão". *Nação e Defesa*, 5(130). 2011, pp. 179-216.

Sopko, John F. (2021) "What we need to learn: lessons from twenty years of afganistan reconstruction". *SIGAR*.

Articulos de revistas de divulgación

González, Francisco José Ruiz. (2009). Estrategía militar y política: temas teóricos y aplicación práctica. *Beletim de informacion* n.º 308. 2009, pp. 29-52.

UNDOC. (2021) "Drug market trends: cannabis opioids". *Austria: United Nations*, 2021. ISBN 9789211483611

Medios comunicación

BBC News. (2021) *Afeganistão: a guerra explicada em 10 pontos*. Disponible en: https://www.bbc.com/portuguese/internacional-57768118

[Consulta: 20 de ocutbre de 2021]

BBC News. (2021) *Afghanistan: What has the conflict cost the US and its allies?* https://www.bbc.com/news/world-47391821

[Consulta: 24 de ocutbre de 2021]

Rasheed, Zaheena, Varshalomidze, Tamila e Gadzo, Mersiha. (2021) *Biden defends Afghanistan pullout amid airport chaos*. Aljazeera [Online]. https://www.aljazeera.com/news/2021/8/16/taliban-says-afghanistan-war-over-as-president-diplomats-flee.

[Consulta: 24 de ocutbre de 2021]

Stavridis, James. (2021) *In the end the Afgan Army was always doomes. Politics & Policy*. *Bloomberg*. [Online]. https://www.bloomberg.com/opinion/articles/2021-08-16/the-afghan-army-was-always-doomed.

[Consulta: 20 de ocutbre de 2021]

Otros

Alberto, José Luis Calvo. (2021) *Tres oportunidades perdidas en Afganistán*. IEEE Documento Opinión 93/2021.

Frías, Carlos Javier. (2021) *Afganistán ¿el fin de la contrainsurgencia*? IEEE Documento Opinión 95/2021.

López-Zuazo, Manuel López-Lago. (2021) *Afganistán y el retorno del talibán*. IEEE Documento de opinión 94/2021.

López-Zuazo, Manuel López-Lago. (2021). *La competición en el contínuum*. IEEE Documento opinion 56/2021.

Ministerio Defensa. (2018) PDC-01(A) *Doctrina para el empleo de las FAS*. s.l. : Ministerio Defensa, 2018. ISBN: 978-84-9091-318-2.

Moreno, Alberto Priego. (2010). *Droga, inestabilidad y subdesarrollo en afganistán: soluciones al círculo vicioso*. IEEE Documento de opinión 15/2010.

Pinto, Roberto (2020) Guerra do Afeganistao: o uso da informação e a comunicação dos EUA, de 2001 a 2006. *Dissertação*. *Escola de Guerra Naval*. Rio de Janeiro

Servert, Rubén García. (2021) *Afganistán: ¿y ahora qué?* IEEE Documento Opinión 99/2021.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 11/10/2021
Aceitação/Acceptance: 05/01/2022

Factores clave en la evaluación del software libre o propietario para su uso en organizaciones militares y de defensa

Lewis Mahecha Ardila[1], Ricardo Naranjo Faccini[2], Carlos A. Castaneda-Marroquín[3], José María Riola[3], Carlos Hernán Fajardo-Toro[4]

lmahecha@ejercito.mil.co; rnaranjo@javeriana.edu.co; carlos.castaneda@enap.edu.co; Chema.riola@rga-psi.es; carlosh.fajardo@esap.edu.co

[1] Ejército Nacional de Colombia, Carrera 54 # 26-25, 111321, Bogotá, Colombia.

[2] Pontificia Universidad Javeriana, Avenida Carrera 7 # 40-62, 110231, Bogotá, Colombia.

[3] Escuela Naval de Cadetes "Almirante Padilla", Barrio Bosque, Isla de Manzanillo, Cartagena de Indias, Colombia.

[4] Escuela Superior de Administración Pública - ESAP, 760046, Cali, Colombia

Pages: 335-346

Resumen: El software libre y de código abierto (FOSS) ha ido creciendo constantemente en importancia, siendo herramientas implementadas en organizaciones privadas y públicas en el mundo. La migración a FOSS es hoy una alternativa que utilizan las instituciones públicas de los países de América Latina debido a su menor Costo Total de Propiedad (TCO) y una mejor gestión de las vulnerabilidades de seguridad. Este documento presenta una metodología que estandariza el proceso de selección de software sin importar si es FOSS o propietario, contemplando una evaluación integral que incluye aspectos técnicos, económicos y de mitigación de riesgos, que permite a los evaluadores y tomadores de decisiones particularmente militares o de defensa, una evaluación correcta y objetiva de elección del software. El método ha sido validado durante el proceso de selección entre diferentes alternativas de un sistema de correo electrónico para el Ejército Nacional de Colombia.

Palabras-clave: Adopción de software libre y de código abierto; Análisis de riesgos; ciberseguridad; Instituciones militares.

Key Factors in Evaluating Open-source or Proprietary Software for Use in Military and Defense Organizations

Abstract: Free and open-source software (FOSS) has been steadily growing in importance, being tools implemented in private and public organizations in the world. Migration to FOSS is today an alternative used by public institutions in Latin American countries due to its lower Total Cost of Ownership (TCO) and better management of security vulnerabilities. This document presents a methodology that standardizes the software selection process regardless of whether it is FOSS

or proprietary, contemplating a comprehensive evaluation that includes technical, economic and risk mitigation aspects, which allows evaluators and decision makers, particularly military or defense, a correct and objective evaluation. choice of software. The method has been validated during the selection process between different alternatives of an email system for the Colombian Armed Forces.

Keywords: Adoption of free and open-source software; Risk analysis; cybersecurity, Military institutions.

1. Introducción

Los estados establecen la defensa de su seguridad a través de una estrategia nacional valorando las amenazas y los riesgos que pueden tener. La aplicación de la ciberdefensa ha otorgado a las fuerzas militares colombianas la responsabilidad de la protección de las Infraestructuras Críticas Nacionales y los intereses nacionales en el ciberespacio que se plasma en los diferentes CONPES desarrollados desde el 2011 (Conpes 3701, 2011). Para poder cumplir esta misión, es necesario una gran inversión en diferentes elementos tecnológicos que permitan desarrollar todas las tareas de defensa, realizando un aprovechamiento racional de los recursos presupuestales asignados, manteniendo niveles aceptables del riesgo. Los costes de adquisición del software propietario (Software Comercial listo para usar - COTS) son elevados y también podrían surgir interrogantes sobre su compatibilidad con la seguridad nacional desde la visión del total control del funcionamiento y procesamiento que realizan las piezas de software al no tenerse acceso al código que se ejecuta.

Las soluciones de software libre y de código abierto (FOSS) llaman la atención al mismo tiempo que aumenta el gasto relacionado con las tecnologías de la información (TI) para la digitalización de las fuerzas militares. Surge la pregunta de si la implementación de FOSS es factible y que su selección como herramienta se pueda realizar de manera objetiva. El propósito de este trabajo es presentar una metodología basada en la evaluación de los riesgos para la correcta selección de soluciones software para las instituciones militares basadas en varios elementos que le permitirán a los diferentes tomadores de decisiones un método objetivo de decidir cómo escoger FOSS o COTS para su uso.

2. Software Libre y Coste total de propiedad

Durante las últimas décadas, el mecanismo de distribución del software está dado por dos modelos: los productos COTS que ofrecen una gran variedad de funcionalidades basado en un modelo de compra y venta de licencias y el FOSS que se distribuyen libremente. COTS son software que es propiedad de un individuo o una empresa donde existen restricciones de su uso basado en un acuerdo de licencia y su código fuente se mantiene en secreto. Existen limitaciones propias del software COTS que han surgido con el tiempo como actualizaciones costosas o debilidades de seguridad, lo que ha llevado a que se vaya consolidando el modelo basado en el software libre y de código abierto. Después de un comienzo lento a fines de la década de 1990 del siglo pasado (Tu, 2000), FOSS ha ido creciendo constantemente en importancia y expandiéndose en muchas arquitecturas de software en todo el mundo. Empresas como Google, Microsoft o IBM participan activamente en proyectos de código abierto. FOSS es un software que puede

ser libremente utilizado, modificado y redistribuido y que cualquier versión posterior basada en un paquete de software libre debe distribuirse con los términos originales de uso. La definición de software libre está estipulada como parte del Proyecto GNU y por la Free Software Foundation (GNU Software Foundation, 2022).

Existen posiciones antagónicas sobre FOSS, por ejemplo, algunos afirman que tienen una calidad menor que el software desarrollado tradicionalmente (Colford, 2009) o empresas que los usan por fiabilidad y seguridad como uno de los principales motivadores para usarlos (Red Hat, 2022). Al igual que una organización de carácter privado, las Fuerzas Militares deben centrar su atención en desarrollar la mejor estrategia de tecnologías de la información que apoye la misión de la organización ofreciendo un correcto funcionamiento de las operaciones de TI, la seguridad y la gestión de costes y gastos. De estos problemas, el presupuesto de tecnologías de la información es un objetivo de gestión continuo en dos aspectos: reducción de costes y aumento de valor del área de TI para el cumplimiento de la misión.

A pesar de los diversos enfoques y preocupaciones sobre qué elementos se deben utilizar al seleccionar FOSS, una idea común es la de reducción de costes. Nuestro estudio usa este enfoque, sin embargo, como se mostrará más adelante, el coste total de propiedad no es suficiente. La definición de TCO es el coste total de propiedad y operación de una pieza de software, que incluye tanto el costo monetario inicial de comprarlo como los costes asociados de implementarlo permitiendo una comparación entre varios productos y servicios de software a través de costes con términos similares (Lerner & Schankerman, 2010)

Las organizaciones que consideren el uso de FOSS buscan determinar los costes reales involucrados en elegir y vivir en un entorno de software de código abierto. A pesar de que a menudo es gratuito, la pregunta de si el FOSS es realmente más barato que COTS posiblemente puede responderse de manera inequívoca, pero no necesariamente responde la pregunta si el software a elegir es lo mejor para la organización.

3. Aspectos y factores clave para la evaluación de adquisición del software

Mientras que FOSS aporta claras ventajas para las organizaciones como la reducción de costes a través del no pago de licencia y la disponibilidad del código fuente para su modificación y revisión (Shaikh, 2012), la adopción de FOSS todavía plantea importantes desafíos de cuáles son los elementos clave para la evaluación de la mejor pieza de software que se debe adquirir por una organización. La confianza de que una pieza de software cumpla con su tarea no solo está relacionado con FOSS si no que es un problema general del software que no está atado al modelo de licenciamiento.

El riesgo real de seguridad en las áreas de tecnologías de la información por una pieza de software no es realmente lo que afecta el proceso de toma de decisiones, sino más bien el riesgo percibido por los tomadores de decisiones que es incorporado en sus factores de decisión para su adopción (Franch Gutiérrez, Susi, Annosi, Ayala Martínez, & P, 2013). La decisión de uso de un software en particular tiene varios riesgos potenciales que se deben evaluar en diferentes dimensiones. Es entonces la gestión de los riesgos lo que puede determinar una mejor elección basada en la evaluación de diferentes dimensiones

y su riesgo asociado y el riesgo aceptable. La gestión del riesgo de seguridad en tecnologías de la información (ISRM) se define como un modelo cíclico que tiene cuatro fases así (Raanan, 2011): identificación, cuantificación, control y monitoreo. Este concepto puede ser usado para determinar una mejor evaluación del uso de la pieza de software.

La imagen a continuación muestra las dimensiones necesarias en el proceso de evaluación del riesgo.

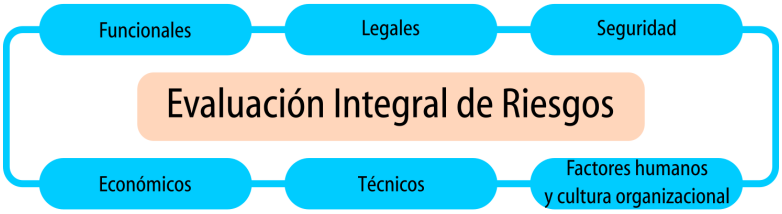


Figura 1 – Dimensiones para adquisición del Software basada en el riesgo

A continuación, se presentan los factores clave que se incluirán en la metodología basado en la evaluación de los riesgos:

Aspectos legales: La revisión legal es importante porque es en muchas situaciones la manera de dirimir conflictos con terceras partes. Se debe tener en cuenta tanto las leyes que puedan regir la contratación y utilización de los servicios asociados a la implementación del proyecto junto con la revisión de los acuerdos de licencia que se deban usar, que muchas veces este último se pasa por alto. En el caso de FOSS el acuerdo de licencia puede estar enmarcado en la licencia GNU, BSD, Apache entre otras. Por ejemplo, la licencia FOSS más utilizada es la licencia pública general GNU la cual tiene dos restricciones: requiere que las versiones modificadas del software también estén abiertas (*copyleft*), y requiere que el código se combine solo con otros programas distribuidos bajo licencias que comparten el primer requisito. Aquí el evaluador podrá verificar el riesgo sobre un tipo de licencia u otro.

Aspectos Funcionales: Los requisitos funcionales definen las funciones que debe tener un software y sus componentes. El inventario concienzudo de todas las tareas que debe realizar el software es parte fundamental en la decisión de usar o no usar un software. Esta tarea puede realizarse a través de la definición de casos de uso que el software debe resolver. Normalmente esta evaluación, aunque dispendiosa es necesaria para separar aspectos deseables de los necesarios permitiendo categorizar y priorizar cada característica para reconocer la pertinencia de un software y poderlo comparar con otras soluciones a la vez que se valora el riesgo que podría llegar a tener si no cuenta con una característica funcional.

Aspectos de seguridad: El software es un elemento dinámico que la organización adquiere y debe gestionarlo a lo largo de su vida en producción. Cualquier software

es susceptible a algún fallo, en ese sentido la seguridad inherente al software debe ser la capacidad de resolver de manera rápida cualquier vulnerabilidad a la que pudiera estar expuesto mediante su soporte. Muchos softwares independientes de su modelo de licenciamiento cumplen con modelos de buenas prácticas de desarrollo que garantizan que tienen un esquema de resolución de errores. En este sentido, en la evaluación de selección basada en una estrategia de mitigación del riesgo pueden enumerarse características como tiempo de vida del software, modelo de soporte, tamaño de la comunidad, tiempos de soporte, elementos que ayudarán a calificar el riesgo asociado en el uso del software. En este punto el evaluador puede acogerse a varios estándares de seguridad, que pueden permitir categorizar diferentes acciones que validen el nivel de madurez del software en términos de integridad, disponibilidad y confidencialidad.

Aspectos Económicos: Las discusiones económicas comienzan con la idea de que es posible ahorrar costes independientemente del modelo del licenciamiento. Sin embargo, el coste real de cualquier software va más allá del precio de licencia e incluye categorías como actualizaciones, capacitación o mantenimiento. Por ejemplo, el código abierto puede generar un desembolso mayor cuando la implementación está mal planificada. Otro ejemplo puede ser la existencia de una solución software de código propietario en contraposición de FOSS que exige una instalación técnica menos compleja lo que repercute en la reducción de costes de los servicios profesionales necesarios para su implementación e implica menores costes internos para el personal de tecnologías de la información. En este caso, la evaluación del coste total de propiedad (TCO) debe permitir calcular todos los desembolsos de dinero en el proyecto y ayudar a crear una comparativa de diferentes opciones de solución. El riesgo se puede valorar por las posibles desviaciones que pueden encontrarse de los elementos que se han incorporado en el cálculo del TCO.

Aspectos técnicos compatibilidad con terceras partes, hardware, software y gobierno de datos: Uno de los principales atractivos del FOSS es su base en estándares abiertos, combinados con código abierto. En conjunto, se entiende que esto reduce el bloqueo que tienen las soluciones propietarias, reduciendo el riesgo en términos de dependencia con terceras partes. El código abierto permite cierta combinación de recursos técnicos, experiencia y talento, y específicamente código para reutilización y personalización. La integración de nuevas piezas de software debe ser compatible con los desarrollos que se puedan hacer a largo plazo. Hay que poder valorar en el caso del software propietario esta capacidad de integración bajo la visión de utilización de estándares.

Es también importante la correcta documentación del software, en el caso del código fuente abierto, esta debe ser completa pues la inversión en tiempo para conocer el funcionamiento puede que haga no viable la selección de este software. También hay que tener en cuenta la documentación orientada al usuario final de cara a permitir la correcta apropiación y uso por parte ellos.

Factores humanos y cultura organizacional: Una actitud positiva de los usuarios estimulada por una correcta gestión del cambio puede ayudar a la adopción de un nuevo software. Igualmente, sí los usuarios tienen las habilidades y experiencia necesarias con las herramientas, la probabilidad de una adopción exitosa aumentará. Esta es una de las dimensiones que pueden catalogarse de mayor riesgo si se subestima o no se tiene

en cuenta en el desarrollo de implantación de un proyecto de software. La valoración de la experiencia de usuario y el uso de la herramienta junto con la gestión del cambio permiten mitigar los riesgos que puedan conllevar la adopción de la solución.

4. Metodología para la selección de software en proyectos de informática

En la adopción de un software, FOSS o COTS, se hace necesaria la comprensión y gestión de todos los riesgos que puedan darse en cada etapa del proceso de su selección (Silic, 2016). Una metodología basada en riesgos que evalúe en cada dimensión y etapa, los riesgos inherentes existentes, permiten al tomador de decisión tener una herramienta que aumenta su confianza en que está tomando una decisión racional alejándolo de la subjetividad y eliminando posibles errores del tipo: FOSS es más económico o COTS es mejor porque existe una empresa que lo respalda.

A continuación, se muestra la metodología desarrollada en la investigación para la elección del software, sin importar su estilo de licenciamiento, donde se combinan los aspectos y factores clave descritos en el anterior apartado con la secuencia de pasos donde se revisan diferentes áreas para la evaluación. La figura siguiente muestra la propuesta metodológica desarrollada para las organizaciones militares.

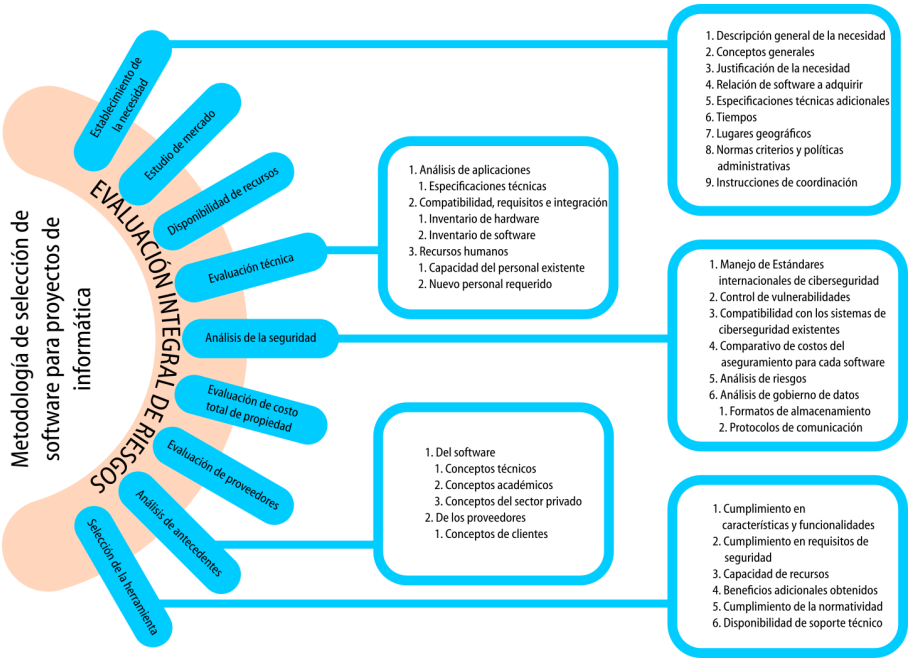


Figura 2 – Metodología de selección del Software

Establecimiento de la necesidad: Describir las razones que llevan a la institución militar a buscar una herramienta informática. Requiere un análisis de la relación entre

el ahorro de recursos que el software permitirá con respecto de los beneficios que se obtendrán al utilizarla. Hay que enumerar claramente la situación actual de la institución y la situación esperada tras la implantación del software en cuanto a personal, cobertura, tiempos de respuesta e inversiones económicas que se permitirán reducir. Igualmente hay que enumerar los beneficios que se espera obtener tras la implantación dando especial importancia a aquellos que soportan o que se encuentren relacionados con la misión de la institución militar. A cada uno de los costes y a cada uno de los beneficios se les debe asignar un nivel de prioridad.

Estudio de mercado: Se realizará una búsqueda en el mercado de la oferta existente de software que cumpla con las funcionalidades y requerimientos descritos durante el establecimiento de la necesidad. Analizando tanto el listado de actuales proveedores como de nuevos actores en el mundo del software COTS que suplan la necesidad descrita. Igualmente habrá que realizar la búsqueda de FOSS que provea solución de tal forma que se encuentren las diversas alternativas existentes a COTS provistas por comunidades que fabrican software libre y open-source.

Una vez se hayan encontrado los candidatos a solución se deberá realizar una verificación de las enumeraciones realizadas durante el Establecimiento de la necesidad, para agregar nuevos elementos identificados al analizar las funcionalidades y beneficios ofrecidas por cualquiera de los candidatos al igual que sus requerimientos. Éste paso, finalizará con la convocatoria a los proveedores para realizar ofertas formales que cumplan con las necesidades establecidas.

Disponibilidad de recursos: Se identificarán los recursos con los que cuenta la entidad para el proyecto de implementación del software, iniciando con el presupuesto disponible pero teniendo también en cuenta aspectos como el personal actual que se destinará en tiempo total o parcial al uso del software; la capacidad disponible del hardware para procesamiento o almacenamiento; el espacio físico destinado al hardware donde funcionará el nuevo software y al personal que lo administrará o utilizará; las redes de comunicaciones existentes y la capacidad de transmisión disponible; por último un inventario del hardware y software existente con el cual el nuevo software deberá interactuar.

Se deben determinar detalladamente los tiempos del proyecto: de cotización, de evaluación y adjudicación, de entrega (refiriéndose a la velocidad de implantación), el tiempo esperado de funcionamiento, de mantenimiento y soporte técnico. Se deben aclarar los lugares geográficos de entrega, funcionamiento del aplicativo, de almacenamiento y de retención de copias de seguridad.

Evaluación técnica: Basados en la necesidad establecida se deben identificar las características de cada uno de los candidatos identificando el cumplimiento de las funcionalidades y su nivel de importancia. También deberá analizarse la compatibilidad con los recursos disponibles de hardware y software y la integración que permite realizar

Hay que determinar la capacidad del personal disponible para instalar/configurar/administrar/utilizar el software y el tiempo que deberán destinar para esas labores para determinar los requisitos que exige cada candidato relacionado con capacitación o captación de nuevo personal.

Análisis de seguridad: Se deberá realizar un análisis de riesgos que verifique la frecuencia histórica de generación de nuevas versiones o parches a cada candidato correlacionándolas con la documentación relacionada con los reportes de vulnerabilidades (*sploits*), de fallos (*bugs*), de puertas traseras (*backdoors*) o huevos de pascua (*easter eggs*) para inferir la ventana de exposición que presenta la herramienta (tiempo que transcurre entre un reporte y la protección del usuario).

También se deberá verificar para cada candidato sus características relacionadas con el gobierno de datos: los formatos de almacenamiento, los protocolos de comunicación, la disponibilidad del código fuente y la posibilidad de ajustarlo o mejorarlo para prevenir que por obsolescencia del programa los datos queden a futuro cautivos en un formato privado que haya perdido el soporte.

Evaluación de costo total de propiedad (TCO): para cada candidato teniendo en cuenta los costes asociados con licenciamiento, renovación de licencias, adquisición de hardware, instalación, configuración, mantenimiento, soporte técnico, integración con otros sistemas de información, ajustes o mejoras y capacitación de usuarios y administradores.

Evaluación de proveedores: basándose en los criterios establecidos en los anteriores puntos se verificarán las diferencias entre las distintas propuestas, incluso de proveedores que ofrezcan la misma herramienta, haciendo especial énfasis en las capacidades que se evidencian para brindar servicios complementarios que mitiguen el costo total de propiedad.

Análisis de antecedentes: Se verificarán conceptos técnicos de expertos que hablen del software tanto del sector privado como de la academia al igual que conceptos de anteriores clientes de cada proveedor.

Selección de la herramienta: Para finalizar el proceso se realizará una verificación del mejor candidato que cumpla con la mayor cantidad de las características y funcionalidades requeridas atendiendo los requisitos de seguridad y las regulaciones sin sobrepasar los recursos disponibles (económicos, humanos, temporales, de hardware y de software). Comparando los beneficios adicionales ofrecidos, la amigabilidad de la herramienta para su instalación, administración y utilización y la disponibilidad de servicios complementarios como soporte técnico, mantenimiento, capacitación y posibilidad de modificaciones, ajustes o mejoras.

5. Aplicación de la metodología dentro del Ejército Nacional de Colombia

Para brindar un ejemplo de aplicación de la metodología aquí propuesta, se presenta el proceso de cambio de la plataforma de correo electrónico que realizó el Ejército Nacional de Colombia (EJC), pasando de utilizar Exchange a usar el software *Zimbra* con licencia del tipo FOSS.

Establecimiento de la necesidad: En el año 2018 el EJC requería optimizar la comunicación y difusión de información tanto para los funcionarios de la institución, militares y civiles, cuya cantidad es tan grande en términos de número de correos y

buzones comenzó a generar inconvenientes tanto funcionales como presupuestales para la fuerza.

Se contaba con 11.000 buzones Microsoft Exchange, que cubrían el 5% del personal militar activo y civiles de planta generando costes anuales de licenciamiento cercanos a los USD 43.000.

De acuerdo con la misión de EJC, es imprescindible manejar altos estándares de seguridad en las comunicaciones relacionadas con la defensa de la soberanía, la independencia y la integridad territorial, con la protección de la población civil y los recursos privados y estatales de tal forma que se evidencia que encargar la custodia de esta información a un ente extranjero repercute en todos los aspectos relacionados con la garantía de confidencialidad. Se estableció que la solución informática debería permitir alojarse en servidores propios en la infraestructura del EJC permitiendo que sus propios funcionarios realicen las labores de administración y protección aplicando las políticas del MDN en cuanto a seguridad informática.

EJC cuenta con una plataforma FOVID (Sistema de Gestión de Folios de Vida) que genera notificaciones con una alta periodicidad, las cuales no estaban llegando a los buzones de correo electrónico debido a la imposibilidad de interacción con MS-Exchange/Outlook.

Determinación de requisitos: De esta forma se diseñaron los requerimientos del proyecto para proveer el gestor de correo electrónico fundamentados en la necesidad para exigir una herramienta que brinde: accesibilidad, identidad del personal, imagen institucional, mejora en las comunicaciones, difusión de la información, uso en otros proyectos como FOVID, notificaciones al personal y cerrar brecha tecnológica. El tiempo de ejecución de la fase de puesta en funcionamiento de la plataforma se estableció en 6 meses.

Estudio de mercado: Se identificaron como los principales exponentes dentro de los gestores de correo electrónico, tanto libres como privados, a los siguientes: *Thunderbird, SeaMonkey, Evolution, Spike, Pimero, eM Client, Mailbird, Pegasus Mail, IONOS Hosted Microsoft Exchange, Google Workspace, Zimbra, Spark, Mailspring*.

Teniendo en cuenta que las soluciones de software libre requieren soporte técnico, que generalmente es brindado por proveedores diferentes al fabricante del software (que generalmente es una comunidad de muchos desarrolladores alrededor del mundo), se identificaron las empresas locales y extranjeras que brindan ofertas relacionadas.

Inventario de hardware: Se procedió a realizar un levantamiento de la capacidad actual de cómputo identificando los equipos disponibles para el montaje de la plataforma enumerando para cada equipo la capacidad de los procesadores y sus núcleos, la arquitectura, la capacidad en memoria RAM y de almacenamiento.

Inventario de software: Se determinó que, adicional a la interacción con el FOVID, el sistema de correo electrónico debería interactuar con el directorio activo existente. También se determinaron las licencias disponibles de sistema operativo actuales y la compatibilidad con sistemas operativos libres adecuadas para el hardware inventariado.

Análisis comparativo de las opciones: Se realizó un análisis teniendo en cuenta aspectos como el sistema operativo, la portabilidad de la versión, la seguridad de las comunicaciones, la compatibilidad, el idioma y las licencias.

Se realizó una comparación del costo total de propiedad de cada una de las plataformas identificadas durante el estudio de mercado al igual que se compararon las características relacionadas con seguridad y los costes asociados con el montaje de las salvaguardas de seguridad exigidas por las políticas de EJC.

Se verificó la frecuencia con la que se producen nuevas versiones o revisiones del software, la variedad de idiomas en que se encuentra la documentación técnica, la frecuencia con la que interactúan los usuarios en los foros de preguntas/respuestas y la cantidad de usuarios registrados en ellos.

Se determinó que los costes de capacitación para los usuarios o para el personal administrativo no era un factor relevante dado que la diferencia de costes de entrenamiento para las diferentes alternativas identificadas no tenía un impacto significativo en el costo total de implementación de la herramienta.

Se identificaron beneficios alternos de la adquisición de las herramientas, como funcionalidades adicionales incluidas dentro del mismo precio del montaje, en particular Zimbra ofrece solución para colaboración de grupos y ampliación de funciones con *Zimlets*; *Mailbird* integración con *Slack* o *Whatsapp* y una función de *Snooze*; Pegasus y *Spark* cuentan con una función de filtros programables; *Mailspring* ofrece una función de traducción y de seguimiento; Exchange incluye Outlook dentro del paquete y Google *Workspace* incluye una Suite ofimática completa.

Se identificó que para algunas de las alternativas identificadas se requería la adquisición adicional de licencias de sistemas operativos privados o que se requería de la adquisición de nuevos equipos de cómputo, por las exigencias de procesamiento de la alternativa. Algunos de estos costes de licenciamiento no correspondían a licencias perpetuas y exigían renovación anual.

Finalmente se realizó una comparación de las características ofrecidas en cuanto a gobierno de la información, teniendo en cuenta quién es el responsable de la custodia y almacenamiento de la información.

Análisis de conceptos técnicos: El análisis comparativo permitió descartar algunas de las soluciones alternativas identificadas en el estudio de mercado y aquellas preseleccionadas, se buscaron experiencias en otras entidades usuarias de estas herramientas para analizar el concepto brindado tras su implantación.

Entre los usuarios se buscaron tanto en la industria y empresa privada como en la academia y en otras fuerzas armadas que actualmente se encontraran utilizando la herramienta. Se encontró, que aparte de la propia experiencia del EJC con 11.000 buzones con Exchange-Outlook, que la Armada Nacional de Colombia utiliza 35.000 buzones con Zimbra, la Fuerza Aérea de Colombia 7.500 con Exchange-Outlook y la Policía 18.000 con Exchange-Outlook, de esta forma la retroalimentación de estas instituciones fue clave para el análisis de conceptos.

6. Conclusiones y trabajos futuros

La metodología propuesta considera el problema de adopción de una herramienta software desde una óptica holística basada en la evaluación de los riesgos para cada dimensión y etapa, lo que significa que no solo se debe enfocar en revisar las propiedades técnicas o en la evaluación económica del software, sino que se evalúa el impacto en términos del riesgo de cada dimensión para encontrar una elección más objetiva. Las dimensiones definidas y etapas de la metodología son cruciales para evaluar y mitigar los riesgos relacionados con la adopción.

Esta herramienta de gestión puede ayudar a las instituciones militares colombianas a mejorar sus procesos de contratación y toma de decisiones en las áreas de tecnologías de la información. La evaluación que realizó El Ejército Nacional de Colombia de usar *Zimbra* ayudada por esta metodología ha permitido incrementar la cobertura de número de buzones de 11000 a 50000, y optimizar recursos económicos, pues la opción seleccionada implicó una inversión de USD 1'858.000, incluyendo soporte, mantenimiento y renovación de licencias de la plataforma, frente a la alternativa COTS de USD 11'000.000 por el mismo tiempo y con el mismo número de buzones.

Consideramos que la metodología aún tiene elementos que se deben mejorar. Se debe incluir una mayor rigurosidad en el cálculo de los riesgos en las diferentes dimensiones, que por ahora es subjetiva dada por el evaluador. También se considera que automatizar este tipo de evaluación sería útil para la gestión de las áreas de tecnologías de la información de las Fuerzas y diferentes dependencias que impliquen compra de software.

Referencias

Colford, S. (2009). Explaining free and open source software. *Bulletin of the American society for Information Science and technology,*, 10-14.

Conpes 3701. (2011). Obtenido de Departamento Nacional de Planeación de Colombia: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Franch Gutiérrez, J., Susi, A., Annosi, M., Ayala Martínez, C., & P, G. (2013). Managing risk in open source software adoption. *Proceedings of the 8th International Joint Conference on Software Technologies*, 258-264.

GNU Software Foundation. (2022). Obtenido de https://www.gnu.org/licenses/licenses.html

Lerner, J., & Schankerman, M. (2010). *The comingled code: Open source and economic development (Vol. 10)*. Cambridge, MA: MIT press.

Raanan, Y. &. (2011). *Operational Risk Management: a practical approach to intelligent data analysis*. John Wiley & Sons.

Red Hat. (2022). *The State of Enterprise Open Source*.

Shaikh, M. &. (2012). Strategic drivers of open source software adoption in the public sector: Challenges and opportunities. European Conference on Information Systems.

Silic, M. &. (2016). The influence of risk factors in decision-making process for open source software adoption. . *International Journal of Information Technology & Decision Making*, 151-185.

Tu, Q. (2000). Evolution in open source software: A case study. *n Proceedings 2000 International Conference on Software Maintenance*, 131-142.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 29/10/2021
Aceitação/Acceptance: 31/01/2022

Control Ganadero: Aplicación móvil para gestionar la información de producción de leche de vaca aplicado a la granja UFPSO

María Camila Sánchez-Velasquez[1], Jesús Alberto Rodríguez-Rodríguez[1], Luis Anderson Coronel-Rojas[2], Dewar Rico-Bautista[2]

mcsanchezv@ufpso.edu.co; jarodriguezr@ufpso.edu.co; lacoronelr@ufpso.edu.co; dwricob@ufpso.edu.co

[1] Plan de estudios de ingeniería de sistemas, Universidad Francisco de Paula Santander Ocaña, Sede Algodonal Vía Acolsure, 546551, Ocaña, Colombia.

[2] Departamento Sistemas e Informática, Universidad Francisco de Paula Santander Ocaña, Sede Algodonal Vía Acolsure, 546551, Ocaña, Colombia.

Pages: 347-359

Resumen: Con la llegada de la era digital, los dispositivos móviles han tomado gran auge debido a la agilidad y practicidad con la que pueden realizar ciertos procesos y actividades. A esto se le suma la diversidad de entornos en los cuales pueden ser aplicados. Hoy en día es posible encontrar aplicaciones orientadas a diferentes campos, uno de estos es la ganadería. El control de producción de leche de vaca es una de las medidas más importantes para el mejoramiento del hato ganadero. El objetivo del desarrollo de la aplicación móvil control ganadero es sistematizar y mejorar la administración de la información de productividad lechera en la granja de la Universidad Francisco de Paula Santander Ocaña. Se hizo más eficiente el proceso de recolección de datos, análisis y la predicción de situaciones que puedan afectar al hato ganadero.

Palabras-clave: Firebase; Ganadería; IoT; Producción lechera.

Livestock Control: Mobile application to manage cow milk production information applied to the UFPSO farm

Abstract: With the advent of the digital age, mobile devices have taken a big boom due to the agility and practicality with which they can perform certain processes and activities. In addition to this, there is the diversity of environments in which they can be applied. Today it is possible to find applications oriented to different fields, one of these is livestock farming. Control of cow's milk production is one of the most important measures for the improvement of the herd. The objective of the development of the mobile application for livestock control is to systematize and improve the management of information on milk productivity on the UFPSO farm. The process of data collection, analysis and the prediction of situations that could negatively affect the cattle herd was made more efficient.

Keywords: Firebase; Livestock; IoT; Dairy production.

1. Introducción

En Colombia, el sector Ganadero es uno de los renglones más importantes en la agroindustria (Guillin, Mairon Fernando. Uron, 2016), los inicios de la ganadería tiene lugar muchos años atrás, en el periodo de la conquista, donde el ganado representaba un insumo indispensable en la alimentación, con el pasar del tiempo la cantidad de animales era tan alta, que superaba las necesidades alimentarias de la población y los animales eran sacrificados con el objetivo de aprovechar su cuero (Readings, 2011). Con el ánimo de controlar las tasas de natalidad y demás temas de la ganadería surgieron entidades como la Federación Nacional de Ganaderos (FEDEGAN), encargada de la toma de decisiones y establecimiento de políticas entre ganaderos. Desde su nacimiento, la ganadería ha tenido diversos cambios en cuanto a la identificación de cada individuo inicialmente se utilizaban marcas de hierro que se calentaban en fuego, señales que cada propietario definía para identificar a los animales de la finca, la realización de cortes en la oreja también es un método que se usa con ese fin; en la actualidad y con el avance de la tecnología la mayor parte de las fincas ganaderas están optando por el uso de dispositivos RIFD, ya que contar con un sistema de identificación favorece tanto al animal como al propietario, debido a que se puede tener a la mano información de cada animal que es de relativa importancia al momento de su comercialización, y se convierte en un mecanismo de garantía sanitaria, es necesario mantener la identificación de los animales o de los productos que se generen a lo largo de la cadena de producción, comercialización y transformación desde su origen con el fin de realizar investigaciones epidemiológicas o establecer acciones correctivas en beneficio de la comunidad consumidora (PRONAGRO, 2009).

De los productos generados por el ganado, los lácteos son sin duda los que han sido mayormente acogidos a nivel mundial, según la Organización de las Naciones Unidas para la Alimentación y la agricultura (FAO) en la mayor parte de Asia, la leche se está transformando en el principal producto de la producción ganadera, (Organizacion de las naciones unidas para la alimentacion y la agricultura, n.d.), llevando así a los Estados Unidos de América, la India y China a la escala de los mejores productores de leche a nivel mundial. El ganado vacuno aporta el 83% de la producción lechera mundial. incluidos por los editores (Jesús et al., 2013). El consumo de lácteos por habitante en los países desarrollados ha alcanzado niveles elevados debido al alto crecimiento poblacional, lo que conlleva a crear medidas que garanticen la producción de leche necesaria para cumplir con la demanda generada, en algunas partes del mundo se crean subsidios y medidas de protección que facilitan este proceso. California es el responsable del 21% del total de leche de la unión americana (Quishpe, 2016).

La granja experimental de la Universidad Francisco de Paula Santander Ocaña nace gracias al inicio del programa de zootecnia, en la actualidad existen 5 proyectos pecuarios dedicados a la producción de animales y subproductos, manejando las especies bovina, caprina, cunícola, porcina y aves de corral, donde todas las actividades se desarrollan en el marco de la bioseguridad y la bioética animal (Barrientos-Avendaño et al., 2018; Rico-Bautista, Trillos-Arenas, et al., 2019; UFPSO, 2016). El proyecto bovino está enfocado en tres aspectos fundamentales, uno de ellos es la producción de leche, en este caso se cuenta con el ganado doble propósito de las razas Gyrolando y Jersy; el segundo es

Zoogenética nativa con las razas Bon, Romosinuano y cruces, por último, está el ganado para carne con la raza Brahman Rojo (Bautista Martínez et al., 2017; Mosquera, 2017).

Se toma una línea fundamental en el campo de la ganadería como es la producción de leche, en la granja de la UFPSO se administran registros diligenciados de manera manual en un cuadernillo de apuntes, donde son registrados los datos de mayor relevancia como lo son fechas de parto, sexo de las crías, celos, fechas de destete, medicamentos utilizados, entre otros (Rico-Bautista, Barrientos-Avendaño, et al., 2019). Posteriormente a esto cada cierto periodo de tiempo se llevan a cabo reuniones para realizar la socialización de la información recolectada, algunos de esos registros son transcritos en una hoja de Excel para asegurar la información de cualquier imprevisto. Todo dato debe ser registrado, medido y si es el caso mejorado, una finca sin registros es como un barco a la deriva, hoy en día, la tecnología puede ser aplicada a los procesos para mejorar su eficiencia, en este caso la tecnología y la ganadería pueden ir de la mano para llevar datos y registros de todas las operaciones que se realizan con el fin de tener información para predecir situaciones que puedan afectar de manera negativa al productor ganadero, en muchos casos los registros manuales no son analizados a cabalidad y algunos aspectos pueden pasar desapercibidos en el momento de la toma de decisiones (Cajicalma Alvarado, 2015; Guillin, Mairon Fernando. Uron, 2016; Quishpe, 2016).

El cruce de razas para mejorar la producción de leche es una alternativa que están tomando los ganaderos, como lo dice Nestlé en su manual de buenas prácticas, se debe tener en cuenta la genética al momento de realizar cruces para generar animales (Bovinos) con características lecheras sobre todo en regiones donde las condiciones climáticas propias de climas tropicales pueden afectar la producción de leche sostenible y competitiva en el mercado (Mosquera, 2017). El resto del artículo está dividido cuatro secciones. En la sección dos se presentan los antecedentes. En la sección tres se presenta el diseño metodológico. En la sección 4 se presentan los resultados y al final las conclusiones.

2. Antecedentes

La tecnología como medio para la centralización de los datos en ámbitos ganaderos es una herramienta fundamental en el momento de la toma de decisiones, es necesario sistematizar los datos como la cantidad de leche extraída en cada ordeño, el número de ordeños por animal, fecha de destete, entre otros con el fin de estimar raciones de alimentación y en determinado caso prevenir cualquier enfermedad detectada con base a una baja producción de leche o leche con características diferentes. El uso de tecnologías de la información en el sector agro ha dado paso para que se hable hoy en día de la ganadería de precisión, que busca incrementar la eficiencia de los procesos productivos llevados a cabo en una granja (Gorandi et al., 2015), el monitoreo de las variables (Fecha de Nto, raza, información de padres, vacunas, enfermedades, fecha de destete, estado de gestación, cantidad de leche producida por 7 día o semana) permiten generar estadísticas que conllevan a tomar decisiones de manera efectiva y que traigan beneficios para el administrador o encargado del hato ganadero (Andrade & Puentes, 2015; Gorandi et al., 2015; Granobles T & Grajales Q, 2015).

A lo anterior mencionado, se le suma la trazabilidad de los individuos, proceso que debe estar presente desde el momento del nacimiento del animal o desde su adquisición, hasta

la venta del mismo, por medio de la trazabilidad, se puede establecer una hoja de vida por animal del hato, donde estarán presentes datos de gran relevancia para el administrador de la finca, como datos secundarios que analizados en conjunto contribuyen a la toma de decisiones asertivas (Granobles T & Grajales Q 2015). Existen otras herramientas que pueden ser implementadas en las granjas para mejorar su administración, identificación de potreros mediante GPS, señalización de instalaciones, establecimiento de protocolos secuenciales tanto para ordeños como para partos, identificación de la rotación de potreros, entre otros (Castillo, 2015). Por otro lado, cabe destacar que cada día se orienta más el mundo tecnológico para contribuir con el desarrollo del agro. (Andrade & Puentes, 2015)

2.1. Proceso manual

Actualmente el proceso de ordeño dentro del hato se realiza de manera mecánica, la leche es extraída mediante una máquina de ordeño, mientras sucede esto, un operario es el encargado de diligenciar las cantidades ordeñadas a cada animal, anotando la información en una hoja, posteriormente esta información es pasada a una aplicación de escritorio, proceso que se realiza cada 8-15 días, cabe destacar que en pleno auge de la tecnología, una aplicación móvil aplicada a este caso, se convertiría en una herramienta de administración para una granja, que permite aplicar la inteligencia de negocios en la ganadería, monitorear y explorar de forma dinámica los indicadores, estableciendo puntos críticos y generando alertas cuando los valores estén por debajo del mínimo aceptable, incidiendo de esta forma en la toma de decisiones certeras que contribuyan al mejoramiento y aumento de la producción lechera, además cabe destacar la disponibilidad de diferentes sensores en el mercado que hacen posible la monitorización de variables, estableciendo un análisis que es favorable para la finca (Castillo, 2015; Cuevas Reyes et al., 2013; Forero Camacho et al., 2013; Martínez-Reina, 2013).

2.2. Uso de dispositivos moviles

En los últimos años con el avance de las tecnologías, los dispositivos móviles se han convertido en una herramienta importante en la vida cotidiana, hoy en día se pueden encontrar aplicaciones móviles orientadas hacia diferentes áreas del conocimiento que brindan apoyo a diversas actividades y hacen más fácil la vida de las personas. El uso de las aplicaciones móviles ha cambiado la forma en la que las empresas laboran, se han convertido en una herramienta para aplicar estrategias de mercadeo y difusión de información, transformándose en una ventaja competitiva para quienes las usan. La aplicación móvil control ganadero está desarrollada para ser utilizada en un dispositivo móvil, bajo el sistema operativo Android (Cajicalma Alvarado, 2015).

El aumento en los sistemas de aplicaciones móviles y la alta competencia entre las empresas, atrajo un incremento en el número de proyectos de aplicaciones móviles. Estas metodologías agiles hacen parte de un grupo de procesos para la creación de software para dispositivos móviles con recursos específicos como pequeña pantalla, APIS y consumo de energía. El desarrollo de aplicaciones móviles es un gran reto debido a que son rápidamente cambiantes en relacion a los requerimientos del negocio y las necesidades técnicas de los sistemas móviles. Muchos estudios han sugerido una solución a los problemas mencionados, se ha sugerido un modelo ágil apropiado para el

desarrollo de aplicaciones móviles. La metodología ágil plantea un modelo de desarrollo a partir de iteraciones que iniciarán en cada una de las fases del ciclo de vida del desarrollo, para ello el manifiesto ágil (2001) ha sido el pilar fundamental del desarrollo ágil, basándose en sus principios:

- La mayor prioridad es satisfacer al cliente mediante la entrega confiable y continua.
- Se entrega el software funcional frecuentemente, entre dos semanas y dos meses, con preferencia al periodo de tiempo más corto posible.
- A intervalos regulares el equipo reflexiona sobre cómo ser más efectivo para a continuación ajustar y perfeccionar su comportamiento en consecuencia.
- Los métodos ágiles son más adecuados para el desarrollo de las aplicaciones móviles por las siguientes razones: Alta volatilidad de entorno, Equipos de desarrollo pequeños, Software no crítico, Ciclos de desarrollo cortos.

3. Diseño metodológico

Para este proyecto se ha definido la metodología de tipo descriptiva, la cual busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice (Hernández Sampieri et al., 1997). El objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables. Los investigadores no son simples tabuladores, sino que recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

- Población. La población objeto de estudio está conformada por los 30 trabajadores de la granja (Incluyendo a estudiantes de beca trabajo y practicantes) de la Universidad Francisco de Paula Santander Ocaña, los cuales están directamente involucrados en el proceso de producción de leche de vaca.
- Muestra. Para este proyecto se decidió el tipo de muestreo probabilístico, con el método aleatorio simple, debido a que cada miembro de la población tiene la misma probabilidad de ser seleccionado como sujeto, dando como resultado una muestra de 15 personas.
- Técnicas. La recolección de información se llevará a cabo mediante dos métodos, uno de ellos es la encuesta, que será aplicada a la muestra seleccionada, y el otro es la observación, donde se busca obtener de forma consciente y dirigida, datos que proporcionen elementos para la investigación.

4. Resultados y discusión

En la UFPSO se cuentan con alrededor de 702 m^2 de área y aparte 7.59 hectáreas destinadas para la producción del alimento, potreros y pastoreo. El grupo de Bovinos se encuentra separado de acuerdo con la funcionalidad de cada uno, el hato lechero se mantiene en una zona cercana a la zona de ordeño mientras que los animales restantes se mantienen en establos ubicados en la zona sur de la infraestructura destinada para tal

fin. Dentro del funcionamiento del hato lechero, se realiza un ordeño mecánico todos los días, dividido en dos sesiones, una en la mañana y otra en la tarde, los datos generados de ambos ordeños son diligenciados a mano en una tabla, donde se registra la cantidad de leche ordeñada en ambas sesiones, posteriormente dichos datos son pasados semanalmente en la aplicación Control Ganadero software que se utiliza actualmente para el manejo o administración de los bovinos en la granja de la Universidad.

4.1. Interfaces

Es importante diligenciar la información de la cantidad de leche extraída en cada ordeño con el fin de estimar futuras raciones de alimentación y en determinado caso prevenir cualquier enfermedad detectada con base a una baja producción de leche o leche con características diferentes, por otro lado, cabe destacar que el uso de indicadores se convierte en algo de vital importancia al momento de medir la capacidad productora de leche con otros productores de la región o a nivel nacional (Quishpe, 2016). Con el desarrollo de nuevas tecnologías de la información y la comunicación (TIC) la ganadería de precisión se ha convertido en una herramienta fundamental para incrementar la eficiencia en los procesos productivos llevados a cabo en una granja (Gorandi et al., 2015), el monitoreo de las variables (Fecha de Nacimiento, raza, información de padres, vacunas, enfermedades, fecha de destete, estado de gestación, cantidad de leche producida por día o semana) permiten generar estadísticas que conllevan a tomar decisiones de manera efectiva y certera (Chalate-Molina et al., 2010; Chalate et al., 2010; Readings, 2011).

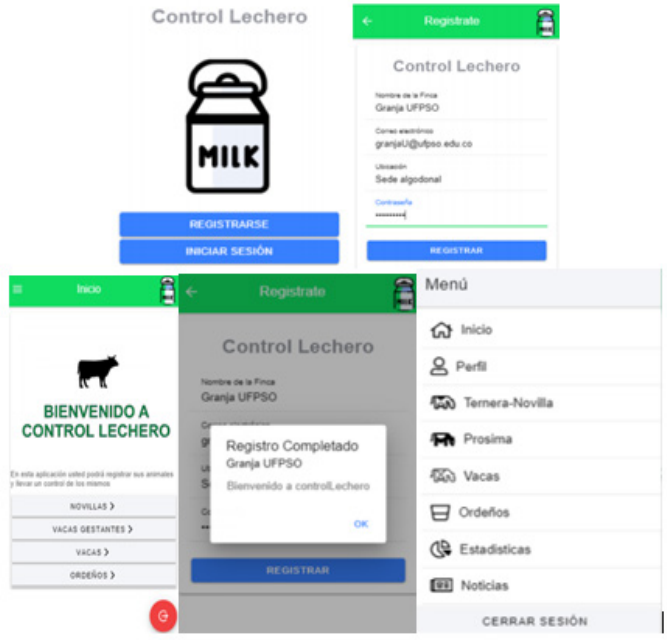


Figura 1 – Interfaces de la App Control Lechero

El control de la producción de leche es una de las medidas más importantes para el mejoramiento del ganado lechero, debido a que es la base para la selección de animales sobresalientes dentro de un hato (Grupo de animales en la ganadería). Solamente a partir de registros lecheros se está en condición de tomar decisiones adecuadas para la selección de las vacas de reemplazo y la eliminación apropiada de aquellas con vientres de baja producción. Por lo general, existen fincas destinadas a la producción de leche, en este caso se eligen razas con historias de productividad superiores, que aumenten la cantidad de leche generada por cierto periodo de tiempo, por decirlo de otra manera, estos tipos de fincas están destinadas a garantizar que la producción de leche en cierto periodo va a aumentar en lugar de disminuir. Las interfaces diseñadas para la aplicación se pueden observar en la Figura 1.

El control y la evaluación de cada vaca o grupo de vacas son importantes cuando se trata de alcanzar un alto nivel de producción de leche (pico alto y larga persistencia). La producción de leche es la variable más interesante para calcular las raciones y tipos de alimentos. Los datos se pueden usar para:

- Calcular y seguir la ingesta de nutrientes
- Controlar los cambios de producción a largo plazo
- Identificar problemas de salud generales

4.2. Prueba piloto

En la actualidad, la tecnología está presente en la cotidianidad innovando en los diferentes sectores de producción con el fin de sacar el mayor provecho, obtener beneficios y reducir las pérdidas, esto se realiza por medio de indicadores productivos y reproductivos, que buscan establecer comparaciones a niveles regionales y medir el grado o la capacidad del ganado con el que se cuenta; por otra parte es de vital importancia hacer un esfuerzo por acortar la brecha entre la ganadería y la tecnología, para lograr recolectar y analizar datos de producción, en este caso en el sector lechero de la UFPSO, es necesario contar con la hoja de vida del animal para tener un mayor conocimiento de los medicamentos aplicados y lograr predicciones en un futuro cercano.



Figura 2 – Prueba piloto

Una granja debe ser medida para poder ser administrada y qué mejor herramienta que la tecnología, las aplicaciones móviles para ganadería ayudan a mantener informados a los ganaderos y almacenar de manera práctica y sistematizada el historial de los animales de un establo. La prueba piloto de la aplicación control ganadero se realizó en la granja de la UFPSO, ver Figura 2, donde se socializó el proyecto con el encargado de la granja en el manejo del control lechero y a los estudiantes que se encontraban en el lugar. Se explicó el contenido de la aplicación, haciendo énfasis en las funciones y se dio paso a que el encargado hiciera uso de la misma, permitiendo que de esta forma se solucionaran algunas dudas que giraban en torno a su operabilidad.

4.3. Descripción de la aplicación

La identificación del animal desde el momento de su nacimiento o adquisición hasta su venta o muerte (Trazabilidad), se ha convertido en un componente fundamental, ver Figura 3a. Cuando se habla de sistemas de trazabilidad, se deben tener en cuenta variables como la identificación del animal, localización, movimientos, procesos de transformación y sacrificios, al hablar de otras razas o género del animal surgen otras variables como etapas de reproducción y fertilidad, proporcionando información al encargado sobre cuál es el momento preciso para la inseminación o reproducción del animal, lo anterior hace que el sistema a desarrollar sea una herramienta de gran ayuda para el manejo de bovinos (Destinados a producción lechera) en la granja de la UFPSO, manteniendo los registros ordenados de forma óptima, datos de forma íntegra, que permitan hacer consulta y verificación de información del animal (ganado lechero) (Arroyave Vargas, 2015; Espinosa et al., 2018).

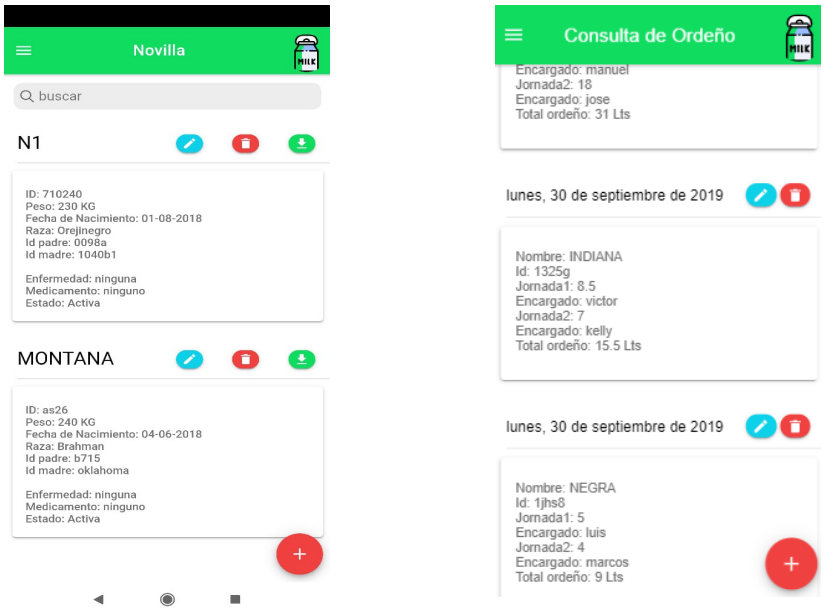


Figura 3 – a) Registro de datos en la aplicación (Novilla). b) Registro y consulta de ordeños

La sistematización y el análisis de datos se constituyen en herramientas fundamentales para la toma de decisiones en el sistema de producción, sin importar si este es agrícola o pecuario, ver Figura 3b. En ganadería bovina es esencial la identificación de los animales para hacerles seguimiento, como también la de los potreros, la señalización de las instalaciones, el establecimiento de protocolos para los diferentes procesos que se llevan a cabo (ordeño, cría, levante, ceba, rotación de potreros, grupos de producción, etc.) Por eso es preciso indicar la importancia que tienen las buenas prácticas ganaderas o lecheras en una finca, se convierten en una hoja de ruta que permite tener resultados positivos de las actividades que se realicen (Andrade & Puentes, 2015; González-Quintero et al., 2020; Morantes et al., 2020).

La interfaz inicial es la presentación de la App, donde se tienen dos opciones registrarse o iniciar sesión, el registro de la App se hace con datos básicos de la finca como nombre, correo electrónico, ubicación y contraseña; para ingresar, todos los datos son obligatorios y deben diligenciarse para poder registrarse. La aplicación móvil está pensada en aquellas fincas que se dediquen netamente a la producción lechera y es por ese motivo que se cuenta con las 3 etapas del ciclo de vida correspondientes a una vaca dedicada a la producción de leche: novillas, vacas próximas, vacas y la sección de ordeño. Cada una de estas etapas mencionadas anteriormente tiene características o datos especiales los cuales son solicitados por la App al momento de hacer un registro, es decir, en el caso de registrar una nueva novilla, la información principal está en su fecha de nacimiento y en la información de salud que esta tiene.

Si se trata de una vaca próxima, los datos principales son la fecha de preñez y la cantidad de descendientes que ha tenido; en el caso de los registros lecheros se llevan a cabo en las dos jornadas, uno al iniciar la mañana y el otro en la tarde, la persona encargada puede diligenciar estos datos de forma independiente, ya sea registrar el ordeño de la mañana tan pronto se realice la actividad o diligenciar ambos ordeños al finalizar la tarde, la aplicación hace la sumatoria diaria de la cantidad producida por cada vaca. La información de los animales registrados y la leche producida persiste en el sistema hasta que el usuario así lo requiera, en el caso de que un animal fallezca, es posible colocar en la hoja de vida del animal que ha fallecido e indicar las observaciones por las cuales falleció. Por otra parte, la aplicación móvil cuenta en su panel principal con un contador que le indica la totalidad de animales que hay registrados en el hato ganadero, haciendo diferenciación entre animales por categoría, además de esto, muestra la totalidad de leche que se ordeñó en el día. Ver Figura 5.

Para hacer más fácil el manejo de la App, la navegación también se realiza por medio del menú, que lleva al usuario a todas partes de la aplicación, pasando por la información de producción lechera, novillas, vacas próximas, cada una de ellas con la información correspondiente a su categoría, es importante indicar que se puede descargar un informe por categoría, logrando obtener un archivo PDF con la información de los animales en una categoría en específico.

En la sección de informes, el usuario tiene acceso al manual de buenas prácticas lecheras, donde están los incisos de sanidad animal, higiene en el ordeño, suministro de agua, y bienestar animal, en estadística está relacionado con dos factores principales uno de ellos es la categorización de los animales y otro es el ciclo lechero donde está la información de las vacas que actualmente se encuentran en producción de leche y los ordeños que

se han efectuado. Ver Figura 6. La sistematización de este tipo de procesos facilita el manejo de una finca, contribuye a administrarla de una mejor manera, contando la información desde cualquier lugar, inclusive si está lejos de la finca, lo que hace más fácil la toma de decisiones de manera acertada y que obtenga beneficios de las mismas.

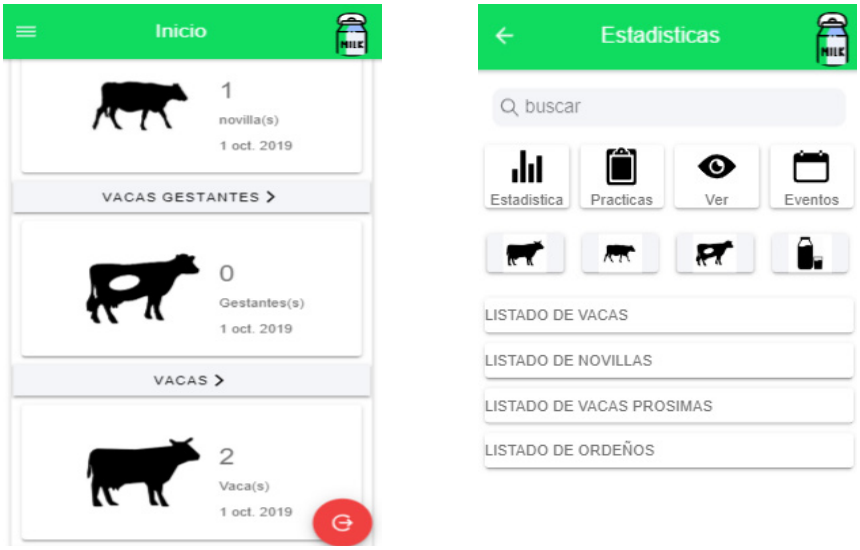


Figura 4 – a) Consultar registros guardados. b) Opciones menú estadísticas

5. Conclusiones

Con los resultados obtenidos del proyecto realizado se puede concluir lo siguiente: Al indagar al personal que labora en la granja se determinó que la mayoría utiliza dispositivos móviles, lo cual es un punto a favor para el desarrollo de la aplicación debido a que con estos dispositivos se pueden sistematizar procesos que se realizan de forma manual y agilizar procesos que son tediosos en un software de escritorio, como es el caso de la gestión de información de bovinos y producción de leche en la granja de UFPS Ocaña.

En la planificación de la investigación, se estudiaron diferentes tecnologías para el desarrollo de la aplicación móvil y se logró concluir con la elección de herramientas que facilitan el uso de una aplicación móvil en el entorno de la granja, como lo es el caso de Firebase, el cual permite almacenar en caché una copia de los datos de cloud firestore que usa la App de forma activa y volver a sincronizar los cambios locales realizados mientras no contaba con acceso a internet.

Se tomó en cuenta las sugerencias que realizaron los trabajadores y estudiantes de beca trabajo de la granja con relación al contenido que debía encontrarse en la aplicación móvil, estas sugerencias fueron analizadas y tomadas como requerimientos funcionales para la aplicación. Bajo la metodología descriptiva se logró puntualizar características

del manejo actual de información de la granja, y conocer aspectos fundamentales para el desarrollo de la aplicación.

En la fase de pruebas, se presentó la aplicación en la granja, haciendo énfasis en su estructura y las funciones que la componen, en este sentido se realizó una prueba con datos reales para estudiar la forma en la que se comporta la aplicación con datos de la vida real, por otro lado, se socializó el diseño, con el cual se estuvo de acuerdo y se realizaron los procesos 140 completos de las diferentes funciones con las que cuenta la App, la prueba piloto permitió conocer fallas y errores en torno al desarrollo.

Referencias

Alvarado, C., & Ricardo, J. (2015). *Desarrollo de una aplicacion, para dispositivos moviles que permita administrar pedidos y controlar ruta de los vendedores*. 129.

Andrade, J., & Puentes, J. (2015). Diseño e implementacion de una aplicación móvil android para la sistematizacion del estudio, la prevención y el control de enfermedades en los cultivos de algodón como herramienta de apoyo para el aprendizaje de los estudiantes del programa ingenieria. *Biblioteca Digital Universidad de Cordoba*, 173.

Arroyave Vargas, M. (2019). La legibilidad y la comunicación visual de las etiquetas con los adultos mayores en Buenos Aires (2015). *Cuadernos Del Centro de Estudios de Diseño y Comunicación*. https://doi.org/10.18682/cdc.vi65.1185

Barrientos-Avendaño, E., Rico-Bautista, D., Coronel-Rojas, L., & Cuesta-Quintero, F. (2018). Granja inteligente: Definición de infraestructura basada en internet de las cosas, IpV6 y redes definidas por software. *Revista Ibérica de Sistemas e Tecnologias de Informação*.

Bautista Martínez, Y., Herrera-Haro, J. G., Espinosa García, J. A., Martínez Castañeda, F. E., Vaquera Huerta, H., Bárcena Gamma, J. R., & Morales, A. (2017). Relación entre las prácticas tecnológicas de manejo, la producción y su asociación con las épocas del año en el sistema de doble propósito del trópico mexicano. *Nova Scientia*. https://doi.org/10.21640/ns.v9i19.986

Castillo, M. J. (2014). Análisis de la Productividad y Competitividad de la Ganadería de Carne en el Litoral Ecuatoriano (Resultados de Consultoría para RIMISP – Parte I). *Serie Documentos de Trabajo Nº 144. Grupo de Trabajo: Desarrollo Con Cohesión Territorial. Programa: Impactos a Gran Escala.*, 71.

Chalate-Molina, H., Gallardo-López, F., Pérez-Hernández, P., Lang-Ovalle, F. P., Ortega-Jiménez, E., & Vilaboa Arroniz, J. (2010). Caracteristicas del sistema de producción bovinos de doble propósito en el estado de Morelos, México Characteristics of the dual purpose cattle production system in Morelos, Mexico. In *Zootecnia Trop*.

Chalate, H., Gallardo, F., Pérez, P., Lang, F. P., Ortega, E., & Vilaboa, J. (2010). Caracteristicas del sistema de producción bovinos de doble propósito en el estado de Morelos, México. In *Zootecnia Tropical*.

Cuevas Reyes, V., Baca del Moral, J., Cervantes Escoto, F., Espinosa García, J. A., Aguilar Ávila, J., & Loaiza Meza, A. (2013). Factores que determinan el uso de innovaciones tecnológicas en la ganadería de doble propósito en Sinaloa, Mexico. *Revista Mexicana de Ciencias Pecuarias*.

Espinosa, J., Vélez, A., Góngora, S., Cuevas, V., Gómez, R., & Rivera, J. (2018). Evaluación del Impacto en la productividad y rentabilidad de la tecnología transferida al sistema de bovinos de doble propósito del trópico mexicano. *Tropical and Subtropical Agroecosystems*.

Forero Camacho, C. A., Rojas Carvajal, G. H., & Argüelles-Cárdenas, J. H. (2013). Capital social y capital financiero en la adopción de tecnologías ganaderas en zonas rurales altoandinas de Colombia. *Corpoica Ciencia y Tecnología Agropecuaria*. https://doi.org/10.21930/rcta.vol14_num2_art:405

González-Quintero, R., Sánchez-Pinzón, M. S., Bolívar-Vergara, D. M., Chirinda, N., Arango, J., Pantévez, H. A., Correa-Londoño, G., & Barahona-Rosales, R. (2020). Caracterización técnica y ambiental de fincas de cría con doble utilización de la vaca, pertenecientes a muy pequeños, pequeños, medianos y grandes productores. *Revista Mexicana de Ciencias Pecuarias*. https://doi.org/10.22319/rmcp.v11i1.4902

Gorandi, E., Moltoni, A., & Clemares, N. (2015). *Collar con tecnología GPS para monitoreo animal*. 1–8.

Guillin, Mairon Fernando. Uron, C. A. (2016). Manejo en el levante de los cruces F1 de ganado criollo romosinuani y costeño con cuernos en la parcela la Troya de la UFPSO. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (1997). *Metodología dela investigación*.

Jesús, P., Celia, C., Juan, Z., & Víctor, B. (2013). Manejo de ganado lechero. *Inifap*, *1*, 42.

Martínez-Reina, A. M. (2013). Caracterización socioeconómica de los sistemas de producción de la región de La Mojana en el Caribe de Colombia. *Corpoica Ciencia y Tecnología Agropecuaria*. https://doi.org/10.21930/rcta.vol14_num2_art:406

Morantes, M., Dios-Palomares, R., Urdaneta, F., Rivas, J., & García-Martínez, A. (2020). Eficiencia técnica en sistemas de producción con bovinos de doble propósito. *Archivos de Zootecnia*. https://doi.org/10.21071/az.v69i266.5114

Mosquera, J. (2017). *MANUAL DE BUENAS PRACTICAS LECHERAS - NESTLE*.

Organizacion de las naciones unidas para la alimentacion y la agricultura. (n.d.). *FAO*.

PRONAGRO. (2009). Manual de buenas prácticas en explotaciones ganaderas de carne bovina. In *Instituto Interamericano de Cooperación para la Agricultura y Secretaría de Agricultura Ganadería, Tegucigalpa, Honduras*.

Quishpe, V. (2016). Propuesta de mejora en el control del proceso productivo para la asociación de productores de leche del cantón Cayambe. caso. CAMPINORTE. *Propuesta de Mejora En El Control Del Proceso Productivo Para La Asociación de Productores de Leche Del Cantón Cayambe. Caso. CAMPINORTE.*

Readings, F. (2011). *Ganaderia y empresarios ganaderos en la araucania 1900*. *2*(2006), 530–537.

Rico-Bautista, D., Barrientos-Avendaño, E., Cuesta-Quintero, F. R., Coronel-Rojas, L. A., Trillos-Arenas, J., & Hernadez-Villamizar, D. (2019). Mobile application for the optimization of milk production and goat feeding processes: Experimental farm of Universidad Francisco de Paula Santander, Ocaña, Colombia. *Journal of Physics: Conference Series*, *1388*, 012028. https://doi.org/10.1088/1742-6596/1388/1/012028

Rico-Bautista, D., Trillos-Arenas, J., Hernández-Villamizar, D. A., Barrientos-Avendaño, E., Coronel-Rojas, L., & Cuesta-Quintero, F. (2019). Management of Caprine Animals in the University Francisco de Paula Santander Ocaña: Case of application of technology. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2018*(E23), 94–106.

T, J. C. G., & Q, A. G. (2015). Plan De Desarrollo De La Ganadería Del Quindío, a Partir Del Enfoque De Sistemas De Producción. *Luna Azul*, *40*, 170–194. https://doi.org/10.17151/luaz.2015.40.12

UFPSO. (2016). *Granja Experimental*.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 11/12/2021
Aceitação/Acceptance: 09/02/2022

Nuevas tecnologías militares en el ámbito aéreo y espacial: Tendencias y cambios en el Derecho Internacional

Zully Ximena Rojas Ortiz[1], Paula Alejandra Prieto Ararat[2]

zully.rojas@epfac.edu.co; paula.prieto@epfac.edu.co

[1] Escuela de Postgrados Fuerza Aérea Colombiana, Carrera 11 No. 102-50, 110111, Bogotá, Colombia.

[2] Escuela de Postgrados Fuerza Aérea Colombiana, Carrera 11 No. 102-50, 110111, Bogotá, Colombia.

Pages: 360-373

Resumen: El presente artículo tiene como objetivo identificar los aportes al Derecho Internacional generados a partir de las tendencias en el uso de nuevas tecnologías militares en el ámbito aéreo y espacial, por medio de una revisión documental sobre nuevas tecnologías militares en los últimos diez años. Para así, dar respuesta a la pregunta: ¿cuáles son los posibles cambios al Derecho Internacional generados a partir de las tendencias en el uso de nuevas tecnologías militares en el ámbito aéreo y espacial?, por medio de la identificación de tendencias en las dimensiones de normatividad, estrategia, ética militar y poder aéreo.

Palabras clave: Tecnologías; Militar; Derecho; Ética; Nuevas Guerras.

New military technologies in the air and space field: Trends and changes in International Law

Abstract: This article aims to identify the contributions to International Law generated from trends in the use of new military technologies in the air and space field, through a documentary review of new military technologies in the last ten years. In order to answers the following question: what are the possible contributions to International Law generated by trends in the use of new military technologies in the air and space field? Through the identification of trends in the dimensions of regulations, strategy, military ethics and air power.

Keywords: Technologies; Military; Law; Ethics, New Wars.

1. Introducción

Son diferentes y necesarios, los beneficios que ofrece la tecnología basada en sistemas de Inteligencia Artificial; es así como diferentes sectores tanto público como privado, han tenido cambios significativos en sus procesos haciéndolos más eficientes con un riesgo que puede ser considerado muy bajo prácticamente nulo. Sin embargo, su acelerado desarrollo e implementación, ha generado diversas inquietudes a nivel social,

económico, jurídico, donde, es importante dirigir la mirada a garantizar la protección de derechos. Es así que el uso de Nuevas Tecnologías en el ámbito militar ha suscitado el debate en su aplicación.

La Fuerza Aérea Colombiana tiene una importante experiencia en el respeto y observancia de las reglas de Derecho Internacional Humanitario, mediante la asistencia de la figura de Asesores Jurídicos Operaciones [ASEJO], en el marco del conflicto, sin embargo, aún no es totalmente certero si la normatividad existente con relación a armas convencionales es suficiente y aplicable al uso de Nuevas Tecnologías Militares.

Ante dicha incertidumbre, se desarrolla este estudio, donde se hace una revisión documental que ha permitido identificar las diferentes posturas que ante el tema se han generado, de igual forma, destacar las tendencias que van teniendo una incidencia importante en el Derecho Internacional.

2. Transformación de la Guerra a la luz de la implementación de IA

Bados y Duran (2015), hacen un análisis de algunas variables que han influido en el rumbo de los conflictos, haciendo una clara distinción de los del pasado con respecto a los contemporáneos, dando origen a lo que se ha denominado las Nuevas Guerras, de acuerdo con lo propuesto y adoptado por Mary Kaldor en 2001. Así se destacan: actores, causas, métodos y estrategias empleadas y formas de financiación; y a los cuales, se adicionan otras tres categorías propuestas por los autores, que se denominarán emergencias complejas, marco geográfico y marco legítimo- legal de la violencia.

Entre las causas se destaca la globalización, "como una consecuencia de la revolución en las tecnologías de la información y también de las drásticas mejoras en la comunicación y el tratamiento de datos" (p. 13); y aquí, es importante entender que la implementación de tecnología además de masificar las redes globales, trascender fronteras, acortar distancias, ha influido en la eficacia y eficiencia en el uso de medios y métodos, configurándose así en un factor crítico y determinante en el marco de los conflictos. Esto, teniendo en cuenta, que el uso e implementación de Inteligencia Artificial [IA], hace viable pensar en guerras a distancia más abstractas, lo que se traduce en un aumento en las acciones militares y a una escala posiblemente incontrolada de los conflictos (Delàs et al, 2018).

De esta manera, las Fuerzas Militares [FFMM], han tenido que ir a la vanguardia de la tecnología, adoptando sistemas que le permitan ser más competentes potencializando sus capacidades, todo ello que conlleva a cumplir su misión tanto institucional como constitucional, por esto mismo, se han visto en la necesidad de incorporar sistemas con Inteligencia Artificial, no obstante, el alcance real todavía es incierto, lo que genera incertidumbre porque se desconoce las consecuencias nocivas. Y aunque, "con estos nuevos medios se adquiere una visión general del teatro de operaciones bélicas gracias a la reducción de la incertidumbre que posibilita la digitalización de la realidad" (García, 2016, p. 269), para Delàs et al, (2018), "las acciones militares y de seguridad con sistemas militares robóticos y drones armados han cambiado radicalmente los escenarios de guerra, que han pasado de concentrarse en objetivos militares y estratégicos a ataques que pueden afectar gravemente la población civil no involucrada".

Esta denominada revolución en asuntos militares, de acuerdo a García (2016), sostenida principalmente sobre tres pilares: tecnológicos, sensores, sistemas de comunicación y armamento, ponen en evidencia la transformación de los conflictos armados por la misma incorporación de las tecnología, al igual que el desarrollo de formas más descentralizadas de organización militar en una sociedad interconectada.

3. Una mirada del Derecho Internacional, con ocasión del uso de las Tecnologías Militares

En los últimos tiempos se ha evidenciado un aumento apresurado y masivo, en el uso de tecnología concerniente a la IA, para dar respuestas a las diferentes necesidades que se han suscitado en el mundo actual. Sin embargo, tanto el desarrollo como la implementación acelerada de estos sistemas, puso en debate, la necesidad de regular este tema, con el propósito de proteger derechos y de evitar daños innecesarios, lo que hasta ahora no han sido evidente, así, mientras que la IA se impulsa cada vez más y va tomando significativos espacios, el tema de regulación para la protección y limitación va más lento; y es que es importante anotar, que no es viable quedarse rezagado al margen de la implementación de Nuevas Tecnología en el ámbito militar, cuando muy posiblemente los "enemigos", si lo hacen. Sin embargo, la discusión se dirige a observar que posibles cambios se están generando en el Derecho.

Así, con los vacíos que se van abriendo en el Derecho Internacional, con ocasión de la incorporación de nuevos sistemas militares autónomos, surge la incertidumbre si lo ya reglado en materia a uso de armas convencionales es suficiente o si se está en un escenario de soft law, donde, no hay claridad de lo permitido y lo no, de acuerdo a Barberis citado por Del Toro, en el Anuario Mexicano de Derecho Internacional Volumen VI, al referirse así a la manera injustificada a las normas que se encuentran en proceso de consolidación y que la doctrina distingue ya con la referencias a la lex lata y lex ferenda.

Se hace necesario, hacer distinción entre hard law y soft law, que de ninguna manera está relacionada con un grado de obligatoriedad establecido por la norma jurídica sino más bien, por la difícil que resulta de comprobar su incumplimiento en una mayor o menor medida. De esta manera, soft law no es totalmente claro, atendiendo a que las normas son obligatorias y las consecuencias jurídicas de su incumplimiento no han de cambiar. Por ello, "la idea de un derecho "blando" no aparece como razonable, siendo el soft law un producto de intereses políticos que buscan otorgar obligatoriedad a ciertos actos y ciertas resoluciones para satisfacer sus propios intereses" (Del Toro,).

Sin embargo, es de mencionar que para este mismo autor, en el derecho internacional los efectos de las diferentes normas y demás instrumentos internacionales son susceptibles de considerarse en una escala que va de lo soft a lo hard, donde la gradación del nivel de obligatoriedad responde tanto a conveniencias políticas como a la búsqueda de una mejor solución a determinada cuestión. No obstante, no todos los problemas se enmarca en una solución jurídica de tipo hard law, por el contrario, en ocasiones instrumentos no vinculantes ofrecen soluciones sean asertivas, sea porque generan consenso de la comunidad internacional, por llenar algún vacío constituyendo criterios de interpretación o por ser la única vía de acuerdo viable.

En un discurso pronunciado por el presidente Obama en el año 2013, en la Universidad Nacional de Defensa, exponía que "la contrainsurgencia y la lucha antiterrorista a través de asesinatos selectivos por drones empiezan a explicarse como una rutina legalizada y normalizada". Lo que abrió la discusión en la responsabilidad en materia de la guerra, con ocasión del uso de drones para los servicios de inteligencia en las Fuerzas Armadas (Kleinschmidt, 2015).

Para Kleinschmid, "los asesinatos selectivos por aviones no tripulados hoy son vistos como eficaces y de bajo riesgo, en comparación con las operaciones militares convencionales" (2015, p. 12). Esa aparente economía, tiende a desdibujar la responsabilidad de los actores en el uso de estas tecnologías, donde, "tanto la extensión como la aceptación ética de daños colaterales siguen siendo controversiales. Pero mientras ese tema domina el debate público y académico, la eficacia de las operaciones de aviones no tripulados para romper las redes terroristas se considera comparativamente asegurada" (Kleinschmidt, 2015, p. 12).

Villamizar (2015), argumenta que por un lado el régimen jurídico positivo de la Guerra Aérea es débil o inexistente, por otro, los adelantos tecnológicos hacen obsoleta buena parte de lo regulado en las reglas de la Guerra Aérea, especialmente cuando se trata de la operación de aeronaves no tripuladas, lo que pone en debate si el Derecho positivo es inexistente u obsoleto, si hay una costumbre internacional en materia de Derecho de la Guerra Aérea que pueda aplicarse a estas para limitar el uso indiscriminado en caso de bombardeo.

Algunos autores han tratado de abordar el tema. Renato Niño (1998) citado por Villamizar (2015), sostiene que: con anterioridad a la segunda guerra mundial las reglas de la guerra aérea, fueron consideradas como una reafirmación del derecho consuetudinario sobre la materia, y aún cuando sus términos se encuentran hoy en día tecnológicamente algo atrasados, se puede decir que todavía se les otorga importancia. P 94

Para Bermejo y Cocchini (2020), los drones son armas cuya legalidad internacional hoy en día está fuera de toda duda, los reproches más intensos que se les ha hecho tienen que ver sobre todo desde la perspectiva del Derecho internacional humanitario, es decir, en caso de conflicto armado. Esto se debe especialmente a que han sido armas utilizadas no sólo entre Estados, como fue el caso en Irak, sino también contra ciertos grupos armados o actores no estatales de difícil calificación, pero cuya característica principal era el de estar armados. (2020, p. 3). Así, la propuesta es que el "Derecho internacional humanitario reconozca una nueva categoría de conflicto armado que pudiera tomar en consideración estos aspectos transnacionales, como se hace en otros sectores internacionales, como es el Derecho internacional económico" (2020, p. 20).

Así las cosas, si bien las reglas de la Guerra Aérea en el Derecho positivo no son suficientes, algunos preceptos se han considerado como estatuto habilitante para la conformación de costumbre internacional, en cuanto a lo que se refiere al

bombardeo, y por tanto se considera una restricción a la idea de una guerra basada en drones que no tenga regulación jurídica alguna en materia internacional (Villamizar 2015).

Así, pese a los vacíos que pueden darse en el Derecho de la Guerra Aérea, ahondados hoy en día por la implementación de tecnología, hay un importante acercamiento en la doctrina que ha tratado el tema del empleo de drones y el DIH, donde se ha hecho una equivalencia, en el sentido que son plenamente aplicables a la operación con estas armas, los principios de proporcionalidad, protección de civiles, responsabilidad de la cadena de mando y que en general el DIH (Casey-Maslen, 2012; Gallais, 2013).

Puntualmente en el caso de la Ciberguerra, sucesos como los ciberataques a la infraestructura crítica tecnoinformacional en Estonia en 2003 han creado la necesidad de analizar la normatividad como es el caso del "Tallinn Manual on the International Law Applicable to Cyber Warfare", conocido también como "Manual de Tallin" el cual es una guía desarrollada a petición del Centro de Excelencia en la Defensa Cooperativa Cibernética de la OTAN y tuvo la participación de alrededor de 20 expertos en la materia.

Dicho manual toma normas vigentes y las adapta a las diferentes situaciones que se puedan presentar en el ciberespacio; para Fonseca et al (2014), esta guía muestra lo flexibles que pueden ser las leyes de la guerra para aceptar este tipo de nuevos conflictos y también aclarar zonas grises. Por ejemplo, los ciberataques llevados a cabo fuera de un contexto de acciones militares son inmediatamente considerados acciones en contra de la ley y por ende llevar al que ejecuta dichas maniobras ante ámbitos penales dependiendo de la gravedad de las consecuencias de dicho ataque.

4. Desarrollo de la Tecnologia Militar

Burmaoglu y Sarıtas (2016), hablan de cómo a través de la historia, la tecnología militar cambio mucho más rápido que la organización y la doctrina militar antes de la primera guerra mundial. En este periodo las tecnologías más importantes fueron la logística, la comunicación y el transporte debido a la creciente movilidad. Ya para la segunda guerra mundial, y durante la guerra fría, se dio prioridad a la innovación tecnológica basada en la ciencia.

Así como hubo una revolución en los asuntos militares, también se observan cambios fundamentales en los contextos externos de la guerra, incluidas las sociedades, las tecnologías, la economía, el medio ambiente, la política y cultura.

De acuerdo con Clausewitz citado por Moliner (2019), se tiene que, en sí, la esencia de la guerra, aun con el paso del tiempo conserva su naturaleza con sus dos elementos fundamentales el objetivo dado por el carácter social dirigido por el carácter político; y el subjetivo que está relacionado con la violencia que se funda desde la propia conciencia humana.

El uso cada vez mayor de las Tecnologías de la Información y la Comunicación en la vida cotidiana también ha influenciado el poder militar, el cual pasa de centrarse del uso de la fuerza al uso de la información y por ende genera un cambio en la naturaleza de las operaciones militares. Es así como para Burmaoglu y Sarıtas (2016), existen cambios impulsados tanto por los conceptos y por la tecnología, y que tienen incidencia en la I+D, militar específicamente en el campo de batalla, ya que se está volviendo en gran medida virtual. Ello genera una mayor proximidad a los civiles y la sociedad, hay

menos tolerancia por las pérdidas de vidas humanas, y operaciones más anticipatorias y preventivas con el objetivo de desactivar en lugar de derrotar.

El escenario impulsado por la tecnología enfatiza las características comunes de los futuros equipos militares mejorados por las TIC, los sensores y los sistemas satelitales, fuentes alternativas de energía para operaciones continuas, y habilidades y capacidad de análisis de big data.

Para Gill y Gill (2019), el auge de las comunicaciones y tecnología ha hecho pensar que es posible que se produzca otra revolución en los asuntos militares y que los países en vía de desarrollo puedan alcanzar más rápidamente los avances de las potencias mundiales. Sin embargo, el análisis de los autores prueba lo contrario, ya que las nuevas tecnologías de información y producción permiten cálculos mucho más complicados y, al mismo tiempo, permiten un mayor nivel de precisión en la fabricación, lo cual conlleva a un número interminable de incompatibilidades y vulnerabilidades de los artefactos desarrollados entre distintos Estados.

Por ahora en el panorama internacional, con el protagonismo de China y los avances de Rusia en la geopolítica, los autores ven como la competencia militar □ tecnológica será clave en el centro de la política internacional, pero la brecha de las potencias frente a los países menos desarrollados será cada vez más amplia.

De igual manera Velázquez (2012) sostiene, que el "derecho influye directamente en las relaciones científicas y tecnológicas al regularlas y enlazarlas, siendo de nueva cuenta el ejemplo más palpable de esta situación el derecho del espacio ultraterrestre, donde los juristas y los internacionalistas se anticiparon en buena medida al promover la elaboración y aplicación de normas al ámbito cósmico□.

No obstante, es importante hacer una diferenciación, de los Sistema Autónomo de Armas Letales [SAAL], de acuerdo con lo que expone Meza (2022), quien aduce que el criterio para ello se puede clasificar en tres categorías según el grado de:

1. Intervención humana
2. Autonomía que tenga el sistema
3. Funciones que tenga el sistema

Con respecto al primer criterio, son cuatro prefijos que se han de tener en consideración, para determinar el grado de intervención del componente humano en la selección tanto del blanco como de la escogencia de forma del ataque, a saber, son:

IN: Dentro del sistema. Son aquellos sistemas que permiten que sea el ser humano, quien seleccione el blanco y la forma como se desarrolla bien sea el ataque o la entrega de armamento.

ON: Con respecto al sistema. Es el sistema quien propone el blanco y la forma de ataque, y el ser humano hace la escogencia y desarrolla la supervisión

OUT: Fuera del sistema. El sistema escoge el blanco y la forma de ataque, el ser humano puede reversar o detener la acción que está desarrollando el sistema, es lo que se ha denominado activación del boto rojo.

El cuarto no se ha desarrollado y existe conceso a nivel internacional de prohibición de tipo de armas donde el ser humano pierda control sobre el sistema.

Con respecto al segundo criterio, es decir, el grado de autonomía del arma, está relacionado con la complejidad el sistema, donde lo determinante es la integración de los datos y los complejos algoritmos que coloca el programador dentro del sistema.

El tercer criterio está relacionado con la función propia del sistema, cuando el arma tiene la capacidad o no de buscar y detectar el blanco, de igual forma, la misma arma tiene dentro de su sistema la capacidad para efectuar la neutralización.

5. Poder aéreo, nuevos retos

Partiendo, que el ciberespacio constituye un nuevo dominio sobre el que los Estados se están aventurando y explorando a pasos agigantados impulsados por el incesante avance tecnológico. La rapidez con la que cambian las tecnologías de la información provoca desafíos constantes que deben ser resueltos por la comunidad internacional a los fines de encontrar el mejor modo de regular este espacio (Llorens, 2016).

Desde la perspectiva de las tecnologías que están aplicándose y generalizándose en las Fuerzas Militares, puede afirmarse que existe una revolución en los quehaceres militares en marcha. Sin embargo, puede considerarse que el verdadero impacto revolucionario de esta nueva Revolución en los Asuntos Militares RAM no reside sólo en la importancia del terreno operativo y tecnológico, sino que va más allá, y es precisamente en su dimensión social, en la imagen que las sociedades se hacen de la guerra, de sus fuerzas armadas y de su utilidad.

Dentro de las innovaciones que reportan los ejércitos del mundo se encuentra la categoría de información, en la que países como Colombia trabajan en soluciones de imágenes de multimisión por medio de cámaras de cuadro térmico que proporcionan a los sistemas de vigilancia multisensores infrarrojos con el fin de mejorar la búsqueda y rescate, reconocimiento e identificación de objetivos, vehículos aéreos no tripulados y protección de la fuerza, así como para apoyar misiones antinarcóticos y antinsurgentes (Comando General de las Fuerzas Militares de Colombia, 2019).

Adicionalmente, los nuevos sistemas van a aportar un sinnúmero de ventajas, pero a la vez plantean nuevas cuestiones problemáticas. Una de éstas, clave en este sentido, es la interoperabilidad entre los sistemas, es decir, la capacidad para transmitir y recibir información entre los mismos. El creciente empleo de fuerzas multinacionales y la ejecución de operaciones conjuntas requieren la integración de sistemas de origen bien diferenciado.

Pues es de saberse, que de acuerdo con Gómez (2015), "los ataques basados en imprecisos patrones de comportamiento y no en la participación directa en las hostilidades o en la condición de miembro de un grupo armado, no sólo constituyen una brecha en la línea de flotación del principio de distinción, sino que quedan muy lejos "de las precauciones y presunciones que se deben aplicar en caso de duda. Asunto, que abre la discusión de adónde se debe dirigir la mirada con el uso de estas nuevas tecnologías que no permite conocer su alcance.

Es de precisar, que los Sistemas Militares de Inteligencia, donde, el Táctico, han sufrido el impacto de dos nuevas realidades, evidentes: la globalización y las nuevas tecnologías. Esto, teniendo en cuenta que los sistemas han evolucionado para adaptarse a las nuevas realidades, generando cambios en la institución, los procedimientos e incluso las doctrinas de empleo (Sainz, 2012).

6. Ética militar en el marco de la Nuevas Tecnologías Militares

La discusión ética se ha venido apartando un poco de lo estrictamente militar e indaga sobre otros posibles usos de las tecnologías militares en otros ámbitos, puntualmente Enemark (2021) habla si la policía debe usar drones armados y de qué forma. Para ello aplica algunos de los principios éticos establecidos sobre el uso de la fuerza por parte de la policía (necesidad, proporcionalidad y precaución) y explora algunos de los desafíos a los que probablemente se enfrentará un oficial de policía "telepresente" que utiliza drones al tratar de adherirse a ellos a estos principios.

El interés del análisis ético también ha venido tomando espacios en la guerra de la información y en el dominio cibernético, así para Lucas (2015) citado por Álvarez (2021), las primera normas y restricciones sobre el comportamiento aceptable durante la ciberguerra fueron llevadas a cabo por personas no especializadas en este campo, pero que consideran la teoría de la guerra justa debía ser extendida a este nuevo dominio (p. 106).

Otro costo político que reduce es la difícil identificación del agresor, sobre todo en el caso de la guerra cibernética, donde el Estado o actor que lo ejecute no puede ser identificado inmediatamente. Sin embargo, al reducir estos costos también puede hacer que los tomadores de decisiones estén más dispuestos a ir a la guerra, es aquí donde el uso de nuevas tecnologías empieza a representar un problema. Un ejemplo

de esto es el tema de las intervenciones humanitarias, ya que, si se reduce el riesgo de incurrir en estas, es más fácil que se tome la decisión de llevarlas a cabo, lo que podría desatar que algunos Estados decidan participar en guerras agresivas disfrazadas de intervención humanitaria.

Lucas (2014), propone que la discusión ética sobre las nuevas tecnologías militares no se limite a afirmar que las normas actuales son obsoletas para dichos avances militares, sino más bien debe analizarse desde como podrían llenarse esos vacíos éticos y normativos que traen consigo estos avances.

Desde el principio de legalidad de la misión, Lucas (2014) tomando perspectivas de otros análisis como el realizado por Wallach (2013), concluye que si dicha misión se ha considerado legalmente permisible y moralmente justificable por todos los demás motivos pertinentes no pierde este estatus únicamente sobre la base de una modificación o cambio en los medios tecnológicos utilizados para llevarla a cabo. Si se reemplaza al piloto por un software, esto no implica un cambio en la legalidad de la misión a menos que la tecnología en cuestión represente o emplee armas o métodos que ya estén específicamente prohibidos bajo las Convenciones de Armas internacionales existentes, o en violación de las prohibiciones en el derecho internacional humanitario.

En el caso del principio de riesgo innecesario, no hay mayores cambios respecto al uso de armas tradicionales, ya que se sigue contemplando el mínimo riesgo para los agentes que realicen actividades en la guerra. Por otro lado, en el principio de asimetría moral con los adversarios, las fuerzas no deben ningún tipo de obligación dada la asimetría en términos tecnológicos con el adversario, ya que, sin importar el tipo de grupo ilegal, todos están violando alguno de los principios legales del Estado donde actúan.

Puntualmente en el uso de artefactos como los sistemas no tripulados, estos satisfacen los requisitos del derecho internacional y la moralidad relacionados con los conflictos armados o la aplicación de la ley siempre y cuando se demuestre que operen de manera similar a los agentes humanos en circunstancias similares, incluso Lucas (2013), argumenta que el uso de un artefacto de este tipo no es solo legalmente permisible, sino moralmente necesario, siempre que su desempeño prometa tanto un riesgo reducido para los agentes humanos.

Coleman (2021), aborda los retos éticos que traen consigo las nuevas tecnologías militares. Tradicionalmente se considera que la teoría de la guerra justa tiene dos aspectos: jus ad bellum (justicia de la guerra), la cual aborda cuándo es correcto recurrir a la guerra en lugar de intentar resolver una disputa por otros medios, y jus in bello (justicia en la guerra) que se ocupa de la conducta de quienes están peleando la guerra, ya sean soldados, marineros, aviadores, o civiles que hayan decidido tomar las armas.

El jus ad bellum, por un lado, consta de seis condiciones que deben cumplirse antes de que un estado esté éticamente justificado para ir a la guerra:

1. Debe haber una causa justa para ir a la guerra
2. Aquellos que decidan ir a la guerra deben hacerlo con las intenciones apropiadas
3. La guerra debe usarse como último recurso
4. La guerra debe ser declarada públicamente y autorizada por una autoridad correspondiente
5. Debe haber una probabilidad razonable de éxito en la guerra
6. El costo total de la guerra, no solo el costo financiero sino el daño involucrado, debe ser proporcional al beneficio que se obtendrá al ir a la guerra.

En concordancia, para Pérez (2017), en el escenario de la guerra y en el marco de la guerra, el ius ad bellum, es considerado como el "elemento del Derecho Internacional que se preocupa por establecer las condiciones en que les es lícito a los Estados recurrir a la fuerza armada" (p.30). Es el fundamento que los habilita para entrar al escenario de la guerra.

Para Coleman (2021), desde la perspectiva del jus ad bellum las nuevas tecnologías militares reducen los costos políticos de recurrir a la guerra sobre todo en términos de reducción de bajas en combate. Los sistemas de armas controlados a distancia como los vehículos aéreos no tripulados (drones), vehículos terrestres, barcos y submarinos controlados a distancia permiten exponer al operador al menor peligro posible. Todo ello conduciendo a la necesidad inminente de justificar el uso de la fuerza, que además de soportase en un marco jurídico debe encontrar fundamento en el campo ético.

Por otro lado, el jus in bello consta de dos principios fundamentales por los cuales los participantes en la guerra la guerra debe tolerar: la discriminación y proporcionalidad.

Dado lo anterior, el autor explica como de los principios de jus ad bellum, solo dos están completamente contemplados por el derecho internacional, los cuales son la causa justa y la declaración de esta por una autoridad correspondiente, mientras que las dos condiciones del jus ad bellum son completamente cobijadas por el derecho internacional.

En cuanto al jus in bello, también cambia el principio de discriminación, puesto que con el uso de armas tradicionales se tiene claro que no se puede atacar deliberadamente a los no combatientes, mientras que con las nuevas tecnologías militares se puede argumentar que se puede atacar a civiles no combatientes con armas no letales como las cibernéticas para alcanzar cierto objetivo y esto no lo haría una mala práctica si se compara con el uso de armas tradicionales letales, por ejemplo.

En este contexto, las nuevas tecnologías militares plantean cuestiones éticas, sobre todo en el caso del jus ad bellum. Lo anterior no quiere decir necesariamente que las nuevas tecnologías sean como tal éticamente problemáticas, pero si podría hacer que los Estados prioricen su uso y resultados por encima de otros aspectos éticos a tener en cuenta, como los Derechos Humanos.

Para otros autores, como Colonomos (2015) hay otro factor de vital importancia que han de considerarse en el marco de la guerra, y tienen que ver con la obligatoriedad de dar continuidad o no a esta, el ius ex bello, que hace referencia aquellas reglas que pretenden limitar las consecuencias de los conflictos armados. En concordancia Mollendorf (2015), expone que el ius ex bello, es el principio que determina si moralmente es viable continuar con la guerra o si por el contrario el mismo contexto es necesario ponerle fin.

Otro aspecto, que se ha de tener en cuenta, en el marco de la ética militar según Murphy (2015), ius post bellum, que se refiere a la transición de la guerra al tiempo de la postguerra, donde se ha de considerar la durabilidad del tiempo de paz, siendo este último elemen central y necesario para la sociedad.

De esta manera, la forma en que se usa la fuerza militar debe adaptarse plenamente a esos principios, pues, es lo que realmente le proporciona legitimidad, y por ende a los imperativos del Derecho Internacional y más precisamente del Derecho Internacional (Rodríguez, et al, 2017, p. 56).

Para Moliner (2020), las nuevas tecnologías disruptivas están comenzando a influir en la evolución y el desarrollo del ser humano como especie y este no un aspecto que se enmarque en la ciencia ficción, sino es un asunto de un futuro inminente y sobre el que no es viable permitir que se materialicen resultados inesperados e indeseados" (p. 216).

Así las cosas, para Scharre (2019), la cuestión está en llegar a determinar si esos sistemas ostentan la capacidad de disponer del juicio moral para asumir responsabilidad de las acciones en el marco de la guerra. De esta manera, para este autor es claro, que, aunque los sistemas de armas posean algoritmos con importantes capacidades, de ninguna manera pueden tomar la decisión sobre la muerte o la vida una misión esencial dentro de la milicia, pues, es de anotar que esta decisión es única del ser humano. De esta manera, el uso de este tipo de armas plantea retos éticos que influyen directamente en la profesión militar (p. 293).

Entonces la mirada de la ética militar se dirige a "determinar los criterios y condiciones que hacen que la guerra, con la violencia como componente esencial de su naturaleza y

que implica el uso de la fuerza letal, sea legítima en su inicio, desarrollo y consecuencias" (Moliner, 2020, p. 8).

Savater (2012) "la ética se ocupa de las cosas que duran, que no se van del todo, que permanecen, de aquello que siglo tras siglo sigue siendo importante para los seres humanos" (p. 11). Lo que conlleva a pensar que en esta era de la tecnología y la información, es importante considerar que en el ámbito ético se encontrara consenso al estar sobre la base de valores y principios dirigen la conducta militar.

Así, en el dilema ético en que se desarrolla el conflicto, de acuerdo a lo expuesto por Coleman (2015), se suscita la constante preocupación para lograr determinar, si la decisión que se adopta se enmarca en lo moralmente admitido, o en caso que esta situación se torne difícil optar por el menor daño posible.

Tanto la implementación como el desarrollo de las nuevas tecnologías sin lugar a duda abren nuevos debates éticos, donde de acuerdo con Shunk (2015), la última decisión recae sobre el militar, la cual, debe estar guiada por la ética y de ninguna manera por la tecnología.

6. Conclusiones

Sin lugar a duda, la implementación de sistemas con Inteligencia Artificial es una necesidad de la que no se puede prescindir hoy, en el marco de los conflictos armados, no obstante, dirigir la mirada en su uso responsable evaluando consecuencias, es uno de los grandes retos que enfrentas la Fuerzas militares, esto, con el ánimo de seguir cumpliendo con lo exigido por el DIH, toda vez, que no es sencillo dimensional el verdadero alcance y por tanto se desconoce la dimensión de los posibles daños.

La transformación a la que hoy se ven enfrentadas las fuerzas militares y más precisamente la Fuerza Aérea, con ocasión a la implementación nuevas tecnologías militares de sistemas con inteligencia artificial, es necesaria, toda vez, que la tecnología ha obligado a adentrarse en ella, generando tendencias y cambios en el Derecho Internacional, sin embargo, se abre el debate de la responsabilidad de su uso, de la distinción y proporcionalidad; principios que se han constituido rectores en el marco de los conflictos:

Desde el punto de vista ético, la guerra cibernética puede ser la cuestión más problemática de las nuevas tecnologías militares a la hora de contemplar el principio de discriminación y los costos de ir a la guerra. A primera vista podrían verse como una acción que tiene costos muy bajos pero el alcance de sus danos podrían ser graves y extenderse a todo tipo de población más allá del campo de batalla.

El componente ético es una de las tendencias más fuertes a la hora de explorar la literatura en nuevas tecnologías militares; se considera que su aporte debe abordarse desde una perspectiva del conceso entre las ventajas que traen dichas tecnologías en cuanto a resultados y la legislación existente pensada para el uso de armas tradicionales, para así evidenciar un panorama de gobernanza productiva de estas para los Estados.

Referencias

Álvarez C. & Jiménez H. (2021). Guerra de Información y ética militar: entre la tradición de guerra justa y la teoría de guerra irrestricta. Capítulo IV. Escuela Superior de Guerra: General Rafael Reyes Prieto.

Ardila-Castro, C. A., Acosta-Guzmán, H. M., Moreno-Peláez, J. E., Cujabante-Villamil, X. A., Librado-Castillo, H., Jiménez-Reina, J., . . . Ramírez-Pedraza, Y. E. (2021). Ética militar y nuevas formas de guerra. Retos para las Fuerzas Armadas colombianas. Colombia. Capítulo VII. Escuela Superior de Guerra: General Rafael Reyes Prieto.

Bermejo García, R., & Cocchini, A. (2020). The Drones under International Humanitarian Law (IHL). Anuario Espanol de Derecho Internacional, 36, 27.

Burmaoglu, S., & Sarıtas, O. (2016). "Changing characteristics of warfare and the future of Military R&D, Technol. Forecast. Soc. Change". http://dx.doi.org/10.1016/j.techfore.2016.10.062

Casey-Maslen, S. (2012). Pandora's box? Drone strikes under jus ad bellum, jus in bello, and international human rights law. International Review of the Red Cross, 94(886), 597-625.

Coleman, S. (2014). Ethical Challenges of New Military Technologies. In New Technologies and the Law of Armed Conflict (pp. 29-41). TMC Asser Press, The Hague.

Coleman, S. (2014). Ethical Challenges of New Military Technologies. In New Technologies and the Law of Armed Conflict (pp. 29-41). TMC Asser Press, The Hague.

Coleman, S. (2015). Ethical dilemmas and tests of integrity. In Key concepts in military ethics (pp. 8-11). University of New South Wales Press.

Colonomos, A. (2015). Is there a Future for 'Jus ex Bello'?. Global Policy, 6(4), 358-368.

Del Toro Huerta, M. I. (2006). El fenómeno del soft law y las nuevas perspectivas del derecho internacional. Anuario mexicano de derecho internacional, 6, 513-549.

Delàs, B., Font, T., Mojal, X. & Rodríguez, J. (2019). Nuevas armas contra la ética y las personas drones armados y drones autónomos. Nuevo informe del Centro de Estudios por la Paz J.M. http://www.centredelas.org/es/.

Duran Cenit, Marién, & Bados Nieto, Víctor-Mario (2015). Las "Nuevas Guerras": Una Propuesta Metodológica Para Su Análisis. Revista UNISCI, (38),9-33. Disponible en: https://www.redalyc.org/articulo.oa?id=76738762001

Enemark, C. (2021). Armed drones and ethical policing: risk, perception, and the tele-present officer. Criminal justice ethics, 40(2), 124-144.

Fonseca, C. E. (2014). El manual de Tallin y la aplicabilidad del derecho internacional de la ciberguerra. Revista de la ESG no.588-143.

Gallais, S. (2013). Cadre juridique de l'emploi des drones au combat. Cadre juridique de l'emploi des drones au combat, 1-192.

Gilli, A., & Gilli, M. (2019). Military Technology: the realities of imitation. CSS Analyses in Security Policy, 238.

Gómez Isa, F. (2015). Los ataques armados con drones en derecho internacional. Los ataques armados con drones en Derecho internacional, 61-92.

Kleinschmidt, J. (2015). Drones y el orden legal internacional. Tecnología, estrategia y largas cadenas de acción. Colombia internacional, (84), 17-42.

Llorens, M. P. (2017). Los desafíos del uso de la fuerza en el ciberespacio. Anuario mexicano de derecho internacional, 17, 785-816.

Lucas Jr, G. R. (2014). Legal and ethical precepts governing emerging military technologies: Research and use. Amsterdam LF, 6, 23.

Meza Rivas, M. J. (2022). Las armas autómatas letales: un desafío para el Derecho Internacional Humanitario, los Derechos Humanos, la Seguridad y el Dersa. Las armas autómatas letales, 1-776.

Moellendorf, D. (2015). Two doctrines of jus ex bello. Ethics, 125(3), 653-673.

Moliner, J. (2018). Algunos problemas éticos de las tecnologías militares emergentes. bie3: Boletín IEEE, (9), 522-541.

Moliner, J. (2020). La ética militar y su importancia para el militar profesional (Doctoral dissertation, UNED. Universidad Nacional de Educación a Distancia (España)).

Murphy, C. (2015). Political Reconciliation, Jus Post Bellum and Asymmetric Conflict. Theoria, 62(145), 43-59.

Nasu, H., & McLaughlin, R. (Eds.). (2014). New technologies and the law of armed conflict. TMC Asser Press.

Nasu, H., & McLaughlin, R. (Eds.). (2014). New technologies and the law of armed conflict. TMC Asser Press.

Perez, M. (2017). El derecho internacional humanitario frente a la violencia bélica: Una apuesta por la humanidad en situaciones de conflicto. In Derecho internacional humanitário (pp. 25-52). Tirant lo Blanch.

Rico, E. D. M. G. (2016). Altas tecnologías, conflictos armados y seguridad humana. Araucaria: Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales, 18(36), 265-293.

Rodríguez Villasante y Prieto, J. L., & López Sánchez, J. (2017). Derecho internacional humanitario: 3ª Edición 2017. Derecho internacional humanitario, 1-1312.

Sainz, J. A. S. (2012). Inteligencia táctica. Revista UNISCI, (28), 213-232.

Savater, F. (2012). Ética de urgencia. Barcelona: Ariel.

Scharre, P. (2019). Army of none: Autonomous weapons and the future of war. WW Norton & Company.

Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.

Shunk, D. (2015). La ética y el soldado potenciado del futuro cercano. Military Review, Tomo 70, Número 4.

Vega, María Eugenia, & Espinoza Aguaida, Juan Pedro (2010). Una lectura acerca de la Revolución en los Asuntos Militares. Revista de Ciencias Sociales (Ve), XVI(1),106-116.[fecha de Consulta 2 de Agosto de 2022]. ISSN: 1315-9518. Disponible en: https://www.redalyc.org/articulo.oa?id=28016297010

Velázquez Elizarrarás, J. C. (2013). The Outer Space Law in Critical Time: Statehood, Monopolization or Universality?. Anuario mexicano de derecho internacional, 13, 583-638.

Villamizar Lamus, F. (2015). Drones:¿ Hacia una guerra sin regulación jurídica internacional?. Revista de Relaciones Internacionales, Estrategia y Seguridad, 10(2), 89-109.

Wallach, W. (2013). Terminating the terminator: What to do about autonomous weapons. Science Progress, 29.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 21/12/2021
Aceitação/Acceptance: 27/02/2022

Producción biológica de ácidos grasos volátiles a partir de lodo primario y lodo digerido de una planta de tratamiento de aguas residuales como fuente de productos biopolímeros en la industria militar

Gracia Jeniffer[1], Cabeza Iván[2], Montenegro Carlos[3], Paola Acevedo[4]

jpgraciar@udistrital.edu.co; ivan.cabeza@unisabana.edu.co; cemontenegrom@udistrital.edu.co; paola.acevedop@ucc.edu.co

[1,3] Universidad Distrital Francisco José de Caldas, Bogotá, 110221, Colombia.

[2] Universidad de la Sabana, Chía, 250001, Colombia.

[4] Universidad Cooperativa de Colombia, Bogotá, 111321, Colombia

Pages: 374-385

Resumen: En la presente investigación se propone la valorización de lodos provenientes de la planta de tratamiento de aguas residuales domésticas El Salitre de Bogotá- Colombia, hacia la producción de ácidos grasos volátiles (AGV) por medio de fermentación anaeróbica, para posteriormente ser utilizados como fuente de carbono en la producción de Polihidroxialcanoatos (PHA's) aprovechables en la industria militar, lo cual se puede impulsar en la implementación de esquemas de biorrefinería. Se realizó un estudio experimental con los parámetros operacionales de temperatura 45°C, pH 9.5, 10.5 y 11.5 y carga orgánica 4 gSV/L y 6 gSV/L para Lodo Digerido, 10 gSV/L y 14 gSV/L para Lodo Primario. La mayor producción de AGV fue de 7392 mg DQO/L empleando Lodo Primario a condiciones de 14 gSV/L, pH de 10.5 y en el día seis.

Palabras-clave: Ácidos Grasos Volátiles, Lodo Primario, Lodo Digerido, Fermentación Anaeróbica.

Biological production of volatile fatty acids from primary sludge and digested sludge from a wastewater treatment plant as a source of biopolymer products in the military industry

Abstract: This research proposes the valorization of sludge from the domestic wastewater treatment plant El Salitre in Bogota, Colombia, towards the production of volatile fatty acids (VFA) through anaerobic fermentation, to be subsequently used as a carbon source in the production of polyhydroxyalkanoates (PHA's) usable in the military industry, which can be promoted in the implementation of

biorefinery schemes. An experimental study was conducted with the operational parameters of temperature 45°C, pH 9.5, 10.5 and 11.5 and organic loading 4 gVS/L and 6 gVS/L for Digested Sludge, 10 gVS/L and 14 gVS/L for Primary Sludge. The highest VFA production was 7392 mg COD/L using Primary Sludge at conditions of 14 gVS/L, pH 10.5 and on day six.

Keywords: *Volatile Fatty Acids, Primary Sludge, Digested Sludge, Anaerobic Fermentation.*

1. Introducción

La sostenibilidad ambiental es protagonista de este siglo, las problemáticas por contaminación a solucionar cada día se hacen más complejas, por esta razón se deben generar alternativas de solución sustentables. Las tasas de generación de residuos sólidos están aumentando rápidamente en todo el mundo, debido al crecimiento de la población, lo que también ha llevado la investigación de alternativas para el tratamiento y la producción de bioproductos a partir de la valorización de los residuos. Los bioproductos de valor añadido pueden obtenerse a partir de diferentes tipos de residuos orgánicos (Liguori, et al., 2013), donde algunos de los principales productos son los biocombustibles y los bioplásticos. Los bioplásticos derivados de polímeros de origen biológico proporcionan una solución al creciente problema de la gestión de diferentes tipos de residuos, como los lodos derivados del tratamiento de aguas residuales.

En ese sentido, esta contribución se adelanta en la producción de ácidos grasos volátiles - AGV empleando diferentes parámetros operacionales, buscando ser una de las alternativas de valorización de los lodos de las Plantas de Tratamiento de Aguas Residuales EDAR, e incluso ser tenido en cuenta en los esquemas de biorrefinería que pueden ser usados en la industria militar.

1.1. Aguas Residuales Domésticas y Lodos de Plantas de Tratamiento

Las aguas residuales domesticas son generadas en hogares donde se descarga agua proveniente del uso final en baños, cocinas y aseo general como lavado de pisos y lavado de ropa (Torres & Briceño, 2016), 80% del total de estas aguas son vertidas sin respectivo tratamiento al entorno al año debido a su alta carga orgánica se pueden presentar afectaciones a los cuerpos de agua como la eutrofización que en consecuencia afecta al ecosistema y la subsistencia de comunidades. Las aguas residuales domésticas se caracterizan por poseer gran cantidad de materia orgánica y alto contenido de tensoactivos y por tanto son un foco de atención ante el problema, se estima que 8% del agua consumida al año a nivel mundial, equivalente a 314,24 km^3, es liberada al ambiente como agua residual doméstica (UNESCO, 2017).

Los lodos que se generan tras el tratamiento de las aguas residuales deben ser tratados y estabilizados para cumplir con la normatividad ambiental y proceder a su respectiva disposición (Jin, et al, 2018). Sin embargo, hoy en día es tendencia implementar esquemas de biorrefinería que se enfoquen en la aplicación de sistemas simples (Banerjee, et al, 2020), donde los residuos de un proceso se utilizan como materia prima para la elaboración de un nuevo producto de valor agregado.

1.2. Ácidos Grasos Volátiles - AGV

Los ácidos grasos volátiles derivados de los Lodos de Plantas de Tratamiento de Aguas Residuales pueden ser aprovechados y comercializados (Atasoy, et al, 2018) gracias a su alta demanda a nivel mundial, debido a su potencial como fuente de carbono para la producción de biopolímeros, fuentes de combustibles, productos farmacéuticos y solventes (Gutiérrez, et al, 2018), teniendo en cuenta este antecedente se considera viable evaluar la producción de AGV en Colombia para darle un valor agregado al residuo.

La obtención de AGV se realiza por fermentación anaeróbica y estos se dan en la segunda etapa de este proceso, llamado acidogénesis (Zhou, et al, 2018), existen diferentes estudios que reportan cuáles son las mejores condiciones de operación para mayor producción de AGV y así mismo formas de recuperación del hidrógeno producido en la etapa de acetogénesis, producto que también puede ser valorado. Durante la fermentación, el grupo de microorganismos responsables de la producción de AGV se conocen como bacterias acetogénicas y bacterias homoacetogénicas, en el proceso de acidogénesis (Yuan, et al., 2019). El proceso de fermentación implica la generación de hidrógeno y AGV (ácido acético, propiónico, butírico y valérico principalmente) (Khan, et al., 2016).

En este trabajo se utiliza lodo primario (LP) y lodo digerido (LD) de la EDAR El Salitre-Bogotá para la producción de AGV, debido a que estos funcionan como fuente de carbono para el crecimiento de microorganismos para la síntesis de biopolímeros (Kumar, et al., 2019) y así producir bioplásticos tipo Polihidroxialcanoatos (PHAs) (Fradinho, et al, 2014)

lo anterior, como una solución para disminuir la producción y el consumo de plásticos provenientes de fuentes fósiles. Por otra parte, el valor en el mercado a nivel mundial del ácido acético, ácido butírico y ácido propiónico es de 400-800 €/ton, 1500-1650 €/ton y 2000-2500 €/ton respectivamente (Atasoy, et al, 2018), sumas significativas para residuos que antes no poseían valor comercial, otra razón por la cual la producción de AGV debe ser optimizado.

De acuerdo con investigaciones anteriores, la extracción de AGV depende de varias condiciones operativas; incluyendo el tipo de reactor, el diseño, la composición del sustrato y el espectro de productos; además de la temperatura, el pH, el tiempo de retención y tasa de carga orgánica, que dependerán de las condiciones previamente establecidas (Khan, et al., 2016; Strazzera, et al., 2018). La optimización en la producción de AGV favorecerá su futuro uso como recurso de carbono en la producción de polihidroxialcanoatos (PHA) y la producción de biocombustibles como el hidrógeno y el metano. Actualmente, este proceso bioquímico se utiliza en todo el mundo para estabilizar los lodos municipales, para tratar las aguas industriales y para la digestión de los residuos orgánicos.

Teniendo en cuenta lo planteado, con el desarrollo de este estudio se busca evaluar el rendimiento en la producción de AGV con LP y LS como sustrato, provenientes de la planta de tratamiento de aguas residuales (EDAR) El Salitre, ubicada en Bogotá, Colombia, variando parámetros de operación para establecer cuáles son las mejores condiciones de producción.

2. Metodología

2.1. Inóculo y lodos de aguas residuales

Para garantizar la puesta en marcha de las pruebas, se utilizó lodo granular metanogénico para el montaje experimental, el inóculo se obtuvo reactor anaeróbico estabilizado de la planta de tratamiento de aguas residuales industriales de Alpina S.A. en Sopo, Cundinamarca (Colombia). Fue necesario realizar un tratamiento de choque térmico para un sistema de fermentación acidogénica, el inóculo se hirvió durante 30 min y se dejó enfriar hasta la temperatura ambiente antes de ser añadido a cada uno de los reactores (Hernández, et al., 2018).

Los lodos primario y digerido de aguas residuales domesticas se recogieron de la planta de tratamiento de aguas residuales (EDAR) El Salitre, que es la principal planta de este tipo en la ciudad de Bogotá (Colombia), las principales características fisicoquímicas de los lodos se muestran en la Tabla 1. Las aguas residuales se mantuvieron en un congelador a -4°C para evitar la degradación microbiológica antes de las pruebas.

Sustrato	% Solidos Totales (ST)	% Materia Orgánica	% Sólidos volátiles (SV)	% Nitrógeno Total Kjeldahl	Demanda Química de Oxígeno DQO mg/L
Lodo Primario	3,91±0,01	69,21 ±0,01	2,71 ± 0,41	0,16 ± 0,01	31600
Lodo Digerido	1,07±0,01	74,24 ±0,01	0,80 ± 0,41	0,19 ± 0,01	11600
Inoculo	5,12±0,49		4.21± 0,41		

Tabla 1 – Características fisicoquímicas del inóculo y de los lodos primario y digerido de aguas residuales domésticas

2.2. Experimentos para obtener AGV

Para determinar las mejores condiciones operativas para la producción de AGV a partir de lodos provenientes de planta de tratamiento de aguas residuales EDAR El Salitre, se evaluarán varios ensayos mediante fermentación acidogénica. La tabla 2. muestra el diseño experimental realizado, en el que fue evaluado la carga orgánica inicial (CO) del reactor (6 gVS/L y 4 gVS/L) para Lodo Digerido y (14 gVS/L y 10 gVS/L) para Lodo Primario, la temperatura (45 °C) y el pH inicial (de 9,5, 10,5 y 11,5). Se utilizaron soluciones reguladoras de pH para gestionar el pH en los reactores. Hubo un total de 12 combinaciones ensayadas por triplicado, las pruebas se realizaron utilizando reactores discontinuos de 200 mL, frascos ámbar con un volumen de trabajo correspondiente al 80% del volumen total (Angelidaki, et al., 2009).

La relación entre el sustrato y el inóculo (S/X) se fijó en 1 para reducir los efectos inhibidores durante la fermentación. Los reactores se llenaron con: el inóculo; la carga orgánica fijada, según la caracterización inicial del sustrato; la solución reguladora de pH, según la combinación; y el volumen de trabajo se completó con agua destilada. Luego,

se ajustó el pH con una solución de NaOH. Los reactores se cerraron herméticamente y se colocaron en un baño termostático para garantizar la condición mesófila establecida para un tiempo de reacción de 12 días. Por último, la productividad de biogás y AGV se controló mediante un muestreo destructivo cada tres días se midió la composición del biogás con el BIOGAS 5000® Landtec y se recogieron muestras para la posterior cuantificación de los AGV producidos durante el tiempo del experimento. Además, para seguimiento del rendimiento de biogás, se estableció un sistema de desplazamiento de volumen, utilizando una solución de NaOH 0,5N como trampa de CO2 (Cendales, 2011).

Sustrato	**Combinación**	**1**	**2**	**3**	**4**	**5**	**6**
Lodo Primario	*Carga Orgánica (gSV/L)*	14	14	14	10	10	10
	Temperatura (°C)	45	45	45	45	45	45
	pH	9,5	10,5	11,5	9,5	10,5	11.5
Sustrato	**Combinación**	**7**	**8**	**9**	**10**	**11**	**12**
Lodo Digerido	*Carga Orgánica (gSV/L)*	6	6	6	4	4	4
	Temperatura (°C)	45	45	45	45	45	45
	pH	9,5	10,5	11,5	9,5	10,5	11,5

Tabla 2 – Condiciones del tratamiento experimental para la fermentación acidogénica de Lodo Digerido y Lodo Primario de EDAR.

El cálculo del rendimiento de producción de AGV, permite evaluar el potencial de acidificación de los lodos Primario y Digerido, donde el rendimiento específico es la relación de la concentración total de AGV del efluente, expresada en los equivalentes de Solidos Volátiles (SV) por gramo de SV alimentado, como se muestra en la Ec. (1) (García-Aguirre, et al., 2017).

AGVrendimiento = (AGVsalida)/(SV alimentado) EC. (1)

2.3. Métodos analíticos

Las mediciones de pH se determinaron utilizando un medidor de pH Edge modelo HI2002. Los sólidos totales (ST), los sólidos volátiles (SV) y materia orgánica (MO) de las muestras de Lodo Digerido y Lodo Primario se determinaron secando las muestras a 105±5°C en un horno y la posterior calcinación a 550±10°C en una mufla, esto según 2540B APHA - SM y D3174 de la Sociedad Americana de Pruebas y Materiales (ASTM). La demanda química de Oxígeno (DQO) se midió utilizando viales comerciales de Hanna Instruments con un rango de 0 a 150 mg/L (HI 93752). El nitrógeno total Kjeldahl (NKT) se evaluó según la D1426 de la ASTM. Ácidos grasos volátiles (AGV) y la alcalinidad (ALK) se midieron según los métodos estándar (APHA, 2005). La medición composición de los gases (CO2, CH4 y O2%) se determinó con el analizador de gases BIOGAS 5000® Landtec.

3. Resultados

La producción de AGV se evaluó como una concentración de (mg DQO/L), la producción se midió cada tres días, con el fin de seguir el comportamiento durante el tiempo de reacción establecido. De acuerdo con el perfil temporal de la fermentación anaeróbica por lotes en las condiciones establecidas, la mayor producción total de AGV, de todas las combinaciones evaluadas actualmente, se consiguió utilizando lodos primarios, con una carga orgánica de 14 gVS/L y un pH de 10,5 (6256±0,2 mg DQO/L en el día 6). Asimismo, para los lodos digeridos, la mayor producción total de AGV se alcanzó con una carga orgánica de 6 gVS/L y un pH de 10,5 (3640±0,05 mg DQO/L en el día 9); véase las Figuras 1 a y 1b.

Como los experimentos se realizaron como un proceso de fermentación anaeróbica convencional, la inoculación y el ajuste del pH fueron clave para evitar los metanógenos y, por tanto, la producción de AGV, al detener la degradación en la etapa acidogénica (Kuruti, et al, 2017). Esto se observa en la producción de AGV reportada para el día tres.

Adicionalmente, la carga orgánica tiene una relación directa con la acumulación de AGV; la producción de AGV también se afecta por las características de los sustratos. Los resultados muestran que el Lodo Primario como fuente de carbono para la producción de AGV es más factible. Lo cual es acorde con los antecedentes que señalan que el aumento de la carga orgánica parece conducir a una mayor acumulación de AGV y a una disminución del pH que favorece la producción de ácidos grasos (Iglesias-Iglesias, et al., 2019; Zeng, Yuan y Keller, 2006).

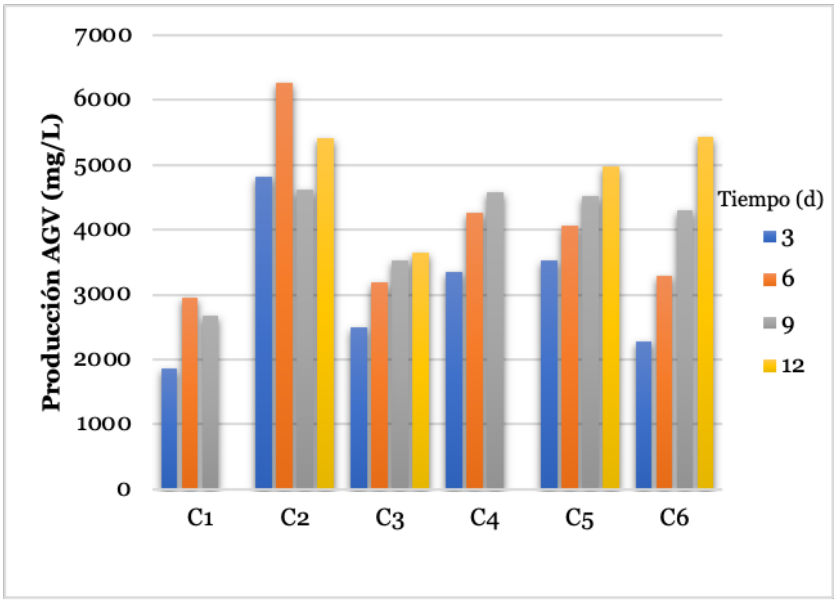


Figura 1a – Producción de AGV durante un tiempo de reacción de 12 días usando Lodo Primario, carga orgánica 14gSV/L (C1-C3) y 10gSV/L (C4-C6)

De hecho, el lodo primario incluye una mayor diversidad de compuestos, junto con diferentes características de biodegradación, que el lodo digerido que ya ha sido tratado en condiciones anaeróbicas (Lim, et al, 2008). De forma similar, Fernández, et al, 2020, se identificó que, debido al excesivo contenido de compuestos orgánicos en los lodos de depuradora, éstos proporcionan un potencial positivo para la recuperación de AGV; sin embargo, la composición y las propiedades de los lodos digeridos pueden limitar su biodegradabilidad y dificultar la producción de AGV.

En el proceso de fermentación anaeróbica, la alta carga orgánica suele utilizarse para mejorar la producción de ácido y acortar el periodo de fermentación (Yuan, et al., 2019); los resultados obtenidos muestran una mayor producción de AGV en los experimentos con la carga orgánica inicial más alta. Estudios anteriores han encontrado logros en la producción de AGV alrededor de 540 a 1900 mg DQO/L a partir de la fermentación de cultivos mixtos de corrientes de aguas residuales (Atasoy, et al, 2019).

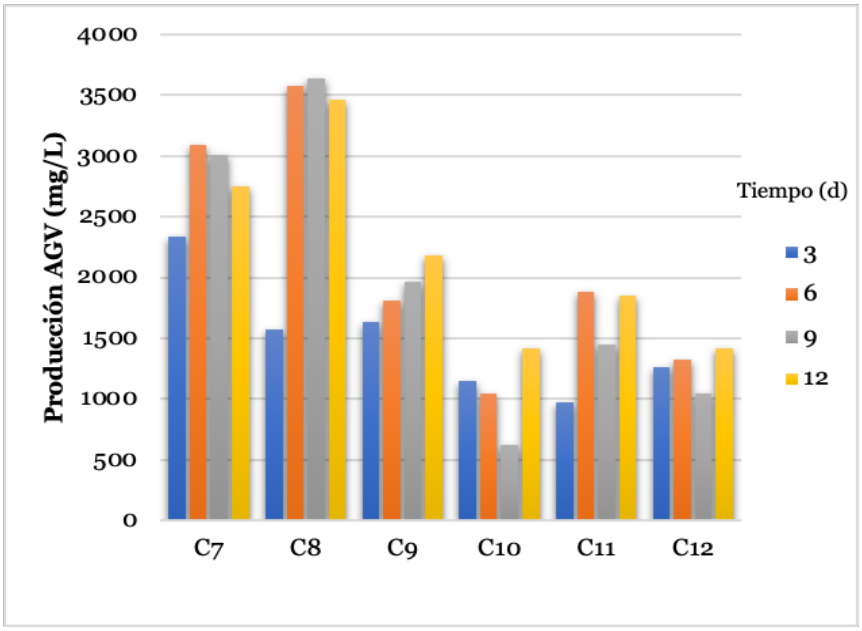


Figura 1 b – Producción de AGV durante un tiempo de reacción de 12 días usando Lodo Digerido, carga orgánica 6gSV/L (C7-C9) y 4gSV/L (C10-C12)

En relación con la relación sustrato/inóculo, Iglesias-Iglesias, et al., 2019 evaluaron diferentes S/X en la fermentación acidogénica de lodos de depuradora, registrando concentraciones de AGV entre 1800 y 2200 mg DQO/L para un S/X de "1". Las menores concentraciones de AGV obtenidas pueden atribuirse a la mayor concentración de sólidos totales en los lodos de depuradora de El Salitre considerando que las investigaciones existentes mostraron que el sustrato con alto contenido de sólidos podría causar una presión de amonio, que podría dirigir la estructura de la comunidad bacteriana hacia una mayor reacción de oxidación de acetato (Li, et al., 2017).

El rendimiento total de AGV para los lodos primarios, fluctuó de 0,27 a 1,34 (g DQO/g SV) para las condiciones con 14gSV y de 0,67 a 2,74 (g DQO/g SV) para las condiciones con 10gSV (ver Figura 2a), mientras que, para los lodos digeridos, fluctuó de 0,52 a 1,82 (g DQO/g SV) para las condiciones con 6gSV y de 0,31 a 1,09 (g DQO/g SV) para las condiciones con 4gSV, (ver Figura 2b).

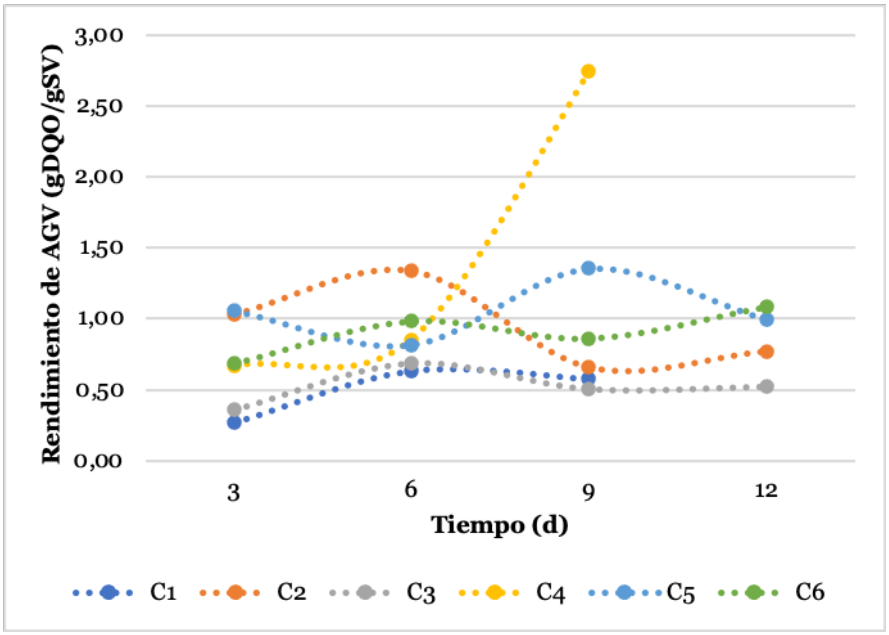


Figura 2 a – Rendimiento de la fermentación acidogénica en términos de eficiencia de producción de AGV durante un tiempo de reacción de reacción de 12 días para Lodo Primario.

Al ser un proceso por etapas, las mediciones generales mostraron que, en la mayoría de los casos, la mayor acumulación de AGV se registró durante los primeros días. Sin embargo, el rendimiento de AGV aumenta durante los últimos días (el caso de C-3, con un rendimiento medio de 0,51 g DQO/g SV, lo que sugiere que los valores de pH más altos aumentan la inhibición del consumo de los AGV producidos por los metanógenos (Jie, et al, 2014; Yuan, et al, 2019). Además, desde el punto de vista del proceso de fermentación bioquímica, los principales metabolitos esperados son el ácido acético, propiónico y butírico; donde el acetato es el principal precursor para la conversión de CH_4, entre el 65 y el 95% se produce a partir del ácido acético (Kumar, et al, 2019).

Es importante tener en cuenta que durante la evaluación en condiciones psicrófilas (5-30 °C) y termófilas (50 a 100°C), la tasa de reacción bioquímica podría cambiar según el crecimiento de los microorganismos (Xiong, et al, 2012). Los cambios en la producción y el rendimiento de los AGV aumentan a la temperatura termófila, debido al aumento de la solubilidad de los carbohidratos y las proteínas; aunque esto también está ligado a la adaptación del cultivo microbiano de los lodos (Hao, et al, 2015; Hasan, et al 2017).

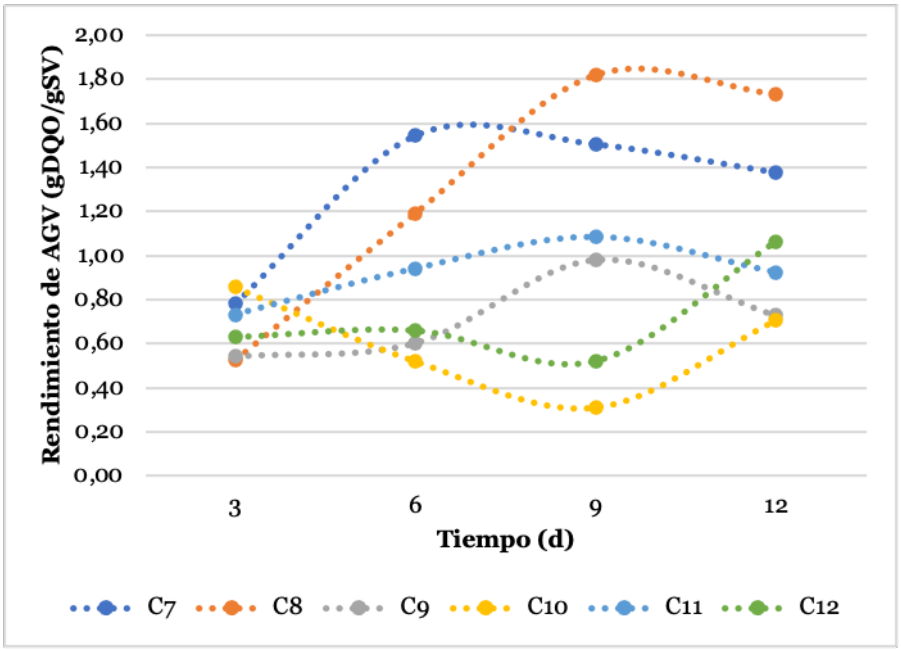


Figura 2 b – Rendimiento de la fermentación acidogénica en términos de eficiencia de producción de AGV durante un tiempo de reacción de reacción de 12 días para Lodo Digerido.

4. Conclusiones

Los resultados obtenidos permiten aplicar las condiciones de fermentación anaeróbica más adecuadas para producir AGV para la posterior producción de productos renovables de valor añadido. El mayor rendimiento se produjo a partir de la fermentación de lodos primarios, bajo un OL de 14 g VS/L, a 35°C y un pH de 11, donde se inhibieron los metanógenos.

Asimismo, el alto contenido en proteínas y de carga orgánica de los ensayos realizados con lodo primario dieron lugar a una producción significativa de AGV, muy diferente a la de los ensayos con lodo digerido. Sin embargo, es importante evaluar en condiciones psicrófilas y termófilas, para establecer los parámetros operativos para el escalamiento del proceso. Por otro lado, los resultados relacionados con la producción de AGVs utilizando como materia prima lodos primarios y lodos digeridos representan una evaluación importante para establecer el potencial de esta biomasa residual para obtener productos de valor añadido. Finalmente, los resultados de esta contribución serán la base para futuras investigaciones sobre la producción de polihidroxialcanoatos de base sostenible, a través de la valorización de las aguas residuales municipales, utilizando los AGVs como sustrato.

Referencias

Angelidaki, I., Alves, D., Bolonzella, L., Borzacconi, J., Campos, A., Guwy, S., Van Lier, J. (2009). Defining the biochemical methane potential (BMP) of solid organic wastes and energy crops: a proposed protocol forbatch assays. *Water Science and Technology*, 59, 927-934

Atasoy, M., Owusu-Agyeman, I., Plaza, E., Cetecioglu, Z. (2018). Bio-based volatile fatty acid production and recovery from waste streams: Current status and future challenges. *Bioresource Technology*, 268, 773–786

Atasoy, M., Eyice, Ö, Cetecioglu, Z. (2019). Volatile fatty acid production from semi-synthetic milk processing wastewater under alkali pH: the pearls and pitfalls of microbial culture. *Bioresource Technology*, 297, 122415

Banerjee, A., Bhaskar, T., Ghosh, D. (2020). A biorefinery approach for sewage sludge. *Waste Biorefinery,* 393–421

Cendales, E. (2011). Producción de biogás mediante la codigestión anaeróbica de la mezcla de residuos cítricos y estiércol bovino para su utilización como fuente de energía renovable. https://repositorio.unal.edu.co/handle/unal/7658

Fernández-Domínguez, D., Astals. S., Peces, M., Frison, N., Bolzonella, D., Mata, J., Dosta, J. (2020). Volatile fatty acids production from biowaste at mechanical-biological treatment plants: Focusing on fermentation temperature. *Bioresource Technology,* 314, 1-32

Fradinho, J., Oehmen, A., Reis, M. (2014). Photosynthetic mixed culture polyhydroxyalkanoate (PHA) production from individual and mixed volatile fatty acids (VFAs): Substrate preferences and co-substrate uptake. *Jurnal of Biotechnology*, 185, 19–27.

García-Aguirre, J., Aymerich, E., González, J., Gutiérrez, M. (2017). Selective VFA production potential from organic waste streams: Assessing temperature and pH influence. *Bioresource Technology*, 244, 1081-1088

Gutiérrez, E., Garcia-Aguirre, J., Irizar, I., Aymerich, E. (2018). From sewage sludge and agri-food waste to VFA: Individual acid production potential and up-scaling. *Waste Management,* 77, 203–212

Hao, J., Wang, H. (2015). Volatile fatty acids productions by mesophilic and thermophilic sludge fermentation: Biological responses to fermentation temperature. *Bioresource Technology,* 175:367-373

Hasan, S., Giongo, C., Fiorese, M., Damasceno, S., Ferrari, T, Savoldi, T. (2015). Volatile fatty acids production from anaerobic treatment of cassava waste water: Effect of temperature and alkalinity. *Enviromental Technology,* 36(20):2637-2646

Hernández, M.A., González, A.J., Suárez, F., Ochoa, C., Candela, A.M., Cabeza, I. (2018). Assessment of the biohydrogen production potential of different organic residues in Colombia: Cocoa waste, pig manure and coffee mucilage, *Chem. Eng. Trans*, 65, 247-252

Iglesias-Iglesias, R., Campanaro, S., Treu, L., Kennes, C., Veiga, M.C. (2019). Valorization of sewage sludge for volatile fatty acids production and role of microbiome on acidogenic fermentation. *Bioresource Technology*, 291

Jie, W., Peng, Y., Ren, N., Baikun, L. (2014) Volatile fatty acids (VFAs) accumulation and microbial community structure of excess sludge (ES) at different pHs. *Bioresource Technology,* 152:124-129

Jin, C., Archer, G., Parker, W. (2018). Current status of sludge processing and biosolids disposition in Ontario. *Resources, Conservation and Recycling,* 137, 21–31

Khan, M.A., Ngo, H.H., Guo, W.S., Liu, Y., Nghiem, L.D., Hai, F.I., Deng, L.J., Wang, J., Wu, Y. (2016). Optimization of process parameters for production of volatile fatty acid, biohydrogen and methane from anaerobic digestion. *Bioresource Technology,* 219, 738-748

Khiewwijit, R., Temmink, H., Labanda, A., Rijnaarts, H., Keesman, J. (2015). Production of volatile fatty acids from sewage organic matter by combined bioflocculation and alkaline fermentation. *Bioresource Technology*, 197, pp. 295–301

Kumar, G., Ponnusamy, V.K., Bhosale, R.R., Shobana, S., Yoon, J.-., Bhatia, S.K., Rajesh Banu, J., Kim, S. (2019). A review on the conversion of volatile fatty acids to polyhydroxyalkanoates. *Bioresource Technology,* 287, 1-12

Kuruti, K., Nakkasunchi, S., Begum, S., Juntupally, V., Anupoju, G. (2017). Rapid generation of volatile fatty acids (VFA) through anaerobic acidification of livestock organic waste at low hydraulic residence time (HRT). *Bioresource Technology,* 238, 188-193

Li, N.,He, J.,Yan, H.,Chen, S.,Dai, X. (2017). Pathways in bacterial and archaeal communities dictated by ammonium stress in a high solid anaerobic digester with dewatered sludge. *Bioresource Technology*, 241, 95-102

Liguori, R., Amore, A., Faraco, V. (2013). Waste valorization by biotechnological conversion into added value products. *Microbiol. Biotechnol*, 97, 6129-6147

Lim, S., Kim, B., Jeong, C., Choi, Y., Ahn, H., Chang H. (2008). Anaerobic organic acid production of food waste in once-a-day feeding and drawing-off bioreactor. *Bioresource Technology*. 99, (16), 7866–7874

Strazzera, G., Battista, F., Garcia, N.H., Frison, N., Bolzonella, D. (2018). Volatile fatty acids production from food wastes for biorefinery platforms: A review, *J. Environ. Manage,* 226, 278-288

Torres, J., Briceño, Y. (2016). Tratamiento de aguas residuales de tipo doméstico a partir de coleópteros scarabaeidae. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/handle/10596/6254

UNESCO. (2017). “Informe Mundial de las Naciones Unidas sobre el Desarrollo de los Recursos Hídricos 2017. Aguas residuales: El recurso desaprovechado”

Xiong, H., Chen ,J., Wang, H, Hanchang, S. (2012) Influences of volatile solid concentration, temperature and solid retention time for the hydrolysis of waste activated sludge to recover volatile fatty acids. *Bioresourse Technology,* 119:285-292

Yuan, Y., Hu, X., Chen, H., Zhou, Y., Zhou, Y., Wang, D. (2019). Advances in enhanced volatile fatty acid production from anaerobic fermentation of waste activated sludge. *Science of The Total Environment*, 694, 1-12

Zeng, R.J., Yuan, Z., Keller, J. (2006). Effects of solids concentration, pH and carbon addition on the production rate and composition of volatile fatty acids in prefermenters using primary sewage sludge, *Water Sci. Technol*, 53

Zhou, M., Yan, B., Wong, J., Zhang, Y. (2018). Enhanced volatile fatty acids production from anaerobic fermentation of food waste: A mini-review focusing on acidogenic metabolic pathways. *Bioresource Technology*, 248, 68–78

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 16/12/2021
Aceitação/Acceptance: 14/02/2022

Tendencias de la acumulación de biogás como fuente energética en la fase acidogénica de la producción de ácidos grasos volátiles a partir de lodos de aguas residuales municipales

Gracia Jeniffer[1], Cabeza Iván[2], Montenegro Carlos[3], Ferrasse Jean-Henry[4]

jpgraciar@udistrital.edu.co; ivan.cabeza@unisabana.edu.co; cemontenegrom@udistrital.edu.co; jean-henry.ferrasse@univ-amu.fr

[1,3] Universidad Distrital Francisco José de Caldas, Bogotá, 110221, Colombia.

[2] Universidad de la Sabana, Chía, 250001, Colombia.

[4] Aix-Marseille Université, Aix en Provence, 13080, France.

Pages: 386-395

Resumen: Los datos que se presentan en este artículo proporcionan resultados cuantitativos sobre la digestión anaeróbica de lodos digerido y primario de una planta de tratamiento de aguas residuales utilizando como inóculo el lodo del digestor de una industria láctea, los datos presentados incluyen: la tasa de producción diaria de biogás como fuente energética, la producción acumulada de biogás y el promedio diario de producción de biogás, en un experimento de producción de ácidos grasos volátiles a escala de laboratorio, que se pretende usar como fuente de carbono para la obtención de bioplásticos tipo polihidroxialcanoatos PHA's. Los reactores operaron bajo temperaturas mesófilas y termófilas, en cargas orgánicas de altas y bajas para cada tipo de lodos y a tres pH diferentes.

Palabras-clave: Biogás, ácidos grasos volátiles, digestión anaeróbica.

Trends in biogas accumulation as an energy source in the acidogenic phase of volatile fatty acid production from municipal sewage sludge

Abstract: *The data* presented in this paper provide quantitative results on the anaerobic digestion of digested and primary sludge from a wastewater treatment plant using digester sludge from a dairy industry as inoculum, the data presented include: daily biogas production rate, cumulative biogas production and average daily biogas production, in a laboratory scale volatile fatty acid production experiment, which is intended to be used as a carbon source for polyhydroxyalkanoates PHA's bioplastics. The reactors were operated under mesophilic and thermophilic temperatures, at high and low organic loads for each type of sludge and at three different pH.

Keywords: Biogas, volatile fatty acids, anaerobic digestion.

1. Introducción

Teniendo en cuenta los enormes desafíos que se enfrentan en materia de sostenibilidad hoy en día, por una parte, la desmedida generación de plásticos contaminantes y por otra la gran producción de lodos en las plantas de tratamiento de aguas residuales municipales. Esta investigación pretende contribuir al desarrollo de alternativas de valorización de los lodos de las PTAR, al ser empleados en la producción de ácidos grasos volátiles como fuete de carbono para la producción de biopolímeros de característica sostenible polihidroxialcanoatos (Molino, 2013). Razón por la cual, el diseño experimental exige llevar los reactores hasta antes de que haya producción de metano, es decir los montajes solo van hasta la fermentación acidogénica y acetogénica (Ekstrand et al., 2022).

1.1. Lodos Primarios y Digeridos

Al emplear una técnica de separación en las aguas residuales se obtiene su material particulado denominado lodos primarios. En las plantas de tratamiento una vez se cuenta con lodos primarios estos se deben espesar vara reducir el volumen de agua de los mismos. De acuerdo con Orozco (2014), la concentración de la materia seca en el fondo de un sedimentador primario puede ser de 25.000 a 50.000 mg/L. El propósito de esta fase es aumentar la materia seca del 5 al 10%.

En los digestores aerobios o anaerobios de las plantas de tratamiento se someten los lodos ya espesados a estabilización, esta fase es importante que en ella se desarrolla la hidrólisis y la materia orgánica se convierte en biomasa bacteriana, hasta que se logra estabilizar y no consumirse más a sí mismos. En esta fase los lodos digeridos se espesan aproximadamente un 12,0%, para finalmente ser deshidratados con la ayuda de centrífugas o filtros y lograr así un biosólido. (Orozco, 2014; Amador et al, 2015).

1.2. La Digestión Anaerobia

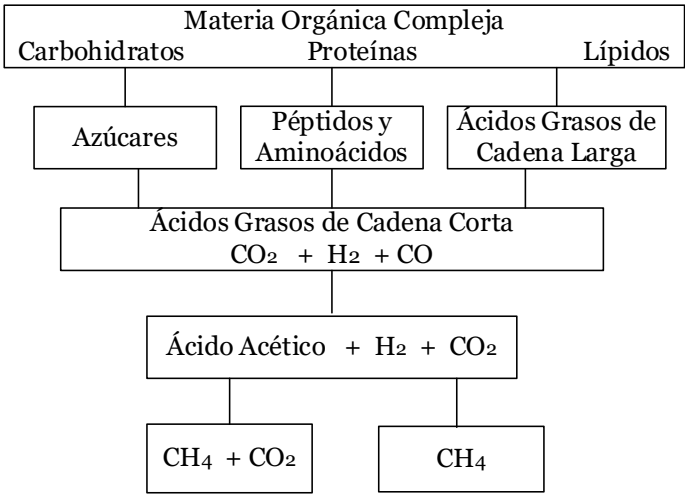


Figura 1 – Degradación de la materia orgánica-Tomado de Rodríguez 2014

El proceso mediante el cual la materia orgánica se biodegrada por la acción bacteriana sin presencia de oxígeno, para producir gases como: hidrógeno, metano y dióxido de carbono se conoce como: digestión anaerobia. (Owusu, 2022)

Durante la digestión anaerobia se dan dos fases continuas: 1. la fase no metanogénica y 2. La fase metanogénica. En la primera, comienza la transformación de la materia orgánica para convertirse en compuestos más simples, en esta fase a su vez se dan dos etapas: la hidrólisis y la acidogénesis. Lo que se genera en la producción de estas etapas serán el sustrato necesario para que los microorganismos puedan producir metano en la fase metanogénica. (Ullah et al, 2017). A continuación, se presenta un resumen de la degradación anaerobia de la materia orgánica.

1.3. La fase no metanogénica

En la fase no metanogénica se desarrolla la actividad de bacterias facultativas, y en esta etapa la materia orgánica compleja es transformada a moléculas más simples de ácidos grasos de cadena corta, que posteriormente sirven de sustrato para la fase metanogénica, en esa transformación tienen lugar tres tipos de reacciones que se realizan de forma sucesiva: primeramente, ocurre la hidrólisis de los polisacáridos, lípidos y proteínas. (Bhatt et al., 2020)

Los productos de este metabolismo son fermentados hasta formar los ácidos grasos, produciéndose pequeñas cantidades de dióxido de carbono. Los ácidos grasos volátiles formados durante la fase no metanogénica son metabolizados por las bacterias metanogénica en la fase de ese nombre produciéndose la mezcla de gases conocida como biogás (Ma0, 2015).

1.4. Bacterias de la fase no metanogénica

Los tres tipos de bacterias que se producen en la fase no metanogénica son: bacterias hidrolíticas, acidogénicas y acetogénicas.

En la etapa fermentativa, se producen las bacterias hidrolíticas solubilizan extracelularmente las moléculas de los polímeros orgánicos de carbohidratos, proteínas y lípidos, formando: azúcares, ácidos grasos, ácidos grasos de cadena larga y aminoácidos.

En la etapa acidogénica, las bacterias acidogénicas utilizan los productos metabólicos de la fase anterior, los cuales son fermentados intercelularmente produciendo los ácidos grasos de cadena corta conocidos como ácidos volátiles, siendo los más importantes de éstos: le acético, propiónico y butírico y en segundo término el valérico y caproico. En este paso de fermentación también hay producción de hidrógeno H_2 y dióxido de carbono CO_2, y la misma actividad bacteriana produce sulfuros y algunos compuestos aromáticos que provienen d ellos aminoácidos que conforman las moléculas de las proteínas.

En la etapa acetogénica, se da el tercer grupo de bacterias constituidas por las bacterias acetogénicas, que transforman a los ácidos grasos producidos en la fase anterior, en ácido acético; este ácido servirá de sustrato para las bacterias metanogénicas. En esta etapa de la digestión anaerobia se produce también dióxido de carbono e hidrógeno, productos que son igualmente sustratos para algunas bacterias metanogénicas. (Chakraborty et al, 2022)

2. Metodología

2.1. Montaje experimental para la obtención de ácidos grasos volátiles

El montaje realizado para la producción de ácidos grasos volátiles - AGVs, se conformó con el uso de un tanque de acero inoxidable que se adaptó como baño termostatizado, y en el cual se ubicaron botellas ámbar con capacidad de 200 mililitros herméticamente selladas para funcionar como reactores, estos a su vez, se conectaron por medio de una manguera a botellas ámbar con 1 Litro de hidróxido de sodio NaOH de concentración 0.5 Normal. Al generarse la producción de biogás, esta solución se desplaza y sale por un orificio cayendo a una botella, lo cual permite medir el volumen del biogás producido que es el volumen desplazado por diferencia de presión por el principio de Pascal.

En la figura 2, se puede ver el esquema del montaje experimental en el laboratorio y las partes que lo componen; (1) reactor, (2) trampa de gases, (3) botellas de medición, (4) tanque termostatizado, (5) bomba de agua, (6) calentador, (7) termopar, (8) manguera, (9) válvula de paso.

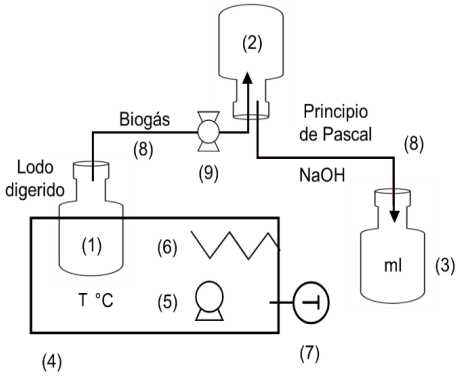


Figura 2 – Esquema del montaje de biodigestión para obtención de ácidos grasos volátiles a escala de laboratorio.

2.2. Inóculo del reactor

La inoculación del reactor anaerobio se llevó a cabo con el lodo del reactor de una planta de industria láctea, la proporción que se usó fue relativa al tipo de lodo y carga orgánica con el que se cargó cada reactor.

2.3. Parámetros del montaje experimental

Se realizó el diseño experimental usado dos tipos de sustrato: lodo primario y lodo digerido y cada uno con carga orgánica alta y carga orgánica baja, a cuatro diferentes temperaturas y tres tipos de pH alcalino (Atasoy et al., 2019,Garcia-Aguirre et al., 2017 ,Owusu-Agyeman et al., 2021), como se explica en la tabla 1, cuarenta y ocho combinaciones en total. El tiempo de retención hidráulica varió, en las temperaturas termófilas fue de máximo 216 horas y a temperaturas mesófilas fue de 288 horas.

Tipo de Lodo	Carga Orgánica (gSV/L)	Temperatura (°C)	pH
Lodo Primario	*10*	25	9.5
		35	10.5
	14	45	11.5
		55	
Lodo Digerido	4	25	9.5
		35	10.5
	6	45	11.5
		55	

Tabla 1 – Condiciones del tratamiento experimental para la fermentación acidogénica de los lodos de aguas residuales

2.4 Lodos de aguas residuales

Para esta investigación se utilizaron lodos provenientes de la planta de tratamiento de aguas residuales PTAR- El Salitre, la cual es la PTAR municipal de la ciudad de Bogotá, se emplearon dos tipos de lodos primarios y digeridos, en la tabla 2 se muestra la caracterización fisicoquímica de los mismos.

Tipo de Lodo	Solidos Totales (TS)	Materia Orgánica (MA)	Solidos Volatiles (SV)	Total de Nitrógeno Kjeldahl (TNK)	Demanda Química de Oxígeno (DQO)
Lodo Primario	3.9	69.2	2,7	0.15	14200
Lodo Digerido	2.1	58.3	1.2	0.11	12550

Tabla 2 – Características fisicoquímicas del inóculo y de los lodos activados residuales

2.5. Técnicas Analíticas

Se realizaron análisis de pH, Sólidos Totales (Método 2540B APHA SM), Sólidos Volátiles (Método ASTM D3174), Nitrógeno Kjeldahl (Método ASTM D1426), Demanda Química de Oxígeno (Método ASTM D1252) y Ácidos Grasos Volátiles (Método 5560D APHA SM) respectivamente. El volumen del biogás fue medido mediante el desplazamiento de una solución de NaOH 0.5 N en una trampa de gases, luego este desplazamiento fue medido en ml, usando la técnica volumétrica descrita por Narayani & Gomathi Priya (2012) y Holliger (2016).

Se realizó la medición del porcentaje de metano CH_4 presente en el biogás producido en los días que duró la digestión anaerobia, utilizando el medidor de gases BIOGAS5000 el cual mide la composición y el flujo de gas con precisión, mediante el software LANDTEC System Gas Analyzer Manager (LSGAM).

3. Resultados

Con los datos de producción de Biogás tomados diariamente en el desarrollo del experimento de producción de los ácidos grasos volátiles, se procedió a realizar el análisis de la producción diaria, así como el promedio y el acumulado de BHP para todas las combinaciones realizadas.

Para la presente contribución, se presentan los gráficos de las tendencias de producción de biogás en los experimentos realizados a lodos originarios de la planta de tratamiento de agua residual el Salitre, para la obtención de ácidos grasos volátiles y se seleccionaron las combinaciones de mejor rendimiento para cada tipo de sustrato y carga orgánica. En la tabla 3 se presentan los datos de las combinaciones de las cuales se analiza la producción de biogás.

Tipo de Lodo	N° Combinación	Carga orgánica gSV/L	Temperatura (C°)	pH	Rendimiento
Lodo Digerido	44 47	4 6	45 45	10.5 10.5	5.268 3.684
Lodo Primario	40 20	10 14	45 25	9.5 10.5	4.2648 4.0268

Tabla 3 – Condiciones de los reactores que presentaron los mejores rendimientos

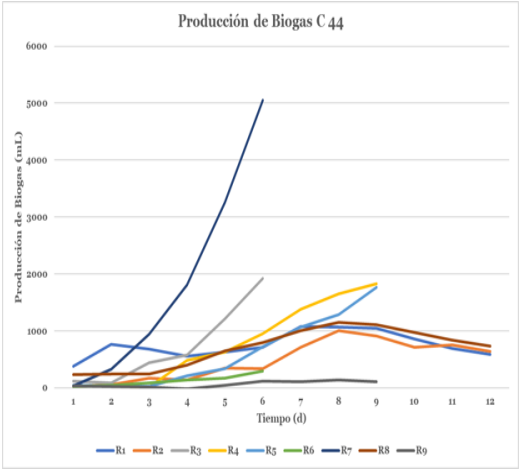


Figura 3a – Producción Acumulada de biogás lodo digerido-6gSV-combinación 44

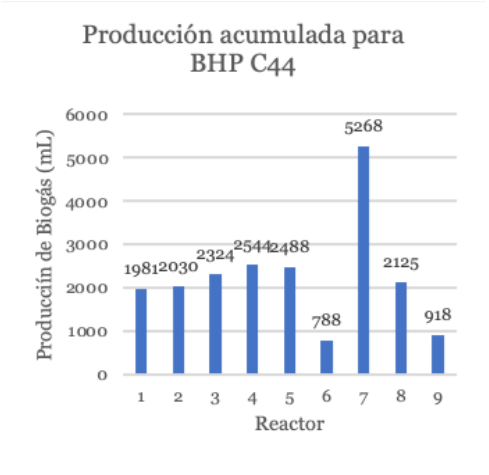


Figura 3b – Producción Acumulada de biogás con corrección de blancos, combinación 44

La combinación 44 de lodo digerido con carga de 6gSV tuvo nueve reactores durante un tiempo de retención hidraúlica de 12 días y los reactores que se mantuvieron durante todo el montaje alcanzaron a acumular hasta 2295 ml de biogás, por su parte los reacores que se destruyeron antes presentaron un comportamiento constante, excepto por el reactor 7 que tuvo una acumulación de biogás superior al promedio, llegando a los 5400 ml. En la figura 3 b se puede observar el cálculo realizado de la acumunación de biogás de cada reactor restando la prducción que tuvieron los reactores blancos o sin lodo.

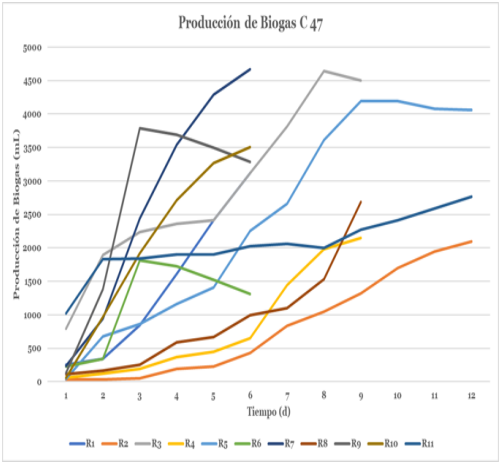


Figura 4a – Producción Acumulada de biogás lodo digerido-4gSV-combinación 47

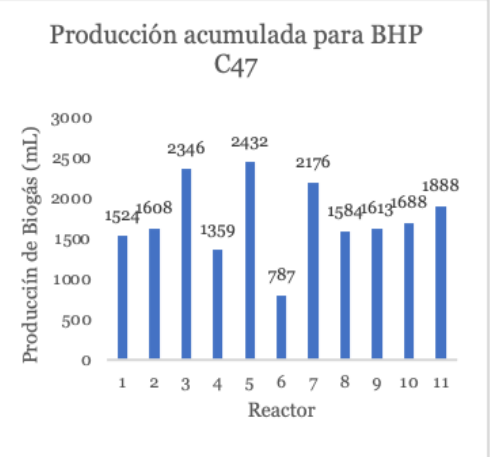


Figura 4b – Producción acumulada de biogás con corrección de blancos, combinación 47

Por su parte la combinación 47 de lodo digerido a 4gSV , presentó un valor acumulado de biogás máximo de 2576 ml en el reactor 5 y los demás reactores presentaron un comportamiento de acumulación que varión entre 1639 y 2477 ml. Así mismo se restó al acumulado diario de producción de biogás la producción promedio de los reactores blancos, encontrando que el reactor 6 presentó la menor acumulación de biogás.

La combinación 40 fue realizada con lodo primario a 10Gsv y presentó una acumulación de biogás de 1477 ml en el reactor 7, en general presenta baja acumulación en todos sus reatores, siendo el reactor 4 el de menor acumulación con 790 ml. Al corregir la acumulación de biogás descontando el valor de la producción de biogás en los blancos se puede evidenciar la tendencia que guarda esta combinación.

Por su parte en la combinación 20, se puede evidenciar el comportamiento de la acumulación del biogás, con producciones por debajo de 1092 ml, e incluso con una muy baja producción de biogás en el reactor tres, que alcanzó un máximo de 191 ml de acumulación en los prmeros tres días. Los anteriores datos tomando la producción acumulada y restando las producción de biogás de los reactores blancos.

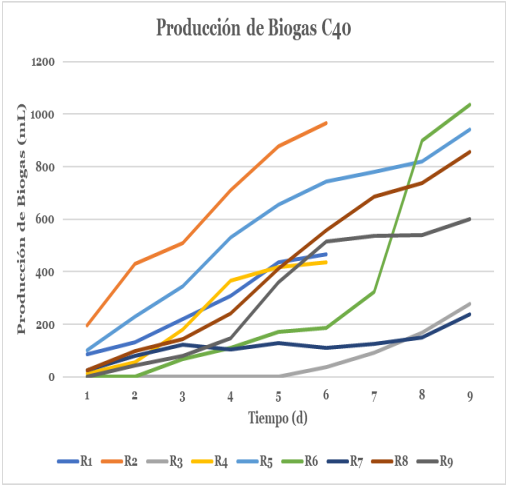


Figura 5a – Producción acumulada de biogás lodo primario-10gSV-combinación 40

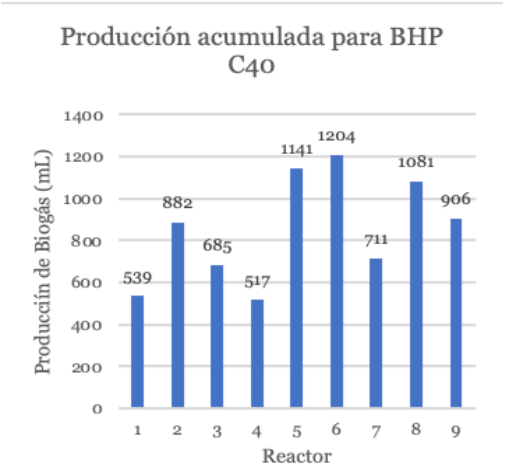


Figura 5b – Producción acumulada de biogás con corrección de blancos, combinación 40

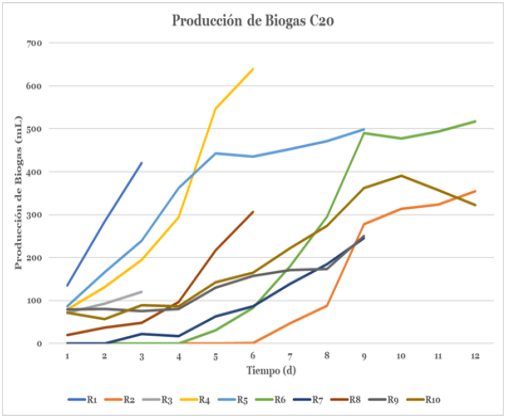


Figura 6a – Producción acumulada de biogás lodo primario-14gSV-combinación 20

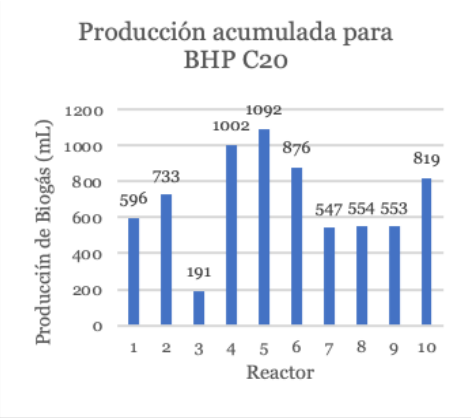


Figura 6b – Producción acumulada de biogás con corrección de blancos, combinación 20

4. Conclusiones

De los resultados obtenidos en las pruebas realizadas se concluyó que teniendo en cuenta únicamente la producción de biogás de los reactores que llegaron hasta el último día, para el caso del lodo primario la producción promedio de biogás varió entre 79,19 ml y 141,7 ml y para el caso del lodo digerido osciló entre 176,67 ml y 185 ml. En cuanto

al valor acumulado del potencial bioquímico de hidrógeno BHP, usando lodo primario estuvo entre 950,3 ml y 1276 ml, para el caso del lodo digerido sus valores estuvieron entre 2215 ml y 2120 ml. Estos resultados de baja producción de biogás demuestran que se el experimento se llevó hasta la fase acidogénica y que se controló con éxito la producción de metano en los reactores, lo que permitió detener la producción a tiempo para que las bacterias acidogénicas y acetogénicas produzcan ácidos grasos volátiles. Sin embargo, se debe prestar atención de la acumulación de estos gases en la producción de pacidos grasos volátiles, en el momento que se realice el escalado de producción a escalas mayores como piloto o industrial.

Referencias

Amador, A., Veliz, L., Eliet; Bataller, Mayra. (2015) Tratamiento de lodos, generalidades y aplicaciones Revista CENIC. Ciencias Químicas, 46, 1-10.

Atasoy, M., Eyice, O., Schnürer, A., Cetecioglu, Z. (2019). Volatile fatty acids production via mixed culture fermentation: revealing the link between pH, inoculum type and bacterial composition. *Bioresourse. Technology*. 292, 1-11. https://doi.org/10.1016/j.biortech.2019.121889

Bhatt, A.H., Ren, Z., Tao, L., (2020). Value proposition of untapped wet wastes: carboxylic acid production through anaerobic digestion. *IScience*. 23 (6), 1-29. https://doi.org/10.1016/j.isci.2020.101221.

Chakraborty, D., Karthikeyan, O.P., Selvam, A., Palani, S.G., Ghangrekar, M.M., Wong, J.W.C. (2022). Two-phase anaerobic digestion of food waste: Effect of semi-continuous feeding on acidogenesis and methane production. *Bioresource Technology*. 346, 1-11. https://doi.org/10.1016/j.biortech.2021.126396

Ekstrand, E., Bjorn, A., Karlsson, A., Kanders, L., Shakeri, S., Karlsson, M., Moestedt, J. (2022). Identifying targets for increased biogas production through chemical and organic matter characterization of digestate from full-scale biogas plants: what remains and why?. *Biotechnology for Biofuels and Bioproducts,* 15(16), 2-22. https://doi.org/10.1186/s13068-022-02103-3

García-Aguirre, J., Esteban, M., Irizar I., González, J., Aymerich, E., 2019. Continuous acidogenic fermentation: Narrowing the gap between laboratory testing and industrial application. *Bioresource Technology*. 282,407-416

Mao, C., Feng, Y., Wang, X., Ren, G. (2015), Review on research achievements of biogas from anaerobic digestion *Renewable and Sustainable Energy Reviews,* 45, pp. 540-555. doi: 10.1016/j.rser.2015.02.032

Molino, A., Nanna, F., Ding, Y., Bikson, B., Braccio, G. (2013). Producción de biometano por digestión anaeróbica de residuos orgánicos. *Combustible,* 103, 1003-1009. doi: 10.1016/j.fuel.2012.07.070

Rodríguez, A., (2014). Viabilidad técnica para producción de biogás a partir de la fracción orgánica de los residuos sólidos urbanos. Trabajo de grado. Universidad EAN, Bogotá.

Orozco, A., (2014) -Bioingeniería de Aguas Residuales. Acodal. Segunda Edición

Owusu, I., Plaza, E., Cetecioglu, Z. (2022) Long-term alkaline volatile fatty acids production from waste streams: Impact of pH and dominance of Dysgonomonadaceae. *Bioresource Technology*. 346, 1-11. https://doi.org/10.1016/j.biortech.2021.126621

Owusu, I., Balachandran, S., Plaza, E., Cetecioglu Z. (2021). Co-fermentation of municipal waste streams: Effects of pretreatment methods on volatile fatty acids production. *Biomass and Bioenergy*. 145. https://doi.org/10.1016/j.biombioe.2020.105950

Ullah Khan, I., Hafiz Dzarfan Othman, M., Hashim, H., Matsuura, T., Ismail, AF, Rezaei-DashtArzhandi, M., Wan Azelee, I. (2017). Biogas as a renewable energy fuel – A review of biogas upgrading, utilisation and storage, *Energy Conversion and Management*. 150, 277-294. https://doi.org/10.1016/j.enconman.2017.08.035

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 12/12/2021
Aceitação/Acceptance: 03/02/2022

Evaluación de riesgos en ciberseguridad: una revisión bibliométrica

Christian Obando-Ibarra[1], Luis Fernando Garcés-Giraldo[1], Jefferson Quiroz-Fabra[2], Martha Benjumea-Arias[2], Alejandro Valencia-Arias[1,3], Luisa Rodríguez Zavala[3], Camilo Patiño-Vanegas[4]

cobando@americana.edu.co; lgarces@americana.edu.co; jeffquirozf@gmail.com; marthabenjumea@itm.edu.co; jvalencia@americana.edu.co; luisa.rodriguez@urp.edu.pe; camilo.patino@ustamed.edu.co

[1] Corporación Universitaria Americana, Cl. 50 #43-65, Medellín, Colombia

[2] Instituto Tecnológico Metropolitano, Departamento de Ciencias Administrativas, Medellín, Colombia.

[3] Universidad Ricardo Palma, 33, Av. Alfredo Benavides 5440, Santiago de Surco 15039, Perú

[4] Universidad Santo Tomas, Cra. 82 #77B-27, 050041, Medellín, Colombia.

Pages: 396-409

Resumen: Pese a los avances técnicos, tecnológicos y científicos en seguridad informática, los diferen tes sistemas informáticos continúan siendo vulnerados con éxito, reflejando vacíos conceptuales y de desarrollo científico. Por tanto, este documento tiene como objetivo identificar la evolución de la temática, sus referentes y sus principales tendencias investigativas. Para ese propósito, se desarrolla un análisis bibliométrico desde la base de datos Scopus entre 2002 hasta la actualidad, siendo analizados los datos a partir de Microsoft Excel y VOSviewer. Los principales resultados reflejan una temática con importante crecimiento exponencial, materializados por autores, revistas e instituciones propias de países desarrollados, que han abordado la temática desde aspectos generales como riesgo, amenaza, seguridad y privacidad. Por ello, se concluye que las principales tendencias investigativas en el tema están marcadas por el desarrollo integral de teorías de juegos, seguridad general computacional, y redes inteligentes, y siempre abarcando el factor humano.

Palabras-clave: Ciberataques; Ciberespacio; Sistemas de seguridad; Scopus; Redes inteligentes.

Risk assessment in cybersecurity: a bibliometric review

Abstract: Despite the technical, technological and scientific advances in computer security, the different computer systems continue to be successfully compromised, reflecting conceptual and scientific development gaps. Therefore, this document aims to identify the evolution of the subject, its references and its main research trends. For this purpose, a bibliometric analysis is developed from the Scopus database between 2002 and the present, the data being analyzed from Microsoft Excel and

VOSviewer. The main results reflect a subject with important exponential growth, materialized by authors, journals and institutions from developed countries, which have approached the subject from general aspects such as risk, threat, security and privacy. Therefore, it is concluded that the main research trends on the subject are marked by the comprehensive development of game theories, general computer security, and intelligent networks, and always encompassing the human factor.

Keywords: Cyberattacks; Cyberspace; Security systems; Scopus; Intelligent networks.

1. Introducción

En los últimos años, la ciencia de datos está revolucionando el contexto informático, lo que ha ocasionado que la ciberseguridad, que cada vez se torna más relevante, haya ocasionado masivos cambios en la tecnología y sus múltiples operaciones (Sarker et al., 2020), teniendo que la evaluación de riesgos desempeña un papel imprescindible para la toma de decisiones efectivas con relación a las estrategias de ciberseguridad que puedan adoptar las organizaciones (Wang, Neil y Fenton, 2020), siendo a su vez relevantes en la gestión de la infraestructura crítica (Mokhor, Gonchar y Dybach, 2019). No obstante, los evaluadores de riesgo se enfrentan a distintos desafíos relacionados con la naturaleza cambiante de los sistemas cibernéticos causados por los avances técnicos, distribución en dominios físicos, y las dificultades en la comprensión de las estructuras de red que, a menudo, incluyen miles de nodos (Ganin et al., 2020), lo que genera que las metodologías de evaluación de riesgos sean diversas y complicadas para el análisis de los investigadores y por tanto existan múltiples definiciones sobre amenaza cibernética (Han y Han, 2021).

Además, teniendo en cuenta que pese a las inversiones en investigación y desarrollo sobre ciberseguridad, los sistemas de información continúan siendo atacados con éxito, ya que, de acuerdo con Hughes y Cybenko (2013), este escaso progreso se debe a que las soluciones técnicas no abordan las compensaciones operativas, los costos de implementación y las adaptaciones del ciberatacante en todo el espectro de vulnerabilidades. Por tanto, algunos autores han establecido los componentes de amenaza, vulnerabilidad y consecuencia como triplete de evaluación de riesgos y han propuesto enfoques basados en decisiones que cuantifican estos componentes (Ganin et al., 2020; Wang, Neil y Fenton, 2020), pese a que autores como Fielder et al. (2018) indiquen la dificultad natural de cuantificar un riesgo. Otros autores han descrito métodos gráficos y analíticos que evalúan el riesgo total de ciberseguridad de los sistemas de información, que se basan en valores máximos de consecuencias para cada riesgo (Mokhor, Gonchar y Dybach, 2019). Finalmente, en la literatura existente se puede evidenciar ausencia de la contribución de los factores humanos en el riesgo de ciberseguridad (King et al., 2018).

Por tanto, existiendo vacíos conceptuales y temáticos en la literatura sobre evaluación de riesgos en ciberseguridad, se torna importante la realización de una bibliometría que permita comprender la evolución de la base intelectual del campo a lo largo del tiempo y los temas principales que contribuyen con su evolución (Sharifi, 2021), para entender, a su vez, como ésta se adapta a las nuevas realidades (Jiménez-García et al., 2020) y permita responder a interrogantes de investigación como: ¿Cómo ha evolucionado el tema? ¿Cuáles son los autores, revistas, instituciones y países más importantes en la

investigación del tema? ¿Cuáles son las temáticas emergentes de las investigaciones sobre evolución de riesgos en ciberseguridad?

2. Metodología

Para el desarrollo de la presente investigación, que es de tipo exploratorio y basada en fuentes secundarias de información, se realizó un análisis bibliométrico, ya que esta metodología es rigurosa en la exploración y análisis de grandes volúmenes de datos científicos y permite, además, identificar los matices evolutivos de un campo específico, así como las áreas emergentes (Donthu et al., 2021). Esta bibliometría se sustenta a partir de la información indexada en la base de datos Scopus ya que es una de las principales bases de datos bibliográficas en el suministro de metadatos e indicadores bibliométricos (Pranckutė, 2021). Para esto, se realizó una ecuación de búsqueda especializada, que relacionara las diferentes formas de indagar la temática de ciberseguridad, y a su vez, se limitara exclusivamente en el segmento del análisis de riesgos; la ecuación de búsqueda es la siguiente:

TITLE(cybersecurity OR {cyber security} OR “cyber-security”) AND (LIMIT-TO (EXACTKEYWORD, “Risk Assessment”)

Al realizar la búsqueda, se obtuvo un total de 508 resultados, comprendidos en el periodo de tiempo entre 2002 y 2022, lo que da a entender que es una temática relativamente reciente en la base de datos. Estos documentos fueron analizados primeramente por la herramienta ofimática de Microsoft Excel®, ya que de acuerdo con Teng et al. (2019) es una de las principales herramientas de análisis de datos que se dispone en la actualidad, siendo complementada, posteriormente, por el software de código abierto VOSviewer, ya que permite identificar las diferentes redes que estructuran los datos bibliográficos con facilidad de uso y múltiples características, como técnicas de agrupamiento (Orduña-Malea y Costas, 2021).

3. Resultados

La presente revisión bibliométrica de la actividad científica sobre evaluación de riesgos en la ciberseguridad, indexada en la base de datos Scopus, tiene como objetivo responder a múltiples preguntas de investigación detalladas en la introducción. Para ese propósito, la Figura 1 da respuesta concreta a la primera pregunta de investigación sobre la evolución del tema, ya que evidencia gráficamente el volumen de publicaciones históricamente. En ese sentido, se pueden observar dos aspectos fundamentales en la figura: el primero, es la cantidad propia de publicaciones en cada año entre 2002 y 2022, teniendo un comportamiento relativamente variable, aunque sin importantes variaciones, donde se posiciona el año 2021 como el año donde mayor número de publicaciones se han registrado, con un total de 91 publicaciones; para el 2022, se han registrado 5 publicaciones, donde la más reciente apunta un acontecimiento previamente dicho: existe un volumen bajo de publicaciones que señalen el aumento y complejidad de las amenazas e incidentes cibernéticos (van der Kleij et al., 2022).

Un segundo aspecto que se puede identificar por medio de la Figura 1, es el comportamiento tendencial de crecimiento de la temática, por medio de una cantidad

acumulada que refleje la cantidad de publicaciones totales que se tiene en un periodo de tiempo específico, comprendido entre 2002 y 2022; este comportamiento, a su vez, fue comparado con una línea de crecimiento exponencial, cuya correlación con la cifra real presenta un coeficiente de correlación o R2 de 0,9622, que, de acuerdo con la escala de medidas establecida por Ratner (2009), indica una fuerte relación positiva entre las variables.

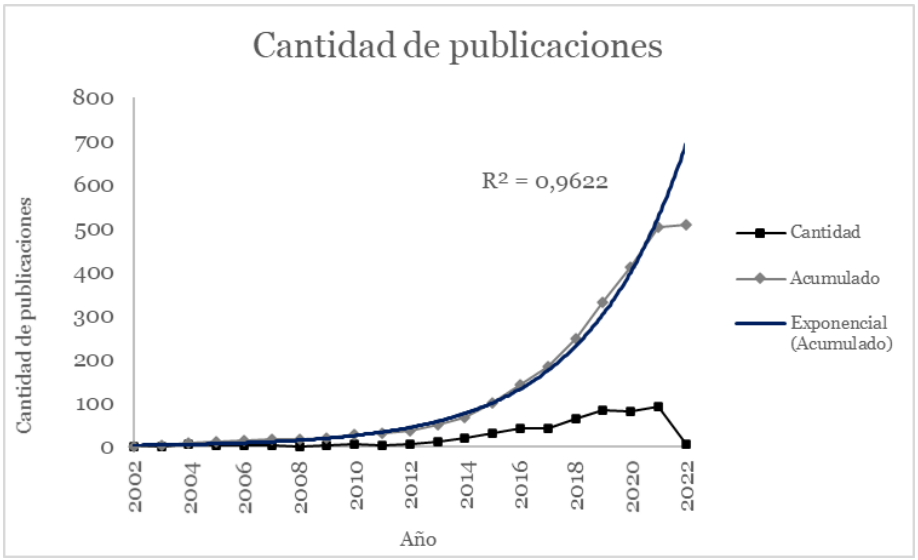


Figura 1 – Cantidad de publicaciones

Los indicadores bibliométricos, son esas leyes de la bibliometría que permiten cuantificar la producción científica e intentar evaluar su impacto en la comunidad científica (García-Villar y García-Santos, 2021), de modo que se proporcione una visión general de las investigaciones que se tienen de un campo específico (Noman et al., 2019). En ese sentido, se tienen los indicadores de calidad que evalúan el impacto de las publicaciones a partir de la cuantificación de las citaciones, así como los indicadores de cantidad que miden la productividad científica a partir del número de publicaciones.

En ese sentido, por medio de la Tabla 1, se puede observar el listado de los diez principales autores en términos de impacto académico y su respectiva productividad científica, de forma que se pueda realizar una comparación entre el número de citaciones y el número de publicaciones. En ese sentido, se tiene que el principal autor en términos de impacto en la actualidad es el inglés Kevin Jones, con un total de 464 citaciones; no obstante, estas citaciones se encuentran distribuidas en únicamente 2 publicaciones, por lo que el autor no se encuentra entre los más productivos académicamente en la temática. Este autor se ha enfocado en investigaciones relacionadas a los métodos de evaluación de riesgo de ciberseguridad; específicamente, su publicación más importante consta en una revisión detallada de veinticuatro métodos de evaluación de riesgo distintos aplicados en el contexto de un sistema de supervisión, control y adquisición de datos (Cherdantseva

et al., 2016). Finalmente, cabe destacar que ninguno de los autores considerados mayormente relevantes en términos de impacto, se encuentra en el ranking de los más productivos en la temática.

			Impacto		Productividad	
N	**Autor**	**País**	**Citaciones**	**Ranking**	**Publicaciones**	**Ranking**
1	Kevin Jones	Reino Unido	464	1	2	98
2	Pete Burnap	Reino Unido	295	2	2	57
3	Andrew Blyth	Reino Unido	293	3	1	300
4	Yulia Cherdantseva	Reino Unido	293	4	1	366
5	Peter Eden	Reino Unido	293	5	1	463
6	Hugh Soulsby	Reino Unido	293	6	1	1221
7	Kristan Stoddart	Reino Unido	293	7	1	1240
8	David Hutchison	Reino Unido	185	8	2	92
9	James H. Graham	Estados Unidos	180	9	1	568
10	Jeffrey L. Hieb	Estados Unidos	180	10	1	626

Tabla 1 – Impacto y productividad por autor

Bajo la misma aplicabilidad de los indicadores bibliométricos de calidad y de cantidad, pero a partir de un espectro diferente, la Tabla 2 refleja el listado de las principales revistas de divulgación científica en términos de impacto o de cuantificación de citaciones, al tiempo que compara su productividad científica en términos de publicaciones. En ese orden de ideas, se tiene que la revista que en la actualidad da cuenta de un mayor número acumulado de citaciones es la revista inglesa Computers and Security, la cual posee una categorización Q1 de acuerdo con el indicador de SCImago de Elsevier y encuentra explicación a tal impacto gracias a la publicación del artículo anteriormente descrito (ver explicación de la Tabla 1). Esta revista, con un total de 399 citaciones, se encuentra también en el top 10 de revistas más productivas en investigaciones sobre evaluación de riesgo en ciberseguridad, con un total de 8 publicaciones.

Cabe destacar que entre las diez revistas más relevantes en términos de calidad o impacto académicos, cuatro de ellas también integran el ranking de las diez revistas científicas con mayor productividad en investigaciones afines a la temática, donde la revista alemana Lecture Notes in Computer Science, que se encuentra actualmente en la octava posición de relevancia con 68 citaciones, es a su vez la revista académica con mayor productividad académica. Esta revista se ha enfocado en la divulgación de materiales en todas las áreas de la informática, y su publicación más importante presenta un análisis de riesgos de ciberseguridad por medio de métodos de inteligencia computacional (Wang et al., 2010).

			Índice SCOPUS	Impacto		Productividad	
N	**Revista**	**País**		**Citaciones**	**Ranking**	**Publicaciones**	**Ranking**
1	Computers and Security	Reino Unido	Q1	399	1	8	6
2	Risk Analysis	Reino Unido	Q1	287	2	12	3
3	ISA Transactions	Estados Unidos	Q1	180	3	1	232
4	International Journal of Critical Infrastructure Protection	Holanda	Q2	171	4	2	40
5	Transport Reviews	Reino Unido	Q1	149	5	1	349
6	IEEE Transactions on Systems, Man, and Cybernetics: Systems	Estados Unidos	Q1	80	6	1	207
7	Proceedings of the IEEE	Estados Unidos	Q1	70	7	2	54
8	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Alemania	Q3	68	8	23	1
9	Reliability Engineering and System Safety	Reino Unido	Q1	61	9	1	321
10	IEEE Access	Estados Unidos	Q1	59	10	12	2

Tabla 2 – Impacto y productividad por revista

Entre los principales resultados, también se encontró una categorización de las instituciones que, en la actualidad, dan cuenta de un mayor número total de citaciones en sus publicaciones sobre evaluación del riesgo en ciberseguridad, y su respectivo

posicionamiento en el ranking de productividad científica, reflejados a partir de la Tabla 3. En ese sentido, se puede apreciar que la institución que en la actualidad posee mayor relevancia académica es la University of Louisville de Estados Unidos, con un total de 362 citaciones, de las cuáles 180 provienen de un artículo que proporciona una descripción general sobre la seguridad cibernética y su evaluación de riesgos (Ralston, Graham y Hieb, 2007). No obstante, esta universidad, con un total de 3 publicaciones afines a la temática central, no se encuentra dentro de las principales instituciones en términos de productividad científica.

En ese sentido, es importante destacar que, si bien existen dos instituciones que integran el listado de las más importantes en términos de impacto y términos de productividad, se destaca la institución china Huazhong University of Science and Technology, que posee un total de 143 citaciones, distribuidas entre 8 publicaciones, lo que la hace octava en el ranking de impacto y primera en el de productividad académica. Esta institución ha enfocado sus publicaciones de evaluación de riesgos en ciberseguridad hacia los sistemas de control industrial, donde de hecho, su publicación más relevante propone una red bayesiana multinivel específica que contiene modelos de ataque, función e incidente adoptados en los sistemas de control industrial (Zhang et al., 2015).

			Impacto		Productividad	
N	**Institución**	**País**	**Citaciones**	**Ranking**	**Publicaciones**	**Ranking**
1	University of Louisville	Estados Unidos	362	1	3	41
2	Cardiff University	Gales	295	2	3	22
3	Aberystwyth University	Gales	293	3	1	125
4	University of South Wales	Gales	293	4	1	490
5	Lancaster University	Reino Unido	199	5	3	30
6	University of Virginia	Estados Unidos	197	6	7	3
7	National University of Singapore	Singapur	149	7	1	337
8	Huazhong University of Science and Technology	China	143	8	8	1
9	Center for Risk Management of Engineering Systems	Estados Unidos	94	9	2	46
10	Southwestern Oklahoma State University	Estados Unidos	80	10	1	382

Tabla 3 – Impacto y productividad por institución

Finalmente, con relación al contexto de los indicadores bibliométricos mencionados previamente, se tiene la categorización en escala de países, donde, por medio de la Tabla 4, se comparan los países que han poseído una mayor relevancia en términos de calidad académica, y su respectivo posicionamiento en la medición de productividad científica. En ese sentido, se puede evidenciar que el país más importante en investigaciones sobre evaluación de riesgos en seguridad cibernética es Estados Unidos, que, con un total de 1406 citaciones y 176 publicaciones, lidera los dos listados. Son múltiples los enfoques que han presentado los estudios en el contexto estadounidense, sin embargo, su publicación más reciente tiene como objetivo añadir un nuevo concepto a las discusiones actuales como es el de huella de ciberseguridad (Levy y Gafni, 2021).

Es imprescindible mencionar que los tres principales países en términos de impacto son, a su vez, los tres principales países en términos de productividad científica en el mismo orden, donde se encuentran Reino Unido y China en segunda y tercera posición respectivamente. Se destaca para el contexto inglés la investigación de los autores Knowles et al. (2015), que traza una agenda investigativa sobre métricas de seguridad de sistemas de control industrial, y para el contexto chino se destaca una revisión del estado de la ciberseguridad de los sistemas de control industrial, realizada por los autores Peng et al. (2012).

			Impacto		**Productividad**	
N	**País**	**Continente**	**Citaciones**	**Ranking**	**Publicaciones**	**Ranking**
1	Estados Unidos	América	1406	1	176	1
2	Reino Unido	Europa	851	2	66	2
3	China	Asia	255	3	39	3
4	Singapur	Asia	157	4	4	23
5	Corea del sur	Asia	134	5	14	6
6	Alemania	Europa	86	6	19	4
7	Canadá	América	66	7	4	20
8	Suecia	Europa	66	8	5	18
9	España	Europa	59	9	15	5
10	Italia	Europa	52	10	12	8

Tabla 4 – Impacto y productividad por país

Complementariamente al análisis de la producción científica en evaluación de riesgos cibernéticos a la escala de países, se presenta la Figura 2 que indica la red de coautoría que han tenido los países para la investigación. Es importante mencionar que toda red de coautoría hace parte de los indicadores de estructura bibliométrica, ya que éstos analizan las conexiones en la actividad científica (Alshater, Atayah y Hamdan, 2021). En ese sentido, se puede evidenciar que se presenta una importante cantidad de conexiones de coautoría, que da indicios sobre las pocas conexiones consolidadas. Se tiene que, si bien no es el clúster temático que abarque más países, el rojo se posiciona como el más importante, siendo compuesto exclusivamente por Estados Unidos, pero presentando

relacionamiento directo con la mayoría de los clústeres temáticos, entre ellos el verde y el amarillo, que son los dos clústeres más numerosos.

El clúster verde, representado por China, Corea del Sur, Hong Kong y Australia, ha dado como resultado diferentes investigaciones que han abordado algunos modelos cuantitativos para la evaluación de riesgos de seguridad cibernética, en ese sentido, se tiene que la más reciente producción científica producto de esa cooperación, propuso un modelo basado en una red bayesiana para evaluar dinámica y cuantitativamente el riesgo de los sistemas de control de supervisión y adquisición de datos (Huang et al., 2017). Por otro lado, el clúster amarillo, compuesto por Reino Unido, Grecia, Emiratos Árabes Unidos y Chipre, dio origen a una reciente investigación que planteó el marco SECONDO con el objetivo de apoyar a las organizaciones con las decisiones relacionadas sobre inversión en seguridad y seguros cibernéticos (Farao et al., 2020).

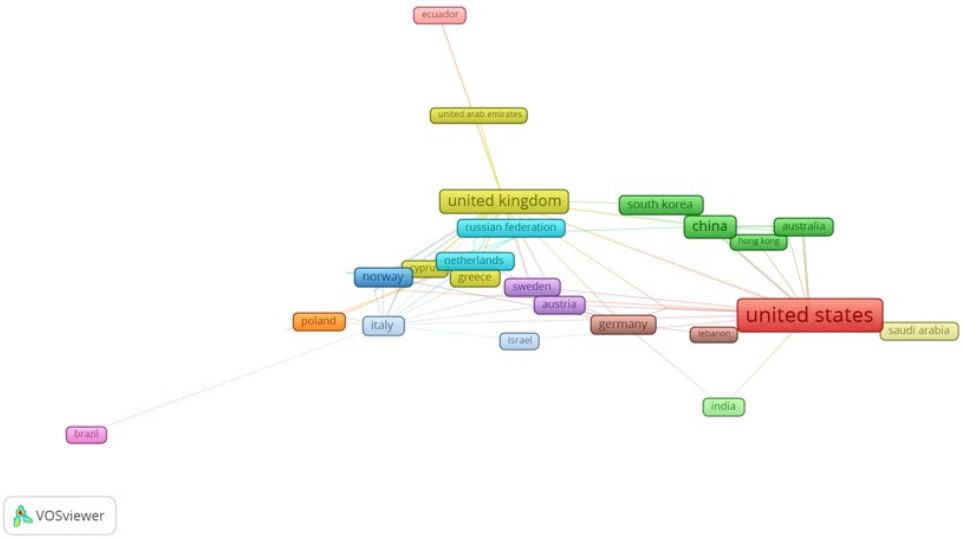


Figura 2 – Red de coautoría de países

Un segundo componente característico de los indicadores bibliométricos de estructura es el análisis de la red de coocurrencia de palabras clave, que indican la frecuencia en que dos o más palabras clave aparecen comunes o tienen uso frecuente en el contexto específico de una investigación (Lozano et al., 2019), obteniendo un total de 5 clústeres temáticos que son detallados en la Figura 3. El principal clúster temático con relación a la cantidad de palabras clave, es el clúster verde, que relaciona los aspectos generales de la ciberseguridad como Información de Seguridad, Amenaza, Riesgo, Seguridad, Privacidad y Política de seguridad; de hecho, todas estas palabras claves coinciden en un estudio reciente que tuvo como objetivo mostrar cómo se puede resolver la creación de un plan de riesgos con la ayuda de un método multicriterio constructivista (Moreira et al., 2021).

En segunda posición de relevancia se encuentran los clústeres rojo y azul, con un total de 5 términos relacionados respectivamente. El clúster rojo se caracteriza por abordar subtemas más técnicos como las Redes Bayesianas, el Internet de las Cosas o la Seguridad Funcional; mientras que el clúster azul aborda los factores relacionados con la ciberseguridad, como el Factor Humano, el Ciberespeacio, la Vulnerabilidad o la Evaluación del Riesgo Cibernético. Posteriormente se tienen los clústeres amarillo y morado, con tres términos relacionados cada uno. El clúster amarillo se enfoca principalmente en todo lo concerniente a la Seguridad Computacional, o la Teoría del Juego, mientras que el clúster morado relaciona las Vulnerabilidades producto de los Ciberataques en las Redes Inteligentes.

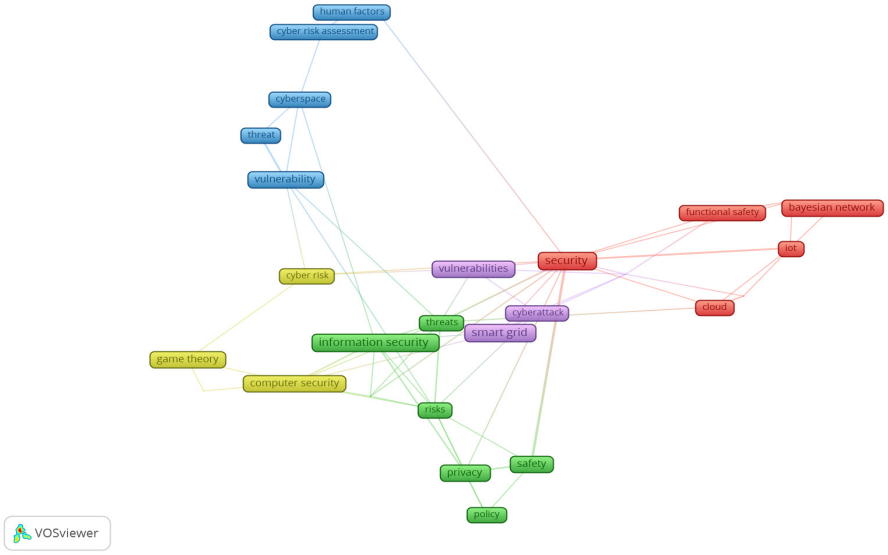


Figura 3 – Red de coocurrencia de palabras clave

4. Conclusiones

Los resultados de la presente investigación permiten concluir que la evaluación del riesgo en la seguridad cibernética o ciberseguridad hace parte de una temática que, dada su importancia entre los nuevos avances técnicos, tecnológicos y científicos, se encuentra en crecimiento constante desde el año 2002 hasta la actualidad; este crecimiento, además, se presenta de forma exponencial, lo que permite concluir también que es una temática que, al no encontrar aún saturación investigativa, continuará en crecimiento, explicado por el desarrollo de métodos de identificación de riesgos, amenazas y vulnerabilidades en el ciberespacio por medio de redes bayesianas o el aprovechamiento del internet de las cosas.

Por otro lado, el análisis bibliométrico permitió reconocer que los autores más importantes en términos de impacto científico, no coinciden con los autores de mayor

productividad académica; particularidad que no coincide con lo evidenciado a la altura de revistas, instituciones o países, ya que se visualizan siempre los más importantes en términos de citaciones, pero, a su vez, algunos de ellos encabezan el ranking de productividad, lo que permite concluir que, si bien es importante contar con un buen volumen de publicaciones en la temática, éstas no son garantía exclusiva de su calidad, por lo que se sugiere a otros autores, especializarse en las temáticas emergentes y así estar a la vanguardia de la temática.

A su vez, se pudo evidenciar que el abordaje de las investigaciones sobre evaluación del riesgo en ciberseguridad se encuentra mayormente desarrollado en el contexto de países desarrollados, lo que se puede notar a partir de la nacionalidad de los autores, del país al que pertenecen las revistas o instituciones, o, en general, en los países donde se ve un mayor desarrollo de la temática, por lo que se puede concluir que es necesario ampliar el volumen y la calidad de las publicaciones sobre evaluación de riesgos en ciberseguridad para el contexto de países en desarrollo, de modo tal que éstas reflejen las características y necesidades que existen a partir del nivel de desarrollo técnico, tecnológico y científico propio del contexto de estos países, y así ampliar la literatura sobre la temática de forma integral.

Con relación a las tendencias investigativas en la temática, se puede observar que, si bien existen algunos aspectos generales que explican la evolución de la temática y que fueron apuntados recientemente, se pueden observar algunas otras temáticas emergentes como el análisis completo de la Seguridad Computacional, la Teoría del Juego o las Redes Inteligentes, que siendo estudiadas en conjunto con las características del factor humano, pueden ser importantes para analizar de forma completa todas las amenazas, riesgos o vulnerabilidades que pueden existir en el ciberespacio, lo que puede ser útil no solo para investigadores, sino para organizaciones en general, que se pueden apropiar de la construcción de conocimiento científico, e incrementar la seguridad cibernética en sus operaciones y en sus procesos de transformación digital, que debe, necesariamente, verse implicados en una sólida política de seguridad informática.

Referencias

Alshater, M. M., Atayah, O. F., & Hamdan, A. (2021). Journal of Sustainable Finance and Investment: A bibliometric analysis. *Journal of Sustainable Finance & Investment*, 1-22. https://doi.org/10.1080/20430795.2021.1947116

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, 1-27. https://doi.org/10.1016/j.cose.2015.09.009

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*, 285-296. https://doi.org/10.1016/j.jbusres.2021.04.070

Farao, A., Panda, S., Menesidou, S. A., Veliou, E., Episkopos, N., Kalatzantonakis, G., ... & Xenakis, C. (2020). SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In *International Conference on Trust and Privacy in Digital Business* (pp. 65-74). Springer, Cham. https://doi.org/10.1007/978-3-030-58986-8_5

Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk assessment uncertainties in cybersecurity investments. *Games*, *9*(2), 34. https://doi.org/10.3390/g9020034

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), 183-199. https://doi.org/10.1111/risa.12891

García-Villar, C., & García-Santos, J. M. (2021). Bibliometric indicators to evaluate scientific activity. *Radiología (English Edition)*, *63*(3), 228-235. https://doi.org/10.1016/j.rxeng.2021.01.002

Han, C. H., & Han, C. (2021). Semi-quantitative cybersecurity risk assessment by blockade and defense level analysis. *Process Safety and Environmental Protection*, *155*, 306-316. https://doi.org/10.1016/j.psep.2021.09.028

Huang, K., Zhou, C., Tian, Y. C., Tu, W., & Peng, Y. (2017). Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)* (pp. 1-6). IEEE. https://doi.org/10.1109/ATNAC.2017.8215355

Hughes, J., & Cybenko, G. (2013). Quantitative metrics and risk assessment: The three tenets model of cybersecurity. *Technology Innovation Management Review*, *3*(8). http://doi.org/10.22215/timreview/712

Jiménez-García, M., Ruiz-Chico, J., Peña-Sánchez, A. R., & López-Sánchez, J. A. (2020). A bibliometric analysis of sports tourism and sustainability (2002–2019). *Sustainability*, *12*(7), 2840. https://doi.org/10.3390/su12072840

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in psychology*, *9*, 39. https://doi.org/10.3389/fpsyg.2018.00039

Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. *Information & Computer Security*, *28*(5), 724-736. https://doi.org/10.1108/ICS-04-2020-0054

Lozano, S., Calzada-Infante, L., Adenso-Díaz, B., & García, S. (2019). Complex network analysis of keywords co-occurrence in the recent efficiency analysis literature. *Scientometrics*, *120*(2), 609-629. https://doi.org/10.1007/s11192-019-03132-w

Mokhor, V., Gonchar, S., & Dybach, O. (2019). Methods for the total risk assessment of cybersecurity of critical infrastructure facilities. *Ядерна та радіаційна безпека*, (2 (82)), 4-8. https://doi.org/10.32918/nrs.2019.2(82).01

Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., de Sousa Júnior, R. T., & Nunes, R. R. (2021). Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology. *IEEE Access*, *9*, 129605-129618. https://doi.org/10.1109/ACCESS.2021.3113178

Noman, M. A., Nasr, E. S. A., Al-Shayea, A., & Kaid, H. (2019). Overview of predictive condition based maintenance research using bibliometric indicators. *Journal of King Saud University-Engineering Sciences*, *31*(4), 355-367. https://doi.org/10.1016/j.jksues.2018.02.003

Orduña-Malea, E., & Costas, R. (2021). Link-based approach to study scientific software usage: The case of VOSviewer. *Scientometrics*, *126*(9), 8153-8186. https://doi.org/10.1007/s11192-021-04082-y

Peng, Y., Jiang, C., Xie, F., Dai, Z., Xiong, Q., & Gao, Y. (2012). Industrial control system cybersecurity research. *Journal of Tsinghua University Science and Technology*, *52*(10), 1396-1408. Disponible en: https://en.cnki.com.cn/Article_en/CJFDTotal-QHXB201210014.htm

Pranckutė, R. (2021). Web of Science (WoS) and Scopus: The Titans of Bibliographic Information in Today's Academic World. *Publications*, *9*(1), 12. https://doi.org/10.3390/publications9010012

Ralston, P. A., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA transactions*, *46*(4), 583-594. https://doi.org/10.1016/j.isatra.2007.04.003

Ratner, B. (2009). The correlation coefficient: Its values range between+ 1/− 1, or do they?. *Journal of targeting, measurement and analysis for marketing*, *17*(2), 139-142. https://doi.org/10.1057/jt.2009.5

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, *7*(1), 1-29. https://doi.org/10.1186/s40537-020-00318-5

Sharifi, A. (2021). Urban sustainability assessment: An overview and bibliometric analysis. *Ecological Indicators*, *121*, 107102. https://doi.org/10.1016/j.ecolind.2020.107102

Teng, C., Reveles, K. R., Obodozie-Ofoegbu, O. O., & Frei, C. R. (2019). Clostridium difficile infection risk with important antibiotic classes: an analysis of the FDA adverse event reporting system. *International journal of medical sciences*, *16*(5), 630. https://dx.doi.org/10.7150%2Fijms.30739

van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. *Computers & Security*, *113*, 102535. https://doi.org/10.1016/j.cose.2021.102535

Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*, *89*, 101659. https://doi.org/10.1016/j.cose.2019.101659

Wang, Y., Ruan, D., Xu, J., Wen, M., & Deng, L. (2010). Computational intelligence algorithms analysis for smart grid cyber security. In *International Conference in Swarm Intelligence* (pp. 77-84). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13498-2_11

Zhang, Q., Zhou, C., Xiong, N., Qin, Y., Li, X., & Huang, S. (2015). Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *46*(10), 1429-1444. https://doi.org/10.1109/TSMC.2015.2503399

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 06/12/2021
Aceitação/Acceptance: 08/02/2022

Tendencias investigativas en el uso de tecnologías de Big Data en sistemas de ciberseguridad

Luis Fernando Garcés-Giraldo[1], Martha Benjumea-Arias[2], Olga Inés Vélez Bernal[3], Alejandro Valencia-Arias[1,4], Luis Tadeo Celi Saavedra[5], Camila Bermeo-Giraldo[6], Jefferson Quiroz-Fabra[2]

lgarces@americana.edu.co; marthabenjumea@itm.edu.co; viceacademica@iumafis.edu.co; jvalencia@americana.edu.co; lcelis@usmp.edu.pe; cies2@escolme.edu.co; jeffquirozf@gmail.com

[1] Corporación Universitaria Americana, Cl. 50 #43-65, Medellín, Colombia

[2] Instituto Tecnológico Metropolitano, Departamento de Ciencias Administrativas, Medellín, Colombia.

[3] Institución Universitaria Marco Fidel Suárez., Cl 48 #Nº 50-30, Bello, Colombia

[4] Universidad Ricardo Palma, 33, Av. Alfredo Benavides 5440, Santiago de Surco 15039, Perú

[5] Universidad San Martín de Porres, Jr. Las, Calandrias N° 151 – 291, Santa Anita 15011, Perú

[6] Institución Universitaria Escolme, Cl. 50 ##40-39., Medellín, Colombia

Pages: 410-420

Resumen: El incesante avance tecnológico producto del internet e Internet de las Cosas, ha traído grandes avances informáticos, así como diferentes retos en términos de ciberseguridad, razón por la cual el presente estudio tuvo como objetivo identificar las principales tendencias investigativas alrededor de estudios que abordaran el uso de tecnologías de Big Data en sistemas de ciberseguridad e identificar las claves para una agenda investigativa. Por tanto, se elaboró un análisis bibliométrico en la base de datos de Scopus, obteniendo un total de 169 registros entre 2012 y 2022, los cuales permitieron identificar que los principales autores y revistas, han abordado palabras clave como Inteligencia Artificial, Big Data Analytics, Deep Learning y Machine Learning, entre otros, lo cuál las ha posicionado entre los principales subtemas derivados de la temática central, constituyéndose como factores claves de investigación futura de una temática reciente.

Palabras-clave: Bibliometría; Inteligencia Artificial; Deep Learning; Machine Learning; Blockchain.

Research trends in the use of Big Data technologies in cybersecurity systems

Abstract: The incessant technological advance product of the Internet and Internet of Things, has brought great computer advances, as well as different challenges in terms of cybersecurity, which is why the present study aimed to identify the main research trends around studies that address the use of Big Data technologies in

cybersecurity systems and identify the keys for an investigative agenda. Therefore, a bibliometric analysis was carried out in the Scopus database, obtaining a total of 169 records between 2012 and 2022, which allowed us to identify that the main authors and journals have addressed keywords such as Artificial Intelligence, Big Data Analytics, Deep Learning and Machine Learning, among others, which has positioned them among the main subtopics derived from the central theme, becoming key factors for future research on a recent theme.

Keywords: Bibliometrics; Artificial Intelligence; Deep Learning; Machine Learning; Blockchain.

1. Introducción

En los últimos años, los innumerables desarrollos de las tecnologías de la información han revolucionado la forma en que las personas hacen uso del internet (Zhang y Ghorbani, 2021), lo cuál ha generado un aumento cada vez más acelerado en la generación de datos, originando diferentes desafíos para el uso de análisis de big data de cara a la construcción o mejoramiento de los sistemas de ciberseguridad (Alani, 2021) por lo que se han desarrollado diferentes sistemas que aprovechan las tecnologías de big data para proteger las redes, equipos y datos de las organizaciones (Ullah y Babar, 2019).

Este contexto responde a las características inherentes a la Cuarta Revolución Industrial o Industria 4.0, cuyo componente fundamental alude al uso de tecnologías como Internet de las cosas, impresión 3D, realidad aumentada, computación en la nube, entre muchos otros, con fines industriales (Rymarczyk. 2020), que, por medio de la generación constante de grandes volúmenes de datos, tiene la capacidad de modificar por completo los procesos productivos como se conocen en la actualidad (Da costa et al., 2019).

Algunos autores argumentan que los datos son un reflejo del entorno en el que se producen, por lo que ellos pueden ayudar a entender el funcionamiento de ese sistema (Rawat, Doku y Garuba, 2019), y dados los desarrollos tecnológicos y la integración de múltiples objetos a internet, hace que los datos sean complejos en sus procesos de adquisición, análisis, almacenamiento, clasificación y transferencia, dando cuenta de la importancia que tiene el Big Data para el desarrollo integral de las tecnologías en la Industria 4.0 (Ansari et al., 2015).

lo cual es entendido por los atacantes maliciosos que analizan las diferentes vulnerabilidades para lanzar ataques cibernéticos y realizar diferentes actividades fraudulentas en línea (Zhang y Ghorbani, 2021), haciendo cada vez más relevante el estudio y aplicación del Big data para el desarrollo de sistemas de ciberseguridad que tengan como objetivo la protección permanente de los activos (Rawat, Doku y Garuba, 2019). Tales sistemas de ciberseguridad o seguridad cibernética hacen alusión a la gestión que las organizaciones adelantan para no vulnerar su información ante la existencia de múltiples riesgos en el contexto de la interconexión, garantizando un nivel óptimo de seguridad en su infraestructura informática (Lykou et al., 2018)

Sin embargo, pese al incremento de la importancia de la temática producto del rápido crecimiento del Internet, Internet de las cosas y otros avances tecnológicos (Rawat, Doku y Garuba, 2019), así como el reconocimiento de la trascendencia de la interoperabilidad, adaptabilidad y garantía de privacidad, aún existen vacíos de investigación teórica y

empírica sobre algunos aspectos técnicos (Ullah y Babar, 2019) por lo que esta carencia de información justifica la importancia inicial de una revisión bibliográfica sobre el estado actual de la temática, así como de sus principales autores, revistas, países y tendencias investigativas derivadas del tema central.

2. Metodología

De acuerdo con el propósito de la investigación, se realiza un estudio exploratorio, basado en fuentes secundarias de información, a partir de un análisis bibliométrico, ya que este método permite evaluar y analizar la producción científica (Moral-Muñoz et al., 2020), que a su vez sirve como insumo principal para el desarrollo de las preguntas de investigación planteadas. La base de datos seleccionada para el desarrollo del estudio es Scopus, ya que se posiciona actualmente como una de las principales bases de datos científicas (Kimmons, Rosenberg y Allman, 2021) y que, así mismo, se posiciona entre las principales bases de datos de indexación de información sobre las tendencias tecnológicas en el marco de la Cuarta Revolución Industrial, como se refleja en Parlina, Ramli y Murfi (2020) quienes revisaron de forma general la información contenida en la base de datos sobre Big Data. A partir de esta fuente de información, se establecen unos criterios de inclusión sobre los estudios que en el título de los registros bibliográficos hablaran sobre Ciberseguridad, y que, de forma exacta, entre las palabras clave que delimitan el contenido de la temática, se encontrara Big Data, de modo tal que se relacionaran directamente los conceptos para dar forma a las características de la investigación. En ese sentido, se ingresó la siguiente ecuación especializada de búsqueda:

TITLE (cybersecurity OR {cyber security} OR “cyber-security”) AND (LIMIT-TO (EXACTKEYWORD, “Big Data”))

Tal ecuación, que relacionó todos los modos de búsqueda del equivalente en inglés de ciberseguridad, limitándose únicamente a todos los aspectos relacionados con Big Data, tal y como se estableció en los criterios de inclusión, obtuvo un total de 178 resultados de forma inicial, que fueron sometidos a criterios de exclusión como registros duplicados o indexados de forma errónea por la base de datos, reduciendo la cantidad a 169 registros, donde el registro más antiguo ubicado en la base de datos es del año 2012, mientras que el documento más reciente data del año 2022. Estos registros fueron analizados a partir de la herramienta ofimática de Microsoft Excel® así como del software de código abierto VOSviewer, donde este último se convierte fundamental para el análisis de las redes de coocurrencia de palabras clave de los autores según la información bibliográfica (Al-Ashmori, Othman y Rahmawati, 2020); a su vez, para el desarrollo de la investigación, se plantean algunos indicadores bibliométricos de calidad o impacto, que se implementan a partir de la cuantificación de las citaciones que tienen los documentos (Elango, 2019) y que permitieran responder a los interrogantes de investigación como: ¿cuáles son los enfoques dados por los principales autores? ¿dónde se concentra la discusión sobre la temática? ¿cuáles son las tendencias investigativas que trazan las principales agendas para futuros trabajos?

3. Resultados

Uno de los principales propósitos de la presente investigación, consistió en la identificación de las tendencias investigativas sobre el uso de tecnologías de Big Data en

sistemas de ciberseguridad, lo cuál implica a su vez, identificar la frecuencia investigativa y determinar, con ello, si se trata de una temática en crecimiento, y de presentarse, analizar el tipo de crecimiento. En ese sentido, por medio de la Figura 1, se puede identificar, por un lado, el volumen de publicaciones anuales, donde son los años 2018 y 2019 los dos años con un mayor número de publicaciones, con 38 y 37 documentos respectivamente, reflejando también, de forma gráfica, la curva de crecimiento acumulado.

Por otro lado, en la misma Figura 1, se puede realizar una comparación entre la curva de crecimiento acumulado encontrada, con la Ley de crecimiento de Price, que de acuerdo con lo indicado por Díaz, Reche y Rodríguez (2018) significa que en los primeros diez años la literatura debe duplicarse, distribuyéndose en etapas de precursores (fase inicial de la literatura), crecimiento exponencial (auge en la producción), crecimiento lineal (consolidación de la temática) y límite de saturación de la temática. En ese sentido, teniendo en cuenta que la información alojada en la base de datos de Scopus sobre la temática tiene una antigüedad de diez años únicamente, se encontró que el crecimiento es más acelerado, ya que no solo se duplica la temática, sino que incrementaría en un 169%. Este alejamiento con respecto a la Ley de Price se puede evidenciar a partir del Valor inicial en la gráfica.

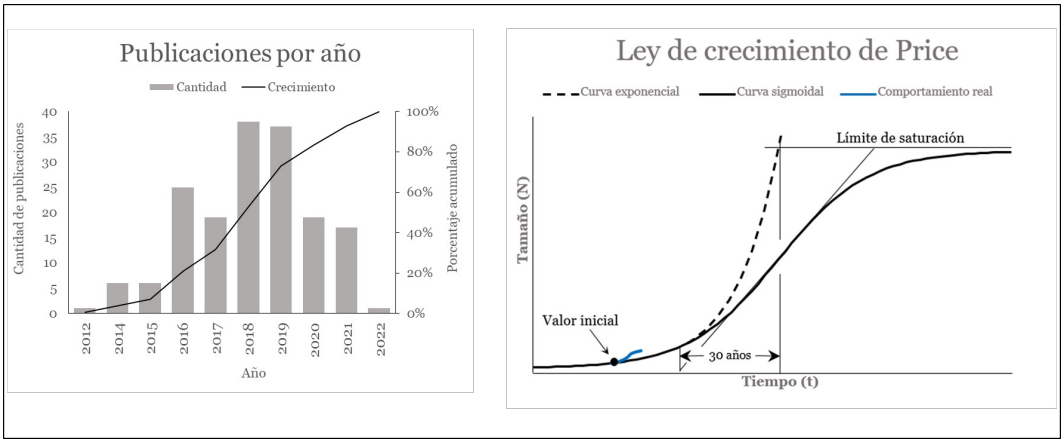


Figura 1 – Publicaciones por año y Ley de crecimiento de Price

A su vez, de acuerdo con la metodología planteada en la investigación, se realizan indicadores bibliométricos de calidad, con el propósito de identificar los principales autores en la temática en términos de cantidad de citaciones. Por eso, por medio de la Figura 2 se identifican los 15 autores con más citas acumuladas, convirtiéndolos en los más importantes en términos de impacto científico. En ese sentido, se puede identificar que existen 10 autores en primera posición, con un total de 91 citaciones; esto se debe a que son coautores de un documento que tuvo como objetivo presentar un sistema operativo de detección de amenazas cibernéticas a partir de aprendizaje automático y minería de datos, proporcionando un servicio importante para los ciberdefensores (Nunes et al., 2016).

Por otra parte, la Figura 2 también permite realizar un análisis comparativo de la estructura de las citaciones, con la Ley de Lotka, que permite analizar la frecuencia de citaciones de los autores (Ichhpujani et al., 2020). En ese sentido, se puede observar que si bien se sigue un patrón relativamente semejante, la estructura de esta literatura científica permite evidenciar que no se cumple con la Ley de Lotka, ya que el 2,97% de los autores, posee el 80% de las citaciones. De forma más global, se tiene que el 0,28% de los autores da cuenta del 25% de citas en el campo, el 0,92% posee el 50% de citaciones en investigaciones sobre el uso de tecnologías de Big Data en sistemas de ciberseguridad, mientras que, por último, el 2,48% da cuenta del 75% del total de citaciones en el área, lo que explica la centralización del impacto, en una fracción corta de autores.

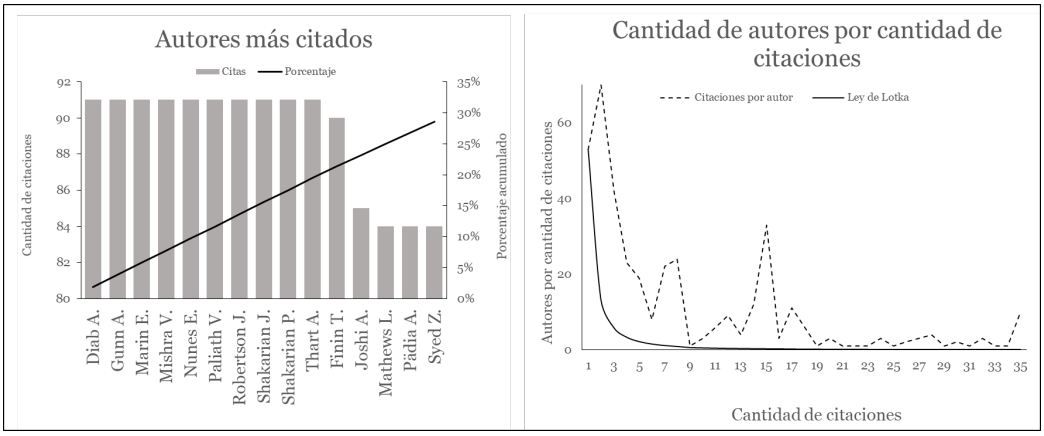


Figura 2 – Autores más citados y cantidad de autores por cantidad de citaciones

Adicionalmente, el presente estudio plantea el mismo indicador bibliométrico de calidad en la escala de las revistas, de modo que la cuantificación de las citaciones permitiese identificar cuáles son las revistas top en la temática, es decir, que cuentan con mayores índices de impacto. En ese sentido, por medio de la Figura 3, se pueden evidenciar dos aspectos relevantes: en primer lugar, las 8 revistas con mayor número total de citaciones, y en segundo lugar, la distribución de citaciones comparada contra la Ley de Lotka. Por ello, se puede identificar que es la revista holandesa Procedia Computer Science, con un total de 90 citaciones, la revista que da cuenta de un mayor impacto académico; esta revista se especializa en la publicación de estudios sobre las ciencias de la computación informática, lo cuál se evidenció en su última publicación sobre la temática donde enfatizan que todo sistema de detección de intrusos de seguridad cibernética debe procesar datos de tráfico de red de gran tamaño lo más rápido posible para detectar el tráfico malicioso lo antes posible (Gupta y Kulariya, 2016). Se destacan otras revistas como AAAI Workshop - Technical Report y Journal of Manufacturing Systems, con un total de 88 y 41 citaciones respectivamente.

Desde otra perspectiva, como se mencionó previamente, se tiene que el 0,28% de las revistas cuentan con el 25% del total de citaciones, el 0,96% de revistas poseen el 50% de citas en investigaciones sobre el uso de tecnologías de Big Data en sistemas de

ciberseguridad, mientras que el 3,03% da cuenta del 75% del total de citaciones. Además, teniendo que el 3,85% de revistas posee el 80% de citas, se evidencia que no se cumple con la distribución mencionada en la Ley de Lotka, cuyos comportamientos se comparan gráficamente por medio de la Figura 3.

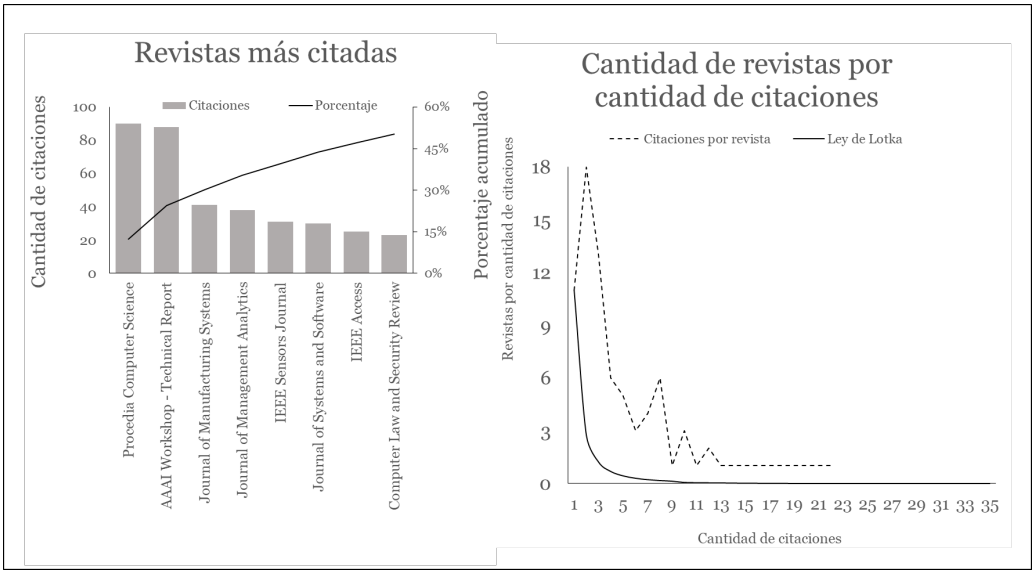


Figura 3 – Revistas más citadas y cantidad de revistas por cantidad de citaciones

Algunos autores como Sanderson, Braby y Bond (2021) han enfatizado en los últimos años sobre la necesidad de distribuir social y globalmente la ciencia. En ese sentido, se extrapolan los términos de los resultados anteriores, a una escala de países, de modo tal que lo evidenciado permita analizar sobre el posicionamiento de la relevancia en la discusión sobre Big Data y ciberseguridad. Por ello, por medio de la Figura 4, se posicionan los 10 países que, en la actualidad, poseen un mayor número total de citaciones en el campo, donde se identifica a Estados Unidos como el país con más relevante en la temática, con un total de 556 citaciones, que equivalen a un 51% sobre el total de estas; donde, si bien para el contexto estadounidense se pueden hallar investigaciones con múltiples enfoques, las investigaciones más recientes tienden al análisis de tecnologías como el Blockchain, donde autores como Demirkan, Demirkan y McKee (2020) la han categorizado como clave para el futuro de la ciberseguridad y otros asuntos organizacionales como la contabilidad empresarial. Se destacan otros países como Reino Unido, Italia y Australia, con 85, 80 y 69 citaciones de manera respectiva.

En segundo término, la Figura 4 permite analizar el comportamiento de la distribución de citaciones entre los países, con lo establecido por la mencionada Ley de Lotka. Por tanto, teniendo en cuenta lo dicho previamente con relación al porcentaje de citaciones sobre el total que posee Estados Unidos (51%), así como el hecho de que el 0,55% del total de países que han investigado sobre los usos de tecnologías de Big Data en sistemas

de ciberseguridad poseen el 80% de las citaciones, se puede observar que tampoco se cumple con la mencionada ley. Esta distribución se puede observar en la comparación gráfica, donde las citaciones por país siguen un comportamiento diferente al establecido en la Ley de Lotka.

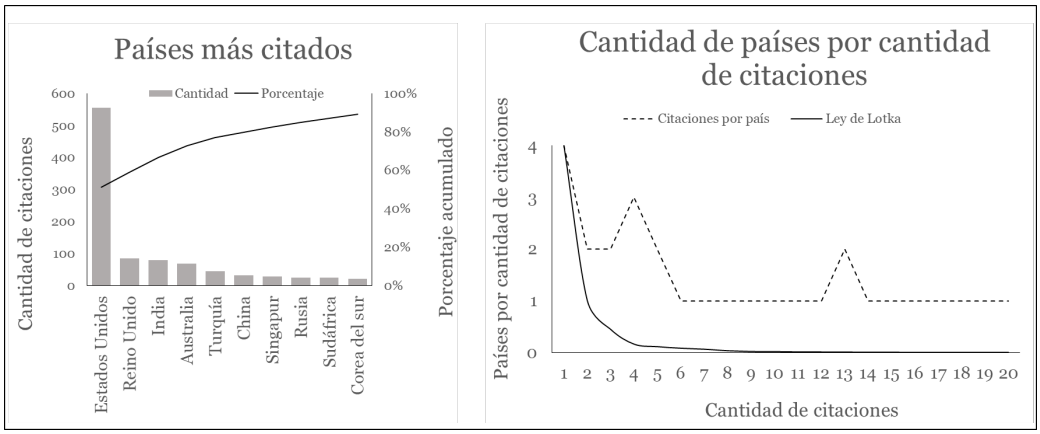


Figura 4 – Países más citados y cantidad de países por cantidad de citaciones

Pasando del análisis de los indicadores bibliométricos de calidad a la escala de autores, revistas y países, el presente estudio investigativo tiene como propósito identificar las líneas temáticas que permitan complementar el abordaje sobre las tendencias investigativas, encontrando, a su vez, los subtemas crecientes, decrecientes y aquellos que emergen a partir de un periodo específico. En ese sentido, por medio de la Figura 5, se identifica por un lado que solo se encuentra un tema decreciente como lo es el de Big Data Analytics, es decir, que en el periodo entre 2019 y 2022 ha sido investigado con menor frecuencia que en el periodo comprendido entre 2012 y 2018, sin desconocer su importancia para procesar, almacenar y recopilar grandes cantidades de datos para su futuro análisis (Rawat, Doku y Garuba, 2019). A su vez, se pueden identificar diferentes términos crecientes, es decir, que entre el último periodo analizado se ha estudiado más recurrentemente, como lo son Deep Learning, Machine Learning e Intrusion Detection, entre otros. Estas palabras clave, en conjunto, fueron abordadas por Wang y Jones (2019) quienes enfatizaron la importancia de la detección temprana de intrusos en redes informáticas para la ciberseguridad por medio de algunas tecnologías de Big Data.

Estos últimos términos en mención son analizados a profundidad en la segunda parte de la Figura, donde se puede evidenciar que Big Data Analytics es el término que ha sido abordado desde mayor anterioridad, y que en el último año se posicionó como la palabra clave mayormente estudiada por los autores, teniendo en segunda posición el término de Artificial Intelligence, y luego Deep Learning y Machine Learning en tercera posición. Por último, se tienen algunos subtemas categorizados como emergentes, es decir, que no fueron abordados entre 2012 y 2018, pero surgieron en la literatura a partir del año 2019, como lo son Anomaly Detection, Cyber-Physical Systems y Artificial Intelligence,

siendo este último el concepto más frecuente en los estudios sobre tecnologías de Big Data en sistemas de ciberseguridad, por lo que puede ser fundamental como tendencia investigativa.

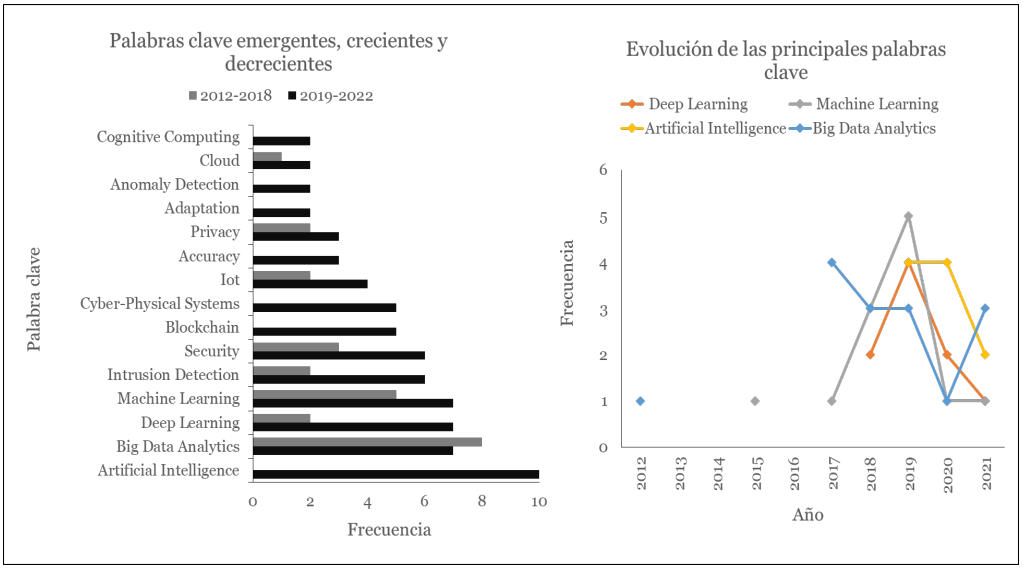


Figura 5 – Principales palabras clave y su evolución

Finalmente, con relación a los resultados del presente análisis bibliométrico, por medio del software VOSviewer se analiza la red de coocurrencia de palabras clave, que de acuerdo con Al-Zaman (2021) hace referencia a la frecuencia con que son utilizadas conjuntamente dos o más palabras claves por los autores. En ese sentido, se tiene que la red de coocurrencia en los trabajos sobre el uso de tecnologías de Big Data en sistemas de ciberseguridad se ve compuesta por un total de cuatro clústeres temáticos como se aprecia en la Figura 6, caracterizados individualmente con un color específico. Por tanto, se tiene que el principal clúster temático es el rojo, que, compuesto por un total de cinco palabras clave, se enfoca en aspectos como Machine Learning, Information Security, y Data Mining. El segundo clúster temático, posicionado en el centro de la red, es el clúster azul, que relaciona conceptos fundamentales como Artificial Intelligence, Intrusion Detection y Deep Learning, que fueron evidenciados previamente como tres de los conceptos fundamentales en la discusión alrededor de la temática (Ver Figura 5).

En la parte inferior, se tiene el clúster temático verde, que relaciona dos conceptos identificados previamente, como Blockchain y Big Data Analytics, en conjunto con Cloud Computing. Finalmente, en la parte superior de la red, se posiciona el clúster amarillo, que se enfoca en la utilización conjunta de conceptos como IoT (Internet of Things) y Cyber-Physical Systems, siendo el primero un concepto creciente, y el segundo uno emergente, identificados en la Figura 5.

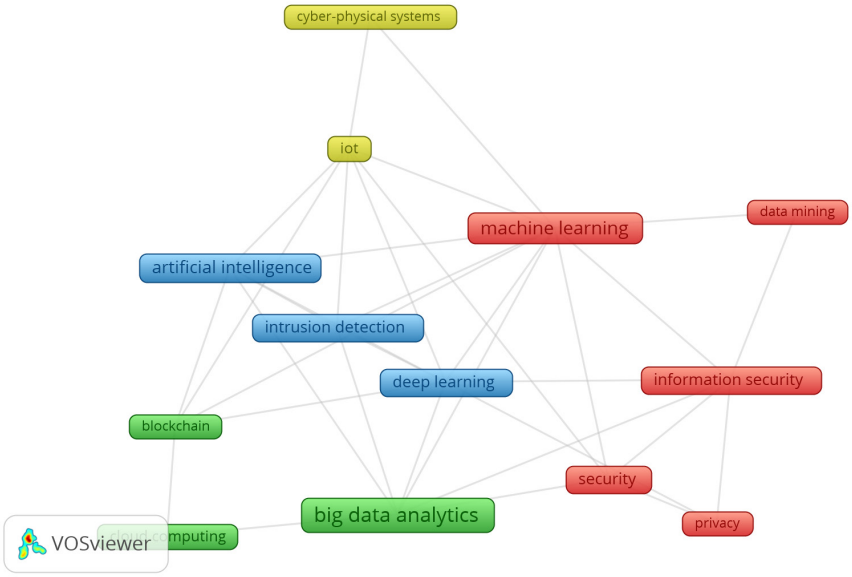


Figura 6 – Red de coocurrencia de palabras clave

4. Conclusiones

A partir de los resultados de la presente investigación, en primer término se puede concluir que, si bien es una temática reciente en la base de datos de Scopus, es una temática que ha presentado un crecimiento más acelerado de lo esperado o proyectado a partir de algunos modelos como la Ley de crecimiento de Price, lo que da cuenta de la relevancia de la temática en las diferentes discusiones informáticas y tecnológicas actuales, a partir del alcance, las posibilidades y las oportunidades que plantean las tecnologías de Big Data para el robustecimiento de los sistemas de ciberseguridad.

Por otro lado, el estudio bibliométrico, que permitió identificar los principales autores y revistas alrededor de la producción científica sobre la temática, permite concluir que su relevancia y trascendencia académica, se debe, a parte de su rigor investigativo, por el abordaje de conceptos muy pertinentes alrededor de la discusión general, como lo son la detección temprana de intrusos o de ciberataques por medio de diferentes metodologías que usan Big Data, así como Inteligencia Artificial, Internet de las Cosas, Machine Learning y demás dinámicas resaltadas; este aspecto da respuesta a la primera pregunta de investigación, con relación a los enfoques dados por los principales autores.

La segunda pregunta de investigación apuntaba al posicionamiento de la discusión, es decir, a los principales contextos donde se abordaban los estudios sobre el uso de tecnologías de Big Data en sistemas de ciberseguridad, por lo que a partir de los resultados de la bibliometría, se concluye que es una temática bastante centralizada, donde se tuvo a Estados Unidos como el gran protagonista, siendo el país más relevante

en términos de impacto científico, con más de la mayoría de citaciones en el campo, y concentrándose en el desarrollo conceptual de aplicaciones de tecnologías de Blockchain para las organizaciones.

Además, se concluye que las tendencias investigativas se perfilan hacia el abordaje de temáticas como Inteligencia Artificial, Big Data Analytics, Deep Learning, o Machine Learning, como los principales conceptos derivados de las investigaciones sobre Big Data y Ciberseguridad, los cuales trazan la agenda investigativa para el desarrollo de una temática que se está consolidando y que su desarrollo teórico, y sobre todo, su aplicación práctica o empírica, pueden resultar en grandes avances técnicos, tecnológicos, informáticos y científicos de cara a los sistemas de seguridad cibernética, ante la multiplicidad de factores de vulnerabilidad que subsisten y emergen en todo el ciberentorno.

Referencias

Alani, M. M. (2021). Big data in cybersecurity: a survey of applications and future trends. *Journal of Reliable Intelligent Environments*, 1-30. https://doi.org/10.1007/s40860-020-00120-3

Al-Ashmori, Y. Y., Othman, I., & Rahmawati, Y. (2020). Bibliographic analysis of BIM success factors and other BIM literatures using Vosviewer: a theoretical mapping and discussion. In *Journal of Physics: Conference Series* (Vol. 1529, No. 4, p. 042105). IOP Publishing. http://dx.doi.org/10.1088/1742-6596/1529/4/042105

Al-Zaman, M. (2021). A bibliometric and co-occurrence analysis of COVID-19–related literature published between December 2019 and June 2020. *Science Editing*, *8*(1), 57-63. https://doi.org/10.6087/kcse.230

Ansari, S., Mohanlal, R., Poncela, J., Ansari, A., & Mohanlal, K. (2015). Importance of big data. In *Handbook of research on trends and future directions in big data and web intelligence* (pp. 1-19). IGI Global. https://doi.org/10.4018/978-1-4666-8505-5.ch001

Da Costa, M. B., Dos Santos, L. M. A. L., Schaefer, J. L., Baierle, I. C., & Nara, E. O. B. (2019). Industry 4.0 technologies basic network identification. *Scientometrics*, *121*(2), 977-994. https://doi.org/10.1007/s11192-019-03216-7

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189-208. https://doi.org/10.1080/23270012.2020.1731721

Díaz, I. A., Reche, M. P. C., & Rodríguez, J. M. R. (2018). Efecto de la metodología mobile learning en la enseñanza universitaria: meta-análisis de las investigaciones publicadas en WOS y Scopus. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (30), 1-16. https://doi.org/10.17013/risti.30.1–16

Elango, B. (2019). A bibliometric analysis of literature on engineering research among BRIC countries, *Collection and Curation*, 38*(1)*, 9-14. https://doi.org/10.1108/CC-05-2017-0017

Gupta, G. P., & Kulariya, M. (2016). A framework for fast and efficient cyber security network intrusion detection using apache spark. *Procedia Computer Science*, *93*, 824-831. https://doi.org/10.1016/j.procs.2016.07.238

Ichhpujani, P., Kalra, G., Kaur, R., & Bhartiya, S. (2020). Evolution of Glaucoma Research: A Scientometric Review. *Journal of Current Glaucoma Practice*, *14*(3), 98. https://dx.doi.org/10.5005%2Fjp-journals-10078-1286

Kimmons, R., Rosenberg, J., & Allman, B. (2021). Trends in educational technology: What Facebook, Twitter, and Scopus can tell us about current research and practice. *TechTrends*, 1-12. https://doi.org/10.1007/s11528-021-00589-6

Lykou, G., Anagnostopoulou, A., Stergiopoulos, G., & Gritzalis, D. (2018, September). Cybersecurity self-assessment tools: evaluating the importance for securing industrial control systems in critical infrastructures. In *International Conference on Critical Information Infrastructures Security* (pp. 129-142). Springer, Cham. https://doi.org/10.1007/978-3-030-05849-4_10

Moral-Muñoz, J. A., Herrera-Viedma, E., Santisteban-Espejo, A., & Cobo, M. J. (2020). Software tools for conducting bibliometric analysis in science: An up-to-date review. http://dx.doi.org/10.3145/epi.2020.ene.03

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., ... & Shakarian, P. (2016). Darknet and deepnet mining for proactive cybersecurity threat intelligence. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 7-12). IEEE. https://doi.org/10.1109/ISI.2016.7745435

Parlina, A., Ramli, K., & Murfi, H. (2020). Theme mapping and bibliometrics analysis of one decade of big data research in the scopus database. *Information*, *11*(2), 69. https://doi.org/10.3390/info11020069

Rawat, D. B., Doku, R., & Garuba, M. (2019). Cybersecurity in big data era: From securing big data to data-driven security. *IEEE Transactions on Services Computing*. https://doi.org/10.1109/TSC.2019.2907247

Rymarczyk, J. (2020). Technologies, opportunities and challenges of the industrial revolution 4.0: theoretical considerations. *Entrepreneurial business and economics review*, *8*(1), 185-198.

Sanderson, C., Braby, M. F., & Bond, S. (2021). Butterflies Australia: a national citizen science database for monitoring changes in the distribution and abundance of Australian butterflies. *Austral Entomology*, *60*(1), 111-127. https://doi.org/10.1111/aen.12513

Ullah, F., & Babar, M. A. (2019). Architectural tactics for big data cybersecurity analytics systems: a review. *Journal of Systems and Software*, *151*, 81-118. https://doi.org/10.1016/j.jss.2019.01.051

Zhang, X., & Ghorbani, A. A. (2021). Human factors in cybersecurity: Issues and challenges in big data. *Research Anthology on Privatizing and Securing Data*, 1695-1725. https://doi.org/10.4018/978-1-7998-8954-0.ch082

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 20/10/2021
Aceitação/Acceptance: 10/01/2022

Definición de Estrategia de Encadenamientos Productivos para el Desarrollo Económico del Municipio de Pore-Casanare

Elkin Olaguer Pérez Sánchez[1], Mauricio Antonio Bedoya Villa[2], Jesus Manuel Ramos Garcia[3], María Quisphi González[4], Patricia Eugenia Escobar Martínez[5], Francisco Javier Arias Vargas[6]

mbedoya@udemedellin.edu.co; eoperez@udemedellin.edu.co; jmrg@azc.uam.mx; proyectos@cstar.com.co

[1]Profesor asociado, Facultad de Ciencias Económicas y Administrativas, Universidad de Medellín, Antioquia, Colombia.

[2]Profesor asociado, Facultad de Ciencias Económicas y Administrativas, Universidad de [3]Medellín, Antioquia, Colombia.

[4]Profesor investigador, Departamento de Administración, Universidad Autónoma Metropolitana Azcapotzalco, México.

[5]Investigador, Centro de Desarrollo Tecnológico C-Star, Casanare, Colombia.

[6]Investigador, Centro de Desarrollo Tecnológico C-Star, Casanare, Colombia.

Pages: 421-435

Resumen: De acuerdo con la unión europea, la bioeconomía es la capacidad de transformar el conocimiento de las ciencias de la vida en productos nuevos, sostenibles, ecoeficientes y competitivos. Lo que permite cerrar los ciclos biológicos, generando proyectos que ayuden a la identificación de actores claves en economía circular y cambio climático. El objetivo del artículo es presentar en el contexto de la bioeconomía, los encadenamientos productivos más promisorios del municipio de Pore a partir las potencialidades productivas en el sector agroindustrial que se puedan desarrollar en el municipio, y que puedan facilitar la construcción de ventajas competitivas. Los resultados permiten concluir que se identificaron dos grandes líneas, orientadas la primera a mantener la producción y construir diferentes encadenamientos en el tiempo, haciendo más eficiente el rendimiento por hectárea y la segunda plantea la oferta de nuevos productos, a partir del aprovechamiento por hectárea de la región.

Palabras-clave: Encadenamiento, agroindustria, productividad, desarrollo.

Definition of Chain Strategy Productive for the Economic Development of the Municipality of Pore-Casanare

Abstract: According to the European Union, the bioeconomy is the ability to transform knowledge from life sciences into new, sustainable, eco-efficient and competitive products. This allows closing the biological cycles, revealing projects

that help identify key actors in the circular economy and climate change. The objective of the article is to present, in the context of the bioeconomy, the most promising productive chains of the municipality of Pore based on the productive potentialities in the agro-industrial sector that can be developed in the municipality, and that can facilitate the construction of competitive advantages. The results allow us to conclude that two large lines were identified, the first aimed at maintaining production and building different chains over time, making the yield per hectare more efficient, and the second raises the offer of new products, based on the use per hectare of the region.

Keywords: Chain, agroindustry, productivity, development.

1. Introducción

Uno de los aspectos más importantes del municipio de Pore, es el reconocimiento de sus fortalezas geográficas, hídricas y culturales, las cuales le han permitido posicionarse como patrimonio cultural, no solo a nivel nacional, sino latinoamericano. Pese a ello las demandas globales, nacionales y locales exigen que los municipios diversifiquen su producción a partir de la identificación de los productos que pueden ayudarles a ser más competitivos. (Drucker, 2002)

El articulo surge en el marco del proyecto "construcción de un modelo para la generación de empresas innovadoras en la zona industrial del municipio de Pore, con el fin de apoyar la reactivación económica en el marco de la postpandemia, para el fortalecimiento de vocaciones en CTeI", presentado en la convocatoria No. 891 de 2020, mecanismo 2, del Ministerio de Ciencia Tecnología e Innovación. El objetivo general es a partir de la identificación de los productos más promisorios del municipio inferir cuales son los potenciales encadenamientos productivos en el sector agroindustrial que se puedan desarrollar en el municipio de Pore, entendiendo encadenamientos productivos como "un conjunto de actores económicos asociados en la cadena de valor de un producto, que interactúan entre sí para obtener beneficios en conjunto y aumentar sus niveles de competitividad". (Pérez Pravia, M.C., Vega De La Cruz, 2021), buscando, a partir de los encadenamientos el aumento de la competitividad del municipio. Uno de los aspectos a superar, son los vacíos de otras producciones que plantean cifras y estadísticas a nivel departamental, sin lograr mostrar de manera concreta la información de cada municipio.

En las investigaciones realizadas sobre el rol de los encadenamientos productivos en el desarrollo económico de las regiones, se ha podido constatar que estos permiten conocer algunos aspectos operativos, tales como los eslabones que los conforman, los productos y las unidades productivas, los procesos y actividades, y la articulación en el espacio territorial. Insertarse en un encadenamiento productivo contribuye a aumentar y mejorar la distribución del ingreso en las economías territoriales, aumenta el intercambio de información, mejora la transferencia de tecnología y el desarrollo de conocimiento y facilita darles respuesta a los requerimientos de la demanda, aumentando los niveles de competitividad de los diferentes actores y eslabones de la cadena, en especial la agricultura (González A, Prego Regalado J.C., Robaina Echevarría L, 2020; Padilla Pérez, R., & Oddone, N, 2016; DNP, 2016; OCDE,2016).

El documento se construye con base en la pregunta de investigación ¿cuáles son los encadenamientos productivos más promisorios del municipio de Pore?, a partir de la

pregunta se plantea como objetivo central, el identificar con base en la revisión de agendas y políticas públicas vigentes y del trabajo con grupos focales, los encadenamientos productivos más promisorios del municipio, dejando claro que no se trata de un ejercicio de identificación de tendencias o de prospección frente a cual es el potencial crecimiento de los renglones de producción agroindustrial actual del municipio, sino un ejercicio que busca identificar cuales son los productos que potencialmente pueden permitir que el municipio construya capacidades que le ayuden a la generación de ventajas competitivas sostenibles.

2. Contexto del municipio de Pore

El municipio de Pore se encuentra ubicado a 5°43´ latitud norte y 72°00´ longitud occidental; con una altitud de 250 M.S.N.M. y geográficamente se localiza en la zona norte del Departamento de Casanare, se encuentra a 71 km de la capital departamental, Yopal, y a 436 km de Bogotá (Plan de desarrollo 2020-2023). La división político-administrativa actual del municipio de Pore, en el área urbana está compuesta por 9 barrios (Plan de desarrollo 2020-2023).

Según los datos del Plan de Desarrollo 2020-2023, la población total del municipio en el año 2019 era 11.968 habitantes, de los cuales 7, 403 están ubicados en el casco urbano y 4.565, se encuentran en la zona rural. Del total de la población el 51.4% son hombres y el 48.4% son mujeres, en la actualidad el municipio no cuenta con certificación en materia educativa, la educación se imparte en 3 Instituciones educativas que tienen 19 sedes. No existen Instituciones de Educación Superior (Plan de desarrollo 2020-2023).

En el sector salud, en el Municipio de Pore se encuentran dos (2) IPS con servicios de baja complejidad habilitados, (1) IPS de carácter público – Centro de Salud de Pore y una IPS de carácter privada – Coomedican, las enfermades que mas inciden en los índices de mortalidad del municipio son: Enfermedades del sistema circulatorio, con un 33,07% del total de fallecimientos, las causas externas con el 22,67% y las Neoplastias con el 14, 93%.

En lo relacionado con el cambio climático, el municipio sufre afectaciones especialmente con las temporadas de lluvias inesperadas, ya que las conexiones erradas de aguas lluvias son la causa del desbordamiento del alcantarillado sanitario en los eventos de lluvia, por cuanto aportan grandes caudales y el alcantarillado sanitario no tiene la capacidad hidráulica para transportar estos caudales.

La sedimentación en las tuberías de aguas lluvias debe ser retirada para no disminuir la capacidad hidráulica del sistema, el plástico y basura botados por la comunidad en las calles y lotes son arrastrados por la lluvia. De igual forma no hay rutas selectivas de reciclaje.

En el municipio no se ha realizado un censo de puntos críticos en el área urbana, para determinar cuáles áreas son más vulnerables a la disposición inadecuada de residuos sólidos y en cuales se generan más residuos sólidos urbanos, para mejorar y ampliar la calidad del servicio en estos sectores. Según la comunidad, uno de estos puntos críticos, es la zona de protección del Rio Pauto. Un dato importante es que en promedio el Municipio de Pore produjo 100ton/mes de residuos sólidos en el año 2019. (Plan de

desarrollo 2020-2023). El municipio de Pore está regado por los ríos Guachiría, Pore, Pauto y numerosos caños y quebradas como La Curama, La Sequí, La Colorada y Caño chiquito (Rojas L. H. 1997).

En lo relacionado con el sector agrícola, los principales renglones de la producción agrícola se dividen en cultivos de ciclo permanente, cultivos de ciclo anual, cultivos de ciclo transitorio -tradicional, cultivos de ciclo transitorio- tecnificado y el cultivo de arroz, con un tratamiento especial. Como puede observarse hasta acá, es amplia la problemática del municipio en las áreas sociales, culturales, económicas y ambientales, lo cual demanda estrategias de intervención de mediano plazo. El artículo, presenta un ejercicio de planeación con enfoque territorial, en el cual se utilizaron como fuente la revisión de las políticas y agendas publicas vigentes, la identificación de las apuestas locales y las reuniones realizadas con las agremiaciones y cultivadores del municipio, para el análisis de la información tomada de las fuentes mencionadas se construyó una matriz FODA como puede verificarse en la figura 1, teniendo en cuenta dimensiones económico-políticas, socio-culturales, ambientales y político- institucionales.



Figura 1 – Matriz DOFA, del municipio de Pore.

2.1. Referentes conceptuales

A pesar de que el tema agroindustrial es de amplio manejo en la literatura tanto local, nacional e internacional, se presenta a modo de reflexión algunos de los conceptos usados en el desarrollo del proceso de investigación que da como resultado la elaboración del presente artículo.

Inicialmente es necesario comprender la agroindustria rural como "la actividad que permite aumentar y retener en las zonas rurales, el valor agregado de la producción de las economías campesinas a través de la ejecución de las tareas de postcosecha en los productos procedentes de explotaciones tales como la selección, el lavado, la clasificación, el almacenamiento, la conservación, la transformación, el empaque. El transporte y la comercialización" (agroindustria rural, Pag 26). Importante explicitar que la agroindustria rural, tiene un contexto especifico en el campo de las regiones más alejadas y que en la mayoría de las oportunidades es desarrollado por el poblador rural, que sufre todas las limitaciones y adversidades climáticas, geográficas y sociales.

En este contexto se entiende el valor agregado, como la agregación de valor, especialmente por otras empresas, a la producción primaria de las economías campesinas, las cuales buscan no solo aumentarlo, sino impedir su salida de las zonas rurales" (Agroindustria rural, pag 28) en otras palabras lo que se busca es la agregación de valor. Vale la pena mencionar que en el devenir histórico de los países en vías de desarrollo, especialmente los países latinoamericanos entre los que se ubica Colombia, se habla de diferentes tipo de agroindustria, entre los que se encuentran las agroindustrias rurales tradicionales, que son las organizaciones que han surgido del ámbito cultural como medio de la subsistencia campesina, al margen del Estado, las ONG o las instituciones educativas, entre las que se ubican la producción de miel de abejas, las elaboraciones artesanales de queso, la mimbrearía y la cestería.

2.2. Los encadenamientos productivos

Para el desarrollo conceptual es necesario hacer claridad frente a la comprensión de la cadena productiva como un sistema constituido por actores interrelacionados y por una sucesión de operaciones de producción, transformación y comercialización de un producto o grupo de productos en un entorno determinado. En las cadenas se encuentran vinculados actores, acciones, relaciones, transformaciones y productos (CICDA-RURALTER, 2004).

Ahora bien, la cadena, como su nombre lo indica, está compuesta por distintos eslabones vinculados por relaciones de producción, transformación, comercialización, consumo o apoyo, entre otras. Como puede verificarse en la figura 2. El territorio, y la articulación al mismo de estas distintas etapas y eslabones, es una noción ausente del concepto de cadena productiva. Las cadenas pueden ser largas o cortas según el número de eslabones que las compongan, pero esta definición no se refiere a un anclaje territorial o geográfico. En cambio, los circuitos de comercialización no solo consideran el entorno, sino también el territorio como elemento central del análisis de las modalidades de comercialización. Por lo tanto, la distancia de circuitos de comercialización no es solo económica sino también geográfica. Por ello, al hablar de circuitos, se hace referencia necesariamente a procesos que se desarrollan en un territorio delimitado (Azevedo, 2012).

Otra forma de analizar la organización de los actores en un sistema de comercialización es a través del lente de los Sistemas Agroalimentarios Localizados (SIAL). Un SIAL corresponde a una concentración territorial de agroindustrias rurales (AIR), activadas por procesos de acción colectiva, respaldadas por redes localizadas de empresas pequeñas de producción y de servicios, y con soporte en dinámicas territoriales e instituciones que promuevan: la interacción territorial, la innovación y la generación de productos de calidad (Boucher y Reyes González, 2011).



Figura 2 – Participantes del encadenamiento productivo.

Otro aspecto a explicitar en el diseño de los encadenamientos productivos son el establecimiento de objetivos comunes entre los integrantes del encadenamiento, en la figura 2, se presentan los participantes de los encadenamientos productivos, teniendo en cuenta las características del producto, las circunstancias del mercado y los participantes; entre los objetivos pueden mencionarse la introducción de productos nuevos en el mercado, mantener o aumentar la cuota de mercado, estrategias para enfrentar a un nuevo competidor, o responder a nuevas regulaciones del gobierno o fortalecer las relaciones existentes con el fin de mejorar la cuota de mercado actual.

Elementos como el manejo de los flujos de información, la realización de evaluaciones permanentes del desempeño del encadenamiento, la explicitación de los beneficios para todos los implicados, la construcción de confianza y el establecimiento de relaciones de mutua cooperación, son aspectos a los que se debe prestar especial atención en los encadenamientos.

En lo relacionado con la evaluación del desempeño del encadenamiento, deben ser las aliadas quienes definan los criterios relevantes para evaluar el desempeño teniendo en cuenta un análisis diferenciado de los productos ofertados, en lo que tiene que ver con la construcción de confianza, es importante que los diferentes aliados en el encadenamiento sientan que el verdadero dinamizador es el trabajo en equipo, la cual se moviliza siempre por una relación gana-gana.

3. Método

Para la identificación de los productos que pueden ser diferenciadores para la definición de los encadenamientos productivos en el municipio del Pore, se parte de la pregunta, ¿Cuáles son los encadenamientos más promisorios del sector agroindustrial

del municipio de Pore? Para la realización de la investigación se utiliza un enfoque cualitativo, el cual permite la integración entre la medición del fenómeno y la explicación de las cualidades que este posee, el trabajo se desarrolla en varias fases, en la primera se examinan los hechos en sí, es decir, se parte de establecer un contacto inicial con el territorio, en este caso el municipio de Pore y en el proceso desarrollar una teoría coherente para representar lo que se observa y poder más adelante identificar cuáles son los encadenamientos más promisorios.

En la segunda etapa se hace la búsqueda, recolección y selección de la información apoyados en las políticas y agendas públicas con información vigente del municipio, las perspectivas y puntos de vista de los participantes en los grupos focales (sus emociones, prioridades, experiencias, significados). La unidad de análisis esta presentada en los documentos y agentes públicas nacionales, departamentales y municipales vigentes, para la revisión se utiliza el análisis de contenido propuesto por (Aktouf, 2013).

En la tercera etapa se utiliza la teoría fundamentada para hacer una explicación general de lo que son los productos agrícolas más prominentes del municipio, a partir de conversatorios con los habitantes, es decir teniendo en cuenta sus puntos de vista, conceptos y opiniones (Taylor y Francis, 2013; Bjursell & Engström, 2019).

Durante el proceso de investigación se tuvo contacto con productores de Pore, así como con Asoplaban, la asociación de bananeros de Pore, la asociación de cultivadores de cacao y la Secretaria de Industria y Turismo del municipio, lo anterior en busca de poder identificar, cuáles han sido las apuestas productivas en términos de producción, comercialización y asociatividad que más se han promovido en Pore, verificar la pertinencia de las asociaciones y agremiaciones ubicadas en el municipio, así como la identificación de la capacidad de convocatoria de cada una, analizar que nuevas opciones de productos agrícolas se puede generar en un municipio, con las características ambientales, económicas, sociales y políticas de Pore y finalmente conocer cuál es la precepción de los productores frente a los desarrollos productivos con potencial de crecimiento para el municipio.

Las unidades de análisis definidas para la investigación, representadas en las agendas y políticas públicas departamentales y nacionales, fueron: Plan Estratégico Municipal de Ciencia Tecnología e Innovación de Pore- PEMCTI 2021-2036, Invierta en Casanare-documento elaborado por la Cámara de Comercio de Casanare en abril del año 2021. El Plan de desarrollo de Pore, 2020-2023“Un gobierno de todos”. Estudio Económico de Casanare Vigencia 2020, Fichas municipales Casanare 2019, Índice Departamental de Competitividad 2019. Dichas unidades de análisis se organizaron en matrices de convergencia como instrumentos que facilitaron la interpretación de la información y la identificación de apuestas productivas.

4. Resultados

4.1. Identificación de ventajas competitivas del municipio de Pore

A partir del análisis de las agendas y políticas públicas se presentan algunos aspectos que hacen parte de potenciales ventajas competitivas que puede aprovechar el municipio de

Pore, para el desarrollo de los encadenamientos productivos, que han sido identificadas durante la última década, los documentos utilizados como fuente fueron construidos con la participación de diversos actores municipales (hombres y mujeres, campesinos, jóvenes, asociaciones e instituciones públicas en el municipio). Las potenciales ventajas competitivas son características propias del municipio que lo diferencia de otros municipios colocándole en una posición relativa superior para competir. Es decir, son atributos que hacen a Pore más competitiva que los otros municipios del departamento de Casanare.

Las características o atributos para ser consideradas como ventajas competitivas deben al menos tener impacto municipal, hacer parte de una agenda o política publica definida por actores con intereses públicos a nivel territorial, que el documento sea elaborado por una entidad reconocida de la región y esta orienta a algún aspecto que favorece el desarrollo local. Una de las características o atributos es el índice de competitividad de Casanare, presentado en el año 2021 por la Cámara de comercio de Casanare, la información arroja entre los resultados: Casanare cuenta con el PIB per cápita más alto de Colombia, en crecimiento y empleo, durante los últimos 5 años. Casanare registró una tasa de crecimiento de 2,4pp, por encima del crecimiento a nivel nacional

En la rama agropecuaria; Casanare alcanzó una participación en el PIB, de $1.55 billones, en lo relacionado con el índice departamental de competitividad. Casanare se destaca como buena práctica en el pilar de mercado laboral (puesto 2). Además, se destaca en pilar educación básica y media (puesto 6), pilar sostenibilidad ambiental (puesto 9), pilar entorno para los negocios (puesto 15). En Casanare persisten oportunidades de mejora en el pilar de innovación y dinámica empresarial principalmente en el indicador de Investigación de alta calidad y revistas indexadas en publindex, así mismo, en el pilar sofisticación y diversificación, especialmente en el indicador de diversificación de la canasta exportadora, entre los factores que intervienen en el proceso de innovación dentro de los territorios. Casanare es destacado en el pilar de infraestructura (2), Capital Humano e Investigación (7) y es claro que se tienen importantes retos en los pilares: Sofisticación de Negocios, producción de conocimiento y tecnología, y producción creativa.

Casanare ocupa el primer lugar en la producción de arroz a nivel nacional con un total 176.878 ha (2020), produciendo el 30% del arroz nacional DANE, ENAM (2020). Ocupa el cuarto lugar en el cultivo de palma de aceite, con una producción de 197.785 toneladas, 13% del área nacional de Palma de Aceite. DANE, SISPA 2020.

Política de Gobierno	**1**	**2**	**3**	**4**	**5**
Plan Estratégico Municipal de Ciencia Tecnología e Innovación. 2021-2036.	Arroz	Caco	Plátano	Piña	Yuca
Invierta en Casanare 2021.	Plátano	Café	Yuca	Cacao	Caucho
Plan de desarrollo “un gobierno de todos” Pore 2020-2023.	Cacao	Maracuyá	Papaya	Piña	Plátano
Estudio económico Cámara de comercio-Vigencia 2020.	Arroz	Plátano	Yuca		

Política de Gobierno	1	2	3	4	5
Fichas municipales Cámara de comercio de Casanare-2019.	Arroz	Cacao	Maíz	Maracuyá	Papaya
Índice departamental de competitividad-2019.	Arroz	Plátano	Maíz	Piña	

Tabla 1 – Definición de encadenamientos promisorios del sector agroindustrial del municipio de Pore.

4.2. Productos con mayor potencial del municipio

Para hacer la identificación de los sectores promisorios del municipio de Pore en el área agrícola, es necesaria la tipificación de cuáles son los productos con mayor tradición y mayor potencial del municipio, para que en articulación con las ventajas competitivas y los resultados obtenidos en la matriz FODA, realizada desde las dimensiones económico-políticas, socioculturales, ambientales y político- institucionales.

De acuerdo con la cámara de comercio de Casanare los cultivos más promisorios en el departamento son: Plátano, Café, Yuca y Cacao. Ya en el ámbito municipal, Plan de Desarrollo del Municipio de Pore 2020-2023: "Un Gobierno de Todos", para el periodo 2020-2023, plantea: que en el municipio el Plátano, el Cacao y la papaya, ocupan los tres primeros lugares en lo relacionado con área sembrada, área cosechada, producción y rendimiento cultivos de ciclo permanente. En los cultivos de ciclo anual la yuca es el principal producto, en los cultivos de ciclo transitorio-tradicional el primer lugar es ocupado por el maíz tecnificado y tradicional, finalmente se menciona como el producto estrella del municipio el arroz, ya que el departamento de Casanare es el primer productor de arroz a nivel nacional, siendo clasificado Pore como una zona apta para la producción de arroz secano utilizando las aguas del río Pauto. (Plan de Desarrollo del Municipio de Pore 2020-2023). En el Plan Estratégico Municipal de Ciencia Tecnología e Innovación, se resaltan como los principales productos en su orden, el plátano, el café, la yuca, el cacao y el caucho. (PEMCTI, Pore 2021-2036). En el estudio económico de la Cámara de comercio-Vigencia 2020, se plantea que el producto más promisorio del municipio es el arroz. (Estudio económico cámara de comercio 2021). De otra parte, las fichas municipales Cámara de comercio de Casanare-2019, plantean que la estructura productiva agroindustrial de Pore, esta soportada por el arroz, el plátano, el caco, el maíz y la Papaya. (fichas municipales Cámara de comercio de Casanare-2019), en la tabla 1 se presenta un consolidado de la caracterización agrícola del municipio que hace cada uno de los actores.

Un aspecto a considerar, expresado por los participantes en los grupos focales, que se realizaron en el municipio, es lo relacionado con el cultivo de heliconias, la cual por sus características de poder soportar el sol todo el año y disponer de la sombra que generan las plataneras puede ser un producto a tener en cuenta para el municipio, ya que en la actualidad se produce, casi bajo las mismas condiciones que la misma maleza, siendo permanentemente desechada por los campesinos por convertirse en un problema para los cultivos del plátano, El aprovechamiento de la heliconia puede convertirla en un producto interesante para el municipio, especialmente por lo precios que está alcanzando el producto en los mercados internacionales.

Finalmente, el Índice departamental de competitividad-2019, elaborado por el Consejo privado de competitividad y la Universidad del Rosario, plantean que los productos arroz, plátano, maíz, son los de mayor crecimiento en el departamento, siendo Pore uno de los municipios productores más importantes.

Actores	Productos seleccionados	Productos seleccionados Resultado final
Agendas y políticas publicas	Arroz, Plátano y Cacao	
Grupos Focales	Arroz, Plátano y Cacao	Arroz, Plátano y Cacao
Comunidad	Arroz, Plátano y Heliconias	

Tabla 2 – Productos con mayor potencial en el municipio de Pore.

Resultado del análisis de las políticas y agendas públicas con información vigente del municipio de Pore, las perspectivas y puntos de vista de los participantes en los grupos focales (sus emociones, prioridades, experiencias, significados). La unidad de análisis fue representada en los documentos y agendas públicas nacionales, departamentales y municipales vigentes, para la revisión se utiliza el análisis de contenido propuesto por Aktouf, 2013; en la gráfica 4, se presenta a modo de síntesis los tres encadenamientos más promisorios del municipio de Pore. Vale la pena mencionar que no existe consenso en el municipio frente a cuales son los productos más promisorios, ya que en algunos de las políticas y agendas consultadas queda la sensación de que lo más importante es mantener la producción de los productos tradicionales y tratar de fortalecerla en el tiempo, haciendo más eficiente el rendimiento por hectárea o utilizando más tecnología en el proceso productivo, mientras que otros, bajo una mirada abierta al mundo y más innovadora proponen que se analice la opción de oferta de nuevos productos, que permitan construir unos encadenamientos productivos diferentes en el municipio, a partir de las fortalezas agroindustriales construidas en los años de generación de productos tradicionales de la región.

Como puede observarse en la tabla 2, el análisis de las políticas y agendas públicas con información vigente del municipio, las perspectivas y puntos de vista de los participantes en los grupos focales permitió identificar los tres productos con mayor potencial de encadenamientos en el del sector agro- industrial en el municipio de Pore, los cuales son el Arroz, como producto tradicional y el de mayor número de hectáreas cultivadas en la región, en segundo lugar se ubicó el plátano como un producto apto para la región, por las características hidrográficas y de suelos y como tercer producto aparece el cultivo de las heliconias, entendido este como una línea que tiene todo el potencial de crecimiento en el municipio y que por los precios que se manejan en los mercados nacionales e internacionales se puede convertir en un producto.

5. Discusión

Luego de la identificación de los productos más promisorios del municipio de Pore, se requiere continuar con la discusión, uno de los aspectos en los que sigue abierto el debate es el tipo de estrategia que se debe proponer para la participación en los encadenamientos, ya que existen algunas propuestas a nivel mundial que han entregado

muy buen resultado y los cuales pueden ser referentes para el País. Entre las estrategias importante de mención están los Sistemas Agroalimentarios Localizados (SIAL), los cuales como lo plantean Boucher y Reyes, corresponde a una concentración territorial de agroindustrias rurales (AIR), activadas por procesos de acción colectiva, respaldadas por redes localizadas de empresas pequeñas de producción y de servicios, y con soporte en dinámicas territoriales e instituciones que promuevan: la interacción territorial, la innovación, la generación de productos de calidad (Boucher y Reyes González, 2011) y aumentar los niveles de competitividad " (Pérez Pravia, M.C., Vega De La Cruz, 2021), lo que puede tener validez para un municipio como Pore, principalmente por el tipo de productos que desde allí se generan como el arroz y el plátano, que pueden participar en este tipo de estrategias.

Otra estrategia viable para lograr encadenamientos productivos a partir de los cultivos más promisorios identificados en Pore, es lo que se conoce como la agricultura por contrato, entendida como "un arreglo contractual no transferible entre productores agrícolas y otras firmas, escrito u oral, que especifique una o más condiciones de producción y una o más condiciones de comercialización, en relación con un producto agrícola" (Prowse, 2012, PEMCTI Pore, 2021). Ya que las grandes empresas que se ubican en la región, como es el caso de Fedearroz, pueden, mediante este tipo de acuerdos, promover estrategias que conlleven a unos precios justos y que beneficien tanto al pequeño agricultor como a los intereses de la empresa.

En el contrato pueden participar, por un lado, los productores (individuales o eventualmente organizados) y por otro, una empresa o firma agroindustrial, como es el caso de Fedearroz, que compra los productos agrícolas como materia prima. Acá pueden darse tres tipos de contratos, contratos que establecen especificaciones de mercado (precios, cantidad y calidad del producto, formas de pago, plazos, etc.), provisión de recursos (de asistencia técnica y gerencial, provisión de insumos, medios de producción, etc.) y contratos de administración (la agroindustria absorbe eventualmente parte de los riesgos de producción y de las decisiones administrativas), siempre y cuando exista por lo menos una condición sobre la producción (Prowse, 2012; Sotomayor, Meneses y Rodríguez, 2013), Esta estrategia puede ayudar a que se de lo que Sotomayor llama articulación desde el mercado hacia la producción, o desde la demanda hacia la oferta (Sotomayor, 2012). La agricultura por contrato ha ido ganando terreno en el mundo por las garantías de equidad y transparencia en los contratos, la implementación de normas y regulaciones y de mejores prácticas de contratación entre los agricultores y los poderes compradores (UNIDROIT, 2014; Eaton y Sheperd, 2001; Pultrone, da Silva y Sheperd, 2014; Comisión Europea, 2014)

Sirven de referencia para el sector agroalimenticio las veinte compañías transnacionales que controlan los mercados de *commodities* como el azúcar, el trigo, la soya, el café, el té, y el maíz (Cargill, Archer Daniels Midland, Conagra, Sara Lee, Louis Dreyfus, Monsanto, Del Monte, Continental, etc.) (Montagut y Dogliotti, 2008). Una estrategia adicional, que ha dado resultados positivos, es la propuesta por Hruska, quien plantea diferentes ejemplos de relacionamiento directo entre pequeños productores y supermercados como Walmart, El Rey o el Grupo Riba Smith en Panamá, o la de Tierra Fértil en Centro y Norteamérica (México, Costa Rica, Nicaragua, Guatemala y el Salvador), que involucra a unos 28 mil pequeños y medianos productores (Hruska, 2013;). Entre las limitaciones del presente estudio es importante aclarar que los resultados obtenidos se deben revisar

permanentemente a la luz de las políticas mundiales y nacionales, de los cambios en los actores, especialmente los lideres de los encadenamientos que actualmente existen en el municipio, siempre en total articulación con los ODS y otras directrices que pueden generar transformaciones y/o ajustes en los resultados. Se recomienda seguir explorando el desarrollo de futuras investigaciones tanto desde el enfoque cuantitativo como el cualitativo, que permitan evaluar de manera permanente los productos más pertinentes para el fortalecimiento y desarrollo de nuevos encadenamientos productivos en el municipio de Pore, y en los municipios de condiciones similares en el norte del departamento de Casanare.

6. Conclusiones

La apertura de los mercados en la que ha venido trabajando el país, mediante tratados de libre comercio y otras formas de integración, ha generado para Colombia el acceso a más de mil quinientos millones de consumidores -según datos del MCIT aquí citado- y cuyo aprovechamiento dependerá, en buena medida, del nivel de integración internacional de los productos y sus encadenamientos agroindustriales locales de cara a los mercados globales. Las condiciones geográficas, características climáticas e hidrográficas de los municipios del norte de Casanare, especialmente Pore, permitieron la identificación de algunas características o atributos, que si se fortalecen pueden llegar a convertirse en capacidades (Barney, 1991: 101; Peteraf, 1993: 180, 183; Teece, D.J., Pisano, G. & Schuen, A. 1997:515). lo que puede generar el desarrollo de ventajas competitivas del municipio, respecto a los demás municipios de la región y del país en general.

Para lograr el desarrollo de capacidades en los diferentes actores de la cadena agroindustrial del municipio, se requiere de establecer acuerdos de voluntades y alianzas que permitan superar las debilidades que actualmente posee el municipio, como la ausencia de una cultura organizativa de la comunidad, lo cual es una práctica arraigada en todos los pobladores, ya que existe una marcada desconfianza por lo que hacen los demás. De igual manera la creación de capacidades regionales en unas líneas específicas del sector agroindustrial debe favorecer la concertación del uso de los suelos, el aumento de los créditos agropecuarios, el aumento de la productividad del sector agropecuario, el fortalecimiento del tejido empresarial y mejorar las condiciones para la comercialización de los productos. Uno de los hallazgos importantes del análisis realizado en las agendas y políticas públicas y la participación en los grupos focales de Pore, es evidenciar la ausencia de un Plan estratégico para el desarrollo agropecuario municipal, que articule lo urbano y lo rural, y que sea construido de manera participativa, entre todos los actores territoriales, buscando alinear las necesidades de la población con la oferta institucional, nacional y local, así como fomentar la concurrencia de acciones y recursos entre las prioridades de los municipios y las políticas de desarrollo agropecuario nacional.

Finalmente, el articulo abre la discusión sobre cuáles pueden ser los productos más promisorios de un municipio con las características de Pore, ya que al trazar una línea que se orienta hacia tres productos se crea un espacio para que los diferentes actores locales y regionales hagan sus análisis y conformen grupos heterogéneos para realizar propuesta que permitan que de manera colectiva se identifiquen los productos que puedan convertir al municipio en una ciudad más prospera y productiva.

Referencias

Azevedo C., (2012), Circuitos de proximidad en la economía alimentaria, Taller-formación, AVSF Universidad Federal de Santa Catarina, La Paz, 8 y 9 de noviembre 2012.

Barney, J.B. 1991. Firm resources and sustained competitive advantage. Journal of Management. Pag 99-129.

Boucher F., Reyes González J.A., 2011, Guía Metodológica para la activación de Sistemas Agroalimentarios Localizados (SIAL), IICA/CIRAD/REDSIAL México: IICA. Disponible en: http://www.iica.int/Esp/Programas/agronegocios/Publicaciones%20de%20Comercio%20Agronegocios%20e%20Inocuidad/B2107e.pdf.

Bjursell, C., & Engström, A. (2019). A Lewinian Approach to Managing Barriers to University–Industry Collaboration. Higher Education Policy, 32(1), Pag 129–148.

Cámara de Comercio de Casanare (2021). Invierta en Casanare.

Cámara de Comercio de Casanare. Estudio económico Vigencia (2020).

Cámara de Comercio de Casanare. Fichas Municipales - Casanare Vigencia 2020.

CICDA-RURALTER, (2004), Guía metodológica para el análisis de cadenas productivas, CICDARURALTER, SNV, INTERCOOPERACIÓN, Lima, Perú. Disponible en: http://www.avsf.org/public/posts/554/gui-a-metodologica-para-el-analisis-de-cadenas-productivas.pdf.

CONSEJO PRIVADO DE COMPETITIVIDAD. Índice Departamental de Competitividad (2019).

Comisión Europea, (2014), Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al comité de las regiones: Hacer frente a las prácticas comerciales desleales en la cadena de suministro alimentario entre empresas, Estrasburgo, Francia, 15 de julio de 2014, pag 472, versión en español. Disponible en: http://ec.europa.eu/internal_

DNP. (2016). Documento CONPES 3866 - POLÍTICA NACIONAL DE DESARROLLO PRODUCTIVO. Bogotá: Departamento Nacional de Planeación.

Eaton C., Shepherd A.W., (2001), Contract farming: partnerships for growth, FAO, Agricultural Services Bulletin, pag 145. Disponible en: http://www.fao.org/docrep/014/y0937e/y0937e00.pdf.

Fundación Centro de Desarrollo Tecnológico para la Sostenibilidad y Competitividad Regional- C-STAR, Plan Estratégico Municipal de Ciencia, Tecnología E Innovación, (2021), PEMCTI PORE 2021-2036.

González Nova Armando, Prego Regalado, Juan C., Robaina Echevarría Lisset. Encadenamiento productivo-valor en el proyecto apocoop, 2020 Estudios del Desarrollo Social: Cuba y América Latina (2020), Pag 75-82.

Grupo Latino, Agroindustria rural ISBN.

Hahn-de-Castro Lucas Wilfried. Encadenamientos regionales en Colombia 2004-2012. (2016) Revista de Economía del Rosario, Pag 19. http://dx.doi.org/10.12804/revistas.urosario.edu.co/economia/a.5240

Hruska A., (2013), Agricultura familiar y acceso a los mercados, Memoria del Seminario-Taller realizado por la oficina Sub-regional de FAO para Mesoamérica, FAO, Ciudad de Panamá, Panamá. Disponible en: http://www.onu.org.pa/media/documentos/FAO/agricultura-familiaracceso-mercados.pdf.

Montagut X., Dogliotti F., (2008), Alimentos globalizados, Soberanía alimentaria y comercio justo, Icaria, Barcelona, 2da edición

OCDE. (2016). Trade in Value Added (TiVA). Recuperado de http://stats.oecd.org/

Padilla Pérez, R., & Oddone, (2016). Manual para el fortalecimiento de Cadenas de Valor. México: CEPAL.

Pérez Pravia, M.C., Vega De La Cruz, L.O. Procedure for risk management of the sustainable production Chain. (2021). Revista Venezolana de Gerencia, Pag 1396-1412.

Peteraf, M. (1993). The cornerstones of competitive advantage: a resource-based view. Strategic Management Journal. Pag 179-191.

Plan de Desarrollo Pore 2020-2023 “Un gobierno de todos”. Alcaldía de Pore. Pag 204.

Prowse M., (2012), Contract Farming in Developing Countries - A Review, Colección “A savoir” n°12 Agencia Francesa para el Desarrollo (AFD), Instituto de Desarrollo, Políticas públicas y Administración, Universidad de Antwerp. Disponible en: http://www.afd.fr/jahia/webdav/site/afd/shared/

Pultrone C., Da Silva C. Y Sheperd A., (2014), Principios rectores para las operaciones responsables de agricultura por contrato, FAO, Roma, Italia. Disponible en: http://www.fao.org/3/a-i2858s.pdf.

Rojas López Hilda, Casanare, Un Departamento que debe conocerse. Comité de Pedagógico Núcleo Educativo 02. (1997). Tunja, Boyacá. Pág. 79-82.

Sotomayor O., Meneses J. y Rodríguez A., (2013), Agrocadenas y redes de actores: políticas de acción pública, coordinación multi-niveles e innovación tecnológica, Unidad de desarrollo Agrícola - División de Desarrollo Productivo y Empresarial - CEPAL, Ministerio de Agricultura, Ganadería y Pesca, Santiago de Chile.

Sotomayor O., (2012), Cadenas productivas y de valor en el sector agropecuario de América Latina y El Caribe, encadenamientos con pequeños productores agrícolas, Seminario Desarrollo de Alternativas de producción sostenible en el Corredor Biológico Mesoamericano México, CEPAL Santiago de Chile, 15 de agosto de 2012. Disponible en: http://www.cepal.org/

Teece, D.J., Pisano, G. & Schuen, A. 1997. Dynamic capabilities in strategic management. Strategic Management Journal, pag,509-534.

UNIDROIT, (2014), Legal Guide on contract farming: Effective contracts are the cornerstone of sustainable contract farming, Project note, UNIDROIT/FAO/IFAD, 16 de Octubre de 2014. Disponible en: http://www.unidroit.org/english/workprogramme/study080a/s-80a-project-note-flyer-01-e.pdf.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 28/12/2021
Aceitação/Acceptance: 23/02/2022

Análisis de los frameworks de ciberseguridad en IIoT existentes

Herberth Alberto Ausecha[1], Katerine Márceles Villalba[2], Siler Amador Donado[3]

Alberto.ausecha@unimayor.edu.co; kmarceles@unimayor.edu.co; samador@unicauca.edu.co

[1,2] Facultad de Ingeniería, Institución Universitaria Colegio Mayor del Cauca, Carrera 7 N° 2-34 Edificio Bicentenario, 190003, Popayán- Cauca, Colombia.

[3] Facultad de Ingeniería Electrónica y Telecomunicaciones, Universidad del Cauca, Carrera 2 #4N-140, 190003, Popayán- Cauca, Colombia

Pages: 436-448

Resumen: Las personas en la actualidad se caracterizan por estar conectadas al internet a través del uso de algún dispositivo, esto hace que puedan llegar a ser vulnerables frente algún ataque informático y quedar expuesto a una amenaza. Esto también aplica a las empresas, dado que cada uno de sus activos de información suelen estar de cara al internet también realizando diferentes transacciones. A partir de ello se vio la necesidad de revisar a través de un análisis sistemático de literatura científica los frameworks de ciberseguridad existentes construidos por diferentes autores con el fin de tenerlos como referentes para la construcción de uno nuevo que integre lo mejor de cada uno y pueda disminuir cada vez más las brechas de seguridad que suelen ser presentadas en el entorno industrial. Cabe anotar, que todo este proceso se llegó a formular bajo la metodología de marco lógico, permitiendo precisar la problemática hasta delimitarla.

Palabras-clave: Ciberseguridad, Framework, Internet de las cosas.

Analysis of existing IIoT cybersecurity frameworks

Abstract: People today are characterized by being connected to the internet through the use of some device, this means that they can become vulnerable to a computer attack and be exposed to a threat. This also applies to companies, since each of their information assets are usually facing the internet, also carrying out different transactions. From this, the need was seen to review, through a systematic analysis of scientific literature, the existing cybersecurity frameworks built by different authors in order to have them as references for the construction of a new one that integrates the best of each one and can reduce more and more the security breaches that are usually presented in the industrial environment. It should be noted that this entire process was formulated under the logical framework methodology, allowing the problem to be specified until it was delimited.

Keywords: Cybersecurity, Frameworks, Internet Of Things.

1. Introducción

En la actualidad el mundo está viviendo por cuarta vez una revolución industrial, también conocida como industria 4.0. Durante el foro Económico mundial de 2016 Klauss Schwab afirmó que la cuarta revolución industrial "Se caracteriza por una fusión de tecnologías que difumina las líneas entre las esferas física, digital y biológica" (Schwab, 2016). Los cambios que ha generado esta evolución tecnológica ha modificado la forma en la que se vive y se trabaja, generando una necesidad en las empresas de integrar nuevas tecnologías para gestionar, controlar y monitorizar de manera automática todos los dispositivos y estar en una constante innovación en este campo no sólo para optimizar sus procesos, sino también para mantenerse en el mercado actual el cual evoluciona y cambia constantemente.

Se puede afirmar que esta revolución trajo un nuevo foco de atención, el cual recae sobre las tecnologías IIoT, dado que están formando parte en la manufacturación inteligente, la cual proporciona bases para tomar decisiones efectivas y optimizadas a través de procesos de toma de decisiones más rápidos y precisos, brindando una mejora en la calidad de los procesos industriales adaptándose a la nueva industria con el uso de computación en la nube, inteligencia artificial (IA), big data, realidad aumentada, entre otros. Aunque la industria 4.0 ha implementado muchas oportunidades en los sectores industriales estos avances han traído consigo algunos problemas de ciberseguridad. Los dispositivos ciberfísicos (CPS) se han convertido en una preocupación por su cada vez más amplia aplicación en la infraestructura de hogares, fábricas, calles, etc., convirtiéndose en posibles vectores de ataque los cuales pueden comprometer los procesos comerciales de las industrias, puntos para acceder a información privada (Walker, Hammoudeh, Aldabbas, Aydin, Dehghantanha, 2019). En conclusión, la cantidad de dispositivos CPS implementados trae consigo un incremento de vulnerabilidades, por lo que se hace necesario la identificación y análisis de los diferentes frameworks de ciberseguridad existentes mediante una revisión sistemática en fuentes especializadas con el fin de referenciar y definir aspectos importantes que permitan llegar a definir y/o proponer el diseño de uno nuevo con el fin de gestionar las diferentes amenazas a la que pueden estar expuestos los dispositivos conectados al internet. Este proceso se llevó a cabo a través de la Metodología de Marco Lógico (MML) siendo una herramienta de gestión de proyectos orientada a objetos, que permitió realizar una óptima planificación, ejecución y evaluación de la propuesta en mención.

A continuación, se presenta el despliegue de este trabajo a través de diferentes secciones, siendo la segunda sección los aspectos preliminares donde se presentan conceptos importantes que se relacionan en el trabajo, en la sección tres trabajos relacionados se presentan los referentes para la construcción de lo desarrollado y finalmente en la cuarta sección se encuentra la metodología donde se hace un despliegue de la misma.

2. Aspectos preliminares

A continuación, se relacionan cada uno de los aspectos que fueron necesarios para tener claridad y así poder llegar al análisis de los diferentes frameworks de Ciberseguridad existentes:

Ciberseguridad. La compañía de seguridad informática internacional Kaspersky define a la ciberseguridad como "la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica." Este término se extiende desde los negocios hasta la informática móvil, abarcando la parte industrial y dentro de esta los dispositivos IoT. Con fin de su implementación en dispositivos IIoT se busca conseguir que estos brinden la mayor confidencialidad, integridad y disponibilidad con el objetivo de proteger los sistemas e información de las industrias (latam.kaspersky.com, 2021).

Frameworks. Es un marco estructurado que recopila y gestiona normativas para el buen funcionamiento de la ciberseguridad. Por lo general, se establece un mapeo con los objetivos de seguridad definidos, por ejemplo: prevenir acceso no autorizado a un sistema a través de controles como el ingresar usuario y contraseña sobre el dispositivo (Anónimo, 2021).

Dispositivos IIoT. El internet de las cosas industrial es una subcategoría del internet de las cosas dentro de la cual se implementan desde sensores ambientales hasta complejos robots industriales, según el autor Gilchris (2016) afirma que el internet proporciona una mejor visión de las operaciones y activos de la empresa Por lo tanto, proporciona un método para transformar los procesos operativos del negocio utilizando como retroalimentación los resultados obtenidos al interrogar grandes conjuntos de datos. La implementación del IIoT permite mejoras en la producción y procesos industriales, convirtiéndose en una base de innovación accesible para todos, sus aplicaciones principales han sido en los procesos de producción, cadenas de suministros, áreas de la salud, e inclusive tienen aplicaciones en ventas al por menor.

Inteligencia artificial. El Autor Kaplan & Haenlein (2019) definen a la inteligencia artificial como "la capacidad del sistema para interpretar datos externos correctamente, aprender de dichos datos y usar esos aprendizajes para lograr objetivos y tareas específicas mediante una adaptación flexible". Actualmente con el auge de los dispositivos IoT generado por la industria 4.0 la se puede recolectar gran cantidad de información a través de los sensores , el cual pueden convertirse en datos útiles de entrada para la IA. En una entrevista sobre su visión de la inteligencia artificial a uno de los pioneros en esta área, el doctor Raj Reddy (Morel, 2011): mencionó que los avances que están ocurriendo ahora en el siglo XXI se basan en sistemas de inteligencia artificial. Como resultado, la IA es básicamente el descubrimiento de nuevos conocimientos y su aplicación se enfoca en resolver problemas que antes no se podían resolver.

Vulnerabilidad. "Es una debilidad presente en los activos" (Incibe, 2015) esta debilidad puede explotarse y afectar negativamente la integridad confiabilidad y disponibilidad de los sistemas. Los dispositivos IIoT no son ajenos a poseer vulnerabilidades dentro de ellos como lo pueden ser contraseñas por defecto débiles.

Amenazas. "Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor" (Incibe, 2015). Las amenazas se dan debido a que los activos de las empresas presentan vulnerabilidades o debilidades y por

consecuencia de la materialización de una amenaza se produce un impacto, el cual suele ser representado como una degradación que afecta el valor del activo.

3. Trabajos Relacionados

Es de mencionar algunos trabajos que se han tenido en cuenta para este proceso de investigación:

AD-IOT: El artículo publicado en el noveno taller y conferencia anual de informática y comunicación "AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning" brinda una propuesta de un sistema enfocado en las ciudades inteligentes, con el cual se busca dar solución o mitigar dos grandes problemas de la ciberseguridad, como son: el ataque del día cero y la detección de los falsos positivos. Esta solución propuesta brinda detección, alerta de anomalías y monitoreo de todo el tráfico en la red para los dispositivos IoT conectados. AD-IOT está basado inteligencia artificial haciendo uso de múltiples algoritmos de aprendizaje de máquina (Bosque aleatorio y árbol extra las cuales son algoritmos de decisión basados en árboles), con la implementación de este sistema el foco central no solo consiste en la mitigación de los ataques, además también busca aumentar la posibilidad de detectar los falsos positivos. Este software está diseñado con el fin de cubrir una gran cantidad de dispositivos en una amplia red, ya que se espera que en él se conecten casas inteligentes, edificios, centros comerciales (Alrashdi et al., 2019). La propuesta de los algoritmos de inteligencia artificial (Machine learning)vista en AD-IoT brinda una óptima opción para tener en cuenta y resolver una de las problemáticas planteadas en este artículo, como lo es la detección de los falsos positivos y el ataque del día cero.

N-Balot: Es una propuesta realizada para un artículo científico "Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders", el cual brinda una solución para ataques de botnets como los son Mirai que causan ataques de denegación de servicios utilizando autoencoders como estrategia para mitigar estas amenazas, para su implementación se utilizaron técnicas de Deep learning por su capacidad de aprender patrones complejos y detectando anomalías cuando se generan comportamientos anormales en los dispositivos IoT. La aplicación de este framework se realiza para la detección de anomalías en el tráfico de red, pero como objetivo central la detección de botnets (Meidan et al. 2018), este framework ofrece una propuesta de una inteligencia artificial, aunque centrada en un tipo de ataque (botnets). En ese sentido, los conocimientos de este trabajo pueden ser aplicados al marco de ciberseguridad que se propone, dado que se retoma su aporte en lo que respecta al uso de la técnica de inteligencia de Deep learning.

4. Metodología

Para llevar a cabo la elaboración del diseño de un marco de ciberseguridad para la mitigación de riesgos, se eligió la Metodología de Marco Lógico (MML) siendo una herramienta de gestión de proyectos orientada a objetos, que permitió realizar una óptima planificación, ejecución y evaluación del proyecto. La cantidad de pasos para la elaboración de esta metodología suele variar dependiendo del autor, para obtener al final una matriz suficientemente completa (*Ortegón, Pacheco y Prieto,* 2017).

Bajo la metodología de marco lógico se construyó el proyecto con la finalidad de alcanzar los objetivos propuestos, a partir de lo anterior se determinó la siguiente fase:

Fase 1: Analizar los Frameworks de ciberseguridad existentes mediante una revisión sistemática en fuentes especializadas con el fin de referenciar y definir aspectos importantes para diseñar un nuevo marco.

Actividad 1: Identificación de Marcos de ciberseguridad existentes.

Con la finalidad de realizar la selección de los frameworks de ciberseguridad en IIoT al estudiar y comparar se recurrió a la información obtenida previamente en la bitácora de gestión de conocimientos relacionada con trabajos similares al propuesto donde se realizó una revisión bibliográfica en la cual se incluía búsqueda de frameworks los cuales resulten relevantes para la realización de esta fase. Para llegar a encontrar estos documentos se realizaron diferentes cadenas de búsqueda las cuales son detalladas en la tabla 1.

Numeración	Cadenas de búsqueda
1	"cybersecurity framework" AND ("IIoT" OR "IoT") AND "artificial intelligence"
2	"cybersecurity framework" AND ("IIoT" OR "IoT") AND "machine learning"
3	"cybersecurity framework" AND ("IIoT" OR "IoT") AND "Deep Learning"
4	"cybersecurity framework" AND ("IIoT" OR "IoT")
5	"(Attacks OR threat) AND "cybersecurity framework" AND ("IoT" OR "IIoT")

Fuente : Propia de los autores

Tabla 1 – Cadenas de búsqueda

EL objetivo de las diferentes cadenas de búsqueda planteadas consiste en buscar frameworks de ciberseguridad para dispositivos IoT e IIoT, los cuales tengan o no implementados en ellos tecnologías de inteligencia artificial (machine learning y Deep learning) de preferencia, con el fin de conocer qué proyectos se han realizado y cómo para tenerlos de referentes. La finalidad de esta búsqueda fue ampliar la cantidad estudios realizados para nutrir esta investigación con la información obtenida de los frameworks ya construidos y determinar cómo estos funcionan en su área de aplicación. Además, al conocer e identificarlos permitirá determinar los elementos que diferenciarán el nuevo framework de los demás. A continuación en la tabla 2 se presentan los resultados obtenidos luego de la depuración de la bitácora de gestión de conocimiento, el cual contiene 52 trabajos relacionados con el tema de estudio; sin embargo, luego de unos criterios de evaluación de calidad que son:

> **CEC 1.** ¿El estudio presenta algún tipo de contribución: metodología, técnica, herramienta, enfoque, modelo, método, estrategia o framework?.
>
> **CEC 2.** ¿El estudio presenta algún método de investigación basado en el análisis y descripción como: estudio empírico, estudio experimental, pruebas de concepto, teórica o caso de estudio?.
>
> **CEC 3.** ¿El estudio menciona y aplica el tipo de contribución planteado?.

CEC 4. ¿El estudio realiza un análisis de los resultados obtenidos?.

Se aplicó la siguiente valoración: S (sí) = 1, P (parcialmente) = 0.5, N (no) = 0. De esta manera, el resultado total para la evaluación de cada estudio (CEC1 + CEC2 + CEC3 + CEC4) puede resultar de la siguiente manera: 0, 0.5 y 1 (incompleto) 1,5 y 2 (regular), 2,5 (bueno), 3 (muy bueno) y 3,5 y 4 (excelente).

Para evaluar cada estudio primario, se establecieron reglas a cada criterio de evaluación, esto con el fin de complementar la parte cualitativa a la valoración:

CEC 1. S, el estudio propone el uso o una nueva metodología, framework, modelo, técnica o herramienta; P, la contribución está presente pero no se describe claramente; N, la contribución no puede ser identificada o no está establecida.

CEC 2. S, el estudio menciona que ha aplicado explícitamente algún método de investigación; P, el estudio presenta información relevante pero no especifica el método de investigación; N, el método de investigación no puede ser identificado o no está descrito.

CEC 3. S, el estudio presenta de forma detallada el tipo de contribución que ha sido llevado a cabo; P, el tipo de contribución llevado a cabo es representado de forma breve; N, el estudio no describe claramente el tipo de contribución llevado a cabo.

CEC 4. S, el estudio presenta un análisis detallado que explique los resultados obtenidos; P, los resultados son explicados brevemente; N, los resultados no pueden ser identificados o no están descritos

Finalmente, se establecieron 22 trabajos como primarios extraídos de diferentes fuentes de bases de datos bibliográficos como: Springer, Science Direct, IEEE Xplore Digital Library y ResearchGate.

No obstante, al tener identificados los trabajos como primarios se llegó a filtrar nuevamente obteniendo 8 trabajos de los 22 que sí realmente apuntan a la construcción y estudio de un framework de Ciberseguridad, como se muestra en la siguiente:

ID	Nombre del estudio	CEC				Calidad	
		1	2	3	4	Cuantitativo	Cualitativo
1	An Ontology-Based Cybersecurity Framework for the Internet of Things. Mozzaquatro, Agostinho, Gonclaves, Martins y Jardim (2018)	S	P	s	p	3	Muy Bueno
2	A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Sohal, Sandhu, Sood y Chang (2018)	S	P	S	N	2,5	Bueno
3	Cybersecurity Framework for IIoT-Based Power System Connected to Microgrid. Ji Woong et al. (2019)	P	P	P	S	2,5	Bueno

ID	Nombre del estudio	CEC				Calidad	
		1	2	3	4	Cuantitativo	Cualitativo
4	Cybersecurity vulnerability mitigation framework through empirical paradigm: enhanced prioritized gap analysis. Gupta, Mylrea y Patangia (2020)	P	S	S	S	3,5	Muy bueno
5	DRAFT - A Cybersecurity Framework for IoT Platforms. Datta (2020)	N	S	P	S	2,5	Bueno
6	Adaptive Cybersecurity Framework for Healthcare Internet of Things. Svetlana y Habtamu (2019)	S	S	S	S	4	Excelente
7	Semi-supervised Learning based Distributed Attack Detection Framework for IoT. Rathore y Hyuk Park (2018)	N	S	S	N	2	Regular
8	Sapiens chain: a blockchain-based cybersecurity framework. Yu, Wang, Qiang y Binxing (2018)	N	S	S	P	2,5	Bueno

Leyenda: S: sí; N: no; P: parcialmente; CEC: Criterio de evaluación de calidad; E: excelente; MB: muy bueno; B: bueno; R: regular; I: incompleto.

Fuente: Propia de los autores.

Tabla 2 – Resultados de estudios principales

Para la calificación de los estudios presentados en la tabla 2 se usaron los mismos criterios de evaluación presentados anteriormente, con esto se buscó estudios que presenten una nueva metodología, técnica o herramienta para solucionar el problema que presenta y que contribuciones aporta en el área donde se aplica.

Actividad 2: Análisis y comparación de los Marcos encontrados.

Con los resultados obtenidos de las búsquedas sistemáticas realizadas anteriormente se encontraron que 3 estudios ofrecen frameworks de ciberseguridad relevantes para esta investigación. A continuación, en la tabla 3 se enlistarán los artículos encontrados y calificados como relevantes para en análisis y comparación, la principal información relevante que se tomará para comparar estos frameworks son la arquitectura y herramientas usadas para su elaboración, si usó una técnica de Inteligencia artificial o no y cuál (machine learning o Deep learning) y también si fue implementado en la las capas catalogadas como nube(cloud) o niebla(fog) y si el enfoque de este framework es la mitigación de vulnerabilidades presentes en los dispositivos IoT e IIoT o detección de ataques a estos. Estas diferentes herramientas y técnicas se tomarán en consideración si será implementada en el framework propuesto.

Actividad 3: Valoración de los Marcos de ciberseguridad existentes usando criterios de calidad.

Con la finalidad de poder dar un valor cuantitativo y cualitativo a los frameworks y sus herramientas presentadas anteriormente en este punto se realizó una tabla comparativa (tabla 4) usando criterios de calidad que permitieron brindar un análisis más significativo

y con ello poder concluir cuales de sus características son más relevantes y/o necesarias en la aplicación del framework a desarrollar en esta investigación. Para la calificación se optó por dar un mayor valor a aquellos que se alineen con la premisa propuesta. Cabe resaltar que la siguiente evaluación de criterios de calidad se enfocó en calificar el aporte que brindan los frameworks a nivel técnico y la información que brinda el estudio sobre dicho framework.

Nombre del estudio	Detección de ataques/ vulnerabilidades	Utiliza una técnica de IA (Cual)	Fog / Cloud	Características del framework
DRAFT - A Cybersecurity Framework for IoT Platforms	Vulnerabilidades	NO	Cloud	SIEM system
An Ontology-Based Cybersecurity Framework for the Internet of Things	Vulnerabilidades	NO	Cloud	SPARQL IoTSec
Semi-supervised learning based distributed attack detection framework for IoT	Ataques	SI (Machine learning)	FOG	ESFCM (ELM - Semi-supervised Fuzzy C-Means)
Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis	Vulnerabilidades	NO	FOG	CyFEr
A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments	Ataques	NO	FOG	Markov model Intrusion Detection System Virtual Honeypot Device
Cybersecurity Framework for IIoT-Based Power System Connected to Microgrid	Vulnerabilidades	NO	Nodo a Nodo	OSINT NESCOR PENTEST
Adaptive Cybersecurity Framework for Healthcare Internet of Things	Ataques	SI (Machine Learning)	Nodo a Nodo	Evolutionary game theory

Fuente: Propia de los autores

Tabla 3 – Comparación de los frameworks

Criterios de evaluación de calidad: El objetivo de los criterios de evaluación de calidad es asegurar una apropiada evaluación de cada estudio que fue considerado primario. Los criterios de evaluación establecidos son:

CEC 1. ¿El estudio presenta un framework que brinde una solución a los ataques en dispositivos IIoT?.

CEC 2. ¿El estudio presenta un framework el cual use la implementación de alguna técnica de inteligencia artificial para el cumplimiento de su tarea?.

CEC 3.¿El estudio presenta un framework el cual puede ser implementado en las capas Cloud o Fog?.

CEC 4. ¿El estudio brinda herramientas o metodologías dentro del framework para mitigar ataques?.

Para cada uno de los criterios de evaluación de calidad, se aplicó la siguiente valoración: S (sí) = 1, P (parcialmente) = 0.5, N (no) = 0. De esta manera, el resultado total para la evaluación de cada estudio (CEC1 + CEC2 + CEC3 + CEC4) puede resultar de la siguiente manera: 0, 0.5 y 1 (incompleto) 1,5 y 2 (regular), 2,5 (bueno), 3 (muy bueno) y 3,5 y 4 (excelente).

CEC 1. S, el estudio presenta una solución a ataques presenten en dispositivos IoT; P, El estudio presenta una solución a vulnerabilidades en dispositivos IoT; N, la contribución no puede ser identificada o no está establecida.

CEC 2. S, el estudio presenta una técnica de inteligencia artificial especificada; P, el estudio presenta una técnica de inteligencia artificial pero no es detallada; N, La técnica de inteligencia artificial no puede ser identificado o no está descrito.

CEC 3. S, el estudio presenta una arquitectura desarrollada e implementada en las capas de Cloud o Fog); P, el tipo de estudio presenta una arquitectura implementada en una arquitectura de nodo a nodo; N, el estudio no describe en que arquitectura fue implementado.

CEC 4. S, el estudio detalla 3 o más características o metodologías implementadas en el framework; P, el estudio detalla 1 o 2 características o metodologías implementadas en el framework; N, el estudio no detalla las características o metodologías que se implementaron en el framework.

ID	Nombre del estudio	Año de la publicación	CEC				Calidad	
			1	2	3	4	Cuantitativo	Cualitativo
1	DRAFT - A Cybersecurity Framework for IoT Platforms	2020	P	N	S	P	3	Muy bueno
2	An Ontology-Based Cybersecurity Framework for the Internet of Things	2018	P	N	S	S	2,5	Bueno
3	Semi-supervised learning based distributed attack detection framework for IoT	2017	S	S	S	P	3,5	Excelente

ID	Nombre del estudio	Año de la publicación	CEC				Calidad	
			1	2	3	4	Cuantitativo	Cualitativo
4	Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis	2020	P	N	P	P	1,5	Regular
5	Cybersecurity Framework for IIoT-Based Power System Connected to Microgrid	2018	S	N	S	S	3	Muy Bueno
6	A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments	2020	P	N	P	S	2	Regular
7	Adaptive Cybersecurity Framework for Healthcare Internet of Things	2019	S	S	p	P	3	Muy bueno
8	Sapiens chain: a blockchain-based cybersecurity framework	2018	P	N	S	P	2	Regular

Leyenda: S: sí; N: no; P: parcialmente; CEC: Criterio de evaluación de calidad; E: excelente; MB: muy bueno; B: bueno; R: regular; I: incompleto

Fuente: Propia de los autores

Tabla 4 – Resultados de estudios principales

Actividad 4: Análisis de los Marcos de ciberseguridad seleccionados y contribución al trabajo actual.

Una vez valorados los frameworks, se procedió a realizar las respectivas conclusiones a partir de las tablas comparativas anteriormente realizadas, junto con ello se logró concluir las semejanzas y diferencias de los frameworks frente al nuevo que se propone a raíz del análisis de los ya existentes teniendo encuenta las características que ya se han aplicado y funcionalidades en los anteriores trabajos, las cuales también pueden ser aplicadas en el nuevo framework. Este análisis también tiene otro aporte qué es conocer lo que ya se ha hecho y cómo se hizo para poder identificar un factor diferencial más específico frente a otros frameworks de ciberseguridad existentes.

Tras una revisión al trabajo realizado de las Tablas 1 y 2 se pueden identificar frameworks de ciberseguridad para dispositivos IoT, los cuales resultan relevantes para un análisis de sus principales características. Los frameworks encontrados y valorados que fueron relevantes para su estudio se listaron en la tabla 3, de ésta se pudo identificar que los frameworks existentes que ofrecen un software de ciberseguridad se centran en los dispositivos IoT, mientras que para los dispositivos IIoT se encuentran principalmente

el framework brindado por el NIST (National Institute of Standards and Technology) y variaciones derivadas de este.

Los diferentes frameworks presentados brindan diferentes herramientas o metodologías, pero uno de los factores comunes principales es que son implementados en las arquitecturas de Cloud o Fog si buscaban cubrir una red de múltiples dispositivos IoT y de esta manera se libraban de una carga de trabajo extra en los dispositivos. Como referencia para la arquitectura a trabajar del nuevo framework, se puede decir que en los estudios encontrados 3 de 8 estaban centrados en la detección de ataques a los dispositivos IoT y a su vez 2 de estos fueron implementados con una arquitectura de Fog, es así como estos mismos estudios presentan una calificación alta en la Tabla 4.

De los frameworks encontrados y calificados como relevantes 2 de estos únicamente presentaban la implementación de una técnica de inteligencia artificial y en ambos casos se utilizó un algoritmo de Machine Learning ,el cual será tenido en cuenta para un proceso posterior en lo que respecta a al diseño e implementación.

El último detalle a considerar presentado en la tabla 3, fue las diferentes herramientas o metodologías implementadas en el framework del estudio analizado. Para la selección de las más relevantes se optó por tener en cuenta principalmente si con la aplicación de estas se puede brindar una detección de ataques en los dispositivos IoT y como segundo parámetro si fueron implementados en una arquitectura de Fog.

El resultado de esta selección fueron las siguientes herramientas/metodologías: Markov model Intrusion, Virtual Honeypot Device, ESFCM (ELM - Semi-supervised Fuzzy C-Means) y Evolutionary game theory, siendo estas las principales a tener en cuenta al momento de decidir la arquitectura del framework también se tendrán en cuenta todos aquellos que puedan ser implementados en una arquitectura de Fog o Cloud (dependiendo de cuál fue la arquitectura seleccionada).

Actividad 5: Identificación del factor diferencial del nuevo Marco de Ciberseguridad.

El principal factor diferencial que se logró identificar a través del análisis realizado frente a los demás frameworks, es que éste será desarrollado con un enfoque para la protección dispositivos IIoT, buscando herramientas y metodologías centradas en la protección de redes con múltiples dispositivos industriales y desarrollado con el uso de herramientas de software libre. La selección de herramientas y metodologías se realizará teniendo en cuenta los ataques más comunes presentes en los dispositivos IIoT. Por el lado de la inteligencia artificial se seleccionará un algoritmo de IA, el cual se enfoque en el análisis de tráfico de red para detectar el tráfico malicioso y así prevenir ataques a los dispositivos inteligentes industriales y pueda dar resultados óptimos con el entrenamiento de una database que cubra amenazas presentes en dispositivos IIoT, por ende disminuir el ratio de falsos positivos y falsos negativos .

5. Conclusiones

Actualmente cada usuario se vuelve vulnerable con el simple hecho de tener algún dispositivo conectado al internet, por lo que se vio necesario a través de este proceso

de análisis realizado, el poder llegar a determinar primero el reconocer los diferentes Frameworks de Ciberseguridad existentes, el cual quedó en evidencia que son muy pocos los autores quienes han trabajado en dicho tema y segundo el llegar a determinar las características esenciales que debería tener un nuevo frameworks a partir de la selección de características de los que están con el fin de tener uno más robusto que permita cubrir cada brecha o debilidad no contemplada por los ya existentes haciendo uso de herramientas de software libre y la inteligencia artificial como también el almacenamiento en la nube para el procesamiento de la data.

Agradecimientos

Agradecimientos a la Universidad del Cauca en especial a su grupo de investigación GTI y al grupo de investigación I+D en Informática de la Facultad de Ingeniería de la Institución Universitaria Colegio Mayor del Cauca, por el apoyo brindado para el desarrollo del proyecto.

Referencias

Anónimo. (02 de 02 de 2021). Frameworks de ciberseguridad y estándares que debes conocer. Obtenido de Proteger mi Pc: https://protegermipc.net/2021/08/19/frameworks-de-ciberseguridad-y-estandares-que-debes-conocer/

Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019). AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019, 305–310. https://doi.org/10.1109/CCWC.2019.8666450

Incibe. (06 de 07 de 2015). Gestión de riesgos. Una guía de aproximación para el empresario. Obtenido de Insititulo Nacional de ciberseguridad Web Site: https://www.incibe.es/protege-tu-empresa/guias/gestion-riesgos-guia-empresario

Latam.kaspersky.com. (2021). What-is-cyber-security @. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT-Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Computing, 17(3), 12-22. doi:10.1109/mprv.2018.03367731

Morel, B. (2011). Artificial intelligence and key to the future of cybersecurity. Proceedings of the ACM Conference on Computer and Communications Security, 93-97. https://doi.org/10.1145/2046684.2046699

Ortegón, E., Pacheco, J., & Prieto, A. (2015). Adm Proy U2-2- Metodología del marco lógico para la planificación, el seguimiento y la evaluación de proyectos y programas. www.cepal.org/es/suscripciones

Schwab, K. (16 de Junio de 2016). World Economic Forum. Obtenido de https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2019). Threats on the horizon: understanding security threats in the era of cyber-physical systems. Journal of Supercomputing, 0123456789. https://doi.org/10.1007/s11227-019-03028-9

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 02/10/2021
Aceitação/Acceptance: 12/01/2022

Buenas prácticas para el desarrollo de software sostenible

Darío Enrique Soto-Duran[1], Adriana Xiomara Reyes-Gamboa[2],
Juan Camilo Giraldo-Mejía[3], Aixa Villamizar-Jaimes[4], Fredy Alonso Vidal-Alegría[5]

**dsoto@tdea.edu.co; axreyes@elpoli.edu.co; jgiraldo1@tdea.edu.co;
aixa.villamizar@tdea.edu.co; fvidal@unimayor.edu.co**

[1] Tecnológico de Antioquia (TdeA), Cl. 78B #72A-220, 050034, Medellín, Colombia.

[2] Politécnico Colombiano Jaime Isaza Cadavid, Carrera 48 No. 7 - 151, 050001, Medellín, Colombia.

[3] Tecnológico de Antioquia (TdeA), Cl. 78B #72A-220, 050034, Medellín, Colombia.

[4] Tecnológico de Antioquia (TdeA), Cl. 78B #72A-220, 050034, Medellín, Colombia.

[5] IU Colegio Mayor del Cauca, Edificio Bicentenario, 190001, Popayán, Colombia.

Pages: 449-460

Resumen: En las últimas décadas, el uso de la tecnología de la información y las comunicaciones (TIC) y los sistemas de software viene en un aumento exponencial, facilitando diferentes procesos y actividades de la vida cotidiana. Sin embargo, el uso de la tecnología afecta significativamente a las crecientes demandas de energía y a las emisiones de gases de efecto invernadero. En consecuencia, surge el concepto de software ecológico que busca la construcción sostenible, basado en el alcance de las TIC en nuestra sociedad en términos económicos, sociales y ambientales. En la actualidad se han identificado dos enfoques de investigación, el primero analiza el consumo de energía en tiempo de ejecución del software y el segundo busca implementar las alternativas que pueden mejorar la sostenibilidad a partir de las buenas prácticas de la construcción de productos de software para generar impacto en entornos productivos. En consecuencia, se analiza diferentes aspectos del entorno de desarrollo para consolidar un conjunto de buenas prácticas que puedan ser incorporados los criterios de desarrollo de software sostenible.

Palabras-clave: Software Sostenible, Tecnologías Verdes, Desarrollo de software.

Good practices for the development of sustainable software.

Abstract: In recent decades, the use of information and communications technology (ICT) and software systems has increased exponentially, facilitating different processes and activities of daily life. However, the use of technology significantly affects growing energy demands and greenhouse gas emissions. Consequently, the concept of ecological software arises that seeks sustainable construction, based on the scope of ICT in our society in economic, social and environmental terms. Currently, two research approaches have been identified, the first analyzes the energy consumption in software execution time and the second

seeks to implement alternatives that can improve sustainability based on good practices in the construction of software products for generate impact in productive environments. Consequently, different aspects of the development environment are analyzed to consolidate a set of good practices that can be incorporated into the criteria for sustainable software development.

Keywords: Sustainable Software, Green Technologies, Software Development.

1. Introducción

La sostenibilidad ambiental es un propósito a nivel mundial, que promueve la reducción del consumo de energía y la emisión de gases de efecto invernadero. La Organización de las Naciones Unidas plantean una agenda estratégica para lograr un ecosistema viable y sostenible a partir de 17 objetivos que son complejos de cumplir, pero reconocen en la tecnología el camino para que se vuelvan alcanzables.

Sin embargo, las TIC también generan impactos negativos en los objetivos de sostenibilidad ambiental, dado que genera altos consumos de energía, pero por otro lado apoyan a las organizaciones en la eficiencia estratégica de los objetivos sostenibles a través de tecnologías como: el teletrabajo, la inteligencia artificial entre otras.

Esta doble incidencia de la tecnología ha llevado a investigar sobre aspectos como el ahorro eficiente de energía derivado de los dispositivos de hardware, sin profundizar en los impactos que produce el software. A nivel de software ecológico o sostenible, surgen investigaciones que se centran en la evaluación del consumo de energía del software en entornos de producción. Otra línea de estudio se asocia a la construcción de productos de software que apoyan iniciativas ambientales y por último se encuentran las investigaciones que analizan los diferentes aspectos de la construcción que inciden en los principios de sostenibilidad del software (Ibrahim, Danbala y Ismail, 2019).

Por lo tanto, cualquier producto ingenieril tiene un ciclo de vida, el cual determina las características de la construcción y operación. En el caso del software se debe analizar los efectos generados en los diferentes momentos del ciclo de vida que permiten identificar prácticas en la construcción de software para el cumplimiento de los criterios ambientales, sociales y económicos propios del concepto sostenible (Naumann et al. 2011).

Dada la necesidad de reducir los efectos negativos sobre el medio ambiente, específicamente la incidencia que tiene el uso de tecnología en cuanto al incremento del consumo energético y las emisiones de gases de efecto invernadero, se plantea un marco de buenas prácticas que buscan generar soluciones de software sostenibles que aporten a los retos energéticos actuales y futuros, a partir de los diferentes eventos transaccionales de datos, prácticas de trabajo, optimización de procesos entre otros.

La presente investigación busca la definición de un framework que facilite el desarrollo de software sostenible, compilando prácticas que propicien la optimización de los procesos y productos asociados la construcción, operación y mantenimiento del software. Para ello, se identifican los patrones arquitectónicos y entornos de trabajo de mayor preferencia para el desarrollo de software a través de un estudio de campo que busca conocer la percepción de las fábricas de software ubicadas en la ciudad de Medellín. Igualmente,

se realiza la caracterización de las prácticas y estrategias concebidas en el contexto del software sostenible. Por último, se consolida un marco de trabajo de buenas prácticas a partir de los aspectos analizados que propician la construcción de software para mitigar los impactos negativos que produce el uso de tecnologías para favorecer un ecosistema responsable y pertinente con la realidad del entorno socioambiental en el que se vive actualmente.

2. Materiales y Metodos

2.1. Revisión de literatura

En esta sección se plantean los estudios desarrollados en el contexto de las tecnologías verdes relacionadas con el desarrollo de software sostenible.

El concepto tecnologías verdes acorde con los autores (Orellana, Guzmán y Sañay, 2021), está definido como el estudio y la práctica de diseñar, desarrollar, usar y disponer de computadoras, servidores y diferentes periféricos tales como monitores, impresoras, dispositivos de almacenamiento, de redes y comunicaciones eficientes con impacto mínimo o nulo en el medio ambiente.

Igualmente, en el contexto de las tecnologías verdes surge el termino software sostenible que según Carrascal (2021), lo define como el producto que genera impactos negativos mínimos en los aspectos económicos, sociales y ambientales como resultado del desarrollo, el despliegue y el uso del software en pro del desarrollo sostenible.

Según los autores Lamis et al. (2020), la virtualización se convierte en un mecanismo que permite compartir los recursos de cómputo en distintos ambientes permitiendo que, funcionen diferentes sistemas en la misma máquina física; para lo cual, se crea un recurso físico único para los servidores, almacenamiento y aplicaciones. Del mismo modo la virtualización se encarga de crear una interfaz externa que esconde una implementación subyacente mediante la combinación de recursos en localizaciones físicas diferentes, o por medio de la simplificación del sistema de control.

Asimismo, en el contexto tecnológico el elemento que disminuye el impacto tecnológico es el Cloud Computing, dado que se convierte en un modelo que, permite el acceso bajo demanda y a través de la red a varios recursos, tales como: redes, servidores, capacidad de almacenamiento, aplicaciones y servicios. Estos recursos pueden ser asignados y liberados de forma rápida y con trámites sencillos, eliminando también los costos fijos y las grandes inversiones en TI. (Castro, 2014).

Por otra parte, existen métricas que permiten evaluar la energía, el rendimiento, la utilización, el consumo y el impacto económico en el uso de la tecnología; lo cual justifica el uso de métodos verdes para controlar estos aspectos en el desarrollo de aplicaciones de software. (Hernández, 2018).

De acuerdo con Olivera y Paz (2018) específicamente para el producto existen métricas que valoran la calidad del software tales como la portabilidad, usabilidad y eficiencia. Siendo un elemento fundamental para lograrlo la arquitectura del software, dado que, a grandes rasgos, es la vista del sistema que incluye los componentes principales del mismo,

la conducta de esos componentes y las formas en que los componentes interactúan y se coordinan para alcanzar la misión del sistema.

En consecuencia, para implementar buenas prácticas con un enfoque sostenible en el desarrollo de software, es necesario establecer un marco de trabajo o framework que integre un conjunto estandarizado de conceptos, prácticas y criterios que faciliten el propósito que se busca en el software (Maia et al., 2019) (Hernández, 2018).

Dado que un framework proporciona una base para crear programas usando un determinado lenguaje de programación y una arquitectura de software, simplificando el proceso de desarrollo ya que proporciona elementos para procesar entradas, gestionar los dispositivos de hardware e interactuar con el software del sistema (Hernández, 2018).

2.2. Metodología

La metodología comprende las investigaciones de tipo descriptiva, exploratoria y correlacional (Cazua, 2006), que a continuación se describen:

- Investigación descriptiva: En un estudio descriptivo se seleccionan una serie de cuestiones, conceptos o variables y se mide cada una de ellas independientemente de las otras, con el fin, precisamente, de describirlas. Estos estudios buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno. Los estudios descriptivos) sirven para analizar cómo es y se manifiesta un fenómeno y sus componentes (ejemplo, el nivel de aprovechamiento de un grupo).
- Investigación exploratoria: El objetivo de una investigación exploratoria es, como su nombre lo indica, examinar o explorar un tema o problema de investigación, sirve para familiarizarse con fenómenos novedosos, permitiendo identificar conceptos o variables promisorias, e incluso identificar relaciones potenciales entre ellas.
- Investigación correlacional: Tiene como finalidad medir el grado de relación que eventualmente pueda existir entre dos o más conceptos o variables, en los mismos sujetos. Más concretamente, buscan establecer si hay o no una correlación, de qué tipo es y cuál es su grado o intensidad (cuán correlacionadas están). En otros términos, los estudios correlaciónales pretenden ver cómo se relacionan o vinculan diversos fenómenos entre sí (o si no se relacionan).

Una vez identificado el problema y definido el alcance del trabajo, los pasos que se seguirán son los que se muestran en la tabla 1.

El estudio se soporta en tres fases para el desarrollo del marco de trabajo que articula el desarrollo de software y concepto de sostenibilidad. Todas las fases están orientados a estructurar el marco de trabajo, que agrupa un conjunto de buenas prácticas a partir del juicio de expertos para establecer la arquitectura de los proyectos de Software, previo a las actividades de construcción del producto.

Fase	Pasos	Actividades
Investigación exploratoria *Fase 1. Identificar los elementos arquitectónicos*	Paso 1.	Diseñar el instrumento del caso de estudio
	Paso 2.	Selección de la Población y muestra
	Paso 3.	Aplicación del instrumento
	Paso 4.	Análisis de los resultados.
Descriptiva *Fase 2. Caracterización del Software Sostenible*	*Paso 1.*	Planificar los criterios de inclusión y exclusión de la revisión de literatura.
	Paso 2.	Búsqueda en la literatura
	Paso 3.	Seleccionar los estudios, aplicando los criterios de inclusión y exclusión
	Paso 4.	Extracción de información de los estudios seleccionados
	Paso 5.	Análisis de la información.
Correlacional *Fase 3. Marco de Trabajo Software Sostenible: por medio de la construcción de un prototipo, para evidenciar*	Paso 1.	Selección de las Practicas Técnicas para el desarrollo sostenible
	Paso 2.	Selección de las buenas practicas del Proceso de desarrollo
	Paso 3.	Selección de la arquitectura
	Paso 4.	Diseño del marco de trabajo
	Paso 5.	Construcción del prototipo
	Paso 6.	Validación

Tabla 1 – Fases de la metodología.

2.2.1. Fase 1: Identificar los elementos arquitectónicos

De acuerdo con lo establecido en la Fase 1, que busca Identificar los elementos arquitectónicos y reconocer las arquitecturas de desarrollo de software a través de un estudio de campo, para determinar las más utilizadas.

Para el desarrollo del estudio de campo se diseñó un instrumento con los siguientes interrogantes:

P1. ¿Qué patrón de arquitectura de software utiliza en su área de trabajo?

P2. ¿Qué framework de desarrollo utiliza en su área de trabajo?

La muestra para el estudio de campo correspondió a 15, el perfil corresponde a expertos que cumplen funciones de arquitectos y/o líderes de desarrollo en las fábricas de software de la ciudad de Medellín y el área metropolitana, todos ellos dieron respuesta las preguntas a partir de su experiencia.

En la Figura 1, se encuentran los resultados obtenidos al primer interrogante frente al patrón arquitectónico instanciado para el desarrollo de soluciones de software.

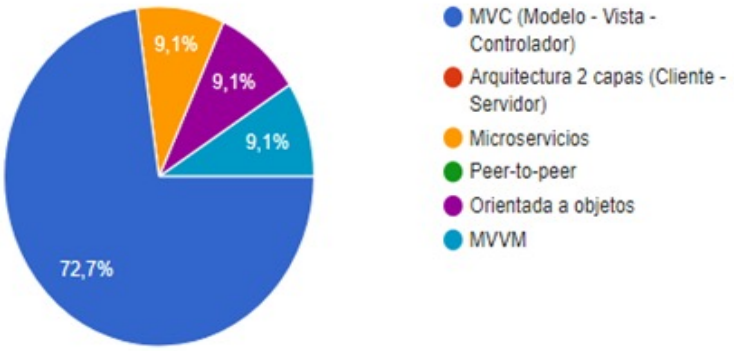


Figura 1 – Uso de patrones arquitectónicos.
Fuente (elaboración propia)

Se obtienen los patrones arquitectónicos mayormente usados: MVC (Modelo–Vista – Controlador), con 72,7% y los patrones microservicios, orientado a objetos y MVVM (Modelo – Vista – Vista – Modelo) cuantificados con 9.1%.

Sin embargo, la elección del patrón arquitectónico debe tener correspondencia con el ambiente para el cual se construye la aplicación. Asimismo, se deben evaluar la conveniencia del patrón frente a los atributos que favorezcan criterios de calidad de la aplicación. A continuación, en la tabla 1, se muestran los criterios planteados a partir de los autores (Giraldo, Vargas y Garzón, 2021), para seleccionar el patrón apropiado para el desarrollo de la aplicación.

Atributos de Calidad	**Ambiente**	**Patrón apropiado**
Mantenibilidad, rendimiento y flexibilidad	Aplicación web	MVC
Mantenibilidad, rendimiento y seguridad	Aplicación web	Microservicios
Modificalidad, rendimiento y testeabilidad	Aplicación Móvil	MVP
Rendimiento, mantenibilidad y velocidad	Aplicación Escritorio	MVC

Fuente: elaboración a partir de (Giraldo, Vargas y Garzón, 2021)

Tabla 2 – Criterios para elegir un patrón de arquitectura

Basados en la información obtenida de la pregunta 2, se identificó que el framework que más utilizan los desarrolladores en sus áreas de trabajo es Spring y en segundo lugar angular.

La elección del framework de desarrollo debe propiciar la implementación del patrón arquitectónico seleccionado previamente.

2.2.2. Fase 2. Caracterización del Software Sostenible

En esta fase se definen las características y prácticas de Software Sostenible, por medio de la revisión documental para realizar el diseño de un marco de trabajo de desarrollo de software. A partir de los autores (Ambrosi y Castro, 2015), (Kocak, 2013) se describen los atributos que comúnmente debe incorporar un software para cumplir con criterios de sostenibilidad, tales como:

- Sostenibilidad ambiental.
- Computación eficiente en energía.
- Eliminación de hardware de manera responsable.
- Uso de fuentes de energías renovables.

Para establecer la sostenibilidad de un producto se requiere analizar las fases del ciclo de vida. Los atributos sociales, ecológicos y económicos deben analizarse en la construcción del software con el propósito de asegurar las fases siguientes como la operación y mantenimiento del producto.

En la tabla 3, se presentan las prácticas de mayor uso en el desarrollo del software sostenible.

Autores	Prácticas técnicas
Swacha (2022)	Virtualización de base de datos
Guamán et al. (2022)	Lenguaje de alto nivel
Mohankumar y Anand (2015)	Virtualización
Santhanam y Keller (2018)	Virtualización y Cloud Computing
Bose y Luo (2011)	Virtualización
García et al. (2015)	Buenas prácticas a nivel de desarrollo
Uddin (2021)	Grid computing, virtualización, cloud computing

Tabla 3 – Prácticas del desarrollo de software sostenible

De acuerdo los autores (Kern, Naumann, Dick, 2015) (Guldner, et al., 2021), las buenas prácticas del proceso desarrollo del software son:

- Selección del patrón de arquitectura.
- Teletrabajo.
- Grupos deslocalizados geográficamente.
- Documentación Digital.
- Tamaño de la documentación.
- Reusó.
- Uso de metodologías agiles.

2.2.3. Fase 3: Marco de Trabajo para el desarrollo de software Sostenible

La fase 3 presenta el diseño del marco de trabajo para el desarrollo de software, basado en el análisis de las arquitecturas y en la definición de características y prácticas de

sostenibles y su validación por medio de la construcción de un prototipo, para evidenciar los beneficios que se obtienen al utilizar las características que ofrece el marco de trabajo

El marco de trabajo se diseñó teniendo en cuenta, dos bloques que se pueden observar en la figura 2.

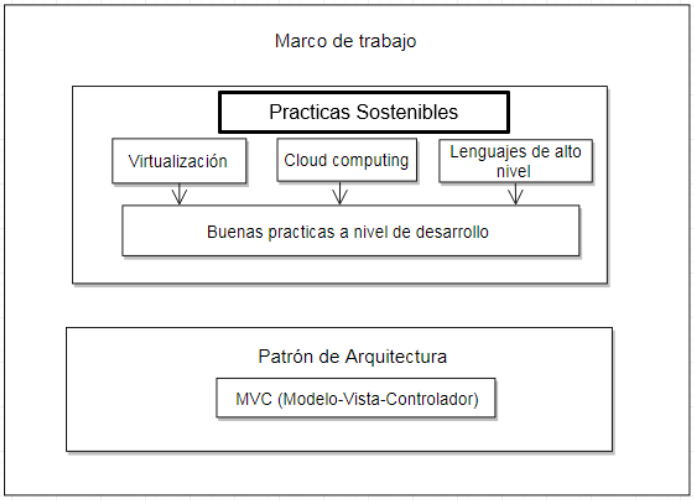


Figura 2 – Marco de trabajo.
Fuente (Elaboración propia)

En el primer bloque se encuentran las prácticas sostenibles requeridas para desarrollar un software, haciendo uso de dos tipos de prácticas:

- Practicas Técnicas: Se refiere a las practicas asociadas a la infraestructura requerida para el desarrollo y producción de la aplicación. Tales como: virtualización, cloud computing, lenguajes de alto nivel.
- Proceso de desarrollo: Las buenas prácticas del desarrollo que propician atributos de calidad del producto en producción y mantenimiento.

En el segundo bloque del marco de trabajo, se expone el patrón de arquitectura definido según el ambiente en el que se despliega la aplicación y los criterios de calidad priorizados en el proceso de desarrollo.

El prototipo construido responde a una aplicación web que soporta el proceso de reservar los laboratorios para una institución educativa y prioriza los criterios de mantenibilidad, rendimiento y flexibilidad.

Por lo tanto, el patrón definido fue MVC, y con base en el marco de trabajo se realizó la construcción del prototipo, el cual soporta el proceso para reservar laboratorios o espacios de prácticas académicas. En la Figura 3, se observa la arquitectura del prototipo basado en el patrón MVC.

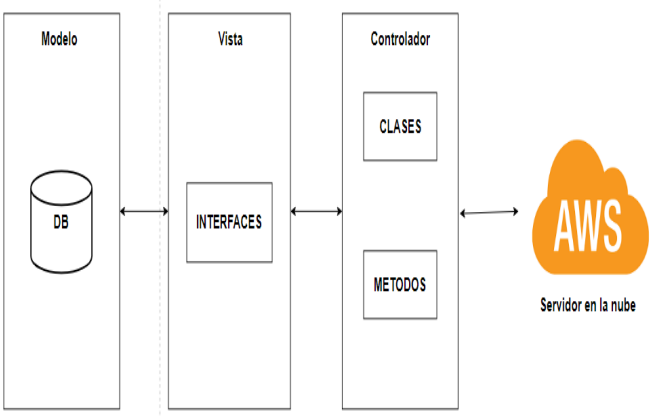


Figura 3 – Arquitectura del prototipo funcional. Fuente (elaboración propia)

Modelo: En la capa del modelo se encuentra alojada la base de datos de la aplicación, donde reposan los datos a procesar en cada operación que se realice dentro del aplicativo.

Vista: En esta capa se encuentran todas las interfaces para interacción con el usuario.

Controlador: En esta capa se encuentra alojada toda la lógica del negocio, que se divide en clases y métodos, y definen las funcionalidades que va a tener el aplicativo.

A nivel del proceso de desarrollo se instanciaron las siguientes practicas: Teletrabajo, Documentación Digital (tamaños de archivo inferiores a 5MB) y se realizó con la metodología ágil SCRUM.

Posterior a la construcción del prototipo se realizó la validación haciendo uso de una herramienta, la cual ayuda a constatar el tiempo de carga del aplicativo.

A partir de los datos generados por la herramienta con la cual se realizó la validación, se obtuvo, las siguientes medidas de desempeño:

- Tiempo de carga: 1.187 segundos.
- Primer byte en cargar: 0.332 segundos.
- Cantidad de peticiones cargadas: 14.

A continuación, en la Figura 4, se muestra en detalle el tiempo de carga de los diferentes scripts que componen la vista del registro de salas.

La eficiencia del prototipo desarrollado permite verificar que se obtiene una respuesta correcta en el menor tiempo posible. Esta característica está relacionada con el rendimiento de un dispositivo en función de su comportamiento temporal, el uso de recursos y la capacidad o límites máximos de funcionamiento. Los tiempos de respuesta y procesamiento, las tasas de rendimiento permiten identificar que los marcos de trabajo propuesto permiten servir de guía para el desarrollo de software sostenible, ya que la eficiencia del desempeño de la aplicación es esencial para el software sostenible.

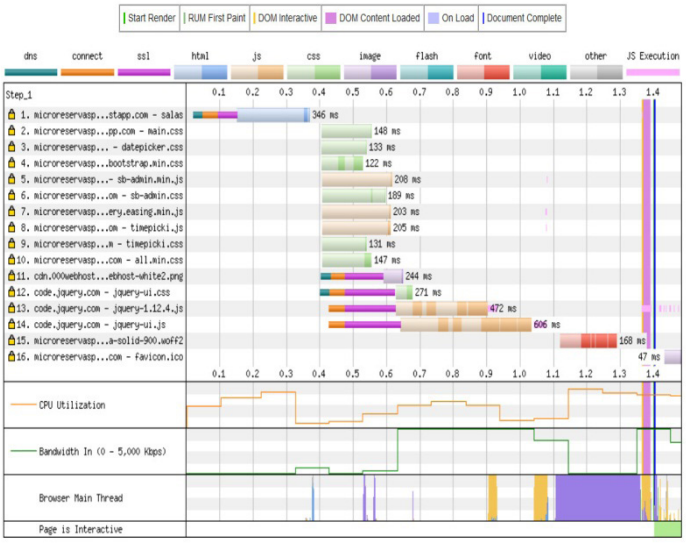


Figura 4 – Tiempo de carga.

Se proyecta como trabajo futuro la definición de un cuadro de mando de indicadores que permita monitorear los procesos asociados a la practicas del marco de trabajo. Igualmente, es necesario construir una herramienta que permita capturar las métricas de desempeño de las aplicaciones en ambientes de producción para cuantificar la demanda de recursos y establecer los rangos tolerancia frente al consumo de energía.

3. Conclusiones

El estudio de campo permitió identificar el patrón de arquitectura más utilizado en el campo laboral. Sin embargo, algunas organizaciones desarrolladoras asumen el patrón arquitectónico por conveniencia o tradición sin evaluar criterios de despliegue y calidad de la aplicación.

Los conceptos como virtualización, cloud computing, lenguajes de alto nivel, buenas prácticas de desarrollo de software brindan los recursos necesarios al momento de construir aplicaciones de software sostenibles debido a que generan impacto en las etapas de operación y mantenimiento del producto de software.

El desarrollo de software sostenible se sustenta en las buenas prácticas para obtener un producto con calidad y a su vez favorezca la reducción del consumo de energía en todas las fases del ciclo de vida de desarrollo de software, dado que incide en las variables sociales, ambientales y económicas que sustentan el concepto de sostenibilidad.

El marco de trabajo se realizó con el objetivo de recopilar los aspectos más relevantes de la sostenibilidad del desarrollo de software y así propiciar una guía tanto para los entornos de desarrollo académico y empresarial.

La validación realizada permitió evidenciar que al desarrollar aplicaciones de software basadas en un marco de trabajo de prácticas sostenibles generan beneficios significativos para el medio ambiente.

Referencias

Bose, R., & Luo, X. (2011). Integrative framework for assessing firms' potential to undertake Green IT initiatives via virtualization–A theoretical perspective. The Journal of Strategic Information Systems, 20(1), 38-54.

Cazua, P. (2006). Introducción a la investigación en ciencias sociales. Buenos Aires.

En Sistemas, L., Ambrosi, V. M., & Castro, N. (2015). GREEN IT.

García-Mireles, G. A., Moraga, M. Á., García, F., Calero, C., & Piattini, M. (2018). Interactions between environmental sustainability goals and software product quality: A mapping study. Information and Software Technology, 95, 108-129.

Giraldo Juan, Vargas Fabio y Garzon Kelly. (2021). Marco de Trabajo para Seleccionar un Patrón Arquitectónico en el Desarrollo de Software. RISTI-Revista Iberica de Sistemas e Tecnologias de Informacao, 2021, num. 25, p. 98-111.

Guamán, D., Pérez, J., Valdiviezo-Diaz, P., & Canas, N. (2022, April). Estimating the energy consumption of software components from size, complexity and code smells metrics. In Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing (pp. 1456-1459).Carrascal Vergara, C. D. (2021). Método para la evaluación de la sostenibilidad del software para el proceso de compra y contratación del sector público.

Guldner, A., Kern, E., Kreten, S., & Naumann, S. (2021). Criteria for Sustainable Software Products: Analyzing Software, Informing Users, and Politics. In Software Sustainability (pp. 17-42). Springer, Cham.

Hernández González, A. (2018). La sostenibilidad y el software. Dilemas Contemporáneos: Educación, Política y Valores, 5(2).

Ibrahim, M. M., Danbala, A. A., & Ismail, M. (2019). Towards attaining reliable and efficient green cloud computing using micro-smart grids to power internet data center. Journal of Computer and Communications, 7(07), 195.

Kern, E., Naumann, S., & Dick, M. (2015). Processes for green and sustainable software engineering. In Green in Software Engineering (pp. 61-81). Springer, Cham.

Kocak, S. A. (2013, October). Green software development and design for environmental sustainability. In 11th International Doctoral Symposium an Empirical Software Engineering (IDOESE 2013). Baltimore, Maryland (Vol. 9).

Lamis Rivero, J. M., Plasencia Soler, J. A., Marrero Delgado, F., & Nicado García, M. (2020). Metodología para priorizar iniciativas de tecnologías de la información sostenibles. Contaduría y administración, 65(2).

Maia, V., Gonçalves, T. G., & da Rocha, A. R. C. (2019, October). Quality Characteristics of Mobile Applications: A Survey in Brazilian Context. In Proceedings of the XVIII Brazilian Symposium on Software Quality (pp. 109-118).

Mohankumar, M., & Anand, M. K. (2015). A Green IT Star Model Approach for Software Development Life Cycle. International Journal of Advanced Technology in Engineering and Science, 3(1), 548-559.

Naumann, S., Dick, M., Kern, E., & Johann, T. (2011). The greensoft model: A reference model for green and sustainable software and its engineering. Sustainable Computing: Informatics and Systems, 1(4), 294-304.

Olivera Cokan, C., & Paz, F. (2018, July). A Web System and Mobile App to Improve the Performance of the Usability Testing Based on Metrics of the ISO/IEC 9126 and Emocards. In International Conference of Design, User Experience, and Usability (pp. 479-495). Springer, Cham.

Orellana, V. D. C. P., Guzmán, D. M. C., & Sañay, I. (2021). Propuesta de un Modelo Teórico para Green IT Governance. Polo del Conocimiento: Revista científico-profesional, 6(5), 29-45.

Pérez, J. M. (2011). Virtualización y green IT (Doctoral dissertation, Universidad Nacional de La Plata).

Reynoso, C. B. (2004). Introducción a la Arquitectura de Software. Universidad de Buenos Aires, 33.

Santhanam, A., & Keller, C. (2018). The Role of Data Centres in Advancing Green IT: A Literature Review. Journal of Soft Computing and Decision Support Systems, 5(1), 9-26.

Swacha, J. (2022). Models of Sustainable Software: A Scoping Review. Sustainability, 14(1), 551.

Uddin, M., Hamdi, M., Alghamdi, A., Alrizq, M., Memon, M. S., Abdelhaq, M., & Alsaqour, R. (2021). Server consolidation: A technique to enhance cloud data center power efficiency and overall cost of ownership. International Journal of Distributed Sensor Networks, 17(3), 1550147721997218.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 16/10/2021
Aceitação/Acceptance: 06/01/2022

Mapeo de Recursos y Capacidades para el fortalecimiento en la Gestión de la Innovación: Un Estudio de Caso en una Pyme del Sector Salud

Mauricio Antonio Bedoya Villa[1], Elkin Olaguer Pérez Sanchez[2], Jesús Manuel Ramos Garcia[3], Juan Carlos Avella[4], Paul Andrés Marino López[5]

mbedoya@udemedellin.edu.co; eoperez@udemedellin.edu.co; jmrg@azc.uam.mx; proyectos@cstar.com.co; pmarino@udemedellin.edu.co

[1] Profesor asociado, Facultad de Ciencias Económicas y Administrativas, Universidad de Medellín, Antioquia, Colombia.

[2] Profesor asociado, Facultad de Ciencias Económicas y Administrativas, Universidad de Medellín, Antioquia, Colombia.

[3] Profesor investigador, Departamento de Administración, Universidad Autónoma Metropolitana Azcapotzalco, México.

[4] Director investigador, Centro de Desarrollo Tecnológico C-Star, Casanare, Colombia.

[5] Profesor coordinador de programa, Facultad de Ciencias Económicas y Administrativas, Universidad de Medellín, Antioquia, Colombia.

Pages: 461-478

Resumen: Los recursos y capacidades son temas determinantes para la supervivencia de las organizaciones en los contextos actuales. El presente estudio se presenta a partir de un caso simple en una pequeña empresa innovadora del sector de la salud. El objetivo de este artículo es realizar un mapeo de recursos y capacidades de acuerdo con seis vectores de innovación en el sistema de gestión de la innovación. Las técnicas de recolección de datos se desarrollaron mediante el uso de un instrumento de mapeo que mide el nivel de madurez y define el perfil tecnológico de la empresa. Los resultados obtenidos demuestran que el desarrollo de los recursos y capacidades inciden de manera significativa en la implementación del sistema de gestión de la innovación. Finalmente, los resultados brindan nuevas ideas para la incorporación rutinas en las actividades de innovación para fortalecer la innovación y la creación de valor en las organizaciones.

Palabras-clave: Recursos, capacidades, gestión, innovación, Pyme

Resources and Capabilities Mapping for strengthening Innovation Management: A case study in an SME in Health sector

Abstract: Resources and capabilities are key issues for the survival of organizations in current contexts. This study is based on a simple case study in an innovative SME

in the health sector. This article aims to map resources and capabilities according to six innovation vectors in the innovation management system. The data collection techniques were developed using a mapping instrument that measures the level of maturity and defines the technological profile of the company. The results obtained show that the development of resources and capabilities has a significant impact on the implementation of the innovation management system. Finally, the results provide new insights for the incorporation of routines in innovation activities to strengthen innovation and value creation in organizations.

Keywords: Resources, capabilities, management, innovation, sme.

1. Introducción

La innovación y la tecnología están ampliamente reconocidas como un factor crucial para el crecimiento económico y fuente de competitividad en ambientes de cambio y complejidad. Actualmente, frente a las dificultades económicas que sufren las empresas en la época de crisis, resultado de la enfermedad del Coronavirus o Covid-19, se ha impactado de manera significativa a la mayoría de las empresas tanto en su estructura operativa como en su capacidad de generar ingresos o nuevas rutas de negocios (Cepal, 2020). Las pequeñas y medianas empresas (Pymes) has sufrido grandes impactos negativos resultado de la crisis económica, debido en gran parte en su poca capacidad de adaptación, sumado a eficiencias tecnológicas, limitada capacidad administrativa, humana y comercial que dificultan la supervivencia, siendo muy vulnerables ante los efectos adversos en la época de pandemia (Silva, Miranda & Hoffmann, 2021).

Generalmente, el sector empresarial de la Pymes ha sido consideradas como cruciales para la generación de empleo y productividad, enfrentando múltiples necesidades frente al cambio necesario por la competencia agresiva en las estructuras de operación y de su capacidad para gestionar la innovación. Para superar esos retos se deben llevar acabos proceso planificados con la intención de construir estrategias y contar con recursos para desarrollar innovaciones continuas durante los periodos de epidemia y crisis (Isaza, Kruger, Zanin, Márquez, Coa, Zanella, & Conte, 2022).

En ese contexto, en los ambientes competitivos actuales las empresas requieren de fortalecer sus recursos y capacidades, ya que han ido evolucionando en paralelo con los cambios en la economía mundial y la globalización. De la misma manera estudios recientes consideran que la transformación de conocimiento basados en las capacidades de innovación comprende un conjunto de valores, normas, creencias, acciones y decisiones para generar el conocimiento necesario para adaptarse a situaciones adversas (Lanzolla, Pesce y Tucci, 2021). Por lo tanto, es vital que las firmas enfrenten nuevos desafíos en ambientes turbulentos mediante el mejoramiento de los recursos y las capacidades para crear nuevos productos, procesos y servicios para obtener mejores niveles de desempeño organizacional (Pandit, D., Joshi, M. P., Sahay, A., & Gupta, R. K.,2018).

Estos recursos y capacidades son generadores de activos tangibles e intangibles, e incluyen otra serie de conocimientos y capacidades administrativas que se componen de ciertos elementos tales como rutinas, procesos organizacionales y el conocimiento que la organización controla para elegir e implementar estrategias, y de esta manera proveer a la firma de un mayor desempeño mediante prácticas innovadoras. En ese sentido,

de acuerdo con Du Plessis y Pretorius (2018) la mayoría de los ejecutivos concuerdan que la innovación es el camino para el éxito, y a pesar de su complejidad, esta debe ser gestionada por un sistema con una estructura formalizada. Por su parte, Chandrabai et al (2018) argumentan que la innovación conlleva a que las organizaciones tengan éxito a través de una buena gestión y la utilización de herramientas como la tecnología ya que forman el corazón o el eje central de la innovación.

Según Pérez et al (2019) el impacto de la gestión de la innovación está condicionado en gran medida en la alta dirección, la cual se verá reflejada en cada una de las funciones e instrumentos habilitados para llevar a cabo una correcta gestión de la innovación. Por ello se considera que la creación de un sistema que cuantifiqué y evalué las variables clave que intervienen en la gestión de la innovación es importante para las organizaciones, y así orientar la toma de decisiones a ciertos criterios previamente establecidos que tengan mayor influencia.

El objetivo de presente artículo es realizar un mapeo de recursos y capacidades en el modelo de gestión de la innovación en una institución prestadoras de servicios de salud (IPS), específicamente en una Pyme que enfrenta el gran desafío de reinventar sus formas de gestionar la innovación y poder generar nuevos modelos de negocios. La investigación surge como resultado de un proyecto de investigación vigente, a partir de una estancia posdoctoral mediante la convocatoria de vocaciones y formación en CTeI para la reactivación económica en el marco de la postpandemia 2020 en el mecanismo 2, desde el Ministerio de Ciencia Tecnología e innovación. Este proyecto busca el fortalecimiento a las capacidades de innovación en el portafolio de servicios de la empresa objeto de estudio la cual fue beneficiaria del programa con recursos del gobierno nacional.

La investigación pretende la identificación de áreas críticas para innovar, que le permita a la organización gestionar la innovación organizacional para la ejecución de proyectos de I+D+i de cara a los desafíos que plantea la reactivación económica y generación de nuevos empleos en el marco de la postpandemia. El diseño metodológico de tipo cualitativo se basa en un instrumento de mapeo según el modelo de evaluación de recursos y capacidades de innovación desarrollado por Bedoya (2018), y adaptado para Pymes, para medir el nivel de madurez de seis vectores dentro de la escala de innovación, utilizando la herramienta de radar de Innovación y de la misma manera dar respuesta a la pregunta de investigación ¿Cómo fortalecer los recursos y capacidades en el sistema de gestión de la innovación en una IPS para la reactivación económica en el marco de la Postpandemia?.

Este documento se encuentra estructurado de la siguiente manera: en primer lugar, se hace una breve introducción al tema destacando la importancia del mapeo de los recursos y capacidades basados en los estudios realizados por los principales autores en la temática. De la misma manera se plantea la pregunta de investigación, en segunda instancia se formulan los antecedentes teóricos de los recursos y capacidades para el fortalecimiento de los sistemas de gestión de la innovación, seguidamente el enfoque de la metodología detalla la forma de sintetizar los datos recolectados y finalmente, se presentan los resultados y la discusión que relacionan las variables clave, las acciones y factores críticos de éxito que permiten mejorar los procesos de gestión innovación en la organización objeto de estudio.

2. Marco teórico

La conceptualización de recursos y capacidades se define a partir de los estudios realizados por Barney (1991), el cual argumenta que la ventaja competitiva de una organización depende del uso sus recursos tangibles e intangibles. Sin embargo, es a partir de las investigaciones realizadas por (Cohen y Levinthal, 1990), que se argumenta sobre la capacidad de la organización para adquirir conocimiento valioso, para luego articularlo mediante procesos de transformación con los conocimientos existentes y de esta forma lograr su aplicación para la creación y explotación de nuevos productos y/o servicios. De la misma manera en estudios realizados por Zahra y George (2002), plantean que las capacidades dinámicas (CD) están compuestas por dos procesos, la capacidad de absorción potencial (Pacap) y la capacidad de absorción realizada (Racap), también conocidas en la literatura como capacidades de absorción (Acap). Cada constructo está conformado por dos subprocesos, la primera por la adquisición y la asimilación y la segunda por los subprocesos de transformación y explotación. Las CD se describen como la habilidad de una organización para percibir, aprovechar y adaptarse con el fin de explorar y explotar competencias específicas internas y externas en ambientes cambiantes. Igualmente, existen estudios que avalan la relación entre las CD y la teoría de recursos se han constituido en las teorías más prominentes para la generación de ventajas competitivas sostenibles (Barney, Ketchen, y Wright, 2011).

El constructo de las CD ha sido estudiado en las organizaciones a partir de diferentes enfoques en los campos de la gestión estratégica, la gestión tecnológica, la gestión de la innovación y el desempeño de la innovación (Cohen y Levinthal, 1990; Zahra y George, 2002; Camisón y Forés, 2010; Volberda, Foss y Lyles, 2010; Harris, Krenz, and Moat, 2021). A pesar de los avances obtenidos, se sigue presentando cierta confusión y diversidad en las definiciones, antecedentes, componentes y productos. Algunos autores en sus estudios las definen como recursos, otros como capacidades dinámicas y algunos más como capacidades organizacionales o como bases de conocimiento (Cohen y Levinthal, 1990; Zahra y George, 2002).

2.1. Capacidad de absorción potencial

Las Pacap incluyen las actividades de adquisición y asimilación, actúa como un puente entre la organización y el entorno (Fosfuri y Tribó, 2008). La adquisición, entendida como una habilidad para identificar y adquirir los nuevos conocimientos por medio rutinas utilizadas para identificar y adquirir datos considerados críticos para las operaciones organizacionales. (Jiménez-Barrionuevo, et al., 2011; Lam et al., 2017). La asimilación está enmarcada en el monitoreo, la adaptación al entorno y la identificación de las necesidades de la empresa, la cual requiere de altos niveles de flexibilidad para que la empresa pueda asimilarlos fácilmente (Rosenkopf y Nerkar, 2001). Es así como el conocimiento adquirido externamente puede incorporar una serie de nuevos procedimientos, los cuales pueden diferir significativamente de las técnicas habituales utilizadas por la empresa (Leonard-Barton, 1995; Szulanski, 1996).

2.2. Capacidad de absorción realizada

Según Zahra y George (2002) la capacidad de absorción realizada Racap, está conformada por dos dimensiones: transformación y explotación. La primera es entendida como

como la capacidad de desarrollar y refinar las rutinas que facilitan la combinación de los conocimientos que tienen los empleados de la organización y articularlos con los nuevos conocimientos que ya han sido adquiridos y asimilados, es decir la combinación del conocimiento nuevo con el conocimiento existente (Volberda et al., 2010; Zahller, 2012; Zahra y George, 2002). El otro subproceso es la explotación del conocimiento valioso, entendido como la capacidad organizativa que permite refinar, extender y apalancar las competencias existentes o crear nuevas competencias que incorporen los conocimientos adquiridos y transformados a sus operaciones (Rangus and Slavec, 2017).

2.3. Gestión de la innovación

Alrededor del término innovación y la forma de gestionarla existe una diversidad en cuanto a puntos de vista y acercamientos sobre lo que se puede definir o no como una actividad innovadora (McFadzean, O'Loughliny Shaw, 2005). De otro lado, la innovación se ha constituido en un factor importante en la estrategia empresarial como un camino que tiene las organizaciones para a la competencia agresiva en los entornos competitivos y los cambios de los mercados, la globalización de las economías en la sociedad del conocimiento (Bedoya, Toro y Arango, 2017). Autores como Schumpeter (1934), reconoce la innovación como aquella actividad que las empresas realizan para crear y mejorar nuevos productos y servicios, procesos, tecnologías, desarrollar nuevos mercados y procesos para enfrentar la competencia. De la misma manera las capacidades de desarrollar la innovación están fuertemente relacionada con las capacidades dinámicas (Shum y Lin, 2010).

De acuerdo con lo propuesto por Miller (1983), las organizaciones que promueven el emprendimiento innovador lo logran a través de la creación o mejora de productos, servicios, procesos, negocios, mercados, alternativas de materiales, y de los cambios estructurales en la gestión de la innovación en la organización. Estudios más recientes conducidos por Du Plessis y Pretorius (2018) consideran que la gestión de la innovación debe ser administrada desde los niveles más altos de la organización, así como también, debe ser parte de la estrategia empresarial. Por lo tanto, gestionar la innovación consiste en un proceso sistemático y específico para adquirir, organizar, mantener, aplicar, compartir y renovar el conocimiento tácito y explícito de todos los miembros de la organización, para aumentar el rendimiento y crear valor (Rivera, Russi y Rua, 2021).

Recientemente, la norma UNE-EN ISO 56002 de marzo de 2021 proporciona una clara orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la innovación aplicable en las organizaciones. Por lo cual define el sistema de gestión de la innovación como: "Un conjunto de elementos interrelacionados y que interactúan con el propósito de realizar valor y que provee un marco de referencia común para desarrollar y desplegar capacidades de innovación, evaluar el desempeño y lograr los resultados previstos" (Figura 1).

El sistema está basado el ciclo PHVA que permite la mejora continua del sistema de gestión de la innovación para asegurar que tanto las actividades como los procesos, recursos y soportes a la gestión logren evaluar la capacidad de una organización para innovar.

De acuerdo con lo anterior, la gestión de la innovación se conciben en la presente investigación como un concepto bastante versátil donde su aplicación puede verse reflejada en seis vectores o variables clave que componen el modelo sobre el cual se mide el nivel de madurez que tiene una empresa para gestionar sus recursos y capacidades para la gestión de la innovación tales como; (1) Estrategia de innovación; (2) Cultura de la innovación; (3) Estructura de la innovación; (4) Procesos de innovación; (5) Recursos para innovar y; (6) Las capacidades para transformar conocimiento en innovaciones.

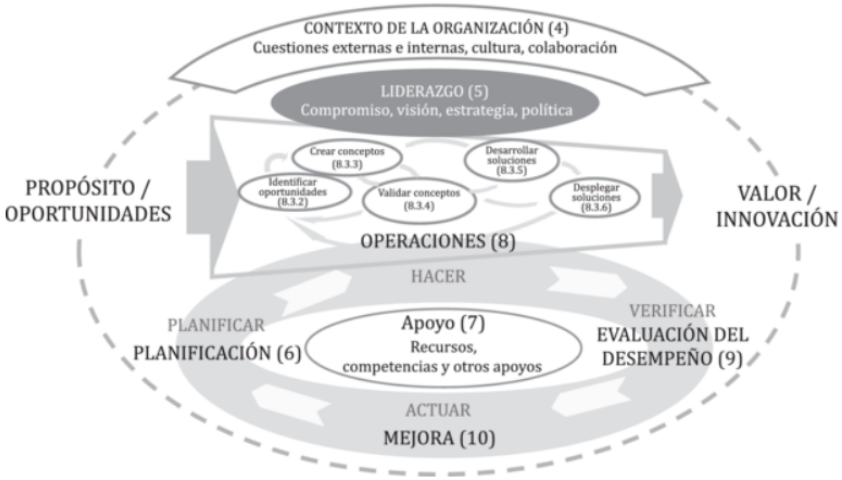


Figura 1 – Representación del marco del sistema de gestión de la innovación según norma ISO 56002:2021

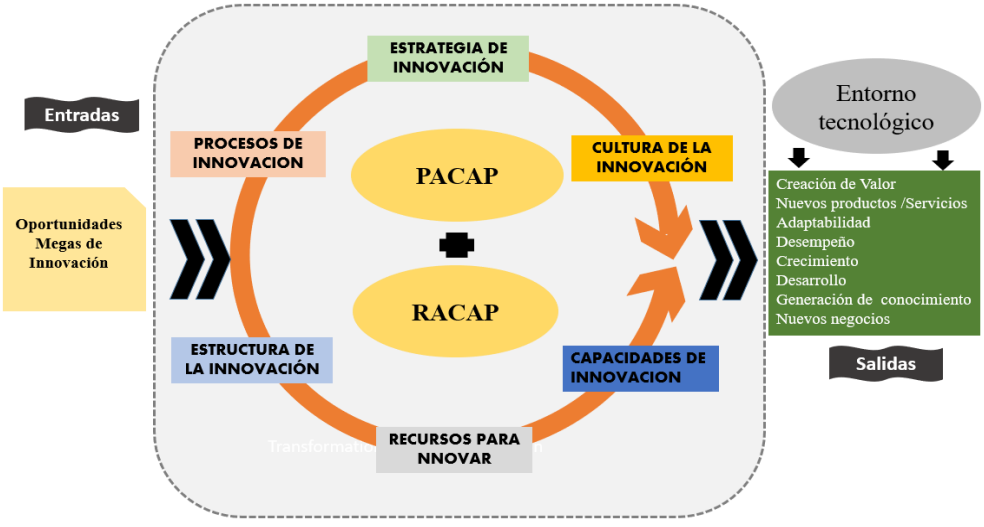


Figura 2 – Marco conceptual de mapeo de recursos y capacidades para el fortalecimiento del sistema de gestión de la innovación.

La figura 2 sintetiza el desarrollo del marco teórico sobre el cual se construye las cuatro dimensiones como una CD ante la necesidad de cambio y evolución de la organización, así como los vectores que integran el moldeo de gestión de la innovación.

El marco conceptual está basado en la interacción de los seis vectores para la evaluación de las capacidades de una empresa para innovar, las cuales interactúan de manera permanente como las rutinas habilitadoras del sistema gestión de la innovación constituidas por las Pacap y las Racap. Ambas capacidades tienen diferentes roles, pero coexisten y son necesarias para determinar el desempeño del sistema de gestión de la innovación por medio del liderazgo de la alta gerencia que se convierte en un aspecto crucial para fortalecer el aprendizaje organizacional (Iqbal, Ahmad & Li 2021). En síntesis, los desarrollos de las cuatro capacidades se construyen una sobre la otra, lo que hacen una CD coherente ante la necesidad de cambio y evolución del sistema de gestión de la organización permitiendo la adaptabilidad a los entornos tecnológicos.

3. Metodología

Bajo un diseño cualitativo se busca dar respuesta a la pregunta de investigación mediante una estrategia de investigación basada en un estudio de caso simple de acuerdo con los postulados de Yin (2009), quien ha establecido las directrices que soportan los diseños y que justifican la estructuración de un estudio de un caso simple. Tratándose de un muestreo aleatorio por conveniencia, la unidad de análisis estuvo compuesta por los líderes que tienen influencia en sistema de gestión de la innovación. Igualmente, se llevó a cabo un mapeo de la gestión de la innovación, como un proceso intencionado y dirigido a determinar las actividades claves o básicas de la empresa en el proceso de fortalecimiento en actividades de I+D+i. Metodológicamente se busca la identificación de los aspectos críticos a mejorar que permitan la gestión integral de la innovación en la empresa. En referencia a la técnica de recolección de datos, se llevó a cabo mediante un sistema de radar de la innovación que permite evaluar los 6 vectores del sistema de gestión de la innovación, todos ellos evaluados por 48 indicadores clave según el modelo de evaluación de recursos y capacidades de innovación desarrollado por Bedoya (2018) en su disertación Doctoral, fruto de una profunda revisión de literatura y el cual fue adaptado para las Pymes en el contexto colombiano.

Para la evaluación de los vectores se utilizó la siguiente escala de valoración: 5. Se cumple Plenamente; 4 Se cumple en alto grado; 3 Se cumple de manera satisfactoria; 2 Se cumple de manera regular; 1 Se cumple de manera insuficiente y; 0 No se Cumple. Para el tratamiento y análisis de datos se utilizó el entorno informático Excel, la cual es la plataforma en la cual está construida la matriz de datos e indicadores de la herramienta de mapeo de innovación.

Seguidamente, para la construcción de la estructura metodológica del estudio de caso se plantearon una serie de fases, de tal manera que el conjunto de actividades que lo componen están formuladas en relación con el objetivo, la pregunta de investigación y los resultados esperados, que sirvieron de sustento para la fundamentación teórica de la estrategia de investigación bajo el diseño del estudio de caso simple, las variables de estudio sujetas a validación en el trabajo de campo, la intervención de la unidad de

análisis, el uso del enfoque cualitativo y así llegar finalmente a los resultados mediante un enfoque de procesos, tal como se relacionan en la figura 3:

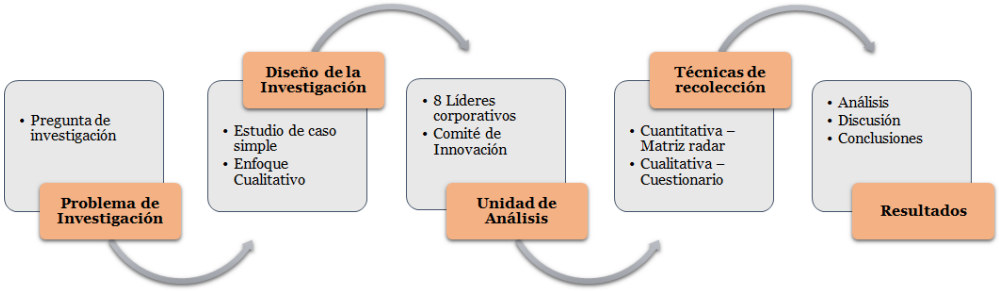


Figura 3 – Fases de la investigación.

4. Resultados

4.1. Perfil innovador de la empresa

La matriz del perfil innovador muestra la ubicación de la IPS en una de las cuatro categorías de perfiles innovadores según el nivel de recursos para innovar versus la capacidad para gestionar la innovación. Para ello se utilizó la herramienta del radar de la innovación para definir el perfil tecnológico de la compañía, el cual es de gran utilidad pues ayuda a comprobar si la empresa está preparada para innovar de forma continua y sostenible de acuerdo con el nivel de madurez.



Figura 4 – Resultado del perfil innovador según el mapeo de recursos y capacidades

El perfil innovador definido en la herramienta busca conocer cuatro categorías a saber: Innovador Naciente, Junior, Máster o Senior de acuerdo con los resultados del patrón de indicadores de las preguntas del cuestionario que alimenta el mapa de radar. La figura 4 muestra el resultado obtenido en la realización del ejercicio de aplicación del cuestionario del mapeo de innovación en la IPS.

Se logra una evaluación final de 2,48 sobre 5, quedando en la categoría del perfil innovador "Naciente", lo que significa que la a empresa presenta no solo algunas dificultades para innovar, sino que presenta situaciones de mejora en lo que se refiere a su actitud frente a la innovación. Aunque la IPS reconoce la innovación como un factor de crecimiento y desarrolla algunas actividades de innovación, apenas está iniciando algunas dinámicas en ese sentido, pero no son las suficientes para crear una ventaja competitiva sostenible.

4.2. Áreas críticas del sistema de gestión de la innovación

La Tabla 1 muestra los resultados globales del ejercicio de identificación de las áreas críticas para innovar.

Vector de Innovación	Factores	Inductores	Valoración Global
1. Estrategia	Estrategia, liderazgo e indicadores	Estrategia global, proactividad, presupuesto, misión y visión, objetivos, indicadores, alineación, planes de acción.	3.0
2. Cultura	Experiencias, hábitos costumbres y creencias	Creatividad, evaluación ideas, políticas, reconocimientos, intercambio, autonomía, tiempo para innovar, toma de riesgos.	2.00
3.Estructura	Estructura y diseño organizacional	Estructura, organigrama, integración, canales, formación, espacios, descentralización, comité formal	4.38
4. Procesos	Procesos, gestión de actividades	Mejora continua, desarrollo de servicios, intercambio ideas, optimización, modelo de gestion, actividades de i+d+i, proceso sistema.	1.50
5.Recursos	Recursos e infraestructura	Tiempo para innovar, programa informático, materiales, presupuesto formal, inversión en activos, métricas, financiación, incentivos.	1.25
6.Capacidades	Adquirir, asimilar, transformar y explotar conocimiento	Adquisición, asimilación, transformación, explotación, redes de conocimiento, prototipado, propiedad intellectual, transferencia.	2.75

Tabla 1 – Resultado del mapeo de innovación por áreas del sistema de innovación.

El objetivo de adjudicar la nota no fue intencionado simplemente para cuantificar el indicador en el cuestionario en cada vector de la herramienta de mapeo, sino más bien la calificación obtenida en conjunto, mediante un ejercicio de construcción colectiva de conocimiento, bajo la premisa de calificar lo más objetivamente posible. En el caso de

la IPS, se definieron las áreas críticas y procesos clave que debe trabajar la IPS en el corto y mediano plazo, los cuales hacen referencia específicamente a cultura, procesos y recursos para innovar, además de definir acciones claras en vía de la consolidación de un sistema de innovación y la construcción de estrategias optimas en I+D+i. Los resultados por áreas se relacionan a continuación:

4.2.1. Mapeo de la estrategia, liderazgo e indicadores

Este vector obtuvo un resultado global de tres (3.0). En ese orden, tres (3) de las dimensiones obtuvieron un resultado de cinco (5.0), lo que indica que la alta dirección de la empresa tiene definido los presupuestos, tiempo y recursos para la planeación, así como la innovación se encuentra explicita en la misión y la visión, además contempla algunos objetivos específicos en temas de innovación. Igualmente se encuentra dos (2) indicadores con clasificación en cero (0). Esta valoración indica que se requiere de una medición de los indicadores de desempeño de las variables asociadas a los objetivos de innovación para alinearlos con los objetivos globales. De la misma manera en referencia a la existencia de un plan de acción para las actividades de innovación, se logra una valoración de dos (2), la cual está muy por debajo de lo mínimo deseado.

4.2.2. Mapeo de la cultura experiencias, hábitos costumbres y creencias

La cultura es la base de la innovación logrando un resultado de dos (2), presentando cuatro (4) indicadores entre cero (0) y uno (1). Según el resultado se puede evidenciar que la empresa carece de un programa formal para evaluar las ideas generadas, además de contar con políticas claras para la promoción, reconocimiento e incentivos que ayudan a los equipos de innovación para que colaboren con la creación de valor del negocio. De la misma manera tres (3) indicadores están por encima de tres (3), lo que demuestra que la empresa si realiza efectivamente algunos esfuerzos en la promoción de una cultura innovadora, y además permite el libre intercambio de ideas entre el personal, la toma de riesgos y la capacidad para asumir retos.

4.2.3. Mapeo de la estructura y diseño organizacional

Aunque la evaluación global es alta con una valoración de cuatro - punto treinta y ocho (4.38). El resultado alto se explica en gran parte por el hecho que la empresa recientemente ha contado con un programa de fortalecimiento empresarial en temas de innovación, mediante el cual ha logrado definir el comité de innovación para la gestión de la innovación. Razón por la cual, cinco (5) de sus indicadores tienen la puntuación máxima, y tres (3) están por encima de lo mínimo deseado. Este equipo, al cual nos referiremos, tiene una estructura de innovación definida con representantes de todas las áreas y procesos de la compañía, y es el máximo responsable de garantizar que el proceso de innovación funcione dentro de la empresa.

4.2.4. Mapeo de los procesos de gestión y actividades

Los indicadores de procesos se encuentran en una valoración de uno punto cinco (1.5) siendo este vector el segundo con la puntuación más baja de todos los resultados globales. Cuatro (4.0) de los indicadores puntúan en cero (0), lo que indica la falta de tener un proceso de innovación optimizado, claro y definido para reducir el riesgo de las nuevas

innovaciones. Igualmente, no existe un modelo de gestión de la innovación explicito que detalle los procesos para la generación de innovaciones en la empresa. Tan solo dos (2) indicadores tiene una valoración de cuatro (4), lo que sugiere que la innovación contempla la mejora de los procesos del negocio, y se realizan algunas actividades para el desarrollo de nuevos productos y/o servicios.

4.2.5. Mapeo de mapeo de recursos e infraestructura

De manera global se logra un resultado de uno punto veinticinco (1.25), siendo la puntuación más baja entre todos los vectores de medición. Se evidencia la falta de recurso económicos para definir programas de incentivos, recompensas y tiempos necesarios para innovar. Adicionalmente la carencia de un programa informático que permita el monitoreo de ideas, procesos, portafolio de proyectos y resultados de innovación. Siete (7) de los indicadores están por debajo de una calificación aceptable y tan solo un indicador se encuentra en un nivel de cuatro (4.0), lo que significa que la empresa invierte regularmente en tecnología maquinaria, bienes y equipos para conseguir ventajas competitivas.

4.2.6. Mapeo de capacidades para adquirir, asimilar, transformar y explotar conocimiento

De acuerdo con el análisis de los resultados se obtiene un puntaje de dos puntos setenta y cinco (2.75), estando muy cerca de lo mínimo deseado para el vector. Lo que demuestra que la empresa hace uso de rutinas y habilidades para adquirir, asimilar, transferir y explotar el nuevo conocimiento para innovar y obtener ventajas competitivas sostenibles, siendo uno de los pilares del mapeo de innovación. El resultado del ejercicio implica que la IPS, está a pocos pasos para lograr el mínimo deseado para pasar la barrera de área critica. Cuatro indicadores logaron estar por encima del margen de lo aceptable y tan solo uno está en nivel de cero (0), indicando que la empresa integra la tecnología creada en su compañía con una que viene de fuera.

3.3. Radar con las áreas críticas del sistema de gestión de la innovación

La gráfica de radar representa de manera sistémica los resultados obtenidos por la empresa en los diferentes vectores de acuerdo con la posición de cada una de ellas, y el valor obtenido en correspondencia al cuestionario de preguntas estipulados en los 48 indicadores que se evaluaron en el mapeo de innovación, permitiendo así identificar el estado actual de la empresa de acuerdo con el desempeño de estas (ver figura 5).

En el radar se identifica un vector sobresaliente en la empresa, cómo es estructura, explicada en gran parte por su organigrama actual que está bien definido, además de la conformación del comité de innovación resultado de la presente consultoría científica. Por encima de la media están los vectores estrategia y capacidades. Los vectores de cultura y especialmente los de recursos y procesos, son de baja calificación y son los vectores más críticos de una intervención con mayor urgencia. Es decir, aunque la institución realiza algunas actividades de innovación, su sistema de gestión de la innovación requiere ser institucionalizado bajo un sistema que permita identificar nuevas oportunidades

de negocio y proyectar la IPS como un actor importante en temas de innovación en la región.

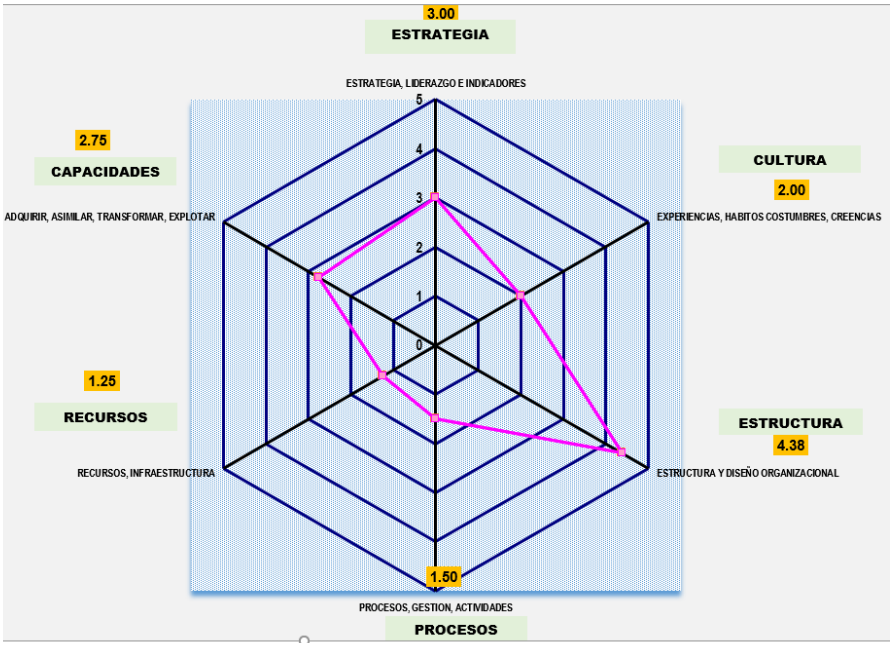


Figura 5 – Radar de innovación resultado de la evaluación de recursos y capacidades para innovar

5. Discusión

El presente estudio evalúa el estado actual de los recursos y capacidades de innovación para el fortalecimiento del sistema de gestión de la innovación en una empresa Pyme del sector de la salud en Colombia. Un mapeo de recursos y capacidades fue conducido con el objetivo de identificar el nivel de madurez y las áreas críticas del sistema de gestión de la innovación a partir de los datos categóricos extraídos de los cuestionarios aplicados según los seis vectores de innovación, según el enfoque metodológico y el marco conceptual y conforme a las conceptualizaciones realizadas por autores en la temática. En ese sentido, los resultados pretendieron responder a la pregunta de investigación ¿Cómo fortalecer los recursos y capacidades en el sistema de gestión de la innovación en una IPS para la reactivación económica en el marco de la Postpandemia? Los resultados obtenidos demuestran que existe un nivel de desarrollo de las Pacap y Racap que inciden de manera significativa en la implementación del sistema de gestión de la innovación.

En ese sentido, las capacidades dinámicas evaluadas en el modelo han permitido identificar y comprender las actividades desarrolladas por la empresa y de esta manera se han logrado asimilar conocimientos para implementar un sistema de innovación, en coherencia con las propuestas desarrolladas por Zahra y George (2002). Sin embargo, el uso de recursos y la implementación de capacidades organizaciones para lograr la

adaptabilidad y la creación de valor en el sistema, requiere de fortalecer una serie de rutinas que demandan recursos, habilidades y procesos para innovar en los ambientes tecnológicos. Los anterior resulta pertinente con los resultados existentes en la literatura por (Gao et al., 2017), quienes demostraron que mediante las CD las organizaciones fortalecen la capacidad para explotar conocimiento valioso hacia la innovación, y para lo cual se hace necesario realizar permanentes ajustes en la tecnología, procesos o metodologías que tiene la empresa, para aprovechar el conocimiento interno y externo para generar nuevos negocios. Por tanto, la medición de recursos y capacidades son factores clave para la organización, porque es allí donde debe concentrar sus esfuerzos cuando la estrategia competitiva es la diferenciación.

Los resultados obtenidos indican a través de la matriz de evaluación, la existencia de aspectos internos y externos que afectan la organización, y el entorno en el cual compite. Razón por lo cual se requiere mejorarlo y actualizarlo mediante un análisis experto, actualizar la visión y misión y formular los indicadores para los objetivos estratégicos con su respectivo plan de acción que defina claramente los responsables, meta e iniciativas estratégicas. Igualmente, los indicadores de resultados sugieren que la IPS debe formalizar mediante la formulación de políticas, un programa que promocione y reconozca a los colaboradores como forma de incentivo, para que éstos contribuyan a la generación y desarrollo de nuevas ideas y generar un clima de colaboración y transferencia de conocimiento. Este panorama general de la organización permite establecer una propuesta de intervención para el fortalecimiento de las capacidades logrando establecer un vínculo entre los problemas, oportunidades de mejora y las necesidades específicas para poder concentrar los esfuerzos de innovación (Chavarriaga, González y Vargas, 2019).

En ese contexto, los sistemas de gestión de la innovación exigen contar con un mecanismo que, en primer lugar, concentre las ideas mediante la creatividad para la mejora o desarrollo de nuevos productos, servicios o procesos; en segundo lugar, evalúe la viabilidad de estas por parte del comité, ya que se constituye en una fuente de información con su respectivo indicador que permite medir el desempeño de un programa de innovación. Para mejorar la capacidad innovadora las empresas deben fortalecer su sistema de gestión, creatividad e innovación ya que les permite aprovechar oportunidades en el mercado (Pérez, 2019). De la misma manera, se debe mejorar sustancialmente un proceso claro para le gestión de la innovación, pues se evidencia que hace falta institucionalizar un modelo para que los colaboradores sigan un proceso de aprendizaje continuo. Es por ello que se requiere tener un inventario actualizado de cómo la empresa analiza información del entorno para generar y gestionar el conocimiento adquirido, ya que es la base de múltiples indicadores que permiten valorar el capital intelectual en términos de habilidades y conocimientos de las personas, y poder mejorar los procesos de investigación y desarrollo en las empresas, tornándose más flexibles y adaptables, utilizando los recursos y aprendizajes externos a la organización (Apostolov, M., y Coco, N.,2021).

En términos generales los resultados ponen de manifiesto la necesidad de incorporar en sus rutinas habilidades de monitoreo del entorno. Esto se puede lograr mediante la institucionalización de un programa de vigilancia tecnológica e inteligencia competitiva, el cual debe estar a cargo del patrocinador de I+D. Por lo tanto, se deben tener más articulación con el ecosistema de innovación de la región, identificando actores clave

para participar en eventos y ruedas de negocios, ya que en estos escenarios participan expertos que tienen un panorama diferente en ciertos temas, lo cual se puede convertir en una oportunidad de obtener nuevas ideas clave para ser desarrolladas o incorporadas en la empresa. Igualmente se ve la necesidad de que la empresa cuente con programas de vinculación con universidades o centros de investigación, ya que de estas instituciones pueden emanar ideas y nuevos conocimientos aplicables en el ámbito empresarial, y que son fuentes valiosas de posibles innovaciones. En ese sentido, mediante la incorporación de esos conocimientos se puede llegar de una manera más fácil y practica a la explotación de nuevos productos o servicios resultados de las innovaciones desarrolladas ratificando así los planteamientos realizados por (Zhu, Zhao y Abbas, 2020), quienes manifiestan que las capacidades de una empresa dependen en gran medida, de la capacidad de absorción de los equipos innovadores mediante el uso de fuentes externas de conocimiento y la interacción entre ellas.

En referencia al presupuesto y recursos para fortalecer la innovación del sistema, especialmente, en este vector se visualiza que deben buscarse recursos para innovar, y adoptar estrategias de financiación para la consecución de recursos y fondos para financiar los proyectos innovadores que hagan parte del portafolio innovador, tanto con entidades de apoyo públicas y privadas de la región o fondos de capital de riesgo, lo que permitirá mejorar dicho indicador. Además, es evidente que las empresas que efectivamente hacen inversión o asignan recursos en actividades de I + D + i, y dedican un porcentaje del presupuesto anual de la empresa a las actividades de innovación, desarrollan de manera continua nuevos conocimientos, que permiten transformar y explotar conocimientos. Por ello se hace necesario fomentar en las Pymes las habilidades en los líderes de innovación para que puedan tener suficientes recursos y rutinas organizacionales para adquirir y asimilar conocimiento de manera sistemática y sistémica con un enfoque estratégico. Además, las percepciones y la experiencia de la alta dirección en esas actividades tienen un rol crucial en las decisiones estratégicas las cuales impactan el desempeño de la firma (Iqbal, Q., Ahmad, N.H. and Halim, H.A., 2020) y son factores determinantes para promover la transferencia de conocimiento y una visión compartida que soportan la capacidad para innovar (Le, P.B. y Lei, H.,2019)

Finalmente, los resultados presentados arriba tienen implicaciones de carácter gerencial, ya que, si los líderes de las organizaciones requieren fortalecer el sistema de gestión de la innovación, deben a como dé lugar, fomentar el desarrollo de las Pacap y las Racap de manera continua, que sirvan de apoyo a la formulación e implementación de las estrategias de innovación. A nivel de adaptabilidad en entornos competitivos, es importante que las empresas permanentemente estén haciendo seguimiento del conocimiento que está generando fuera de los límites de la organización, para así mantener actualizada la estrategia de innovación, y poder establecer vínculos permanentes con los stakeholders del ecosistema de innovación en el cual se encuentran inmersas.

6. Conclusiones

Este documento integra elementos teóricos y empíricos realizados por los investigadores acerca del uso de recursos y capacidades en los modelos de gestión de la innovación, básicamente con el objetivo de establecer unas variables clave para fortalecer el

desarrollo de capacidades de la innovación. De esta manera, se pudieron relacionar las variables clave que contribuye a robustecer el campo de conocimiento y la literatura existente, además que provee de nuevas ideas que permiten evaluar las condiciones y características necesarias del contexto interno y externo que deben estar presentes para fortalecer el campo de la gestión de la innovación.

Evaluar las capacidades de innovación con la metodología del mapa de radar en una empresa del sector de la salud, permitió evidenciar un estado general de la empresa, así como identificar las áreas críticas de la compañía, definiendo su perfil tecnológico y hacer un inventario de los recursos y capacidades clave que debe fortalecer la compañía que se convierte en un insumo importante para formular el plan de mejoramiento en los seis vectores del sistema de innovación que le permita a la empresa avanzar a un siguiente nivel en su modelo de gestión de la innovación.

Los resultados de este estudio demuestran que cuando se tiene una evaluación de todos los indicadores del sistema de gestión de la innovación, se puede tener un panorama más claro para desarrollar acciones y decisiones para lograr la adquisición, asimilación, transformación y explotación de conocimiento en las organizaciones, ya que permiten implementar estrategias de intervención en las áreas críticas posibilitando fortalecer el portafolio de productos y servicios.

Este artículo reconoce que existen limitaciones. Primero, se debe reconocer que el marco conceptual presentado en este estudio no es de carácter generalizable, ya que la visión estratégica, recursos y capacidades son propios y limitados en cada organización y del ambiente donde interactúan y segundo, tratándose de un estudio de caso simple en una pyme no es posible llegar a generalizaciones a todo tipo de tamaño en diferentes tamaños o sectores de la economía. Futuras investigaciones podrían contribuir a nivel empírico en la incorporación de nuevas variables que pudieron quedar por fuera de los intereses de esta investigación, tales como políticas e incentivos gubernamentales, fuentes de financiación, elementos de la transformación digital, entre otras, así como hacer estudios de caso múltiples entre empresas que compitan en ecosistemas de innovación en diferentes regiones.

Referencias

Apostolov, M. and Coco, N. (2021). Digitalization-based innovation—a case study framework. International Journal of Innovation and Technology Management, 18,05, 2050025

Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of management, 17(1), 99-120

Barney, J. B., Ketchen, D. J., & Wright, M. (2011). The Future of Resource-Based Theory: Revitalization or Decline? Journal of Management, 37(5), 1299–1315. http://doi.org/10.1177/0149206310391805.

Bedoya, M. A., Alzate, B. A., & Giraldo, L. M. (2018,). Corporate Entrepreneurship and Entrepreneurial Orientation: The Impact on Managing Capabilities for Innovation. In Portland 2018.

Bedoya, M. A., Toro, I. D., & Arango, B. (2017). Emprendimiento corporativo e innovación: una revisión y futuras líneas de investigación. Revista Espacios, 38(17).

Camisón, C., y Forés, B. (2010). Capacidad de absorción: antecedentes y resultados.

Cepal (2020). "El desafío social en tiempos del COVID-19". Comisión Económica para América latina y el Caribe. Informe Especial COVID-19, N° 3, Santiago, 12 de mayo.

Chandrabai, T., Ramesh, E., & Kumar, M. (2018). The role of technology management on innovationsuccess and performance of organization-empirical study. International Journal of Civil Engineering and Technology, 9(13), 819-26.

Chavarriaga, P. A. I., González, C. L., & Vargas, F. A. R. (2019). Evaluación de capacidades de innovación. Estudio de caso en una Institución Prestadora de Servicios de Salud (IPS) colombiana. Gerencia y Políticas de Salud, 18(37), 1-29.

Cohen, W.M., Levinthal, D.A. (1990). Absorptive capacity: a new perspective on learning and innovation. Administrative Science Quarterly 35, 128–152.

Du Plessis, M. J., & Pretorius, M. W. (2018, August). Does my organization need an innovation management function? : Towards a model for evaluation. In 2018 Portland International Conference on Management of Engineering and Technology (PICMET) (pp. 1-10). IEEE

Fosfuri, A. and Tribó, J. (2008). Exploring the antecedents of potential absorptive capacity and its impact on innovation performance. Omega, 3, 173-187.

Gao, Shijia; Yeoh, William; Wong, Siew Fan; Scheepers and Rens. (2017). A literature analysis of the use of Absorptive Capacity constructs in IS research International Journal of Information Management. Vol. 37 Issue 2, p36-42. 7p. DOI: 10.1016/j.ijinfomgt.2016.11.001

Harris, R. and Krenz, A. and Moat, J. (2021) 'The efects of absorptive capacity on innovation performance: a cross-country perspective.', Journal of Common Market studies., 59 (3). pp. 589-607.

Isaza, J. R. F., Kruger, S. D., Zanin, A., Márquez, V. J. B., Coa, L. M. D., Zanella, C., & Conte, A. (2022). Caracterización en la gestión de innovación de pymes por efecto del Coronavirus: estudio comparativo Colombia y Brasil. Revista Estrategia Organizacional, 11(1).

Iqbal, Q., Ahmad, N. H., & Halim, H. A. (2021). Insights on entrepreneurial bricolage and frugal innovation for sustainable performance. Business Strategy & Development, 4(3), 237-245.

Jiménez-Barrionuevo, M.M.; García-Morales, V.J. and Molina, L.M. (2011).: Validation of an instrument to measure absorptive capacity. Technovation, 31(5–6), 190-202. doi: 10.1016/j.technovation.2010.12.002

Lam, S. K., Sleep, S., Hennig-Thurau, T., Sridhar, S. and Saboo, A.R. (2017). Leveraging frontline employees' small data and firm-level big data in frontline management: An absorptive capacity perspective. Journal of Service Research 20,1, 12–28

Lanzolla, G., Pesce, D. and Tucci, C. L. (2021). The digital transformation of search and recombination in the innovation function: Tensions and an integrative framework. Journal of Product Innovation Management, 38, 1, 90-113. https://doi.org/10.1111/jpim.12546

Le, P. B., and Lei, H. (2019). Determinants of innovation capability: the roles of transformational leadership, knowledge sharing, and perceived organizational support. Journal of knowledge management

Leonard-Barton, D. (1995). Wellsprings of knowledge: Building and sustaining the sources of innovation

McFadzean, E., O'Loughlin, A., Shaw, E. (2005). Corporate entrepreneurship and innovation part 1: the missing link. European Journal of Innovation Management, 8(3), 350 - 372.

Miller, D. (2011). Miller (1983) revisited: A reflection on EO research and some suggestions for the future. Entrepreneurship: Theory & Practice 35(5): 873-894.

Pandit, D., Joshi, M. P., Sahay, A. and Gupta, R. K. (2018). Disruptive innovation and dynamic capabilities in emerging economies: Evidence from the Indian automotive sector. Technological Forecasting and Social Change, 129, 323-329.

Pérez, C. M. (2019). Innovación empresarial al servicio de la micro y pequeña empresa nortesantandereana: por la competitividad regional. *ECONÓMICAS CUC, 40*(1), 91-104. https://doi.org/10.17981/econcuc.40.1.2019.06.

Pérez-Campdesuñer, R., Ruiz-de la Peña, J., García-Vidal, G., Sánchez-Rodríguez, A., & Martínez-Vivar, R. (2019). Structural equations model to analyze the incidence of variables related to innovation management in organizations. International Journal of Engineering Business Management, 11, 1847979019856265.

Rangus, K. and Slavec, A. (2017). The interplay of decentralization, employee involvement and absorptive capacity on firms' innovation and business performance. Technological Forecasting and Social Change., 120: 195–203.

Rivera Ramirez, P. A., Russi Ardila, J. T., & Rua Moreno, L. T. (2021). Gestion organizacional para la mejora del area de gestion comercial en la empresa cosmeticos andre mediante la aplicación de innovacion.

Rosenkopf, L. and Nerkar, A. (2001). Beyond local search: boundary-spanning, exploration, and impact in the optical disk industry. Strategic Management Journal, 22(4), 287-306

Schumpeter, J. (1934). The Theory of Economic Development, Cambridge University Press, Cambridge.

Shum, P. and Lin, G. (2010). A resource-based view on entrepreneurship and innovation. International Journal of Entrepreneurship and Innovation Management, 11, 3, 264–281. http://doi.org/10.1504/IJEIM.2010.031901.

Silva, D. L. B. D., Miranda, A. L., & Hoffmann, V. E. (2021). Viva ou Deixe Morrer: estratégias para o enfrentamento da COVID-19 sob a perspectiva empresarial em São Luís do Maranhão, Brasil. Revista Brasileira de Pesquisa em Turismo, 15.

Szulanski, G. (1996). Exploring internal stickiness: Impediments to the transfer of best practice within the firm. Strategic Management Journal,17, 27-43.

Teece, D.J., Pisano, G., Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509–533.

Volberda, H. W., Foss, N. y Lyles, M. (2.010). Absorbing the Concept of Absorptive Capacity: How To Realice Its Potential in the Organization Field. Organization Science.

Yin, R. K. (2009). Case Study Research: Design and Methods. SAGE Publications.

Zahller, K. A. (2012). Scientia potentia est: Organixational Learning absorptive Capacity and the Power of Knowledge. En Y. K. Dwivedi, & e. al, Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 2. Orlando, Florida: University of Central Florida doi: 10.1007/978-1-4419-9707-4_6.

Zahra, S. A., George, G. (2002). Absorptive capacity: A review, reconceptualization, and extension. Academy of management review, 27(2), 185-203.

Zhu, H., Zhao, S., and Abbas, A. (2020). Relationship between R&D grants, R&D investment, and innovation performance: The moderating effect of absorptive capacity. Journal of Public Affairs, 20, 1, e1973.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 02/10/2021
Aceitação/Acceptance: 09/01/2022

Mapeo sistemático sobre la integración de tecnologías de inteligencia artificial y recursos TIC en aprendizaje-enseñanza musical

Cristian Fabian Bravo Mosquera[1], Manuel Francisco Silva Joaqui[2], Maria Isabel Vidal Caicedo[3], Eleonora Palta Velasco[4]

cfbravo@unimayor.edu.co; mfsilva@unimayor.edu.co; mvidal@unimayor.edu.co; eleonorapalta@unimayor.edu.co

[1]Institución Universitaria Colegio Mayor del Cauca. Edificio Bicentenario, carrera 7 # 2-34.

[2]Institución Universitaria Colegio Mayor del Cauca. Edificio Bicentenario, carrera 7 # 2-34.

[3]Institución Universitaria Colegio Mayor del Cauca. Edificio Bicentenario, carrera 7 # 2-34.

[4]Institución Universitaria Colegio Mayor del Cauca. Edificio Bicentenario, carrera 7 # 2-34.

Pages: 479-490

Resumen: Las herramientas software en la práctica de temáticas musicales proporcionan beneficios para el área de música, es por ello que representa gran utilidad en los programas de licenciatura en música, apoyando al docente en sus estrategias de enseñanza. El presente artículo realiza una investigación que brinda un mapeo sistemático de la integración de tecnologías de IA (inteligencia artificial) y recursos TIC (Tecnologías de la Información y Comunicaciones) en aprendizaje-enseñanza musical. Como resultado, se encontraron 12 estudios, los cuales fueron analizados y comparados considerando el tipo de estudio, la relación de integración de IA con el área de música, criterios de integración definidos, los métodos de validación usados, y las herramientas software propuestas. Además, expone una vista general de diseños, propuestas software y herramientas de evaluación melódica y musical, permitiendo conocer el avance en algoritmos clave para la integración de nuevas tecnologías y, a su vez, tener conocimiento de las ventajas de trabajar conjuntamente entorno a la música con las TIC en propuestas futuras.

Palabras-clave: Enseñanza-aprendizaje musical, apoyo tecnológico, inteligencia artificial, procesamiento de audio, TIC

Systematic mapping on the integration of artificial intelligence technologies and ICT resources in music learning-teaching

Abstract: Software tools in the practice of musical themes provide benefits for the music area, which is why they represent great utility in music degree programs, supporting teachers in their teaching strategies. This article carries out research that provides a systematic mapping of the integration of AI (artificial intelligence) technologies and TIC (Information and Communication Technologies) resources in music learning-teaching. As a result, 12 studies were found, which were analyzed

and compared considering the type of study, the relationship of AI integration with the area of music, defined integration criteria, the validation methods used, and the software tools proposed. It also provides an overview of designs, software proposals and melodic and musical evaluation tools, allowing to know the progress in key algorithms for the integration of new technologies and, in turn, to have knowledge of the advantages of working together around music with TIC in future proposals.

Keywords: Music teaching-learning, technological support, artificial intelligence, audio processing, TIC

1. Introducción

La integración de tecnologías de Inteligencia Artificial (IA) y recursos de las tecnologías de la Información y Comunicación (TIC) presenta grandes avances para el área de educación musical, contando con las posibilidades de generar interés en las personas que se adentran en la carrera profesional de música, por otro lado brindar apoyo hacia el docente en sus estrategias de enseñanza, al proporcionar recursos de aprovechamiento de la tecnología como eje central, en esta área donde su enfoque precede en herramientas tecnológicas didácticas o que generen interés al estudiante, con el fin de lograr materializar el conjunto de estrategias de enseñanza impartidas por el docente, estrategias empleadas por estudiantes y tecnología, en este caso tecnología de IA.

En este artículo se presenta un mapeo sistemático sobre la integración tecnologías inteligentes y recursos TIC en el aprendizaje-enseñanza musical. Inicialmente se presenta una selección de trabajos y estudios que permitan tener una idea clara sobre la implementación de la IA en el área musical, evidenciando los estudios realizados, diseño de arquitecturas, etapas de desarrollo, evaluación de resultados y aceptación de llevar a cabo la integración. Una vez seleccionados los estudios se clasifican de acuerdo con el tipo de estudio, soluciones propuestas, alcance en la investigación y desarrollo del mismo, evaluación de propuestas o recolección de información basado en los resultados obtenidos y se expone algunos factores a tener en cuenta para la implementación de tecnologías de IA en el área de música. De acuerdo con esto, este artículo se ha organizado con la siguiente estructura: Se presenta una vista general al método implementado para realizar el mapeo sistemático, resultados y técnicas implementadas para recolección de la información. Finalmente, conclusiones sobre el proceso de mapeo sistemático y trabajos futuros.

2. Trabajos relacionados

Luego de realizar una revisión a diferente literatura relevante acerca de herramientas tecnológicas para aprendizaje/enseñanza musical, se logra evidenciar la existencia de herramientas que permiten reforzar diferentes áreas de la educación musical. Sin embargo, las herramientas encontradas implementan técnicas para aprendizaje gramatical, de escritura musical o proponen software para producción y procesamiento de audio. Algunas de las investigaciones encontradas entre 2000 y 2022 han logrado mostrar un avance en el desarrollo e implementación del área TIC en los diferentes programas de aprendizaje, incluso algunas haciendo uso de la IA como base necesaria para la determinación de acciones para proporcionar métodos de enseñanza más efectivos y personalizados.

En (Valdivia Terrazas, Calsina Ponce, & Velazco Reyes, 2021) busca proporcionar un enfoque hacia el diseño experimental, que permita mejorar las aptitudes en los procesos de composición, arreglos musicales y orquestación. El uso del software proporciona el desarrollo de los aprendizajes para el uso de tareas, actividades estructuradas y guiadas, con instrucciones y recursos bien definidos, por medio de software como Sibelius y Finale pretende brindar un editor de partituras completo para escribir, ejecutar, imprimir y publicar partituras de música.

En (Nijholt, Reidsma, Ebbers, & Maat, 2008) un sistema que permite la dirección artificial para el análisis del audio a tiempo real de música interpretada por músicos. detecta en tiempo real el tempo y la dinámica, compara los resultados con las partituras y modifica el comportamiento de dirección cuando los músicos se desvían de la interpretación deseada. Este sistema hace uso de algunos módulos para la recolección y procesamiento de la información como, por ejemplo: Un módulo de percepción, que pretende analizar la partitura y la música interpretada, Módulo de cognición, el cual toma decisiones partiendo del análisis de la información, módulo de animación, el cual interpreta o permite visualizar los gestos de un director de acuerdo con las decisiones tomadas.

3. Metodología

El propósito de este estudio es indagar e identificar el estado del arte de herramientas tecnológicas para aprendizaje/enseñanza musical, analizando las principales características y tecnologías utilizadas. De la misma manera, generar la posibilidad de fomentar el desarrollo de futuras investigaciones con la integración TIC, haciendo uso de tecnologías innovadoras que permitan facilitar los procesos de aprendizaje-enseñanza musical. Teniendo en cuenta que el estudio es un tipo de mapeo sistemático, se tomaron en cuenta las recomendaciones propuestas en (Vakkalanka, Petersen, & Kuzniarz, 2015).

La pregunta de investigación principal definida para la elaboración de este trabajo es: ¿Qué estudios e iniciativas se han llevado a cabo para la integración de IA en aprendizaje-enseñanza musical?

La pregunta principal se dividió en seis preguntas más concretas que puedan ser analizadas detalladamente, tal como se muestra en la Tabla I.

#	Pregunta
RQ1	¿Qué estudios primarios existen para la integración de IA en el área de música?
RQ2	¿Qué tipos de soluciones han sido propuestas para integrar IA en el área de música y cuál es su alcance?
RQ3	¿Cuáles son los criterios usados para la integración de IA en el área de música?
RQ4	¿Qué herramientas software se han propuesto para la integración de IA en la música?
RQ5	¿Qué estrategias de validación se han usado en cada estudio?
RQ6	¿Cuáles son los factores de éxito o fracaso en la integración de IA en el área de música?

Fuente: Los autores

Tabla I – preguntas de investigación

En la tabla II se encuentran las cadenas de búsqueda básicas generadas a partir de palabras clave.

Cadenas de búsqueda básicas
(“inteligencia artificial” AND “música”)
(“Solfeo” AND “Inteligencia Artificial”)
intelligent tutoring system AND music
(“software” and “intelligence” and “music”)
Applied Intelligence of Music
artificial intelligence in music education

Fuente: Los autores

Tabla II – cadena de búsqueda

Las fuentes con las que se llevó a cabo el mapeo sistemático fueron: i) Bases de datos científicas: Science Direct, Springer Link, IEEE Xplore, EBSCO, Google Scholar. Asimismo, el rango de tiempo establecido fue desde el 2000 a abril de 2022.

Se realizaron búsquedas las bases de datos utilizando las cadenas de búsquedas propuestas y se utilizaron los criterios de inclusión: i) estudios que proponían estrategias o metodologías con el uso de tecnología para el área de música, ii) estudios escritos en inglés y español iii) estudios de publicaciones en revistas científicas y los criterios de exclusión se tomaron en cuenta: i) estudios que no proponían el uso de tecnología para el área de música, ii) estudios que no contaban con estrategias o metodologías para el área de música, iii) duplicidad de estudios.

4. Resultados

En la tabla III se presenta un consolidado con los motores de búsqueda y estudios analizados y seleccionados. Después de realizar la revisión de la información obtenida en los motores de búsqueda, se logró encontrar entre 10.000 a 100.000 registros de referencia, un gran volumen de información relacionada, pero al realizar las iteraciones de selección, se obtuvieron 28 estudios relevantes y se seleccionaron 12.

Fuente de búsqueda	Resultados encontrados	Estudios relevantes	Estudios seleccionados
Google académico	935.106	12	4
IEEE XPLORER	86	8	5
SpringerLink	38.109	4	1
EBSCO	949,791	4	2
Science Direct	26,306	3	0
TOTAL	973.843	31	12

Fuente: Los autores

Tabla III- estudios analizados y seleccionados

A continuación, se presentan los resultados del análisis de cada uno de los estudios relevantes logrados en la investigación.

4.1. Pregunta RQ1. Estudios para la integración de IA en el área de música

En la Tabla IV se muestran los estudios primarios incluyendo: Identificación del estudio, nombre del estudio, año de publicación y referencia. Los estudios se obtuvieron de las bases de datos científicas.

Id	Nombre del estudio	Año	Referencia
E1	Artificial Intelligence in Music Education: A Critical Review.	2000	(Holland, 2000)
E2	Interactividades en música sistema de tutoría inteligente	2005	(Phon-Amnuaisuk & Chee, 2005)
E3	The Virtual Conductor: Learning and Teaching about Music, Performing, and Conducting	2008	(Nijholt, Reidsma, Ebbers, & Maat, 2008)
E4	Design of an architecture for a MIDI based music e-tutor	2010	(Stanly & Ilango, 2011)
E5	Sing Master: An Intelligent Mobile Game for Teaching Singing	2016	(Dzhambazov & Goranchev, 2016)
E6	Artificial intelligence in music education	2020	(Yang F. , 2020)
E7	Application and Study of Musical Artificial Intelligence in Music Education Field	2020	(Yuan, 2020)
E8	Software Musical en la Enseñanza-Aprendizaje de los Estudiantes de Música de la Universidad Nacional del Altiplano Puno	2021	(Valdivia Terrazas, Calsina Ponce, & Velazco Reyes, 2021)
E9	Piano Performance and Music Automatic Notation Algorithm Teaching System Based on Artificial Intelligence	2021	(Yang Y. , 2021)
E10	Music Tutor: Application of Chord Recognition in Music Teaching	2021	(Liu, 2021)
E11	Handbook of Artificial Intelligence for Music	2021	(Miranda E. R., 2021)
E12	The Use of Wireless Network Combined with Artificial Intelligence Technology in the Reform of Music Online Teaching System	2022	(Yu L., 2022)

Fuente: Los autores

Tabla IV – estudios primarios

4.2. Pregunta RQ2. Tipos de soluciones propuestas y alcance de la integración

Se realiza la clasificación de los estudios según las propuestas de solución que se plantean. De igual manera, se clasifica en la columna de alcance si se proponen soluciones para la integración de herramientas tecnológicas en el área de música integrando la IA.

A partir del análisis de la información recolectada se puede destacar:

El tipo de solución que más se propone corresponde método de tutoría musical (E6, E8, E10), seguido de método de dirección musical (E3), diseño de método de tutoría musical (E2, E9), diseño de un modelo de tutoría musical (E4), método de tutoría vocal (E5), investigación de integración de IA y música (E1, E11), evaluación de implementación (E12).

	Tipo de solución	**Alcance**
E1	Investigación de integración de IA y música	Enfoque investigativo
E2	Diseño de método de tutoría musical	Enfoque investigativo
E3	Método de dirección musical	Propuesta software
E4	Diseño de un modelo de tutoría musical	Proyecto
E5	Método de tutoría vocal	Propuesta software
E6	Método de tutoría musical	Enfoque investigativo
E7	Método de evaluación de conocimientos	Enfoque investigativo
E8	Método de tutoría musical	Enfoque de desarrollo
E9	Diseño de método de tutoría musical	Propuesta software
E10	Método de tutoría musical	Propuesta software
E11	Investigación de integración de IA y música	Enfoque investigativo
E12	Evaluación de implementación	Proyecto

Fuente: Los autores

Tabla V – Tipos de soluciones y alcance de la integración

Con relación al alcance previsto, el 33.3 % brinda una solución basada propuestas de software diseñado y estructurado para el aprendizaje musical (E3, E5, E9, E10), el 41.6 % a un enfoque investigativo sobre la implementación de herramientas, áreas de control y el impacto en el área de música (E1, E2, E6, E7, E11), el 16.7% permite una vista a proyectos implementados en el área, la evaluación de rendimiento y efectividad(E4, E12) y el 8.3% plantea con enfoque de desarrollo la ejecución de métodos para el aprendizaje musical (E8).

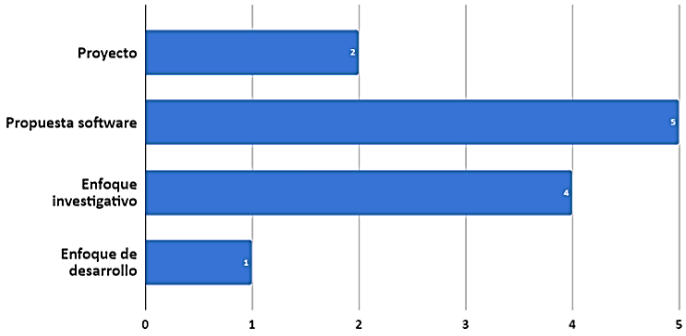


Figura I – alcance de la integración de las propuestas

4.3. Pregunta RQ3. Criterios usados para la integración de IA

En la tabla VI se especifican los criterios que se usaron para clasificar los estudios de acuerdo con las propuestas de cada uno en la implementación de la IA en el área de música. Se han definido cuatro categorías C1: Soluciones que permiten evaluar la implementación de IA en el proceso de aprendizaje musical. C2: Soluciones que permiten verificar los resultados de la implementación de la IA en el proceso de aprendizaje musical. C3: Soluciones que permiten evaluar el procesamiento y control de la información en las herramientas software. C4: Soluciones que definen las características y arquitectura de sistemas inteligentes para aprendizaje musical.

Categoría	Estudios
C1	E2, E4, E9
C2	E3, E12
C3	E3, E5, E9, E10
C4	E1, E6, E12

Fuente: Los autores

Tabla VI – tipos de soluciones y alcance de la integración

Las categorías descritas no son exclusivas, por ejemplo, el estudio E3 permite evaluar el procesamiento y control de la información de música, y también permite verificar los resultados de la implementación de IA en el proceso de aprendizaje musical.

Id	Elementos que se evalúan
E1	Realiza una revisión crítica de los principales enfoques para el uso de la IA en el área musical, desde instrucción asistida por computadora, sistemas de tutores inteligentes, un asistente de dirección musical, hasta educación musical teórica, con conceptos y técnicas en el área. Finalmente, se permite dar una crítica haciendo un comparativo en el diferente uso de técnicas y herramientas en la actualidad respecto a épocas anteriores, donde la implementación de la IA no resultaba tan común.
E2	Análisis basado en la interactividad de los estudiantes con la interfaz, la cual permite recolectar información, y así, evaluar la aprobación y comportamientos de los individuos frente al contenido musical, gráfico y textual.
E3	Realiza una evaluación en tiempo real, al audio recibido de la interpretación que realizan los músicos, y así, poder determinar acciones para corregir el tempo o ajustar la interpretación, con base en la partitura, reglas y expresiones de un director musical.
E4	Indaga sobre las posibilidades de crear un profesor de música en forma digital, que permita de forma virtual enseñar a los estudiantes un instrumento musical por medio de tecnología MIDI. Por esto, se realiza un estudio de las diferentes áreas de aprendizaje musical, y se determina la implementación del profesor de música, a su vez, diseñando una estructura que permita materializar el asistente inteligente.
E5	Se propone una herramienta móvil inteligente, que permite a los usuarios aprender canto. Hace uso de un asistente inteligente el cual propone material de estudio (canciones), evalúa el nivel de entonación, y así, generar corrección que se deben realizar basándose en el análisis de la información.

Id	Elementos que se evalúan
E6	Realiza un análisis de los medios en que se puede aplicar la IA, como el desarrollo de herramientas musicales en línea, reconocimiento de audio, presentación de material para estudio, visualizando las diferentes perspectivas de la implementación en el campo musical. En conclusión, se logra determinar que la tecnología en el área musical poco a poco ha ido incorporándose, pero necesita más apoyo y soporte en medios digitales y la nube para así permitir un apoyo más eficaz en el área de la educación musical.
E7	Determina la necesidad de fomentar la IA en los programas de postgrado en los conservatorios de música. En una vista a diferente material científico, muestran la necesidad de material de aprendizaje musical con implementación de IA para así facilitar la oferta de nuevos cursos. Esta investigación trata de identificar las principales áreas de la música con necesidad de implementación de IA como por ejemplo la identificación de partituras, la reparación de música y tener una vista general a divulgación de contenidos científicos de música y la IA.
E8	Refleja la implementación de herramientas existentes como componentes para la recolección de información musical, dando un vistazo sobre términos generales musicales, herramientas en diferentes áreas y los datos de los estudiantes sobre los test de reconocimiento visual, auditivo, interpretación y teoría musical. Parte desde la opinión de los estudiantes para determinar la valoración de la implementación de herramientas.
E9	Estudia las diferentes formas de implementación de IA en el proceso de aprendizaje de piano, haciendo uso de modelos matemáticos se propone un algoritmo que permite identificar la información y procesarla para así, lograr un entrenamiento íntegro del piano. Para la educación de piano es importante comprender las diferentes áreas, reglas, comportamiento del audio e interpretación de los estudiantes, y que permiten el diseño de la herramienta de integración IA al área de aprendizaje musical.
E10	Proponen una herramienta que funcionará como tutor, realizando sugerencias a los alumnos sobre su interpretación según la extracción de datos. Realiza el reconocimiento del mismo acorde entre diferentes instrumentos para identificar las diferentes características y proporcionar un plan de practica más claro y eficaz.
E11	Pretende dar a conocer las condiciones de la IA para adaptación en la comprensión musical, ramas que se podrían abordar y aplicaciones que son usadas para procesamiento de señales y sonido. Se intenta mostrar una idea definida de las características, criterios y factores necesarios para la implementación de herramientas en el área de música.
E12	Propone una vista a la propuesta de reforma en la educación musical por medio de un sistema en línea, se genera un sistema que permita realizar la creación musical por medio de IA y que por medio de esto el algoritmo puntúe al usuario. Calcula el impacto de la implementación de la IA en el aprendizaje musical, abordando diferentes cambios en el sistema tradicional.

Fuente: Los autores

Tabla VII – Elementos que se evalúan en cada estudio

4.4. Pregunta RQ4. Herramientas software de IA integradas en la música

Solamente los estudios E1, E3, E9 y E12 proponen herramientas software para la implementación de IA en la música. El estudio E1 propone un programa para Macintosh basado en el sistema experimental Vivace que evalúa los aspectos de conducción de voces de la armonización a cuatro partes.

El estudio E3 presenta la propuesta de un sistema que permite la dirección artificial para el análisis del audio a tiempo real de música. Detecta en tiempo real el tempo y la dinámica, compara los resultados con las partituras y modifica el comportamiento de dirección cuando los músicos se desvían de la interpretación deseada.

El estudio E9 propone el lenguaje Prolog y el sistema de aprendizaje asistido por música con el fin de estudiar en profundidad el principio y proceso de funcionamiento de la tecnología de grabación automática de música, para que el sistema de asistente de IA se pueda aplicar mejor a la enseñanza de la música.

El estudio E12 brinda la propuesta de un modelo de combinación de la tecnología IA y el sistema de educación en línea de música en el entorno de la red inalámbrica de quinta generación (5G).

4.5. Pregunta RQ5. Estrategias de validación de los estudios

En la Tabla VIII se pueden observar las estrategias de validación usadas en cada estudio.

Id	Estrategia de validación
E3	Se realizaron entrevistas a directores de orquesta y posteriormente una interacción de los músicos de orquesta con el director virtual, considerando las recomendaciones y comentarios de los directores.
E4	El sistema se probó con un conjunto de entradas de prueba (piezas musicales interpretadas) y comparando los resultados con resultados de expertos en evaluación de interpretación de partituras.
E8	Se hicieron encuestas para estudiantes del Programa de Música de la Universidad Nacional del Altiplano de Puno, antes y después de la intervención con los sistemas seleccionados (Sibelius y Finale).
E9	Se validó la herramienta con datos de prueba empleando la minería de datos.
E12	Se hicieron encuestas en línea a más de 1000 personas conformadas por profesionales y aficionados de la música.
E1, E2, E5, E6, E7, E10, E11	No es mencionada alguna estrategia de validación.

Fuente: Los autores

Tabla VIII – Estrategias de validación

4.6. Pregunta RQ6. Factores de éxito o fracaso en la integración de IA

A partir de los estudios analizados se ha identificado un conjunto de factores de éxito o fracaso que podrían ser tenidos en cuenta en trabajos de implementación de IA en el área de música (Tabla IX).

Factor 1. Adaptación en áreas donde existen formas de identificar y categorizar errores sistemáticos.	**Descripción**	Tales áreas son escasas en la música, lo que conlleva a ajustar el trabajo existente en tales áreas, y para identificar otras relativamente bien definidas en la música donde se aplican reglas y objetivos estrictos y rápidos.
	Fuente	**E1, E7**
Factor 2. Características de los datos a usar.	**Descripción**	Para el procesamiento con IA, este requiere audios de interpretación de instrumentos o interpretación vocal, partituras o información MIDI necesaria a la hora de realizar comparativos, reglas o normas a tener en cuenta en la música y el estudio de estado por parte de la IA que se genere al comparar la información de la partitura y el audio.
	Fuente	**E3, E4, E5, E9, E10**
Factor 3 Selección de área de implementación	**Descripción**	Requiere seleccionar un enfoque o área de implementación que permita desarrollar una idea clara en el funcionamiento de la IA. Por lo tanto, se clasifica en sistema de identificación o lectura de audios que permitan realizar un comparativo de los audios con las partituras o información MIDI y general una evaluación del estado de la interpretación, también, el sistema de apoyo teórico, que permite al estudiante según sus reacciones y aceptación al material determinar las rutas y planes de aprendizaje personalizado a este.
	Fuente	**E1, E2, E6, E7, E8, E9**
Factor 4 Arquitectura o estructura de funcionamiento	**Descripción**	Es necesario implementar una arquitectura de funcionamiento para el procesamiento del audio indicado, requiere desde componentes, módulos, reglas, normas y la implementación correcta del algoritmo de identificación o guía de aprendizaje área musical teórica
	Fuente	**E2, E4, E9**

Fuente: Los autores

Tabla IX – Factores para tener en cuenta en la integración de ia

5. Conclusiones

Como resultado del mapeo sistemático, se encontraron y seleccionaron doce (12) estudios primarios que tienen como enfoque la implementación de la IA en los diferentes procesos del área de música, publicados entre 2000 y abril de 2022. Partiendo del análisis de los estudios primarios, se puede observar que existen herramientas tecnológicas que brindan solución para áreas específicas de la música, contemplando la implementación de IA en dichos procesos.

Al analizar los estudios primarios se puede observar que existe integración de tecnología de IA en área específicas de la música, lo que propicia un alcance limitado hacia dichas áreas, tal como lo hace en E3 que el enfoque es en la práctica musical, lo que hace es simular a un director musical, dirigiendo de acuerdo a la captura de audio y adaptarse al cambio de tempo, ritmo y demás factores que perciba de los músicos en vivo, con el mismo enfoque se hace en E4 y E5, que cambian su estructura a detección de errores

de acuerdo a una melodía generada, lo que hace es comparar el audio generado por el que agrega o captura del usuario que realiza dicha práctica de melodía y posteriormente presenta los resultados de su práctica.

Como trabajo futuro se espera llevar a cabo la actualización del mapeo sistemático presentado, esto con el fin de incluir nuevos trabajos y tener una visión actualizada del estado del arte alrededor de la integración de tecnología de IA en el aprendizaje-enseñanza musical. Asimismo, como trabajo futuro se espera analizar la relación de los factores identificados y su aplicabilidad en gran parte de las áreas que posee la música. Teniendo en cuenta el análisis de los trabajos analizados y del creciente interés de la educación musical en la adopción de tecnologías como IA y recursos TIC, también se espera diseñar una solución que sirva de referencia para la integración de IA en aprendizaje-enseñanza musical, que facilite su implementación y utilización en la educación a nivel nacional e internacional.

Agradecimientos

Los estudiantes Manuel Silva y Cristian Bravo agradecen la contribución y orientación por parte de los docentes María Isabel Vidal y Eleonora Palta, y a la Institución Universitaria Colegio Mayor del Cauca.

Referencias

Dzhambazov, G., & Goranchev, K. (2016). Sing Master: An Intelligent Mobile Game forTeaching Singing. *8th International Conference on Games and Virtual Worlds for Serious Applications (VS-GAMES)*. doi:10.1109/VS-GAMES.2016.7590364

Liu, S. (2021). Music Tutor: Application of Chord Recognition in Music Teaching. *2021 International Conference on Signal Processing and Machine Learning (CONF-SPML)*. doi:10.1109/CONF-SPML54095.2021.00038

Simon, H. (2000). Artificial Inteligence in Music Education: A Critical Review. *Contemporary Music Studies. doi: 10.4324/9780203059746*

Miranda, E. R. (2021). *Handbook of Artificial Intelligence for Music* (1 ed.). Springer, Cham. doi:10.1007/978-3-030-72116-9

Nijholt, A., Reidsma, D., Ebbers, R., & Maat, M. (2008). The Virtual Conductor: Learning and Teaching about Music, Performing, and Conducting. *2008 Eighth IEEE International Conference on Advanced Learning Technologies*. doi:10.1109/ICALT.2008.43

Phon-Amnuaisuk, S., & Chee, K.-S. (2005). Interactivities in music intelligent tutoring system. *Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05)*. doi:10.1109/ICALT.2005.178

Stanly, M., & Ilango, K. (2011). Design of an architecture for a MIDI based music e-tutor. *International Conference on Audio, Language and Image Processing*. doi:10.1109/ICALIP.2010.5685054

Vakkalanka, S., Petersen, K., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. doi:10.1016/j.infsof.2015.03.007

Valdivia Terrazas, R. F., Calsina Ponce, W. C., & Velazco Reyes, B. (2021). Software musical en la enseñanza-aprendizaje de los estudiantes de Música de la Universidad Nacional del Altiplano Puno. *12*(1). doi:10.33595/2226-1478.12.1.471

Yang, F. (2020). Artificial Intelligence in Music Education. *2020 International Conference on Robots & Intelligent System (ICRIS)*. doi:10.1109/ICRIS52159.2020.00124

Yang, Y. (2021). Piano Performance and Music Automatic Notation Algorithm Teaching System Based on Artificial Intelligence. *Mobile Information Systems, 2021*, 13. doi:10.1155/2021/3552822

Yu, L. (2022). The Use of Artificial Intelligence Combined with Wireless Network in Piano Music Teaching. *Wireless Communications and Mobile Computing, 2022*, 18. doi:10.1155/2022/7989620

Yu, L., & Luo, Z. (2022). Artificial Intelligence Techniques for Joint Sensing and Localization in Future Wireless Networks. *Wireless Communications and Mobile Computing, 2022*, 18. doi:10.1155/2022/7989620

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 05/10/2021
Aceitação/Acceptance: 15/01/2022

Diseño de una aplicación gamificada como apoyo en los cursos de Física Cinemática en la Institución Universitaria Colegio Mayor del Cauca

Sebastian Quilindo[1], Royer Muñoz[2], Maria Isabel Vidal[3]

jquilindo@unimayor.edu; cormunozm@unimayor.edu.co; mvidal@unimayor.edu.co

[1] Estudiante Ingeniería Informática Institución Universitaria Colegio Mayor del Cauca, Popayán, 190001, Cauca, Colombia.

[2] Estudiante Ingeniería Informática Institución Universitaria Colegio Mayor del Cauca, Popayán, 190001, Cauca, Colombia.

[3] Docente Asistente, Facultad de Ingeniería, Institución Universitaria Colegio Mayor del Cauca , Popayán, 190001, Cauca, Colombia.

Pages: 491-500

Resumen: En la actualidad gracias al desarrollo de los video juegos y la gamificación, el desarrollo de aplicaciones gamificadas está teniendo una atención importante dentro de la educación. De esta manera se han aplicado en diferentes áreas del conocimiento y han tomado fuerza y popularidad. Aplicaciones como Doulingo, Minecraft: Education Edition, Kahoot! entre otros ha permitido que se presente una revolución en la forma como se aprende, incluyendo conceptos mecánicas y dinámicas de juego que favorecen el aprendizaje, especialmente en jóvenes y nuevas generaciones que tienen una muy buena relación con las Tecnologías de la Información y la Comunicación. Existen diversas investigaciones que presentan beneficios en el uso de aplicaciones gamificadas que incluyen diferentes tipos de actividades en diversas áreas del conocimiento, son usadas con el fin de diversificar y crear actividades gamificadas llamativas y que apoyen al estudiante en su proceso de aprendizaje. Pero la pregunta a la que todo esto nos lleva es ¿Cómo se logra esto? Realmente es posible gracias a la experiencia de usuario al cual llevamos a los estudiantes, quienes salen por un momento de un entorno de educación tradicional mezclando actividades lúdicas que seguramente son usadas en otros entornos, permitiendo que el estudiante haga asociaciones y relaciones entre conceptos y vivencias favoreciendo su proceso de aprendizaje. Este articulo presenta el desarrollo de una aplicación gamificada aplicada a los cursos de física mecánica de la facultad de Ingeniería de la Institución Universitaria Colegio Mayor del Cauca.

Palabras-clave: Dinámicas de Juego, Física Mecánica, Gamificación, Mecánicas de Juego

Design of a gamified application to support Kinematic Physics courses at the Institución Universitaria Colegio Mayor del Cauca

Abstract: Nowadays, thanks to the development of video games and gamification, the development of gamified applications is having an important attention within education. In this way they have been applied in different areas of knowledge and have gained strength and popularity. Applications such as Doulingo, Minecraft: Education Edition, Kahoot! among others, have allowed a revolution in the way people learn, including mechanical concepts and game dynamics that favor learning, especially in young people and new generations that have a very good relationship with Information and Communication Technologies. There are several researches that present benefits in the use of gamified applications that include different types of activities in various areas of knowledge, they are used in order to diversify and create striking gamified activities that support the student in their learning process. But the question that all this leads us to is: How can this be achieved? It is really possible thanks to the user experience to which we take the students, who leave for a moment of a traditional educational environment mixing playful activities that are surely used in other environments, allowing the student to make associations and relationships between concepts and experiences favoring their learning process. This article presents the development of a gamified application applied to the mechanical physics courses of the Engineering faculty of the Institution Universitaria Colegio Mayor del Cauca.

Keywords: Game Dynamics, Mechanical Physics, Gamification, Game Mechanics

1. Introducción

El desarrollo de una aplicación Gamificada para apoyo en la enseñanza de la física mecánica en los cursos de física de la facultad de Ingeniería de la Institución Universitaria Colegio Mayor del Cauca surge de las dificultades manifestadas por los estudiantes, usuarios del curso, identificadas a partir de una encuesta aplicada en donde se reúnen diferentes aspectos de la percepción y la forma como los estudiantes reciben el curso de física, específicamente el área de física mecánica, corresponde al entendimiento de los conceptos adquiridos y luego aplicarlos en actividades prácticas, teniendo en cuenta que dichos conceptos y la forma como se aplican suelen ser complejos y se dificulta el desarrollo de actividades prácticas y evaluativas. A partir de ellas se propone la construcción de una serie de actividades que apalancadas en dinámicas y mecánicas de gamificación se proponen con el fin de generar una aplicación gamificada que serán aprovechados para el estudiante.

Finalmente el diseño del juego fue presentado a 5 expertos entre los cuales se tenían profesores de la asignatura, estudiantes con la asignatura cursada y estudiantes con la asignatura no cursada y se obtuvo una retroalimentación sobre el diseño del mismo, con la cual se procederá a su construcción.

2. Aspectos preliminares

2.1. Gamificación

La gamificación se entiende como la unión de mecánicas, elementos y dinámicas que llevan al usuario a vivir una experiencia de juego inmersas en el uso de una aplicación

destinada a la enseñanza o entrenamiento de un tema específico (Valda Sanchez & Arteaga Rivero , 2015). En la actualidad la gamificación se presenta como buena alternativa a las estrategias de enseñanza tradicionales utilizadas en el aula, y ha sido ampliada a uso en el ámbito universitario como lo demuestran algunos estudios, generando mayor interés en los estudiantes y mejorando el proceso de aprendizaje de los mismos (Lozada-Ávila). En la siguiente grafica se presentan aspectos importantes que deben estar incluidos en la aplicación para que exista la gamificación.

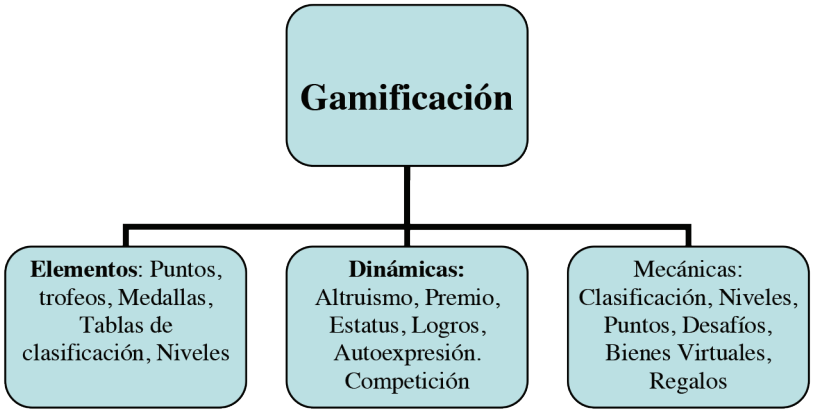


Figura 1 – Aspectos de Gamificación (Borrás Gené, 2022)

Las mécanicas del juego pueden ser consideradas como aquellos componentes que hacen que el juegador se interese en el juego y que el proceso gamificado avance. Entre sus elementos se destacan los retos, la posibilidad de competición, la cooperación, las transiciones y las recompensas entre otros (Quintanal Pérez, Opcion).

Las dinamicas por el contrario, en una aplicación gamificada corresponden a un concepto mas abtracto, en el cual permiten y buscan generar emociones en el jugador como la felicidad ganar, la curiosidad, el altruismo. Todas las herramientas diseñadas en el juego deben buscar apalancar dichas dinamicas y estas permiten ejercutar las mecanicas del juego (Cuba Rondón, 2021).

2.2. Aplicación Gamificada

Generalmente, una aplicación gamificada son aquellos módulos o desarrollos de software que dentro de su implementación se incluyen aspectos de gamificación con el fin de mejorar la experiencia de usuario y en casos específicos relacionados con educación se pretende mejorar la experiencia de aprendizaje en los estudiantes (Lobo Rueda , Paba Medina, & Torres Barreto, 2020). La gamificación, ha ganado importancia debido a que es usada al igual que en los videojuegos con el objetivo de generar una influencia positiva sobre los jugadores fomentando de forma positiva el aprendizaje del Estudiante (Díaz Cruzado).

2.3. Física Mecánica

La mecánica dentro del área de conocimiento de la Física hace referencia al análisis y estudio correspondiente al movimiento y reposo de los cuerpos, de esta manera se tiene en cuenta elementos como su comportamiento y evolución temporal en caso de la acción sobre si misma de diferentes fuerzas (Tipler & Mosca, 2008). En la siguiente figura se presenta la clasificación de la Física Mecánica

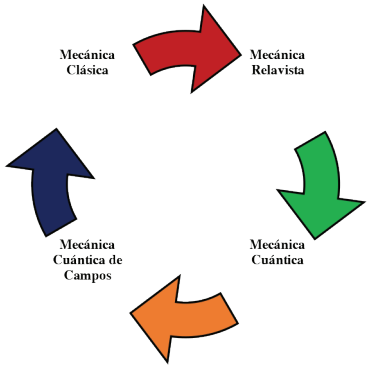


Figura 2 – Clasificacion de la Fisica (Tipler & Mosca, 2008)

2.4. Metodologia

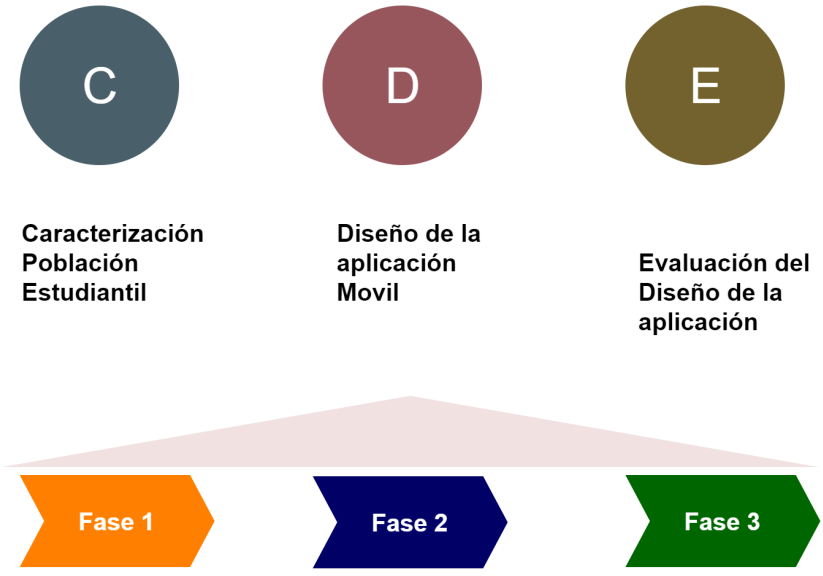


Figura 3 – Metodología de desarrollo del proyecti, Elaboración propia.

Para el desarrollo del proyecto se propuso abarcar 3 fases. En la fase inicial se realiza la caracterización de la población estudiantil del curso de física de la Institución Universitaria Colegio Mayor del Cauca, a través de un instrumento diseñado con el fin de obtener la experiencia de aprendizaje y los elementos relevante que afectan el proceso. En la segunda fase se procede a realizar el diseño de la aplicación teniendo en cuenta como insumos tanto el conocimiento de experto en el área como la experiencia de aprendizaje de la población estudiantil. Finalmente en la tercera fase, es realizado un Focus Group que permite evaluar el diseño por parte de profesores expertos en el área, estudiantes que recientemente habían cursado la asignatura y estudiantes que estaban iniciando el curso de la misma. En la siguiente figura se presenta la metodología abordada.

3. Desarrollo del proyecto

3.1. Recolección de la información academica y estudiantil

3.1.2. Informaciíon general sobre la asignatura de Fisica

Denfro de la formación del programa acádemico de Ingeniería Informática se tiene una asignatura que lleva por nombre Fisica Mecanica, ubicado en segundo semestre. En ta siguiente tabla se presenta el contenido sintetico de la asignatura.

Numero	Tema
1	Introducción: la física y la medición
2	Vectores
3	Movimiento en una dimensión
5	Las leyes del movimiento
6	Movimiento en dos dimensiones
7	Trabajo y energía
8	Energía potencial y conservación de la energía
9	Momento lineal y colisiones
10	Rotación de un cuerpo rígido alrededor de un eje fijo
11	Movimiento de rodadura, momento angular y momento de fuerza
12	Equilibrio estático

Tabla 1 – Contenido sintetico de la asignatura Fisica Mecanica

Esta información se retoma en el aparte de Diseño de la aplicación gamificada, en la tercera fase del desarrollo.

3.1.3. Caracterización de la población estudiantil

Con el objetivo de caracterizar la población estudiantil, se diseño un instrumento en el cual se obtienen datos de estudiantes que permitieron conocer datos básicos como su nivel de escolaridad, datos frente a la experiencia que tuvieron cuando cursaron la asignatura. En la siguiente tabla se muestran las preguntas formuladas en el instrumento, agrupadas por secciones. La primera sección de preguntas sobre información personal utiliza algunas preguntas abiertas. En la segunda sección en donde se hace referencia a los cursos de física mecánica abordados por el estudiante utiliza preguntas en su mayoría cerradas con valoraciones preestablecidas. En una tercera sección se solicita información sobre los temas específicos de la asignatura.

A continuación, se presentan los resultados de la aplicación del instrumento utilizado para la caracterización de la población estudiantil.

En total la encuesta fue diligencia por 40 estudiantes, de los cuales 10 no se encontraban asistiendo a la asignatura. Tomando como universo los 30 estudiantes que, si cursaban o habían cursado la asignatura, se tiene que el 31% de los encuestados viven en la ciudad de Popayán, mientras el resto vienen en zonas rurales y deben desplazarse hasta la ciudad para asistir a clases. Frente a la pregunta ¿Qué nivel de conocimiento tiene sobre la asignatura? El 9.5% tiene un conocimiento de nivel 1, el 52,4% de los encuestados consideran que tienen un nivel 3, mientras el 33,3& tienen un nivel 4 y el 9,5% tiene un nivel 5. De igual manera se evidencia que las actividades mas utilizadas en el aula de clase son: las clases magistrales, los laboratorios y trabajos grupales. En cuanto a las actividades a desarrollarse en los cursos, en la encuesta se propone incluir videos explicativos de las temáticas y los laboratorios. En cuanto las temáticas en las cuáles se presenta mayor dificultad de entendimiento y aprendizaje se presentan en la siguiente tabla, en donde se puede observar que el tema de energía y trabajo es uno de los más difíciles de apropiar según los estudiantes.

Sección	Pregunta	Tipo de pregunta
Información Personal	¿Cuál es su edad Actual?	Abierta
	¿Cuál es su lugar de Nacimiento?	Abierta
	¿Cuál es su nivel de escolaridad?	Cerrada. Presenta 5 niveles: Bachiller, Técnico, Tecnólogo, Universitario, Otro:
Información sobre la asignatura	¿Está cursando el componente de modulo Física Mecánica o lo ha cursado en semestres anteriores? Seleccione una opción	Cerrada. Pociones sí y no.
	¿Qué nivel de conocimiento tienes sobre la asignatura de física?, 1 es mínimo y 5 es máximo	Cerrada
	¿Qué actividades se utilizan en clase para abordar estos temas? seleccione una o más de una	Cerrada. Presenta 5 opciones. Y permite el espacio para consignar alguna actividad que no se encuentra en la lista y podría ser útil para el diseño de la gamificación de la aplicación.
	¿Qué actividades le gustaría que se utilicen para el desarrollo de las clases?	Abierta

Sección	Pregunta	Tipo de pregunta
Información sobre las temáticas de la asignatura	Sistemas coordinados	Cerrada. Se indica el nivel de dificultad de 1 a 5, siendo 1 el valor más bajo y 5 el valor más alto.
	Componentes de un vector y vector unitario	Cerrada. Se indica el nivel de dificultad de 1 a 5, siendo 1 el valor más bajo y 5 el valor más alto.
	Cruz y sus aplicaciones de la física	Cerrada. Se indica el nivel de dificultad de 1 a 5, siendo 1 el valor más bajo y 5 el valor más alto.
	Diagrama de movimiento	Cerrada. Se indica el nivel de dificultad de 1 a 5, siendo 1 el valor más bajo y 5 el valor más alto.
	Movimiento unidimensional	Cerrada. Se indica el nivel de dificultad de 1 a 5, siendo 1 el valor más bajo y 5 el valor más alto.
	Movimiento de proyectiles	Cerrada. Se indica el nivel de dificultad de 1 a 5, siendo 1 el valor más bajo y 5 el valor más alto.
	Leyes de Newton	Cerrada. Se indica el nivel de dificultad de 1 a 5, siendo 1 el valor más bajo y 5 el valor más alto.
	Movimiento circular	Cerrada. Se indica el nivel de dificultad de 1 a 5, siendo 1 el valor más bajo y 5 el valor más alto.
	Trabajo y energía	Cerrada. Se indica el nivel de dificultad de 1 a 5, siendo 1 el valor más bajo y 5 el valor más alto.
	Energía cinética	Cerrada. Se indica el nivel de dificultad de 1 a 5, siendo 1 el valor más bajo y 5 el valor más alto.

Tabla 2 – Preguntas del instrumento utilizado para la caracterizacion poblacion estudiantil

Tema	Valoración
Introducción: la física y la medición	2
Vectores	1
Movimiento en una dimensión	1
Las leyes del movimiento	1
Movimiento en dos dimensiones	2
Trabajo y energía	5
Energía potencial y conservación de la energía	4
Momento lineal y colisiones	2
Rotación de un cuerpo rígido alrededor de un eje fijo	3
Movimiento de rodadura, momento angular y momento de fuerza	4
Equilibrio estático	4

Tabla 3 – Preguntas del instrumento utilizado para la caracterizacion poblacion estudiantil

3.2. Diseño de la aplicación móvil

Una vez obtenidos los resultados de la caracterización, se procede a identificar las actividades en las cuales se propone aplicar gamificación con el fin de favorecer el aprendizaje de los estudiantes.

Para esta actividad se tuvo el acompañamiento de un experto en la temática y profesor titular de la asignatura.

En esta fase de trabajo surge una pregunta ¿Cuál es la diferencia entre un juego y una aplicación Gamificada?

Básicamente la respuesta a este interrogante se enfoca desde la utilización del juego como un elemento de diversión, sin embargo, dentro de la clasificación de juegos se tiene una categoría de Juegos serios, cuya diferencia con el primer concepto radica en que además de su finalidad de diversión tiene una finalidad educativa o de entrenamiento. A su vez dentro de los juegos serios existe muchas subcategorías, entre ellos los de tipo edutaiment. Los juegos además tienen como fundamento una historia, que enmarca las aventuras o las acciones que el jugador debe alcanzar y en algunos casos un avatar con el cual se identifica el jugador (Chipia Lobo, 2011). La aplicación gamificada no tiene historia, su fin no es diversión, son aplicaciones que pretenden desarrollar una o varias actividades que pueden considerarse rutinarias y que mediante gamificación se convierten en divertidas, generando en el usuario una experiencia de usuario agradable y divertida. Los juegos proporcionan inmersión mientras las aplicaciones gamificadas difícilmente pueden lograrlo (Aguilera Castillo, Fúquene Lozano , & Ríos Pineda, 2014).

El diseño de la aplicación considero prioritarios aquellos con valoración mas baja. Y se considera construir una aplicación que tiene 3 partes: la sección en la cual se explica la teoría, una segunda sección donde están los ejercicios prácticos, en donde se aplica gamificación y videos explicativos de los laboratorios.

A continuación, se presenta el mokups desarrollado para el tema de Energía y Trabajo.

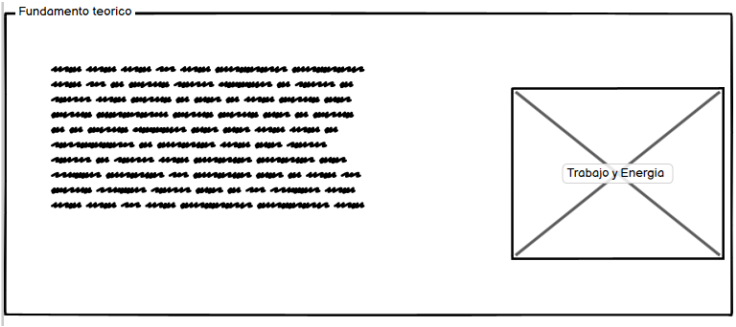


Figura 4 – Mocab fundamento teorico trabajo y energia. Elaboración propia.

En el primer mokup se presenta el contenido teórico acompañado con una imagen y texto. En el segundo mokup se presenta un ejercicio de aplicación sobre la temática. Se consideran entonces asignación de puntaje 5 puntos para el desarrollo correctamente, 3 puntos con algunos errores y 0 si esta totalmente errado. También se incluyen premios

y reconocimientos para el estudiante que tenga mayor puntaje. Por cada tema te tienen 3 o 4 ejercicios de aplicación, los cuales van aumentando la complejidad de resolución. Cada vez que el estudiante pierda un intento pierde vitalidad y puede perder la vida. Por cada 30 puntos gana una vida adicional, lo que hace que pueda seguir en la competencia.

Al final de cada temática, se realiza una retroalimentación y se proporciona un video con la practica de laboratorio para dicho tema.

3.3. Evaluación del diseño de la aplicación

Para la evaluacion se propone realizar la tecnica de Focus Group, la cual es una tecnica de investigación cualitativa que es usada para recolectar opiciones de expertos sobre un tema o aplicación especifica. En general se pretende abrir un espacio de dicusion para obtener una buena retroalimentacion (Tomat, 2012). Para la evaluación de este diseño se propuso que el focus group estuviera compuesto por 5 personas como se sugiere. En la siguiente tabla se presentan los perfiles seleccionados:

Experto	Perfil
Experto 1	Docente fisica y matematicas
Experto 2	Docente fisica y matematicas
Experto 3	Estudiante que ya ha cursado la asignatura
Experto 4	Estudiante que ya ha cursado la asignatura
Experto 5	Estudiante que no ha cursado la asignatura.

Como resultado de la evaluación se obtuvo lo siguiente

- Los puntajes asignados al exito de realización del ejercicio de aplicación debe ser proporcional a su complejidad, por ejemplo el primer ejercicio de aplicación de un tema especifico podra tener un puntaje 5 pero el siguiente debera tener un puntaje mayor y asi sucesivamente ir mejorando hasta alcanzar un buen nivel.
- Se debe proporcionar la posibilidad de conocer el posicionamiento del grupo, es decir que el usuario pueda ver como se encuentra respecto a los demas usuario en cuanto a puntaje.
- Es importante que cada usuario tenga la posibilidad de ver su progreso y realizar nuevos intentos para pasar los retos.
- Deben haber retos sorpresa, que funcionen de manera aleatoria y que den puntaje adicional al obtenido, ademas debe ser un puntaje con un valor mucho mas alto en comparación con los otros retos.
- Se sugiere que premie a cada participante con insigneas que permita distinguirlo de los demas participantes.
- Ademas de incluir los videos de los laboratorios, se sugiere en una nueva version incluir un simulador del laboratorio, lo que podria hacerla mas atractiva.

4. Conclusiones

Las aplicaciones gamificadas son una excelente alternativa para usarse en proceso de apoyo en educaciòn. Permite que actividades cotidianas realizadas al interior del aula de clase se puedan gamificar, incluyendo dinamicas y mecanicas que hagan interesante la

actividad presentada a los estudiantes y permiten dinamismo en el aula, impacto en el estudiante y aprendizaje significativo.

Una vez realizado la evaluación del diseño, se recibio la retroalimentaciòn, las cuales llevan a repensar la aplicación, teniendo en cuenta tecnologias como aplicaciones distribuidas y procesamiento en la nube, permitiendo asi el uso masivo de la misma.

La Gamificación en la actualidad es una herramienta interesante que propone revolucionar el proceso de enseñanza aprendizaje, sin embargo requiere en algunos casos estar acompañada de herramientas tecnologicas que apoyen este proceso, lo que puede hacer costoso la implementación de estos sistemas.

Referencias

Borrás Gené, O. (22 de 02 de 2022). *Gamificar una propuesta docente diseñando experiencias positivas de aprendizaje*. Obtenido de Universidad Politecnica de Madrid: https://oa.upm.es/35517/1/fundamentos%20de%20la%20gamificacion_v1_1.pdf

Cuba Rondón, E. (2021). Aplicación de la gamificación en el diseño de actividades en la Educación a Distancia. *RCCI*.

Quintanal Pérez, F. (Opcion). Aplicación de herramientas de gamificación en física y química de secundaria. *2016*, : 327-348.

Aguilera Castillo, A., Fúquene Lozano , C. A., & Ríos Pineda, W. F. (2014). Aprende jugando: el uso de técnicas de gamificación. *Im-pertienente*, 125-143.

Chipia Lobo, F. J. (2011). Juegos serios: alternativa innovadora. *II Congreso en linea en conocimiento libre y educacion CLED 2011* (pág. 18). on-line: e-ponencias.

Díaz Cruzado, J. (s.f.). El Potencial de la Gamificación aplicada al Ambito Educativo.

Lobo Rueda , M. A., Paba Medina, M. C., & Torres Barreto, M. (2020). Análisis descriptivo de experiencias gamificadas para enseñanza y aprendizaje en educación superior en ingeniería. *Revista Espazios*, 21-38.

Lozada-Ávila, C. (s.f.). La gamificación en la educación superior: una revisión sistemática. *Revista de Ingenierias Universidad de Medellin*.

Tipler, & Mosca. (2008). *Fisica para la Ciencia y la Tecnología*. Barcelona: Editorial Revertè.

Tomat, C. (2012). Focus group: Its application potential in the study of urban acoustic. *Atenea Digital*, 129-152.

Valda Sanchez, F., & Arteaga Rivero , C. (2015). Diseño e implementación de una estrategia de gamificacion en una plataforma virtual de educación. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, 65-80.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 14/10/2021
Aceitação/Acceptance: 13/01/2022

Pasos para diseñar un modelo de madurez con marco de trabajo ágil para la implementación a sistemas de gestión de la seguridad de TI alineado a las políticas de gobierno colombiano para el sector público

Katerine Márceles Villalba[1], Siler Amador Donado[2]

kmarceles@unimayor.edu.co; samador@unicauca.edu.co

[1] Facultad de Ingeniería, Institución Universitaria Colegio Mayor del Cauca, Carrera 7 N° 2-34 Edificio Bicentenario, 190003, Popayán- Cauca, Colombia.

[2] Facultad de Ingeniería Electrónica y Telecomunicaciones, Universidad del Cauca, Carrera 2 #4N-140, 190003, Popayán- Cauca, Colombia

Pages: 501-507

Resumen: En la actualidad las empresas del sector público a pesar de tener un modelo de seguridad y privacidad de la información en ocasiones tienen dificultad en el proceso de la implementación y el medir el estado de madurez del mismo, por ello a través de esta propuesta se entregan pautas y los pasos a seguir para llegar a diseñar un modelo de madurez basado en un marco de trabajo ágil, el cual les permitirá poder adaptarlo a sus necesidades y ritmo en cuanto a tiempo como recursos. Este proceso se propone bajo la metodología exploratoria articulado a fases que conllevarán a obtener lo planteado.

Palabras-clave: Ágil, Gobierno, Modelo, Políticas, Seguridad de la Información.

Steps to design a maturity model with an agile framework for the implementation of IT security management systems aligned to the policies of the Colombian government for the public sector

Abstract: Currently, companies in the public sector, despite having an information security and privacy model, sometimes have difficulty in the implementation process and in measuring its maturity, which is why, through this proposal, they deliver the guidelines and the steps to follow to design a maturity model based on an agile framework, which will allow them to adapt it to their needs and pace in terms of time and resources. This process is proposed under the exploratory methodology articulated in phases that will lead to obtaining what is proposed.

Keywords: Agile, Government, Model, Policies, Information Security.

1. Introducción

Actualmente las empresas del sector público tienen como exigencia la implementación de las políticas digitales en el marco de la seguridad informática, hasta el el punto de tener

manuales, lineamientos y un modelo de madurez del sistema de gestión de seguridad de la información emanados por el Ministerio de la tecnologías y comunicaciones – Mintic, Colombia. Sin embargo, se ha evidenciado que a la fecha las entidades del sector público han tenido ciertos inconvenientes en cuanto a la implementación y seguimiento a través de la guía del modelo de madurez diseñada para medir el grado de avance e implementación de ésta, por ser un documeto que a pesar de encontrarse de manera detalla su explicación resulta siendo compleja de enteneder para las organizaciones, por ello lo que se busca con esta propuesta es entregar las pautas necesarias para quienes los requieran puedan llegar a generar una guía que les permita a través de un marco ágil de trabajo llegar a una implementación del Sistema de gestión de seguridad de información de manera sencilla y rápida.

Lo anterior, conlleva a proponer y responder la siguiente pregunta: ¿Cómo impactaría la implementación de un marco de trabajo ágil sobre un modelo de madurez aplicado a un sistema de gestión de la seguridad de TI acorde a las políticas de gobierno establecidas para el sector público?, por lo que a través de este trabajo se proporcionarán las pautas a seguir que permitirán determinar cómo sería el impacto de dicho marco con el fin de disminuir los riesgos.

A continuación, se presenta el despliegue de este trabajo a través de diferentes secciones, siendo la segunda sesión los aspectos preliminares donde se presentan conceptos importantes que se relacionan en el trabajo, en la sección tres trabajos relacionados se presentan los referentes para la construcción de lo desarrollado y finalmente en la cuarta sección se encuentra la metodología donde se hace un despliegue de la misma.

2. Aspectos preliminares

Entre los conceptos que abarca el trabajo de investigación se encuentran:

- *Sistemas integrados de gestión de TI*: Entre algunos de ellos están, la norma ISO/IEC 20000 (ISO/IEC, ISO/IEC 20000:2010), el cual promueve la adopción de un enfoque de procesos integrados para una provisión adecuada de servicios gestionados satisfaciendo los requisitos del negocio y de los clientes por medio de una mejora continua a través del modelo PDCA (20000, 2018).

  La norma ISO/IEC 27001:2013, se caracteriza por promover un enfoque basado en procesos y especificar los requisitos para la creación, implantación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) dentro del contexto empresarial.

  Este estándar se caracteriza por su PDCA, el cual permite hacer uso de él para realizar una implementación adecuada, secuencial y cíclica dentro de un ámbito enmarcado en la seguridad (27001:2013, 2013).
- *Modelo de madurez*: Como modelos de madurez de procesos reconocidos, se encuentran el modelo CMM, el cual contempla un modelo propio con las áreas de proceso específicas de la gestión de servicios; así mismo se tiene como referente también la norma ISO/IEC 15504, que comprende aspectos relacionados con la gestión de servicios alineado con el estándar ISO/IEC 20000 (ISO/IEC, ISO/IEC 15504-10:2011).

- Gobierno en línea: El Gobierno en Línea es una estrategia definida mediante el Decreto 1151 de 2008, por el Gobierno Nacional, el cual busca generar una inclusión social y competitividad del país a través de la apropiación y el uso adecuado de las Tecnologías de la Información y las Comunicaciones (TIC), con el ánimo de mejorar la eficiencia y transparencia del Estado Colombiano por medio la construcción gradual de un gobierno electrónico, enmarcado en la seguridad de la información (Mintic, 2017).
- Marco de trabajo ágil: Un marco de trabajo ágil es aquel que se detaca por evaluar la dirección de un proyecto a medida que se desarrolla su ciclo de vida a través de iteraciones, dando la posibilidad a los equipos de trabajo de corregir a tiempo las variaciones al inicio de cada iteración, reduciendo de esta manera el impacto de cualquier error o falla cometido en las etapas previas (Abrahamsson, 2002) (Canos, 2010).
- Manual de Gobierno Digital: Abarca el desarrollo del proceso de implementación de la política digital a través de cuatro grandes momentos: 1. Conocer la política; 2. Planear la política; 3. Ejecutar la política; y 4. Medir la política, los cuales incorpora acciones que permitirán implementar la política en las entidades públicas de nivel nacional y territorial (Comunicaciones, Abril de 2019).
- Política de Gobierno Digital: Actual directriz del Ministerio Tecnologías de la Información y las Comunicaciones – MINTIC , que reemplazó Gobierno en Línea donde se definen los lineamientos, estándares y proyectos estratégicos que debe llevar a cabo el Estado Colombiano.

Debido a lo anterior, la metodología de marco de trabajo ágil aplicado a las TIC surge como acción de mejora para aplicarlo a procesos complejos que permitiendo de alguna u otra forma innovar a la velocidad requerida del mercado (Fuentes, 2017), por lo que se pretende que a través de ésta se logre adaptar un sistema de gestión de seguridad de la información de manera eficaz y con una simplicidad que pueda ser empleada por cualquier organización.

3. Trabajos Relacionados

A continuación se relacionan algunos trabajos de investigación que aportaron en la construcción de esta propuesta:

En el trabajo presentado por (Calafat, 2012), titulado “Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros”, tiene como propósito desarrollar un modelo integrado para facilitar la implantación de los estándares de gestión de TI mediante la combinación de las mejores prácticas facilitando la implantación de las normas relacionadas con ellas y de esta manera reducir esfuerzos. En este trabajo se destaca el proceso metodológico implementado para conseguir ese modelo alineado a estándares.

En cuanto al proyecto (González Díaz, 2016))“Guía de incidentes de seguridad de la información para la oficina de tecnología de la información y la comunicación – OTIC del Ministerio de Salud y protección social, tomando como base la ISO/IEC 27001:2013, propone definir una metodología de gestión de riesgos basada en diferentes normas y estándares para la creación de una guía de gestión de incidentes

de seguridad de la información, de esa forma permitir mejorar los tiempos de respuestas y la eficacia de la de la atención de incidentes alineados al estandar del SGSI. Se retoma de éste la importancia de la inclusión del estándar de riesgo dentro de los procesos de implementacion en el sistema de gestión de seguridad de la información.

Con relación al trabajo presentado por (Escorcia, 2017), titulado "Marco de gobierno, Gestión y arquitectura de TI para el diseño e Implementación de Sistemas de información en Entidades públicas Colombianas", tiene como finalidad construir una ruta y guía de implementación del marco propuesto, para mejorar la transparencia en cuanto al acceso e interoperabilidad pública de la información. En ésta se hace enfasis en la importancia que se le dá en cuanto a la implementación de una arquitectura que logré brindar seguridad a la información desde un punto de vista legal y gubernamental, los cuales son aportes importantes para la inclusión en esta propuesta de investigación que se esta estructurando.

En lo que respecta al trabajo realizado por (Ventura, 2018), titulado Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C – La Molina, propone la creación de un sistema web que permita gestionar tanto el sistema de gestión de seguridad de la información como también los activos, lo cual aportaría mucho este trabajo por lo que se estudiaría de qué forma a través de una aplicación se podría alinear el modelo de madurez para la implementación de de la política de seguridad digital en las entidades del sector público.

En virtud de lo anterior, cada una de las investigaciones presentadas aportaron significativamente tanto en la formulación, justificación y aspectos metodologicos para la construcción de esta propuesta.

4. Metodología

La metodología que se tiene propuesta para el desarrollo de este proyecto fue dividida en cuatro fases como se describe a continuación, es de aclarar que cada fase depende de la realización de la fase anterior, buscando así el cumplimiento de los objetivos propuestos el cual se proponen los siguientes:

- Establecer un estudio comparativo entre los estándares enfocados a sistemas de gestión basado en procesos y los lineamiento de la política digital para determinar el grado de convergencia entre ellos
- Analizar los diferentes modelos de madurez existentes para determinar el más adecuado en la integración de los sistemas de gestión de la seguridad de TI basados en procesos.
- Determinar el marco ágil de trabajo más adecuado que garantice una
- óptima adaptación de los sistemas de gestión de la seguridad integrados en el área de TI.
- Operacionalizar el modelo de madurez que permita la integración de sistemas de gestión basado en la política de gobierno digital.
- Verificar el modelo de madurez propuesto en una empresa del sector público.

Para lograr lo anterior se plantean las acciones a manera de fases:

✓ Fase 1: Búsqueda de información.

- Identificación de los estándares enfocados a procesos basados en sistemas de gestión, modelo de madurez y marco de trabajo ágiles.
- Especificación de las características de cada uno de los elementos antes mencionados.

✓ Fase 2: Criterios y selección

- Establecimiento del criterio o criterios convergentes en los sistemas de gestión y política digital.
- Establecimiento de criterios para la selección y ajustes al modelo de madurez adecuado.
- Establecimiento de criterios o criterio con relación al marco de trabajo ágil para la selección del más adecuado.

✓ Fase 3: Ejecución y control

- Construcción del modelo de madurez que permita la integración de sistemas de gestión basado en la política digital Colombiana.
- Verificación del modelo de madurez propuesto en una empresa del sector público.

✓ Fase 4: Resultados

- Análisis de los resultados obtenidos.

El esquema de fases propuestas anteriormente busca realizar una investigación exploratoria, la cual consiste en proporcionar una visión general sobre una realidad o un aspecto de ella, de una manera tentativa o aproximada tal y como menciona Miguel Rojas en su libro Metodología de la Investigación. Dicho esto, el trabajo a realizar busca una metodología que se pueda ajustar a las fases descritas para el cumplimiento del mismo. Dentro de la búsqueda de la metodología se opta por aplicar a la ejecución de las fases, G.Q.M (Goal Question Metric) , la cual consta de tres niveles y seis pasos descritos en el artículo The Goal Question Metric (van Solingen & Rombach, 2002). El primer nivel es el nivel conceptual (Goal o Meta) donde indica que se deben establecer metas para el proyecto, las cuales serán sometidas a una serie de preguntas. A esta etapa de preguntas se le conoce como el nivel operacional (Question o Pregunta). Este nivel operacional busca otorgar un valor cuantitativo o cualitativo por medio de las preguntas realizadas a las metas propuestas del proyecto, dando así el inicio al nivel cuantitativo (Metric o Métricas). El nivel cuantitativo toma como base los valores obtenidos del nivel operacional y los cuantifica otorgando resultados que nos informan si las metas propuestas para el proyecto han sido realizadas satisfactoriamente. El proyecto toma las cuatro fases inicialmente mencionadas y aplica la metodología GQM, cabe resaltar que el nivel conceptual son las metas del proyecto, lo cual se llegarán alcanzar a partir del cronograma que se establezca y dinámicas de la organización al momento de implementarse.

5. Conclusiones

En la actualidad se ha denotado un requerimiento en especial a las entidades públicas en lo concerniente a la implementación de la política de Gobierno Digital, el cual tiene como objetivo mejorar el funcionamiento de éstas mediante la implementación de recursos TIC, al incluir éste último mediante uno de sus ejes transversales buscan mantener la confidencialidad, disponibilidad e integridad de los activos de información de las entidades que cobija el estado y de esta manera salvaguardar la privacidad de los datos.

Por ello con este proceso que se propone se pretende que a través de un marco de trabajo ágil se logre implementar un sistema de gestión enmarcados en el área de la seguridad de de la tecnología y de la información, mediante un modelo de madurez con lineamientos establecidos en la política de gobierno digital enmarcado en el estándar ISO/IEC 27001:2017, de esta manera disminuir el riesgo a ser vulnerable y a su vez generar menos duplicidad de información en los procesos y procedimientos de las empresas del sector público, el determinar el grado de madurez de una empresa teniendo un enfoque del sistema de gestión integrado desarrollado con el modelo propuesto, reducir costos en cuanto a la implementación no solo en dinero sino también en tiempo, hasta llegar a la reutilización e integración de actividades en caso de que la organización ya se encuentre certificada por algún sistema de gestión.

Agradecimientos

Agradecimientos a la Universidad del Cauca en especial a su grupo de investigación GTI y al grupo de investigación I+D en Informática de la Facultad de Ingeniería de la Institución Universitaria Colegio Mayor del Cauca, por el apoyo brindado para el desarrollo del proyecto.

Referencias

Abrahamsson, P. Y. (2002). Agile software development methods Review and analysis. s.l. . VTT Publications.

Calafat, A. L. (2012). Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros. Palma.

Canós, J. H. (2010). Métodos ágiles en el desarrollo de software S.I. Universidad Politécnica de Valencia.

Comunicaciones, M. d. (Abril de 2019). Manual de Gobierno Digital - Decreto 1008 de 2018 . Bogotá: Mintic.

Escorcia, H. S. (2017). Marco de gobierno, Gestión y arquitectura de TI para el diseño e Implementación de Sistemas de información en Entidades públicas Colombianas . Universidad del Norte - Barranquilla.

Fuentes, S. (14 de 9 de 2017). DirectorTIC . Obtenido de La metodología agile: nuevas formas de trabajo para el desarrollo de proyectos: https://directortic.es/estrategia-it/la-metodologia-agile-nuevas-formas-trabajo-desarrollo-proyectos-2017091418485.htm

González Díaz, J.E. y Parrado. V. (2016). Guía De Gestión De Incidentes De Seguridad De La Información Para La Oficina De Tecnología De La Información Y La Comunicación – Otic Del Ministerio De Salud Y Protección Social, Tomando Como Base La Norma Iso 27001:2013. Universidad Piloto De Colombia , Facultad De Postgrados Especialización En Seguridad Informática. Bogotá: Universidad Piloto De Colombia .

ISO/IEC, I. O. (s.f.). ISO/IEC 15504-10:2011. Information technology – Process assessment – Part 10: Safety extension.

ISO/IEC, I. O. (s.f.). ISO/IEC 20000:2010. Information technology – Service Management.

Mintic, M. d. (2017). Mintic. Obtenido de Gobierno en Línea: https://www.mintic.gov.co/portal/604/w3-article-5306.html)

Ventura, J. M. (2018). Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C – La Molina . Lima-perú: Universidad César Vallejo.

Van Solingen, B. C., & Rombach. (2002). Goal question metric (gqm) approach.

20000, I. (2018). BSI. Obtenido de Gestión de Servicios de TI ISO/IEC 20000: https://www.bsigroup.com/es-ES/ISOIEC-20000-Gestion-de-Servicios-de-TI/

27001:2013, I. (2013). International Organization for Standardization. Obtenido de https://www.iso.org/isoiec-27001-information-security.html

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 11/12/2021
Aceitação/Acceptance: 03/02/2022

Saber Pro en programas de formación militar y policial: minería de datos para la identificación de factores asociados a los resultados

Gladys Irene Arboleda-Posada[1], David Alberto García-Arango[2], Aura María Vasco-Ospina[3], Santiago Restrepo Garizabal[4], Jairo Andrés Sastoque-Zapata[5]

giarboleda@americana.edu.co; dagarcia@coruniamericana.edu.co; amvasco@americana.edu.co; srestrepo@americana.edu.co; jsastoque@coruniamericana.edu.co

[1,2,3,4,5] Corporación Universitaria Americana, 00504, Medellín, Colombia.

Pages: 508-516

Resumen: Las pruebas censales han sido consideradas como un componente de medición del nivel de calidad de los programas formativos. En el presente artículo, se identifican factores o conjuntos de variables asociadas a los niveles de desempeño en pruebas de fin de carrera para programas de formación relacionada con el campo militar o policial. Las pruebas en mención reciben el nombre de Saber Pro y evalúan niveles de competencias genéricas y competencias profesionales, la comprensión de variables que intervienen en los niveles de desempeños evaluados, dan una medida adicional acerca de la consolidación de perfiles de egreso. La metodología fue de enfoque mixto y aplicó algoritmos de análisis factorial con rotación varimax a 654 registros de resultados de las pruebas realizadas entre 2012 y 2019. Los resultados permiten identificar aspectos en materia de gestión curricular para el incremento en el desempeño en los resultados y en general para el desarrollo de estrategias orientadas hacia el mejoramiento continuo.

Palabras-clave: Saber Pro; formación militar; formación policial; niveles de desempeño; minería de datos

Saber Pro in military and police training programs: data mining for the identification of factors associated with the results

Abstract: Census tests have been considered as a component for measuring the level of quality of training programs. In this article, factors or sets of variables associated with performance levels in end-of-career tests for training programs related to the military or police field are identified. The tests studied are called Saber Pro and evaluate levels of generic and professional skills, the understanding of variables that intervene in the levels of performance evaluated, give an additional measure about the consolidation of graduation profiles. The methodology was of a mixed approach and applied factorial analysis algorithms with varimax rotation to 654 records of results of the tests carried out between 2012 and 2019. The

results allow the identification of aspects in terms of curricular management for the increase in performance in the results and in for the development of strategies oriented towards continuous improvement.

Keywords: Saber Pro; military training; police training; performance levels; data mining

1. Introducción

El desarrollo de políticas educativas es un proceso en continua construcción y que es demarcado por las estrategias de desarrollo sostenible del país. En este sentido, la formación de la fuerza pública no es la excepción. En Colombia, la consideración de políticas en materia educativa para programas formativos asociados a la fuerza pública han sufrido variaciones en razón de los cambios sociales, culturales y económicos por los que ha atravesado el país pasando desde la creación de la Escuela Militar de Cadetes "General José María Córdova" en 1888 (Presidencia de la República de Colombia, 1888) y las subsecuentes generaciones de establecimientos educativos que han sido creados desde los diferentes decretos hasta los respectivos planes de acción estratégica integrados desarrollados en el gobierno actual.

En todo ese trayecto se identifican como documentos rectores los propuestos a través del Proyecto Educativo de las Fuerzas Armadas (PEFA) (Ministerio de Defensa Nacional, 2008), el Sistema Educativo de las Fuerzas Armadas (SEFA) (Ministerio de Defensa Nacional, 2010) y el Plan Estratégico del Sistema Educativo de las Fuerzas Armadas (PESE) (Ministerio de Defensa Nacional, 2008), estos documentos cuya vigencia se tuvo hasta 2019, establecieron lineamientos el marco estratégico para la fomulación de la "Política de Educación para la Fuerza Pública (PEFuP) 2021-2026: hacia una educación diferencial y de calidad" (Ministerio de Defensa Nacional, 2021). Este último marco normativo establece políticas orientadoras que direccionarán el sistema educativo de la fuerza pública colombiana atendiendo a los compromisos establecidos con los Objetivos de Desarrollo Sostenible en tanto no solo aporta a una educación de calidad desde el cuarto objetivo en tanto "la educación es uno de los motores más poderosos y probados para garantizar el desarrollo sostenible" (Naciones Unidas - CEPAL, 2016), sino que aporta al desarrollo de la paz, justicia e instituciones sólidas en tanto se aboga por "la promoción de la paz, acceso universal a la justicia, y reducir el maltrato, la trata de personas, la corrupción, y todas las formas de violencia" (Naciones Unidas - CEPAL, 2016) en tanto, la educación como acción transformadora provee los espacios de conceptualización adecuados para la construcción colectiva de valores característicos del deber ser materializados en la consideración efectiva del respecto de los derechos humanos, la equidad, la pertinencia y el enfoque humanista en la toma de decisiones.

Teniendo en cuenta la pertinencia de la consolidación de la integralidad de la formación de la fuerza pública en Colombia y atendiendo a los diferentes retos que implica este compromiso en el contexto colombiano, el presente escrito se centra en el análisis de resultados de las pruebas Saber Pro para programas de formación policial y militar con el objetivo de identificar factores relacionados con los resultados en éstas. Los resultados permiten considerar estrategias de mejoramiento de los programas formativos en materia de gestión curricular.

2. Metodología

El desarrollo metodológico de la investigación fue de enfoque mixto en cuanto consideró el tratamiento de variables cuantitativas y categorías cualitativas que analizadas en conjunto contribuyen a una comprensión más integral del objeto de estudio (Monje Álvarez, 2011). El razonamiento utilizado es inductivo en tanto se generan relaciones entre las entradas y salidas de un modelo de análisis factorial como base para el desarrollo de modelos de minería de datos (Díez Arias, 2016).

Respecto a los pasos para el desarrollo del análisis se procedió en primer lugar con la consecución e integración de datos de las bases del Instituto Colombiano para el Fomento de la Educación Superior (ICFES) utilizando los resultados de las pruebas Saber Pro entre los años 2012 y 2019, y las respectivas pruebas asociadas Saber 11 utilizando la base de datos denominada "Llave_Saber11_2006-1_2019-2_SaberPRO_2012-1_2019-2.txt" donde se identificaron resultados de módulos de competencias genéricas para las pruebas Saber Pro, junto con otras variables y categorías de análisis, tal y como se presenta en la Tabla 1.

Descripción	Variable/Categoría
Género	ESTU_GENERO
Departamento de residencia	DEPTO_RESIDENCIA_SBPRO
Estado civil	ESTU_ESTADOCIVIL
Etnia del estudiante	ESTU_ETNIA
Área de residencia del estudiante	ESTU_AREARESIDE
Educación del padre	FAMI_EDUCACIONPADRE
Cantidad de personas en el hogar	FAMI_PERSONASHOGAR
Acceso a internet	FAMI_TIENEINTERNET
Horas semanales que trabaja el estudiante	ESTU_HORASSEMANATRABAJA
Departamento donde se oferta el programa formativo	ESTU_PRGM_DEPARTAMENTO
Metodología del programa formativo	ESTU_METODO_PRGM
Núcleo de conocimiento del pregrado	ESTU_NUCLEO_PREGRADO
Municipio de la Institución	ESTU_INST_MUNICIPIO
Departamento de la Institución	ESTU_INST_DEPARTAMENTO
Carácter académico de la institución	INST_CARACTER_ACADEMICO
Departamento de presentación de la prueba	ESTU_DEPTO_PRESENTACION
Puntaje global estandarizado de la prueba Saber 11	PUNTAJE_GLOBAL_ESTANDARIZADO_ICFES
Puntaje razonamiento cuantitativo	MOD_RAZONA_CUANTITAT_PUNT
Puntaje lectura crítica	MOD_LECTURA_CRITICA_PUNT
Puntaje competencias ciudadanas	MOD_COMPETEN_CIUDADA_PUNT
Puntaje de inglés	MOD_INGLÉS_PUNT
Puntaje comunicación escrita	MOD_COMUNI_ESCRITA_PUNT
Nivel de desempeño	NIVEL_DESEMPENO

Tabla 1 – Variables y categorías de análisis. Elaboración propia.

Es así como las variables y categorías anteriormente descritas, se relacionan entre sí con la finalidad de identificar pesos en los factores predictores de los resultados globales de la prueba. Para tal efecto se generó un procedimiento estructurado de minería de datos utilizando el software SPSS Modeler (IBM Corporation, 2013) (Figura 1) en el cual se ejecutan diferentes nodos de minería de datos basados en el algoritmo de Redes Neuronales de perceptrón multicapa.

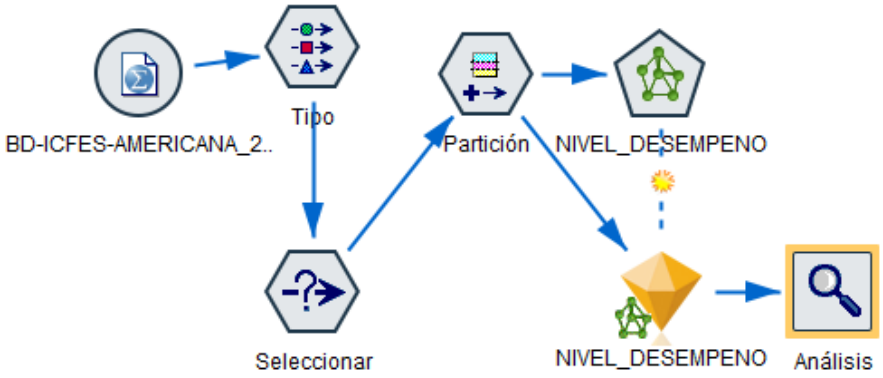


Figura 1 – Procedimiento de ejecución del modelo de minería de datos. Elaboración propia.

En la Figura 1 se puede observar un primer nodo de base de datos que luego está conectado con un nodo de selección de tipo de variables, allí se identifican las entradas y salidas del modelo (nodo "Tipo"), posteriormente se seleccionan los programas cuyo núcleo de formación se relaciona con el campo militar o policial en el nodo "Seleccionar" con la ecuación: ESTU_NUCLEO_PREGRADO /= 'FORMACIÓN RELACIONADA CON EL CAMPO MILITAR O POLICIAL', logrando de esta forma la selección de 654 programas en este campo, de los cuales mediante el nodo "Partición" se elige el 70% (455) como muestra de entrenamiento, 20% (125) como muestra de comprobación y 10% (74) como muestra de validación.



Figura 2 – Relaciones entre variables

Con la selección de los datos se procedió a aplicar un nodo de perceptrón multicapa con semilla 229176228 donde primero se generaron como entradas los resultados de los

módulos de la prueba Saber Pro y como salida los resultados Globales para de esa manera identificar el módulo que más capacidad de predicción o explicación de resultados da, como se explica en la Figura 2.

Seguidamente, se aplica la misma estructura, pero considerando categorías cualitativas de las presentadas en la Tabla 1 y que toman como variable de salida el nivel de desempeño.

Finalmente se analizan los resultados obtenidos identificando los niveles de predicción de cada variable o categoría de estudio.

3. Resultados

Los resultados de la investigación se componen de dos partes principales: resultados cuantitativos conformados por la identificación de puntajes de módulos con mayor peso en el cálculo de los resultados de las pruebas Saber Pro (módulos de la prueba que aportan más a la predicción del resultado de la prueba) y los resultados cualitativos, donde se relacionan entre sí diferentes categorías de análisis socioeconómico en la dirección de puntuaciones de los resultados de las pruebas Saber 11.

3.1. Resultados cuantitativos

La consideración de los resultados cuantitativos, arroja cálculos en términos de variables determinantes de los resultados, en ese sentido, se encontrará cuál fue el módulo que a la luz del modelo de redes neuronales incidió de forma más significativa en los resultados. El modelo aplicado a los módulos de competencias genéricas de las pruebas Saber Pro, arroja los resultados de la Figura 3.

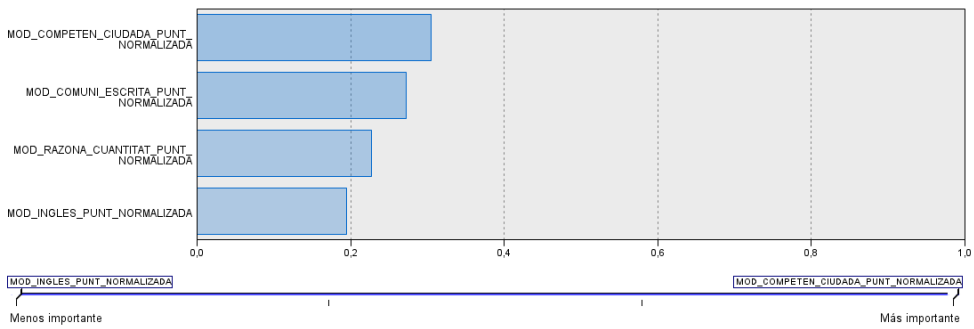


Figura 3 – Importancia del predictor para el nivel de desempeño en las pruebas saber Pro en el estudio cuantitativo. Elaboración propia.

El modelo de redes neuronales se logra consolidar en este caso con una precisión de 92,5% donde en un 94,5% de los casos predice el nivel 1 (el estudiante obtiene de 0 a 150 puntos) y en un 93,1% de los casos predice el nivel 2 (el estudiante está por encima de la media, es decir, por encima de 150 puntos).

Se identifica entonces como predictor más importante el módulo de competencias ciudadanas con un peso de 0,31; seguidamente se tiene el módulo de competencia escrita con un peso de 0,27; posteriormente el módulo de razonamiento cuantitativo con un peso de 0,23 y por último el módulo de inglés con un peso de 0,19. La matriz de clasificación de valores previstos por observados se puede observar en la Figura 4.

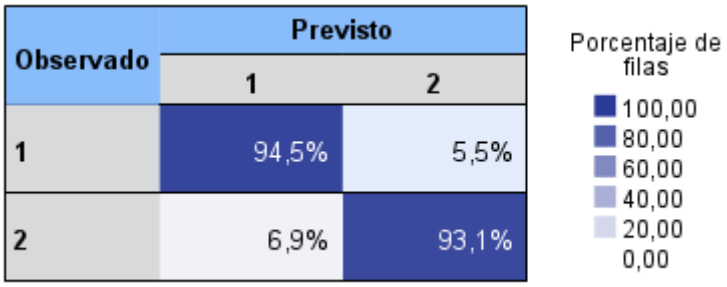


Figura 4 – Porcentaje de relación entre resultados observados y resultados previstos para el estudio cuantitativo.

Se puede identificar en la matriz un alto porcentaje de resultados que predice el modelo y que efectivamente son resultados clasificados en los niveles 1 y 2 respectivamente (diagonal principal de la tabla, en azul oscuro), se presenta entonces un error del modelo de 6,9% para prediciones del nivel 1 que realmente son del nivel 2 y de 5,5% para predicciones del nivel 2 que realmente son del nivel 1.

3.2. Resultados cualitativos

Respecto a los resultados cualitativos, se consideró el mismo modelo pero teniendo en cuenta las siguientes categorías: género, departamento de residencia, estado civil, etnia del estudiante, área de residencia del estudiante, educación del padre, cantidad de personas en el hogar. acceso a internet, horas semanales que trabaja el estudiante, departamento donde se oferta el programa formativo, metodología del programa formativo, núcleo de conocimiento del pregrado, municipio de la Institución, departamento de la Institución, carácter académico de la institución, departamento de presentación de la prueba y puntaje global estandarizado de la prueba Saber 11 (única variable de tipo cuantitativo continuo).

Para este caso, no se utilizaron variables directamente asociadas a los resultados sino que se exploró mediante un cribado de variables el conjunto de categorías que podrían explicar mejor el resultado en la prueba Saber Pro. En ese sentido, es previsible que el porcentaje de relación entre resultados previstos y resultados observados sea menor que el obtenido en los resultados cuantitativos, sin embargo, se presenta como un aspecto aportante el hecho de lograr clasificaciones de las categorías por nivel de importancia predictiva. Es así como el modelo, aplicado a las categorías anteriormente mencionadas reporta el resultado que se presenta en la Figura 5.

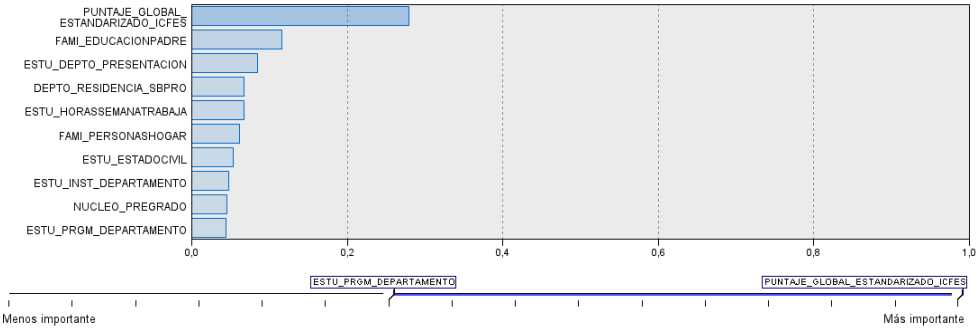


Figura 5 – Importancia del predictor para los niveles de desempeño en el estudio cualitativo. Elaboración propia

De las categorías relacionadas se identifica como principal predictor el puntaje global estandarizado ICFES con un peso de 0,28. El puntaje corresponde a un valor estandarizado de los resultados del estudiante en una prueba previa al examen saber Pro y que se realiza en grado 11, antes de ingresar a la educación universitaria. Se siguen en orden de la educación del padre (0,12), el departamento en el cual presentó la prueba el estudiante (0,08), departamento de residencia (0,07), horas a la semana que labora el estudiante (0,07), cantidad de personas que conviven en el hogar (0,06), estado civil del estudiante (0,05), departamento donde vive el estudiante (0,05), núcleo de formación del programa (0,05) y departamento donde se oferta el programa.

Como es de esperarse, el modelo obtiene un nivel de precisión del 72,7%, el cual aún sigue presentando resultados interesantes en términos de clasificación de las categorías de análisis. La matriz de clasificación de valores previstos por observados se presenta en la Figura 6.

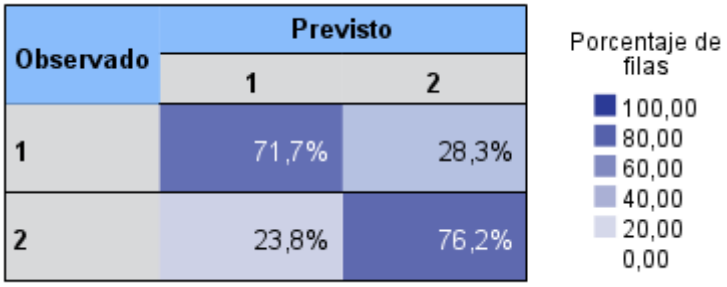


Figura 6 – Porcentaje de relación entre resultados observados y resultados previstos para el estudio cualiativo.

Se puede identificar en la matriz un moderado porcentaje de resultados que predice el modelo y que efectivamente son resultados clasificados en los niveles 1 y 2 respectivamente (diagonal principal de la tabla, en azul oscuro), se presenta entonces un error del modelo

de 23,8% para prediciones del nivel 1 que realmente son del nivel 2 y de 28,3% para predicciones del nivel 2 que realmente son del nivel 1.

4. Conclusiones

El desarrollo de la investigación arroja que un determinante importante en los resultados de las pruebas Saber Pro para programas de formación policial y militar fue el resultado en el módulo de competencia ciudadana, al ser éste un módulo que a consideración del modelo determinó una diferenciación clara de clasificación de los resultados en los dos niveles especificados, se hace menester que los programas formativos incentiven el estudio en competencias ciudadanas, considerándolas desde el análisis del contexto y su importancia en la toma de decisiones clave en el ejercicio profesional, de lo anterior, se deben considerar estrategias que consideren como eje central las competencias ciudadanas de tal forma que éstas tengan mayor relevancia en el proceso formativo. Para tal fin, se propone la implementación de estudios de caso en los cuales se identifiquen las rutas de acción más apropiadas en el contexto de aplicación y en consideración con las regulaciones existentes.

Llama la atención que desde el análisis cualitativo, el nivel educativo del padre tenga un valor predictivo más alto que otras variables solo superado por el resultado en las pruebas Saber 11, en ese sentido es importante dar cuenta que un mayor nivel de formación del padre podría incidir en un mayor conocimiento de competencias ciudadanas desde el hogar, lo cual es coherente con estudios como los propuestos por Camacho González & Contreras Badel (2020) donde se indica que al hacer un rastreo de documentación de 2016 a 2020, el rol del padre en el marco de la educación, aporta significativamente a una formación íntegra.

En materia de gestión curricular, el desarrollo de este tipo de análisis permite la identificación de escenarios para diferentes variables que inciden en el proceso formativo. Es así como por ejemplo, la inclusión a nivel microcurricular de proyectos transversales que consideren la responsabilidad en materia de competencias ciudadanas, permitirían en el marco de los hallazgos de esta investigación, un mejoramiento de los resultados en las pruebas Saber, atendiendo a los principios de formación integral y mejoramiento continuo de los programas formativos.

Referencias

Camacho González, D. L., & Contreras Badel, H. S. (2020). *Estado del conocimiento: familia y formación ciudadana*. Bogotá: Politécnico Grancolombiano.

Díez Arias, F. (2016). *Aplicación de la minería de procesos al análisis y modelado de misiones multi-robot*. Madrid: Universidad Politécnica de Madrid.

IBM Corporation. (10 de Julio de 2013). *IBM SPSS Modeler 16: Algothms Guide & Applications Guide*. Obtenido de https://www.ibm.com/support/pages/node/612163#en

Ministerio de Defensa Nacional. (2008). *Plan Estratégico del Sistema Educativo de las Fuerzas Armadas 2007-2019*. Bogotá D.C. Obtenido de https://goo.gl/PcFkeJ

Ministerio de Defensa Nacional. (2008). *Proyecto Educativo de las Fuerzas Armadas - PEFA*. Bogotá D.C.

Ministerio de Defensa Nacional. (2010). *Lineamientos Curriculares Fuerzas Militares. Sistema Educativo de las Fuerzas Armadas*. Bogotá D.C.

Ministerio de Defensa Nacional. (2021). *Política de Educación para la Fuerza Pública*. Bogotá D.C.: Ministerio de Defensa Nacional.

Monje Álvarez, C. A. (2011). *Metodología de la investigación cuantitativa y cualitativa*. Neiva: Universidad Surcolombiana.

Naciones Unidas - CEPAL. (2016). *Agenda 2030 y los Objetivos de Desarrollo Sostenible. Una oportunidad para América Latina y el Caribe*. Santiago de Chile: Naciones Unidas.

Presidencia de la República de Colombia. (1888). *Decreto 1003 de 1888*. Obtenido de https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1205554

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 08/10/2021
Aceitação/Acceptance: 26/01/2022

Modelo de Datos - Contexto Universitario: premisa para agilidad, disponibilidad y toma de decisiones apoyado en información

Javier Condor[1], Nelson Salgado[2], Henry N. Roa[3], Juan Francisco Chafla[4]

jwcondor@puce.edu.ec; nesalgado@puce.edu.ec; hnroa@puce.edu.ec; jchafla390@puce.edu.ec

[1,2,3,4] Pontificia Universidad Católica del Ecuador, Quito, Pichincha, Ecuador.

Pages: 517-527

Resumen: Considerando el marco legal vigente, las instituciones de educación superior, con la intención de automatizar los procesos, integrar y normalizar la información, han implementado sistemas que acceden a distintas fuentes de datos, lo que en ocasiones deriva en multiplicidad de bases de datos que son difíciles de sincronizar y operar. Desde la perspectiva del diseño de software, se puede construir un modelo de datos para el contexto universitario que cumpla con lo establecido en el marco legal. Para esto se necesita datos almacenados de manera integrada con la menor redundancia posible. En este contexto, se propone un modelo de datos flexible que sostiene los módulos de un sistema de información integrado en donde interactúan los diferentes procesos de gestión, y el cual permite generar información para ayudar a la toma de decisiones y mejorar el accionar de la organización.

Palabras-clave: BDD (base de datos); MER (Modelo Entidad Relación); modelamiento de datos.

Data Model - University Context: premise for agility, availability and Decision-Making supported by information

Abstract: Considering the current legal framework, higher education institutions, with the intention of automating processes, integrating, and standardizing information, have implemented systems that access different data sources, which sometimes results in a multiplicity of databases that are difficult to sync and operate. From the perspective of software design, a data model can be built for the university context that complies with the provisions of the legal framework. This requires data stored in an integrated manner with as little redundancy as possible. In this context, a flexible data model is proposed that supports the modules of an integrated information system where the different management processes interact, and which allows the generation of information to help decision-making and improve the actions of the organization.

Keywords: BDD (database); ERM (Entity Relationship Model); data modeling.

1. Introducción

El modelamiento de los datos es una técnica que fue perfeccionándose desde los años 70, para responder a las necesidades de información, especialmente en ese entonces de los contextos productivos, bancarios y de investigación de las fuerzas armadas (Coronel, 2011).

Cuando la computación y los equipos se transforman a personales, permite que muchos profesionales tengan acceso a distintos tipos de aplicaciones denominados motores de bases de datos con un paradigma de libre uso; así como, el denominado venta bajo licencia; manteniéndose, el modelamiento de los datos como un cimiento fundamental para un sistema de información.

En la actualidad el modelamiento de entidades, la selección adecuada del tipo de dato para cada característica de la entidad y la forma de conectarse los objetos de las entidades entre ellos, permite que todo lo relacionado con datos (ingreso, almacenamiento, procesamiento, actualización) (Silberschatz, 2006) sea de manera flexible y acorde a los cambios constantes de los contextos diarios; uno de ellos, el contexto universitario.

Para el modelamiento de cubos de información; es decir aquella que se consigue con información histórica, se desarrollaron algunas técnicas basadas en el modelo entidad relación; una de las más utilizadas es el modelo estrella (Silberschatz, 2006).

Considerando el marco legal vigente en el Ecuador y las posibles actualizaciones de este, las instituciones de educación superior, con la intención de automatizar los procesos, integrar y normalizar la información han implementado sistemas desarrollados por ellas mismas o por terceros que acceden a distintas fuentes de datos, lo que en ocasiones deriva en multiplicidad de sistemas y bases de datos que a medida que la información se vuelve extensa, son difíciles de sincronizar y operar satisfactoriamente.

Con este marco regulatorio existe la demanda de un modelo de datos que contemple los ejes establecidos; es decir: la docencia, la investigación y la vinculación con la sociedad, como se presenta en la Fig.1 (Coronel, 2011).



Figura 1 – Ejes universitarios

Los ejes universitarios no son aislados; de esta manera, docencia interactúa con investigación y con vinculación, investigación interactúa con vinculación y docencia;

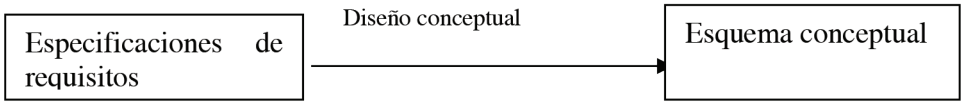
así como también lo hace vinculación. Existe una interacción de los tres ejes cuando la investigación es aplicada a una comunidad o a la sociedad por parte de los docentes; como se presenta en la Fig 1.

Desde el punto de vista del diseño de software y la programación por capas, en la capa de datos, se puede partir con la premisa de la propuesta de la construcción de un modelo de datos para el contexto universitario que pueda cumplir con lo anterior. Para lo que se necesita: Los datos correspondientes, almacenados de manera integrada, con la menor redundancia, aplicando técnicas de modelamiento, con la aceptación de grupos focales de actores universitarios, para responder de manera inmediata a las necesidades de información de los distintos roles universitarios, con los respectivos niveles de autorización.

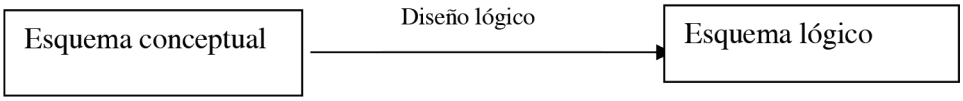
De esta manera el modelo de datos propuesto plantea sostener los distintos módulos de un sistema de información integrado, para el accionar de la universidad, en donde interactúan: los procesos de gestión de infraestructura física, gestión de empleados, el registro contable, los procesos financieros; en conjunto con: los procesos de docencia, estructura académica, movilidad de estudiantes, proyectos de investigación multidisciplinarios, e interactuando con la sociedad en sus diferentes áreas.

2. Metodología

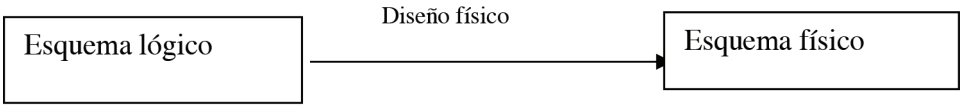
La metodología utilizada para el modelo de datos; parte de las especificaciones de requisitos,



- Esquema conceptual: Descripción de alto nivel del contenido de información de la base de datos, independiente del SGBD que se utilizará.
- Modelo conceptual: Lenguaje que se utiliza para describir esquemas conceptuales
- Propósito Obtener un esquema completo que lo exprese todo.



- Esquema lógico Descripción de la estructura de la base de datos según el modelo del SGBD que se utilizará.
- Modelo lógico Lenguaje que se utiliza para describir esquemas lógicos; hay varios modelos lógicos: de red, relacional, orientado a objetos.
- Propósito Obtener una representación que use de la manera más eficiente los recursos disponibles en el modelo lógico para estructurar datos y modelar restricciones.



- Esquema físico Descripción de la implantación de una BD en la memoria secundaria: estructuras de almacenamiento y métodos usados para tener un acceso efectivo a los datos. El diseño físico se adapta al SGBD específico que se va a utilizar.

Para la especificación de los requisitos se parte de la revisión de leyes, reglamentos y normas definidas por el estado ecuatoriano, de esta manera se consiguen crear el modelo entidad relación, las entidades maestras, sus relaciones existentes y los atributos de datos que conforman las tablas del modelo.

Se continua con la identificación de roles, para especificar las autorizaciones respectivas permisos de acceso para las distintas tablas del modelo que tendrá la data transaccional validada por procesos que serán utilizadas por los usuarios a través de cubos de información.

2.1. Revisión del marco legal regulatorio universitario

En nuestro país el marco legal regulatorio del contexto universitario, está supeditado a la Constitución del estado (Estado Ecuatoriano, 2008), llevando esto a un marco legal de la educación superior a través de la LOES, que bajo la supervisión de los organismos tales como CES, CEAACES y SENECYT definen, regulan y controlan su ejecución.

Los organismos anteriores han impuesto un marco regulatorio en concordancia con el plan nacional del buen vivir (Semplades, 2017) y el modelo de desarrollo del país, generando reglamentos específicos tales como el Reglamento de escalafón docente investigador (CES, 2012); el Reglamento Régimen académico (CES, 2014), el Reglamento de armonización de títulos, entre otros.

Este marco legal regulatorio ha tenido varios cambios y ajustes en estos años; que al parecer seguirán ajustándose por la realidad del país y la participación de los representantes universitarios.

2.2. Identificación de roles universitarios

El contexto universitario, tenía hasta antes del marco legal mencionado como eje principal la docencia por lo que los roles identificados plenamente se mantienen, así: docente, coordinador de área, director de carrera, subdecano, decano, director general académico, vicerrector y rector, en conjunto con los comités internos; tales como: Consejo de Escuela, consejo de facultad, Consejo académico. De igual manera los estudiantes tienen su representación en las asociaciones de escuela y la federación de estudiantes universitarios.

El marco regulatorio ha incluido la investigación y la vinculación con la sociedad como otros ejes de suma importancia en el contexto universitario, por lo que los roles de auxiliar, investigador y director de proyecto de investigación se visualizan de manera importante,

así también su coordinación a través del director de investigación. En lo relacionado con vinculación surgen roles como el de tutor estudiantil, docente consultor, docente tutor de prácticas pre profesionales, docente tutor de responsabilidad universitaria, de mismo modo coordinado por un docente por carrera para prácticas y responsabilidad social y un director de estos aspectos a nivel de universidad.

El contexto universitario es gestionado por procesos de carácter administrativo y financiero; por lo que, los roles administrativos y financieros se mantienen vigentes. Estos roles facilitan la asignación y aprobación de permisos concedidos sobre los comandos SQL DML (Data Manipulation Language) (S=select, I=insert, D=delete, U=update, G=grant, RV=revoke).

Áreas	Roles
Directivos	Rector
	Prorector
	Vicerrector
	Director general
	Director
Academia	Decano
	Subdecano
	Director de carrera
	Director de laboratorio
	Coordinador de área
	Docente
	Tutor
	Estudiante
	Graduado

Tabla 1 – Roles por área

Como se presenta en la Tabla 1, cada eje o área tiene roles establecidos como en el área de directivos lo son: Rector, Pro-rector, Vicerrector, Director General y Director.

2.3. Identificación de procesos universitarios

En base al numeral 2.1, los procesos de docencia se ven adicionados con: prácticas pre profesionales, segunda lengua y el proceso de titulación que hoy se lo ve plasmado en el transcurso de la carrera.

Los procesos que van madurándose son los relacionados con gestión de los proyectos de investigación, los mismos que deben alinearse al plan de buen vivir (Semplades, 2017), y a la matriz productiva [10] en base a los objetivos estratégicos del estado, sin por ello descuidar los temas multidisciplinarios, convenios internacionales y contexto mundial.

En lo relacionado con vinculación se van especificando procesos para las practicas pre profesionales la iteración con las empresas que suscriben cartas de intención, servicios a

terceros de docentes profesionales y responsabilidad social universitaria conjuntamente con la iteración con la comunidad, los ejecutores de los proyectos de responsabilidad universitaria y su retroalimentación e incidencia (CES, 2014).

La gestión administrativa del contexto universitario se mantiene vigente es así como los procesos de compras, adquisiciones, inventarios, gestión de la planta física, aulas, laboratorios y otros espacios de la universidad se mantienen. Los procesos de gestión de activos fijos toman importancia por la diversidad de artículos, productos, materiales e insumos que se requiere en el contexto.

El componente financiero se mantiene con los procesos relacionados con contabilidad, presupuestos y seguimiento de proyectos en cuanto al registro del recurso financiero que ingresa y que es necesario para el adecuado funcionamiento de la organización.

2.4. Identificación de entidades con sus características e iteraciones entre ellas

La entidad docente, debe ser replanteada de acuerdo a las nuevas necesidades de información y especializarse en otras entidades para cumplir con los datos de tutores de estudiantes, tutores de prácticas pre profesionales, tutores de responsabilidad universitaria. Así también como los respectivos coordinadores por carrera en cada uno de los aspectos mencionados.

La entidad estudiante, debe ser replanteada de acuerdo a las nuevas necesidades de información y especializarse en otras entidades para cumplir con los datos de tutorados, estudiantes en prácticas pre profesionales, estudiantes de responsabilidad universitaria; como lo presenta la Fig.2.



Figura 2 – Entidad estudiante

La Fig.2, presenta características de estudiantes como campos definidos en tipo de datos especializados como lo son los dominios: tipo de identificación, tipo de sexo y estado del registro. Se plantea que el código del estudiante sea un valor numérico auto incremental, mientras que la identificación sea un valor único en toda la tabla.

La entidad empleada, debe ser replanteada de acuerdo a las nuevas necesidades de información y generar herencia en docentes y administrativos

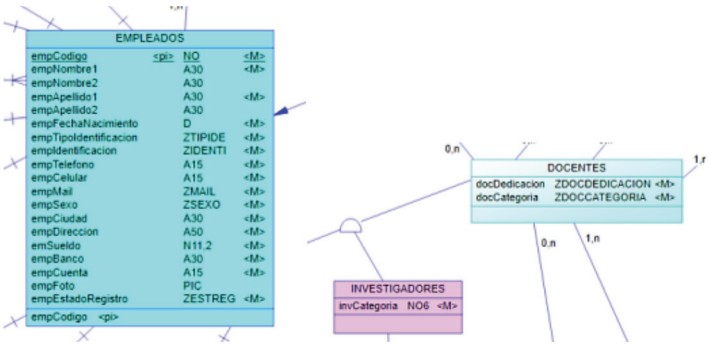


Figura 3 – Entidad empleado herencia a docente e investigador

La iteración entre los docentes con los estudiantes es de muchos docentes interactúan con muchos estudiantes, de esta manera se facilita el registro y seguimiento de docencia, aprobación, participación en prácticas o en responsabilidad universitaria asociado con las empresas y las comunidades.

La Fig.3, presenta características de empleados como campos definidos en tipo de datos especializados como lo son los dominios: tipo de identificación, tipo de sexo, correo electrónico y estado del registro para borrado lógico de información del empleado. Se plantea que el código del empleado sea un valor numérico auto incremental, mientras que la identificación sea un valor único en toda la tabla.

Los docentes e investigadores heredaran todos los campos de los empleados, adicionándose campos como el tiempo de dedicación, la categoría docente o categoría de investigador.

Las entidades compras, proveedores, productos, artículos, bienes, servicios, clientes mantienen su vigencia, pudiendo optimizarse los datos que permitan su rápida ubicación y estatus de los mismos. Entidades como cuentas, registros contables, usuarios responsables, y detalle de la transacción contable deben mantener coherencia con las buenas prácticas en sus respectivas áreas.

La Tabla 2, presenta las transacciones básicas presentes en cada módulo del área académica; así, por ejemplo: matricula, que es un proceso que debe mantener consistencia con los requisitos que debe tener un estudiante, los límites para la toma de cátedras, límite para el número de horas de clases, cruces de horarios, entre otras. Otras transacciones presentadas son distribución semestral de docentes, estructura de

malla curricular, estructura académica, préstamos de libros, asignaciones de tutores o capítulos de una disertación.

Áreas	Módulo	Transacción
Academia	Estudiantes	Matricula
	Docentes	Distribución semestral
	Carreras	Malla curricular
	Estructura académica	Áreas académicas
	Bibliotecas	Préstamo de libro
	Tutorías	Asignación tutor
	Titulación	Capítulos de disertación

Tabla 2 – Transacciones académicas

3. Propuesta de modelo universitario

El modelo de datos propuesto utilizando el motor de base de datos postgreSQL [16, 17], se presenta en la Fig.4 de manera global:.

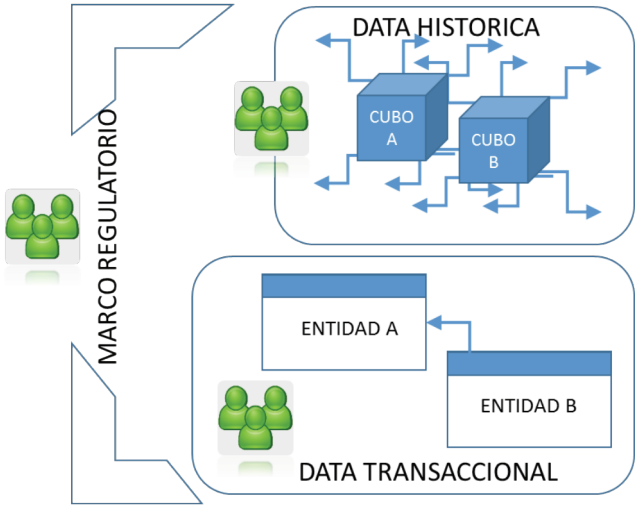


Figura 4 – Esquema global de modelo de datos universitario

De la revisión del marco regulatorio; y de los usuarios expertos en su accionar, se presenta el modelo separando la data transaccional o diaria de la data histórica o hecho consumado.

El modelo de datos transaccional es el resultado del análisis del entorno universitario, determinándose las distintas entidades; sus características y las relaciones que existen

entre ellas. Lo anterior diseñado bajos los conceptos del modelo entidad relación (Silberschatz, 2006)

Para la información histórica, se recomienda utilizar el modelo de estrella para los distintos cubos de información, la misma que permitirá generar los indicadores que los entes reguladores necesitan, así como dar seguimiento de optimización de los recursos universitarios, por parte de las autoridades (Ramez, 2010).

3.1. Aceptación por parte del grupo focal

Consideramos de suma importancia la aceptación por parte del usuario con roles universitarios del modelo propuesto, debido a que los mismos son y serán quienes utilizarán el sistema de información generado sobre este modelo de datos.

Para lo anterior es necesario identificar dos o más usuarios, con los roles identificados en el estudio, que tengan experiencia en sus funciones asignadas para de esta manera ser el grupo focal, quienes validaran el modelo, la funcionalidad del sistema de información y las necesidades de información para toma de decisiones y presentación de indicadores a los entes reguladores

3.2. Resultados y Discusión

El uso de dominios, permite consolidar la validación de campos similares; como, por ejemplo: "Dólar"; de tipo numérico de nueve enteros y dos decimales, utilizado para todos los campos que registran valores monetarios en dólares. Otros dominios planteados son: "correo electrónico", "tipo de identificación", "forma de pago" etc.

El modelo de datos transaccional planteado de manera consolidada, reúne todas las entidades del mundo universitario y las que puedan seguirse generando. Esta integración permite disminuir la redundancia de datos, obtener las consultas a una sola base de datos y disminuir la extracción y procesamiento de datos cuando se tienen bases separadas. Con esta propuesta se puede conseguir separar la data transaccional del día a día de la data histórica, es decir cuando se cierra un ciclo académico.

La centralización de los datos y el proceso de traslado a bases de datos históricas da a las instituciones de educación superior la capacidad de toma de decisiones con la aplicación de Bussines Intelligence o Data Analítica.

La especificación de roles o grupos de usuarios, permite definir los permisos de acceso, visualización y uso de la data; tanto de la data diaria como de la data histórica. Esto aplica también a los roles de tipo técnico.

Para futuras discusiones se plantea las siguientes interrogantes que pueden ser despejadas con los grupos focales en conjunto con los especialistas de IT (Information Technology):

a. ¿El modelo de datos cumple las leyes, reglamentos y normativas del contexto universitario?
b. ¿Están definidos los procesos del nuevo contexto universitario?

c. ¿Se han seleccionado adecuadamente usuarios representativos de cada rol universitario?
d. ¿Están identificadas todas las entidades sus características y la iteración entre ellas?

Una vez aprobado el modelo de datos es necesario definir una estrategia acorde a la realidad universitaria para adquirir, desarrollar o contratar el sistema de información que viabilice lo detectado, socializado y acordado.

El paradigma de desarrollo de aplicación in situ vs el paradigma on cloud será un tema de discusión y selección de mejor alternativa, considerando la realidad universitaria, su capacidad financiera y operativa.

4. Conclusiones y recomendaciones

El modelado de datos con la metodología entidad-relación cumple con el objetivo de ser el pilar fundamental para el soporte de un sistema de información integrado, que permita responder de manera ágil las necesidades de información, así como los constantes cambios del marco regulatorio, por lo tanto, de los procesos del contexto y de los roles y funciones designadas.

La selección de un motor de base de datos es un tema de suma importancia tomando en cuenta la cantidad de usuario (control de accesos y autorizaciones), protección de la información identificada como sensible, confiabilidad en la transaccionalidad de los datos, disponibilidad de información 24/7 que es el actual paradigma de disponibilidad.

Debe definirse de manera técnica la periodicidad de información que se considerará mantener en línea, sugiriéndose el concepto semestral académico, así como el periodo semestral administrativo. De igual manera debe considerarse la periodicidad de un estudiante con ese rol que idealmente sería de 4, 5 o 6 años hasta su titulación.

Un estándar de interface es el web browser, el mismo que permitirá la accesibilidad desde cualquier parte del mundo que se disponga de acceso a internet. Facilitará la iteración con la base de datos y flexibilizará la iteración con usuarios.

El concepto de alta disponibilidad se sugiere considerarlo por tratarse de una organización con miles de usuarios de los roles principales, así como por la cantidad de información solicitada en cualquier momento tanto por usuarios internos como externos.

Para finalizar considerar a las Tecnologías de Información y Comunicación, como servicios a los cuales se debe aclarar y afinar los niveles de calidad requeridos en función al costo beneficio entregado a la organización.

Referencias

Ramez E, 2010. Fundamentos de Bases de Datos (5ª). México: Pearson Educación.

Silberschatz, 2006. A. Fundamentos de Bases de Datos (5ª). Madrid: McGraw-Hill.

Coronel, 2011. M. Bases de datos e Implementación (9na.) México: CENCAGE.

Estado Ecuatoriano, 2008. Constitución Política del Ecuador 2008, Quito.

Estado Ecuatoriano, 2015. Enmiendas a la Constitución de la República del Ecuador 2015, Quito.

Estado Ecuatoriano, 2010. LOES Ley Orgánica de Educación Superior aprobada el 4 de agosto del 2010, Quito.

Estado Ecuatoriano, 2011. Reglamento a la Ley Orgánica de Educación Superior aprobada el 1 de septiembre del 2011, Quito.

Senplades, 2013. Plan Nacional para el Buen Vivir 2013-2017, Quito.

Senplades, 2017. Plan Nacional de Desarrollo 2017-2021.Toda una Vida, Quito.

Senplades, 2012. Transformación de la matriz productiva, Quito.

CES, 2012. Reglamento de Escalafón y Carrera del Docente e Investigador, Quito.

CES, 2014. Reglamento Régimen Académico Codificado, Quito.

CES, 2015. Reglamento de armonización de la nomenclatura de títulos profesionales y grados académicos que confieren las IES, Quito.

Ceaaces, 2018. Modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas, Quito.

Senacyt, 2016. Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, Quito.

DB-Engines (30 de 12 de 2021). https://db-engines.com/en/ranking

Comparison of relational database management systems (30 de 12 de 2021). https://en.wikipedia.org/wiki/Comparison_of_relational_database_management_systems

Cóndor J, 2018. Modelo de Datos contexto Universitario. Ecuador, Caso de Estudio, Pontificia Universidad Católica del Ecuador PUCE.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 26/12/2021
Aceitação/Acceptance: 25/02/2022

Competencias para el Emprendimiento en el Contexto Covid-19

Sussy Bayona-Oré[1]

sbayonao@hotmail.com

[1] Vicerrectorado de Investigación, Universidad Autónoma del Perú, Villa el Salvador Km. 16.3, Lima-Perú

Pages: 528-536

Resumen: El emprendimiento es un proceso creativo que contribuye a la generación de empleo y una pieza clave para la prosperidad económica y acelerador de la innovación. Es un proceso que empieza con la intención de emprender y donde uno de los componentes básicos son las competencias del emprendedor. El emprendedor es la persona que tiene los conocimientos y las competencias para generar y ejecutar una idea de negocio exitoso, en especial en épocas de crisis. En este artículo se presenta una revisión de la literatura sobre las competencias del emprendedor en el contexto Covid-19. Los resultados muestran que las competencias para el emprendimiento se vieron fortalecidas tales como la adaptación al cambio, resiliencia, innovación and autoeficacia.

Palabras-clave: emprendimiento; resiliencia; innovación; competencias, Covid-19.

Competences for Entrepreneurship in the Covid-19 Context

Abstract: Entrepreneurship is a creative process that contributes to the generation of employment and a key element for economic prosperity and an accelerator of innovation. It is a process that begins with the intention of undertaking and where one of the basic components is the skills of the entrepreneur. The entrepreneur is the person who has the knowledge and skills to generate and execute a successful business idea, especially in times of crisis. This article presents the literature review on entrepreneurial skills in the Covid-19 context. The results show that the competencies for entrepreneurship were strengthened, such as adaptation to change, resilience, innovation, and self-efficacy.

Keywords: Entrepreneurship; resilience; innovation; competences; Covid-19.

1. Introducción

El emprendimiento es un término que cobra importancia frente a la necesidad de superar problemas económicos y sociales. El emprendimiento es clave para la prosperidad económica y contribuye a la generación de empleo (Soluk et al., 2021), el desarrollo

económico (Kotsopoulos et al., 2022) así como un factor para el desarrollo sostenible (Galindo-Martín et al., 2021).

Al ser el emprendimiento un impulsor de nuevos empleos, contribuye a la generación de empleo, lo que ha dado lugar a iniciativas que se enfoquen en su creación y fortalecimiento (Chen, 2021). Por ello, es importante que se fomente el emprendimiento en especial en épocas de crisis. El emprendimiento como competencia es un factor de éxito en el mundo globalizado y para mejorar el contexto socioeconómico (Piedra & Caro, 2019).

Con la propagación del Covid-19 las organizaciones en general se vieron impactos por las medidas para manejar la crisis sanitaria como el distanciamiento social. Este nuevo escenario ha generado que la acción de emprender cobre mayor importancia, considerando que frente a la pérdida de un empleo (necesidad) o la oportunidad, surgieron nuevos emprendimientos (Haeffele et al., 2020).

Para emprender es importante tener una idea clara, que puede surgir por una necesidad insatisfecha, como resultado de un estudio o la observación del mundo real. La idea para emprender un negocio debe aportar valor a los grupos de interés. En este proceso, un punto de partida para emprender es que el emprendedor se sienta motivado, además de tener las capacidades, conocimientos y habilidades necesarias.

A la persona que identifica una oportunidad y decide iniciar un negocio se le denomina emprendedor (Devece et al., 2016). Para un emprendimiento exitoso, se requiere que el emprendedor tenga competencias tales como resiliencia, innovación, autoeficacia, control percibido del comportamiento, motivación, adaptación al cambio y asumir riesgos entre otros.

En el emprendimiento, la autoeficacia permite que la persona se sienta segura para iniciar un negocio. La seguridad de la persona, basado en sus conocimientos, experiencia para emprender y la resiliencia han sido mencionados como los constructos claves que determinan el éxito de un emprendimiento (Acevedo-Duque et al., 2021). La resiliencia y la autoeficacia como características del emprendedor son cruciales en determinar cómo los emprendedores se recuperan de la incertidumbre (Prah & Sibiri, 2021)(Prah & Sibiri, 2021; Sumaryani, 2018). La capacidad de generar ideas y la creatividad son otras características esenciales en el emprendimiento.

El propósito de este artículo es conocer las características de los emprendedores mediante la revisión de artículos relacionados con el emprendimiento y las competencias.

Este artículo ha sido estructurado en 5 secciones que incluye esta Introducción. En la sección 2 se presenta conceptos de emprendimiento, emprendedor y emprender. En la sección 3 se presenta la metodología. En la sección 4 se presenta las competencias identificadas en la revisión de literatura. Finalmente, en la sección 5 se presenta las conclusiones.

2. Marco Teórico

El emprendimiento proviene del término emprendedor (pionero). Está relacionado con la capacidad que tienen las personas de hacer un esfuerzo para alcanzar su meta. Un componente central para el emprendimiento es la creatividad, un factor de la

personalidad del emprendedor que es un componente central de la alerta emprendedora (Urban, 2020). Dependiendo del estado en que se encuentre el emprendimiento se pueden clasificar a los emprendedores en naciente y activo. Naciente son los que están en el proceso de crear su empresa y (2) activo a los que ya tiene una empresa.

Emprender consiste en tener una idea clara para realizar los pasos necesarios para iniciar un negocio que genere valor. La idea de emprender puede surgir al observar las necesidades que existen en el entorno, ser independiente, incrementar ingresos, continuar la tradición familiar o como resultado de estudios o análisis.

El emprendedor es "la persona que organiza y opera una o varias empresas, asumiendo cierto riesgo financiero en el emprendimiento" (Cánovas, Konate y Rubio, 2014). El emprendedor puede ser definido como la persona que identifica la oportunidad, tiene la idea de negocio y organiza los recursos para ponerlo en marcha, asumiendo nuevos retos. Es el "individuo que explora una oportunidad de negocio por medio de alguna forma de innovación" (Leite Gustmann de Castro et al., 2021, p. 51).

La definición de emprendedor varía según los enfoques. En el enfoque económico se interesa en logros alcanzados y su impacto en el sistema económico, a los sociólogos les interesa el comportamiento que tiene lugar en la sociedad y los psicólogos se interesan en las características personales.

3. Metodología

El propósito de este trabajo es determinar las competencias necesarias de los emprendedores en el escenario Covid-19. Los términos *Competences* or *Skills* or *Habilities* y *Entrepreneurship* fueron utilizados para identificar los artículos publicados en la base de datos SCOPUS. Los artículos fueron publicados en el periodo 2019-2022 y deben tratar las competencias para el emprendimiento. No se incluyen artículos cortos.

Los datos relevantes fueron extraídos en una hoja de cálculo. Los datos generales de artículo, las competencias, definiciones y el impacto en el escenario COVID-19 fueron recolectados.

4. Resultados

Con el propósito de conocer el interés de los investigadores en el tema de competencias para el emprendimiento, se utilizó la cadena de búsqueda formada por las palabras claves y los conectores lógicos AND y OR. Los resultados muestran el crecimiento sostenido a partir del año 2015 y en especial en el periodo 2019-2021. En la Figura 1 se presenta el crecimiento anual de publicaciones.

4.1. Sobre el Emprendimiento

De la revisión de literatura, se concluye que no existe consenso en la definición exacta de emprendimiento, es ampliamente utilizado en la literatura académica y a pesar de que existen muchos estudios enfocados en el emprendimiento (Afawubo & Noglo, 2022) la definición depende del enfoque de los autores. Las definiciones van desde considerar al emprendimiento como competencia y parte de la vida (Piedra & Caro, 2019) o como un

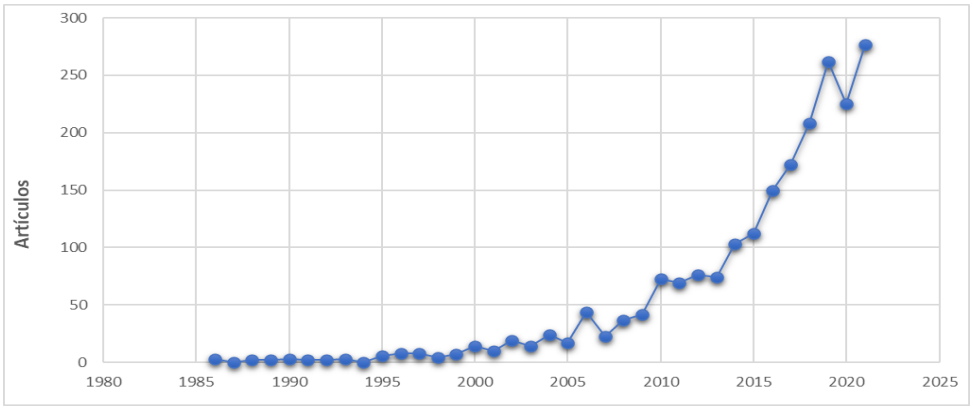


Figura 1 – Crecimiento anual de las publicaciones 1986-2021

estilo de vida fundamental en la sociedad (McMullen & Bergman, 2017) que requiere de una planificación adecuada de los recursos para hacerla sostenible (Sarma, 2020).

El emprendimiento como competencia es la capacidad de generar ideas para crear valor para otros. Este valor creado puede ser social, cultural o financiero (Piedra & Caro, 2019). Desde el punto de vista de Schepers et al. (2021) el emprendimiento tiene como finalidad generar un bienestar económico.

El emprendimiento es importante en todos los sectores. En el caso de las instituciones públicas el emprendimiento es clave para el desarrollo e implementación de políticas, considerando que, en un escenario de cambios, la demanda de los servicios públicos cambia (Demircioglu & Chowdhury, 2021). En el contexto de la Covid-19 muchos trámites que ofrecían las instituciones públicas, que requerían la presencia física del ciudadano, tuvieron que ser rediseñados para ser ofrecidos en línea.

4.2. Competencias para el emprendimiento

De la revisión de literatura se identificaron un conjunto de competencias para el emprendimiento. Las competencias emprendedoras involucran la capacidad de crear una nueva organización, desde su invento o solución, que trae al mercado como una oportunidad comercial. A continuación, se presenta las competencias para el emprendimiento tales como resiliencia, innovación, autoeficacia, motivación, adaptación del cambio y asumir riesgos.

4.2.1. Resiliencia

La resiliencia es la habilidad de poder surgir y atravesar todas las adversidades que se le presenten al emprendedor. Es uno de los constructos claves para determinar el emprendimiento exitoso (Schepers et al., 2021) y está relacionada con la perseverancia de una persona el cual le permite superar las adversidades que se le presente. Una persona resiliente supera las dificultades mediante un proceso para buscar una vida significativa (Lin & Wen, 2021). Esta competencia está relacionada con la capacidad de adaptación de las personas y de su actitud frente a nuevas situaciones que obstaculicen

alcanzar una meta (Prah & Sibiri, 2021). La resiliencia es una competencia muy importante (Kotsopoulos et al., 2022) especialmente en las épocas de adversidades como es la pandemia debido al Covid-19. Además, la resiliencia no solo está relacionada con factores internos y personales como la proactividad, sino por factores externos (Prah & Sibiri, 2021).

4.2.2. Innovación

La innovación es un componente central de la alerta emprendedora (Urban (2020) y tiene impacto en la intención de emprender (Khadri et al., 2020). La competencia de innovar es importante para generar y poder ofrecer productos y servicios innovadores. A través de la innovación el emprendedor será capaz de diferenciar rápidamente su emprendimiento del resto del mercado, con el beneficio de atraer una mayor cantidad de clientes. El emprendedor será capaz de aplicar nuevas ideas para desarrollar procesos, productos y servicios orientadas a incrementar la productividad y competitividad (Valenzuela-Keller et al., 2021). La Covid-19 impone grandes desafíos y exige innovación y capacidad de innovar (Kostopoulos et al., 2018) para adaptar los modelos de negocios que les permita sobrevivir a la crisis (Leite Gustmann de Castro et al., 2021).

4.2.3. Autoeficacia

La competencia autoeficacia es muy importante para el crecimiento del emprendedor y un factor muy importante en la adversidad (Kotsopoulos et al., 2022). Se caracteriza como la convicción en las propias competencias para llevar a cabo una actividad (Alshebami et al., 2020). Así mismo, la autoeficacia de los emprendedores esta asociado positivamente con el crecimiento del negocio (Kotsopoulos et al., 2022).

4.2.4. Control percibido sobre el comportamiento

El control percibido sobre el comportamiento está muy relacionado a la autoeficacia y se refiere a la facilidad o dificultad percibida para emprender tomando en cuenta las experiencias pasadas y anticipándose a las dificultades y obstáculos que puedan surgir. Se refiere al control del individuo sobre las acciones que son necesarias para realizar comportamientos (Gieure et al., 2019). El control percibido es la percepción personal del control que tiene sobre ciertos comportamientos (Sadat & Lin, 2020) y es muy importante para predecir la intención emprendedora (Khadri et al., 2020).

4.2.5. Competencia motivación

Es un aspecto fundamental en el emprendimiento que impulsa a la persona a realizar un determinado acto por la recompensa o beneficio interno y personal asociado con este acto (Al-Habaibeh et al., 2021). Así mismo, la motivación es importante para que las personas puedan ser más innovadoras y emprendedores (Demircioglu & Chowdhury, 2021). La motivación es un componente de la inspiración emprendedora definida como el cambio de emociones y la mente (Wang et al., 2021) y un factor esencial de orientación emprendedora (Iqbal et al., 2021) en especial la motivación intrínseca.

4.2.6. Adaptación al cambio

En tiempos de crisis y en un entorno de cambios permanentes la competencia de ser flexible y adaptarse rápidamente a los cambios es una competencia muy valorada. Adaptarse a los cambios o nuevas circunstancias, permite a los emprendedores nuevas oportunidades de aprendizaje. La adaptación es la principal competencia que un emprendedor debe tener cuando desea desarrollar el emprendimiento durante cualquier época de crisis, debido a la necesidad de realizar cambios.

Es decir se precisa que los emprendedores sean flexibles y agiles para responder a las necesidades del mercado y las demandas sociales (Leite Gustmann de Castro et al., 2021). La adaptación a los cambios ayuda a los emprendedores surgir en épocas difíciles, en su crecimiento empresarial (Kotsopoulos et al., 2022). La adaptación que impone el contexto actual en relación a las capacidades dinámicas obliga al uso de medidas momentáneas para atender la demanda (Leite Gustmann de Castro et al., 2021).

4.2.7. Disposición a asumir riesgos

Las características personales tienen influencia sobre la intención de emprender y asumir riesgos, es una característica importante para el emprendimiento (Khadri et al., 2020). Al ser el riesgo un factor relacionado con la creación de un negocio, un emprendedor debe estar dispuesto a asumirlo. La sobrecarga de trabajo desequilibrada y las presiones para desempeñarse con tiempo podrían afectar la salud (Gerards et al., 2021).

5. Conclusión

El emprendimiento permite generar empleo y es base del desarrollo económico y social. Para un emprendimiento exitoso es importante que el emprendedor, la persona que inicia un negocio, tenga las competencias que le permita ser un emprendedor exitoso, es decir que sea sostenible en el tiempo, en especial en épocas de crisis. En este artículo se ha revisado las competencias en el emprendimiento a partir de la revisión de la literatura. Las competencias en un escenario Covid-19 implican tener una fuerza psicológica para afrontar las adversidades y situaciones inesperadas, es decir los emprendedores deben tener la competencia resiliencia. Además, los emprendedores deben tener la capacidad para adaptarse rápidamente a los cambios. Las competencias autoeficacia y control percibido del comportamiento son importantes porque son predictores de la intención emprendedora. La motivación es una competencia importante del emprendedor en especial la motivación intrínseca. En el contexto de la pandemia debido a la Covid-19 el emprendedor ha tenido que asumir riesgos y ser resiliente para superar la crisis y sobreponerse a la adversidad.

Referencias

Acevedo-Duque, Á., Gonzalez-Diaz, R., Cachicatari Vargas, E., Paz-Marcano, A., Muller-Pérez, S., Salazar-Sepúlveda, G., Caruso, G., & D'Adamo, I. (2021). Resilience, leadership and female entrepreneurship within the context of smes: Evidence from latin america. *Sustainability (Switzerland)*, *13*(15). https://doi.org/10.3390/su13158129

Afawubo, K., & Noglo, Y. (2022). ICT and entrepreneurship: A comparative analysis of developing, emerging and developed countries. *Technological Forecasting and Social Change*, *175*(xxxx), 121312. https://doi.org/10.1016/j.techfore.2021.121312

Al-Habaibeh, A., Watkins, M., Waried, K., & Javareshk, M. B. (2021). Challenges and opportunities of remotely working from home during Covid-19 pandemic. *Global Transitions*, *3*, 99–108. https://doi.org/10.1016/j.glt.2021.11.001

Alshebami, A. S., Al-Jubari, I., Alyoussef, I. Y., & Raza, M. (2020). Entrepreneurial education as a predicator of community college of Abqaiq students' entrepreneurial intention. *Management Science Letters*, *10*(15), 3605–3612. https://doi.org/10.5267/j.msl.2020.6.033

Chen, X. (2021). Immigrant-owned small businesses' participation in diaspora philanthropy: a case study during the COVID-19 outbreak. *New England Journal of Entrepreneurship*, *24*(2), 105–121. https://doi.org/10.1108/NEJE-08-2020-0033

Demircioglu, M. A., & Chowdhury, F. (2021). Entrepreneurship in public organizations: the role of leadership behavior. *Small Business Economics*, *57*(3), 1107–1123. https://doi.org/10.1007/s11187-020-00328-w

Devece, C., Peris-Ortiz, M., & Rueda-Armengot, C. (2016). Entrepreneurship during economic crisis: Success factors and paths to failure. *Journal of Business Research*, *69*(11), 5366–5370. https://doi.org/10.1016/j.jbusres.2016.04.139

Galindo-Martín, M. Á., Castaño-Martínez, M. S., & Méndez-Picazo, M. T. (2021). Effects of the pandemic crisis on entrepreneurship and sustainable development. *Journal of Business Research*, *137*(August), 345–353. https://doi.org/10.1016/j.jbusres.2021.08.053

Gerards, R., van Wetten, S., & van Sambeek, C. (2021). New ways of working and intrapreneurial behaviour: the mediating role of transformational leadership and social interaction. In *Review of Managerial Science* (Vol. 15, Issue 7). Springer Berlin Heidelberg. https://doi.org/10.1007/s11846-020-00412-1

Haeffele, S., Hobson, A., & Storr, V. H. (2020). Coming Back from Covid-19: Lessons in Entrepreneurship from Disaster Recovery Research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3592966

Iqbal, S., Martins, J. M., Mata, M. N., Naz, S., Akhtar, S., & Abreu, A. (2021). Linking entrepreneurial orientation with innovation performance in smes; the role of organizational commitment and transformational leadership using smart pls-sem. *Sustainability (Switzerland)*, *13*(8), 1–18. https://doi.org/10.3390/su13084361

Khadri, N. A. M., Wei, E. K., Bakar, A. S. A., Sidek, S., Hasbolah, H., & Muhammad, N. M. N. (2020). Effects of entrepreneurial family background on students' entrepreneurial intention: A study at Universiti Malaysia Kelantan, Jeli Campus and Universiti Utara Malaysia, Sintok Campus. *International Journal of Criminology and Sociology*, *9*(December 2020), 2303–2310. https://doi.org/10.6000/1929-4409.2020.09.275

Kostopoulos, G., Kotsiantis, S., Ragos, O., & Grapsa, T. N. (2018). Early dropout prediction in distance higher education using active learning. *2017 8th International Conference on Information, Intelligence, Systems and Applications, IISA 2017*, *2018-Janua*, 1–6. https://doi.org/10.1109/IISA.2017.8316424

Kotsopoulos, D., Karagianaki, A., & Baloutsos, S. (2022). The effect of human capital, innovation capacity, and Covid-19 crisis on Knowledge-Intensive Enterprises' growth within a VC-driven innovation ecosystem. *Journal of Business Research*, *139*(October 2020), 1177–1191. https://doi.org/10.1016/j.jbusres.2021.10.055

Leite Gustmann de Castro, B., Eccel Pontelli, G., De Fátima Paz Nunes, A., Marques Kneipp, J., & Medianeira Flores Costa, V. (2021). Empreendedorismo e coronavírus: impactos, estratégias e oportunidades frente à crise global. *Estudios Gerenciales*, *37*(158), 49–60. https://doi.org/10.18046/j.estger.2021.158.4304

Lin, Q., & Wen, J. J. (2021). Family business, resilience, and ethnic tourism in yunnan, china. *Sustainability (Switzerland)*, *13*(21), 1–9. https://doi.org/10.3390/su132111799

McMullen, J. S., & Bergman, B. J. (2017). Social Entrepreneurship and the Development Paradox of Prosocial Motivation: A Cautionary Tale. *Strategic Entrepreneurship Journal*, *11*(3), 243–270. https://doi.org/10.1002/sej.1263

Piedra, N., & Caro, E. T. (2019). EntreCompOnto: An Ontology for Semantic Representation of Entrepreneurship Competences. *Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018*, *December*, 1113–1118. https://doi.org/10.1109/TALE.2018.8615415

Prah, D., & Sibiri, H. (2021). The resilience of African migrant entrepreneurs in China under COVID-19. *Journal of Entrepreneurship in Emerging Economies*, *13*(5), 1119–1133. https://doi.org/10.1108/JEEE-05-2020-0111

Sarma, S. K. (2020). Investigating Failed Social Entrepreneurship: A 'Process Research' Perspective. *Springer Proceedings in Business and Economics*, 79–93. https://doi.org/10.1007/978-981-13-9769-1_5

Schepers, J., Vandekerkhof, P., & Dillen, Y. (2021). The impact of the covid-19 crisis on growth-oriented smes: Building entrepreneurial resilience. *Sustainability (Switzerland)*, *13*(16), 1–20. https://doi.org/10.3390/su13169296

Soluk, J., Kammerlander, N., & Darwin, S. (2021). Digital entrepreneurship in developing countries: The role of institutional voids. *Technological Forecasting and Social Change*, *170*, 120876. https://doi.org/10.1016/j.techfore.2021.120876

Sumaryani, S. (2018). *Model development of production management unit to enhance entrepreneurship attitude of vocational school students from fashion department* (S. Nurmasitah, A. Kusumastuti, D. Hartanto, & H. Prasetiawan (eds.); Vol. 1941). American Institute of Physics Inc. https://doi.org/10.1063/1.5028113

Valenzuela-Keller, A. A., Gálvez-Gamboa, F. A., Silva-Aravena, E., & Moreno-Villagra, M. (2021). Actitudes emprendedoras de estudiantes universitarios de primer año en Chile. *Formación Universitaria*, *14*(4), 103–112. https://doi.org/10.4067/s0718-50062021000400103

Wang, C., Mundorf, N., & Salzarulo-McGuigan, A. (2021). Entrepreneurship education enhances entrepreneurial creativity: The mediating role of entrepreneurial inspiration. *International Journal of Management Education*, *xxxx*, 100570. https://doi.org/10.1016/j.ijme.2021.100570

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 04/10/2021
Aceitação/Acceptance: 24/01/2022

Benefícios e Riscos do Uso da Computação em Nuvem no Setor Público: uma análise baseada em artigos disponibilizados em bases dados acadêmicas de 2017 a 2021

Davidson Juarêz David[1], Carlos André de Melo Alves[1], Rafael Rabelo Nunes[1,2,3], Roque Magno de Oliveira[1]

davidsondavi@gmail.com; carlosandre@unb.br; rafaelrabelo@unb.br; roque@unb.br

[1] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Administração, CEP 70910-900 Brasília-DF Brasil

[2] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP 70910-900 Brasília-DF Brasil

[3] Centro Universitário Atenas, Rua Euridamas Avelino de Barros, nº 1400, Prado, CEP 38602-002 Paracatu-MG Brasil

Pages: 537-549

Resumo: O objetivo deste artigo foi analisar os benefícios e os riscos do uso da computação em nuvem no setor público, baseado em artigos disponibilizados em bases de dados acadêmicas, no período de 2017 a 2021. Trata-se de pesquisa descritiva com abordagens qualitativa e quantitativa, considerando amostra não probabilística de oitenta artigos. O tratamento dos dados empregou análise de conteúdo, considerando *checklist* contendo 12 subcategorias agrupadas em 2 categorias baseadas no referencial teórico. Após exame de 960 subcategorias, constatou-se no total 24,17% dessas subcategorias presentes. As subcategorias associadas aos benefícios e aos riscos da computação em nuvem apresentaram, respectivamente, 27,29% de presença e 21,04% de presença. As subcategorias 'Redução de Custos' e 'Vulnerabilidades quanto à Segurança' estiveram presentes em 56,25% da amostra de artigos. Este estudo trata tema atual e pode trazer reflexões sobre a adoção da computação em nuvem no setor público.

Palavras-chave: Computação em Nuvem; Benefícios e Riscos da Computação em Nuvem; Setor Público; Análise de Conteúdo.

Benefits and Risks of Cloud Computing use in the Public Sector: An analysis based on articles available in academic databases from 2017 to 2021

Abstract: The purpose of this article was to analyze the benefits and risks of using cloud computing in the public sector, based on articles made available in academic databases, from 2017 to 2021. This is descriptive research with qualitative and

quantitative approaches, considering a non-probabilistic sample of eighty articles. Data treatment used content analysis, considering a checklist containing 12 subcategories grouped into 2 categories based on the theoretical framework. After examining 960 subcategories, a total of 24.17% of these subcategories were present. The subcategories associated with the benefits and risks of cloud computing presented, respectively, 27.29% presence and 21.04% presence. The subcategories 'Cost Reduction' and 'Vulnerabilities regarding Security' were present in 56.25% of the sample of articles. This study deals with a current topic and can bring reflections on the adoption of cloud computing in the public sector.

Keywords: Cloud computing; Risks and Benefits of Cloud Computing; Public sector; Content Analysis.

1. Introdução

As inovações na área da Tecnologia da Informação - TI têm contribuído para que dados e informações sejam processados e armazenados com agilidade. Nesse contexto, é adequado estudar as alternativas encontradas pelas organizações para viabilizar o processamento e o armazenamento desses dados e informações. Entre essas alternativas está presente a computação em nuvem (Araújo & Alves, 2019).

Segundo o National Institute of Standards and Technology - NIST, a computação em nuvem pode ser definida como um modelo para habilitar o acesso por rede ubíquo, conveniente e sob demanda a um conjunto compartilhado de recursos de computação (como redes, servidores, armazenamento, aplicações e serviços) que possam ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços (Mell & Grance, 2011). Logo, a 'nuvem', como também é conhecida, pode ser acessada pelos usuários de uma organização em diferentes locais.

O estudo da computação em nuvem no setor privado vem sendo objeto de diversas pesquisas acadêmicas. Por outro lado, há carência de estudos sobre a computação em nuvem no setor público. Os governos são mais cautelosos do que as empresas em adotar os serviços de computação em nuvem (Yang & Tate, 2012). Observa-se, ainda, que a adoção de novas tecnologias na esfera pública ocorre de modo mais lento em função de algumas características burocráticas desse setor (Medeiros & Souza Neto, 2016).

Entre os aspectos que podem ser analisados ao considerar a computação em nuvem no setor público estão os benefícios e os riscos[1] envolvidos no emprego dessa tecnologia (Zissis & Lekkas, 2011; Paquette, Jaegger & Wilson, 2010). O estudo de tais benefícios e riscos, inclusive, pode ser realizado empregando o exame do conteúdo de artigos científicos que tangenciem o tema e estejam presentes em bases de dados acadêmicas (Vieira & Meirelles, 2015).

Considerando os argumentos mencionados nos parágrafos anteriores, o objetivo deste estudo é analisar os benefícios e riscos do uso da computação em nuvem no setor público,

[1] Para os fins deste estudo, o termo 'risco' no contexto em estudo da computação em nuvem, é a possibilidade que algum evento imprevisto, falha, ou mesmo mau uso dessa tecnologia, ameace um objetivo de negócio de uma organização (Veras, 2012).

com base em artigos disponibilizados em bases de dados acadêmicas, no período de 2017 a 2021. Trata-se de pesquisa descritiva com abordagens qualitativa e quantitativa, com uma amostra não probabilística de oitenta artigos. Na análise buscou-se examinar o teor dos artigos de acordo com benefícios e riscos da computação em nuvem no setor público, empregando um quadro com 12 subcategorias agrupadas em 2 categorias baseadas no referencial teórico.

Quanto à contribuição teórica, este estudo diferencia-se de outras pesquisas anteriores, como Vieira e Meirelles (2015), porque aborda em período recente características sobre benefícios e riscos da computação em nuvem. Diferencia-se, também, por contribuir para a literatura sobre a computação em nuvem com foco no setor público e por contemplar evidências de benefícios e de riscos sobre o uso da computação em nuvem no referido setor.

Quanto à contribuição prática, este estudo pode ser útil para as organizações públicas, tendo em vista que a contratação de serviços de nuvem é um assunto relevante para o planejamento estratégico de tecnologia da informação dessas organizações. O estudo pode ser útil, também, para acadêmicos e cidadãos usuários dos serviços públicos oferecidos de forma virtual pelas organizações públicas.

Este estudo é relevante socialmente porque no período em estudo houve a decretação de Pandemia decorrente da doença COVID-19 em março de 2020 pela World Health Organisation (WHO, 2020). Constata-se que após tal decretação houve aumento da demanda por uso de recursos tecnológicos para a prestação de serviços de forma virtual, por exemplo por meio de teletrabalho. Assim, este estudo abordando a computação em nuvem no setor público, trata tema atual em momento oportuno para o setor público e para a sociedade de forma mais ampla.

Por fim, o artigo está organizado da seguinte forma: além desta introdução, a Seção 2 apresenta o referencial teórico, a Seção 3 aborda a metodologia adotada neste estudo, a Seção 4 exibe os resultados e a Seção 5 mostra as conlusões e as recomendações da pesquisa. As referências constam do final do estudo.

2. Referencial Teórico

2.1. Computação em Nuvem: Aspectos Conceituais, Benefícios e Riscos

Segundo Cai et al. (2015), a ideia da computação em nuvem remonta aos anos de 1960, quando o conceito de computação de utilidade foi proposto pelo cientista da computação John McCarthy. Em 1966, Douglas Parkhill propôs que ela seria utilizada pelos setores público e privado. Em 2006, a expressão começou a ser empregada por empresas como Google, Amazon e outras (Yang & Tate, 2012; Araújo & Alves, 2019; Silva et al., 2020).

A computação em nuvem faz parte de um processo de evolução da arquitetura de TI, que teve o seu início por meio da arquitetura de mainframe e foi passando pela arquitetura cliente-servidor. A arquitetura de mainframe baseou-se em computadores de grande porte que processavam dados de forma centralizada, buscando melhor aproveitar recursos. A grande desvantagem da arquitetura baseada em mainframe consistia nos custos tanto de aquisição, quanto de manutenção, que eram bastante elevados (Araújo & Alves, 2019).

A arquitetura cliente-servidor surgiu para atender demandas das organizações que necessitavam de arquitetura com menores custos, maior flexibilidade e que tivesse a capacidade de ser distribuída para ambientes externos. A arquitetura cliente-servidor propõe que os aspectos de processamento e de armazenamento dividam-se em diferentes computadores conectados em rede (Medeiros & Neto, 2016).

A arquitetura da computação em nuvem é baseada em centros de processamento de dados (datas centers), responsáveis pelo processamento e o repositório de dados, combinando as duas arquiteturas citadas nos dois parágrafos anteriores. Um data center é um conjunto integrado de componentes de alta tecnologia que fornecem serviços de infraestrutura de TI de valor agregado, cuja função é processar e armazenar uma grande demanda de dados, para qualquer tipo de organização (Veras, 2012). Os refeirdos data centers podem estar localizados em diversos países (Silva et al., 2020).

A computação em nuvem contribui para que dispositivos possam acessar, armazenar e processar as informações digitais por meio da internet. Cabe ressaltar que o NIST define que a computação em nuvem possui como características essenciais o 'Autoatendimento sob demanda', o 'Amplo acesso à rede', a 'Combinação de recursos', a 'Rápida elasticidade' e o 'Serviço medido' (Mell & Grance, 2011).

Em relação aos modelos de serviços a computação em nuvem pode ser disponibilizada em uma *Infrastructure as a Service* (IaaS), em *Platform as a Service* (PaaS) ou em *Software as a Service* (SaaS). Além disso, os quatro modelos de implantação de computação em nuvem definidos pelo NIST são conhecidos como, nuvem privada (*private cloud*), nuvem pública (*public cloud*), nuvem comunitária (*community cloud*) e nuvem híbrida (*hybrid cloud*) (Laudon & Laudon, 2014).

É adequado mencionar que a redução de custos é apontada como um dos principais benefícios da computação em nuvem, visto que ao não utilizar o modelo de computação em nuvem, as organizações terão de considerar análise de investimento para a aquisição de recursos e de sua chegada e instalação (Meijer & Brown, 2014). A computação em nuvem, ainda, por oferecer acesso a recursos que são compartilhados e provisionados de acordo com as necessidades, contribui para otimizar gastos com a infraestrutura de TI (Marston et al., 2011; Robu, 2012; Géczy et al., 2012; Bidgoli, 2011; Meijer & Brown, 2014; Vieira & Meirelles, 2015).

O crescimento do foco no negócio da organização contratante é outro benefício que pode motivar a contratação dos serviços na nuvem, visto que ao se contratar um provedor de serviços em nuvem as questões relacionadas a atualização da infraestrutura de TI serão de responsabilidade da empresa contratada. Por sua vez, a organização contratante terá mais tempo para focar em seus negócios, resultando no aumento da eficiência (Zota & Fratila, 2013; Vieira & Meirelles, 2015).

Embora a computação em nuvem apresente benefícios é importante ressaltar os riscos na adoção dessa tecnologia (Veras, 2012). Segundo Viera e Meirelles (2015) os riscos relacionados à segurança preocupam as organizações ao adotarem a computação em nuvem. A este respeito, os provedores necessitam estabelecer políticas de segurança que atendam a diferentes usuários e processos, realizem o descarte adequado dos dados inutilizados e garantam a privacidade e a confidencialidade dos dados acessados pela internet.

Outro risco a ser considerado é o oriundo de questões legais, abrangendo regulação e legislação do uso da computação em nuvem pelos países. A este respeito, é adequado avaliar as responsabilidades quanto ao tratamento das informações considerando diferentes regiões geográficas onde os data centers estão localizados, antes de se propor a contratação do serviço de nuvem (Géczy et al, 2012).

O comprometimento da disponibilidade dos serviços é outro risco que deve ser avaliado pelas organizações. Para isso, os provedores devem manter os serviços disponíveis ou mesmo ter um plano de continuidade na eventualidade da ocorrência de uma indisponibilidade (Kalyvas et al., 2013; Vieira & Meirelles, 2015). Em adição, verifica-se que o serviço prestado de computação em nuvem sujeita-se a acordos de nível de serviço ou *Service Level Agreement* – SLA, estabelecido entre provedores dos serviços e organizações contratantes. Os SLAs podem ser definidos para a aplicação ou para a infraestrutura de TI (Veras, 2012).

2.2. Benefícios e Riscos da Computação em Nuvem no Setor Público

Na introdução foi citado que nos últimos anos houve a emergência de iniciativas no setor público para emprego da computação em nuvem, em que pese a literatura sugira que governos em geral são mais cautelosos do que as empresas privadas em adotar os serviços de computação em nuvem (Yang & Tate, 2012).

Nesta seção enfatizam-se exemplos de benefícios da computação em nuvem no setor público, bem como dos riscos de sua utilização no referido setor. Para orientar essa narrativa, inicialmente exibe-se a Tabela 1. A tabela exibe 12 subcategorias associadas a 2 categorias, descritas na sequência.

Categoria	Subcategoria
Benefícios	Desempenho
	Redução de Custos
	Escalabilidade
	Resiliência e continuidade de negócios
	Capacidade de manutenção
	Melhoramentos quanto à Segurança
Riscos	Comprometimento da disponibilidade dos serviços de nuvem
	Defasagem entre recursos tecnológicos do setor público e do prestador de serviço de nuvem
	Falta de integridade dos dados e das informações
	Possibilidade do prestador do serviço de nuvem de não ser Auditável
	Vulnerabilidades quanto à segurança (abrangem: 1- acesso não autorizado; 2 - vazamento de dados; e 3 - deficiências nos mecanismos de segurança referentes aos terceirizados.)
	Questões legais (inclusive questões dispondo sobre a legislação transfronteiriça)

Fonte - adaptado a partir do referencial teórico, principalmente, Zissis e Lekkas (2011) e Paquette et al. (2010).

Tabela 1 – Benefícios e Riscos do uso da nuvem no setor público

Inicialmente, sobre o desempenho citado na Tabela 1, constata-se que o modelo de computação em nuvem contribui para aumentar a agilidade dos serviços prestados aos cidadãos, a colaboração entre as organizações públicas e a eficiência dos seus processos (Zissis & Lekkas, 2011). A respeito da redução de custos, também citada na Tabela 1, existem exemplos de países como EUA, Reino Unido e Brasil, em que a redução de custos apresenta-se entre argumentos que impulsionam serviços de nuvem no setor público (Shin, 2013; Jones, 2015; Brasil, 2021).

A respeito da escalabilidade, descrita na Tabela 1, constata-se que serviços de nuvem podem expandir conforme demanda da organização pública, por meio da possibilidade de virtualização fornecida pelos provedores do serviço. Outros benefícios são contribuir para simplificar a capacidade de manutenção e para melhoramentos quanto à segurança da informação e comunicação, incluindo infraestrutura de segurança unificada (Zissis & Lekkas, 2011).

Verifica-se que a adoção da computação em nuvem melhora a resiliência (Jones, 2015). Sobre resiliência e continuidade de negócios citados na Tabela 1, os data centers dos provedores do serviço de nuvem distribuem-se em diferentes locais, o que contribui para continuidade dos negócios das organizações públicas, em caso de falha ou desastres naturais que afetem uma região específica.

Apesar de a computação em nuvem no setor público ter potencial para ajudar a modernizar as organizações, qualquer implementação deve considerar tanto os benefícios quanto os riscos (Jones, 2015). Neste sentido, discorre-se a seguir sobre os riscos da computação em nuvem no setor público enumerados na Tabela 1.

Quanto à disponibilidade dos serviços de nuvem, segundo Paquette et al. (2010), os acordos de níveis de serviço - SLAs deverão especificar os serviços contratados a fim de evitar dúvidas sobre a empresa provedora e o funcionamento da infraestrutura da nuvem. Atenção deve ser dada para possível defasagem entre os recursos tecnológicos do setor público e os fornecidos pelo prestador dos serviços de nuvem, que poderá causar falhas de processamento ou de armazenamento dos dados e das informações.

Especial cuidado deve ser dado pela organização pública quanto à falta de integridade dos dados e das informações. Tais dados e informações devem ser mantidos precisos, validos e seguros enquanto disponibilizados. Atenção deve ser dada à capacidade do provedor de serviço para assegurar todos privilégios de acesso para que a nuvem possa ser auditada segundo regulamentações e requisitos estabelecidos por agências reguladoras (Paquette et al., 2010).

Por fim, o uso da computação em nuvem deve estar em conformidade com as leis e os regulamentos, e contratos transparecer as responsabilidades dos provedores de nuvem quanto aos requisitos de privacidade (Shin, 2013). Ainda, cuidados devem ser tomados pela organização pública para monitorar os potenciais riscos decorrentes de exposição do prestador de serviço a vulnerabilidades quanto à segurança, abrangendo acesso não autorizado, vazamento de dados e deficiências no tratamento de terceirizados (Paquette et al., 2010).

3. Metodologia

Para alcançar o objetivo propostos neste estudo foi realizada pesquisa descritiva (Sampieri et al., 2013) com abordagens qualitativa e quantitativa. O estudo compreende exame do conteúdo de artigos acadêmicos publicados a respeito da computação em nuvem no setor público em bases de dados acadêmicas.

A população pesquisada neste estudo é composta por artigos publicados nas seguintes bases de dados acadêmicas: *EBSCO, Emerald Insight, SAGE Jounarls, Science Direct, SpringerLink e WEB of Science*. Todas essas bases apresentaram artigos revisados por pares. Vale ressaltar que a amostra é não probabilística, pois a escolha dos elementos não depende da probabilidade, mas de critérios estabelecidos pelos pesquisadores (Sampieri et al., 2013). A amostra foi selecionada conforme critérios apresentados em três etapas a seguir descritas:

- Na 1ª etapa, a pesquisa foi realizada nas bases de dados citadas no parágrafo anterior desta seção, empregando as palavras em inglês 'computação em nuvem' associadas com as palavras 'setor público', utilizando o operador booleano 'AND'. Os resultados foram os seguintes: 570 artigos na EBSCO, 1.911 artigos na *Emerald Insight*, 10.307 artigos na *Science Direct*, 2.971 artigos na *SAGE Jounarls*, 18.037 artigos na *SpringerLink* e 302 artigos na *WEB of Science*.
- Na 2ª etapa, aplicaram-se os seguintes filtros: artigos oriundos de revistas cuja avaliação é feita por pares, artigos de pesquisa, período de publicações dos artigos de 2017 a 2021 (período de cinco anos completos mais recentes). Após aplicar os filtros chegou-se a 424 artigos na EBSCO, 450 artigos na *Emerald Insight*, 75 artigos na *SAGE Jounals*, 429 artigos na *Science Direct*, 174 artigos na *SpringerLink* e 92 artigos na *WEB of Science*.
- Na 3ª etapa, após excluir nove artigos repetidos, foi realizada uma leitura dos títulos, resumo e palavras-chaves, com a finalidade de se verificar se possuíam relação com os objetivos propostos neste estudo. Assim, a amostra foi selecionada com 9 artigos da EBSCO, 10 artigos da *Emerald Insight*, 3 artigos da *SAGE Jounarls*, 22 artigos da *Science Direct*, 17 artigos da *SpringerLink* e 19 artigos da *WEB of Science*. Após essa etapa, a quantidade de 80 artigos que foram selecionados para a seleção da amostra deste estudo.

Os artigos foram coletados em periódicos disponíveis em bases de dados selecionadas a partir do Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES (Capes, 2021). Os dados foram coletados no intervalo entre o dia 6/5/2021 e 31/12/2021. A coleta dos dados foi feita nas 6 bases dados mencionadas nesta seção, sendo todas elas indexadas ao Portal da CAPES, o qual foi acessado remotamente pelo recurso Comunidade Acadêmica Federada - CAFE.

O tratamento e a análise dos dados coletados empregou a análise de conteúdo, que pode ser entendida como "um conjunto de técnicas de análise das comunicações visando obter, por procedimentos, sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a interferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) destas mensagens." (Bardin, 1977, p. 42).

Corroborando com a pesquisa de Viera e Meirelles (2015), foram identificados os benefícios e os riscos do uso da computação em nuvem no setor público presentes nos artigos selecionados para a amostra por meio de análise de conteúdo, considerando as categorias e subcategorias apresentadas na Tabela 1, citada na Seção 2.2 do referencial teórico.

A referida Tabela 1 apresenta duas categorias e doze subcategorias, sendo seis subcategorias associadas a benefícios da computação em nuvem e as outras seis subcategorias associadas a riscos da computação em nuvem. Os benefícios foram baseados no referencial teórico, principalmente em Zissis e Lekkas (2011). Quanto aos riscos do uso da computação em nuvem em organizações públicas, subcategorias basearam-se, também, no referencial teórico, especialmente em Paquette et al. (2010).

Como a Tabela 1 com 12 subcategorias foi empregada na análise do conteúdo de cada um dos 80 artigos da amostra, ao todo foram examinadas 960 subcategorias. A regra de enumeração adotada na análise de conteúdo foi a presença ou a ausência de cada subcategoria no texto dos artigos analisados (Bardin, 1977). A presença das categorias foram verificadas por meio da leitura dos resumos, resultados e conclusões de cada artigo.

Por fim, após a realização da análise de conteúdo, foram usados recursos de estatística descritiva para organizar, resumir e representar os dados (Larson & Farber, 2010). Assim, os dados da amostra oriundos da análise de conteúdo foram representados de modo resumido por meio da contagem de frequência de presença e ausência, bem como por percentuais de subcategorias presentes agrupados por categoria. Com a finalidade de confeccionar tabelas exibidas nas análises dos resultados, foram utilizados os softwares Microsoft Excel e LibreOffice Calc.

4. Resultados

Esta seção apresenta os resultados do estudo. Exibe-se, inicialmente, os resultados por subcategoria, apresentando-se, ao final, uma consolidação dos resultados por categoria indicativa de benefícios e riscos da computação em nuvem no setor público.

Inicialmente, após exame de 960 subcategorias, os resultados da análise de conteúdo dos artigos da amostra permitiram elaborar a Tabela 2, que apresenta a segmentação em doze subcategorias dos benefícios e riscos identificados nos 80 artigos selecionados como amostra nesta pesquisa. Para se chegar a esta tabela, para cada artigo foram examinadas 12 subcategorias segmentadas em duas categorias descritas na Tabela 1 da Subseção 2.2 deste estudo.

Verifica-se na Tabela 2 que com relação aos benefícios, a subcategoria ‘Redução de Custos’ esteve presente em 45 artigos (56,25% do total da amostra). Já a subcategoria ‘Desempenho’ esteve presente em 26 artigos (32,50% do total da amostra). Na sequência, a subcategoria ‘Melhoramentos quanto à Segurança’, foi identificada em 23 artigos (28,75% do total da amostra).

Categoria	Subcategoria	P	A	P%
Benefícios	Desempenho	26	54	32,50
	Redução de Custos	45	35	56,25
	Escalabilidade	18	62	22,50
	Resiliência e continuidade de negócios	14	66	17,50
	Capacidade de manutenção	5	75	6,25
	Melhoramentos quanto à Segurança	23	57	28,75
Riscos	Comprometimento da disponibilidade dos serviços de nuvem	14	66	17,50
	Defasagem entre recursos tecnológicos do setor público e do prestador de serviço de nuvem	10	70	12,50
	Falta de integridade dos dados e das informações	7	73	8,75
	Possibilidade do prestador do serviço de nuvem de não ser Auditável	4	76	5,00
	Vulnerabilidades quanto à segurança (abrangem: 1- acesso não autorizado; 2 - vazamento de dados; e 3 - deficiências nos mecanismos de segurança referentes aos terceirizados.)	45	35	56,25
	Questões legais (inclusive questões dispondo sobre a legislação transfronteiriça)	21	59	26,25

Fonte – Dados da pesquisa

Legenda – 'P' é quantidade de artigos com a subcategoria presente, 'A' é quantidade de artigos com a subcategoria ausente e 'P%' é percentual de artigos com a subcategoria presente.

Tabela 2 – Benefícios e riscos identificados na amostra

A respeito da subcategoria 'redução de custos', citada na Tabela 2, verifica-se no referencial teórico deste estudo que a computação em nuvem, por oferecer acesso a recursos que são compartilhados e provisionados de acordo com as necessidades, contribui para otimizar gastos com a infraestrutura de TI (Marston et al., 2011; Robu, 2012; Géczy et al., 2012; Bidgoli, 2011; Meijer & Brown, 2014; Vieira & Meirelles, 2015). Constatou-se, ainda, com base no referencial teórico, que a redução de custos apresenta-se entre argumentos que impulsionam serviços de nuvem no setor público (Shin, 2013; Jones, 2015)

O referencial teórico expôs, com base em Marston et al. (2011) que a computação em nuvem representa a união das duas principais tendências em TI, a eficiência e a agilidade dos negócios, argumento que corrobora o benefício de desempenho identificado em artigos da amostra e apresentado na Tabela 2. Em consonância os benefícios resiliência e continuidade de negócios e melhoramentos quanto à segurança. Ainda, o uso da computação em nuvem no setor público contribui para o aprimoramento da segurança e a centralização da infraestrutura de TI (Jones, 2015).

No tocante aos riscos, a Tabela 2 mostra que a subcategoria 'Vulnerabilidades quanto à segurança' esteve presente em 45 artigos (56,25% do total da amostra de artigos), seguido pela subcategoria 'Questões Legais', presente em 21 artigos (26,25% do total da amostra de artigos). Prosseguindo, a subcategoria 'Comprometimento da Disponibilidade dos

Serviços de Nuvem' esteve presente em 17,50% do total da amostra, com 14 artigos e a subcategoria 'Defasagem entre Recursos Tecnológicos do Setor Público e do Prestador de Serviço de Nuvem' teve presença em 10 artigos (12,50% do total da amostra). Por fim, a Possibilidade do Prestador do Serviço de Nuvem de não ser Auditável, com 4 artigos (5,00% do total da amostra).

No que concerne aos riscos apresentados na Tabela 2 a subcategoria 'Vulnerabilidades quanto à segurança' apresenta, também, evidência no estudo de Vieira e Meirelles (2015). Rubo (2012) salienta as os cuidados com as questões se justificam para as organizações, pois as suas informações confidenciais são coletados, armazenados e processados por empresas terceirizadas.

No que se refere à subcategoria 'Questões legais' apresentadas na Tabela 2, Géczy et al. (2012) ressaltam que as diferentes legislações em regiões geográficas distintas devem ser sempre consideradas pelas organizações antes da contratação do serviço de nuvem. Quanto à subcategoria 'Comprometimento da disponibilidade dos serviços de nuvem da referida Tabela 2, é necessário que os provedores de serviços de nuvem possuam um plano de continuidade em caso de uma indisponibilidade" (Kalyvas et al 2013; Vieira & Meirelles, 2015). Vale relembrar que Paquette et al. (2010) explicam que os acordos de nível de serviço, SLA, deverão especificar com clareza os serviços contratados e os agentes públicos responsáveis pelos processos licitatórios, de contratação dos serviços em nuvem, deverão ter noção sobre os riscos e os impactos que uma possível interrupção poderá acarretar ao órgão contratante.

Cabe destacar o baixo percentual de presença da subcategoria 'Possibilidade do prestador do serviço de nuvem de não ser auditável apresentada na Tabela 2, não corrobora com a literatura. Paquette et al. (2010) explicam que a auditoria possibilita avaliar a integridade das informações armazenadas na nuvem. Ainda, Marston et al. (2011) alertam que as organizações deverão desenvolver políticas de auditoria de TI que atendam os requisitos das regulamentações nacionais e internacionais.

Por fim, com base no Teor da Tabela 2, foi possível elaborar a Tabela 3 com os resultados da análise de conteúdo dos 80 artigos da amostra considerando a análise por categoria. Segundo a Tabela 3 os resultados permitiram identificar 232 subcategorias, totalizando 24,17% das 960 subcategorias analisadas. Foi apurada a presença de 131 subcategorias, correspondendo a 27,29% das subcategorias associadas à categoria 'benefícios da computação em nuvem' e foi apurada a presença de 101 subcategorias, correspondendo a 21,04% das subcategorias associadas à categoria 'riscos da computação em nuvem'.

CATEGORIA	P	A	P%
Benefícios	131	349	27,29
Riscos	101	379	21,04
Total	232	728	24,17

Fonte – dados da pesquisa, elaborados a partir dos totais da Tabela 2

Legenda – 'P' é quantidade de artigos com a subcategoria presente; 'A' é quantidade de artigos com a subcategoria ausente; e 'P%' é percentual de artigos com a subcategoria presente na categoria.

Tabela 3 – Resultado da análise de conteúdo - por análise de categoria

5. Conclusões

O objetivo deste artigo foi analisar os benefícios e riscos do uso da computação em nuvem no setor público, com base em artigos disponibilizados em bases de dados acadêmicas, no período de 2017 a 2021. Este estudo pode trazer reflexões que ajudem a melhor entender a adoção da computação em nuvem no setor público.

Realizou-se pesquisa descritiva, com abordagem qualitativa e quantitativa. Foi empregada a análise de conteúdo para tratar dados de uma amostra de oitenta artigos selecionados em bases de dados acadêmicas. Na análise buscou-se examinar o conteúdo dos artigos da amostra de acordo com benefícios e riscos da computação em nuvem no setor público, empregando-se um quadro com 12 subcategorias agrupadas em 2 categorias baseadas no referencial teórico.

Após exame de 960 subcategorias, os resultados permitiram identificar o total de 232 subcategorias presentes, o que representa 24,17% do total de subcategorias. Verificou-se, também, que 131 subcategorias são associadas aos 'Benefícios da computação em nuvem', representando 27,29% das subcategorias associadas a esta categoria, e 101 subcategorias são associadas aos 'Riscos da computação em nuvem', representando 21,04% das subcategorias associadas a esta categoria.

A análise por subcategoria permitiu constatar, quanto aos benefícios do uso da computação em nuvem, que a subcategoria a 'Redução de custos', com 45 artigos representou o total de 56,25% da amostra. Por sua vez, a subcategoria 'Capacidade de manutenção' apresentou 5 artigos, representando 6,25% do total da amostra. Quanto aos riscos da computação em nuvem no setor público, a subcategoria 'Vulnerabilidades quanto à segurança' esteve presente em 45 artigos, correspondendo a 56,25% do total da amostra. Por sua vez, a 'Possibilidade do prestador do serviço de nuvem de não ser auditável', esteve presente em 4 artigos, equivalente a 5,00% do total da amostra. Assim, os achados deste estudo indicaram, de maneira geral, que os benefícios e riscos da computação em nuvem não se distribuiram de maneira uniforme.

Este estudo trata tema atual, apresentando contribuições para avançar na investigação do estudo da computação em nuvem no setor público, inclusive reflexões para acadêmicos e demais partes interessadas. De notar que os resultados apresentados levam em conta o teor dos artigos que foram publicados num período específico. Adicionalmente, este trabalho enfatizou o conteúdo dos artigos examinados, em especial os benefícios e os riscos do uso da computação em nuvem. Estes argumentos indicam que pesquisas futuras podem ser efetuadas para contemplar aspectos não abordados por este estudo.

São recomendações para pesquisas futuras: (A) realizar estudos para verificar publicações sobre os benefícios e os riscos da computação em nuvem no setor público em outros períodos de análise; (B) realizar estudos com foco em análises considerando co-citações e coautoria de artigos relativos ao tema abordado neste estudo; (C) realizar novas pesquisas para verificar a redução dos custos que a adoção da computação em nuvem pode proporcionar no setor público; e (D) realizar estudos, na forma de casos, para analisar os principais riscos decorrentes do uso da computação em nuvem nas organizações públicas, especialmente no tocante às eventuais vulnerabilidades quanto à segurança nessas organizações.

Referências

Araújo, C. C. L, & Alves, C. A. M. (2019). Computação em nuvem: um estudo sobre a distribuição da produção de artigos publicados no período de 2007 a 2016. *Revista de Tecnologia Aplicada*. 8(1), 20-32. http://dx.doi.org/10.21714/2237-3713rta2019v8n1p20.

Bardin, L (1977). *Análise de Conteúdo*. Edições 70.

Bidgoli, H. (2011). Successful introduction of Cloud Computing into your organization: a six-step conceptual model. *Journal of International Technology and Information Management*, 20(1), 20-38.

Brasil. (2021). *Adoção de serviços de computação em nuvem pelo governo federal*. Gov. br Ministério da Economia. https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/computacao-em-nuvem.

Cai, Y., Lu, W., Wang, L., & Xing, W. (2015) Cloud computing research analysis using bibliometric method. *International Journal of Software Engineering and Knowledge Engineering*, 25(3), 551-571. https://doi.org/10.1142/S0218194015400203

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. (2021). *Portal de Periódicos CAPES/MEC*. http://www.periodicos.capes.gov.br.

Géczy, P., Izumi, N., & Hasida, K. (2012). Cloudsourcing: managing cloud adoption. *Global Journal of Business Research*, 6 (2), 57-70.

Jones, S. (2015). Cloud computing procurement and implementation: Lessons learnt from a United Kingdom case study. *International Journal of Information Management*, 35 (6), 712-716.

Kalyvas, J. R.; Overly, M. R.; & Karlyn, M. A. (2013). Cloud Computing: A Practical Framework for Managing Cloud Computing Risk – Part I, *Intellectual Property & Technology Law Journal*, 25 (3), 7-18.

Larson, R.; & Faber, E. (2010). *Estatística Aplicada* (4ª Ed). Editora Pearson.

Laudon, K. C., & Laudon J. P. (2014). *Sistemas de Informação Gerenciais* (11a. Ed). Editora Pearson.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—the business perspective. *Decision Support Systems*, 51(1), 176-189.

Medeiros, M. F. M. de, & Neto, M. V. S. (2016). Uso da computação em nuvem no setor público: um estudo de caso com gestores de TI do estado do Rio Grande do Norte e do Governo Federal. *Revista Gestão & Tecnologia*, 16 (1), 135-156.

Meijer, C. R. W. & Brown, A. (2014). Transaction banking in the cloud: Towards a new business model. *Journal of Payments Strategy & Systems*, 8(2), 206-223.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing: recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-145. https://doi.org/10.6028/NIST.SP.800-145

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the Security Risks Associated with Governmental Use of Cloud Computing. *Government Information Quarterly*, 27 (3), 245-253. https://doi.org/10.1016/j.giq.2010.01.002.

Robu, M. (2012). Cloud computing based information systems – present and future. *USV Annals of Economics & Public Administration*, 12 (2), 94-100. http://www.annals.seap.usv.ro/index.php/annals/article/viewFile/593/512

Sampieri, R. H., Collado, C. F., & Lucio, M. D. P. B. (2013). *Metodologia de Pesquisa* (5. ed). Mc Graw-Hill.

Shin, Dong-Hee. (2013). User centric cloud service model in public sectors: policy implications of cloud services. *Government Information Quarterly*, 30 (2), 194-203. https://doi.org/10.1016/j.giq.2012.06.012

Silva, F. R., Soares, J. A., Serpa, M. da. S., Maitino Neto, R., Aleixo Junior, J. F. M., Oliveira, H. S. de., & Pichetti, R. F. (2020). *Cloud Computing*. Sagah, 2020.

Veras, M. (2012). *Cloud Computing: nova arquitetura da TI*. Brasport.

Vieira, C. S., & Meirelles, F. S. (2015). Computação em Nuvem: análise bibliométrica da produção científica sobre os fatores que influenciam as empresas no seu uso. *Revista Eletrônica Gestão e Serviços*, 6 (2), 1215-1230. https://doi.org/10.15603/2177-7284/regs.v6n2p1215-1230

World Health Organisation (2020). *WHO caracterizes COVID-19 as a pandemic*. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen.

Yang, H., Tate, M. A (2012). Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for Information Systems*, 31 (article 2), 35-60. https://doi.org/10.17705/1CAIS.03102

Zissis, D.; Lekkas, D. (2011). Securing e-Government and e-Voting with an Open Cloud Computing Architecture. *Government Information Quarterly,* (28)2, 239–251, https://doi.org/10.1016/j.giq.2010.05.010.

Zota, Razvan-Daniel, Fratila, Lucian-Alexandru. (2013). Cloud standardization: Consistent business processes and information. *Informatica Economica*, 17 (3), 137-147. https://revistaie.ase.ro/content/67/12%20-%20Zota,%20Fratila.pdf

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 03/12/2021
Aceitação/Acceptance: 07/02/2022

Contaminación cero: la propulsión basada en hidrógeno del buque colombiano de apoyo a catástrofes

Diana Ramírez[1], Omar Vásquez[1], José María Riola[2]

DRamirez@cotecmar.com; OVasquez@cotecmar.com; Chema.riola@rga-psi.es,

[1] Corporación Cotecmar, zona industrial Mamonal km 9, Cartagena de Indias, Colombia

[2] Escuela Naval Almirante Padilla, Cartagena de Indias, Colombia

Pages: 550-559

Resumen: Dadas las áreas naturales protegidas en las que deberá navegar el Buque de Apoyo Logístico y Cabotaje Liviano (BALC-L) en sus misiones de ayuda humanitaria y apoyo a catástrofes en el interior fluvial del país, es clara la necesidad de dotar al buque de un sistema de propulsión que no contamine, por lo que se ha decidido en su diseño optar por una versión cuya propulsión esté basada en el empleo del nuevo vector energético basado en hidrógeno. Un vector energético calificado como limpio y renovable, y que en el diseño del buque se ha considerado que debe basarse en el empleo de pilas de combustible para conseguir una propulsión eficiente. Este artículo presenta un acercamiento a la tecnología de las pilas de combustible desde la perspectiva de los diseñadores navales en la realización de un programa de I+D y el caso práctico de su aplicación a este buque.

Palabras-clave: BALC-L; I+D; Pila de Combustible; Hidrogeno; Propulsión.

Zero pollution: the hydrogen-based propulsion of the Colombian disaster support ship

Abstract: Given the protected natural areas in which the Logistical Support and Light Cabotage Ship (BALC-L) must navigate in her missions of humanitarian aid and support for catastrophes in the country's interior rivers, there is a clear need to provide the ship with a propulsion system that does not pollute, so it has been decided in its design to opt for a propulsion version based on the use of the new energy vector on hydrogen. An energy vector qualified as clean and renewable, and that in the ship design it has been considered the use of fuel cells to achieve efficient propulsion. This paper presents an approach to fuel cell technology from the perspective of R&D program naval designers and the practical case of their application to this ship.

Keywords: BALC-L; I+D; Fuel Cell; Hydrogen; Propulsion.

1. Introducción

Todos hemos terminado de aprender que la energía basada en combustibles fósiles es inviable a medio plazo (Salaet y Roca, 2010) debido al alto coste que representa para la humanidad. Es una urgencia planetaria el desarrollar otras fuentes energéticas que se caractericen por su limpieza y su carácter renovable (UPME, 2015). Hay muchos desarrollos tecnológicos en áreas muy diversas, pero hay un amplio consenso en que las tecnologías basadas en el hidrógeno (figura 1) son las alternativas más prometedoras. Ello se debe a que al no producir contaminación supondrán un enorme beneficio medioambiental. Pero para que esta alternativa sea una realidad se necesita desarrollar una serie de desafíos técnicos que van desde su producción hasta su logística.



Figura 1 – Industria del hidrógeno. (Fuente: Lenovo)

El hidrógeno como vector energético está permitiendo que se puedan desarrollar una gran cantidad de tecnologías. Las pilas de combustible alimentadas con hidrógeno están consiguiendo alcanzar altas eficiencias que dan lugar a aplicaciones móviles y estacionarias que permitirán alcanzar los objetivos previstos en las políticas energéticas del sector transporte, así como en las políticas de la generación distribuida de potencia.

En el contaminante mundo del automóvil se han enfocado los esfuerzos hacia el mundo de las baterías eléctricas y las pilas de combustible, por lo que es normal que empiecen a aparecer soluciones innovadoras de su adaptación a la complicada propulsión marítima.

La Organización Marítima Internacional (OMI) está liderando la regularización de la descarbonización en los buques con normativas para la reducción de las emisiones de gases que producen efecto invernadero como el SO_x con la resolución MPEC 70, el NO_x con la resolución MPEC 177, CO_2, etc.

Y además, la OMI ha designado una serie de áreas de control de emisiones (ECA), figura 2, para dichas reducción de emisiones en zonas marítimas específicas como

son la del Mar Báltico, el norte y oeste del Mar Caribe, el Canal de la Mancha o el Mar Mediterráneo. Según el gobierno francés (DP, 2019) el establecimiento de la zona ECA en el Mar Mediterráneo supone un gran beneficio socioeconómico ya que determina que el dióxido de azufre (SO_2) se reducirá un 77 %, el dióxido de nitrógeno (NO_2) en un 76 % la materia particulada en un 20 % y una reducción considerable del nivel de ozono troposférico, un contaminante que está aumentando debido al calentamiento global.

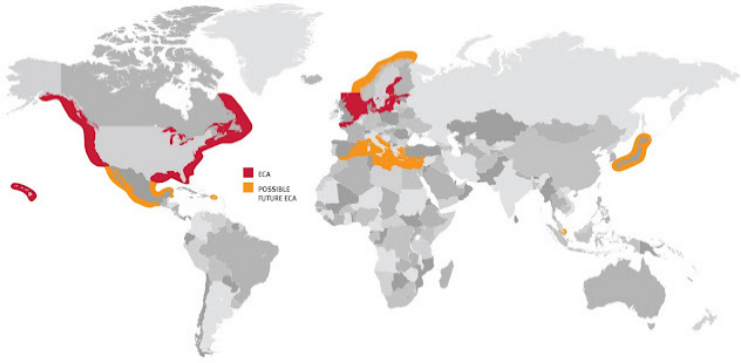


Figura 2 – Zonas ECA. (Fuente: IMO)

Y dentro del mundo de la certificación de los buques, son las Sociedades de Clasificación las que están publicando directrices técnicas para que las nuevas construcciones cumplan con las normativas de seguridad en el empleo de sistemas generadores de energía eléctrica basada en pilas de combustible, como fueron las primeras del Det Norske Veritas (DNV, 2003) o las últimas del American Bureau of Shipping (ABS, 2021) y Bureau Veritas (BV, 2022). Este interés también se expone en los buques de guerra (Fernández Jove et al, 2019) principalmente en las construcciones de submarinos (Monereo, 2015) como el de la figura 3 y en los sumergibles operados remotamente (ROV).



Figura 3 – Submarino S-80. (Fuente: Armada)

Una célula de combustible es un sistema electroquímico (Cifuentes et al, 2019) que consigue extraer la energía química que posee un combustible y transformarla en energía eléctrica. Y su éxito radica en que en sus reacciones sólo se emite calor, agua y en ocasiones, dióxido de carbono (CO_2). Y una primera ventaja medioambiental es obvia si pensamos en el buque navegando en áreas protegidas, ya que debido a su propulsión eléctrica el nivel de vibraciones y ruidos es mínimo (Beltrán et al, 2012) (OMI, 1981), lo que repercute directamente en mejores condiciones para la fauna fluvial, principalmente la que sufre las transmisiones de ruido radiado al agua.

Existen diferentes tipos de células de combustible, pero por sus características para el sector naval la más adecuada parece la célula tipo PEMFC o de membrana de intercambio de protones, aunque también se trabaja con las de carbonatos fundidos (MCFC) y óxido sólido (SOFC). La membrana impide el paso de los electrones, pero permite que los iones H^+ lleguen al cátodo. Estas células tienen un ánodo, un cátodo y un electrolito entre ellos o membrana para el intercambio de protones. Así, el hidrógeno se introduce en el ánodo y se produce:

$$H_2 \rightarrow H^+ + 2\ e^-$$

Los iones H^+ llegan hasta el cátodo, produciendo:

$$2\ e^- + 2\ H^+ + 0{,}5\ O_2 \rightarrow H_2O$$

Esta reacción exotérmica tiene una entalpía de formación de -285,8 kj/mol. Y la cantidad de energía a producir depende del número de celdas en serie que forman la pila, tipo, tamaño, presión y temperatura.

2. Potencia

La polarización (V) de la pila de combustible es el voltaje entre los electrodos y viene dada por la expresión:

$$V = N\ (V_{CA} - R_e\ D_i - P_T\ L_n\ D_i - C_1\ e^{C2\ Di})$$

Donde,

N: número de células de la pila

V_{CA}: voltios en circuito abierto

R_e: resistencia específica

D_i: densidad de corriente

P_T: pendiente de Tafel o representación gráfica de una porción de línea recta de una curva de polarización (Sánchez, 2020)(Estupiñan et al, 2014)

$C1$ y C_2 son constantes

La potencia de la pila en watios responde a la expresión:

$$P = \eta V D_i S$$

Donde η es el rendimiento y S el área de la célula.

Y el caudal másico a obtener, que se requiere de hidrógeno, suele calcularse con la siguiente expresión:

$$M_{H2} = P / \eta F_u PCI_{H2}$$

Siendo PCI el poder calorífico inferior del hidrógeno o entalpía de combustión por unidad de masa, de valor 120MJ/kg y F_u es el factor de utilización, que se suele estimar en unos valores entre 0,8 y 0,95 debido a que alguna cantidad del hidrógeno no se termina de disociar en el ánodo.

El almacenamiento del hidrógeno puede hacerse en estado gaseoso a alta presión o en estado líquido si se conserva a menos de -239°C. A la presión estándar de 700 bares, la densidad tiene un valor de aproximadamente 0,04 kg/l, por lo que necesita tanques muy voluminosos para el almacenamiento.

De lo presentado aquí se deduce que el problema de que el sector de la construcción naval no haya alcanzado una madurez definitoria para los grandes buques es debido a estos elevados pesos y volúmenes de almacenamiento (García, 2010). En nuestro caso, se presentan las mejores características para utilizar este combustible, un buque de carga relativamente pequeño, con una exigencia de velocidad baja y una necesidad alta de respeto del entorno medioambiental.

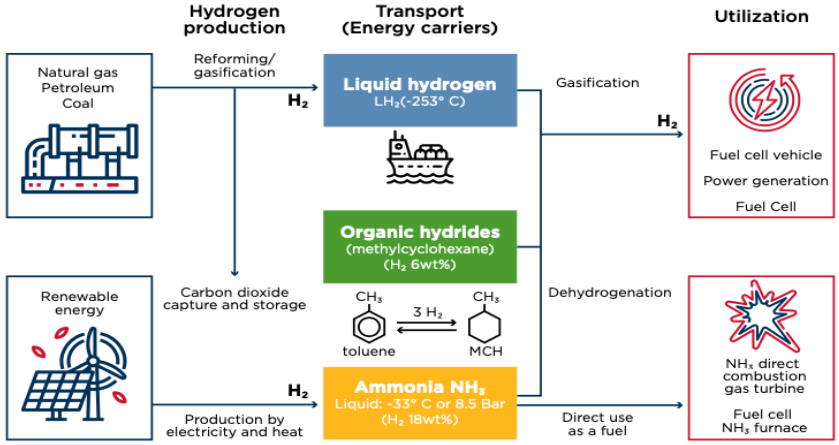


Figura 4 – Producción y utilización de hidrógeno y amoniaco. (Fuente: ABS)

Deberemos de tener en cuenta que el uso de los derivados del hidrógeno, como el amoniaco, que tienen una mayor probabilidad de ser usados en los grandes buques al necesitar mucho menor volumen de almacenamiento, lo que implica importantes beneficios ambientales y económicos, una vez que se han reducido sus costes de producción, almacenamiento, transporte, distribución y uso (figura 4).

3. El Buque BALC-L

El buque BALCL es un diseño desarrollado como proyecto de investigación con financiación del Fondo Francisco José de Caldas del Ministerio de Ciencia, Tecnología e Investigación de Colombia. Sus misiones principales son el desarrollo de operaciones de asistencia humanitaria, atención de desastres y apoyo logístico en poblaciones vulnerables del pacífico colombiano, permitiendo a la Armada Nacional de Colombia cumplir con sus objetivos de desarrollo social integral.

El entorno operacional de esta embarcación le impone retos excepcionales que han condicionado sus parámetros de diseño y que han sido evaluados en la fase de exploración tecnológica de su diseño conceptual. Se pueden mencionar dos de estos retos:

- Es necesario que el buque navegue en vías fluviales de muy bajo calado por lo cual se realizaron procesos de optimización estructural procurando un bajo peso en rosca y un calado de operación de 1,2 metros.
- Es necesario que el buque navegue en zonas protegidas como parques naturales, por lo cual se considera necesaria la integración de sistemas de generación de potencia con baja huella de carbono respecto a los sistemas convencionales con motores de combustión.

Bajo estas premisas se consideró oportuno la aplicación del hidrógeno como fuente alternativa de energía en este buque. Una vez desarrollado el diseño básico del buque, sus dimensiones principales son las siguientes:

Eslora Total (L):	43,50 m
Eslora entre Perpendiculares (Lpp):	40,18 m
Manga (B):	8,00 m
Puntal de Trazado (D):	2,30 m
Calado de diseño (T):	1,20 m
Desplazamiento @ calado de diseño	313,20 t

Su arreglo de espacio y capacidades corresponden a una embarcación tipo anfibia de desembarco con compuerta en proa para el ingreso y despliegue de equipos y vehículos a tierra sin la intervención de muelles o instalaciones portuarias.

Los propulsores del buque son del tipo *pump je*t o bombas de chorro azimutales que le proporcionan una gran maniobrabilidad en canales restringidos y accesibilidad a sitios de muy baja profundidad por la ausencia de apéndices bajo el casco.

De acuerdo con los resultados de las pruebas de canal con modelo a escala presentados en la Figura 5, la potencia propulsiva requerida por el buque para desarrollar una velocidad de 8 nudos en aguas someras es de aproximadamente 420 kW.



Figura 6 – Isométrico diseño externo BALCL. (Fuente: Cotecmar)

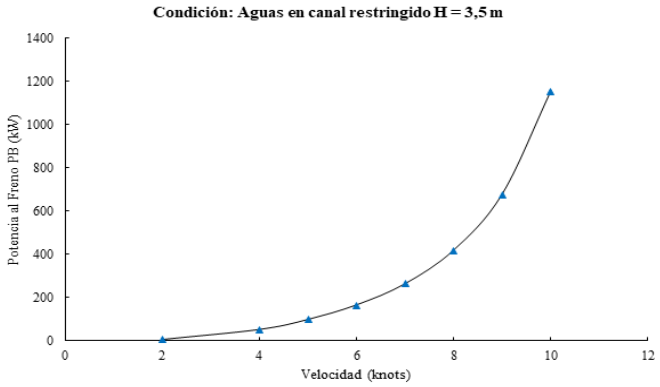


Figura 7 – Estimación de potencia al freno a partir de la condición "Aguas en canal restringido H = 3,5 m (Fuente: COTECMAR)

Esta demanda de energía propulsiva representa el mayor componente del consumo energético del buque, y como segundo componente importante se encuentra la carga eléctrica del resto de sistemas y equipos requeridos para la operación del buque, denominada "carga de hotel" y estimada en aproximadamente 80 kW.

A partir de estas capacidades se realizó el dimensionamiento de la planta de generación de energía a partir del H2.

La cantidad de celdas de combustible para el sistema de propulsión se estima teniendo en cuenta una potencia máxima aproximada de 420 kW requerida para la operación de los motores a la velocidad máxima de 8 nudos y la capacidad nominal de equipos comerciales disponibles en el mercado que puede generar hasta 70kW, por lo tanto, la cantidad de celdas sería de 6.

La cantidad de hidrógeno como combustible para las celdas se estima teniendo en cuenta los kilogramos de hidrógeno necesarios para generar la potencia requerida por los motores durante el tiempo estimado de la navegación a las distintas velocidades; conociendo que para la generación de 1 kWh se consume 0.1 kg de hidrógeno, se obtiene que la cantidad total de kilogramos de hidrógeno requeridos considerando el perfil operacional es de 95,5 kg por día de 6 horas de navegación

Se consideraron tanques de hidrógeno con capacidad para almacenar 8.5 kg de H2, por lo cual la cantidad de tanques requeridos, con una reserva del 10% se estima en 12 tanques.

La cantidad de baterías del sistema es también calculada con la energía requerida para soportar la carga máxima de 263kW durante 0,9 horas acorde al perfil operacional con un margen de 35% en la profundidad de descarga, teniendo en cuenta que cada batería tiene la capacidad de almacenar 44,2kWh, se requieren catorce (14) baterías para soportar la carga para la velocidad máxima durante 0,9 horas).

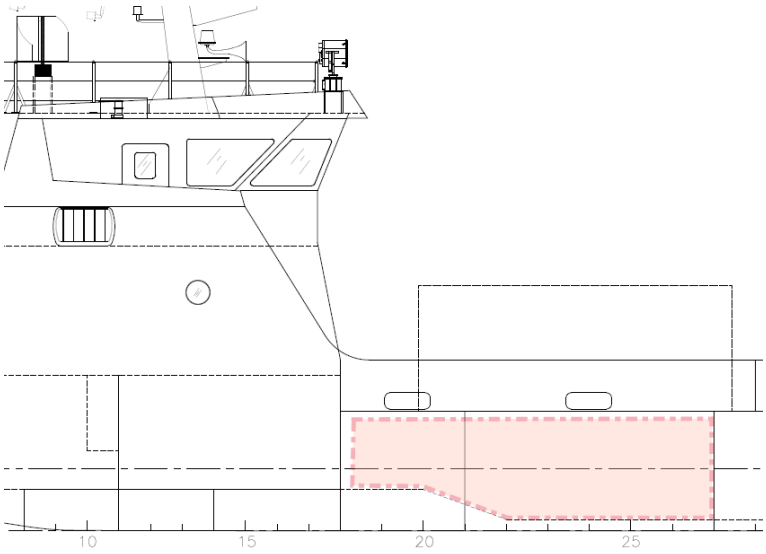


Figura 8 – Disposición del espacio para localización de los equipos del sistema de generación de energía por Hidrógeno (Fuente: COTECMAR)

El principal compromiso de la implementación de esta tecnología sobre los parámetros de diseño del buque está en términos de costo, peso y volumen. Para los dos últimos se cuenta con un compartimiento reservado para la distribución de los equipos sistema, como se muestra en Figura 6, el cual cuenta con un volumen disponible de 76 m^3 y en peso aproximadamente 20 toneladas, correspondiente al combustible Diesel que se dejaría de embarcar.

4. Conclusiones

- Actualmente, la economía del hidrógeno no ha alcanzado la madurez suficiente para poder competir con los combustibles fósiles. Pero es una solución que evita el almacenamiento del CO2 en la atmosfera y que contribuye a rebajar la alteración del clima en el planeta. La utilización del hidrógeno como vector energético proporciona una reducción de emisiones, sustancias contaminantes y de efecto invernadero.
- El hidrógeno es abundante en la Tierra y se puede producir en cantidades que satisfagan las demandas de todos los medios de transporte. Si este se produce mediante energías renovables se convertirá en el combustible de las próximas décadas. Las pilas de combustible están asociadas directamente al hidrógeno y los sistemas propulsivos basados en ellas aparecen como la solución limpia más inmediata.
- Del trabajo desarrollado, se puede afirmar que el hidrógeno parece ser el combustible perfecto para este tipo de buques de apoyo a catástrofes BALC-L. Y el hecho de que su uso como vector energético reduzca las emisiones de sustancias contaminantes y a su funcionamiento silencioso, presenta una solución correcta a la propulsión en zonas de enorme valor medioambiental, como lo son las zonas fluviales del interior del país. Si el Gobierno apuesta por esta tecnología, el prototipo está listo para su construcción.
- Además, que existe un atractivo nicho de mercado de buques de menos de 500 toneladas, formado principalmente por buques turísticos fluviales, transbordadores de pasajeros y automóviles, barcazas o remolcadores, que trabajan en ríos, canales, puertos o costeando y que son cerca del 25% de la flota mundial, para los que el hidrógeno les ofrece enormes beneficios medioambientales.
- En el diseño del buque se ha definido un espacio con reserva de volumen y peso para la implementación futura que puede ser escalable de las baterías, tanques y otros equipos de los sistemas de almacenamiento del H2. Las pilas de combustible ayudarán a la tendencia de que las propulsiones futuras de los buques serán totalmente eléctricas esto dará una mayor transcendencia a la utilización de microrredes eléctricas a bordo.

Referencias

ABS. (2021). Hydrogen as marine fuel. American Bureau of Shipping.

Beltrán, P, Díaz, J.I., Salinas, R. (2012). Achievement of the new underwater radiated noise requirements by the Spanish shipbuilding industry. 11th European Conference on Underwater Acoustics, Edimburgo, UK.

BV. (2022). Guidelines for fuel cell systems on board commercial ships. Bureau Veritas.

Cifuentes, B., Bustamante, F., Cobo, M. (2019). Producción de H2 apto para celdas de combustible a partir de la conexión del reformado con vapor de etanol y la oxidación preferencial de CO. Repositorio de la Universidad Pedagógica y Tecnológica de Colombia.

DP (2019). La creación de una zona ECA en el Mediterráneo. Diario del Puerto. Barcelona, España.

DNV. (2003). Guidelines for the use of fuel cell systems on board of ships and boats. Det Norske Veritas.

Estupiñan H., Peña, D., Quijano, E., Peñate, R. (2014). Evaluación de la corrosión de una aleación Pb-Ca-Sn por medio de técnicas electroquímicas. Universidad Nacional, Medellín, Colombia.

Fernández-Jove, A., McKinlay, A. & Riola, J.M. (2019). Optimization of the Life Cycle in the warships: maintenance plan and monitoring for cost reduction. Proceeding of the International Ship Design & Naval Engineering Congress (CIDIN) and XXVI Pan-American Congress of Naval Engineering, Maritime Transportation and Port Engineering (COPINAVAL). Singapore: Springer.

García, A. (2010). Producción, almacenamiento y distribución de hidrógeno. Instituto Nacional de Técnica Aeroespacial (INTA), Torrejón de Ardoz, España.

Monereo, N. (2015). El futuro del arma submarina: el S-80. Revista General de Marina, Cap. 11, pp. 357-365.

OMI. (1981). Resolution A.468(XII) Code on noise levels on board ships. Organización Marítima Internacional, Londres, UK.

Salaet, S., Roca, J. (2010). Agotamiento de los combustibles fósiles y emisiones de CO2: algunos posibles escenarios futuros de emisiones. Universidad de Santiago de Compostela. Revista Gallega de Economía, vol. 19, núm. 1, pp. 1-19

Sánchez, A. (2020). Montaje y puesta a punto de un potenciostato para llevar a cabo medidas de corrosión electroquímica. Universidad Carlos III, Madrid, España.

UPME, (2020). Integración de las energías renovables no convencionales en Colombia. Unidad de Planeación Minero Energética. Ministerio de Minas y Energía.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 16/12/2021
Aceitação/Acceptance: 05/02/2022

Sistema de telemedicina IoT de monitoreo de signos vitales y alertas de distanciamiento físico para enfermedades respiratorias

Steven Pérez[1], Juan P. Pallo[2], Santiago Manzano[3], Marco Jurado[4], Dennis Chicaiza[5]

sperez8452@uta.edu.ec; juanppallo@uta.edu.ec; victorsmanzano@uta.edu.ec; marcoajurado@uta.edu.ec; dv.chicaiza@uta.edu.ec.

[1] Universidad Técnica de Ambato, 180103, Ambato, Ecuador.

Pages: 560-572

Resumen: La pandemia del COVID-19 provocó complicaciones al sistema de salud en el Ecuador, tanto para la atención medica como para la prevención de la transmisión de enfermedades respiratorias. El proyecto desarrollado es un sistema de telemedicina conformado por: Un brazalete portable para la adquisición de datos, un servidor de almacenamiento de información en la nube para mostrarla en un aplicativo web y un asistente en la aplicación Telegram para consultas y alertas con un smartphone. Los niveles de BPMs, SpO2 y temperatura corporal son medidos en el brazalete de bajo costo y enviados al servidor a través del protocolo CoAP. El grupo de prueba para la validación de los datos fue de 20 personas que se encuentran entre los 25 y 40 años de edad, obteniendo una fiabilidad del dispositivo dentro de los valores permitidos por la Organización Panamericana de la Salud (OPS).

Palabras-clave: Monitoreo, Signos Vitales, IoT, COAP.

Electronic Vital Signs Monitoring System Based on IoT-COAP Protocol

Abstract: The COVID-19 pandemic caused complications to the health system in Ecuador, both for medical care and for the prevention of the transmission of respiratory diseases. The project developed is a telemedicine system consisting of: A portable bracelet for data acquisition, a server for storing information in the cloud to display it in a web application and an assistant in the Telegram application for consultations and alerts with a smartphone. BPMs, SpO2 and body temperature levels are measured on the low-cost cuff and sent to the server via the CoAP protocol. The test group for data validation was 20 people between 25 and 40 years of age, obtaining a reliability of the device within the values allowed by the Pan American Health Organization (PAHO).

Keywords: Monitoring, Vital Signs, IoT, COAP.

1. Introducción

Los principales problemas que existen al momento de contener la propagación de virus es un control inadecuado para comprobar la sintomatología con que se encuentran las personas que probablemente contrajeron el virus del tipo SARS-CoV; debido a que no se cuenta con una medición exacta de los síntomas que presenta la persona hasta que se acerque a un Centro de Salud o sea visitado por una brigada del Ministerio de Salud Pública (Freitas, 2021).

El acelerado avance de la tecnología ha permitido implementar dispositivos inteligentes en cada aspecto de nuestras vidas y la salud no es la excepción. Los dispositivos IoT (Internet of things) han mejorado las metodologías de control y monitoreo del individuo moderno, obteniendo grandes cantidades de información sobre una persona con el objetivo de procesar esta data de manera eficiente (Placencia et al., 2017).

Este artículo presenta un sistema de telemedicina que tiene como objetivo principal la monitorización de signos vitales del usuario utilizando un protocolo IoT como CoAP (Constrained Application Protocol). Sin embargo, esta no es la única característica que posee el sistema electrónico, también cuenta con funciones como alertas para mantener el distanciamiento físico entre usuarios, una interfaz web que muestra todos los signos vitales almacenados por el dispositivo con un registro temporal, por último, un bot en la aplicación Telegram que permite realizar consultas sobre los datos más recientes del paciente.

El dispositivo de adquisición es una pulsera portable que está compuesto por: el microcontrolador ESP-8266, el sistema de energía, una pantalla OLED para visualizar los datos y los sensores para obtener la temperatura corporal, la saturación de oxígeno y el ritmo cardiaco del usuario. La comunicación inalámbrica que utiliza el microcontrolador es WiFi empleando el protocolo IoT CoAP para la transferencia de datos con el servidor, una base de datos diseñada en MySQL para el almacenamiento de los signos vitales de cada paciente y un programa desarrollado en Python que controla el bot creado dentro de la aplicación Telegram.

El proyecto está desarrollado con software de código abierto y elementos electrónicos de bajo costo que trabajan en conjunto para formar un sistema de monitoreo de signos vitales que genera un registro para que el profesional de la salud reconozca anomalías en los signos vitales que presenta el paciente, conocer el estado en el que se encuentra y detallar indicaciones para el mejor tratamiento posible del usuario.

En la sección 2 del documento se detalla un compendio de trabajos relacionados sobre el uso de la telemedicina en el contexto del COVID-19. La sección 3 se presentan conceptos claves para el entendimiento y contextualización de esta investigación. El caso de estudio es presentado en la sección 4, mientras la implementación de la propuesta de solución se presenta en la Sección 5. En la sección 6 se discuten los resultados de la implementación del sistema y finalmente, en la sección 7 se discuten las conclusiones y trabajos futuros.

2. Obras relacionadas

En esta sección se presentan trabajos que implementan la telemedicina y el IoT con sus distintos protocolos y tecnologías. Gracias a este análisis, se obtiene una idea general

de investigaciones e implementaciones, tecnologías y arquitecturas utilizadas en la telemedicina.

En el año 2018, Zakariya Alaseel y Debatosh Debnath presenta una propuesta sobre un sistema de monitoreo de signos vitales con la finalidad de mantener supervisados a pacientes que presenten enfermedades graves y poder alertar sobre su estado de salud en caso de la presencia de anomalías. Demostrando que el sistema es funcional y con el uso del sistema es posible generar un ahorro a los usuarios al momento de realizar un monitoreo constante de las diferentes señales vitales, en este caso la temperatura corporal y la presión arterial (Alaseel & Debnath, 2018).

En el mismo año Sahmi Imane, Mazri Tomader y Hmina Nabil realizan un estudio de varios sistemas de atención medica con sus beneficios y debilites considerando los protocolos basados en IoT más utilizados como MQTT (Message Queuing Telemetry Transport) y COAP. Dentro de los resultados se describe un sistema de salud inteligente y de vanguardia, estableciendo mejorar a los problemas de topología fija con la que cuentan los sistemas de salud y la rapidez con la que avanzan los ciberataques (Imane et al., 2019).

MyVitalGear es un dispositivo desarrollado por Mas Azalya y Yuan Wen en el año 2018, este dispositivo trabaja con una comunicación bluetooth y una aplicación móvil. Este trabajo presenta resultados positivos en la toma de datos de signos vitales y abre la puerta a cambios que se pueden aplicar en el diseño original como implementar otros protocolos de comunicación, la reducción del tamaño del dispositivo o reducir el consumo de energía del sistema (Yusof & Hau, 2019).

El 2019 Manuel García, Nino Pilueta y Moises Jardiniano desarrollaron VITAL-APP que utiliza el protocolo de comunicación Zigbee para la adquisición y visualización de señales. El sistema fue probado en 70 pacientes hospitalizados monitorizando los signos vitales que son la temperatura corporal, el ritmo cardiaco y la saturación de oxígeno. Dentro de la investigación los resultados mostrados son la aceptación del sistema IoT en centros de salud por factores como la eficiencia, la influencia social y los beneficios; también existió un porcentaje de desconfianza por la seguridad de los datos de los pacientes (Garcia et al., 2019).

Anene Nduka y sus colegas en el año 2019 publicaron su trabajo sobre un sistema de monitoreo IoT para el sector de la salud. Todo el sistema trabaja en tiempo real y adquiere datos de temperatura corporal, la respiración y los latidos. El dispositivo presentaba variaciones de aproximadamente 0.5 en los valores medidos, por lo que los investigadores coincidieron que puede ser una opción para el monitoreo de signos vitales, pero puede ser objeto de varias mejoras (Nduka et al., 2019).

En (Garces-Salazar et al., 2021) presenta un sistema de telemedicina centrado en el hogar, con manejo de la nube y dispositivos IoT. Los niveles de BPMs y SpO2 del usuario son medidos mediante una pulsera de bajo coste y son enviados por bluetooth a una aplicación para Android TV. El sistema fue probado mediante una encuesta a 40 profesionales de la salud para valorizar el sistema, obtenido una alta aceptación como un sistema útil para el sector médico.

Con base en los trabajos relacionados con el monitoreo de signos vitales utilizando protocolos de comunicación IoT y aplicándolo en sistemas de salud, la investigación cuenta con una base teórica muy importante y varios desafíos a considerar al momento de desarrollar el artículo sobre el sistema de monitoreo de signos vitales utilizando el protocolo IoT COAP.

3. Estado del arte

En esta sección se describe todos los conceptos utilizados para la implementación del proyecto de investigación.

3.1. E-Salud

Con el despliegue de las tecnologías informáticas y de comunicaciones se abren cada vez nuevas funciones al momento de procesar, almacenar y transportar datos. Del mismo modo, las plataformas brindan infraestructura con entornos más amigables y efectivos tanto para los usuarios como para los proveedores. El concepto de e-salud representa a los dispositivos electrónicos y tecnologías de comunicación utilizadas en aplicaciones médicas, que tiene como principal objetivo el manejo de datos clínicos para una atención presencial o a distancia. Otros objetivos que se persigue con el desarrollo tecnológico dentro del campo de la salud son (Roberto J Rodrigues, 2003):

- Mejorar la productividad individual y organizacional.
- Aumentar la eficiencia de las acciones.
- Promover la eficiencia interna de las organizaciones.
- Mejorar las relaciones e intercambios con los clientes, proveedores y otros interesados.

Los productos de e-Salud se pueden utilizar en casos de prevención, diagnóstico, monitorización, emergencias, vigilancia epidemiológica, áreas de acción, consultas, juntas médicas o incluso se puede aplicar la telepresencia o la ubicación remota dependiendo del tratamiento.

3.2. IoT en e-Salud

Se encuentra actualmente dispositivos IoT en cada aspecto de la vida cotidiana, sin embargo ha tomado una fuerza peculiar dentro de la salud siendo de gran ayuda desde las intervenciones rápidas hasta la teleconsulta. Estos dispositivos se caracterizan por adquirir gran cantidad de información en tiempo real, de igual manera procesarla y generar una respuesta. Funcionan adquiriendo datos del ambiente sensores, enviando la información utilizando un protocolo de comunicación ligero, procesando los datos y finalmente presentándolos en un aplicativo.

Los servicios de salud que han sido habilitados con sistemas IoT presentan beneficios como la reducción de costos, calidad de servicio y reducción en el tiempo de detección de problemas presentados por el paciente. El sistema IoT consta de tres partes (Karthick & Pankajavalli, 2020):

Partes	Descripción
Topología	Analiza los elementos físicos que son utilizados dentro de la red como son los actuadores, sensores y equipos de comunicación. Para la elección de la topología se deben considerar varios factores en los equipos como es el costo, el consumo eléctrico, la confiabilidad y el tipo de comunicación que maneja.
Arquitectura	Esquema físico, virtual o híbrido de la red, que incluyen tanto a sensores, actuadores, plataforma de la nube, protocolos de comunicación, capas de comunicación, principios de funcionamiento y la organización del sistema.
Plataforma	Plataforma encargada de conectar a los dispositivos con las aplicaciones de la nube. Desde este punto de la red IoT se realizan las funciones como son la administración de datos, el control, monitoreo y la seguridad entre dispositivos conectados.

Tabla 1 – Partes del Sistema de red IoT (Karthick & Pankajavalli, 2020).

3.3. CoAP

El protocolo COAP fue diseñado por IETF (Internet Engineering Task Force) que trabaja con aplicaciones de comunicación máquina a máquina(M2M) y para la automatización de sistemas que reducen gastos, incluso mejorar la entrega de paquetes y aumenta la simplicidad de las interfases con HTTP. COAP es un protocolo de tipo solicitud/ respuesta soportando múltiples suscriptores de forma asincrónica proporcionando un mejor rendimiento, su uso es adecuado para entornos restringidos, dispositivos de baja capacidad y bajo consumos de energía como redes WPAN. El protocolo COAP es conocido por su sencillez y aprovecha Protocolo de Datagramas de Usuario (UDP) para las solicitudes multidifusión y unidifusión.

En una red que trabaja con protocolo CoAP se reconocen a dos tipos de dispositivos que son los clientes y los servidores. Una de las ventajas al usar el protocolo COAP es que puede existir comunicación entre todos los dispositivos de la red, sean clientes o servidores (Imane et al., 2019).

4. Caso de estudio

El caso de estudio implementado es un sistema de telemedicina IoT de monitoreo de signos vitales y alertas de distanciamiento físico, con almacenamiento en el servidor para cada usuario, utilizando protocolo IoT y dos interfaces para el manejo de los datos: Interfaz web realizada con un servidor LAMP y la segunda forma de consultar datos es mediante un bot realizado en Telegram con librerías en Python. En la figura 1 se muestra el diagrama de disposición del sistema de telemedicina IoT.

La capa de sensado se realizó en un brazalete portátil que cuenta con el microcontrolador esp-8266 para el procesamiento de datos y la comunicación con el servidor. Los sensores utilizados para el monitoreo de las señales vitales son: MLX 90614 para la temperatura corporal y MAX30100 para medir el ritmo cardiaco y la saturación de oxígeno. Estos sensores se comunican con el microcontrolador utilizando el protocolo I2C y funcionan con una alimentación de 3.3V. El suministro de energía se conforma con una batería

LiPo de 3.7 V a 650mAh y el cargador para baterías TP4056. Para monitorizar la información del brazalete se agregó una pantalla OLED de 128*64 pixeles que recibe los datos mediante la comunicación I2C.

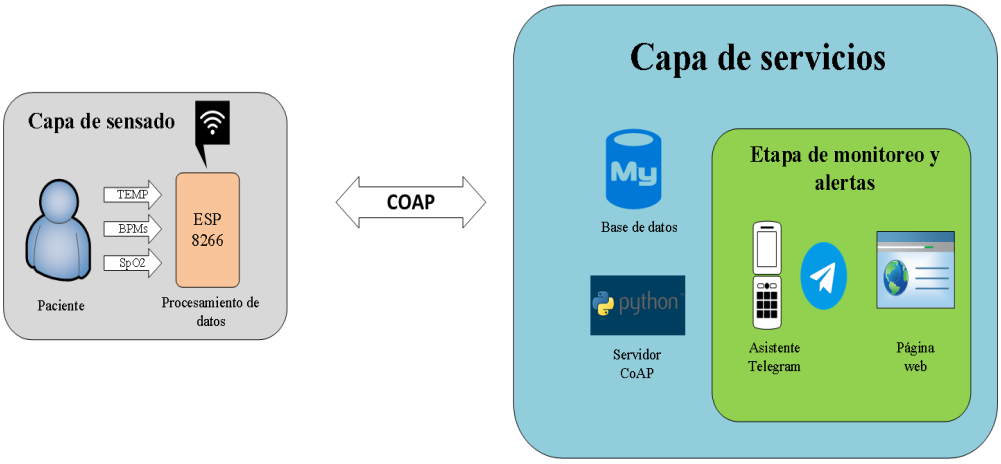


Figura 1 – Arquitectura del sistema de telemedicina IoT.

La capa de servicio consta con un servidor Ubuntu en la nube utilizando el servicio de Azure. Para el almacenamiento de la información de cada usuario se utilizó la base de datos MySQL, donde fue necesaria la creación de una base de datos relacional con 3 tablas: signos vitales, pacientes y tipo de usuario. En el servidor se encuentran alojados dos scripts de Python: a) Realiza consultas cada minuto al brazalete utilizando el protocolo CoAP y esta información adquirida es almacenada en la base de datos, b) Permite la interacción con la aplicación Telegram.

La etapa de monitoreo y alertas dispone de un sitio web compuesto por diferentes páginas: presentación de la información del dispositivo, registro de usuarios, ingreso al sistema, dashboard para el monitoreo de los signos vitales dependiendo del nivel de acceso de usuario. Además, dentro de esta etapa se encuentra el asistente virtual en la aplicación Telegram, que mediante comandos permite obtener información para manejo del asistente y realizar consultas a la base de datos sobre los signos vitales más recientes con el nombre y fecha en el cual se realizó la medida.

5. Implementación de la propuesta

5.1. Brazalete portable

Una vez seleccionado todos los componentes del brazalete portable, es necesario realizar las conexiones y probar el funcionamiento de cada elemento del circuito. En la figura 2 se presenta el diagrama de bloques con el que cuenta este dispositivo.

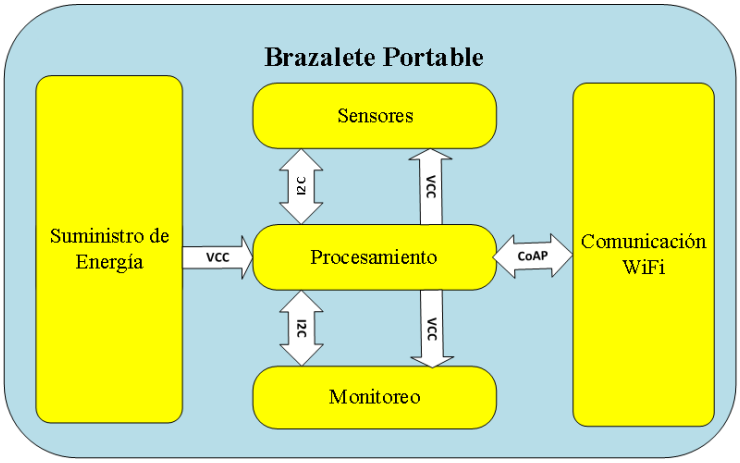


Figura 2 – Diagrama de bloques del brazalete portable.

En el funcionamiento del brazalete portable el suministro de energia es el encargado de brindar independencia al sistema durante un aproximado de 5 horas en un funcionamiento constante. El microcontrolador ESP-8266 se encarga de la recepción de datos desde los sensores y el envío de información sobre el sistema a la pantalla OLED mediante la comunicación I2C. Además, el procesador también se encarga de conectarse a Internet utilizando WiFi y enviando los datos al servidor con el protocolo CoAP.

El dispositivo también cuenta con una función de distanciamiento físico, la misma que determina de acuerdo con un indicador de potencia de la señal recibida (RSSI) dentro de una misma red tomando como referencia una señal de 1mW. Debido a la variación de intensidad de la señal que se genera, y de manera experimental con un rango de señal determinada, se verifica si los dispositivos se encuentran a una distancia aproximada de un metro. Este indicador se agregó en la programación y en la pantalla OLED de monitoreo en la parte superior junto al indicador de batería.



Figura 3 – Ubicación del sensor MAX30100 en el brazalete portable.

Una vez implementado de brazalete portable es necesario colocarlo de manera correcta bajo el pulgar a la altura de la muñeca para que los sensores realicen mediciones lo más confiables posible. En las figuras 3 se observa la ubicación del sensor MAX30100 en el brazalete y en la figura 4 se observa el brazalete colocado de manera correcta y en funcionamiento.



Figura 4 – Brazalete en funcionamiento

5.2. Capa de servicios

Dentro del servidor Ubuntu el primer paso fue estructurar la base de datos, ya que de esto depende el sistema de monitoreo con datos como ID del paciente, registro temporal, nombre, apellido y las muestras de signos vitales. Dentro de la base de datos también se define el tipo de usuario que utiliza el sistema de monitoreo, es decir, un paciente puede observar solo su información mientras que el personal de salud puede tener acceso a los datos de todos los usuarios. En la figura 5 se muestra la estructura de la base de datos en MySQL Workbench.

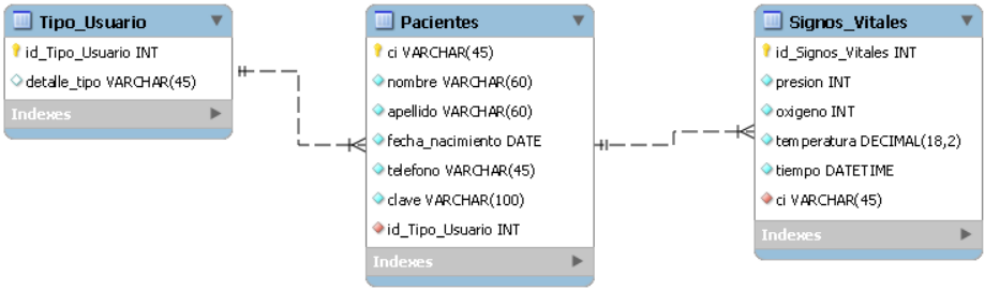


Figura 5 – Estructura de la base de datos en MySQL Workbench.

Para la transferencia de información entre el brazalete y el servidor fue necesario el desarrollo de un script en Python con librerías que permitan el uso del protocolo CoAP y la conexión con la base de datos realizada en MySQL. Dentro del código fue necesario colocar datos como la ip del brazalete, las etiquetas que representan a cada uno de los signos vitales adquiridos y la información personal del usuario. Una vez que el script obtiene todos los reportes, se establece el mismo formato y se enlaza con la base de datos para almacenarlos y utilizarlos en la etapa de monitoreo.

El sitio web se desarrolló con la ayuda de plantillas del sitio Bootstrap, que cuenta con varios diseños para el desarrollo del sitos web con diversas funciones. La plantilla seleccionada cuenta con una página de inicio netamente informativa, donde se muestra el sistema y sus beneficios, a continuación, tiene un formulario de registro para ingresar los datos del usuario o los datos del profesional de la salud. Cuenta con un control de acceso para poder ingresar a la interfaz y tener a disposición el registro de signos vitales. Para terminar con el sitio, se implementó una página con diferente despliegue de información determinada del usuario. En la figura 6 se muestra la interfaz web terminada para los dos tipos de usuario.

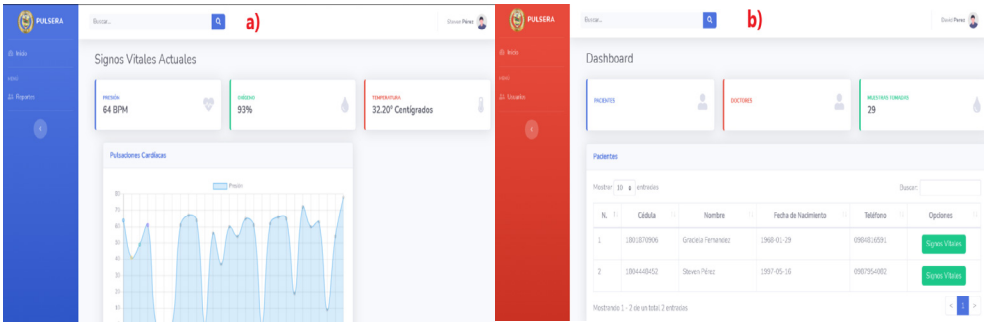


Figura 6 – a) Interfaz web para paciente. b) Interfaz web para personal de salud.

Para el bot en Telegram es necesario tener una cuenta en esta aplicación y con el uso de comandos configurar el ID, el nombre de usuario y la foto de perfil. Al crear este asistente se genera un token para acceder mediante la API HTTP y con la librería pyTelgramBotAPI en Python se programa las acciones a cargo del bot. Con ayuda de más librerías en el código de Python, el bot puede leer varios comandos, presentar información o también realizar consultas directamente a la base de datos.

El comando “/start” da la bienvenida al usuario a esta interfaz y presenta las funciones que tiene a disposición. El comando “/help” únicamente muestra un mensaje que tiene el link a la página web y para terminar el comando “/SV” que realiza consultas de los últimos signos vitales adquiridos por el brazalete con la marca temporal. En la figura 7 se muestra una interacción del bot con un usuario que realiza una consulta de sus últimos signos vitales.

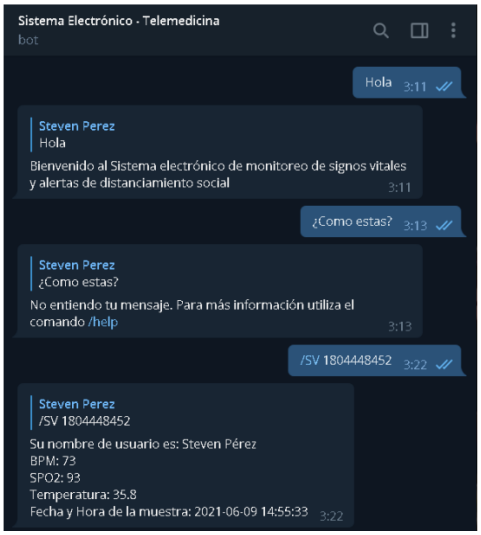


Figura 7 – Funcionamiento del bot programado en Telegram.

6. Resultados obtenidos

Para la comunicación entre el dispositivo de adquisición de signos vitales y almacenamiento de los datos se utilizó un protocolo IoT como COAP. La transmisión de datos entre el servidor y cliente representa la parte del sistema electrónico que tiene una arquitectura orientada al internet de las cosas. Con ayuda del software Wireshark se analizó el flujo en la red y se verifico el funcionamiento del protocolo con sus mensajes de confirmación cada vez que se transfiere información del cliente al servidor o viceversa. En la figura 8 se observa el flujo de datos en la red adquirido con el software Wireshark, que muestra datos como: el protocolo, fuente, destino, tiempo, longitud, payload.

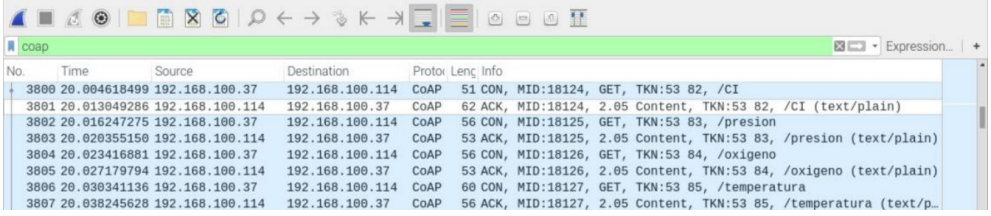


Figura 8 – Análisis del protocolo COAP con Wireshark.

La validación de los datos sobre signos vitales se desarrolló en un grupo de prueba de 20 personas entre los 25 y los 40 años de edad (10 hombres y 10 mujeres). En el análisis de la confiabilidad de datos se comparó el sistema de telemedicina IoT con dispositivos médicos comerciales utilizando los métodos gráficos lineal y Bland-Altman. En la figura

9 se muestran los resultados de la comparación entre los valores adquiridos por cada dispositivo, el gráfico de cada signo vital incluye la línea de tendencia y la ecuación de la recta que representaría el valor ideal por el cual deben pasar todos los puntos al tener medidas iguales.

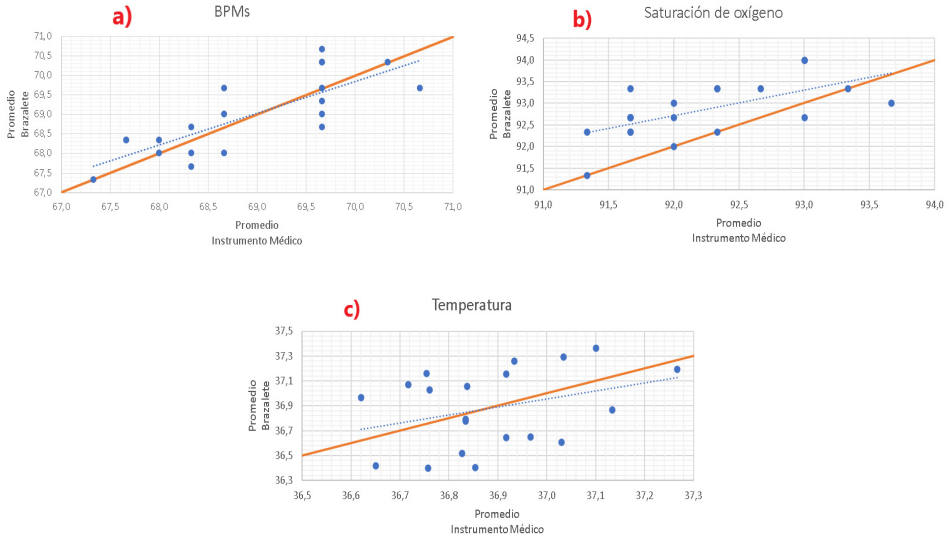


Figura 9 – Resultados de la relación entre sistema de telemedicina y dispositivos medicos comerciales: a) ritmo cardiaco, b) saturación de oxigeno y c) temperatura corporal.

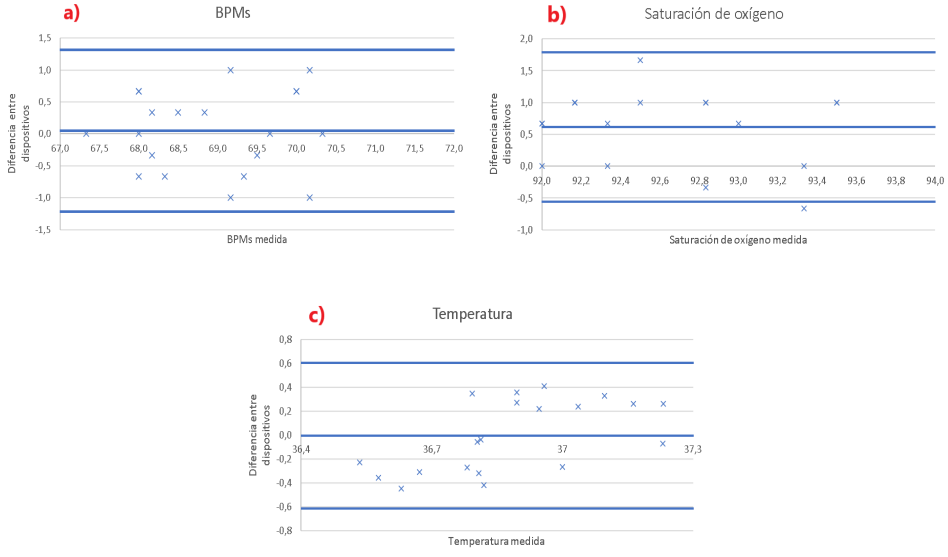


Figura 10 – Gráficos de Bland-Altman que muestran las diferencias entre medidas obtenidas de: a) ritmo cardiaco, b) saturación de oxígeno y c) temperatura corporal.

Para realizar el análisis estadístico de los datos con los pruebas obtenidas, se realizo un promedio de los valores, el error entre las mediciones y por último la desviación. Con estos datos se grafica el diagrama de Bland–Altman, que representa la diferencias entre un valor medidos con dos diferentes métodos. En la figura 10 encontramos la relación de los signos vitales medidos con el brazalete frente a los medidos por los equipos médicos comerciales, donde se puede observar que la gran mayoría de los datos no se encuentran alejados de la media.

7. Conclusiones

El sistema de telemedicina se enfocó a la comprobación de la sintomatología con la que se encuentran las personas en un espacio determinado, teniendo en cuenta valores de temperatura corporal, saturación de oxígeno y el ritmo cardiaco, signos que son controlados con mayor frecuencia en las consultas médicas para determinar síntomas de una posible enfermedad respiratoria.

El dispositivo representa una alternativa para el control de enfermedades respiratorias con la obtención de un margen de error en temperatura corporal de 0,74%, saturación de oxígeno de 0,82% y BPMs de 0,75%, rangos de errores aceptados por la Organización Panamericana de la Salud para la toma de datos en pacientes y en condiciones de movimiento.

El protocolo CoAP con arquitectura RESTful es utilizado para el intercambio de datos en las solicitudes y respuestas del dispositivo. De este modo la base de datos se actualiza de manera constante con intervalo de un minuto entre ellas y las interfaces para el control y el almacenamiento se encuentran disponibles a través de la página web o utilizando la aplicación Telegram.

Los trabajos futuros se centrarían en combinar la adquisición de datos de signos vitales con el diagnostico oportuno de enfermedades respiratorias utilizando algoritmos de inteligencia artificial.

Agradecimientos: *Los autores agradecen a la Universidad Técnica de Ambato (UTA) y a la Dirección de Investigación y Desarrollo (DIDE) por su apoyo en la realización del proyecto "Sistema electrónico de monitoreo de bioseñales y alertas de distanciamiento social para la prevención de SARS-COV2 aplicando Inteligencia Artificial".*

Referencias

Alaseel, Z., & Debnath, D. (2018). Vital Signs Monitoring System in Cloud Environment. *IEEE International Conference on Electro Information Technology*, *2018-May*, 73–78. https://doi.org/10.1109/EIT.2018.8500304

Freitas, E. D. (2021). Sistema Nacional Sanitario ecuatoriano y el COVID-19. *Scielo*, *2*, 1–7. https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/---sro-lima/documents/publication/wcms_799790.pdf

Garces-Salazar, A., Manzano, S., Nuñez, C., Pallo, J. P., Jurado, M., & Garcia, M. (2021). Plataforma IoT de bajo-coste para aplicaciones de telemedicina. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao.*, 490–499. https://doi.org/10.17013/risti.n.pi-pf

Garcia, M. B., Pilueta, N. U., & Jardiniano, M. F. (2019). VITAL APP: Development and User Acceptability of an IoT-Based Patient Monitoring Device for Synchronous Measurements of Vital Signs. *2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management, HNICEM 2019*. https://doi.org/10.1109/HNICEM48295.2019.9072724

Imane, S., Tomader, M., & Nabil, H. (2019). Comparison between CoAP and MQTT in Smart Healthcare and Some Threats. *International Symposium on Advanced Electrical and Communication Technologies, ISAECT 2018 - Proceedings*, 1–4. https://doi.org/10.1109/ISAECT.2018.8618698

Karthick, G. S., & Pankajavalli, P. B. (2020). A Review on Human Healthcare Internet of Things: A Technical Perspective. *SN Computer Science*, *1*(4), 1–19. https://doi.org/10.1007/s42979-020-00205-z

Nduka, A., Samual, J., Elango, S., Divakaran, S., Umar, U., & Senthilprabha, R. (2019). Internet of Things Based Remote Health Monitoring System Using Arduino. *Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019*, 572–576. https://doi.org/10.1109/I-SMAC47947.2019.9032438

Placencia, F., Manzano, S., Pallo, J. P., Jurado, M., & Chicaiza, D. (2017). Embedded device for blood pressure monitoring. *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2017 - Proceedings*, *2017-Janua*, 1–5. https://doi.org/10.1109/CHILECON.2017.8229505

Roberto J Rodrigues. (2003). e-Salud en Latinoamérica y el Caribe: tendencias y temas emergentes. In *Organización Panamericana de la Salud* (p. 208). http://apps.who.int/medicinedocs/documents/s16588s/s16588s.pdf

Yusof, M. A., & Hau, Y. W. (2019). Mini home-based vital sign monitor with android mobile application (myVitalGear). *2018 IEEE EMBS Conference on Biomedical Engineering and Sciences, IECBES 2018 - Proceedings*, 150–155. https://doi.org/10.1109/IECBES.2018.8626639

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 05/10/2021
Aceitação/Acceptance: 03/01/2022

Mitigação dos Riscos à Privacidade através da Anonimização de Dados

Juliano Rodrigues Ferreira[1], João Alberto Pincovscy[2], Cileno de Magalhães Ribeiro[3], Edna Dias Canedo[4], Fábio Lúcio Lopes de Mendonça[5]

juliano.ferreira@aluno.unb.br; joao.pincovscy@aluno.unb.br; cileno.ribeiro@aluno.unb.br; ednacanedo@unb.br; fabio.mendonca@redes.unb.br

1 2 3 4 5 Universidade de Brasília - UNB, Campus Universitário Darcy Ribeiro, Brasília -DF, CEP: 70910-900, Brasil

Pages: 573-585

Resumo: A Lei Geral de Proteção de Dados Pessoais (LGPD), (aprovada em 2018 no Brasil), obriga a realização da anonimização e a pseudoanonimização para dados pessoais. Diante disso, esse trabalho traz um estudo de caso de privacidade de informações, no qual, se estabelece uma proposta de mitigação dos riscos envolvidos por meio da aplicação de técnicas de anonimização. O objetivo deste trabalho foi enfatizar técnicas de anonimização possíveis, reforçando sua importância na preservação dos dados. Para tanto, foram pesquisados trabalhos nos quais suas peculiaridades na aplicação de técnicas para anonimização atingem sucesso no cumprimento da legislação. Os resultados demonstram a necessidade da seleção correta na técnica de anonimização, visando evitar a possibilidade de identificação dos registros. Como conclusão, se estabeleceu a importância de definir e implementar técnicas de anonimização para proteção de dados, possibilitando salvaguardar a privacidade de pessoas e evitar possíveis ataques de cruzamentos de informação.

Palavras-chave: Anonimização; Pseudoanonimização; Cruzamento de dados; Privacidade.

Mitigation of Privacy Risks after Data Anonymization

Abstract: The General Personal Data Protection Law (LGPD), whichpassed in 2018 in Brazil, requires anonymization and pseudo-anonymization for personal data. Therefore, this work presents a case study of information privacywhere a proposal to mitigate the risks involved is established through the application of anonymization techniques . The objective of this work is to emphasize possible anonymization techniques, reinforcing their importance in data preservation. For that, literature was researched, specifically works with where peculiarities in the application of techniques for anonymization achieve success in complying with the legislation. The results demonstrate the need for the correct selection of the anonymization technique, in order to avoid the possibility of identifying the records. In conclusion,

the importance of defining and implementing anonymization techniques for data protection was established, making it possible to safeguard people's privacy and avoid possible attacks of information crossing.

Keywords: Anonymization; Pseudoanonymization; Data crossing; Privacy.

1. Introdução

A Lei Geral de Proteção de Dados Pessoais (LGPD)(Lei nº 13.709, 2018) aprovada em 2018 e que entrou em vigor em 2020, obriga a anonimização e a pseudoanonimização para dados pessoais. A própria lei define anonimização como "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". A pseudo anonimização é definida como "o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro"(Lei nº 13.709, 2018).

Cabe ressaltar que as organizações possuem informações que desejam publicar, mas estas informações podem conter dados pessoais sensíveis (Xue et al., 2011). Em muitos países como no Brasil, Europa e Estados Unidos, os dados médicos são considerados sigilosos desde os primórdios da medicina (Hipócrates, seu patrono, que viveu na grécia por volta de 460 a.C., pregava que a relação entre paciente e médico é secreta (Scarton, [s.d.]). Assim foram desenvolvidos vários métodos e técnicas para realização da anonimização, como sistemas para busca de amostras de bases de dados para execução de pesquisas e trabalhos com a devida anonimização por cifração (Alferes et al., 2011). Utilização de *gateways* para acesso á bases de dados (Bhowmik et al., 2021), utilização da taxonomia em árvore, como método de parcelamento os dados (Rani & Rao, 2021), dentre outros. Nestes estudos os métodos de anonimização para realização de *datamining* (Mineração de Dados com preservação de Privacidade - PPDM), são basicamente de três tipos (Rani & Rao, 2021):

- Método PPDM baseado em perturbação;
- Método PPDM baseado em criptografia;
- Método PPDM baseado em anonimização.

Os métodos baseados em perturbação transformam os dados em uma forma diferente usando técnicas de distorção de dados como adição de ruído, rotação e projeção (Li et al., 2021). Os métodos baseados em criptografia, cifram total ou parcialmente os dados. E os métodos baseados em anonimização transformam os dados substituindo os dados mais específicos por dados menos específicos por generalização para fornecer privacidade (Rani & Rao, 2021). Assim, diante das discrepâncias de conceitos, podemos inferir que a LGPD trata o termo anonimização não como um método e sim como uma forma de ofuscar a informação, impossibilitando a sua associação a um indivíduo.

Toda a problemática dos métodos apresentados é o esforço computacional para modificar as bases de dados e quando necessário recuperá-la de forma íntegra, (Rhahla et al., 2021) além dos possíveis ataques de exfiltração de dados que podem ocorrer mesmo com a adoção dos métodos supracitados (Zheng & Shen, 2021)(Boenisch et al., 2021).

Sendo assim, o objetivo deste trabalho é aplicar técnicas de anonimização para validação em um estudo de caso e avaliar os riscos envolvidos nesse processo de anonimização. Para isso realizamos pesquisas sobre as principais técnicas de anonimização e pseudoanonimização; fizemos a seleção de um subconjunto de dados em uma base de dados hipotética; e aplicamos técnicas de anonimização e pseudoanonimização de dados selecionadas na base de escolhida.

Como contribuição podemos citar que a aplicação adequada de técnicas de anonimização podem resultar na efetiva proteção de dados, reduzindo os riscos associados e mantendo o potencial de utilização da informação. Buscamos ainda apresentar os riscos potenciais à privacidade de dados mesmo após a aplicação de técnicas de anonimização. A inovação reside na discussão do entendimento, inclusive preconizado pela LGPD, de que a simpls aplicação de técnicas de anonimização ou pseudoanonimização de dados seria suficiente para a proteção, porém existem riscos que devem ser considerados.

2. Definições e Trabalhos Correlatos

Nesta seção serão apresentadas as técnicas de anonimização e a aplicação em cenários especficos de utilização das bases de dados.

2.1. Definições

Segundo o Artigo 5 da LGPD/2018, define-se "Anonimização: como a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (Lei nº 13.709, 2018).

Nos órgãos públicos e privados, segundo a LGPD, é importante que se tenha uma política de governança onde seja indicada a condução do processo de anonimização de dados pessoais e sensíveis (Dias, 2022). Dessa forma, evita-se caso de quebra de privacidade com dados insuficientemente anonimizados, possibilitando que todos os campos de dados confidenciais sejam anonimizados, a fim de remover informações pessoais e reter o que for necessário para análise ou pesquisa posterior.

Pseudonimização é uma técnica de segurança para substituir dados sensíveis por dados fictícios realistas, tendo como definição: "pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (Lei nº 13.709, 2018). Destaca-se que ao manter os dados identificados em um ambiente separado, eles só se tornam identificáveis quando os dois elementos são mantidos juntos.

Anonimato ou anonimização é uma técnica que prevê o tratamento dos dados sensíveis para que sejam transformados em dados anonimizados. Assim, por definição "dados anonimizados são os dados relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento" (Cristina & Mahle, 2021). De acordo com essa definição e amparada na LGPD, o titular pode pedir a retirada de dados que possibilitem a sua identificação; os dados vão continuar armazenados, mas não vai mais ser possível identificar a quem

aqueles dados correspondem. Para que essa técnica seja eficiente, ela tem que tornar 'impossível' a identificação do titular daqueles dados (Potiguara Carvalho et al., 2020).

Vale destacar que com o avanço da tecnologia, essa técnica fica cada vez mais passível de reversão, porém a própria lei diz que o mecanismo que for usado no momento dessa anonimização tem que ser considerado razoável e disponível, logo dependente de interpretação. Com a anonimização, os dados são apagados de qualquer informação que possa servir como identificador de uma pessoa, trasnformando dados pessoais em não identificáveis. Essa definição faz com que os dados sejam despojados de qualquer identificação, tornando impossível derivar insights sobre um indivíduo (Cristina & Mahle, 2021).

Mascaramento ou Supressão é uma técnica que utiliza a disponibilização de bases de dados, com informações que não identificam os usuários, porém que pareçam ser reais. As técnicas de mascaramento de dados são: a) substituição: substituição randômica de conteúdo por informações sem relação com o dado real; b) embaralhamento (Shuffing): substituição randômica do dado real por um dado derivado da própria coluna da tabela; c) Blurring: técnica aplicada a números e datas que muda o valor do dado por uma percentagem do seu valor original; e d) Anulação/Truncagem: substitui os dados sensíveis por valor nulos (Azambuja et al., 2019). Assim, a supressão ou mascaramento de dados é uma forma extrema de anonimato. Substitui as informações por algum valor fixo de texto pré-definido (ou em alguns casos, uma tarja preta). Observa-se como vantagem a facilidade de implementar e a eficácia na remoção dos dados. Analogamente, nota-se como desvantagem a perda de qualquer valor estatístico ou analítico dos dados.

Generalização é uma técnica que condiz na substituição dos valores de atributos semi-identificadores por valores menos específicos e com semântica consistente. Assim sendo, os dados são substituídos por valores de categorias mais amplas, por exemplo: o valor 19 do campo "Idade" pode ser substituído por '≤ 20′, o valor '23' por '20 <Idade ≤ 30 ', etc. Dessa forma, percebem-se como vantagens: a possibilidade da análise de dados por categorias além dos dados permanecerem úteis para outras finalidades. Ao passo que se caracteriza como desvantagem o retorno dos dados à sua forma identificável original (Azambuja et al., 2019).

Criptografia homomórfica permite que plataformas de computação em nuvem possam realizar cálculos em dados criptografados homomorficamente sem nunca ter acesso aos dados originais. A implantação da criptografia homomórfica tem uma série de desafios porque esse sistema de criptografia ainda está em desenvolvimento. Suas restrições são baseadas principalmente em como as funções matemáticas são suportadas em dados criptografados (Neto et al., 2020).

Criptografia também é uma técnica que traduz os dados sensíveis em formato criptográfico, sendo necessária uma ou duas chaves secretas para acesso aos dados. Existem dois esquemas de criptografia de dados conhecidos: criptografia simétrica (uma chave) e criptografia assimétrica (duas chaves relacionadas) (Alexandrini & Nardelli, 2021). Em verdade, a escolha de esquemas de criptografia assimétrica, como RSA, DSA ou ECC, que usam duas chaves: pública e privada, aumentam a segurança da informação. (Štarchoň & Pikulík, 2019).

Além dessas técnicas criptográficas, temos a computação segura multipartes, que vem sendo adotada em técnicas de aprendizado de máquina que preservam privacidade; estas permitem a anonimização dos dados usados no treinamento/derivação do modelo, do próprio modelo derivado, e também da consulta (Neto et al., 2020).

Tokenization é uma técnica de abordagem não matemática para proteger dados em repouso que substitui dados sensíveis por substitutos não sensíveis. Essa técnica não altera o tipo ou comprimento dos dados, podendo ser processada por sistemas herdados, tais como bases de dados que podem ser sensíveis ao comprimento e tipo de dados, mantendo a informação sensível oculta. A título de exemplificação a tokenização pode ser usada na segurança dos pagamentos móveis, pois protege as credenciais de pagamento, substituindo-as por um número gerado aleatoriamente que se assemelha ao número de conta primária do cliente, onde apenas o banco e o processador de pagamento podem ler de volta o dado (Štarchoň & Pikulík, 2019).

2.2. Trabalhos Correlatos

As pesquisas nos Estados Unidos sobre o tema são muito úteis, pois abrangem várias situações que só depois da LGPD temos como desafio. No artigo (Gunawan et al., 2021) o autor mostra a importância da anonimização dos dados contidos em uma receita médica, pois existe a correlação direta entre o remédio vendido pelas farmácias e a doença do comprador, apresentando técnicas para ofuscar esta associação. Neste trabalho buscou-se ofuscar os dados de remédios para doenças graves. Por exemplo, na prescrição de Paracetamol não existem dados a serem ofuscados, pois, é um remédio genérico. Por outro lado, a prescrição de uma droga relacionada a problemas do coração devem ser ofuscadas. Pelas amostras estatísticas, o trabalho mostrou que a anonimização destes dados não gera uma perda substancial de dados em pesquisas estatísticas.

Outro fator a se abordado é a utilidade dos dados anonimizados, que em algumas pesquisas podem interferir nos resultados. No artigo (Prata et al., 2020), o modelo de anonimização utilizando o modelo de análise de variância com múltiplos fatores foi aplicado aos dados do Exame Nacional de Desempenho dos Estudantes de graduação no Brasil (ENADE) de 2018. Em uma primeira análise, observou-se que mesmo sendo aplicada a técnica de k-anonimização em meio milhão de registros , ainda teriam um volume muito alto de registros únicos, levando em consideração o código da área do curso, região onde funcionou o curso, idade, gênero, raça/cor e média final do estudante, os níveis de educação da Mãe e do Pai o rendimento do agregado familiar. Assim tiveram que fazer um série de iterações utilizando o Modelo k-anonimato, Modelo ℓ-diversidade e o Modelo t-proximidade para alcançar resultados estatísticos robustos com poucas distorções, trabalhando com dados anonimizados.

Entretanto, de acordo com as pesquisas realizadas, fica evidente que outros métodos de anonimização aplicados a cenários específicos similares podem resultar em sucesso. No artigo (Affonso et al., 2017), utilizou-se como exemplo um conjunto de dados com valores simulados de sujeitos envolvidos em consultas médicas. A base de dados foi estruturada a partir dos elementos da guia de consulta definida no padrão Troca de Informação da Saúde Suplementar – TISS (ANS, 2016), disponibilizada pela Agência Nacional de Saúde – ANS. Primeiramente suprimiram os atributos identificadores

únicos e a generalização dos semi-identificadores que possuem valores do tipo data; em seguida no valor do procedimento foram adicionados valores aleatórios (ruídos) por meio da distribuição normal gaussiana; após vários cálculos matemáticos e estatísticos, chegou-se à conclusão de que ao gerar um conjunto de dados modificados privados para um atributo, é possível preservar a mesma estrutura estatística dos dados originais.

Em outra abordagem, para dados disponibilizados na Internet, por vezes as técnicas de anonimização não são suficientes. No artigo (Potiguara Carvalho et al., 2020), os autores utilizaram dados de fichas financeiras de clientes como amostra inicial. Efetuaram as seguintes estratégias de anonimização: supressão, generalização, agregação, adição de ruídos e substituição. Entretanto, mesmo com a aplicação das técnicas supracitadas, com a utilização de Big Data e acesso a outras fontes de informação, como redes sociais, ainda assim seria possível a identificação de alguns registros.

Um problema observado é a utilidade dos dados após a aplicação de técnicas de anonimização. No artigo (Gunawan, 2020) o autor propôs uma anonimização de dados através do método de substituição. Resultados experimentais mostraram que o método proposto reduz com êxito a probabilidade de sucesso de ataque em um banco de dados anonimizado, ao mesmo tempo em que pode minimizar a perda de informações e preservar as propriedades do banco de dados anonimizado tão semelhante ao original. Embora o método proposto funcione bem na preservação da utilidade dos dados e manutenção das propriedades do banco de dados, deve-se observar que, pela natureza do método de substituição, ele emite distorção de informações.

Após a análise dos trabalhos publicados sobre anonimização observamos que existe um cuidado na técnica de anonimização utilizada, pois pode haver perda de qualidade de acurácia para a pesquisa na utilização dos dados ou até perda de informações importantes, que tornam a base de dados inutilizada.

3. Estudo de Caso

Conforme já contextualizado anteriormente nesse artigo, duas legislações merecem destaque: a European General Data Protection Regulation (GDPR), sendo a legislação baseada na legislação Europeia, e a LGPD, a Lei Geral de Proteção de Dados de agosto de 2018, que é a legislação brasileira a respeito da proteção de dados pessoais. As duas legislações apresentam vários aspectos em comum, em razão do objetivo final de regular a utilização e proteção de dados pessoais ser o mesmo. E merece destaque que ambas legislações apresentam a técnica de Anonimização de dados (Rhahla et al., 2021). Porém a Anonimização de dados não é livre de riscos envolvidos na sua utilização. Existem dois riscos importantes em relação a anonimização de dados, o risco de se perder a capacidade de utilização de dados e o risco de reindentificação desses dados (Canedo et al., 2021).

É importante uma análise adequada das informações armazenadas para reduzir esses riscos envolvidos, tanto no aspecto de utilização do dado como no problema de reindentificação (Piras et al., 2019). E nesse contexto ganha importância a necessidade de uma gestão adequada dessas informações, com a realização de uma governança de dados (Potiguara Carvalho et al., 2020) visando identificar adequadamente quais informações devem ser protegidas, qual técnica de anonimização aplicar e avaliar a manutenção da capacidade de utilização dessa informação.

Considerando um conjunto de informações hipotético, visando aplicação adequada das técnicas de anonimização de dados em busca da proteção dessas informações, a governança de dados preconiza que esses dados sejam analisados e classificados de acordo com suas características e potencial de associação com um indivíduo específico. Dessa maneira, as informações são classificadas em um primeiro tipo de dados que seriam os identificadores de informação pessoal e um segundo tipo de dados que seriam os dados auxiliares, aqueles que não remetem diretamente a identificação de um indivíduo.

Outro aspecto que deve ser considerado nessa classificação das informações é o volume de dados disponível na base de dados trabalhada, pois esse aspecto influencia na capacidade potencial de reindentificação e associação de dados (Carauta Ribeiro & Dias Canedo, 2020), visto que existe um aumento da capacidade inferir determinadas informações a partir de dados disponíveis. A Proteção de Dados Pessoais envolve todos aqueles papéis com interesse na informação, os controladores do dado, processadores (usuários da informação) do dado e o indivíduo a quem o dado se refere (Štarchoň & Pikulík, 2019).

Outra abordagem considerada para a proteção de dados é o uso da técnica de pseudoanonimização de dados (Štarchoň & Pikulík, 2019) sendo uma técnica estruturada na criptografia de dados. Os dados pseudoanonimizados podem ser considerados um subconjunto dos dados pessoais. Com a criptografia dos dados identificadores de informação pessoal, sendo o subconjunto de dados que identifica um indivíduo, e mantendo os dados auxiliares armazenados separadamente, somente é possível atribuir os dados a um indivíduo com informações adicionais ou com a chave criptográfica. Porém, nesse caso, é importante considerar que os dados pseudoanonimizados permitem, de alguma maneira, a reindentificação de um determinado indivíduo (Štarchoň & Pikulík, 2019).

3.1. Hipótese

A avaliação adequada das técnicas de anonimização pode ser efetiva na proteção de dados pessoais sem comprometimento da utilização das informações das bases de dados. Considerando que a seleção de técnicas de anonimização adequadas a cada tipo de dado identificado pode auxiliar no processo de proteção de dados.

3.2. Problema

Como definir quais técnicas de anonimização devem ser utilizadas e de que maneira identificar os dados a serem protegidos, buscando permitir que esses dados ainda possam ser utilizados sem comprometer a privacidade do indivíduo associado a esse dado.

Além disso, deve ser considerado os riscos envolvidos nesse processo de proteção de dados, como o risco de reindentificação das informações e perda de utilidade da informação.

3.3. Objetivo

Buscou-se demonstrar o resultado da anonimização com a possibilidade de utilização parcial das informações sem comprometimento dos dados.

Existe ainda o objetivo de se buscar o alinhamento com as diretrizes definidas nas legislações de proteção de dados.

3.4. Metodologia

Visando avaliar a aplicação de técnicas de anonimização foi selecionado um subconjunto de dados, incluindo informações pessoais para apresentação de um estudo de caso, aplicando a anonimização em dados desanonimizados como Dados de identificação pessoal, sendo aqueles que podem remeter diretamente a identidade de um indivíduo, e por essa razão devem ser protegidos conforme a legislação (Lei nº 13.709, 2018).

A Amostra de dados representada pela Figura 1 foi obtida de fonte aberta, do site da Câmara Legislativa do Brasil (Câmara dos Deputados, 2022). Tratam-se de informações pessoais de Deputados Federais, mas que estão divulgadas abertamente em razão do princípio da transparência. No cenário abordado nesse trabalho, iremos propor a anonimização de determinadas informações pessoais, porém preservando o potencial de utilização do dado (Canedo et al., 2021), ou seja, buscando permitir que a utilização de dados da base apresentada ainda seja possível mesmo com a anonimização de informações.

	id	nomeCivil	cpf	sexo	dataNascimento	ufNascimento	municipioNascimento	escolaridade	uri
1	66179	NORMA AYUB ALVES	28008901187	F	1959-09-07	ES	Vitória	Superior	https://dadosabertos.camara.leg.br/api/v2/deputados/66179
2	66828	FAUSTO RUY PINATO	28022995819	M	1977-06-01	SP	Fernandópolis	Superior	https://dadosabertos.camara.leg.br/api/v2/deputados/66828
3	67138	IRACEMA MARIA PORTELLA NUNES...	37311638372	F	1966-04-23	PI	Teresina	Superior	https://dadosabertos.camara.leg.br/api/v2/deputados/67138
4	68720	FABIO HENRIQUE SANTANA DE ...	41330200578	M	1972-06-19	SE	Simão Dias	Superior	https://dadosabertos.camara.leg.br/api/v2/deputados/68720
5	69871	JOAO CARLOS BACELAR BATISTA	10626409500	M	1957-07-09	BA	Esplanada	Mestrado	https://dadosabertos.camara.leg.br/api/v2/deputados/69871
6	72442	FELIPE AUGUSTO LYRA CARRERAS	86488023420	M	1975-04-16	PE	Recife	Superior ...	https://dadosabertos.camara.leg.br/api/v2/deputados/72442
7	73424	SIMÃO SESSIM	03441067720	M	1935-12-08	RJ	Rio de Janeiro	Superior	https://dadosabertos.camara.leg.br/api/v2/deputados/73424
8	73433	ARLINDO CHIGNALIA JUNIOR	06821146187	M	1949-12-24	SP	Serra Azul	Pós-Graduação	https://dadosabertos.camara.leg.br/api/v2/deputados/73433
9	73441	CELSO UBIRAJARA RUSSOMANNO	01252958803	M	1956-08-20	SP	São Paulo	Superior	https://dadosabertos.camara.leg.br/api/v2/deputados/73441
10	73460	GUSTAVO BONATO FRUET	64446379968	M	1963-04-18	PR	Curitiba	Superior	https://dadosabertos.camara.leg.br/api/v2/deputados/73460
11	73463	OSMAR JOSÉ SERRAGLIO	01773852949	M	1948-05-23	RS	Erechim	Mestrado	https://dadosabertos.camara.leg.br/api/v2/deputados/73463

Figura 1 – Tabela do banco de dados sem anonimização

Observando a Figura 1, verifica-se que são apresentadas de maneira transparente dados que podem ser classificados como dados pessoais, como, nome civil, CPF, sexo, data de nascimento, UF de nascimento, município de nascimento e escolaridade.

Nesse contexto cabem duas categorias de classificação para essas informações: a primeira como dados de identificação pessoal e dados auxiliares (Canedo et al., 2021), sendo que a primeira categoria remete diretamente à identificação do indivíduo e os dados auxiliares não identificam de maneira isolada o indivíduo, porém podem auxiliar nessa identificação.

Na primeira categoria de dados de identificação pessoal podem ser incluídos o Nome Civil, CPF e data de nascimento. Na segunda categoria, como dados auxiliares podem ser indicados o sexo, UF de nascimento, município de nascimento e escolaridade.

Dessa maneira uma possibilidade de anonimização dessas informações buscando proteger a privacidade dos dados pessoais, com a aplicação de técnicas de anonimização nos dados classificados como dados de identificação pessoal.

Em nosso exemplo foi utilizada a ferramenta Excel para o mascaramento, substituição e supressão de informações. Essa ferramenta foi utilizada a título de exemplo, apenas para simular a aplicação dessas técnicas, não foram utilizados algoritmos de aplicação automática dessas técnicas, mas sim a ferramenta com o objetivo de simular e demonstrar o resultado dos dados anonimizados.

ID	Nome Civil	CPF	SEXO	Data de Nascimento	Uf Nascimento	Municipio	Escolaridade
66179	NORMA AYUB ALVES	28008901187	F	07/09/1959	ES	Vitória	Superior
66828	FAUSTO RUY PINATO	28022995819	M	01/06/1977	SP	Fernandópolis	Superior
67138	IRACEMA MARIA PORTELLA NUNES NOGUEIRA LIMA	37311638372	F	23/04/1966	PI	Teresina	Superior
68720	FABIO HENRIQUE SANTANA DE CARVALHO	41330200578	M	19/06/1972	SE	Simão Dias	Superior

Figura 2 – Base de dados antes da anonimização.

3.5. Resultados

Na Figura 2 é apresentado um subconjunto de dados listados na Figura 1 a título de exemplo de como os dados são apresentados antes do processo de anonimização. Considerando os dados pessoais apresentados na figura 2 é possível selecionar técnicas de anonimização a serem utilizadas.

Para o dado pessoal denominado Nome Civil a proposta para estudo de caso é de aplicação da técnica de supressão (Canedo et al., 2021) que implica na exclusão dessa informação da base de dados. Essa técnica é uma opção quando a informação tem um grau de associação com o indivíduo muito grande e quando a informação não é necessária para a obtenção de outras informações como consolidações estatísticas.

Para o dado pessoal CPF, a proposta nesse estudo de caso é a aplicação da técnica de mascaramento, em que parte significativa das informações são mascaradas por caractere pré-definido. Essa técnica permite uma identificação parcial do registro, porém não permite a associação direta com o indivíduo.

Por último, em relação à data de nascimento, a técnica aplicada é a de substituição, que trata do embaralhamento dessas informações na base de dados, fazendo uma troca das informações na base de dados.

Assim é possível ter a utilidade das informações em relação à data de nascimento dos indivíduos cadastrados, porém sem a associação direta a identificação ou reidentificação desse indivíduo.

1	ID	CPF	SEXO	Data de Nascimento	Uf Nascimento	Municipio	Escolaridade
2	66179	XXXXXXXX187	F	23/04/1966	ES	Vitória	Superior
3	66828	XXXXXXXX819	M	19/06/1972	SP	Fernandópolis	Superior
4	67138	XXXXXXXX372	F	07/09/1959	PI	Teresina	Superior
5	68720	XXXXXXXX578	M	01/06/1977	SE	Simão Dias	Superior

Figura 3 – Base de dados anonimizada.

Observando a Figura 3, é possível verificar o resultado das aplicações das técnicas de anonimização propostas.

3.6. Discussão

O resultado permite ainda a utilidade de informações como Sexo, Data de nascimento, UF e municípios de nascimento e, ainda, escolaridade. Porém, esse processo evita a imediata identificação dos indivíduos cadastrados nessa base de dados.

Cabe, no entanto, uma observação adicional dos riscos envolvidos no processo de anonimização apresentado nesse estudo de caso, como dados auxiliares não foram anonimizados. É importante o registro da ameaça de reidentificação dos dados (Štarchoň & Pikulík, 2019) quando da associação dessas informações com outros dados obtidos em fontes abertas, como seria o caso de consulta em fonte aberta viabilizar a associação da data de nascimento, uf e do município de nascimento com a identidade do indivíduo.

4. Conclusões

Analisando a LGPD, observamos obviamente que a legislação tem grande preocupação com os dados dos indivíduos obrigando a anonimização. Entretanto, quando nos aprofundamos nas questões técnicas, nos deparamos com situações que, a princípio, atenderiam plenamente a legislação, mas diante de uma análise mais aprofundada descobrimos que a realidade não é exatamente esta.

Primeiramente, já nos deparamos com diferença de definições no que se refere ao termo anonimização, pois no meio acadêmico técnico, o termo é considerado um dos métodos utilizados para preservação de privacidade de dados. Assim, seria mais apropriado utilizar o termo "privacidade de dados" e não "anonimização".

Outra descoberta relevante em nossa pesquisa foi que existe uma vasta pesquisa em privacidade de dados, com inúmeras técnicas para a "anonimização", e quase todas realmente efetivas. Entretanto, cada técnica utilizada se adéqua a um cenário específico para ser realmente efetiva e eficiente no que se refere à utilização dos dados.

Em nosso estudo de caso ficou evidente que a utilização da bases de dados anonimizada em pesquisas controladas é extremamente útil e eficiente, atendendo com êxito a LGPD. Como utilizamos técnicas simples de ofuscação de informações, esta base anonimizada deve ser utilizada em ambientes de redes controladas. Caso fôssemos expor as informações na Internet, esta estaria sujeita à reindentificação do indivíduo efetuando o cruzamento de informações de outras fontes de dados.

Essa ameaça pode ser minimizada com aplicação de técnicas de anonimização adicionais nessas informações (Štarchoň & Pikulík, 2019), porém é importante a avaliação de cenário no caso concreto para evitar a redução significativa de utilidade do dado com a anonimização mais ampla das informações (Canedo et al., 2021).

Os ataques à "anonimização" são um fator determinante neste tema. Apesar de as pesquisas nesta área estarem avançadas, os ataques também estão cada vez mais sofisticados. Aliadas à sofisticação temos ainda as capacidades computacionais e a vastidão de fontes de dados abertas na Internet, que possibilitam cruzamentos infinitos de registros, tornando os ataques mais eficientes.

Através do estudo de caso apresentado, outros atores podem utilizar técnicas similares às apresentadas nesse estudo para avançar na abordagem de proteção de dados.

Neste trabalho não fizemos uso de técnicas de Aprendizado de Máquinas e da Inteligência Artificial. Entretanto, fica para reflexão o cenário atual onde técnicas de IA estão cada vez mais presentes na governança dos dados necessitaremos de um cuidado cada vez maior para anonimizar as informações.

Agradecimentos

Os autores agradecem o suporte da ABIN TED 08/2019, além do CNPq, CAPES e Câmara dos Deputados do Brasil pela disponibilização das bases de dados e pesquisa.

Referências

Affonso, E. P., De Oliveira, S. C., & Sant'Ana, R. C. G. (2017). Análise do equilíbrio entre privacidade e utilidade no acesso a dados. *Informacao e Sociedade*, *27*(1), 81–92. https://doi.org/10.22478/ufpb.1809-4783.2017v27n1.29422

Alexandrini, F., & Nardelli, C. (2021, dezembro). Primeira Fase da Segurança da Informação e LGPD Aplicado no Desenvolvimento de Software Governo Eletrônico. *Revista de Extensão e Iniciação Científica da UNISOCIESC*, 20. https://doi.org/10.13140/RG.2.2.30059.46883

Azambuja, A. J. G. de, Granville, L. Z., & Sarmento, A. G. M. (2019). A privacidade, a segurança da informação e a proteção de dados no Big Data. *Parcerias Estratégicas*, 9–32. https://tinyurl.com/26vwz3cx

Bhowmik, C., Momin, M. A. I., Shanta, F. J., & Haque, M. M. (2021). Database Security as a Gateway to Privacy Preserving Data Mining. *International Conference on Robotics, Electrical and Signal Processing Techniques*, 125–130. https://doi.org/10.1109/ICREST51555.2021.9331190

Boenisch, F., Munz, R., Tiepelt, M., Hanisch, S., Kuhn, C., & Francis, P. (2021). Side-Channel Attacks on Query-Based Data Anonymization. In *Proceedings of the ACM Conference on Computer and Communications Security* (Vol. 1, Número 1). Association for Computing Machinery. https://doi.org/10.1145/3460120.3484751

Câmara dos Deputados. (2022). *Dados Abertos da Câmara dos Deputados*. https://dadosabertos.camara.leg.br/

Canedo, E., Cerqueira, A., Gravina, R., Ribeiro, V., Camões, R., Reis, V., Mendonça, F., & Sousa Jr., R. (2021). *Proposal of an Implementation Process for the Brazilian General Data Protection Law (LGPD)*. 19–30. https://doi.org/10.5220/0010398200190030

Carauta Ribeiro, R., & Dias Canedo, E. (2020). Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security. *The 21st Annual International Conference on Digital Government Research*, 175–184. https://doi.org/10.1145/3396956.3398252

Cristina, A., & Mahle, O. (2021). *A Autodeterminação Informativa como Fundamento da Lei Geral de Proteção de Dados Brasileira: Uma Análise a Partir da LGPD* [Universidade Federal de São Carlos]. https://repositorio.ufscar.br/bitstream/handle/ufscar/15630/Ana Cristina Oliveira Mahle essa.pdf?sequence=1&isAllowed=y

Dias, S. P. (2022). *Autonomia Heteronoma e Discriminação Algorítmica: Análise do piso normativo para admissão do tratamento discriminatório de dados pessoais do titular* [Universidade Federal de Ouro Preto]. http://shorturl.at/qvKTW

Gunawan, D. (2020). A Data Anonymization Method to Mitigate Identity Attack in Transactional Database Publishing. *2020 8th International Conference on Information and Communication Technology, ICoICT 2020*. https://doi.org/10.1109/ICoICT49345.2020.9166262

Gunawan, D., Nugroho, Y. S., Maryam, & Al Irsyadi, F. Y. (2021). Anonymizing Prescription Data against Individual Privacy Breach in Healthcare Database. *2021 9th International Conference on Information and Communication Technology, ICoICT 2021*, 138–143. https://doi.org/10.1109/ICoICT52021.2021.9527430

José Alferes, D., Miguel Goulão, D., José Alberto Cardoso Cunha Arguente, D., Vitor Manuel Beires Pinto Nogueira Vogal, D., & José Júlio Alves Alferes, D. (2011). *Building Anonymised Database Samples Dissertação para obtenção do Grau de Mestre em Engenharia Informática*. Universidade Nova de Lisboa.

Lei nº 13.709, de 14 de A. de 2018. (2018). *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Legislação Brasileira. http://shorturl.at/tzCW9

Li, J., Han, L., Chen, R., Zhang, H., Han, B., Wang, L., & Cao, X. (2021). Identity-Preserving Face Anonymization via Adaptively Facial Attributes Obfuscation. *MM 2021 - Proceedings of the 29th ACM International Conference on Multimedia*, 3891–3899. https://doi.org/10.1145/3474085.3475367

Neto, H. N. C., Mattos, D. M. F., & Fernandes, N. C. (2020). Privacidade do Usuário em Aprendizado Colaborativo: Federated Learning, da Teoria à Prática. In E. Viefas (Org.), *Minicursos do SBSeg* (p. 101-). Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. https://www.lgpdbrasil.com.br/.

Piras, L., Al-Obeidallah, M. G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., Bernard, J. B., Fiorani, M., Magkos, E., Sanz, A. C., Pavlidis, M., D'Addario, R., & Zorzino, G. G. (2019). DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11711 LNCS*, 78–93. https://doi.org/10.1007/978-3-030-27813-7_6

Potiguara Carvalho, A., Potiguara Carvalho, F., Dias Canedo, E., & Potiguara Carvalho, P. H. (2020). Big data, anonymisation and governance to personal data protection. *ACM International Conference Proceeding Series*, 185–195. https://doi.org/10.1145/3396956.3398253

Prata, P., Ferrão, M. E., Santos, W., & Sousa, G. (2020). Privacy preserving versus utility preserving in data anonymization: A study in higher education. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2020*(E40), 112–127. https://doi.org/10.17013/RISTI.40.112-127

Rani, V. U., & Rao, M. S. (2021). PrivGuard: Sensitivity Guided Anonymization based PPDM with Automatic Selection of Sensitive Attributes. *2021 7th International Conference on Advanced Computing and Communication Systems, ICACCS 2021*, 1832–1837. https://doi.org/10.1109/ICACCS51430.2021.9441991

Rhahla, M., Allegue, S., & Abdellatif, T. (2021). Guidelines for GDPR compliance in Big Data systems. *Journal of Information Security and Applications*, *61*(June), 102896. https://doi.org/10.1016/j.jisa.2021.102896

Scarton, R. R. ([s.d.]). *Violação do Segredo Profissional Dos Médicos: Aspectos Jurídicos e (Bio)Éticos - Âmbito Jurídico - Educação jurídica gratuita e de qualidade*. Recuperado 31 de maio de 2022, de http://shorturl.at/eCLN1

Štarchoň, P., & Pikulík, T. (2019). GDPR principles in Data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones. *Procedia Computer Science*, *151*, 303–312. https://doi.org/10.1016/J.PROCS.2019.04.043

Xue, M., Karras, P., Raïssi, C., & Pung, H. K. (2011). Utility-driven anonymization in data publishing. *International Conference on Information and Knowledge Management, Proceedings*, 2277–2280. https://doi.org/10.1145/2063576.2063945

Zheng, J., & Shen, X. (2021). Pattern mining and detection of malicious sql queries on anonymization mechanism. *IEEE Access*, *9*, 15015–15027. https://doi.org/10.1109/ACCESS.2021.3052956

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 20/12/2021
Aceitação/Acceptance: 26/02/2022

Modelos analíticos para identificar patrones de delitos financieros: Una revisión sistemática de la literatura

Maritza Murillo Ortíz[1], Lillyana María Giraldo Marín[2], Herman Horacio Jaramillo Villegas[3], Carlos César Piedrahita Escobar[4]

mary_m220@hotmail.com; lmgiraldo@udemedellin.edu.co; hjaramillo@udemedellin.edu.co; cpiedrahita@udemedellin.edu.co

[1] Estudiante Maestría en Modelación y Ciencia Computacional, Universidad de Medellín, Antioquia, Colombia

[2] Profesor titular, Facultad de Ingenierías, Universidad de Medellín, Antioquia, Colombia

[3] Profesor, Facultad de Ciencias Básicas, Universidad de Medellín, Antioquia, Colombia

[4] Profesor, Facultad de Ciencias Básicas, Universidad de Medellín, Antioquia, Colombia

Pages: 586-598

Resumen: Uno de los más grandes retos a los que se enfrentan hoy en día las instituciones financieras es al riesgo de delitos financieros que son cada vez más sofisticados y de naturaleza global, considerando las tendencias en aumento de algunos tipos de modalidades cada vez más usadas. Por tal motivo, se desarrolló una revisión sistemática de la literatura alrededor del tema para saber qué modelos analíticos son lo más usados y han logrado detectar situaciones anómalas. De esta revisión se identificó que de la mano de la tecnología y de modelos analíticos supervisados como *Support Vector Machine (SVM)*, Redes Neuronales, entre otros, se pueden mitigar de forma considerable muchas de las amenazas que existen hoy en el mercado y así lograr impedir pérdidas millonarias, sin embargo, es importante según la literatura, tener en cuenta que una de las principales dificultades para detectar el fraude o cualquier otro delito financiero son los datos desequilibrados, ya que esto implica que probablemente los resultados generados muestren un sesgo hacia la clase mayoritaria y en casos extremos pueden ignorar por completo la clase minoritaria.

Palabras-clave: Delitos financieros, *Machine Learning*, modelos analíticos

Analytical models to identify financial crime patterns: a systematic literature review

Abstract: One of the greatest challenges facing financial institutions today is the risk of financial crimes that are increasingly sophisticated and global in nature, considering the increasing trends of some types of modalities. For this reason, a systematic literature review on the subject was developed to find out which analytical

models are the most used and we managed to detect anomalous situations. From this review, it was identified that, thanks to technology and supervised analytical models such as Support Vector Machine (SVM), Neural Networks, among others, many of the threats that exist in the market today can be considerably mitigated and in this way, it is important to prevent million-dollar losses, however, according to the literature, it is important to take into account that one of the main difficulties in detecting fraud or any other financial crime is unbalanced data, since this implies that the results generated probably show a bias towards the majority class and, in extreme cases, may completely ignore the minority class.

Keywords: Financial crimes, Machine Learning, analytical models

1. Introducción

El mundo vive hoy un período de cambio tecnológico, geopolítico y socioeconómico sin precedentes. Para la industria de servicios financieros, este entorno crea una gran oportunidad para proporcionar servicios más rápidos, seguros y asequibles a poblaciones más grandes y diversas, pero también crea riesgos de delitos financieros que son cada vez más sofisticados y de naturaleza global (Asobancaria, 2020).

La delincuencia financiera abarca desde el robo o el fraude cometido por individuos malintencionados, hasta operaciones a gran escala planeadas por grupos de delincuencia organizada presentes en todos los continentes. Se trata de actividades delictivas graves cuya importancia no debería minimizarse pues, más allá del impacto social y económico, por lo general están estrechamente vinculadas con la delincuencia violenta e incluso el terrorismo (INTERPOL, 2021).

Con la digitalización y el crecimiento del uso de canales virtuales para todo tipo de actividades, incluyendo las relacionadas con el sector financiero, la inversión en la lucha contra delitos financieros en Colombia creció 20% a US$180 millones durante 2020, comparado con US$150 millones en 2019. Según un estudio de la compañía global de datos y análisis LexisNexis Risk Solutions, durante el 2020 en el mundo se destinaron US$213.900 millones a este tipo de prevención, superando los US$ 1 8 0 . 9 0 0 millones registrados en 2019. Entre los crímenes financieros que se destacan en América Latina se encuentran el lavado de dinero, la financiación terrorista y el soborno. Los sectores que más se han visto impactados por este tipo de prácticas delictivas han sido el sector de empresas especializadas en la comercialización masiva de productos o servicios; el *e-commerce*; los bienes raíces; los servicios profesionales, como derecho o contaduría; los medios de comunicación y juegos de azar (República, 2021).

La digitalización del mundo, la importancia de los datos, la anonimidad del internet, entre otros factores, han causado una constante evolución en la forma en la que los delincuentes cometen sus fraudes. Estos han desarrollado nuevas y más eficientes formas de cometer ilícitos, en las que la exposición al riesgo de ser capturado es menor y la probabilidad de éxito mayor. Como consecuencia, las empresas del mundo están siendo cada vez más conscientes de los riesgos de robo de información o recursos a los que están expuestos, y de la inminente posibilidad de ser víctima de algún fraude que afecte a la compañía y sus clientes (Asobancaria, 2020).

Las instituciones financieras deben garantizar la implementación continua de un conjunto completo de medidas para minimizar los riesgos de transacciones ilegales, incluido el uso de herramientas automatizadas de recopilación y análisis de datos. La implementación de algoritmos de aprendizaje automático efectivos, diseñados para detectar operaciones anómalas, puede reducir los riesgos de delitos financieros (Baesens, Höppner, & Verdonck, 2021).

Por lo anterior, en este trabajo se realizó una revisión sistemática de la literatura (RSL) alrededor del tema, buscando responder las siguientes preguntas:

PI01. ¿Qué modelos analíticos son más utilizados para la identificación de patrones de delitos financieros?

PI02. ¿Cuáles tipos de software son los más usados para la identificación de patrones de delitos financieros?

PI03. ¿Cuáles son las métricas de evaluación más utilizadas para verificar el rendimiento de los modelos usados para identificar delitos financieros?

PI04. ¿Cuáles son los desafíos investigativos en la implementación de modelos analíticos para la identificación de patrones de delitos financieros?

El documento presenta la revisión de literatura e incluye el apartado de la metodología, en el cual se detalla la búsqueda de información y se caracterizan los documentos encontrados. Adicionalmente se presentan las conclusiones y referencias utilizadas.

Se espera que este trabajo ayude a guiar futuras investigaciones en el tema y sea un insumo importante frente a la lucha contra los delitos financieros.

2. Metodología

La metodología de RSL utilizada en este trabajo es la propuesta inicialmente por el autor Jorge Iván Pérez Rave en su publicación (Pérez, 2012) y mejorada posteriormente en su publicación (Pérez, 2019). Para dar respuesta a las preguntas planteadas se realizó una búsqueda en la base de datos Scopus usando la siguiente combinación de términos:

((TITLE-ABS-KEY (“financial crimes” OR fraud OR “money laundering”))

AND (TITLE-ABS-KEY (“data mining” OR “machine learning” OR “statistics”)))

La búsqueda se realizó en marzo de 2022 y arrojó un total de 3900 publicaciones. Luego se limitaron los resultados a las publicaciones escritas en inglés y español, también a que sólo fueran artículos publicados en los últimos seis años (2016 - 2022) y que tuvieran libre acceso, obteniendo finalmente un total de 717 artículos.

Posteriormente, para seleccionar cuáles de estas publicaciones se usarían en la revisión, se realizó un análisis de relevancia de los artículos “espacio literario relevante” el cual permite identificar el número de artículos que representan la mayor proporción de citaciones relevantes, mostrado en la Figura 1. La totalidad de artículos encontrados en la búsqueda fue de 717, pero para la construcción del espacio literario relevante, se eliminaron aquellos artículos que no tuvieran ninguna citación, quedando en total 494

artículos. Del diagrama, se concluye que el 25.1% (126 artículos) de éstos constituyen lo "poco vital" al sumar entre ellos el 80% del total de citaciones.

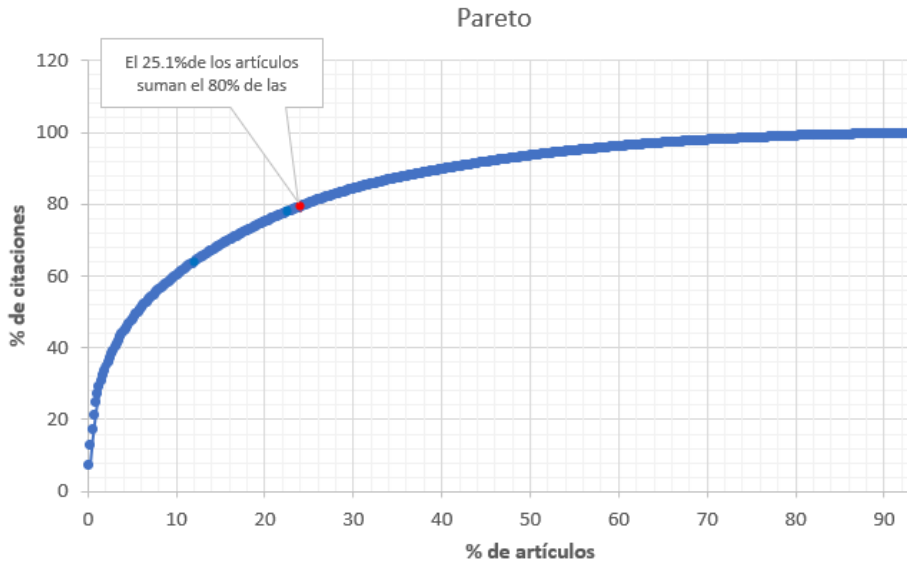


Figura 1 – Diagrama de Pareto para los artículos encontrados.
Fuente: Elaboración propia a partir de la metodología de RSL propuesta por Pérez-Rave.

Finalmente, se pasó a leer el resumen de los 126 artículos priorizados con el Pareto. Se consideró como factor importante para la selección de los artículos, que el resumen de estos estuviera relacionado de manera directa con el tema de estudio y a los que se lograra tener acceso, seleccionando finalmente 30 artículos para la revisión, los cuales se listan en la Tabla 1:

ID	Título	Autor	Año	Citaciones
1	A survey of predictive modeling on imbalanced domains	Branco P., Torgo L., Ribeiro R.P.	2016	347
2	A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data	Goldstein, M., & Uchida	2016	306
3	REV2: Fraudulent user prediction in Rating platforms	Kumar S., Kumar M., Hooi B., Faloutsos C., Makhija D., Subrahmanian V.S.	2018	107
4	Credit card fraud detection: A realistic modeling and a novel learning strategy	Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi	2018	105
5	Credit Card Fraud Detection Using AdaBoost and Majority Voting	Randhawa, K., Loo, C. K., Seera	2018	90

ID	Título	Autor	Año	Citaciones
6	Using social network analysis to prevent money laundering	Fronzetti Colladon, A., & Remondi	2017	73
7	SCARFF: A scalable framework for streaming credit card fraud detection with spark	Carcillo, F., Dal Pozzolo	2018	65
8	BIRDNEST: Bayesian inference for ratings-fraud detection	Hooi B., Shah N., Beutel A., Günnemann S., Akoglu L., Kumar M., Makhija D., Faloutsos C.	2016	55
9	A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks	Alauthaman M., Aslam N., Zhang L., Alasem R., Hossain M.A.	2018	51
10	Behavior monitoring methods for trade-based money laundering integrating macro and micro prudential regulation: A case from China	Chao, X., Kou, G., Peng	2019	44
11	A cluster-based boosting algorithm for bankruptcy prediction in a highly imbalanced dataset	Le, T., Hoang Son, L., Vo, M., Lee	2018	41
12	Auto insurance fraud detection using unsupervised spectral ranking for anomaly	Nian, K., Zhang, H., Tayal	2016	40
13	Recent Progress of Anomaly Detection	Xu X., Liu H., Yao M.	2019	36
14	CoDetect: Financial Fraud Detection with Anomaly Feature Detection	Huang, D., Mu, D., Yang	2018	35
15	An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection	Makki, S., Assaghir, Z., Taher	2019	23
16	An effective financial statements fraud detection model for the sustainable development of financial markets: Evidence from Taiwan	Jan, C	2018	22
17	Comparison of Data Mining Classification Algorithms Determining the Default Risk	Çığşar, B., & Ünal	2019	21
18	RCLens: Interactive Rare Category Exploration and Identification	Lin, H., Gao, S., Gotz, D., Du, F., He, J., & Cao	2018	20
19	Anomaly detection in wide area network meshes using two machine learning algorithms	Zhang, J., Gardner, R., & Vukotic	2019	20
20	Kernel density estimation based sampling for imbalanced class distribution	Kamalov	2020	19

ID	Título	Autor	Año	Citaciones
21	Combining unsupervised and supervised learning in credit card fraud detection	Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi	2021	18
22	HiDDen: Hierarchical dense subgraph detection with application to financial fraud detection	Zhang S., Zhou D., Yildirim M.Y., Alcorn S., He J., Davulcu H., Tong H.	2017	16
23	An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine	Taha, A. A., & Malebary	2020	14
24	A state of the art survey of data mining-based fraud detection and credit scoring	Zhou X., Cheng S., Zhu M., Guo C., Zhou S., Xu P., Xue Z., Zhang W.	2018	13
25	Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective	Canhoto A.I.	2021	12
26	Multiple perspectives HMM-based feature engineering for credit card fraud detection	Lucas Y., Calabretto S., Portier P.-E., Caelen O., Granitzer M., Laporte L., He-Guelton L.	2019	12
27	Detection of violations in Credit Cards of Banks and financial institutions based on Artificial neural network and Metaheuristic optimization algorithm	Monirzadeh, Z., Habibzadeh, M., Farajian, N.	2018	3
28	robROSE: A robust approach for dealing with imbalanced data in fraud detection	Baesens, B., Höppner, S., Ortner, I., & Verdonck	2021	1
29	Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection	Itoo, F., Meenakshi, & Singh	2021	1
30	Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks	Benchaji, I., Faculty of Sciences IPSS, University Mohammed V, Rabat, Morocco, Douzi, S., & Ouahidi	2021	1

Tabla 1 – Selección de artículos. Fuente: elaboración propia

3. Resultados de la RSL

Se realizó una lectura completa de cada uno de los artículos seleccionados en la Tabla 1 y tras su lectura, se hizo una ficha técnica por cada artículo revisado. Después se realizó una tabla de características de cada artículo, donde el objetivo era verificar las respuestas

que cada artículo analizado daba a las preguntas realizadas. Por último, se realizó un análisis de la tabla de características en conjunto, es decir, un análisis desde cómo los diferentes artículos seleccionados daban respuesta a las preguntas, con el objetivo de identificar patrones o respuestas comunes.

3.1. Hallazgos

Para dar respuesta a las diferentes preguntas de RSL se utiliza la Tabla 1 y sus ID.

PI01: ¿Qué modelos analíticos son más utilizados para la identificación de patrones de delitos financieros?

Si bien, la literatura presenta de manera ampliada la aplicación de diversos modelos analíticos para la identificación de patrones de delitos financieros, los modelos más relevantes son el *SVM* presentándose en el 23% [2,5,6,12,17,25,27] de los artículos revisados, seguido por *Random Forest* [4,7,9,26] y Redes Neuronales [4,15,16,9] cada uno con un 13% de los artículos, , a continuación el Análisis de Red [3,6,14], *K-Nearest Neighbor* (*KNN)* [2,20,3], *Adaboost* [5,11,19] y *Naive Bayes* (NB) [10,15,8] con la misma frecuencia de aparición cada uno (10%), finalmente, con menor frecuencia, pero igualmente efectivos según los autores, se encuentran el Aprendizaje Activo [18], *Cboost* [11], Regresión Logística [17] y Valores Atípicos [21] cada uno con una frecuencia de 3%. En la Figura 3 se muestran los modelos analíticos más usados para la identificación de patrones de delitos financieros, acorde a los artículos revisados en esta RSL:

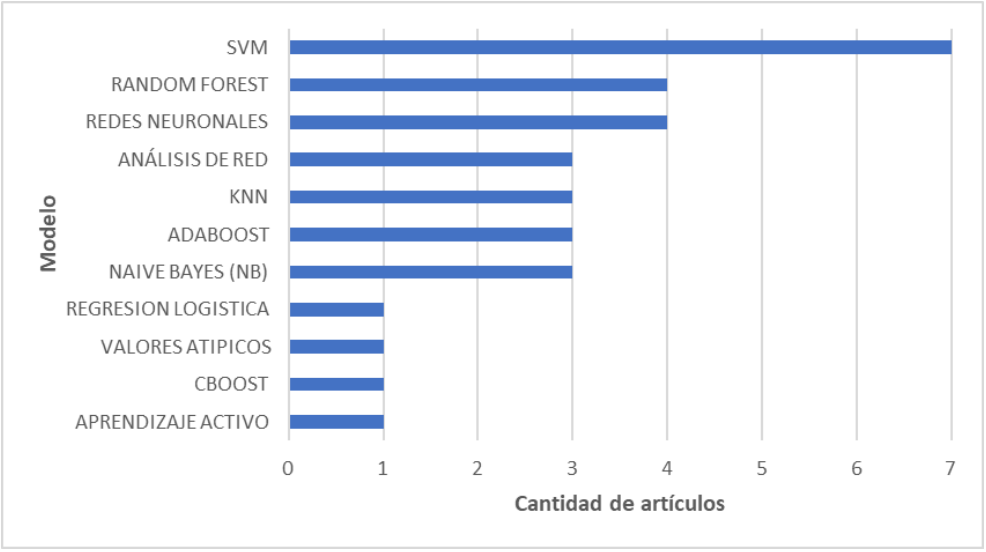


Figura 2 – Modelos más utilizados para la identificación de patrones de delitos financieros.
Fuente: Elaboración propia

PI02: ¿Cuáles tipos de software son los más usados para la identificación de patrones de delitos financieros?

De los artículos analizados, se encontraron software y lenguajes de programación en los que fueron implementados los modelos o técnicas analíticas con el propósito de identificar patrones de delitos financieros, en tres de los artículos [1,15,20] usaron el lenguaje de programación R, en el cual se puede implementar los algoritmos o modelos analíticos alrededor del tema, seguido de *MATLAB* con 2 artículos [9,27] el cual es una herramienta que permite desarrollar modelos de técnicas de aprendizaje automático a la medida y permite la repetición, mantenimiento, y reutilización rápida a través de la automatización. También hacen mención a otros software como *WEKA* [17], *PerfSonar* [19], *IBM SPSS Modeler* [16] y el lenguaje de programación Python [11].

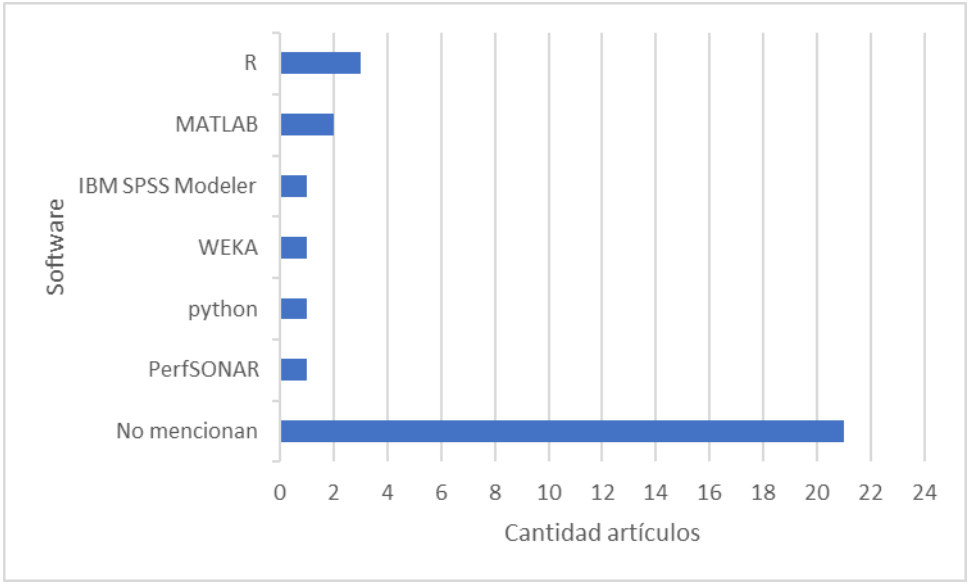


Figura 3 – Software usados para identificación de delitos financieros.
Fuente: elaboración propia

PI03: ¿Cuáles son las métricas de evaluación más utilizadas para verificar el rendimiento de los modelos usados para identificar delitos financieros?

El indicador *"Area Under the Curve"* (AUC) es el área bajo la curva *"Receiver Operating Characteristic"* (ROC) y es la métrica de medición más utilizada para validar el rendimiento de los modelos que logren identificar patrones de delitos financieros. De acuerdo con la RSL realizada, en 10 de los artículos analizados [2,4,10,11,14,15,19,21,24,26] mencionan esta métrica. Seguido se encuentra la Validación Cruzada [16,9,22,25] con 4 artículos, la Precisión con 3 artículos [4,15,17], luego el Criterio de Información Bayesiano (BIC) con 2 artículos [6,26] y finalmente existen otras métricas utilizadas por los autores en donde son mencionadas cada una en un artículo, Accuracy [5], Media F [17], G-Mean [20], Akaike [10]. En 7 artículos de la RSL no se logra identificar cuál métrica fue la utilizada.

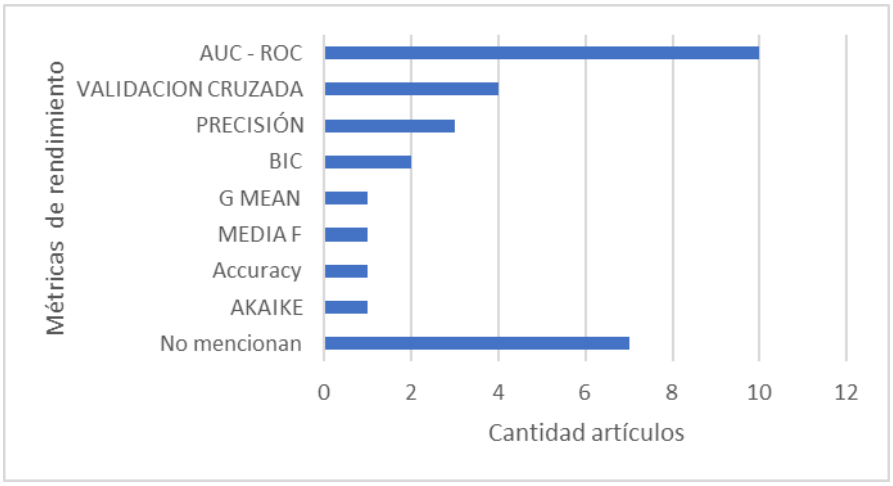


Figura 4 – Métricas de rendimiento. Fuente: elaboración propia

PI04: ¿Cuáles son los desafíos investigativos en la implementación de modelos analíticos para la identificación de patrones de delitos financieros?

De la RSL realizada, se identificó que el desempeño de un modelo que logre identificar patrones de delitos financieros no sólo depende del modelo analítico aplicado, sino que también es importante considerar durante el aprendizaje de estos posibles patrones, factores como el desequilibrio de las clases[1], lo cual es uno de los desafíos en la mayoría de los artículos [1,2,4,7,15,18,30]. También hacen mención en [4,9] de la dinámica del fraude, lo cual hace que las entidades financieras se vean enfrentadas a nuevos retos para la detección tanto de fraudes como para cualquier otro delito financiero, en [12,25] hacen referencia a que, obtener etiquetas, es muy costoso y finalmente en [13] mencionan que tener datos con alta dimensionalidad es un desafío en la implementación de modelos analíticos para identificar fraude.

4. Conclusiones

La industria de servicios financieros tiene una gran oportunidad para proporcionar servicios más rápidos, seguros y asequibles a poblaciones más grandes y diversas, pero también presenta nuevos riesgos de delitos financieros que son cada vez más sofisticados y de naturaleza global. Sin embargo, de la mano de la tecnología y de soluciones analíticas se puede mitigar de forma considerable muchas de estas amenazas.

Con base en la RSL, se identificó cuáles son los modelos analíticos más usados para la detección de delitos financieros, encontrando modelos de clasificación como las Máquinas de Soporte Vectorial (SVM), Árboles Aleatorios (*Random Forest)* y las Redes Neuronales,

[1] El número de registros para una de las clases es inferior al resto, en este caso, son menos los casos con delitos financieros a los que no lo son.

son los tres más utilizados para abordar este tipo de problemática. El algoritmo *Random Forest,* de acuerdo a los autores, presenta resultados muy competitivos dentro de los demás modelos de clasificación, siendo sencillo, rápido y fácilmente paralelizable.

Aunque dentro de la revisión, la mayoría de los autores (Makki et al, 2019; Lin et aI, 2018) coincidían en que el desequilibrio de clase alta es naturalmente inherente para la problemática de nuestro interés que es detectar delitos financieros, como por ejemplo el fraude o lavado de activos, esto se ha convertido en un desafío ya que los datos altamente desequilibrados implican que muy probablemente los resultados generados muestren un sesgo hacia la clase mayoritaria y en casos extremos pueden ignorar por completo la clase minoritaria, la cual es precisamente la de nuestro interés. Respecto a este desafío de desequilibrio de clases, es conveniente estudiarlo con mayor profundidad, pues existen investigaciones que se centran específicamente en este tema.

Dentro de los modelos analíticos analizados en la revisión sistemática, muchos de los algoritmos usados los cuales se basan en inteligencia artificial, fueron implementados en diversos software o lenguajes de programación como *Matlab, IBM SPSS Modeler, PerfSONAR, Python, R y Weka*, los cuales se adaptan con facilidad a la necesidad de identificación de delitos financieros.

Finalmente, respecto a los modelos analíticos mencionados, también fue de nuestro interés conocer cuáles son las métricas de evaluación más utilizadas para verificar el rendimiento de los modelos, encontrando que el *AUC* es la métrica con la que se evaluaron la mayoría de los modelos de las publicaciones revisadas.

Referencias

Alauthaman, M., Aslam, N., Zhang, L., Alasem, R., & Hossain, M. A. (2018). A P2P botnet detection scheme based on decision tree and adaptive multilayer neural networks. Neural Computing and Applications, 29(11), 991-1004. doi:10.1007/s00521-016-2564-5

Asobancaria. (26 de 5 de 2020). Asobancaria. Obtenido de https://www.asobancaria.com/wp-content/uploads/1234VF.pdf

Baesens, B., Höppner, S., Ortner, I., & Verdonck, T. (2021). robROSE: A robust approach for dealing with imbalanced data in fraud detection. Statistical Methods & Applications, 30(3), 841–861. https://doi.org/10.1007/s10260-021-00573-7

Benchaji, I., Faculty of Sciences IPSS, University Mohammed V, Rabat, Morocco, Douzi, S., & Ouahidi, B. E. (2021). Credit card fraud detection model based on LSTM recurrent neural networks. Journal of advances in information technology, 12(2), 113–118.

Branco, P., Torgo, L., & Ribeiro, R. P. (2016). A survey of predictive modeling on imbalanced domains. ACM Computing Surveys, 49(2) doi:10.1145/2907070

Canhoto, A. I. (2021). Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. Journal of Business Research, 131, 441-452. doi: 10.1016/j.jbusres.2020.10.012

Carcillo, F., Dal Pozzolo, A., Le Borgne, Y.-A., Caelen, O., Mazzer, Y., & Bontempi, G. (2018). SCARFF: A scalable framework for streaming credit card fraud detection with spark. An international journal on information fusion, 41, 182–194.

Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. Information Sciences, 557, 317–331.

Chao, X., Kou, G., Peng, Y., & Alsaadi, F. E. (2019). Behavior monitoring methods for trade-based Money Laundering integrating macro and micro prudential regulation: A case from China. Technological and economic development of economy, 25(6), 1081–1096.

Çığşar, B., & Ünal, D. (2019). Comparison of data mining classification algorithms determining the default risk. Scientific Programming, 2019, 1–8.

Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8), 3784–3797.

Fronzetti Colladon, A., & Remondi, E. (2017). Using social network analysis to prevent money laundering. Expert Systems with Applications, 67, 49–58.

Goldstein, M., & Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PloS One, 11(4), e0152173.

Hooi, B., Shah, N., Beutel, A., Günnemann, S., Akoglu, L., Kumar, M., . . . Faloutsos, C. (2016). BIRDNEST: Bayesian inference for ratings-fraud detection. Paper presented at the 16th SIAM International Conference on Data Mining 2016, SDM 2016, 495-503. doi:10.1137/1.9781611974348.56 Retrieved from www.scopus.com

Huang, D., Mu, D., Yang, L., & Cai, X. (2018). CoDetect: Financial fraud detection with anomaly feature detection. IEEE access: practical innovations, open solutions, 6, 19161–19174.

Itoo, F., Meenakshi, & Singh, S. (2021). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. International Journal of Information Technology, 13(4), 1503–1511.

Jan, C.-L. (2018). An effective financial statements fraud detection model for the sustainable development of financial markets: Evidence from Taiwan. Sustainability, 10(2), 513.

Kamalov, F. (2020). Kernel density estimation-based sampling for imbalanced class distribution. Information Sciences, 512, 1192–1201.

Kumar, S., Kumar, M., Hooi, B., Faloutsos, C., Makhija, D., & Subrahmanian, V. S. (2018). REV2: Fraudulent user prediction in rating platforms. Paper presented at the WSDM 2018 - Proceedings of the 11th ACM International Conference on Web Search and Data Mining, 2018-Febuary 333-341. doi:10.1145/3159652.3159729 Retrieved from www.scopus.com

Le, T., Hoang Son, L., Vo, M., Lee, M., & Baik, S. (2018). A cluster-based boosting algorithm for bankruptcy prediction in a highly imbalanced dataset. Symmetry, 10(7), 250.

Lin, H., Gao, S., Gotz, D., Du, F., He, J., & Cao, N. (2018). RCLens: Interactive rare category exploration and identification. IEEE Transactions on Visualization and Computer Graphics, 24(7), 2223–2237.

Lucas, Y., Calabretto, S., Portier, P. -., Caelen, O., Granitzer, M., Laporte, L., & He-Guelton, L. (2019). Multiple perspectives HMM-based feature engineering for credit card fraud detection. Paper presented at the Proceedings of the ACM Symposium on Applied Computing, Part F147772 1359-1361. doi:10.1145/3297280.3297586 Retrieved from www.scopus.com

Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M.-S., & Zeineddine, H. (2019). An experimental study with imbalanced classification approaches for credit card fraud detection. IEEE access: practical innovations, open solutions, 7, 93010–93022.

Monirzadeh, Z., Habibzadeh, M., & Farajian, N. (2018). Detection of violations in credit cards of banks and financial institutions based on artificial neural network and metaheuristic optimization algorithm. International Journal of Advanced Computer Science and Applications, 9(1), 176-182. doi:10.14569/IJACSA.2018.090124

Nian, K., Zhang, H., Tayal, A., Coleman, T., & Li, Y. (2016). Auto insurance fraud detection using unsupervised spectral ranking for anomaly. Journal of Finance and Data Science, 2(1), 58-75. doi: 10.1016/j.jfds.2016.03.001

Pérez Rave, J. (2012). Revisión Sistemática de Literatura en Ingeniería (Sello Editorial Universidad de Antioquia, Dic. 2012, ISBN: 978-958-714-543-4).

Pérez-Rave, J. (2019). Revisión Sistemática de Literatura en Ingeniería, ampliada y actualizada (Sello Editorial IDINNOV, Dic. 2019, ISBN: 978-958-58897-6-7).

Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit card fraud detection using AdaBoost and majority voting. IEEE access: practical innovations, open solutions, 6, 14277–14284.

República, E. L. (21 de 6 de 2021). Diario la República. Obtenido de https://www.larepublica.co/finanzas/delitos-financieros-le-costaron-us180-millones-a-las-entidades-colombianas-en-2020-3188958

Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE access: practical innovations, open solutions, 8, 25579–25587.

Xu, X., Liu, H., & Yao, M. (2019). Recent progress of anomaly detection. Complexity, 2019 doi:10.1155/2019/2686378

Zhang, J., Gardner, R., & Vukotic, I. (2019). Anomaly detection in wide area network meshes using two machine learning algorithms. Future Generations Computer Systems: FGCS, 93, 418–426.

Zhang, S., Zhou, D., Yildirim, M. Y., Alcorn, S., He, J., Davulcu, H., & Tong, H. (2017). HiDDen: Hierarchical dense subgraph detection with application to financial fraud detection. Paper presented at the Proceedings of the 17th SIAM International Conference on Data Mining, SDM 2017, 570-578. doi:10.1137/1.9781611974973.64 Retrieved from www.scopus.com

Zhou, X., Cheng, S., Zhu, M., Guo, C., Zhou, S., Xu, P., . . . Zhang, W. (2018). A state of the art survey of data mining-based fraud detection and credit scoring. Paper presented at the MATEC Web of Conferences, 189 doi:10.1051/matecconf/201818903002 Retrieved from www.scopus.com

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 30/10/2021
Aceitação/Acceptance: 31/01/2022

Emprego dual - civil e militar - do 5G na defesa brasileira: uma proposta para o SISFRON, sob domínio do Exército

Ricardo Cincinato Freitas de Oliveira[1], Georges Daniel Amvame Nze[2], Ugo Silva Dias[2]

cincinato.ricardo@aluno.unb.br; georges@unb.br; udias@unb.br

[1]Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE), Departamento de Engenharia Elétrica – Universidade de Brasília (UnB), Brasília-DF, Brasil, Zipcode 70.910-900

[2]Departamento de Engenharia Elétrica – Universidade de Brasília (UnB), Brasília-DF, Brasil, Zipcode 70.910-900

Pages: 599-615

Resumo: Atualmente o advento do 5G no mundo tornou possível o emprego dual - civil e militar - das suas tecnologias na defesa de países estrangeiros. Este trabalho realizou uma pesquisa bibliográfica e documental, de natureza aplicada, com abordagem qualitativa e objetivo exploratório sobre diversos estudos científicos globais, publicações e livros entre os anos 2018 a 2022, versando sobre o uso dual do 5G no exterior e no Brasil. Foram analisadas as possibilidades e limitações do emprego dual do 5G nas defesas estrangeiras e brasileira nos trabalhos correlatos, os quais serviram de arcabouço teórico para a resolução do tema proposto. Consequentemente, como resultado do estudo realizado, este trabalho propôs o emprego dual do Ecossistema 5G Brasil na defesa brasileira, em particular no SISFRON, descrevendo seu emprego pelo Exército Brasileiro, assim como suas vantagens para o desenvolvimento do Brasil.

Palavras-chave: Defesa; 5G; SISFRON; Exército.

Civil and military dual employment of 5G in Brazilian defense: a proposal for SISFRON, under the Army's domain

Abstract: Currently, the advent of 5G in the world has made possible the dual use - civil and military - of its technologies in the defense of foreign countries. This paper conducted a bibliographic and documental research, of applied nature, with qualitative approach and exploratory objective on several global scientific studies, publications and books between the years 2018 to 2022, dealing with the dual use of 5G abroad and in Brazil. The possibilities and limitations of the dual employment of 5G in foreign and Brazilian defenses were analyzed in related works, which served as the theoretical framework for the resolution of the proposed theme. Consequently, as a result of the study conducted, this paper proposed the dual employment of the 5G Brazil Ecosystem in Brazilian defense, particularly in SISFRON, describing its employment by the Brazilian Army, as well as its advantages for the development of Brazil.

Keywords: Defense; 5G; SISFRON; Army.

1. Introdução

O Brasil está situado no Continente Americano, com área aproximada de 8.5 Km² é o 5º maior país do mundo em extensão territorial, dispõe de cerca de 24,5 mil Km de fronteiras, sendo 7,5 mil Km marítimos e 17 mil Km terrestres (PND, 2012), possui população estimada em 2021 de 213.317.639 pessoas, e está dividido politicamente em cinco regiões: Norte, Sul, Centro-Oeste, Nordeste e Sudeste (IBGE, 2021).

O Brasil mantém relações internacionais amistosas com os 10 países vizinhos por meio das repartições Consulares brasileiras e faz limites à norte com a Guiana Francesa (Departamento Ultramarino da França), Suriname, Guiana, Venezuela, Colômbia e Peru; à oeste com Bolívia e Paraguai; à sul com Argentina e Uruguai; e à leste com o Oceano Atlântico (PND, 2012).

O § 2º, do Art. 20, da Carta Magna Brasileira de 1988, explica que a faixa de 150 Km de largura do limite para o interior do território brasileiro ao longo dos cerca de 17 mil Km das fronteiras terrestres delimita uma área de aproximadamente 2,535 milhões de Km², denominada unicamente como faixa de fronteira, que é considerada fundamental para defesa do território nacional (BRASIL, 1988). A defesa dessa faixa de fronteira terrestre é realizada pelas Forças Armadas (FA): Marinha do Brasil (MB), Exército Brasileiro (EB) e Força Aérea Brasileira (FAB), sob coordenação do Estado-Maior Conjunto das Forças Armadas (EMCFA), do Ministério da Defesa (MD).

O Sistema Integrado de Monitoramento de Fronteiras (SISFRON) é um importante projeto estratégico do Exército iniciado em 2010, originado da Política Nacional de Defesa (PND) de 2008, e continua em plena expansão. É formado pelos Subsistemas de Sensoriamento, de Apoio à Decisão e de Apoio à Operação e permeia em três outros projetos estratégicos do Plano Estratégico do Exército (PEEx) 2020-2023: OEE 1 - Contribuir com a dissuasão extrarregional; OEE 3 - Contribuir com o desenvolvimento sustentável e a paz social; e OEE 9 - Aperfeiçoar o sistema de ciência, tecnologia e inovação (CEADEx, 2020).

De acordo com (Direito da Comunicação, 2020) o Departamento de Defesa dos Estados Unidos da América (EUA), conhecido como Pentágono, está empregando o uso dual civil e militar do 5G com algumas das faixas do espectro eletromagnético (3.100-3.450MHz e 3.450-3.980 MHz), nos programas de modernização da defesa norte-americana, e considera isso essencial para a segurança econômica e segurança nacional dos EUA. Por meio de parcerias comerciais com empresas de alta tecnologia (Ericsson, AT&T, Vectrus, GE Research, GBL System Corp, Oceus Network, Booz Allen Hamilton, General Dynamics Mission Systems, Nokia, etc) estão sendo desenvolvidas soluções tecnológicas derivadas do 5G para as Forças Armadas dos EUA: Marinha (*Navy*), Exército (*Army*) e Força Aérea (*USAF*).

Este trabalho tem por objetivo propor o emprego dual civil e militar do 5G na defesa brasileira, por meio de equipamentos, serviços e produtos derivados das tecnologias do Ecossistema 5G Brasil, integrados aos subsistemas do SISFRON, sob domínio do EB.

Este trabalho está dividido em 5 Seções: a Seção 1 é a Introdução, que caracteriza alguns aspectos políticos gerais do Brasil em relação aos seus países vizinhos, cita algumas

legislações relacionadas à defesa da faixa fronteiriça brasileira, cita sumariamente o SISFRON, e apresenta algumas soluções tecnológicas de uso dual do 5G já empregadas pelo Pentágono na defesa dos EUA. A Seção 2 apresenta os Fundamentos Teóricos, descreve o SISFRON, descreve o Ecossistema 5G Brasil e discute os trabalhos correlatos sobre o uso dual civil e militar do 5G nas defesas estrangeiras. A Seção 3 apresenta a Metodologia empregada no trabalho, fruto da pesquisa bibliográfica e documental, revisão de artigos científicos, publicações e livros dos anos de 2018 a 2022. A Seção 4 apresenta os Resultados e discussões sobre o tema e propõe algumas tecnologiais civis do 5G para fins militares no SISFRON, sob domínio do Exército. Por fim, a Seção 5 apresenta as Conclusões deste trabalho, seguidos pelos agradecimentos e referências.

2. Fundamentos teóricos

Na (END, 2012) o Exército Brasileiro deve: contribuir para a soberania nacional; garantir os poderes constitucionais; garantir a lei e a ordem; cooperar com o desenvolvimento nacional e o bem-estar social; e salvaguardar os interesses nacionais. E a Força Terrestre (F Ter) deve ter condições de neutralizar concentrações de forças hostis junto à fronteira terrestre; contribuir para a defesa do litoral e para a defesa antiaérea no território nacional; entre outras capacidades.

Segundo (VERDE OLIVA, 2012) o SISFRON foi instituído sob a égide do trinômio monitoramento/controle, mobilidade e presença; visando aumentar a presença do Estado Brasileiro, a dissuasão e o poder do EB na faixa de fronteira, além da coleta de informações de áreas remotas onde ocorrem diversos crimes: ambientais; narcotráfico; contrabando de explosivos, armas e munições; roubo de cargas e veículos; evasão de divisas e lavagem de dinheiro; e descaminho de produtos falsificados levados para o interior do País.

Todos esses crimes geram o aumento da criminalidade e da violência generalizadas nas comunidades brasileiras, desde as pequenas cidades lindeiras das regiões Norte, Centro-Oeste e Sul, até as grandes metrópoles das regiões Sudeste e Nordeste, mais afastadas da faixa da fronteira, as quais se abastecem desses produtos ilícitos.

O 5G 3GPP foi apresentado ao mundo pela União Internacional de Telecomunicações (ITU) durante a Conferência Mundial de Radiocomunicações 2015 (WRC-15) e foi desenvolvido pela *International Mobile Telecommunication (IMT)* "*IMT for 2020 and beyond*" (ITU, 2016).

Em (Fang & Qian, 2020) a arquitetura do 5G 3GPP está baseada em "Tecnologias Avançadas" que são diversas inovações disruptivas ao padrão atual 4G (LTE-A) de comunicações móveis, tais como: *enhanced Mobile Broadband (eMBB)* ou banda larga móvel aprimorada; *Ultra-Reliable Low Latency Communication (URLLC)* ou comunicação de baixa latência ultraconfiável; e *massive Machine Type Communication (mMTC)* ou comunicação do tipo máquina massiva. Essas inovações tecnológicas do 5G podem ser muito úteis no uso dual em indústrias e cidades inteligentes, assim como nos sistemas de comunicações, comando e controle, de vigilância e de armas da defesa brasileira.

2.1. Sistema Integrado de Monitoramento de Fronteiras (SISFRON)

Segundo (Melo, 2017) é um importante projeto estratégico do EB, pois realiza a integração de dados de inteligência processados nos três níveis decisórios brasileiros: Estratégico, Operacional e Tático.

Foi instituído pela Portaria nº 3.090/MD, de 11 de outubro de 2011, que criou a comissão para acompanhamento da implantação, desenvolvimento e transformação do SISFRON.

Está em operação nos Comandos Militares de Área (C Mil A) constantes na faixa de fronteira: Comando Militar da Amazônia (CMA) em Manaus/AM), Comando Militar do Norte (CMN) em Belém/PA, Comando Militar do Oeste (CMO) em Campo Grande/MS e Comando Militar do Sul (CMS) em Porto Alegre/RS.

Em (EME, 2021), no ano de 2021 foi concluído 100% da implementação do Projeto Piloto Fase 1 de 2010, nos 700 Km da faixa de fronteira, na área do CMO (Campo Grande/MS), especialmente na área da 4ª Bda C Mec (Dourados/MS) formada pelas organizações militares (OM): 4ª Cia Eng Cmb, 9º GAC, 10º R C Mec, 11º R C Mec, 17º R C Mec, 14ª Cia Com e 20º RCB.

No ano de 2022, o SISFRON segue adiante com a implantação da Fase 2 (2020-2023) do SAD 2, nas áreas da 18ª Bda Inf Fron (Corumbá/MS), 15ª Bda Inf Mec (Cascavel/PR), 13ª Bda Inf Mtz (Cuiabá/MT), 2ª Bda Inf Sl (São Gabriel da Cachoeira/AM), 16ª Bda Inf Sl (Tefé-AM), 17ª Bda Inf Sl (Porto Velho/RO), 14º RC Mec (São Miguel do Oeste/SC).

O emprego do SISFRON está amparado legalmente pela Portaria nº 322-EME, de 8 de dezembro de 2015 (EB20-D-10.022), que orienta o emprego da Força Terrestre (F Ter) na faixa de fronteira; Portaria nº 512-EME, de 11 de dezembro de 2017, que aprovou a implantação do SISFRON (EB20-D-08.010) e Portaria nº 305-EME, de 12 de dezembro de 2018, que aprovou as Diretrizes de Iniciação dos Projetos das Fases 2, 3 e 3A (SAD 2, SAD 3 e SAD 3A) do SISFRON.

No dia 7 de abril de 2022 o Exército e a Embraer assinaram o contrato para o desenvolvimento e implantação da Fase 2-SAD2 do SISFRON nas áreas das 13ª Bda Inf Mtz (Cuiabá/MT) e 18ª Bda Inf Fron (Corumbá-MS), na faixa de fronteira oeste junto do Paraguai (1.209 Km) e Bolívia (1.314 Km), totalizando-se 2.523 Km, ambas áreas do CMO.

O SISFRON é composto pelo Subsistema de Sensoriamento (SS), Subsistema de Apoio à Decisão (SAD) e Subsistema de Apoio à Atuação (SAA) (BRASIL, 2013). A sua principal função é fornecer o alerta antecipado e responder prontamente a qualquer ameaça ou agressão, especialmente na região Amazônica, que detém 20% da disponibilidade mundial de água doce.

2.1.1. Subsistema de Sensoriamento (SS)

De acordo com (BRASIL, 2013) o SS é formado por pessoal e material especializado na área de inteligência militar (IM): inteligência de fontes humanas, inteligência do sinal e inteligência de imagens. Atualmente os sensores do SISFRON ficam operando 24/7 automaticamente de modo estático, mas também podem ser empregados de modo

dinâmico nas operações Ágata, do MD. Sensores mais empregados nas operações: eletromagnético, satelital de imagens espectrais (desmatamento, poluição de rios/ lagos, movimento de embarcações e comboios de veículos, etc), radar de vigilância terrestre SABER (movimento de veículos e pessoas); radar de vigilância aeroespacial BRADAR (movimentação e aproximação de aeronaves e drones); VANT Harpia com SAR de câmeras especiais de alta resolução (infravermelha e termal), e sensores de comunicações (GE); câmeras, binóculos termais e monóculos de visão noturna; entre outros sensores portáteis do 6º Batalhão de Inteligência Militar (6º BIM).

2.1.2. Subsistema de Apoio à Decisão (SAD)

De acordo com (BRASIL, 2013) o SAD é formado por pessoal e material especializado nas áreas de inteligência militar, comunicações (Com), guerra eletrônica (GE) e guerra cibernética (G Ciber).

O 6º BIM, que também participa diretamente do SS, é responsável por: coletar, receber, processar, armazenar e distribuir os dados de inteligência das diversas fontes do SISFRON, do 9º B Com GE e das agências do governo, tais como: ABIN, PF, PRF, IBAMA, entre outras. Faz parte da Infovia de Campo Grande/MS adjunto do CMO.

O 9º Batalhão de Comunicações e Guerra Eletrônica (9º B Com GE) é responsável por estabelecer as ligações de comunicações, o comando e controle e a consciência situacional do CMO com as suas OMDS e agências governamentais na área de Campo Grande/MS. Faz parte da Infovia de Campo Grande/MS adjunto ao CMO.

A 14ª Companhia de Comunicações é responsável por estabelecer as ligações de comunicações e o comando e controle da 4ª Bda C Mec com suas OMDS e agências governamentais na área de Dourados/MS. Faz parte da Infovia adjunto ao Comando da 4ª Bda C Mec em Dourados/MS.

O Módulo de Telemática Operacional (MTO) é um tipo de sistema de comunicações tipicamente militar, denominado Sistema de Comunicações Tático (SISTAC), pois é empregado diretamente no cumprimento de missões táticas, durante o transcurso das operações em áreas rurais e semiurbanas. Embora, também pode operar como Sistema de Comunicações de Área (SCA) em áreas urbanas, devido às suas características militares: flexibilidade, modularidade, robustez e segurança da informação. Foi fabricado no Brasil pelo Consórcio Embraer durante o Projeto Piloto do SISFRON iniciado em 2010 e, findado em 2021, empregado na área dos 700 Km da faixa de fronteira da 4ª Bda C Mec.

Segundo (HARRIS, 2015) o MTO é composto por 3 padrões de cabines (*Shelters)* militar S-788/BR, designadas como Postos de Comunicações (PC) para os escalões: Grande Unidade (GU), Unidade (U) e Subunidade (SU).

Os PC GU e PC U podem ser embarcados sobre as Viaturas de Comando e Controle (VCC), ou embarcados nas viaturas Agrale Marruá ¾ Ton AM23VTL, enquanto que os PC SU podem ser transportáveis em mochilas individuais pelos combatentes empregadas nas missões de patrulhas e reconhecimentos de fronteira. Abaixo estão descritos os equipamentos embarcados nas cabines do MTO, tomando-se por base o PC GU mais completo, conforme descrito na Tabela 1 abaixo.

Tipos de PCs	Equipamentos embarcados nas cabines dos PC
GU - Grande Unidade	dispõe de 2 Rádios Transceptores Micro-ondas RF-7800W-OU500 (HCLOS); 1 par de Antenas Micro-ondas Omnidirecionais RF-RF-7800W-AT206; 1 Rádio Transceptor Multibanda RF-7800M-MP; 1 par de Antenas Setoriais Parabólicas MIMO RF-7800W-AT203; 1 Rádio Transceptor Portátil RF-7800V-HH; 1 Amplificador Adaptador Veicular (VAA) RF-7800VV501 (até 50 W); 1 conjunto de Antenas Veiculares Omnidirecionais com GPS RF-387-AT002; 1 Roteador Cisco 2921; 1 *Access Point Airguard 3e-525A-3* (Ponto de Acesso); 4 Telefones VoIP; 2 *Notebooks* robustecidos (*Toughbook CF-31 Panasonic*); 1 Bancada para 2 operadores; e 2 Cadeiras de escritório com rodízios. Acoplado à estrutura da cabine (Shelter S-788BR) estão: 1 Grupo Moto Gerador Siemens (GMG); 1 Mastro pneumático para instalação das antenas; 1 ar condicionado; e 1 escada de alumínio retrátil para acesso ao seu interior.
U - Unidade *SU - Subunidade*	dispõe de todos os equipamentos do PC GU, exceto: 1 Rádio Transceptor Micro-ondas RF-7800W-OU500 (HCLOS) e 1 par de Antenas Micro-ondas Omnidirecionais RF-RF-7800W-AT206.
Rpt - Repetidor	é especialmente mobiliado com 2 Rádios Transceptores RF-7800M-MP e 2 pares de Antenas Setoriais Parabólicas MIMO RF-7800W-AT203, para realizar a repetição dos sinais dos PC GU/PC U/PC SU com modulação AM/FM e exclusiva Forma de Onda de Rede de Banda Larga Adaptável (ANW2/ANW2C). Contudo, não dispõe de 2 Rádios Transceptores RF-7800W-OU500 (HCLOS); 2 pares de Antenas Micro-ondas Omnidirecionais RF-RF-7800W-AT206; e 1 *Access Point Airguard 3e-525A-3* (Ponto de Acesso).

Tabela 1 – Tipos de Postos de Comunicações do SAD

Segundo (HARRIS, 2015) os PC GU/PC U/PC SU podem: estabelecer redes Ponto Multiponto (PMP) e Ponto a Ponto (PTP) com rádios transceptores RF-7800W-OU500 Micro-ondas com enlaces de frequências na faixa SHF (4,5 a 5,85 GHz) de 10 até 30W tipo HCLOS até 216 Mbps; Duplexação por Divisão de Tempo (TDD) e Multiplexação Ortogonal por Divisão de Frequência (OFDM); usar larguras de banda de quatro canais (5, 10, 20, 40 MHz); usar modulação por Deslocamento de Fase Binária (BPSK), Modulação por deslocamento de Fase de Quadratura (QPSK), 16 Modulações de Amplitude de Quadratura (QAM) e 64 QAM); usar criptografias AES 128/256 bits com chaves de até 64 caracteres; e protocolo de Autenticação X509.

O MTO com os rádios transceptores RF-7800M-MP Multibanda dos PC GU/PC U/PC SU podem: estabelecer enlaces de frequências nas faixas VHF/UHF (30-2.000 MHz) até 20W; usar modulação AM, FM (desvio de 5; 6,5; 8 kHz), FSK, ASK; usar Forma de Onda de Rede de Banda Larga Adaptável (ANW2/ANW2C), Frequência Fixa de Linha de Visada VHF/UHF (VULOS), QUICKLOOK 1A e 2 *Frequency Hopping* (salto de frequência); usar criptografias AES 128/256 bits com chaves de até 64 caracteres e Citadel para VULOS; permitir o tráfego *unicast* ou *multicast* por meio de IP, com o notebook da VCC ou Chat Tático (TAC CHAT) via interface *Ethernet;* buscar novas redes de comunicações junto aos outros sistemas integrados na Infovia.

Em (HARRIS, 2015) foi possível estabelecer uma rede de comunicação PMP entre 1 VCC, 1 PC GU e 1 PC SU no terreno, transmitindo imagens de vídeo a dezenas de quilômetros e fornecendo o acesso à Internet para os outros PC U/PC SU até 100 Km de distância

da base de operações. A integração de qualquer cenário remoto é possível através dos sistemas de comunicações via satélite SISCOMIS e SGDC-1.

Dessa forma, é possível trafegar pela Infovia praticamente todos os dados coletados na campanha e processados em tempo real, desde as imagens captadas dos sensores estáticos instalados na faixa de fronteira (câmeras termais de vigilância de alta definição, sensores infravermelhos de alarme de perímetro e câmeras de longo alcance com visão noturna), como também dados dos sensores dinâmicos (Radar SABER M-20, Radar SABER M-60 e Radar SABER M-200), até os dados do VANT Radar SAR quando ativado em voo e das imagens geradas pelo Satélite Geoestacionário de Defesa e Comunicações Estratégicas 1 (SGDC-1), que opera na Banda Ka (civil) e na Banda X (militar). Conforme ilustra a Figura 1 abaixo.

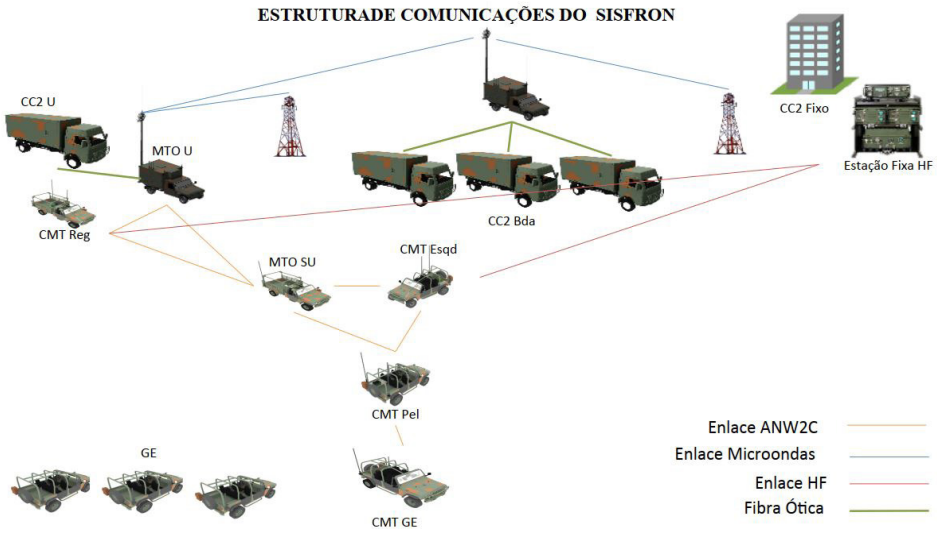


Figura 1 – Visão simplificada da Arquitetura da rede MTO do SISFRON. Fonte: HARRIS

Da Figura 1 acima, entende-se que o alcance das comunicações das redes dos PC GU/PC U/PC SU/VCC dependem exclusivamente do canal pelo qual irão trafegar as informações coletadas nos sensores pelos equipamentos de Tecnologias da Informação e Comunicação (TIC), por exemplo: Roteador Cisco 2921, *Access Point Airguard 3e-525A-3* e rádios transceptores da HARRIS; todos embarcados nos PCs.

Ora os dados são trafegados no espectro eletromagnético via enlaces de rádios transceptores da HARRIS, Motorola e RRF-HF (HCLOS, ANW2C, VLOS, SRDT, RRF-SEC-HF) ou pelos enlaces satelitais (SISCOMIS e SGDC-1). Ora são trafegados na Infovia do SISFRON, tais como: fibra óptica, micro-ondas, Rede Privativa Corporativa de Dados (EBNet), Rede Integrada de Telecomunicações do Exército (RITEx), Sistema Nacional de Telecomunicações (SNT) e Internet.

Quando as redes de comunicações dos PCs estão integradas totalmente na Infovia, na EBNet ou na RITEx, essas redes utilizam o *backhaul* da fibra óptica do SNT, seu alcance dependerá do sinal laser das fibras ópticas multimodo (locais) e monomodo (metropolitanas), e podem ser interligadas com quase todas as 570 OM do EB, destas 66 dispõe de nós exclusivos na faixa de fronteira e outras 152 OM contam com nós contratados da empresa Embratel, prestadora do serviço de telecomunicações no Brasil. Presume-se que quando o MTO está interconectado pela Internet o seu alcance seria global em teoria.

A Infovia é um sistema de telecomunicações estratégicas considerado como a "espinha dorsal" (*backbone*) do SISFRON, e recebeu um aporte considerável de recursos financeiros durante o Projeto Piloto Fase 1 (SDA1), pois realiza a interligação dos 3 subsistemas SS, SAD e SAA do SISFRON.

A Infovia é composta por 2 infraestruturas: 1 física e 1 lógica. Na infraestrutura física existem: edificações, torres, postes, sistema de alimentação (gerador e banco de baterias), cercas, e cabine (*Shelter* de PVC/concreto) para os equipamentos da infraestrutura física; enquanto que na infraestrutura lógica temos os diversos equipamentos de TIC: sítios de antenas, rádios micro-ondas, radomes, geradores, banco de baterias, roteadores, servidores, *switchs, hacks*, cabos e conectores de fibras ópticas, cabos e conectores de par trançado não blindado (UTP), computadores de mesa, computadores portáteis (*notebooks*), câmeras especiais tipo *Speed Dome*, e sensor de presença infravermelho.

A Infovia dispõe de 68 Torres de Comunicações Micro-ondas (TCM) com estações-rádios e antenas de micro-ondas denominadas Ponto de Presença (PP) e Pontos de Repetição (PR).

A Infovia realiza as comunicações entre os PP e PR com radioenlaces de micro-ondas trafegando exclusivamente dados em modo *fullduplex* até 144 Mbps, operando nas faixas de frequências de 8,0-8,5 GHz.

Os PP são responsáveis pelo tráfego dos dados coletados nos diversos sensores fixados nas TCM, encaminhando-os para os CRM lotados nos C Mil A (CMO, CMA, CMN e CMS), bem como para o CM de Brasília/DF. Enquanto que os PR apenas realizam as retransmissões dos dados com outros PR e PP até os destinos finais.

As TCM e seus PP estão dispostos nas OMDS participantes do SISFRON, tais como: 6º CTA (Campo Grande/MS), 4ª Bda C Mec (Dourados/MS), 13ª Bda Inf Mtz (Cuiabá/MT), 18ª Bda Inf Mtz (Corumbá/MS), entre outras OM e cidades das 68 presentes na Infovia do SISFRON.

2.1.3. Subsistema de Apoio à Atuação (SAA)

De acordo com (BRASIL, 2013) o SAA é formado pelo Centro de Monitoramento (CM) lotado em Brasília-DF; pelos Centros Regionais de Monitoramento (CRM) lotados nos Comandos Militares de Área: CMO, CMA, CMN e CMS; e pelos Centros Regionais de Interação (CRI) lotados nas áreas das agências governamentais de cada estado brasileiro. O Projeto Piloto do SISFRON contempla 7 Centros (C) de C2 fixos e 10 CC2 móveis. Os CC² fixos estão instalados nos CRM, enquanto que os C² móveis estão instalados nas

VCC. O Comandante da missão e seu Estado-Maior podem realizar seus planejamentos, divulgar suas ordens fragmentárias e acompanhar o desencadeamento das ações táticas dos escalões subordinados, com maior flexibilidade e rapidez às operações, empregando as VCC.

2.2. O Ecossistema 5G Brasil

Segundo (Telebrasil 5G Brasil, 2018) o Projeto 5G Brasil batizou o 5G 3GPP de "Ecossistema 5G Brasil", seguindo o exemplo da *Association GSM (GSMA, 2022)* na divulgação do Ecossistema 5G mundial fundamentado em três grandes pilares: alcance; conectividade para o bem; e serviços e soluções da indústria.

O Projeto 5G Brasil é formado por instituições brasileiras ligadas ao governo, ao comércio, à indústria, à pesquisa e à academia. É uma associação brasileira de fomento à implantação do 5G no Brasil, que busca de forma voluntária divulgar o Ecossistema 5G Brasil. Conforme ilustra a Figura 2 abaixo.



Figura 2 – Agentes do Ecossistema 5G brasileiro. Fonte: Telebrasil 5G Brasil

Da Figura 2 acima, deduz-se que as partes interessadas (*stakeholders*) na implantação do Ecossistema 5G Brasil tem um caminho a ser explorado pela frente, pois há diversos processos em andamento no governo brasileiro para se definir qual será a matriz fornecedora dos equipamentos e serviços do 5G 3GPP que o Brasil adotará na implantação a partir de 2022.

Para divulgar e coordenar a implantação do Ecossistema 5G Brasil, o governo brasileiro elaborou a Estratégia Brasileira de Redes de Quinta Geração por meio do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC, 2019). Conforme (Anatel, 2021) a Agência Nacional de Telecomunicações (Anatel) publicou o Edital de Licitação nº 1/2021-SOR/SPR/CD-ANATEL, em 24 de setembro de 2021. Dessa forma expediu a outorga necessária para liberar o uso comercial das radiofrequências nas faixas de 700 MHz; 2,3 GHz; 3,5 GHz e 26 GHz; com prazo de 20 anos para exploração das

operadoras de telefonia, podendo ser prorrogável por mais 10 anos. Conforme ilustra a Figura 3 abaixo.

Faixa	Banda	Bloco	Oferta de bloco na 1ª rodada	Resultado esperado	Oferta de bloco na 2ª rodada	Spectrum Cap	Compromisso	Observação
700 MHz	708 - 718 MHz 763 - 773 MHz	Nacional	10 + 10 MHz	Sobras de 10 + 10 MHz para nova operadora atacadista	5 + 5 MHz	Art. 1º, Inciso I, da Resolução nº 703/2018	ERB 4G ou superior em localidades e trechos de estradas	Não é admitida a participação no Leilão daquelas operadoras que já dispõe de autorização na Faixa 700 MHz ou esteja em processo de transferência de controle societário
2,3 GHz	2.300 - 2.390 MHz	Regional	90 MHz	8 operadoras com 40 MHz e 8 operadoras com 50 MHz	Não há	50 MHz	95% de cobertura de municípios sem 4G + Ativar 4G em localidades	Não há
3,5 GHz	3.300 - 3.700 MHz	Nacional e Regional	400 MHz	80 MHz por operadora	20 MHz	100 MHz	ERBs 5G + Limpeza da Banda C + Programa Amazônia Integrada e Sustentável (PAIS) + Rede Privativa de Comunicação da Administração Pública Federal (RAAPF)	1ª rodada com único bloco de 10 + 10 MHz: - 4 nacionais de 80 MHz. - 8 regionais de 80 MHz, sendo possível arrematar no máximo dois blocos regionais 2ª rodada com 2 blocos de 5 + 5 MHz: - Blocos de 20 MHz, caso não haja vencedor para algum dos lotes nacionais ou ao menos um lote regional
26 GHz	24,3 - 27,5 GHz	Nacional e Regional	3.200 MHz	400 MHz por operadora	200 MHz	1 GHz	Não há	5 blocos nacionais com 400 MHz e 21 blocos regionais com 400 MHz

Figura 3 – Quadro resumo do Edital de Licitação nº 1/2021. Fonte: o Autor

Da Figura 3 acima, infere-se que o Ecossistema 5G Brasil: será implantado ainda em 2022, com 3.710 MHz do espectro eletromagnético licitado pela Anatel (Telesintese, 2021); irá gerar desenvolvimento socioeconômico por meio de empregos diretos e indiretos nas comunidades implantadas; será o principal meio da população obter comunicações, informação e lazer; realizará a inclusão digital na educação básica; irá atender áreas remotas da Amazônia; e ampliará significativamente a cobertura atual do 4G nos municípios e rodovias federais.

Segundo (DMAnápolis, 2021) com o leilão do Ecossistema 5G Brasil o Tesouro Nacional estima receber R$ 3,06 bilhões com as vendas diretas dos lotes, receber R$ 7,57 bilhões para o custeio da internet nas escolas de educação básica e R$ 39,1 bilhões pelos investimentos restantes obrigatórios constantes do edital; inclusive receber uma rede exclusiva de comunicação governamental na Administração Pública Federal (APF) em Brasília/DF.

2.3. sTrabalhos correlatos

É inegável que a tecnologia 5G está revolucionando o mundo atualmente, pois permite o uso dual das tecnologias oriundas do 5G, tanto na esfera civil, para fins comerciais e sociais, como na esfera militar, para fins de defesa e segurança pública.

A 10ª Conferência de Sistemas e Tecnologia Militar 2021 ocorreu de 23 a 26 de novembro de 2021, em Brasília/DF, no Estádio Nacional de Brasília Mané Garrincha, contou

com representantes das indústrias nacionais de defesa; autoridades diplomáticas e do governo; políticos; militares das Forças Armadas; integrantes da Segurança Pública; pesquisadores; estudiosos; jornalistas especializados; e abordou diversas pesquisas e propostas sobre o emprego do 5G na esfera militar.

Estudos recentes foram publicados no meio acadêmico global e apontam algumas possibilidades e limitações do emprego dual das tecnologias derivadas do 5G na esfera militar, conforme descrito na Tabela 2 a seguir.

Contudo, há poucas publicações de estudos acadêmicos versando sobre o emprego dual das tecnologias oriundas do 5G na esfera militar brasileira, sendo esse trabalho de grande importância para sanar as lacunas desse conhecimento e, pode, inclusive, subsidiar outros estudos de aplicações teóricas e/ou práticas na área da defesa brasileira.

Estudos publicados	**Citações de até 3 aplicações militares do 5G**
Bhardwaj, A. (2019) - 5G for Military Communications	Comunicações e controle de voo para veículos hiper planados (*hyper glided vehicles HGV*) com velocidades hipersônicas; e dispositivos vestíveis tipo relógios e roupas que se comunicam entre as frações do grupo de combate, e caso alguém seja ferido em um conflito, automaticamente o cinto irá aplicar uma injeção de primeiros socorros, haverá uma mensagem de alerta para a base de saúde se preparar, que providenciará o apoio imediato com ambulância autônoma ou viatura blindada com o restante do pelotão até o local da ocorrência com ressuprimento de emergência.
Harvey, J. F. et al. (2019) - Exploiting High mm-wave Bands for Military Communications, Applications, and Design	Redes locais especiais de baixíssima cobertura que aumentam o sigilo; arranjos de antenas direcionais de alto ganho e alta eficiência energética; e enxames de robôs autônomos ou semi-autônomos para espionagem, vigilância, ataques com fogos cinéticos (mísseis e bombas) e não-cinéticos (eletrônicos).
Sharma, K. et al. (2020) - Wearable Computing for Defence Automation: Opportunities and Challenges in 5G Network	Plataformas de comunicações aéreas podem interligar os comandantes de pelotões diferentes entre si e com outros grupos de combate aumentando a consciência situacional e melhorando a tomada de decisões sob estresse no campo de batalha; exoesqueleto reduz a fadiga do combatente; e computação confiável no C2 com: blockchain, redes definidas por software e aprendizado distribuído.
Ferreira, J. (2020) - Aplicabilidade da Tecnologia 5G Para Uso dos Órgãos de Segurança Pública	Personalização nas comunicações da segurança pública usando o IP Multimídia System (IMS) para a função de Push-to-Talk (PTT) nos aparelhos móveis celulares; uso de robôs remotos para atividades de risco de morte na desativação de explosivos; e integração de imagens geradas em câmeras fixadas nos uniformes dos agentes de segurança (*bodycam*).
Pedro, J. (2021) - O Impacto das Redes 5G na Segurança e Defesa Nacional	Gestão automatizada de estoques em Bases Inteligentes; telemedicina; e segurança das instalações de bases com câmeras dotadas com inteligência artificial.
Wade, Dani. (2021) - 5G network information technology and military information communication data services	Bases militares inteligentes com logística autônoma executada por robôs (drones, veículos terrestres, embarcações): ressuprimento automático no campo de batalha (munição, água, ração, remédio, combustível, etc); relógios inteligentes com altímetro, barômetro, bússola, pedômetro, batimentos cardíacos, pressão sanguínea, GPS e ligações rádio; e redes móveis definidas por software anti-bloqueio (jamming) e anti-aquisição (hacking).

Tabela 2 – Estudos publicados sobre emprego dual do 5G na Defesa

Em (Bhardwaj, 2019) seu trabalho apresenta diversas tecnologias do 5G para emprego militar na Índia: HetNets, SDN, NFV, Comunicações M2M, mmWave, e MIMO maciço. Também analisa os desafios e serviços de segurança oferecidos pelo grupo 3GPP *Security Association* 3 (SA3), os cenários futuros do espaço de batalha que se beneficiam das tecnologias 5G e as oportunidades futuras.

Em (Harvey, J. F. et al, 2019) seu trabalho aborda como as ondas milimétricas (*mmWaves*) do 5G podem ser aproveitadas nas comunicações militares de banda mais alta (6, 27, 39, 41, 72 e 141 GHz) com arranjos de antenas dipolo em simulações realizadas no MATLAB. Foram analisadas as alterações das comunicações entre as antenas (área de cobertura, radiância, direcionalidade do lóbulo principal e atenuação do sinal em dBi) sob parâmetros de condições ambientais críticos como chuva e atenuações de absorção atmosférica. Tais fatores críticos influenciam diretamente nas áreas de cobertura e nas taxas de dados trafegados (transmitidos e recebidos). Destaca-se também no estudo as exigências de comunicações especiais de redes locais militares para uma Brigada (composta por 3.000 até 11.000 militares) modular comandada por um Coronel nos EUA, dotada de sistemas de inteligência, comunicações, armas, logística, redes WiFi contra sortidas de enxames de Drones equipados com munições letais ou não letais, capacidades de guerra eletrônica (jamming) e cibernética (hacking), tecnologia de engodo, sistemas de navegação falsa, e sensores avançados para inteligência, vigilância e reconhecimento.

Em (Sharma, 2020) seu estudo apresenta conceitos, equipamentos e serviços da Internet das Coisas do Campo de Batalha (IoBT), que possibilitam plena realização do sensoriamento, de comunicações e de computação onipresentes, entre humanos e máquinas no campo de batalha. Também discute como as soluções baseadas em computação vestíveis desempenham um papel importante na automação da defesa. A automação na defesa proporciona maior agilidade no ciclo de tomada de decisão dos comandantes aliados e inimigos, influenciando diretamente nas ações futuras das tropas, porque permite que as agências de inteligência militares tomem decisões com base nas análises em tempo real, geradas pela integração de informações (voz, dados e imagem) de uma ampla gama de dispositivos vestíveis no campo de batalha. O estudo conclui sobre os desafios futuros no desenvolvimento de tecnologias vestíveis e propôs um protótipo de relógio inteligente com tecnologia de criptografia simétrica denominada PUF ID.

Em (Ferreira, 2020) seu estudo aborda a arquitetura 5G RAN (*Radio Access Network*) e suas Redes Heterogêneas (*HetNets*), que permitem a formação de uma rede multicamada, sendo que cada camada independente tem potência de transmissão e área de cobertura diferente das demais, a fim de possibilitar a interoperabilidade, confiabilidade, segurança e disponibilidade de comunicações para o Sistema Nacional de Comunicações Críticas (SISNACC) do Brasil, envolvendo as Forças Armadas, os Órgãos de Segurança Pública, Fiscalização, Repressão e Controle da Defesa Civil.

Em (Pedro, 2021) é apresentada uma visão geral das tecnologias 5G e também identificados os impactos das redes 5G nas FA portuguesas por meio de entrevistas diretas com autoridades militares portuguesas da Marinha, Exército e Aeronáutica, realizadas pela plataforma *Microsoft Teams*. São analisados contextos das orientações

recebidas da União Europeia (EU) e das Organizações do Tratado do Atlântico Norte (OTAN), em consideração as caraterísticas e os campos de aplicação da tecnologia 5G na esfera militar. O artigo fornece conclusões e recomendações às partes interessadas nas comunicações 5G para o uso dual, incluindo a identificação de áreas de desenvolvimento posterior em Portugal.

Em (Wade, 2021) são abordados aspectos teóricos das tecnologias 5G para uso militar global e a comparação de velocidade de transmissão de pacotes de dados de um arquivo em uma rede móvel entre dois protocolos distintos: *Low Latency Communication Ultra-Reliable (LLCUR) e Data Named Design (DND)*. Assuntos abordados: sistema de antenas distribuídas (DAS) que compartilha a faixa de ondas milimétricas baseada em redes 5G; rede óptica passiva (PON) que tem se tornado uma topologia multiponto-ponto para o uso efetivo de pesquisas de texto; velocidade das redes militares deve-se ter alta capacidade com enlaces sem fio e anti-bloqueio. Seu estudo conclui e demonstra um incremento de 18% de velocidade na transmissão de pacotes TCP/IP e UDP pelo protocolo LLCUR (90%) sobre o protocolo DND (72%), ou seja, um ganho significativo para redes militares de comando e controle (C^2), logo poderia reduzir mortes no Teatro de Operações.

Por todo o exposto, deduz-se que a tecnologia 5G pode estimular ainda mais seu emprego na esfera militar nos próximos anos, em que pese a necessidade de estudos mais detalhados por causa dos desafios técnicos intrínsecos na pesquisa, na criação, na adoção e na implantação de novos produtos e serviços derivados do 5G, nos sistemas de defesa de cada país adotante.

3. Metodologia

Este trabalho realizou uma pesquisa bibliográfica e documental, de natureza aplicada, com abordagem qualitativa e objetivo exploratório sobre diversos estudos científicos globais, publicações e livros entre os anos 2018 a 2022, que demonstram o uso dual do 5G no exterior e apresenta uma sugestão para o Brasil.

Buscou-se analisar nos trabalhos correlatos as principais tecnologias derivadas do 5G já empregadas na esfera militar nos EUA, na China, na Coreia do Sul, na Índia, e em Portugal, as quais também podem ser implementadas no Brasil.

Em que pese a necessidade de estudos complementares mais detalhados, por causa dos desafios técnicos intrínsecos na criação, na comercialização e na adoção de novos produtos e serviços derivados do 5G para os sistemas de defesa de cada país adotante, espera-se que os resultados apresentados sejam coerentes com a aplicação dual do 5G na defesa brasileira realizada no SISFRON.

4. Resultados e discussões

Os EUA já dispõe de tecnologias derivadas do 5G implementadas pelo Pentágono no uso dual pela Marinha (*Navy)*, pelo Exército (*Army)* e pela Força Aérea (*USAF)*, que permitiram: automatizar tarefas logísticas em bases inteligentes; economizar recursos

financeiros em treinamentos com óculos de realidade virtual (RV) e óculos de realidade aumentada (RA); empregar inteligência artificial na gestão das frequências de rádios transceptores; realizar o compartilhamento dinâmico de frequências dos radares; melhorar os sistemas de comando e controle e as comunicações móveis ultra-rápidas entre os escalões de comando, os escalões subordinados e suas peças de manobra; aplicar a aprendizagem de máquina na coexistência da tecnologia de uso duplo do 5G; realizar telemedicina (cirurgias e diagnósticos remotamente); usar arranjos de antenas direcionais com MIMO e *beamforming* entre suas bases e seus veículos autônomos de reconhecimento, vigilância e de assalto, entre outras aplicações militares no campo de batalha.

Logo, fica evidente para o MD a necessidade de empregar também as tecnologias derivadas do Ecossistema 5G Brasil na esfera militar brasileira, por meio da integração direta no SISFRON.

A Infovia considera dividir o tráfego em 2 *backbones* de até 288 Mbps, sendo 1 *backbone* de 144 Mbps para as OM situadas no estado do Mato Grosso do Sul (MS) e 1 *backbone* de 144 Mpps para as OM situadas no estado do Mato Grosso (MT).

Nas regiões metropolitanas a arquitetura de rede da Infovia está estruturada com fibra óptica multimodo, realizando a interligação dos PP e PR às OM do SISFRON. Os PP podem utilizar o *backhaul* da rede metropolitana de fibra óptica trafegando dados até 1 Gbps via *Ethernet* (TCP/IP) entre os roteadores de camada 3 com os switchs de camada 3, ambos lotados nos CRM (CMO, CMA, CMN e CMS).

A Infovia poderá integrar as tecnologias do 5G SA *(Stand Alone)* diretamente nos PP e PR, utilizando-se de rádios micro-ondas do tipo 5G RAN (5G *Radio Access Network)* com frequências na faixa de 26 GHz, pois essa faixa será menos demandada no início da implantação do Ecossistema 5G Brasil.

A Infovia poderá ativar o reuso de frequências (*backhauling)* das fibras ópticas multimodos das redes metropolitanas que ligarão as ERB das redes móveis do 5G nas áreas urbanas do SISFRON, realizando o fatiamento da Rede Principal (*Core network*) em camadas de aplicações disponibilizando maior capacidade de assinantes ao mesmo tempo e maior confiabilidade no tráfego dos dados.

A Infovia poderá utilizar Redes Definidas por Software (SDN) para melhorar a segurança das subredes virtuais criadas para os PP; e também para melhorar as comunicações entre os servidores dos PP nessas redes por meio do mMTC (massivo Tipo de Comunicação de Máquina).

A Infovia poderá utilizar arranjos de antenas especiais de ondas milimétricas (*mmWave*) com *Beamforming* e MIMO com o rádio 5G RAN junto aos sensores e câmeras de vigilância especiais fixados nas TCM, aumentando-se consideravelmente as taxas de transmissão *fullduplex* de 144 Mbps (micro-ondas) para 1 Gbps (5G) por meio da comunicação ultra-confiável de baixa latência (uRLLC).

O CM (Brasília/DF) e os demais CRM (Campo Grande/MS, Manaus/AM, Belém/PA e Porto Alegre/RS) poderão implantar Redes Heterogêneas (*HetNets*) para realizarem

comunicações móveis melhoradas de banda larga (eMBB), aumentando o tráfego de dados entre os roteadores e switchs de camada 3, dos atuais 1 Gbps até 100 Gbps.

Durante as missões reais executadas pelos Grupos de Inteligência (GI) do 6º BIM, poderão ser estabelecidas células tipo pico e femto (alguns metros), entre os smartphones 5G dos operadores de inteligência, visando diminuir o alcance dos sinais para fora das áreas de interesse e aumentar o sigilo das comunicações nas ações de vigilância de alvos e pontos sensíveis durante o dia, e principalmente, à noite.

5. Conclusões

O SISFRON vem mantendo o sensoriamento das áreas de interesse na fronteira terrestre brasileira desde a sua implantação no ano de 2010, fornecendo dados de inteligência preciosos para as autoridades civis e militares nos níveis Estratégico e Operacional. E no nível Tático facilita o emprego das Forças Armadas e das agências governamentais nas Operações Ágata de combate aos ilícitos fronteiriços.

De acordo com (Telesintese, 2021) o 5G não é uma opção, mas será um dos alicerces da sociedade moderna e será o principal meio de comunicação, informação e entretenimento. Seus sistemas, tecnologias e arquiteturas das redes móveis continuarão a evoluir para melhorar a eficiência e uso do espectro eletromagnético, além de contribuir para as economias e empregos em nível global.

Seguindo o exemplo dos países estrangeiros EUA, China, Coreia do Sul, Índia e Portugal, que já implementaram tecnologias civis e militares no Estado da Arte do 5G (eMBB, URLLC e mMTC) nas suas defesas e segurança pública, o Ministério da Defesa (MD) brasileiro pode implantar o Ecossistema 5G Brasil na defesa brasileira, iniciando-se no SISFRON, devido a sua importância estratégica, operacional e tática.

Por fim, apesar dos desafios atuais e futuros na implantação do Ecossistema 5G Brasil, percebe-se que seu emprego dual na defesa brasileira porporcionará avanços tecnológicos importantes para o EB, assim como para o Brasil, visando: ampliar a interoperabilidade das Forças Armadas brasileiras nas áreas de atuação do SISFRON; inceremetar cooperações diplomáticas e militares com os 10 países vizinhos no combate aos ilícitos; consolidar ações protetivas e sociais do Estado brasileiro junto das comunidades mais carentes estabelecidas na faixa de fronteira terrestre; e estimular o desenvolvimento da indústria nacional de defesa.

Agradecimentos

Os autores agradecem o suporte da Agência Brasileira de Inteligência (ABIN) TED 08/2019, à Fundação de Apoio à Pesquisa (FUNAPE) e ao Exército Brasileiro.

Referências

Agência Nacional de Telecomunicações (Anatel). (2021). *Anatel publica edital do leilão do 5G*. https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-publica-edital-do-leilao-do-5g

Bhardwaj, A. (2019). *5G for Military Communications*. Third International Conference on Computing and Network Communications (CoCoNet'19). CAIR DRDO Bangalore, India. 2019. https://www.sciencedirect.com/science/article/pii/S0141933120306128.

BRASIL. (1988). *Constituição da República Federativa do Brasil*. Revisada em 2016. https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf

BRASIL. (2012). *Política e Estratégia Nacional de Defesa*. https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/ENDPND_Optimized.pdf

BRASIL. (2013). *Sistema Integrado de Monitoramento de Fronteiras (SISFRON)*. (2013). Palestra ministrada no CMO em Campo Grande/MS. https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cedn/palestras-junho-2013/o-sisfron-projeto-estrategico-do-exercito.pdf

Centro de Educação a Distância do Exército (CEADEx). (2020). *Plano Estratégico do Exército* 2020-2023. http://www.ceadex.eb.mil.br/images/legislacao/XI/plano_estrategico_do_exercito_2020-2023.pdf

Direito da Comunicação. (2020). *Aplicações militares da tecnologia de 5G nos Estados Unidos*. https://direitodacomunicacao.com/br/aplicacoes-militares-da-tecnologia-de-5g-nos-estados-unidos/#_ftnref1

DMAnápolis, o seu jornal diário. (2021). *Com a promessa de plugar de vez a economia, 5G vai a leilão*. https://www.dmanapolis.com.br/noticia/14906/com-a-promessa-de-plugar-de-vez-a-economia-5g-vai-a-leilao

Fang. D & Qian. Y (2020). *5G Wireless Security and Privacy: Architecture and Flexible Mechanisms*. in IEEE Vehicular Technology Magazine, vol. 15, no. 2, pp. 58-64, June 2020, DOI: 10.1109/MVT.2020.2979261.

Ferreira, J. (2020). *Aplicabilidade da Tecnologia 5G para Uso dos Órgãos de Segurança Pública*. http://www.ebrevistas.eb.mil.br/OC/article/view/6017

GSM Association (GSMA). (2022). *About Us*. https://www.gsma.com/aboutus/

HARRIS. (2015). *Treinamento Sistema MTO*. Versão 2.0.

Harvey, J. et al. (2019). *Exploiting High mm-wave Bands for Military Communications, Applications, and Design*. IEEE, Vol 7, 2019. https://ieeexplore.ieee.org/document/8692347

Instituto Brasileiro de Geografia e Estatística (IBGE). (2022). *Cidades e Estados*. https://www.ibge.gov.br/pt/cidades-e-estados.html

ITUnewslog. (2016). *IMT-2020 makes progress in developing 5G standard*. https://newslog.itu.int/archives/1210.

Melo, C. (2017). *Sistema de Monitoramento de Fronteiras (SISFRON): Uma importante ferramenta de apoio à Defesa Nacional*. https://repositorio.uninter.com/handle/1/237

Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). (2019). *Estratégia Brasileira de Redes de Quinta Geração*. https://antigo.mctic.gov.br/mctic/export/sites/institucional/sessaoPublica/arquivos/estrategia5g/Documento-base-da-Estrategia-Brasileira-de-5G.pdf

Pedro, J. (2021). *O Impacto das Redes 5G na Segurança e Defesa Nacional*. Repositórios Científicos de Acesso Aberto de Portugal. https://www.rcaap.pt/detail.jsp?locale=pt&id=oai:comum.rcaap.pt:10400.26/38162

Sharma, P. Park, J. Park, J. & Cho, K. (2020). *Wearable Computing for Defence Automation: Opportunities and Challenges in 5G Network*. in IEEE Access, vol. 8, pp. 65993-66002, 2020, doi: 10.1109/ACCESS.2020.2985313.

Telebrasil 5G Brasil. (2018). *Ecossistema 5G Brasil: agentes*. https://5gbrasil.telebrasil.org.br/ecossistema/agentes

Telesintese. (2021). *Portal de Telecomunicações, Internet e TICs*. Apresentacao-da-Analise-do-5G-v04.pdf. https://www.telesintese.com.br/wp-content/uploads/2021/02/Apresentacao-da-Analise-do-5G-v04.pdf

VERDE OLIVA, Ano XL, Nº 217, Especial, Centro de Comunicação Social do Exército. (2012). SISFRON. *Sistema Integrado de Monitoramento de Fronteiras*. Páginas 13 a 19. https://pt.calameo.com/exercito-brasileiro/read/001238206bb7f4646da49

Wade, D. (2020). *5G network information technology and military information communication data services*. 2020. Kindle Edition.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 15/12/2021
Aceitação/Acceptance: 28/02/2022

Protocolos de Autenticação e Controle de Acessopara Aplicação das Forças Armadas e Orgãos de Segurança Pública em Redes Móveis 4G/LTE e 5G

Jose Ricardo[1], Ugo Dias[2]

ricardoferreiracmf@gmail.com; ugodias@gmail.com

[1] Departamento de Engenharia Elétrica, Graduação. Programa de Engenharia elétrica, Universidade de Brasília, Brasil, 70910-900

[2] Departamento de Engenharia Elétrica, Graduação. Programa de Engenharia elétrica, Universidade de Brasília, Brasil, 70910-900

Pages: 616-628

Resumo: As Forças Armadas do Brasil (FA), constituídas pela Marinha, pelo Exército e pela Força Aérea, são instituições nacionais, permanentes e regulares que têm como missão constitucional zelar pela defesa da Pátria, pela garantia dos poderes constitucionais e, por iniciativa destes, da lei e da ordem, nesse sentido necessitam de sistemas confiáveis com alta taxas de dados para a garantia do comando e controle dos elementos componentes da Força Terrestre. Por outro lado, os Órgãos de Segurança Pública compostos por agências policiais, corpos de bombeiros, esquadrões de resgate, serviços médicos de emergência e outras entidades são os principais responsáveis pela atuação em situações críticas, necessitam, portanto, de serviços de voz e dados com alto quality of service (QoS), confiabilidade e segurança. Assim, aumentando as capacidades de salvar vidas e controlar situações de risco. Dessa forma, ambos vem implementando a tecnologia de rede de acesso a longa distância, o 4G Long Term Evolution (LTE) e futuramente o 5G, permitindo uma rede com grande mobilidade e qualidade dos dados. Para garantir a segurança dessas comunicações é necessário um protocolo de segurança que possa garantir a segurança e confiabilidade dos serviços de comando e controle utilizados pelos órgãos de Segurança Pública. Nesse sentido, será analisado o protocolo de criptografia EPS-AKA, suas características e vulnerabilidades. Por fim, será apresentado os possíveis mecanismos de mitigação dessas vulnerabilidades para as redes 4G, além dos desafios para a evolução em redes 5G.

Palavras-chave: Forças Armadas; Órgãos de Segurança Pública; 4G LTE; 5G; protocolo EPS-AKA.

Authentication and Access Control Protocols for Application of the Armed Forces and Public Security Organs in 4G/LTE and 5G Mobile Networks

Abstract: The Armed Forces of Brazil (FA), are composed by the Navy, the Army and the Air Force, are national, permanent and regular institutions whose

constitutional mission is to ensure the defense of the Fatherland, the guarantee of constitutional powers and, on their initiative, of law and order, in this sense, need reliable systems with high data rates to guarantee the command and control of the component elements of the ground force. On the other hand, Public Security Bodies made up of law enforcement agencies, fire departments, rescue squads, emergency medical services and other entities are primarily responsible for acting in critical situations, therefore requiring voice and data rate with quality of service (QoS), reliability and security. Thus, increasing the capacities to save lives and control risk situations. In this sense, both have been implementing 4G LTE and in the future the 5G high-speed data access network technology, allowing a network with high mobility and high data rates. 4G LTE and in the future the 5G. To ensure the security of these communications, a security protocol is needed that can guarantee the security and reliability of the command and control services used by public security agencies. In this sense, the EPS-AKA encryption protocol, its characteristics and vulnerabilities will be analyzed. Finally, the possible mechanisms for mitigating these vulnerabilities for 4G networks will be presented, in addition to the challenges for the evolution in 5G networks.

Keywords: Armed Forces, Public security agencies, 4G LTE, 5G, EPS AKA protocol.

1. Introdução

As tecnologias de rede de acesso e comunicações móveis 4G e 5G, devido a suas particularidades, é vista como uma solução altamente promissora no sentido de atender os serviços de missão crítica, principalmente levando-se em consideração o grande fluxo de taxas de dados e um número muito grande de usuários. Assim, essa rede deverá garantir a interoperabilidade, confiabilidade, segurança e disponibilidade aos sistemas de comando e controle (C2) das Forças Armadas e dos Órgãos de Segurança Pública, Fiscalização, Repressão e Controle e Defesa Civil, nos níveis federal, estadual e municipal, e também a outros usuários de interesse do Estado Brasileiro, melhorando assim a Segurança Nacional, com reflexos diretos na Defesa Nacional. Possibilitando assim a ampliação do sistema, com redução dos custos, além de melhorar a gestão pública. Porém, essa tecnologia não foi projetada para cumprir os requisitos de confiabilidade, confidencialidade e autenticidade nos padrões exigidos em serviços de missão crítica.

Em redes 4 G LTE, o *Extensible Authentication Protocol* (EAP) é uma estrutura de autenticação, não um mecanismo de autenticação específico. EAP-AKA é um dos métodos de EAP que usa o mecanismo de autenticação e acordo de chave, *Authentication and Key Agreement* (AKA) com base em mecanismos de desafio-resposta. O EAP-AKA é usado nas redes móveis de 4ª geração (LTE) como mecanismo de Autenticação do Sistema de Pacotes Evoluído e Acordo de Chave (EPS-AKA). As vulnerabilidades do EPS-AKA são a divulgação da identidade do usuário, ataques *Man in the Middle* e ataques de negação de serviços (DoS).

Nesse contexto, se faz necessária uma análise das características dos sistemas de autenticação e controle de acesso à rede do protocolo EAP-AKA do Sistema de Comunicações Criticas 4G/LTE de modo a entender seu funcionamento, verificar as suas falhas e apontar soluções que possam ser utilizado por todos os órgãos de segurança

pública gerando, assim um alto grau de confiabilidade nesses sistemas de comunicações críticas. Possibilitando a utilização do sistema de comunicações 4G e 5G com todas as suas aplicações, como serviço de banda larga móvel garantindo os altos padrões de segurança exigidos pelas demandas dos Órgãos de Segurança Pública e Forças Armadas.

2. Trabalhos Relacionados

Foram analisados diversos trabalhos relacionados, os quais tratam de soluções para as vulnerabilidades do EPS-AKA.

Nos trabalhos (Cao J, Ma M, Li H, Zhang Y, Luo Z , 2014) e (Tsay J-K, Mjølsnes SF , 2012) os autores analisam a vulnerabilidade de divulgação do IMS que é uma das identificações do usuário. A vulnerabilidade ocorre quando o IMSI é transmitido em mensagens de paginação da rede para o usuário (Do MME para *eNodeBs* e da *eNodeB*s para UEs), a fim de localizar um UE específico (por exemplo, quando um UE recebe uma chamada). Em casos de handover entre MMEs, se ocorrer uma falha de sincronização, o novo MME ou o anterior solicita o IMSI do UE. Um invasor pode acionar um procedimento de *paging* sem alertar o usuário, farejar as mensagens de *paging* entre a rede e um UE para decodificá-las e adquirir o IMSI, ou espionar a conexão para capturar IMSIs. Para essa vulnerabilidade os autores apresenta, nos trabalhos (Abdo JB, Demerjian J, Ahmad K, Chaouchi H, Pujolle G, 2013) e (Li X, Wang Y, 2014), como solução a utilização de criptografia de chave pública para todas as mensagens entre o UE e a rede.

Nos trabalhos (Abdrabou MA, Elbayoumy ADE, El-Wanis EA, 2015) e (Park Y, Park T, 2007) os autores analisam a vulnerabilidade da divulgação do identificador temporário GUTI, o qual tem a função de proteção contra a divulgação de localização do UE, pode causar os mesmos problemas como divulgação IMSI. Utilização de um eNodeB falsa que finge ser legítima, operando com alta potência ela obriga o UEs a se conectar com ela, causando ataques man-in-themiddle (MitM). Ataques man-in-the-middle (MitM, em que o invasor se faz passar pela rede como legítimo UE). Para essa vulnerabilidade o autor apresenta no trabalho (Abdo JBB, Chaouchi H, Aoude M, 2012) e (Fouque P-A, Onete C, Richard B, 2016) como solução a utilização de criptografia de chave pública para todas as mensagens entre o UE a rede, inclusive a GUTI.

No trabalho (Shaik A, Borgaonkar R, Asokan N, Niemi V, Seifert J-P, 2015) o autor analisa a vulnerabilidade da divulgação do Av do UE, UE verifica o intervalo SQN após obter o AV da rede. Quando um UE malicioso envia um pedido várias vezes usando o IMSI de um UE, a quantidade de SQN aumenta de uma forma não contada pela rede. Então, quando o UE verdadeiro envia um pedido real para a rede, eles terão um intervalo SQN muito distante, assim o UE terá falha de sincronização. Para essa vulnerabilidade o autor apresenta, no trabalho (Shaik A, Borgaonkar R, Asokan N, Niemi V, Seifert J-P, 2015) como solução a utilização de criptografia de chave pública e assinatura digital.

Dessa forma os autores se preocuparam apenas com a segurança da troca de informações entre os componentes do sistema, não levando em consideração a necessidade de segurança orgânica e operacional. Isso se deve ao fato da análise feita pelas autores ser de sistemas de telefonia móvel de uso civil.

O objetivo desse trabalho é propor soluções para sistemas de telefonia móvel para aplicações de comunicações críticas. Nesse sentido procurou-se apresentar soluções que não foram propostas nos trabalhos pesquisados.

As soluções propostas por esse trabalho englobam segurança de acesso à rede, segurança no domínio da rede, segurança no domínio da aplicação.

3. Arquitetura das Redes 4G

3.1. Características Gerais do 4G

O 4G LTE é um sistema de telefonia celular de rede de acesso sem fio para longa distância. Os dispositivos iPhones, Black Berrys e dispositivos Android empregam a infraestrutura de telefonia 4G celular para enviar/receber e-mail, navegar na Web, tuitar e baixar música, enquanto se movimentam. Gerando assim trafego de dados com alta mobilidade com velocidades até 350 km/h.

3.2. Arquitetura da Tecnologia 4G LTE

A arquitetura 4G, apresentada na Figura 1, combina muitos componentes funcionais para garantir autenticação e controle de acesso (Cao J, Ma M, Li H, Zhang Y, Luo Z, 2014). Todos os componentes da rede têm o mesmo protocolo IP e se comunicam entre si por meio de uma rede IP típica (por meio de interfaces lógicas). Os principais componentes responsáveis pela autenticação e controle de acesso são o *User Equipment (*EU), *Evolved Node B* (ENodeB), *Home Subscriber Server* (HSS) e o *Mobility Management Entity* (MME). Cada um desses componentes da rede possuem atribuições bem definidas.

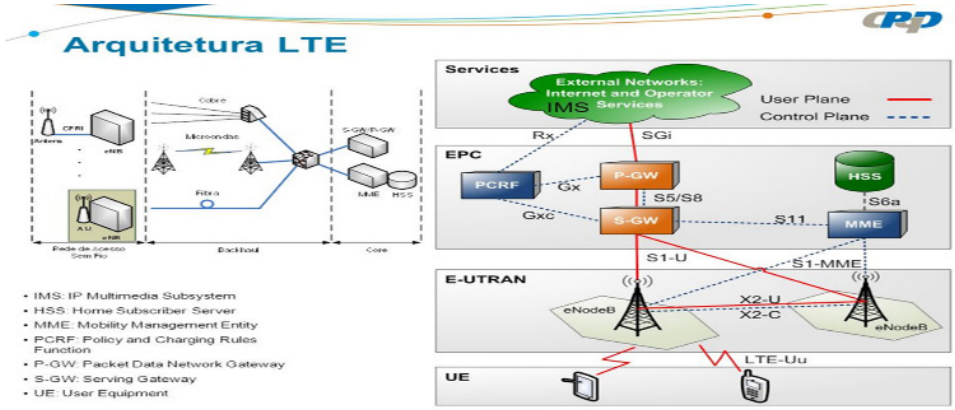


Figura 1 – Arquitetura da rede 4G LTE.

UE (user equipment): um dispositivo móvel que inclui um UICC (cartão de circuito integrado universal, um cartão SIM) integrado com o USIM (módulo de identidade do assinante universal), (Tsay J-K, Mjølsnes SF, 2012).

ENodeB (Evolved Node B): Consiste em uma antena e um conjunto de transceptores, é o principal componente da *Evolved Universal Terrestrial Radio Access Network* (EUTRAN), (Li X, Wang Y (2011).

MME (Mobility Management Entity): O principal nó de controle da rede (Abdrabou MA, Elbayoumy ADE, El-Wanis EA, 2015). O MME realiza a autenticação, rastreamento das localizações da UE e pela seleção dos gateways (decidindo os caminhos dos pacotes de dados).

HSS (Home Subscriber Server): É um servidor de dados que armazena os dados do assinante (incluindo suas identidades, direitos e perfis de assinatura) e as chaves secretas (Park Y, Park T, 2007).

S-GW (Serving Gateway): ancora o portador de dados e roteia pacotes de dados para o UE.

P-GW (Packet Data Network Gateway): conecta à rede central do pacote às redes externas, como a Internet, e fornece endereços IP para a UE.

4. Características e Tipos de Serviços de Missões Críticas com 4G LTE 5G

As Comunicações Críticas são sistemas de comando e controle (C2) que se utilizam de infraestruturas, fixas ou móveis, com elevada capacidade de sobrevivência e que geram áreas de cobertura, nas quais grupos de conversação definidos previamente dispõe de comunicações, de voz e dados, com possibilidade de enlaces ponto a ponto, com elevadas disponibilidade, confiabilidade e segurança, cuja principal característica é a capacidade de prover os serviços de missão crítica em prol do cidadão. Eles são usualmente chamados de Proteção Pública e Socorro a Desastres (PPDR, na sigla em inglês), tanto na Defesa, Segurança Pública, Defesa Civil, Fiscalização, Repressão e Controle. Para as Forças Armadas, tem como características operar em locais isolados, fronteiras com Área Rural, longe de centros urbanos, onde é comercialmente inviável a cobertura de operadoras comerciais. Os principais serviços requeridos para a aplicação 4G LTE para esses órgãos são os seguintes:

Aplicativos de comando e controle com comunicação IP: Eles permitem que grandes números de serviços sejam fornecidos, como, por exemplo, *streaming* de vídeo e comunicação de voz (PTT e VoIP) em tempo real (Fouque P-A, Onete C, Richard B, 2016).

Interoperabilidade entre rede de rádio APCO 25 e 4G LTE: Plataforma de interoperabilidade integra redes de rádio comunicação e redes LTE para entregar serviços unificados pareando voz missão crítica com banda larga e aplicações multimídia. Viabilizando a convergência de tecnologias, e a convivência de serviços existentes e serviços emergentes intensivos em dados sobre uma mesma infraestrutura, possibilitando, desta forma, uma transição suave para o LTE (Shaik A, Borgaonkar R, Asokan N, Niemi V, Seifert J-P, 2015). No caso específico das Forças Armadas, é utilizado o servidor *wave* como plataforma de interoperabilidade para entregar as redes 4G LTE e a rede APCO 25, apresentado na Figura 2.

Mobilidade em operações táticas: Podem ser utilizadas plataformas móveis veiculares como apoio táticos, com possibilidade de prover temporariamente cobertura em uma determinada região que necessite de comunicação crítica fornecendo aplicações de voz em grupo, videoconferência, vídeo em tempo real, utilização de aplicativos de comando e controle como o pacificador que apresenta em uma carta digital a posição dos usuários do sistema em tempo real.

Atuação em locais isolados*:* Fronteiras com Área Rural, longe de centros urbanos onde é comercialmente inviável a cobertura de operadoras celulares comerciais com soluções fixas, móveis e portáteis.

Gerenciamento e operação: Gerenciamento centralizado de performance de missão crítica e indicadores de disponibilidade otimizados modelos de chamadas através de redes de rádio.

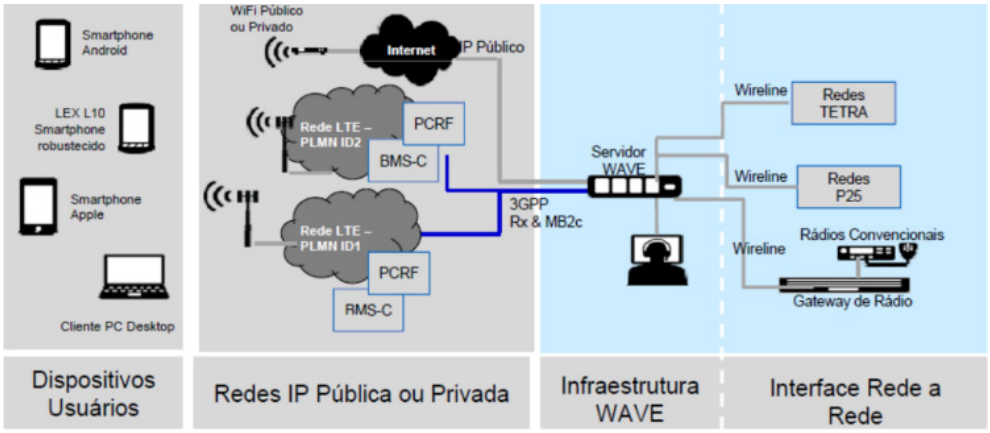


Figura 2 – Interoperabilidade entre rede de rádio APCO 25 e 4G LTE.

5. Princípios de Segurança de Redes Aplicados a Segurança Pública

Podemos identificar os princípios da comunicação segura que são desejáveis para as comunicações normais e obrigatórias para as comunicações críticas utilizadas pelas FA e órgãos de segurança pública.

Confidencialidade: Apenas o remetente e o destinatário pretendido poderão entender o conteúdo da mensagem transmitida. O fato de intrusos conseguirem interceptar a mensagem exige, necessariamente, que esta seja cifrada de alguma maneira para impedir que seja entendida por um interceptador.

Integridade de mensagens: O remetente e o destinatário querem assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão.

Autenticação do ponto final: O remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação, confirmar que a outra parte é de

verdade quem alega ser. A comunicação pessoal entre seres humanos resolve facilmente esse problema por reconhecimento visual.

Segurança Operacional: Hoje quase todas as organizações (empresas, universidades etc.) possuem redes conectadas à Internet pública. Essas redes podem ser comprometidas por atacantes que ganham acesso a elas por meio da Internet pública. Os atacantes podem tentar colocar *worms* nos hospedeiros na rede, adquirir segredos corporativos, mapear as configurações internas da rede e lançar ataques de *DoS*. Os mecanismos operacionais, como firewalls e sistemas de detecção de invasão, são usados para deter ataques contra a rede de uma organização. Um firewall localiza-se entre a rede da organização e a rede pública, controlando os acessos de pacote de e para a rede. Um sistema de detecção de invasão realiza uma "profunda inspeção de pacote", alertando os administradores da rede sobre alguma atividade suspeita.

O sistema de redes utilizadas pelos órgãos de Segurança Pública e Forças Armadas devem possuir tais requisitos, impedindo o monitoramento identificação, acesso, gravação, modificação, inserção ou eliminação de mensagens ou conteúdo de mensagens.

6. Princípios do Protocolo de Segurança AKA

Na rede LTE, o protocolo EPS-AKA é usado como um mecanismo de autenticação entre o UE (através de seu cartão SIM) e a rede, onde o *Extensible Authentication Protocol* (EAP) é uma estrutura de autenticação, não um mecanismo de autenticação específico, proporcionando o transporte e o uso de material de chave e parâmetros gerados por métodos EAP (3GPP Security Architecture, 2017). O EAP-AKA é um dos métodos do EAP que usa o mecanismo de autenticação e acordo de chave (AKA) baseada em mecanismos de desafio-resposta e criptografia de chave simétrica, fornecendo autenticação automática (rede autentica o UE e o UE autentica a rede servidora), (3GPP Security Architecture, 2017). Os parâmetros de autenticação e controle de acesso trocados entre a rede servidora e o UE trafegam em claro, não sendo protegidos por nenhum tipo de criptografia. A figura 3 descreve esse procedimento.

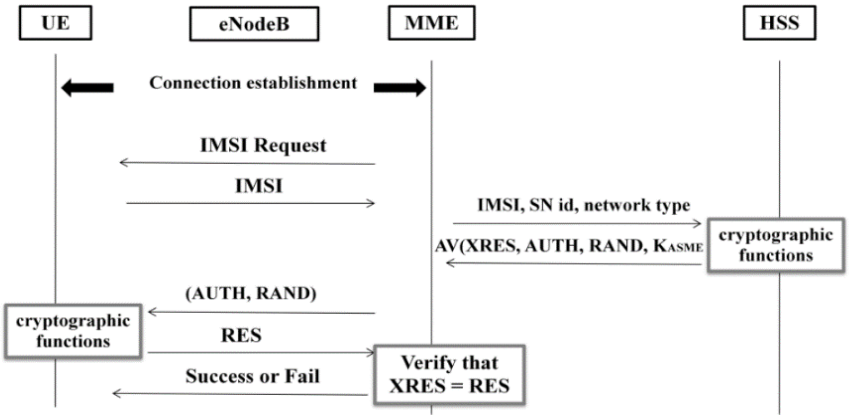


Figura 3 – Autenticação do protocolo EPS-AKA.

O procedimento de autenticação começa após o estabelecimento da conexão entre UE e MME como segue (Forsberg D, Horn G, Moeller W-D, Niemi V, 2012) e (Abdrabou MA, Elbayoumy ADE, El-Wanis EA , 2015):

MME envia um pedido de ID ao UE via eNB.

UE respondem por IMSI.

MME solicita um vetor de autenticação EPS (AV) do HSS, com base no IMSI, o HSS procura a chave K e um número de sequência associado a esse IMSI, o AuC aumenta o SQN e gera um desafio aleatório (RAND) ao lado do mestre chave K como entrada para funções criptográficas e gera AV, este AV consiste em: XRES, AUTN, KASME e RAND.

HSS/AuC envia o AV para o MME, o MME mantém o KASME e o XRES, mas encaminha o RAND e o AUTN para a UE.

Tanto o RAND quanto o AUTN são enviados ao UE para calcular sua própria versão do AUTN usando sua própria chave K e SQN e compará-lo com o AUTN recebido do MME, para fazer o usuário autenticar a rede, se o UE corresponder, calcular RES usando funções criptográficas com a tecla K e o RAND. Também calcula CK e IK.

Envia o RES de volta ao MME, o MME autentica o terminal verificando se o RES é igual a XRES. Isso conclui a autenticação mútua. O UE então usa o CK e o IK para calcular o KASME da mesma maneira que o HSS. Então tanto UE quanto MME agora têm a mesma chave KASME.

Em seguida, o MME envia para a UE o processo de autenticação de sucesso ou falha.

7. Vulnerabilidade do Protocolo AKA

A primeira vulnerabilidade, Divulgação da identidade do usuário: É causada quando o UE se registra na rede pela primeira vez, tendo em vista que o UE transmite IMSI em texto claro. Assim, o invasor pode capturar o IMSI como mostrado na Figura 4. O invasor pode personificar o UE depois e enviar o IMSI para o MME para obter algumas informações.



Figura 4 – Divulgação da identidade do usuário.

A segunda vulnerabilidade, Ataque Man In The Middle (MITM): É aquela em que o invasor obtém o IMSI do UE e, em seguida, tenta se registrar com BS genuíno por este IMSI, em seguida, a rede envia RAND e AUTN (Fouque P-A, Onete C, Richard B ,2016). O invasor se desconecta quando esses parâmetros são recebidos. Depois disso, o UE genuíno se registra com um BS falso enviando o RAND e o AUTN original e fazendo com que ele calcule RES conforme mostrado na Figura 5.

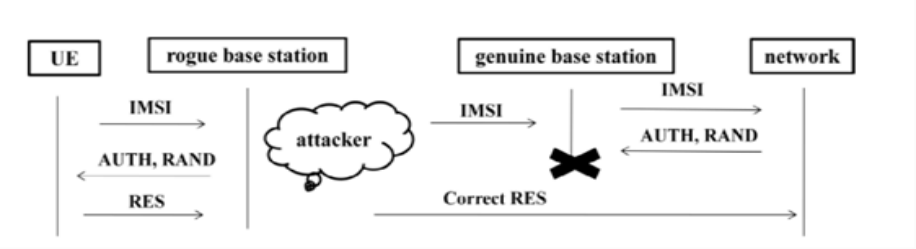


Figura 5 – Ataque MITM.

A terceira vulnerabilidade, Ataque de negação de serviços (DoS): Aparece uma vez que o MME gerencia vários eNBs na arquitetura LTE plana, as estações base nas redes LTE são mais suscetíveis aos ataques em comparação com aquelas na arquitetura UMTS, onde a rede servidora no UMTS apenas gerencia alguns RNCs de forma hierárquica. Uma vez que um adversário compromete a estação base, ele pode colocar ainda mais em perigo toda a rede devido à natureza totalmente IP do LTE (Forsberg D, Horn G, Moeller W-D, Niemi V, 2012). O adversário pode lançar ataques DoS ao HSS e ao MME.

8. Possíveis Soluções para a Segurança dos Serviços de Comunicações Críticas no Protocolo AKA

A primeira vulnerabilidade, Divulgação da identidade do usuário: É causada quando o UE se registra na rede pela primeira vez, tendo em vista que o UE transmite IMSI em texto claro (Agrawal, “Heterogeneous networks, 2009). Assim, o invasor pode capturar o IMSI como mostrado na Figura 6. O invasor pode personificar o UE depois e enviar o IMSI para o MME para obter algumas informações.



Figura 6 – Divulgação da identidade do usuário.

A segunda vulnerabilidade, Ataque Man In The Middle (MITM): É aquela em que o invasor obtém o IMSI do UE e, em seguida, tenta se registrar com BS genuíno por este IMSI, em seguida, a rede envia RAND e AUTN (Cao J, Ma M, Li H, Zhang Y, Luo Z, 2014). O invasor se desconecta quando esses parâmetros são recebidos. Depois disso, o UE genuíno se registra com um BS falso enviando o RAND e o AUTN original e fazendo com que ele calcule RES conforme mostrado na Figura 7.

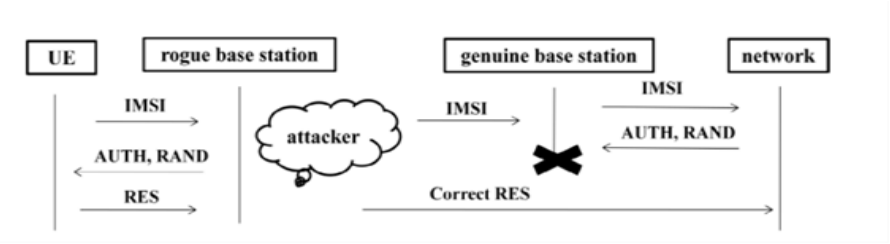


Figura 7 – Ataque MITM.

A terceira vulnerabilidade, Ataque de negação de serviços *(DoS)*: Aparece uma vez que o MME gerencia vários eNBs na arquitetura LTE plana, as estações base nas redes LTE são mais suscetíveis aos ataques em comparação com aquelas na arquitetura UMTS, onde a rede servidora no UMTS apenas gerencia alguns RNCs de forma hierárquica. Uma vez que um adversário compromete a estação base, ele pode colocar ainda mais em perigo toda a rede devido à natureza totalmente IP do LTE (Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo, 2014). O adversário pode lançar ataques DoS ao HSS e ao MME.

9. Possíveis Soluções para a Segurança dos Serviços de Comunicações Críticas no Protocolo AKA

Um recurso de segurança de redes de comunicações críticas é um recurso de serviço que atende a um ou vários requisitos de segurança. Um mecanismo de segurança é um elemento usado para realizar um recurso de segurança. Todos os recursos e mecanismos de segurança formam a arquitetura de segurança. Um exemplo de um recurso de segurança é a confidencialidade dos dados do usuário. O 3GPP classifica o recurso de segurança na rede LTE em cinco grupos, conforme segue:

Segurança de acesso à rede: o conjunto de recursos de segurança que fornecem aos usuários acesso seguro aos serviços 4G e que, em particular, protegem contra ataques no link de acesso rádio, pode ser implementada com a utilização de criptografia de chave pública. Sendo essa utilizada para criptografar as mensagens de autenticação entre o usuário e a rede, impedindo assim, a divulgação do IMS.

Segurança de domínio de rede: o conjunto de recursos de segurança que permitem que os nós no domínio do provedor troquem dados de sinalização com segurança e protejam contra ataques na rede fixa.

Segurança de domínio do usuário: o conjunto de recursos de segurança que protegem o acesso a estações móveis.

Segurança do domínio do aplicativo: o conjunto de recursos de segurança que permite que os aplicativos do usuário e do domínio do provedor troquem mensagens com segurança.

Visibilidade e configurabilidade da segurança: o conjunto de recursos que permite informar ao usuário se um recurso de segurança está em operação.

10. Desafios de Autenticação e Controle de Acesso para Implementação de Redes 5G

O 5G possui a capacidade de implementar os mesmos serviços que o 4G LTE para as Forças Armadas e os Órgãos de Segurança Pública. Além disso, devido as suas características como baixa latência, alta taxas de dados, maior, acessibilidade e conectividade para um número muito grande de usuários e suporte a serviços de *Internet of Things* (IoT) irá aumentar a qualidade dos serviços assim como o aumento do número de dispositivos conectados por quilometro quadrado, apoiando as operações com grande concentração de usuários. Por outro lado, coexiste uma maior necessidade de segurança do sistema, e os requisitos de segurança específicos do serviço devem ser considerados ao projetar a autenticação adequada e mecanismos de controle de acesso para redes 5G com procedimentos de autenticação AKA rápidos. Nesse contexto, duas soluções vem para tentar diminuir esse problema de segurança nas redes 5G. A primeira é o fatiamento de rede, que é uma solução para atender a requisitos de tipos de serviços diferentes em uma mesma rede física. É uma divisão lógica, com várias camadas, de uma rede física. Cada camada física de rede é dividida por várias funções de rede para fornecer recursos específicos atendendo um tipo específico de uso. Diferentes tecnologias como o *Software defined Network* (SDN) e *Network Function Virtualization* (NFV) serão usadas para implantar o fatiamento. A segunda é o controle de acesso à rede heterogênea o que propicia a garantia de acesso de várias tecnologias a uma rede 5G. Ela possibilita que provedores de acesso não 3rd *Generation Partnership Project* (3GPP) e tenham seus próprios servidores *Authentication, Authorization and Accounting* (AAA), e realizem o gerenciamento da conexão entre diferentes servidores AAA, especialmente em cenários de roaming, protegendo a rede contra o acesso não autorizado nesta infraestrutura heterogênea.

11. Conclusão

As Forças Armadas e os Órgãos de segurança Públicas ao aplicarem os serviços da tecnologia 4G e 5G obterão um aumento significativo na eficiência da sua atribuição constitucional de Garantia e manutenção da paz social. Além disso, o uso compartilhado

dessa tecnologia possibilitará redução de custos de implantação gerando economicidade para os gastos públicos. Nesse sentido, esses serviços proporcionados pelo 4G e 5G deverão prover um nível maior de segurança e confiabilidade, por outro lado, o protocolo de autenticação e controle de acesso EPS-AKA da tecnologia 4G é vulnerável a vários tipos de ataque como, por exemplo, a divulgação do IMSI, ataque *Man In The Middle* (MITM) e ataque de negação de serviços (DoS).

Essas vulnerabilidades fazem com que os serviços necessários a demanda de alta taxa de dados dos Órgãos de Segurança Pública e Forças Armadas não possuam confiabilidade exigida por esses sistemas. Nesse contexto, é necessário adotar soluções de segurança a redes 4G e o 5G, tais como segurança de acesso à rede, segurança de domínio de rede, segurança de domínio do usuário e segurança do domínio do aplicativo que possam garantir essa confiança e segurança, de modo que seja possível a utilização da rede por um grande número de usuários com tráfego de dados de alta capacidade sem prejuízo aos usuários.

A partir do estabelecimento de um alto nível de segurança nas redes 4G e 5G os serviços de aplicativos de comando e controle com comunicação IP irão garantir as trocas de informações entre os diversos usuários do sistema. Além disso proporcionaram interoperabilidade entre rede de rádio APCO 25 e 4G LTE. Por outro lado, permitirá a operação e conexão dos usuários em operações táticas atuando em locais isolados.

Por fim, a possibilidade de gerenciamento remoto das operações utilizando redes 4 G e 5G seguras dotaram os comandantes da operação de ampla consciência situacional aumentando a probabilidade de sucesso de operações das Forças Armadas e os Órgãos de Segurança Pública.

Em síntese, a combinação dos recursos de segurança na rede, aliada a metodologias bem aplicadas de segurança operacional poderão garantir a confiabilidade do sistema, assim como o sucesso da utilização dos serviços de banda larga providos pela rede 4G e o 5G para os Órgãos de Segurança Pública e Forças Armadas.

Referências

A. Agrawal, “Heterogeneous networks: A new paradigm for increasing cellular capacity,” Qualcomm, Jan. 29, 2009. [Online]. Available: http://netseminar.stanford.edu/seminars/, accessed on Jan. 20, 2015.

Abdo JBB, Chaouchi H, Aoude M (2012) Ensured confidentiality authentication and key agreement protocol for EPS. In: Broadband Networks and Fast Internet (RELABIRA), 2012 Symposium on, pp 73–77

Abdo JB, Demerjian J, Ahmad K, Chaouchi H, Pujolle G (2013) EPS mutual authentication and crypt-analyzing SPAKA. In: Computing, Management and Telecommunications (ComManTel), 2013 International Conference on, pp 303–30

Abdrabou MA, Elbayoumy ADE, El-Wanis EA (2015) LTE authentication protocol (EPS-AKA) weaknesses solution. In: Intelligent Computing and Information Systems (ICICIS), 2015 IEEE Seventh International Conference on, pp 434–441

Abdrabou MA, Elbayoumy ADE, El-Wanis EA (2015) LTE authentication protocol (EPS-AKA) weaknesses solution. In: Intelligent Computing and Information Systems (ICICIS), 2015 IEEE Seventh International Conference on, pp 434–441

B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed, Extensible Authentication Protocol (EAP), RFC 3748, 2004

Cao J, Ma M, Li H, Zhang Y, Luo Z (2014) A survey on security aspects for LTE and LTE-A networks. IEEE Commun Surv Tutorials 16(1):283–302.

Chunyu Tang, David A. Neumann, and Susanne Wetzel, Analysis of authentication and key establishment in inter-generational mobile telephony 2013.

Fouque P-A, Onete C, Richard B (2016) Achieving better privacy for the 3GPPAKA protocol, IACR Cryptology ePrint Archive, vol 2016, p 480

Fang-Yie Leu, IIsun You, Yi-Li Huang, Kangbin Yim, Cheng-Ru Dai1, Improving Security Level of LTE Authentication and Key Agreement Procedure, 2012.

Forsberg D, Horn G, Moeller W-D, Niemi V (2012) LTE security. Wiley

Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo, A Survey on Security Aspects for LTE and LTE-A Networks, 2014.

Li X, Wang Y (2011) Security enhanced authentication and key agreement protocol for LTE/SAE network. In: Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, pp 1–4

Park Y, Park T (2007) A survey of security threats on 4G networks. In: Globecom Workshops, 2007 IEEE, pp 1

Shaik A, Borgaonkar R, Asokan N, Niemi V, Seifert J-P (2015) Practical attacks against privacy and availability in 4G/LTE mobile communication systems, arXiv preprint arXiv:1510.07563

Tsay J-K, Mjølsnes SF (2012) A vulnerability in the umts and lte authentication and key agreement protocols. In: International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, pp 65–76

Universal Mobile Telelecommunications System (UMTS); LTE; Mission Critical Push to Talk (MCPTT) Over LTE; Stage 1, Version 13.3.0 Release13,document3GPPTS22.179,3rdGenerationPartnershipProject (3GPP), Jan. 2016

3GPP (2017) Security Architecture, TS 33.102, Tech. Spec. 14.1.0

3GPP (2017) Network Architecture,TS23.002, Tech.Spec.14.1.0[13] Cao J, Ma M, Li H, Zhang Y, Luo Z (2014) A survey on security aspects for LTE and LTE-A networks. IEEE Commun Surv Tutorials 16(1):283–302

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 22/10/2021
Aceitação/Acceptance: 12/01/2022

Metodología para la detección de minería ilegal mediante el uso de imágenes de radar Sentinel como herramienta para la defensa y seguridad del territorio: Caso de estudio Río Quito, Chocó

Jonathan Sandoval[1], Luis Castillo[2], Erika Upegui[2]

jssandovall@correo.udistrital.edu.co; esupeguic@udistrital.edu.co

[1] Maestría en Ciencias de la Información y las Comunicaciones, Grupo GEFEM, Universidad Distrital Francisco José de Caldas, Bogotá D.C., Carrera 7 No. 40B - 53, 110231, Bogotá D.C., Colombia.

[2] Ingeniería Catastral y Geodesia, Grupo GEFEM, Facultad de Ingeniería, Universidad Distrital Francisco José de Caldas, Carrera 7 No. 40B - 53, 110231, Bogotá D.C., Colombia.

Pages: 629-642

Resumen: Una de las principales características de las imágenes capturadas por radares de apertura sintética (SAR) es la posibilidad de ser generadas casi que en cualquier condición climática permitiendo de esta manera extraer información de la superficie terrestre en zonas con predominante presencia de nubes. En este trabajo se desarrolló una metodología para la detección de minería ilegal mediante el uso de imágenes de radar Sentinel sobre un área en el territorio colombiano históricamente afectada por minería ilegal y con presencia predominante de nubes a lo largo del año, ubicada en el municipio de Río Quito en el departamento Chocó - Colombia. Se empleó la técnica de clasificación supervisada usando el método de máxima verosimilitud involucrando características de textura obteniendo un coeficiente kappa de 0.82 y una exactitud global de 89%. La implementación de la metodología demostró el gran potencial de involucrar imágenes provenientes de sensores activos en la identificación del fenómeno de minería ilegal en la zona de estudio.

Palabras-clave: Sentinel; Radar de Apertura Sintética (SAR); textura, minería ilegal; clasificación supervisada.

Methodology for the detection of illegal mining through the use of Sentinel radar images as a tool for the defense and security of the territory: Case study Río Quito, Chocó

Abstract: One of the main characteristics of the images captured by synthetic aperture radars (SAR) is the possibility of being generated in almost any climatic condition, thus allowing information to be extracted from the earth's surface in areas with a predominant presence of clouds. In this work, a methodology was developed for the detection of illegal mining through the use of Sentinel radar images over an area in the Colombian territory historically affected by illegal

mining and with the predominant presence of clouds throughout the year, located in the municipality of Quito River in the department of Chocó. The supervised classification technique was used using the maximum likelihood method involving texture characteristics, obtaining a kappa coefficient of 0.82 and an overall accuracy of 89%. Implementation of the methodology demonstrated the great potential of involving images from active sensors in the identification of the phenomenon of illegal mining in the study area.

Keywords: Sentinel; Synthetic Aperture Radar (SAR); texture, illegal mining; supervised classification.

1. Introducción

En los últimos años, la minería ha desempeñado un papel significativo en el desarrollo económico y social de las regiones con vocación minera de Colombia debido al gran potencial geológico del país, el cual abre la posibilidad de realizar una amplia y variada explotación de productos de gran interés económico como el carbón, grava, arena, arcilla, níquel, cobre, hierro, esmeraldas, plata y oro, entre otros (Rojas Villarraga, 2021).

En Colombia, el oro desempeña un rol importante en el crecimiento del sector minero energético, ya que, aunque no es el mineral principalmente explotado, su producción se incrementó de 37,5 toneladas en el 2019 a 47,8 toneladas para el 2020; año en el cual se presentó el precio históricamente más alto con valores aproximados de US $2.100 dólares la onza para el mes de agosto del 2020 (Oficina de las Naciones Unidas Contra la Droga y el Delito - UNODC, 2021)

Según Guiza Suarez (2014) el 66% de la actividad minera que se ejecuta en Colombia se realiza sin contar un título minero y en cuanto a la minería aurífera, el 87% se realiza de manera ilegal, conformada principalmente por minas de pequeña y mediana extensión, con un aproximado de 6811 pequeñas minas y 2173 minas de mediana extensión.

De acuerdo a lo anterior, y considerando las cifras expuestas por Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC, 2021), el territorio colombiano con evidencias de explotación de oro de aluvión se incrementó en cerca de un 28% durante el periodo de tiempo del 2014 al 2020, aumentando de 78,939 hectáreas a 100,752 hectáreas, de las cuales cerca de la mitad se desarrollan en zonas excluidas de actividad minera, por encontrarse en zonas de conservación y protección ambiental en las cuales no está autorizada la actividad de explotación.

Briceño (2013) sugiere que esta actividad ha pasado inadvertida y ha sido poco intervenida en comparación con otros fenómenos de seguridad como el narcotráfico, secuestro, hurto o extorsión, pese a que esta actividad ilegal genera una mayor cantidad de recursos en comparación con otras actividades ilícitas y criminares, produciendo un significativo porcentaje de violencia asociada a las actividades de los grupos armados ilegales.

En Colombia, si bien, dicha actividad ilegal representó un 80% de la explotación aurífera en los departamentos de Valle del Cuca, Cauca, Nariño y Córdoba durante el periodo comprendido entre el año 2019 y el primer semestre del año 2020, las cifras son relativamente mucho mayores en los departamentos de Antioquia y Chocó, los cuales son los departamentos más afectas por esta peligrosa actividad (Oficina de las Naciones

Unidas Contra la Droga y el Delito - UNODC, 2021) y además cuentan con condiciones topográficas y meteorológicas muy particulares.

De acuerdo con Rueda y Poveda (2006) la ubicación geográfica del departamento del Chocó genera una alta presencia de nubosidad por cuenta de las corrientes superficiales que penetran al interior del país, debido a los vientos trans-ecuatoriales que golpean sobre el Océano Pacífico y obtienen una trayectoria en sentido de oeste a este, lo cual ha resultado ser una gran dificultad y limitante para aplicar técnicas de teledetección mediante el uso de imágenes ópticas (Quejada, 2019; Riveros, 2020; Perea et al., 2022).

Una imagen pude considerarse desde un punto de vista físico como una distribución de energía electromagnética independientemente del tipo de sensor utilizado en su captura (Ormeño, 2006). Sin embargo, se puede definir como una matriz digital que es capturada por un sensor ubicado en un satélite que órbita alrededor de la tierra colectando la energía reflejada por los elementos de la superficie terrestre (Martínez & Díaz, 2005). De acuerdo con la definición de Lira (2018) las imágenes satelitales de Radar son aquellas que son capturadas en el rango del espectro electromagnético correspondiente al microondas, cuyas longitudes de onda oscilan entre los 0.3 mm y los 100 cm, siendo de esta manera las longitudes de ondas más amplias utilizadas en teledetección (Canada Centre for Remote Sensing, 2001), estas son generalmente monoespectrales no obstante es posible capturarlas en diferentes longitudes de onda y polarizaciones.

Un sistema de radar se fundamente en el cálculo del tiempo de retorno de una señal emitida y retro dispersada con la intensión de determinar a qué distancia de la antena que emite dicha señal, se encuentra el objeto detectado, para de esta manera cuantificar las características físicas del objeto como por ejemplo su tamaño y textura (Hanssen, 2001). Una de las ventajas más significativas de colectar imágenes de Radar es que se permite capturar información sin depender de las condiciones atmosféricas de la zona al momento de la captura e incluso sin importar la cobertura de nubes (Hernandéz, 2014) lo cual hace de este tipo de imágenes una herramienta ideal para obtener información en zonas como las que presenta esta problemática y la zona estudio.

Por otro lado, el término textura es usado para caracterizar la rugosidad que ostenta la superficie de un elemento o fenómeno, siendo este un descriptor usado con bastante frecuencia en los métodos de procesamiento digital de imágenes y reconocimiento de patrones (Cámara, 2005). En términos generales, la textura da cuenta de la posible rugosidad o suavidad de una región, destacando el contraste espacial presente en los diferentes elementos que la conforman (Belmonte & Caamaño, 2009). Así, al analizar una imagen satelital, la textura se interpreta como la cuantificación de la variación espacial de valores de tono (Cámara, 2005), esta variación emana de la relación que existe entre la resolución propia del sensor y el tamaño de los elementos presentes en dicha imagen; lo cual implica que la identificación de un elemento cuya superficie en la imagen sea menor a 2 mm^2 deba realizarse a través de la variabilidad espacial que genera, debido a que su discriminación visual no es posible (Chuvieco, 1995).

De acuerdo con Rees (2005) es posible definir la clasificación de imágenes satelitales como el segmento de la teledetección en la cual por medio de los datos presentes en la imagen se toman decisiones. Dicho proceso de clasificación radica en categorizar los niveles digitales continuos detectados por los sensores de manera tal que cada píxel

que forma la imagen es asignado a una clase, las cuales pueden representar distintos tipos de coberturas (Arango et al., 2005). Algunas aproximaciones a estas técnicas se encuentran en trabajos como el de Killeen y su equipo (2005) quienes realizan la estratificación de la vegetación y el cambio de uso de suelo en los Yungas y Alto Beni en donde vincularon imágenes capturadas en banda L del radar JERS como insumo para definir regímenes hídricos para identificar zonas inundables. El trabajo de Carvalho y su equipo (2010) quienes caracterizaron los gradientes de vegetación en una zona de sabana, usando imágenes de radar provenientes del satélite ALOS/PALSAR. Más recientemente se encuentra el proyecto de Arantzazu, (2016) que clasifica cultivos a partir de observaciones de teledetección radar en zonas de secano y regadío mediante el uso de imágenes de radar satelital provenientes de la constelación ERS-2, ENVISAT y RADARSAT-2 (banda C) y ALOS/PALSAR (banda L) para la comunidad de Navarra. En este trabajo, el autor realiza la comparación de los resultados obtenidos a partir de imágenes ópticas y de imágenes de radar. Posteriormente, Valencia y Upegui (2020) realizan una propuesta metodológica para generar mapas de cobertura de la tierra a partir de imágenes de radar ALOS/PALSAR: Estudio de caso Mompós, Colombia. En 2021, Chamorro propone la metodología para determinar áreas afectadas por minería ilegal usando imágenes satelitales ópticas PlanetScope en el municipio del Bagre ubicado en el departamento de Antioquia en Colombia

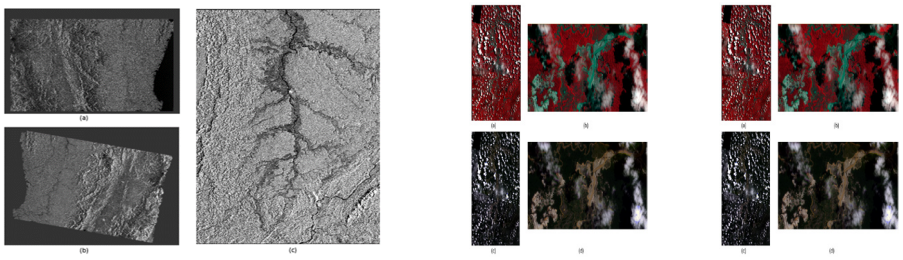
Este trabajo tiene como objetivo proponer una metodología para la detección de minería ilegal, empleando como insumo imágenes de Radar (de la constelación Sentinel) y aplicando técnicas de clasificación de imágenes apoyados en las características de textura de esta cobertura. Tomando como caso de estudio una zona ubicada en el municipio de Río Quito del departamento de Chocó en Colombia, al ser este departamento una de las zonas más afectadas por esta actividad en Colombia, el cual es afectado por una alta presencia de nubosidad durante gran parte del año. El resultado permitirá ser usado como herramienta para la defensa y seguridad del territorio.

2. Materiales y métodos

2.1. Zona de estudio

La zona seleccionada corresponde al municipio de Río Quito, ubicado en el departamento de Chocó (Colombia). Tiene una extensión territorial de 70 Km2, ubicado en el centro del departamento del Chocó en la denominada subregión del Atrato a 30km de la capital del departamento por vía fluvial. Para el censo de 2015 reportaba 8961 habitantes. Sus principales fuentes de ocupación son la minería, la agricultura, la pesca y explotación maderera.

Para el desarrollo del proyecto se cuenta con una imagen Sentinel 1 (figura 1a) capturada en modo Interferometric Wide Swath del 07 de marzo de 2022. Este modo de toma cubre una franja de 250 km brindando una resolución espacial de 5 metros por 20 metros (Agencia Espacial Europea - ESA, 2022). Igualmente, para la fase de entrenamiento y la validación se tiene un mosaico óptico generado a partir de imágenes PlanetScope capturadas entre el 17 y el 23 de abril de 2022. El mosaico tiene 4 bandas (azul, verde, rojo, infrarrojo cercano) permitiendo tener una visualización en verdadero color (Figura 1b) como falso color estándar (Figura 1c); la resolución espacial es de 3 metros.



a) b) c)

Figura 1 – Datos disponibles a) Imagen de radar sin procesamiento, b) Imagen en verdadero color c) Imagen en falso color estándar

El software utilizado para el procesamiento corresponde a SNAP desarrollado por la Agencia Espacial Europea publicado bajo la licencia GPL-3 y sus fuentes están disponibles en GitHub.

2.2. Metodología propuesta

Este trabajo propone una metodología compuesta de 5 fases como se presenta en la figura 1. Para su construcción se analizaron experiencias de investigaciones elaboradas con anterioridad para diferentes aplicaciones en las cuales se incluyeron imágenes de radar para elaborar la clasificación de algún tipo específico de cobertura o se efectuó la identificación de minería ilegal usando imágenes satelitales ópticas.

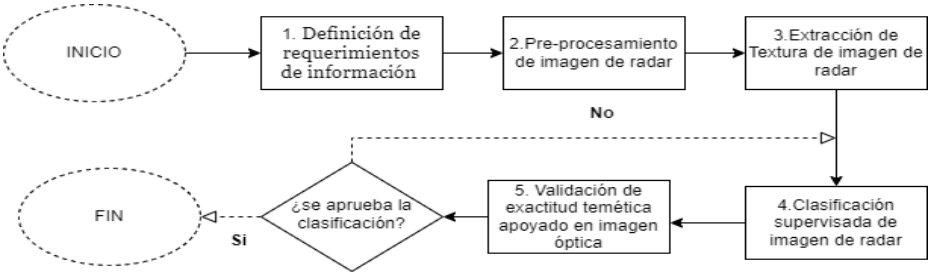


Figura 2 – Flujo de trabajo de las fases de la metodología desarrollada

2.2.1. Fase 1: Definición de requerimientos de información

En esta fase se realiza el proceso de identificación de requerimientos de información, seleccionando la fuente de imágenes satelitales (radar y ópticas) a usar tanto para los procesos de clasificación como validación. El proceso de selección de imágenes se realizó mediante el análisis de dos (2) dimensiones tanto para las imágenes de radar como para las imágenes ópticas; los satélites sobre los cuales se analizaron estas dimensiones fueron seleccionados con base en las imágenes usadas en las investigaciones tomadas

como referencia (Arantzazu, 2016), (Carvalho et al., 2010), (Killeen et al., 2005), (Evans & Costa, 2013), para la generación de esta metodología y su importancia en la industria.

Las dimensiones analizadas son en primer lugar, el aspecto técnico en el cual se evaluaron las características propias de cada constelación y los productos que son puestos a disposición por los operadores de estas, y en segundo lugar el acceso efectivo a la imagen.

2.2.2. Fase 2: Pre-procesamiento de imagen radar

En esta fase se realiza el pre-procesamiento de la imagen de radar por medio de cuatro procesos, a saber: calibración radiométrica; reducción de speckle; ortorectificación; y recorte.

1. *Calibración radiométrica:* Con este proceso se busca garantizar que los valores que presenta cada píxel que conforman la imagen de radar sean valores de la retrodispersión del radar sobre la superficie reflectante (Evans & Costa, 2013)
2. *Reducción de Speckle (moteado)*: En una imagen de radar se evidencian dos tipos de textura entre ellas la de la varianza de la imagen que es conocida como moteado o speckle, siendo esta una característica inherente a las imágenes radar (García et al., 2003). De acuerdo con (García et al., 2003) el speckle o moteado debe ser reducido de una imagen de radar antes de realizar el procesamiento de los datos, dado que cualquier procesamiento ejecutado sobre una imagen antes de reducirlo genera ruido que es incorporado en la imagen generando una degradación de esta.
3. *Ortorectificación*: Con este proceso se corrigen y eliminan las distorsiones geométricas que se encuentran en la imagen de radar, además de ser georreferenciadas y generadas es geometría Ground Range (Byun et al., 2015).
4. *Corte de imagen de radar*: A través de este proceso se selecciona el área de interés que corresponde aproximadamente a 125.000 hectáreas.

2.2.3. Fase 3: Extracción de textura de imagen de radar

De acuerdo con (Guerra, 2002) una de las características más importantes aplicadas en la identificación de objetos o regiones de interés en la imagen de radar es la textura. A diferencia del color y brillo en una imagen óptica que están asociados a los pixeles que conforman una imagen, el cálculo de la textura se genera con base en grupos de pixeles conectados, por lo cual las características de textura en una imagen contienen información sobre la distribución espacial de las variaciones de tonos entre cada cobertura (Guerra, 2002).

Este proceso es realizado con ayuda de la matriz de co-ocurrencia la cual describe la frecuencia de un nivel de gris que aparece en una posición de la imagen en una relación espacial especifica con otro valor de gris, dentro del área de una ventana determinada. La configuración de los parámetros de entrada utilizada corresponde a lo propuesto por Fragoso-Campón y Quirós (2019) en donde se selecciona tamaño de la ventana de 9x9, se incluyen todos los ángulos, se usa un cuantificador probabilístico con 32 niveles cuantificadores, y un desplazamiento de 4 con un número de valor de dato de -999.0 .

Una vez finalizado el proceso se realiza una inspección visual del método de textura en el cual es más notoria la presencia de minería ilegal.

2.2.4. Fase 4: Clasificación supervisada de imagen radar

En esta fase se realiza el proceso de clasificación supervisada usando el método de máxima verosimilitud el cual consiste en realizar el cálculo de la probabilidad que tiene cada píxel que conforma la imagen que está siendo clasificada de pertenecer a una de las clases definidas. Por lo cual, cada píxel es se asignado a la clase en la cual presenta una mayor probabilidad de pertenecer (Ahmad & Quegan, 2012). Este método ha sido ampliamente utilizado mostrando buenos resultados (Verdú & Martínez, 2001; Anaya, 2014; Gomariz et al., 2014).

Como requisito en la clasificación supervisada es necesario definir unas zonas de entrenamiento como referencia, para esto se hizo uso de un mosaico construido a partir de imágenes ópticas de la constelación PlanetScope (Nalvarte & Mamani, 2021).

Una vez entrenado el modelo, se genera una clasificación con dos clases, la primera asociada a las zonas con presencia de minería ilegal y la segunda asociada a zonas cubiertas por otro tipo de cobertura. Como vector característico en la clasificación se utilizaron tanto la imagen de radar orto rectificada como las medidas texturales calculadas en la etapa anterior.

2.2.5. Fase 5: Validación de exactitud temática apoyado en imagen óptica

La validación temática de la clasificación se realiza a través del coeficiente kappa, que es una medida de concordancia entre la clasificación y la referencia teniendo en cuenta el azar, el valor oscila entre 0 y 1, y los valores superiores a 0.8 indican una clasificación temática casi perfecta (Cerda & Villarroel. L, 2008). En este proyecto 500 puntos aleatorios fueron distribuidos entre las dos clases seleccionadas y fueron verificados tomando como referencia la interpretación visual de la imagen óptica.

3. Resultados

Los resultados se presentan de acuerdo a las fases de la metodología.

3.1. Resultados de la Definición de requerimientos de información

La tabla 1 presenta los aspectos analizados en la dimensión que abarca las características técnicas para las imágenes de radar; en cuanto a las variables de modo y resolución se consideraron las que aportan la mayor riqueza espacial y su disponibilidad sobre la zona de estudio.

Al analizar los aspectos técnicos de los satélites cuyas imágenes de radar son candidatas, se observan tres opciones de bandas, destacando la banda C con 4 satélites capturando en esta longitud de onda, la banda L con dos satélites y la banda X únicamente con el satélite Cosmo-SkyMed. En la variable de resolución espacial resaltan los satélites Radarsat-2, Sentinel-1, ALOS-PALSAR y Cosmo-SkyMed. Sin embargo, esta metodología involucra

como factor para la selección de las imágenes una dimensión que analiza el acceso efectivo a las imágenes, sin limitarse únicamente a las características técnicas de estas.

SATÉLITE	MODO	RESOLUCIÓN	BANDA	POLARIZACIÓN
Radarsat-2	Wide Ultra-Fine	3 x 3 metros	C	Quad Pol (HH+HV+VH+VV)
ALOS-PALSAR	FBS – Fine resolution	10 x 10 metros	L	Single Pol (HH o VV) en modo fino
ERS-1	SAR Imaging mode	30 x 30 metros	C	Single Pol (VV)
ERS-2	SAR Imaging mode	30 x 30 metros	C	Single Pol (VV)
JERS-1	Standard Mode	18 x 18 metros	L	Single Pol (HH)
Sentinel-1	Interferometric Wide Swath	5 x 20 metros	C	Dual Pol (HH+HV o VH+VV)
Cosmo-SkyMed	Stripmap Himage	5 x 5 metros	X	Dual Pol (HH+HV o VH+VV) o Single Pol (HH o VV) según modo

Tabla 1 – Características sistemas de radar

La Tabla 2 presenta los aspectos analizados en la dimensión que abarca el acceso efectivo a las imágenes de radar, la variable cobertura evalúa la existencia de imágenes que cubran el área de interés, por su parte la variable archivo describe la temporalidad de la cual se tienen imágenes disponibles y, por último, la variable acceso define las constelaciones que disponen sus imágenes para uso libre no comercial y aquellas constelaciones privadas que requieren el pago de licenciamiento.

SATÉLITE	COBERTURA	ARCHIVO	ACCESO
Radarsat-2	Total, sobre el área de interés	De 2007 a la fecha	Licenciamiento privado
ALOS-PALSAR	Total, sobre el área de interés	De 2006 a 2011	Licenciamiento libre no comercial
ERS-1	Sin cobertura, sobre el área de interés	De 1991 a 2000	Licenciamiento libre no comercial, disponible sólo para residentes en EE. UU.
ERS-2	Sin cobertura, sobre el área de interés	De 1995 a 2011	Licenciamiento libre no comercial, disponible sólo para residentes en EE. UU.
JERS-1	Sin cobertura, sobre el área de interés	De 1992 a 1998	Licenciamiento libre no comercial, disponible sólo para residentes en EE. UU.
Sentinel-1	Total, sobre el área de interés	De 2014 a la fecha	Licenciamiento libre no comercial
Cosmo-SkyMed	Total, sobre el área de interés	De 2007 a la fecha	Licenciamiento privado

Tabla 2 – Características sistemas de radar

Al estudiar la dimensión de acceso efectivo a las imágenes, se destaca la imposibilidad al momento de realizar esta investigación de acceder a imágenes de los satélites ERS-1, ERS-2 y JERS-1 para los usuarios que no son residentes del territorio de los Estados Unidos de América (EE. UU.) lo cual hace necesario tener que descartar la selección de este tipo de dato. En segundo lugar, las constelaciones que se encuentran activas en el momento de realizar esta investigación son Radarsat-2 y Cosmo-SkyMed, las cuales cuentan con licenciamiento privado y Sentinel-1 con un licenciamiento libre para uso no comercial.

Como resultado de analizar las dos dimensiones planteadas como criterios de selección de las imágenes de radar, fue seleccionada 1 de las 7 constelaciones evaluadas, obteniendo finalmente, como resultado de la Fase 1 la selección de imágenes provenientes de Sentinel-1.

3.2. Resultados Pre-procesamiento de imagen radar

Como resultado de los cuatro procesos se generó una imagen corregida radiométricamente, con speckle reducido, ortorectificada y con cobertura del área de interés como se observa en la Figura 3.

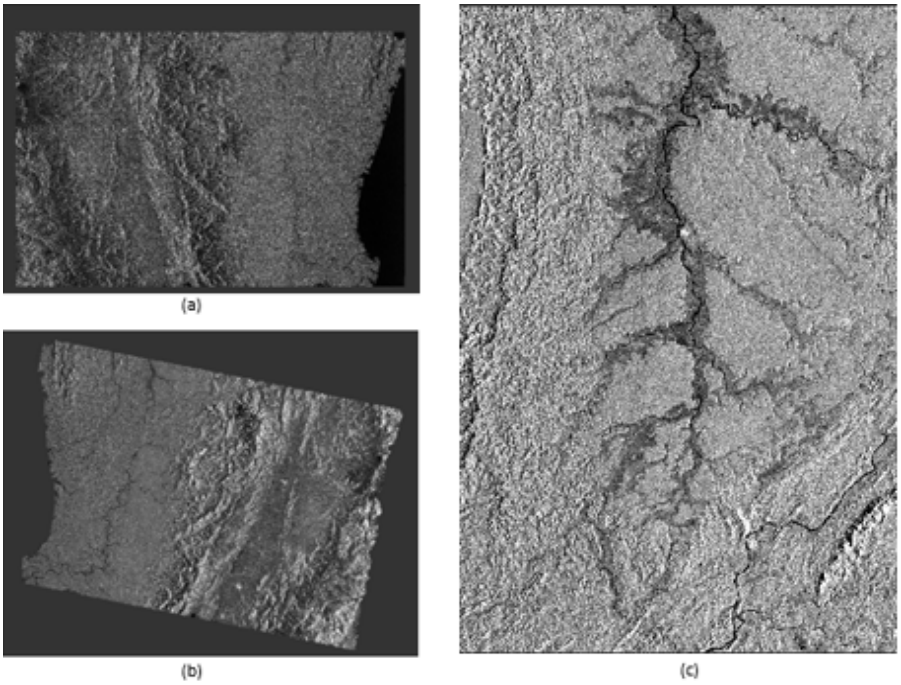


Figura 3 – resultados preprocesamiento de imagen radar a) Imagen sin procesamiento b) Imagen procesada c) Corte de imagen a límite de zona de interés

3.3. Resultado Extracción de textura de imagen de radar

La figura 4 muestra las medidas de textura generadas.

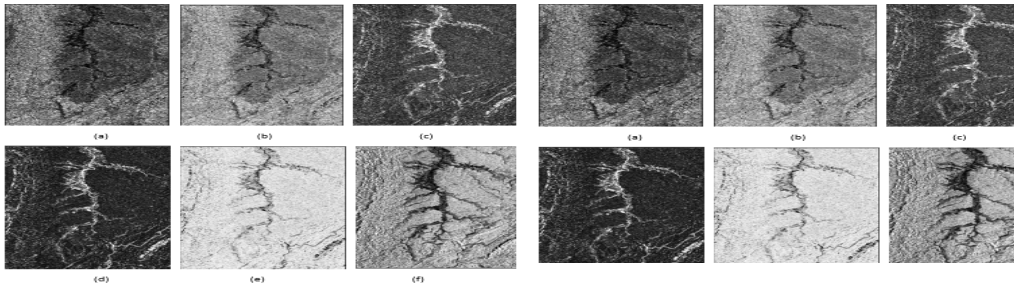


Figura 4 – Medidas de textura a) Contraste b) Disimilaridad c) Homogeneidad d) Energía e) Entropia f) GLCM Media

3.4. Resultados de Clasificación supervisada de imagen radar

La figura 5 muestra el resultado de la clasificación supervisada (100 muestras de entrenamiento fueron utilizadas), en donde el color rojo representa las zonas con presencia de minería ilegal y el color verde da cuenta de los otros tipo de cobertura. Se evidencia una concentración muy notoria del fenómeno de minería ilegal entorno a la ronda del cuerpo de agua presente en la zona.

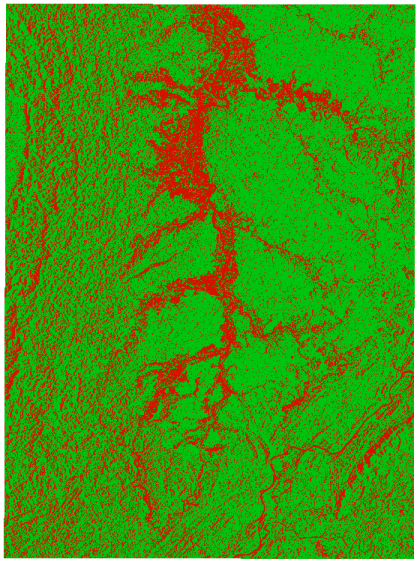


Figura 5 – Resultado del proceso de clasificación supervisada por máxima verosimilitud

3.5. Resultado Validación de exactitud temática

La distribución aleatoria de los 500 puntos para la validación de la clasificación se muestra en la Figura 6.

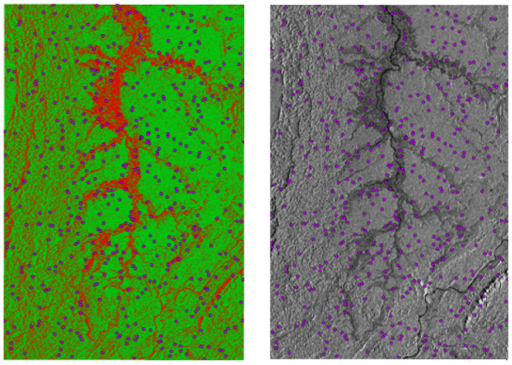


Figura 6 – Distribución de puntos de chequeo a) Vista de puntos de chequeo sobre clasificación b) Vista de puntos de chequeo sobre imágenes de radar

El coeficiente kappa obtenido fue un valor fue de 0.82 y la exactitud global alcanza el 89%, lo cual permite considerar conforme el proceso de clasificación al obtener un índice kappa superior al 0.81 definido como indicador de una clasificación temática casi perfecta.

4. Conclusiones

El presente trabajo plantea una metodología en cinco fases enfocada a la detección de minería ilegal como herramienta para la defensa y seguridad del territorio, mediante el uso de insumos de libre acceso como son las imágenes de Radar Sentinel-1 y el software SNAP.

La aplicación de la metodología en la zona de estudio alcanzó muy buenos resultados en la identificación de este fenómeno sobre un territorio colombiano históricamente afectado por minería ilegal y con presencia predominante de nubes a lo largo del año, ubicado en el municipio de Río Quito en el departamento Chocó.

Los resultados son prometedores ya que permiten a las autoridades detectar zonas con posible ocurrencia de minería ilegal en la zona de estudio y abre la posibilidad de implementar esta metodología en otras zonas donde la inspección visual aérea es limitada por la constante presencia de nubes con la intención de validar y estandarizar esta metodología.

Por último, implementar el uso de imágenes de licenciamiento libre de uso no comercial permite garantizar la disponibilidad y acceso de imágenes para replicar la metodología en

zonas con distintas condiciones de topografía, coberturas y texturas, siendo esta última como se observó en este caso de estudio, una herramienta fundamental para caracterizar el fenómeno de minería ilegal por medio de la rugosidad de este fenómeno, siendo este un descriptor usado con bastante frecuencia en los métodos de procesamiento digital de imágenes y reconocimiento de patrones.

Referencias

Agencia Espacial Europea - ESA. (2022). https://www.esa.int/Space_in_Member_States/Spain/El_programa_Copernico.

Ahmad, A., & Quegan, S. (2012). Analysis of Maximum Likelihood Classification on Multispectral Data. In *Applied Mathematical Sciences* (Vol. 6, Issue 129).

Anaya, J. (2014). *Sinergia entre datos ópticos y radar para determinar coberturas del suelo: resultados preliminares para la región de Urabá, Colombia*.

Arango, M., Branch, J., & Botero, V. (2005). Clasificación no supervisada de coberturas vegetales sobre imágenes digitales de sensores remotos: "Landsat-ETM+." *Revista Facultad Nacional de Agronomía*, 2611–2634.

Arantzazu, U. (2016). *Clasificación de cultivos a partir de observaciones de teledetección radar. Aplicación a zonas de secano y regadío de Navarra*.

Belmonte, I., & Caamaño, S. (2009). *Una aplicación basada en imágenes SAR para el monitoreo y prevención de inundaciones en Argentina*.

Briceño, J. (2013). *La minería ilegal como la amenaza más importante para la seguridad nacional: el caso de las FARC*. http://www.eltiempo.com/justicia/

Byun, Y., Han, Y., & Chae, T. (2015). Image fusion-based change detection for flood extent extraction using bi-temporal very high-resolution satellite images. *Remote Sensing*, *7*(8), 10347–10363. https://doi.org/10.3390/rs70810347

Cámara, A. (2005). *Método contextual para fusión de datos*.

Canada Centre for Remote Sensing. (2001). *Material educativo para teledetección mediante radares*. http://www.ccrs.nrcan.gc.ca/ccrs/learn/tutorials/gsarcd/contact_e.html

Carvalho, L., Rahman, M., Hay, G., & Yackel, J. (2010). *Optical and SAR imagery for mapping vegetation gradients in Brazilian savannas: synergy between pixel-based and object-based approaches*.

Cerda, J., & Villarroel. L. (2008). Evaluación de la concordancia inter-observador en investigación pediátrica: Coeficiente de Kappa. *Revista Chilena de Pediatría*, *79(1)*, 54–51.

Chamorro, F. (2021). *Metodología para determinar las áreas afectadas por minería ilegal por medio de imágenes satelitales Sentinel y técnicas de percepción remota en el Bagre, Antioquia*.

Chuvieco, E. (1995). *Fundamentos de teledetección* (2nd ed.).

Evans, T. L., & Costa, M. (2013). Landcover classification of the Lower Nhecolândia subregion of the Brazilian Pantanal Wetlands using ALOS/PALSAR, RADARSAT-2 and ENVISAT/ASAR imagery. *Remote Sensing of Environment*, *128*, 118–137. https://doi.org/10.1016/j.rse.2012.09.022

Fragoso-Campón, L. Quirós, E. (2019). Sentinel Toolbox Application (SNAP) aplicado a la clasificación supervisada de imágenes PNOA. In Luis A. Ruiz, Javier Estornell, Abel Calle y Juan Carlos Antuña-Sánchez (Eds.). *Teledetección: hacia una visión global del cambio climático*, pp. 263-266. Ediciones Universidad de Valladolid.

García, R., González, C., de La Vega, R., Valverde, A., & Sebem, E. (2003). *Análisis Del Comportamiento De Filtros De Reduccion De Speckle Ee Imagenes Ers2-Sar*.

Gomariz, F., Alonso, F., & Cánovas, F. (2014). Clasificación multitemporal de usos del suelo en la Cuenca del Río Vinalopó (Comunidad Valenciana) mediante diferentes algoritmos de clasificación supervisada y variables auxiliares. *XVI Congreso de Tecnologías de La Información Geográfica*.

Guerra, P. A. (2002). *Tratamiento y Procesamiento de una Imagen RADARSAT de Cartagena (2000) y Aplicación de Técnicas de Fusión de Imagenes*.

Guiza Suarez, L. (2014). *La realidad de la minería ilegal en países amazónicos:* Sociedad Peruana de Derecho Ambiental.

Hanssen, R. (2001). *Radar interferometry: data interpretation and error analysis*.

Hernandéz, I. (2014). *Análisis de subsidencia del terreno en el valle de Toluca a partir del método Dual Pair Interferometry (DPI)*.

Killeen, T., Siles, T., Soria, L., & Correa, L. (2005). *Estratificación de vegetación y cambio de uso de suelo en los* (Vol. 40, Issue 3).

Lira, J. (2018). *Tratamiento Digital de Imágenes Multiespectrales* (3rd ed.). https://www.researchgate.net/publication/283080110

Martínez, J., & Díaz, J. (2005). *Percepción remota "Fundamentos de teledetección espacial."*

Nalvarte, G., & Mamani, M. (2021). *Análisis espacio temporal del uso de suelo en concesiones de castaña mediante la aplicación de imágenes del satélite Landsat en la microcuenca Manuripe-Madre de Dios, períodos 2004-2020*.

Oficina de las Naciones Unidas Contra la Droga y el Delito - UNODC. (2021). *Colombia Explotación de oro de aluvión*.

Ormeño, S. (2006). *TELEDETECCION FUNDAMENTAL 3ª Edición* (3rd ed.). Escuela Técnica Superior De Ingenieros En Topografia, Geodesia Y Cartografía Departamento De Ingeniería Topográfica Y Cartografía.

Perea, M., Leal, J., & Oviedo, F. (2022). Spectral characterization and monitoring of mangrove forests with remote sensing in the Colombian pacific coast: Bajo Baudó, Chocó. *Granja*, *34*(2), 26–42. https://doi.org/10.17163/LGR.N34.2021.02

Quejada, J. (2019). *Afectaciones por minería en la subzona hidrográfica de Río Quito, mediante la interpretación de imágenes satélites*.

Rees, G. (2005). *The remote sensing data book*. Cambridge University Press.

Riveros, F. (2020). *Deforestación en el departamento del Chocó por medio de imágenes satelitales LANDSAT y SENTINEL durante el periodo 2015-2019*.

Rojas Villarraga, M. (2021). *Explotación Minera En Colombia*.

Rueda, O., & Poveda, G. (2006). *Variabilidad espacial y temporal del chorro del "Choco" y su efecto en la hidroclimatología de la región del pacífico colombiano*. https://www.researchgate.net/publication/301612753

Valencia, B. & Upegui E. (2020). Propuesta metodológica para generar mapas de cobertura de la tierra a partir de imágenes de radar ALOS/PALSAR: Estudio de caso Mompós, Colombia. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 56-68

Verdú, J., & Martínez, J. (2001). Aplicación de imágenes radar de satélite a la cartografía de la vegetación en zonas boreales. *Revista de Teledetección*, *16*, 37–40.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 13/10/2021
Aceitação/Acceptance: 15/01/2022

Continuidad operacional de las redes de gas en Chile

Manuel Sepulveda[1], Vicente Salas [1], Gustavo Gatica[1], John Ríos.

m.sepulvf@gmail.com; v.salassanchez@uandresbello.edu; ggatica@unab.cl; john.rios@unab.cl

[1] Facultad de Ingeniería, Universidad Andres Bello, Antonio Varas 880, Providencia, 7500971, Chile.

Pages: 643-653

Resumen: Chile es una larga y angosta franja de tierra, en zonas tiene sólo 90 kilómetros desde la cordillera al mar, como en otras alcanza una distancia de 445 kilómetros. El gas natural es el principal medio de calefacción en zonas urbanas y el combustible preferido en procesos industriales térmicos que requieren disminuir su huella de carbono. En este contexto, los ductos deben atravesar desiertos, ríos, zonas con bosques entre otros. Las técnicas de construcción de dichos ductos, al igual como los materiales empleados son diversos, dada la sismicidad presente en Chile. Se propone una evaluación económica que involucra resiliencia de servicio en una zona del norte del país, donde las características geográficas de los atraviesos y los efectos del cambio climático, obligan a las empresas a sobredimensionar las medidas de mitigación y los procedimientos de mantención, para contribuir en la continuidad operacional.

Palabras-clave: Infraestructura; frágil; alternativas: transporte; infraestructura; gasoductos.

Operational continuity of gas networks in Chile

Abstract: Chile is a long and narrow strip of land, in some areas it is only 90 kilometers from the mountain range to the sea, as in others it reaches a distance of 445 kilometers. Natural gas is the main means of heating in urban areas and the preferred fuel in thermal industrial processes that require reducing their carbon footprint. In this context, the pipelines must cross deserts, rivers, forested areas, among others. The construction techniques of these pipelines, as well as the materials used, are diverse, given the seismicity present in Chile. An economic evaluation is proposed that involves service resilience in an area in the north of the country, where the geographical characteristics of the crossroads and the effects of climate change force companies to oversize mitigation measures and maintenance procedures, to contribute in operational continuity.

Keywords: Infrastructure; fragile; alternatives: transportation; infrastructure; gas pipelines

1. Introducción

Se presenta una revisión a la red de suministro de gas natural en Chile, dada las condiciones geográficas es frágil por cuanto no se dispone de vías alternativas ante eventos que impliquen una interrupción de las actuales rutas. Chile al ser tan extenso, sísmico, y angosto no tiene infraestructura que permita generar *bypass* para el transporte. Por lo anterior, se dispone de camiones que transportan gas natural licuado criogénico, y que forman parte de lo denominado gaseoducto virtual, porque reemplazan extensas longitudes de tuberías.

El terminal marítimo de gas natural, se encuentra ubicado en Quintero, a sólo 156 kilómetros de la capital Santiago de Chile, su funcionamiento data del 2009, momento en el cual por motivos geopolíticos el país de Argentina bloqueó los envíos de gas natural a Chile, por los gasoductos que llegan a los grandes centros urbanos de Chile.

La infraestructura chilena dispone de una regasificadora a 457 kilómetros al sur de Santiago de Chile, en la localidad de Pemuco en la región de Ñuble, Provincia del Biobío, que tiene una capacidad de 600 mil metros cúbicos, escalable a 1.200.000 metros cúbicos, dependiendo de la demanda en la octava región. Existen otras plantas regasificadoras que forman parte de este modelo de gaseoducto virtual. Las plantas de Coquimbo, Osorno, Valdivia, Puerto Montt entre otras, más las plantas regasificadoras para instalaciones industriales. Todas dependen de camiones y la disponibilidad de las rutas, que siempre son fáciles de interrumpir por demandas sociales y/o gremiales.

Se dará una mirada a las distintas alternativas de transporte del gas natural, las que estarán asociadas a las dos formas de almacenamiento, como gas comprimido y licuado criogénico.

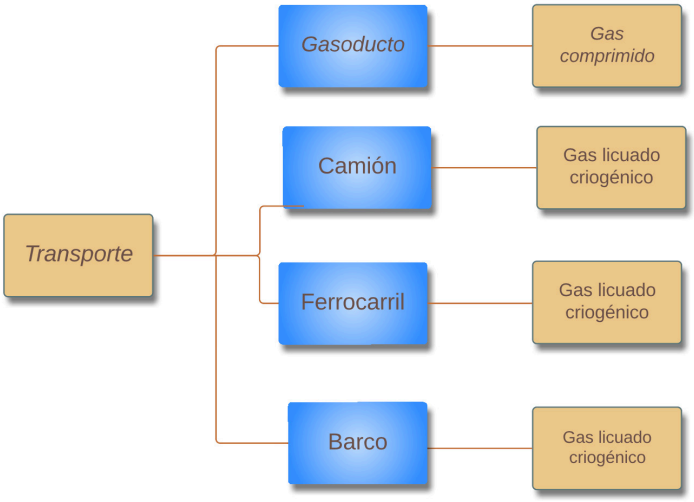


Figura 1 – Medios de transporte.
Fuente: Elaboración propia.

En la Figura 1, se puede observar los distintos medios de transporte de Gas Natural que pueden ser empleados en Chile, destaca que el transporte por camiones sobrepasa el 90% de la infraestructura, lo cual lo hace vulnerable a movimientos sociales y gremiales de toda índole. La fragilidad se evidenció, luego del movimiento social de Octubre del 2019, en donde la distribución en algunas zonas del país estuvo al límite del colapso.

2. Un poco de história del gas natural en Chile

Enap inició la distribución de Gas Natural (GN) en Punta Arenas y Puerto Natales el año 1971. Entre los años 1997 y 1999 se inicia la distribución de GN procedente de Argentina en La Región Metropolitana (RM), Regiones de Valparaíso y Concepción. Así se convierte en una industria emergente hasta el año 2004, en donde Argentina suspendió gradualmente el suministro a Chile. Desde el año 2004 al 2010, la industria debió suministrar una mezcla de propano aire, en reemplazo

del gas natural y mientras se construía el primer terminal marítimo de gas natural licuado en Quintero el año 2009 y posteriormente en Mejillones, el año 2010 (Metrogas, 2015).

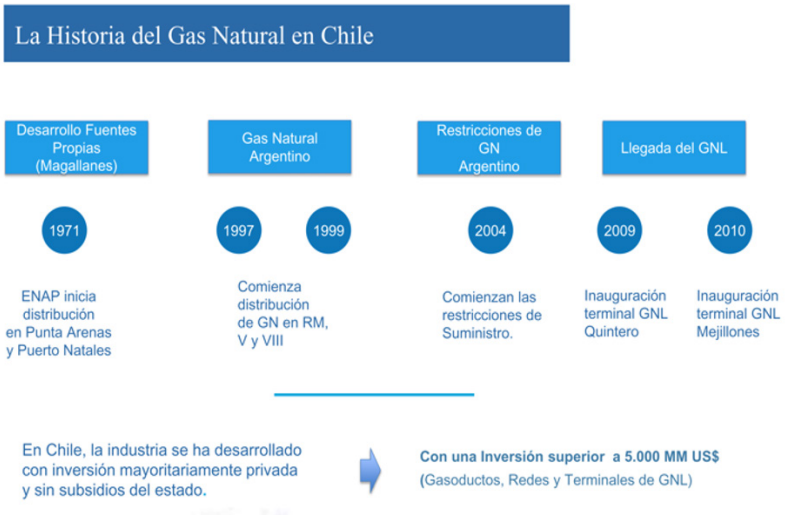


Figura 2 – Desarrollo del. Gas natural en Chile.
Fuente (Metrogas, 2015)

La figura 2 muestra cómo evolucionó la industria de gas natural en Chile, desde el inicio de la distribución en Magallanes, hasta la inauguración del terminal GNL en Mejillones.

De la infraestructura expuesta y según la naturaleza del producto transportado, se puede dividir en dos. Las que no representan riesgo a personas y bienes y las que, si representan riesgo, en general las que transportan combustibles. Para estas existen normas nacionales y extranjeras que velan por la seguridad de las operaciones (Integridad de

redes) que está enfocada en abordar factores internos, que son propios de la durabilidad de los materiales y factores externos, que están relacionados con variables que pueden ser personas, operaciones con maquinarias, factores ambientales como clima, humedad, salinidad, rayos, sismos, aluviones (American Society of Mechanical Engineers, 2004).

En Chile existen varios gaseoductos que alimentan distintas regiones del país cómo se aprecia en las figuras 3 y 4

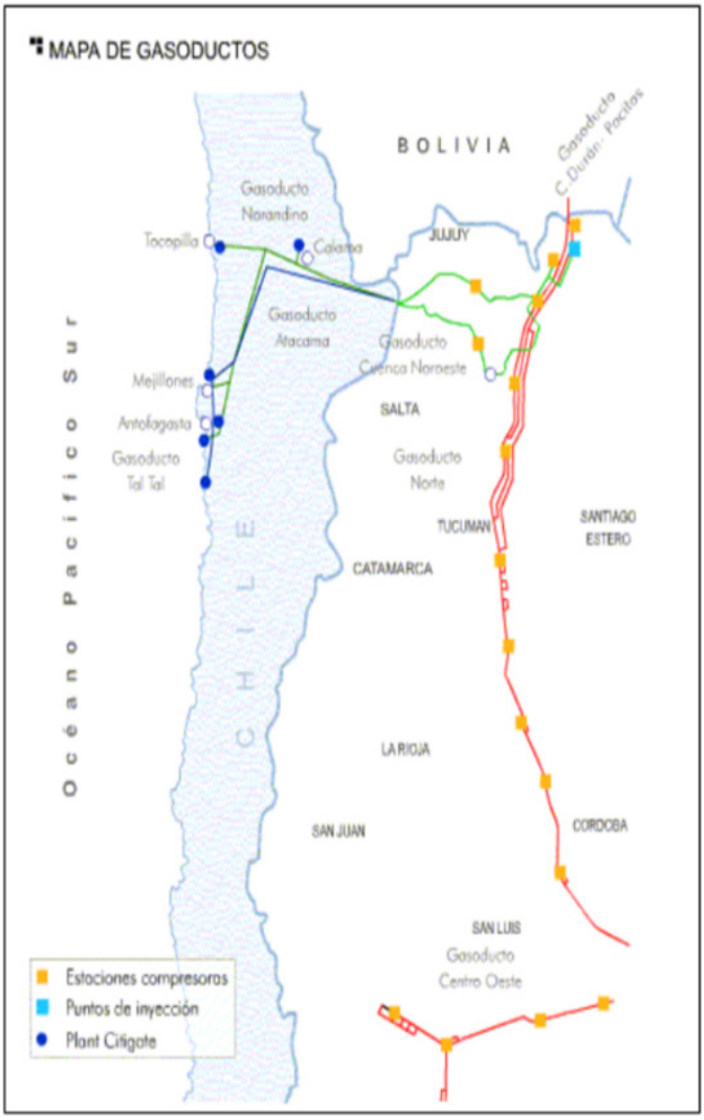


Figura 3 – Mapa gaseoductos zona norte de Chile.
Fuente (CNE, s. f.)

La figura 3 muestra las redes de transporte de gas natural que bridan suministro a la región de Antofagasta. Originalmente recibían suministro desde Argentina. Actualmente, el suministro se recibe desde el termina de gas natural licuado en Mejillones, donde se gasifica y se inyecta al gasoducto en estado gaseoso comprimido.



Figura 4 – Mapa gaseoductos Zona Centro y Sur.
Fuente (CNE, s. f.)

La figura 4 muestra la red en la zona central y sur, las que ya no dependen del gas natural proveniente de Argentina. El gas se recibe en el puerto de Quintero, se inyecta a la red de la zona central y Enap lo transporta por camiones hasta la planta regasificadora de Pemuco en donde se inyecta al gaseoducto Pacífico.



Figura 5 – Camión criogénico de transporte gas natural licuado: Fuente (*Conoce el gasoducto virtual, la apuesta de Enap para impulsar la masificación del gas - Electricidad*, s. f.)

La figura 5 muestra uno de los 25 camiones que Enap dispuso para formar parte del gasoducto virtual.

Dado lo anterior, se requiere de planes de mitigación, para generar rutas alternativas para la continuidad operativa del suministro. Una alternativa, es generar convenios con Argentina, para inyectar gas desde las principales ciudades chilenas, para proveer gas natural mediante bypass a zonas distantes más de 500 km de distancia. Un ejemplo de ello, se puede visualizar en la Figura 4, en donde al inyectar gas desde Santiago de Chile, se puede proveer con gas al sur del país. En particular el Gran Concepción, mientras se termina la construcción de un terminal marítimo en Talcahuano, distante 14 kilómetros de Concepción.

3. Integridad de redes como una forma de bridar seguridad operacional y disminuir la probabilidade de accidentes

El proceso de velar por las operaciones seguras en la red se denomina “Integridad de redes”. Se debe considerar en todas las etapas, diseño y construcción, operación, mantenimiento y término de operaciones. (ASME B31.8S, 2010)

La integridad de la red está afectada por factores internos, que son propios de la durabilidad de los materiales y factores externos que están relacionados con variables que pueden ser, personas, operaciones con maquinarias, factores ambientales como clima, humedad, salinidad y factores de corrosión, rayos, sismos, aluviones y otros. (American Society of Mechanical Engineers, 2004)

La figura 6 muestra la brecha entre la curva de resistencia de la tubería y el esfuerzo a la que está sometida (presión). Una pérdida de material por corrosión, desplazará la curva *f (r)* hacia la izquierda, disminuyendo la brecha y generando la probabilidad de falla por ruptura.

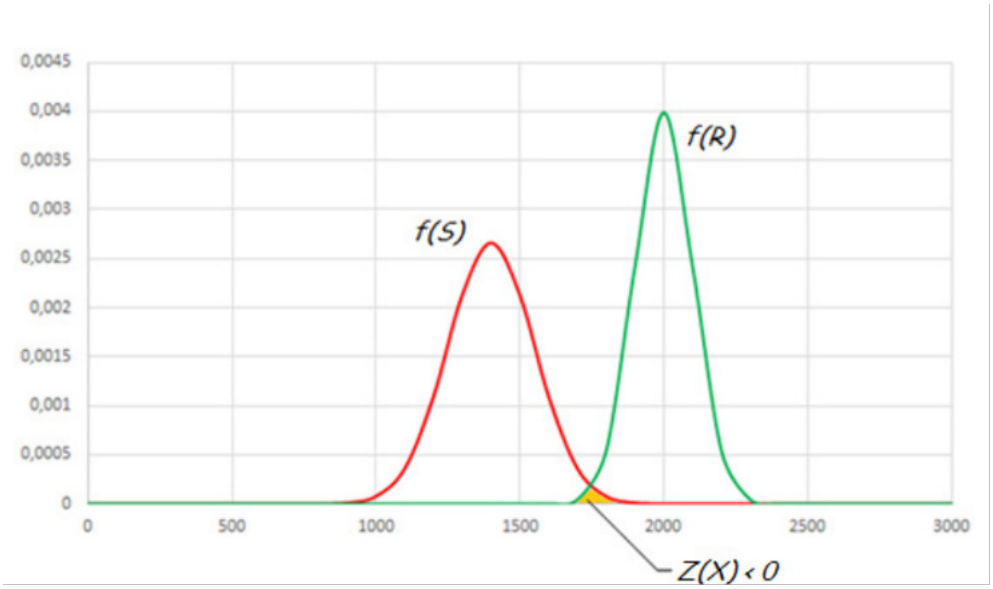


Figura 6 – Interacción entre resistencia y demanda.
Fuente: (*Cálculo de la Tasa de Falla de Tuberías - Predictiva 21*, s. f.)

El Manual (1991a, lib. ANSI ASME B31 G) que forma parte del código ASME B31 para tuberías de presión en sistemas de transporte y distribución para hidrocarburos, gas, amoniaco anhidro, alcoholes. Establece estándares de aceptación para tuberías que puedan tener corrosión antes, o durante la fabricación y/o Instalación.

Durante 1970 y 1971, se realizaron 47 pruebas de presión en varios tamaños de tuberías para evaluar la efectividad de las expresiones matemáticas determinando el esfuerzo de áreas corroídas. El diámetro de la tubería examinado fue en el rango de 16 pulgadas hasta 30 pulgadas y el rango de los espesores pared varió de 0.312 pulgadas a 0.375 pulgadas. Los materiales de tubería estuvieron en un rango de esfuerzo a la cedencia de 25,000 psi para API 5L grado A-25 a aproximadamente 52,000 psi para 5LX Calidad X-52 (Suplemento & Asme, 1991b)

Representación gráfica explicativa de corrosión en profundidad y longitud, se describe en la Figura 7, en donde, lo principal es el hecho que la infraestructura debe ser revisada periódicamente, pese a que los materiales están diseñados para una durabilidad superior a los 20 años. Cabe destacar que Chile al ser un país sísmico, la infraestructura está sobredimensionada con materiales lo suficientemente elástico para resistir terremotos.

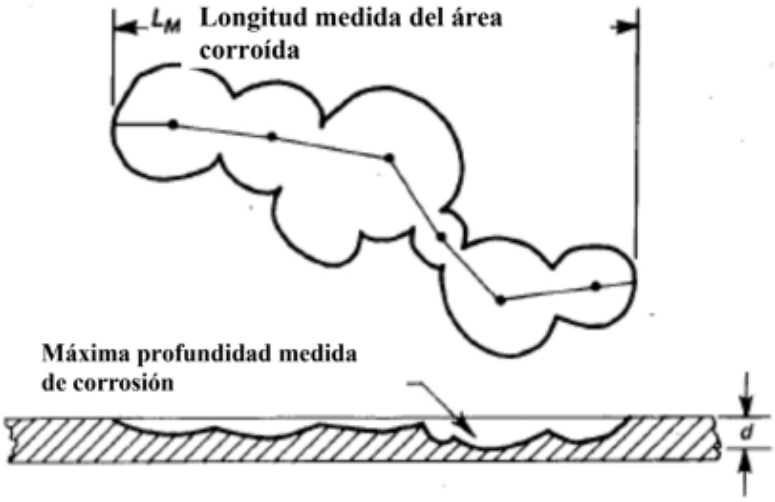


Figura 7 – Representación de profundidad y longitud de la corrosión.
Fuente : (Suplemento & Asme, 1991a)

Estas alteraciones a las tuberías podrían obligar a disminuir la presión máxima de operación de gasoducto. (Suplemento & Asme, 1991b)

Bajo esta situación se potencia el concepto de planificar mantención basada en el riesgo como lo indican las normas API (American Petroleun Institute), la que se basa en el conocimiento y la experiencia de ingenieros, inspectores, analistas de riesgo y otro personal en la industria química y de hidrocarburos (API, 570 THIRD EDITION, 2010).

Se realizan mediciones de corrosión realizando ensayos no destructivos que permiten conocer el grado de deterioro que tienen las tuberías empleando un dispositivo electrónico denominado pig, el que se introduce en las tuberías y las recorre impulsado por la presión del gas. El equipo mide el espesor en los 360 grados y el toda la longitud de la tubería recorrida, almacena los datos en una memoria la que es descargada en el punto de destino.

3.1. Propuestas alternativas de transporte de gas natural

Existen otras formas de transportar gas natural desde un punto a otro cómo se indica en la figura 1 que tienen ventajas y desventajas las que deben ser evaluadas al momento de diseñar la red.

Las figuras 8, 9 y 10 comparan ventajas y desventajas de los distintos medios de transporte para el gas natural, dependiendo de su almacenamiento. Sin evaluar costos, se aprecia que el gasoducto representa la mejor condición de continuidad operacional por disponer de un flujo continuo. Están construidos tuberías soldables de acero al carbono, categorizados como de alto esfuerzo y baja aleación como los descritos en ASTM A 53 a 106 y A381. Son API 5L (B31.8, 2021)

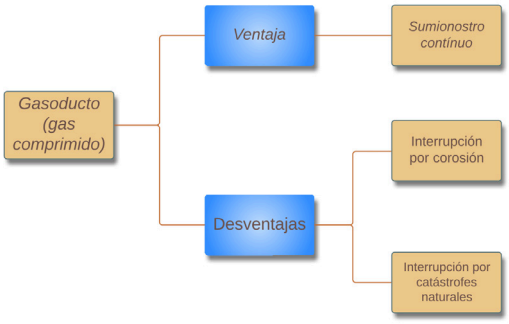


Figura 8 – Ventajas y desventajas del transporte por gasoducto. Fuente: Elaboración propia

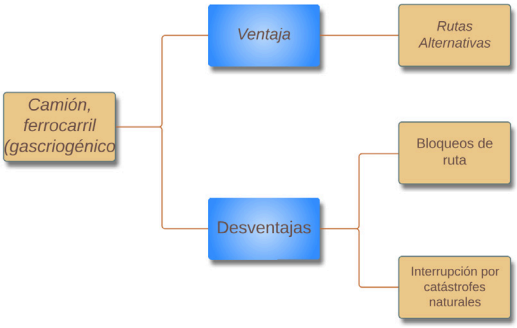


Figura 9 – ventajas y desventaja de transporte por camión ferrocarril.
Fuente: Elaboración propia

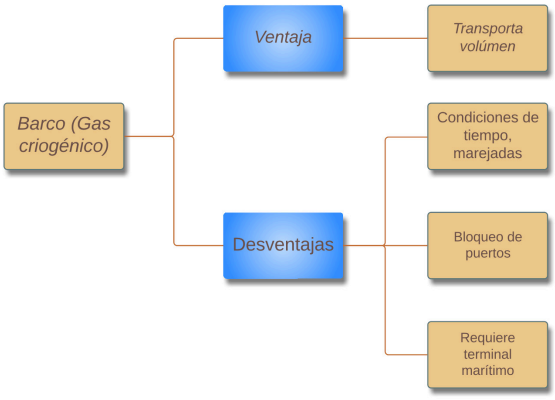


Figura 10 – ventajas y desventajas de transporte por barco. Fuente: Elaboración propia

4. Conclusiones

Chile posee una red de gas natural fragmentada que nació conectada a los gasoductos de Argentina. Producto de la suspensión de suministro el gobierno se vio en la obligación de generar una logística de abastecimiento distinta, incorporando dos terminales de GNL, uno en Quintero y el otro en Mejillones, desarrollando además una red de gasoducto virtual, que transporta gas líquido criogénico por camiones para aquellas ciudades que no tienen red y para clientes industriales de alto consumo, cuyos procesos estén con políticas de disminución de la huella de carbono. Este tipo de transporte se ve amenazado por interrupciones de caminos por protestas gremiales ocasionando siempre la posibilidad de interrumpir el suministro de gas de una ciudad. Se deben considerar alternativas, cómo transporte por tren, que no se encuentra implementado, o generar convenios con Argentina para utilizar sus redes durante los bloqueos de caminos. La figura 4 muestra que existe conexión entre la zona central y la zona sur a través de Argentina, los que podrían ser utilizados al menos hasta que se termine la construcción del próximo terminal marítimo de gas natural licado de Talcahuano, el que descargá, almacenará y regasificará hasta 4 MM de metros cúbicos al día. (*GNL Talcahuano - Terminal Marítimo*, s. f.)

Referencias

American Society of Mechanical Engineers. (2004). Managing System Integrity of Gas Pipelines. *ASME Code for Pressure Piping, 2004*, 60. https://law.resource.org/pub/us/cfr/regulations.gov.docket.03/asme.b31.8s.commentary.pdf

API, 570 THIRD EDITION, N. 2009. (2010). *API 570, Piping Inspection Code : In-service Inspection , Rating , Repair , and Alteration of Piping Systems. November 2009*.

ASME B31.8S. (2010). *Gestión de Integridad de sistemas de Gasoductos* (Vol. 2010).

B31.8, A. (2021). *Page 1 (row 1, column 1). 2004*.

Cálculo de la Tasa de Falla de Tuberías - Predictiva 21. (s. f.). Recuperado 26 de octubre de 2021, de https://predictiva21.com/calculo-tasa-falla-tuberias-confiabilidad-estructural/

CNE, 2006. (s. f.). *1.1.1 Desarrollo (Gasoductos)*. Recuperado 2 de agosto de 2021, de https://hrudnick.sitios.ing.uc.cl/alumno06/Swap/node5.html

Conoce el gasoducto virtual, la apuesta de Enap para impulsar la masificación del gas - Electricidad. (s. f.). Recuperado 6 de mayo de 2022, de https://www.revistaei.cl/2014/07/12/conoce-el-gasoducto-virtual-la-apuesta-de-enap-para-impulsar-la-masificacion-del-gas/#

GNL Talcahuano - Terminal Marítimo. (s. f.). Recuperado 6 de mayo de 2022, de https://www.gnlt.cl/index.php

Metrogas. (2015). *Gas natural en Chile*. http://www.metrogas.cl/administradores/userfiles/2_Gianni Bozzo.pdf

Suplemento, U., & Asme, B. (1991a). *ANSI ASME B31G Manual para determinar el esfuerzo remanente de líneas corroídas* (Vol. 1991).

Suplemento, U., & Asme, B. (1991b). *ANSI ASME B31G Manual para determinar el esfuerzo remanente de líneas corroídas. 1991.*

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 13/12/2021
Aceitação/Acceptance: 07/02/2022

Minería de datos educativos: Incidencia de factores socioeconómicos en el aprovechamiento escolar

Jorge Pincay-Ponce[1, 2], Jorge Herrera-Tapia[1], Jackeline Terranova-Ruiz[1], Marely Cruz-Felipe[2], Juan Sendón-Varela[1], Lytyet Fernández-Capestany[1]

jorge.pincay@uleam.edu.ec; jorge.herrera@uleam.edu.ec; jackeline.terranova@uleam.edu.ec; juan.sendon@uleam.edu.ec; marely.cruz@utm.edu.ec; lytyet.fernandez@uleam.edu.ec

[1] Universidad Laica Eloy Alfaro de Manabí, Manta, 130802, Manabí, Ecuador.

[2] Universidad Nacional de la Plata, 1900, La Plata, Argentina.

[2] Universidad Técnica de Manabí, Portoviejo, 130105, Manabí, Ecuador.

Pages: 654-667

Resumen: La minería de datos educativos es un compendio de métodos eficaces para detectar patrones de situaciones que afectan diversos aspectos de la escolaridad, sin embargo, no es del todo claro en qué momentos de un curso académico los factores socioeconómicos pueden tener más incidencia en el aprovechamiento. En este estudio se ha tomado una muestra transversal aleatoria de datos de calificaciones parciales progresivas y de factores socioeconómicos de alumnos de una escuela ecuatoriana, para estimar las influencias de estos factores en su aprovechamiento mediante algoritmos de clasificación. Con el empleo de Reglas de Asociación y Árboles de Decisión, se precisó en un 90% que los factores socioeconómicos influyen el aprovechamiento de los estudiantes de modo especial en el primero de los dos quimestres que componen un periodo académico, y, en el segundo el mayor dominio de aprendizajes reflejado en notas se relaciona más con las calificaciones de los componentes parciales. Este modelo de análisis puede ser aplicado a todos los niveles de educación.

Palabras-clave: Mining Student; CN2; Árboles de decisión; Clasificación; Naive Bayes.

Educational data mining: Incidence of socioeconomic factors on school achievement

Abstract: Educational data mining is a compendium of effective methods to detect patterns of situations that affect various aspects of schooling; however, it is not entirely clear at what times of an academic year socioeconomic factors may have more impact on achievement. In this study, a random cross-sectional sample of data from progressive partial grades and socioeconomic factors of students from an Ecuadorian school has been taken, to estimate the influences of these factors on their achievement through classification algorithms. With the use of Association Rules and Decision Trees, it was specified in 90% those socioeconomic factors influence

the achievement of students in a special way in the first of the two semesters that make up an academic period, and, in the second the Greater mastery of learning reflected in grades is more related to the grades of the partial components. This model of analysis can be applied to all levels of education.

Keywords: Mining student; CN2; Decision Trees; Classification; Naïve Bayes.

1. Introducción

En la actualidad es importante extraer información significativa de una gran cantidad de datos y en ese sentido según (Sun, 2022), la minería de datos educativos como disciplina emergente se ocupa de desarrollar métodos para explorar los datos únicos y cada vez más a gran escala que provienen de entornos educativos y así comprender mejor a los estudiantes, a la enseñanza y a la gestión de los maestros. Si bien, se debe reconocer la proliferación de muchos sistemas de gestión de la información educativa, a consideración de (Fu & Hwang, 2018; McNeish & Wolf, 2020), la utilización de datos allí almacenados se limita a consultas o cálculos de promedios, de rangos u otros, pero no se suele buscar relaciones entre los puntajes o, determinar factores afectan de modo clave el rendimiento de los estudiantes o cuales serían las posibles tendencias de desarrollo futuro a partir del rendimiento y del comportamiento actual.

A decir de varios autores, que han evaluado las asociaciones entre el momento y la duración del nivel socioeconómico bajo durante la infancia y el rendimiento académico en la escuela, la educación tiene implicaciones de por vida para el bienestar (van Zwieten et al., 2021). Años antes, otros estudios detectaron que, por ejemplo, el aprovechamiento en matemáticas tiene relación con las diferencias en la situación económica familiar, seguidas de la segregación escolar, aun resaltando que las configuraciones familiares biparentales o padre-presente versus monoparental o padre-ausente son probablemente insignificantes como causa cuando el estatus económico está controlado (Entwisle & Alexander, 1992).

En todo caso, varias investigaciones parecen coincidir en que las diferencias individuales en los llamados factores no cognitivos han ganado una atención generalizada en los últimos años (Ng-Knight & Schoon, 2017), en tanto que algunos investigadores han referido a la calidad del docente como un factor de importancia para disipar la problemática (Hanushek et al., 2019).

Vistos como factores socioeconómicos influyentes en el aprovechamiento escolar, también se puede tomar como referencia a los trabajos de (Helal et al., 2018; Roh et al., 2016) que en sus estudios a estudiantes universitarios encontraron que los puntajes estaban muy influenciados por factores como la dirección del hogar, los ingresos anuales familiares, la educación de la madre, los hábitos de vida y características sociodemográficas como la raza, el género y la situación económica. Varios estudios como los de (Bedir, 2019; Ismail et al., 2019; Macías-Mendoza et al., 2016). coinciden en que, debido a sus diferencias individuales, los estudiantes tendrán diferencias significativas en los resultados de aprendizaje, por lo que la calidad de la enseñanza se puede mejorar si las calificaciones futuras de los estudiantes se pueden predecir utilizando sus calificaciones existentes, y las estrategias de enseñanza se pueden cambiar adecuadamente.

En el presente estudio transversal de una muestra aleatoria de alumnos de primaria de una escuela ecuatoriana, se usan los promedios finales de cada alumno, sus componentes individuales y un conjunto de datos de factores socioeconómicos para estimar las influencias de estos factores en su aprovechamiento escolar. Entre otros, se detectó que, entre los aspectos sociales de respuestas más frecuentes en los modelos, están el estado civil de los padres, su trabajo y escolaridad alcanzada. En menor medida, el comportamiento o conducta de los alumnos y como dato llamativo, que los alumnos con más hermanos suelen alcanzar con lo justo sus aprendizajes requeridos. Existe poca influencia del ingreso familiar o del grado que cursa el alumno para determinar su aprovechamiento.

En las siguientes secciones se detallan los materiales y métodos de uso en la investigación, se presentan los resultados, se los discute y los autores exponen sus conclusiones del respecto.

2. Materiales y Métodos

Se investigó una hipótesis que podría explicar el rendimiento más bajo entre los estudiantes, siendo esta, que existe una relación positiva entre el tipo de estructura familiar, así como otras condiciones socio económicas favorables y el nivel de aprendizaje alcanzado por los estudiantes, con base en la escala de calificaciones, que viene propuestas por el Ministerio de Educación de Ecuador, son:

- DAR: Domina los aprendizajes requeridos, desde 9,00 hasta 10,00.
- AAR: Alcanza los aprendizajes requeridos, desde 7,00 a 8,99.
- PAAR: Próximo a alcanzar los aprendizajes requeridos, de 4,001 a 6,99.
- NAAR: No alcanza los aprendizajes requeridos, menos o igual a 4.

Para ello se empleó análisis de datos para determinar la incidencia de factores socioeconómicos en el aprovechamiento escolar, para lo cual se siguió los pasos establecidos en la metodología Knowledge Discovery in Databases, KDD (Fayyad et al., 1996). KDD fue distribuida tal cual muestra la Tabla 1:

Fases de KDD	Distribución en el artículo
Selección	2. Materiales y métodos
Preprocesado	2. Materiales y métodos
Transformación	2. Materiales y métodos
Minería de datos	3. Resultados
Evaluación	3. Resultados

Tabla 1 – Adaptación de la metodología seguida con respecto de KDD

Respecto de la obtención de los datos, que se corresponden a una muestra transversal del año lectivo 2019, esta almacena información del aprovechamiento académico, representado por las calificaciones, y las condiciones socioeconómicas de los alumnos

de una escuela de Ecuador. Originalmente las calificaciones estaban disponibles en la institución educativa en diversas hojas de cálculo que las autoridades descargaban desde un sistema informático proporcionado por el Gobierno del País, mismo que el personal de la escuela había alimentado previamente. A esos datos se los limpió, preparó y transformó para ser analizados mediante algoritmos de clasificación como lo son las reglas de asociación y los árboles de decisión. Según la IEEE, los algoritmos mencionados están entre los más usados en temas de investigación en general (Pincay-Ponce, Angulo-Murillo, et al., 2020; Pincay-Ponce, Sánchez-Andrade, et al., 2020; Sharma et al., 2020).

Por otra parte, los datos de condiciones socioeconómicas estaban al custodio del Departamento de Consejería Estudiantil (DECE), que es la instancia responsable de la atención integral de los estudiantes, quienes si bien los tenían en formato digital .docx de Microsoft Word, lo enlazaban "de forma manual" con los datos de aprovechamiento.

2.1. Preparación de los datos

En este paso se construyó una base de datos en SQL Server 2014 Enterprise, para relacionar mediante varias tablas los datos de aprovechamiento con los datos socioeconómicos de cada alumno. Posterior a la construcción de la base de datos, se diseñaron varias vistas mediante prueba-error, hasta obtener una de 6628 filas y 76 atributos, la vista se importó a Microsoft Excel 2019 y desde allí se generó su equivalente en formato de Valores Separados por Comas (CSV) para ser procesada en el software de análisis ORANGE, versión 3.29.3.

El conjunto de datos guarda calificaciones del promedio anual de los alumnos en cada materia. El promedio anual deriva de 2 promedios quimestrales y dicho promedio deriva de 3 promedios parciales por quimestre. En los aspectos socio económico se almacena información sobre: Tipo de familia, ingreso mensual familiar, parentesco del representante, sector de dirección domiciliaria, cantidad de personas que viven en casa, escolaridad alcanzada por los padres, servicios básicos de los que se dispone, entre otros que se pueden explorar a detalle desde este enlace.

Con esos datos, se empleó el algoritmo Apriori (Agrawal & Srikant, 1994) disponible para la obtención de Reglas de Asociación desde Orange y SimpleTreeLearner como una implementación de Árboles de Decisión que utiliza la relación de ganancia para la clasificación y la medida del promedio de los cuadrados de los errores o desviaciones (MSE) para la regresión. Con ambos algoritmos se logró identificar de forma ágil los factores de tipo socioeconómicos que más pueden influir en el aprovechamiento de los estudiantes.

2.3. Transformación de los datos

Preprocesamiento general aplicado al DATASET que sirve para todas las hipótesis

- En un inicio se estableció algunos atributos como objetivos o de clases: El promedio anual de las dos notas quimestrales, el equivalente cualitativo del promedio anual de las dos notas quimestrales, equivalente cualitativo (ABC) del comportamiento del alumno en el primer quimestre y el equivalente cualitativo (ABC) del comportamiento del alumno en el segundo quimestre.

- Se detectó y prescindió de atributos de alta variabilidad como apellidos y nombres y de baja variabilidad como el de jornada dónde todos cursan la jornada matutina.
- Se detectó, rellenó o limpió atributos de estados civiles de padres con 1600 valores nulos por el valor "SIN ESPECÍFICAR". Hubo casos similares para profesión del Padre, Madre o Representante y parentesco con el alumno, estructura familiar… en todos los casos se procedió de la misma manera.
- Se transformó el tipo de datos Número de hermanos de numérico a Categórico.
- Se identificó que en cada Quimestre se diseña un proyecto escolar por cada uno de los tres parciales que incluye el Quimestre, es cual es calificado en escala cualitativa: EX=Excelente, MB=Muy Bueno, B=Bueno, Regular=R. También se guarda un promedio cualitativo de los tres proyectos de cada Quimestre. Dado eso, en el modelo sólo se usará el promedio cualitativo de proyectos del Quimestre 1 y del Quimestre 2.
- Se identificó mediante Correlación de PEARSON, correlaciones +1, entre los siguientes pares de atributos (ver Tabla 2), esto porque cada promedio de los parciales quimestrales sobre 10 (PROM1 y PROM2), es llevado mediante regla de 3 a sobre 8 (1PRO80 y 2PRO80), para complementarla sobre 10 con la calificación de un examen tomado sobre 10 (EXA1 y EXA2) pero que a su vez es llevado a sobre 2 (1EXA20, 2EXA20). Por tanto, en el modelo no se considerarán las notas sobre 20 y sobre 80: 1EXA20, 2EXA20, 2PRO80, 1PRO80.

	Correlación	Variable 1	Variable 2
1	+1.000	1EXA20	EXA1
2	+1.000	2EXA20	EXA2
3	+1.000	2PRO80	PROM2
4	+1.000	1PRO80	PROM1

Tabla 2 – Vista parcial de las correlaciones de Pearson para algunos pares de características

- Se construyó nuevos atributos como Cursos a partir de información de otros campos como Grado y Paralelo.

A continuación, se muestra el detalle de la inclusión y exclusión de características por aplicar en los modelos:

- Características: DMEstadoCivil, DMInstruccion, DPEstadoCivil, DMProfesionOcupacion, DPInstruccion, DRParentesco, DPProfesionOcupacion, DRInstruccion, NumeroHermanos, EstructuraFamiliar, DRProfesionOcupacion, IngresoMensual, LuzElectrica, AguaPotable, Telefono, Alcantarillado, Internet, TVCable, Celular, Computador, Discapacidad, FechaIngreso, MateriaDificultosa, ProcedeDeOtraInstitucion, ReprobadoRepetido, Enfermedad, Grado, Paralelo, Materia, nPQP1, nPQP2, nPQP3, PROM1, EXA1, QUI1, nQUI1, nSQP1, nSQP2, nSQP3, PROM2, EXA2, QUI2, nQUI2, ComportamientoPQP1, ComportamientoPQP2, ComportamientoPQP3, ComportamientoSQP1, ComportamientoSQP2, ComportamientoSQP3, PQP1, PQP2, PQP3, SQP1, SQP2, SQP3, ProyEscPQ, ProyEscSQ, Sector (TOTAL: 58 FEATURES)

- Atrubutos meta: ApellidosNombres, ListadoEstudiantes
- Atributos objetivos: nPromAnual, ComportamientoPQ, ComportamientoSQ, PromAnual
- Atributos removidos: 13 (Jornada, ProyEscSQP3, 2EXA20, Id, ProyEscPQP2, ProyEscSQP1, ProyEscPQP3, 1EXA20, 1PRO80, ProyEscPQP1, ProyEscSQP2, 2PRO80)

3. Resultados y Discusión

Con respecto de la hipótesis planteada, se detectó la existencia de una relación positiva entre el tipo de estructura familiar de tipo nuclear, aquella formada por formado por los padres y sus hijos e identificada por el atributo EstructuraFamiliar, así como otras condiciones socio económicas favorables y el nivel de aprendizaje alcanzado por los estudiantes. Para esto se fijó el promedio anual como atributo de clase o target, junto con la escala cualitativa de notas que se mostró en la sección de materiales y métodos, y se aplicó el algoritmo CN2 Rule Induction, para listar de forma ordenada las reglas de clasificación de los ejemplos con respecto de la clase. Además de establecer que las reglas tendrán una longitud máxima de cinco antecedentes y que para su generación de Covering Exclusive, se utilice la Entropía como heurística de búsqueda.

Ahora, dado que el árbol de decisión se puede linealizar en reglas de decisión, donde el resultado es el contenido del nodo hoja o atributo de clase, y las condiciones a lo largo de la ruta forman una conjunción en la cláusula if, se recurrió al empleo de Tree, para generar un árbol completo, con al menos dos instancias por nodos hojas, ni subconjuntos menores de cinco instancias. Además, se fijó la profundidad máxima o poda del árbol en 100 niveles.

Junto a los clasificadores CN2 Rule Induction y Tree, se empleó el clasificador probabilístico Naive Bayes porque funciona bien con atributos categóricos como el Target de esta hipótesis, e incluso si se tratase de un alto número de atributos de entrada. Su asunción de independencia entre los atributos de entrada, razón que deriva en su nombre, lo torna de muy rápida ejecución (Razaque et al., 2017).

Con respecto del entrenamiento de los algoritmos clasificadores CN2 Rule Induction y Tree, Se especificó un subconjunto de datos de tipo de muestreo determinista con el 70% de datos aleatorios, es decir, que, de las 6628 instancias de entrada, se toman como muestra 4640 y restan 1988 que más adelante se configuran como datos de prueba.

En lo concerniente a la evaluación de los modelos en los datos de prueba que son el 30% del Dataset, para el promedio sobre las clases (Average over classes), se determinó que:

- Dado que la precisión de la prueba depende de qué tan bien el test separó el grupo de datos probado y que el Area Under Curve ha fluctuado en el rango 0.974 – 0.991, se lo puede interpretar como Excelente para distinguir entre las clases positivas y negativas.
- El Accuracy, o proximidad de los resultados de la medición al valor real, también es excelente. CN2 alcanza la mayor Accuracy en instancias clasificadas correctamente con 0.974, la precisión más baja es la de Naive Bayes lo cual se

entiende dada su asunción de independencia entre los atributos de entrada o características con la que se ejecuta, aun así, alcanza un muy buen 0.900.

- La Precisión, entendida como la proporción de verdaderos positivos entre los casos clasificados como positivos es 0.973, guardando cercanía de milésimas con Recall, entendida como la proporción de verdaderos positivos entre todos los casos positivos en los datos. Excepto de nuevo para Naive Bayes, dónde decayó levemente a un 0.900. La media armónica ponderada de precisión y recuperación, F1, de la clasificación de los antecedentes de aprovechamiento y socio económicos con respecto al promedio anual en escala cuantitativa fue muy alta.

En suma, es poco probable que un árbol sea mejor clasificador que CN2 para este conjunto de datos, pero cualquiera de ellos luce ligeramente mejor que un Naive Bayes. La Tabla 3 resume estos hiper parámetros:

Model	AUC	CA	F1	Precision	Recall
Tree Promedizo Nominal	0.973	0.972	0.972	0.973	0.972
Naive Bayes	0.990	0.900	0.909	0.935	0.900
CN2 rule inducer	0.989	0.973	0.973	0.974	0.973

Tabla 3 – Tabla relacional de resultados para AUC, CA, F1, Precision y Recall, de cada modelo aplicado

A continuación, se listan algunos resultados de Tree junto con los de CN2.

- El Árbol de Decisión mostró que el 57.2% de los alumnos ALCANZA LOS APRENDIZAJES REQUERIDOS: desde 7,00 a 8,99. Dependiendo casi exclusivamente de las notas del segundo quimestre y del proyecto escolar. En el mismo sentido, los detalles socioeconómicos como la profesión del Padre fueron de especial relevancia en el caso dónde él DOMINA LOS APRENDIZAJES REQUERIDOS: desde 9,00 hasta 10,00. Es decir, para el segundo Quimestre se suele depender de las notas cosechadas en el primer quimestre, con independencia de si estas crecen o decrecen ligeramente, pero en el Primer Quimestre parece haber más relación con la ocupación del Padre para que el alumno llegue al máximo aprovechamiento, esto con cierta independencia de si el representante en la escuela es la madre u otra persona. La dependencia de las otras variables socioeconómicas no se observa en los primeros nueve niveles del árbol.
- El CN2 aporta datos similares, pero agrega detalles como que los alumnos que ingresaron en 2013, es decir, de los niveles superiores de la escuela y que ALCANZARON LOS APRENDIZAJES REQUERIDOS en el Quimestre 2 (7,00 a 8,99), tienen un 97% de probabilidad de ALCANZAR LOS APRENDIZAJES REQUERIDOS en el promedio Anual. Este dato corresponde a 180 ejemplos.
- El CN2 reporta que los alumnos cuya ocupación del Padre es Comerciante y que ALCANZARON LOS APRENDIZAJES REQUERIDOS en el Quimestre 2 (7,00 a 8,99), tienen un 96% de probabilidad DE ALCANZAR LOS APRENDIZAJES REQUERIDOS en el Promedio Anual (7,00 a 8,99). Este dato corresponde a 174 ejemplos.

- El CN2 reporta que los alumnos cuya estructura familiar es Extendida, es decir, una familia que puede incluir abuelos, tíos, primos y otros consanguíneos; y que ALCANZARON LOS APRENDIZAJES REQUERIDOS en el Quimestre 2 (7,00 a 8,99), tienen un 94% de probabilidad de ALCANZAR LOS APRENDIZAJES REQUERIDOS en el Promedio Anual (7,00 a 8,99). Este dato corresponde a 100 ejemplos.
- En el mismo sentido de ALCANZAR LOS APRENDIZAJES REQUERIDOS, se observa incidencias de problemas en la Materia de Lenguaje, como, por ejemplo, de enfermedades como Asma o un alto número de hermanos (5).
- Al igual que el Árbol de decisión, CN2 relaciona la nota del Primer Quimestre con la profesión del padre, al indicar que si el alumno DOMINA LOS APRENDIZAJES REQUERIDOS: desde 9,00 hasta 10,00 en el Quimestre 1 y la ocupación del Padre es COMERCIANTE, entonces tiene una probabilidad del 72,7% de llegar al máximo aprovechamiento (9-10) y 9,1% de probabilidad en cualquiera de los otros niveles de aprovechamiento. También influye favorablemente que los padres estén casados y que la madre tenga Educación Superior.

La menor precisión del Naive Bayes se aprecia mejor en la matriz de confusión de la Figura 2, de clasificaciones correctas. De izquierda a derecha y de arriba hacia abajo el orden de los valores del Target es: Domina los aprendizajes requeridos (9,00 hasta 10,00), Alcanza los aprendizajes requeridos (7,00 a 8,99), Próximo a alcanzar los aprendizajes requeridos (4,001 a 6,99) y No alcanza los aprendizajes requeridos (menos o igual a 4). El mayor problema de Naive Bayes sucede en clasificar cuando el alumno está Próximo a alcanzar los aprendizajes requeridos (4,001 a 6,99). En contraste con Naive Bayes, la Figura 1 muestra las matrices de confusión para Cn2 y Tree.

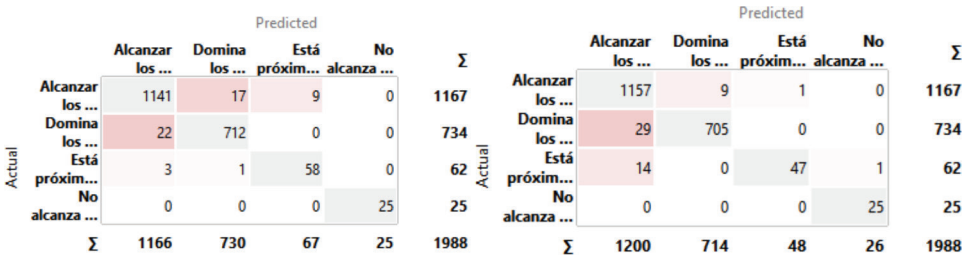


Figura 1 – Matriz de confusión del modelo clasificador CN2 Rules Induction y Tree

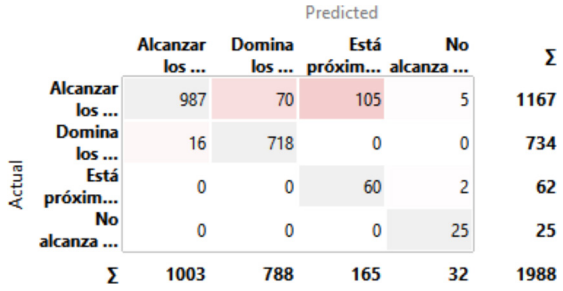


Figura 2 – Matriz de confusión del modelo clasificador Naive Bayes

Como una variante de la hipótesis anterior, empleando el equivalente cuantitativo del promedio anual, que es un valor comprendido entre 0 y 10, dejando que Tree calcule las divisiones adecuadas y las represente como nodos al generar el árbol, en tales circunstancias se esperó conseguir nuevas reglas acordes con las notas en su naturaleza numérica y finalmente se realizó las predicciones de los futuros promedios anuales.

Teniendo el promedio anual como Target y en escala numérica, se generó un árbol completo, con un número mínimo de instancias por hojas de 2, sin dividir subconjuntos menores de 5 instancias y fijando la profundidad máxima (poda) del árbol en 100 niveles.

Con respecto del entrenamiento del modelo en estas circunstancias, se especificó un tipo de muestreo determinista con el 70% de datos aleatorios para entrenamiento y 30% para pruebas. En la Tabla 4 se resaltan los mejores resultados obtenidos de la evaluación de estos modelos, para los siguientes hiper parámetros, dónde los valores resaltados en amarillo son las primeras mejores opciones y las celestes son las segundas mejores opciones. Los mejores resultados se consiguen con Training Data, lo que era de esperarse y de descartarse también, luego la segunda mejor opción es la validación cruzada y una tercera, sin embargo, la más recomendada es la de evaluar el modelo con los datos de testeo (30% de la data total en este caso).

Stratified 10-fold Cross validation	**Stratified Shuffle split, 10 random samples with 70% data**
MSE: 0.002911963998059096 RMSE: 0.05396261667172095 MAE: 0.023512351153688424 R2: 0.998467195728125	MSE: 0.004033378387145827 RMSE: 0.06350888431665154 MAE: 0.02871190698927583 R2: 0.9979114729772719
No sampling, test on training data	No sampling, test on testing data
MSE: 0.00039862889962690926 RMSE: 0.019965693066530628 MAE: 0.006639986073540057 R2: 0.9997901690815381	MSE: 0.0041699828490290285 RMSE: 0.06457540436597381 MAE: 0.02201208099472545 R2: 0.9977344046828394
MSE, Error medio al cuadrado: Los valores más cercanos a 0 son mejores en esta medida de la calidad de un estimador. RMSE, El error cuadrático medio: cuantifica cuán diferente es un conjunto de valores, cuanto más pequeño es su valor, es mejor. MAE, Error absoluto medio: MAE mide la magnitud media de los errores en un conjunto de predicciones, sin tener en cuenta su dirección. R2: Es el porcentaje de variación de la variable de respuesta que explica su relación con una o más variables predictoras. R2 es mejor si es mayor, y significa mejor ajuste del modelo a sus datos.	

Tabla 4 – Resultados obtenidos según diversos tipos de validación de los modelos

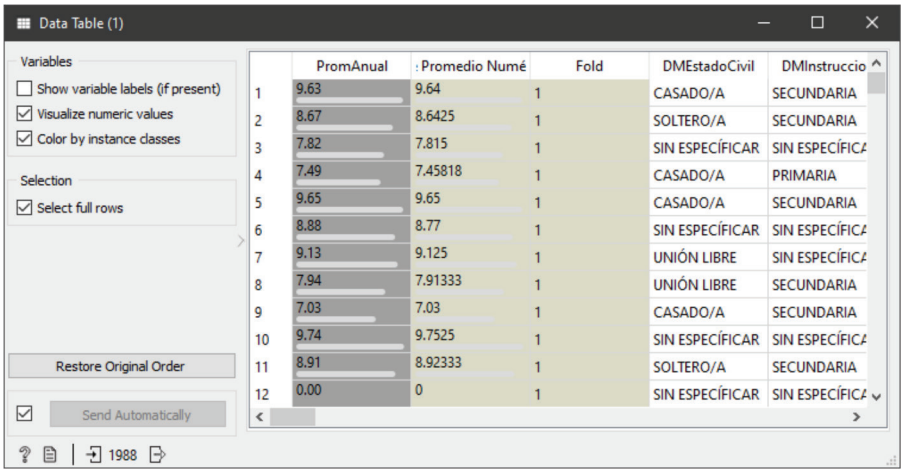
Además, se listan algunos resultados:

- En 156 casos, las notas de 6.4 +/- 0.5 en el Quimestre 1 significan que en el promedio anual el alumno es PRÓXIMO A ALCANZAR LOS APRENDIZAJES REQUERIDOS, siempre que la nota del Quimestre 2 sea 6.9 +/- 0.2. En adelante en el Quimestre 1, en 21 casos, suelen tener 7.4 +/- 0.1 los alumnos cuyos padres

tienen una profesión en la que están laborando. En los otros 63 casos, suele influir tanto la profesión de los padres como si están casados, para que el alumno esté apenas PRÓXIMO A ALCANZAR LOS APRENDIZAJES REQUERIDOS. Incide también si tiene problemas en las materias de Matemáticas e Inglés. En menor medida, es decir en niveles más bajos del árbol, afecta la tenencia de servicios como TV por cable o el grado que cursan en la escuela.

- En 1915 casos, las notas de 9.2 +/- 0.2 en el Quimestre 1 significan que en el promedio anual el alumno DOMINA LOS APRENDIZAJES REQUERIDOS, siempre que mantenga la misma regularidad en el Quimestre 2, lo que a su vez se relaciona con una buena regularidad con la nota del Quimestre 1. En los niveles inferiores del árbol, asoman el comportamiento del alumno (que es cualitativo: A, B y C), la colegiatura alcanzada por los padres y la profesión de los padres.
- En 2504 casos, las notas de 8.2 +/- 0.3 en el Quimestre 1 significan que en el promedio anual el alumno ALCANZA (con las justas) LOS APRENDIZAJES REQUERIDOS, siempre que mantenga la misma regularidad en el Quimestre 2, lo que a su vez se relaciona con una buena regularidad con la nota del Quimestre 1 (Igual que en la Hipótesis 1). En los niveles inferiores del árbol, asoman el tener problemas en materias relacionadas al Arte y el Lenguaje, el estado civil de los padres, el número de hermanos, e incluso el ingreso familiar. En menor medida, influye también el sector, lo cual no sorprende si en Ecuador, se privilegia que los alumnos de las escuelas sean habitantes del sector dónde se localiza la escuela.
- Para finalizar, en 55 casos, existe una estrecha relación, casi determinante entre el incumplimiento de los proyectos escolares y que el alumno NO ALCANCE LOS APRENDIZAJES REQUERIDOS.

Con los datos reportados en el modelo, se realizó una predicción de como serían los siguientes promedios anuales, resultando los que se muestran parcialmente en la Figura 3, en la segunda columna.



	PromAnual	Promedio Numé	Fold	DMEstadoCivil	DMInstruccio
1	9.63	9.64	1	CASADO/A	SECUNDARIA
2	8.67	8.6425	1	SOLTERO/A	SECUNDARIA
3	7.82	7.815	1	SIN ESPECÍFICAR	SIN ESPECÍFICA
4	7.49	7.45818	1	CASADO/A	PRIMARIA
5	9.65	9.65	1	CASADO/A	SECUNDARIA
6	8.88	8.77	1	SIN ESPECÍFICAR	SIN ESPECÍFICA
7	9.13	9.125	1	UNIÓN LIBRE	SIN ESPECÍFICA
8	7.94	7.91333	1	UNIÓN LIBRE	SECUNDARIA
9	7.03	7.03	1	CASADO/A	SECUNDARIA
10	9.74	9.7525	1	SIN ESPECÍFICAR	SIN ESPECÍFICA
11	8.91	8.92333	1	SOLTERO/A	SECUNDARIA
12	0.00	0	1	SIN ESPECÍFICAR	SIN ESPECÍFICA

Figura 3 – Vista parcial de las predicciones obtenidas, la primera columna corresponde a la predicción, la segunda corresponde al valor actual del promedio

4. Discusión

Con el empleo de Reglas de Asociación y Árboles de Decisión, en esta investigación se identificó a factores de tipo socioeconómicos que pueden influir o relacionarse con el aprovechamiento de los estudiantes y se ha determinado, que estos factores suelen tener mayor efecto en el primer quimestre de los dos que componen un periodo académico, pues en el segundo quimestre, el mayor dominio de aprendizajes reflejado en notas se relaciona más con las calificaciones, de ese modo se complementa a otras interesantes propuestas basadas en algoritmos genéticos y redes neuronales, enfocados en predecir una calificación como lo son los trabajos de (Li & Wang, 2022; Lodhi & Kukreja, 2022; Sun, 2022). En investigaciones que emplearon árboles de decisión como las de (Jiang, 2021; Yang, 2021) se ha logrado precisiones sobre el 88% y en la presente se alcanzó valores por sobre el 90%.

Dentro de los aspectos sociales de respuestas más frecuentes en los modelos, están su trabajo y su escolaridad alcanzada, adicionando el estado civil de los padres en relación con los trabajos de (Helal et al., 2018; Roh et al., 2016). En menor medida, el comportamiento o conducta de los alumnos en la escuela, así como dato llamativo, que los alumnos con más hermanos suelen alcanzar con lo justo sus aprendizajes requeridos, lo que de modo indirecto se puede relacionar con el ingreso familiar y del grado que cursa el alumno, mismo que se estimó a partir del año de ingreso del alumno a la institución.

En detalle, el Árbol de Decisión muestra que el 57.2% de los alumnos ALCANZA LOS APRENDIZAJES REQUERIDOS: desde 7,00 a 8,99. Dependiendo casi exclusivamente de las notas del segundo quimestre y del proyecto escolar. En el mismo sentido, los detalles socioeconómicos como la profesión del Padre son de especial relevancia en el caso dónde él DOMINA LOS APRENDIZAJES REQUERIDOS: desde 9,00 hasta 10,00. Es decir, para el segundo Quimestre se suele depender de las notas cosechadas en el primer quimestre, con independencia de si estas crecen o decrecen ligeramente, pero en el Primer Quimestre parece haber más relación con la ocupación del Padre para que el alumno llegue al máximo aprovechamiento, esto con cierta independencia de si el representante en la escuela es la madre u otra persona. La dependencia de las otras variables socioeconómicas no se observa en los primeros 9 niveles del árbol.

5. Conclusiones

Los factores socioeconómicos influyen en el promedio anual de los alumnos, de modo especial en primera parte del periodo, pues se ha notado que, en el segundo quimestre, el mayor dominio de aprendizajes se relaciona más con las calificaciones asociada a cada componente calificado del parcial propiamente.

De entre los factores socioeconómicos, en concordancia con los modelos, se establece que los de más influencia son el estado civil de los padres, su trabajo, su escolaridad alcanzada y en menor medida, el comportamiento o conducta de los alumnos en la escuela, además, llama la atención además que los alumnos con más hermanos suelen alcanzar con lo justo los aprendizajes requeridos y, que existe poca influencia del ingreso familiar y del grado que cursa el alumno, mismo que se estimó a partir del año de ingreso del alumno a la institución.

Respecto de las herramientas de minería de datos, estas son de gran importancia y utilidad para descubrir patrones y regularidades entre grandes volúmenes de datos, sin embargo, sigue siendo transcendental conocer el dominio del conjunto de los datos para una óptima preparación de estos, pues la preparación de los datos condiciona de sobremanera los resultados generados en los modelos. En los datos analizados, los clasificadores alcanzan excelentes Accuracy siendo ligeramente menor Naive Bayes, pero en todos los casos el Accuracy fue superior al 90%.

Finalmente, éste trabajo presentó la aplicación de modelos de minería de datos en la detección de incidencias de factores socioeconómicos en el aprovechamiento escolar, pero puede ampliarse para abordar las decisiones y su ejecución en pro de solucionar los posibles inconvenientes de los alumnos y reevaluarlos periódicamente con modelos similares. También es posible desarrollar modelos de analítica de datos para efectuar predicciones con oportunidad de tiempo, tan pronto se disponga de datos, sin esperar que el problema llegue a suscitarse.

Referencias

Agrawal, R., & Srikant, R. (1994). Fast algorithms for mining association rules. *Proc. 20th Int. Conf. Very Large Data Bases, VLDB*, *1215*, 487–499.

Bedir, H. (2019). Pre-service ELT teachers' beliefs and perceptions on 21st century learning and innovation skills (4Cs). *Journal of Language and Linguistic Studies*, *15*(1), 231–246.

Entwisle, D. R., & Alexander, K. L. (1992). Summer Setback: Race, Poverty, School Composition, and Mathematics Achievement in the First Two Years of School. *American Sociological Review*, *57*(1), 72. https://doi.org/10.2307/2096145

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI Magazine*, *17*(3), 37.

Fu, Q.-K., & Hwang, G.-J. (2018). Trends in mobile technology-supported collaborative learning: A systematic review of journal publications from 2007 to 2016. *Computers & Education*, *119*, 129–143.

Hanushek, E. A., Peterson, P. E., Talpey, L. M., & Woessmann, L. (2019). The achievement gap fails to close. *Education Next*, *19*(3), 8–17.

Helal, S., Li, J., Liu, L., Ebrahimie, E., Dawson, S., Murray, D. J., & Long, Q. (2018). Predicting academic performance by considering student heterogeneity. *Knowledge-Based Systems*, *161*, 134–146.

Ismail, S. N., Nur, A. H. B., Raman, A., & Purnomo, Y. W. (2019). A Mixed-Method Study of the Epistemological Teacher-Beliefs towards Educational Research in Classroom Teaching Practices. *International Journal of Instruction*, *12*(3), 393–406.

Jiang, X. (2021). Online English teaching course score analysis based on decision tree mining algorithm. *Complexity*, *2021*.

Li, B., & Wang, S. (2022). Design of the Online Learning System for College Physical Education Teaching Based on the BP Neural Network. *Wireless Communications and Mobile Computing*, *2022*.

Lodhi, S., & Kukreja, V. (2022). Deep Neural Network for Recognition of Enlarged Mathematical Corpus. *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, 411–415.

Macías-Mendoza, D., Santamaría-Philco, A., Zavala-Alcívar, A., Ayoví-Ramírez, M., & Pincay-Ponce, J. I. (2016). Gestión pedagógica: clima social en el aula, desde la percepción de estudiantes y profesores. *REFCalE: Revista Electrónica Formación y Calidad Educativa. ISSN 1390-9010*, *4*(1), 125–138.

McNeish, D., & Wolf, M. G. (2020). Thinking twice about sum scores. *Behavior Research Methods*, *52*(6), 2287–2305.

Ng-Knight, T., & Schoon, I. (2017). Can Locus of Control Compensate for Socioeconomic Adversity in the Transition from School to Work? *Journal of Youth and Adolescence*, *46*(10), 2114–2128. https://doi.org/10.1007/s10964-017-0720-6

Pincay-Ponce, J. I., Angulo-Murillo, N. G., Herrera-Tapia, J. S., & Delgado-Muentes, W. R. (2020). Técnicas de minería de datos como soporte para la gestión de un sistema de comercialización de energía eléctrica. *Mikarimin. Revista Científica Multidisciplinaria. e-ISSN 2528-7842*, *6*(2), 19–34. https://tinyurl.com/y47xak9m

Pincay-Ponce, J. I., Sánchez-Andrade, D. A., Caicedo-Ávila, I. V., & Macías-Valencia, D. G. (2020). Clasificación de pacientes según su posibilidad de adquirir diabetes mellitus empleando algoritmos de machine learning. *IV Congreso Internacional: Tecnologías de La Información y Computación (CITIC 2020)*, 1–13.

Razaque, F., Soomro, N., Shaikh, S. A., Soomro, S., Samo, J. A., Kumar, N., & Dharejo, H. (2017). Using naïve bayes algorithm to students' bachelor academic performances analysis. *2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, 1–5.

Roh, S.-B., Oh, S.-K., Park, E. K., & Choi, W. Z. (2016). Design of radial basis function neural networks with principal component analysis and linear discriminant analysis for black plastic identification. *2016 Joint 8th International Conference on Soft Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems (ISIS)*, 764–768.

Sharma, A., Ram, A., & Bansal, A. (2020). Feature Extraction Mining for Student Performance Analysis. In *Proceedings of ICETIT 2019* (pp. 785–797). Springer.

Sun, G. (2022). Application of GA-BP Neural Network in Online Education Quality Evaluation in Colleges and Universities. *Mobile Information Systems*, *2022*.

van Zwieten, A., Teixeira-Pinto, A., Lah, S., Nassar, N., Craig, J. C., & Wong, G. (2021). Socioeconomic Status During Childhood and Academic Achievement in Secondary School. *Academic Pediatrics*, *21*(5), 838–848. https://doi.org/10.1016/j.acap.2020.10.013

Yang, Y. (2021). The evaluation of online education course performance using decision tree mining algorithm. *Complexity*, *2021*.

Critérios Editoriais

A RISTI (Revista Ibérica de Sistemas e Tecnologias de Informação) é um periódico científico, que foca a investigação e a aplicação prática inovadora no domínio dos sistemas e tecnologias de informação.

O Conselho Editorial da RISTI incentiva potenciais autores a submeterem artigos originais e inovadores para avaliação pelo Conselho Científico.

A submissão de artigos para publicação na RISTI deve realizar-se de acordo com as chamadas de artigos e as instruções e normas disponibilizadas no sítio Web da revista (http://www.risti.xyz).

Todos os artigos submetidos são avaliados por um conjunto de membros do Conselho Científico, não inferior a três elementos.

Em cada número da revista são publicados entre cinco a oito dos melhores artigos submetidos.

Criterios Editoriales

La RISTI (Revista Ibérica de Sistemas y Tecnologías de la Información) es un periódico científico, centrado en la investigación y en la aplicación práctica innovadora en el dominio de los sistemas y tecnologías de la información.

El Consejo Editorial de la RISTI incentiva autores potenciales a enviar sus artículos originales e innovadores para evaluación por el Consejo Científico.

Lo envío de artículos para publicación en la RISTI debe hacerse de conformidad con las llamadas de los artículos y las instrucciones y normas establecidas en el sitio Web de la revista (http://www.risti.xyz).

Todos los trabajos enviados son evaluados por un número de miembros del Consejo Científico de no menos de tres elementos.

En cada número de la revista se publican cinco a ocho de los mejores artículos enviados.

Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

©RISTI 2022 http://www.risti.xyz

