



ISSN: 1646-9895

Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

J u n h o 1 9 • J u n e 1 9



©AISTI 2019 <http://www.aisti.eu>

Nº 32

Edição / Edición

Nº 32, 06/2019

Tiragem / Tirage: 1000

Preço por número / Precio por número: 17,5€

Subscrição anual / Suscripción anual: 30€ (2 números)

ISSN: 1646-9895

Depósito legal:

Indexação / Indexación

Academic Journals Database, CiteFactor, Dialnet, DOAJ, DOI, EBSCO, GALE, IndexCopernicus, Index of Information Systems Journals, ISI Web of Knowledge, Latindex, ProQuest, QUALIS, SciELO, SCImago, Scopus, SIS, Ulrich's.

Propriedade e Publicação / Propriedad y Publicación

AISTI – Associação Ibérica de Sistemas e Tecnologias de Informação

Rua Quinta do Roseiral 76, 4435-209 Rio Tinto, Portugal

E-mail: aistic@gmail.com

Web: <http://www.risti.xyz>

Director

Álvaro Rocha, Universidade de Coimbra

Coordenadores da Edição / Issue Coordinators

Jeimy Cano, Universidad de los Andes, Colombia

Álvaro Rocha, Universidade de Coimbra, Portugal

Conselho Editorial / Editorial Board

Carlos Ferrás Sexto, Universidad de Santiago de Compostela

Gonçalo Paiva Dias, Universidade de Aveiro

Jose Antonio Calvo-Manzano Villalón, Universidad Politécnica de Madrid

Luís Paulo Reis, FEUP, Universidade do Porto

Manuel Pérez Cota, Universidad de Vigo

Ramiro Gonçalves, Universidade de Trás-os-Montes e Alto Douro

Conselho Científico / Scientific Board

Adolfo Lozano-Tello, Universidad de Extremadura, ES

Adrián Hiebra Pardo, Universidad de Santiago de Compostela, ES

Alberto Fernández, Universidad Rey Juan Carlos, ES

Alberto Bugarín, Universidad de Santiago de Compostela, ES

Alejandro Medina, Universidad Politécnica de Chiapas, MX

Alejandro Peña, Escuela de Ingeniería de Antioquia, CO

Alexandre L'Erario, Universidade Tecnológica Federal do Paraná, BR

Ana Azevedo, Instituto Politécnico do Porto, PT

Ana Isabel Veloso, Universidade de Aveiro, PT

Ana Maria Correia, ISEGI, Universidade Nova de Lisboa, PT

Ana Paula Afonso, Instituto Politécnico do Porto, PT

Anabela Mesquita, Instituto Politécnico do Porto, PT

Angelica Caro, Universidad del Bío-Bío, CL

António Coelho, FEUP, Universidade do Porto, PT

António Godinho, ISLA-Gaia, PT

Antonio Jesus Garcia Loureiro, Universidad de Santiago de Compostela, ES

António Pereira, Instituto Politécnico de Leiria, PT

Armando Mendes, Universidade dos Açores, PT

Arnaldo Martins, Universidade de Aveiro, PT
Arturo J. Méndez, Universidad de Vigo, ES
Baltasar García Pérez-Schofield, Universidad de Vigo, ES
Bráulio Alturas, ISCTE - Instituto Universitário de Lisboa, PT
Brígida Mónica Faria, ESTSP, Instituto Politécnico do Porto, PT
Carlos Costa, Universidade de Aveiro, PT
Carlos Carreto, Instituto Politécnico da Guarda, PT
Carlos Morais, Instituto Politécnico de Bragança, PT
Carlos Vaz de Carvalho, Instituto Politécnico do Porto, PT
Carmen Galvez, Universidad de Granada, ES
Ciro Martins, Universidade de Aveiro, PT
Daniel Polónia, Universidade de Aveiro, PT
Daniel Riesco, Universidad Nacional de San Luis, AR
David Fonseca, Universitat Ramon Llull, ES
David Ramos Valcarcel, Universidad de Vigo, ES
Diego Ordóñez-Camacho, Universidad Tecnológica Equinoccial, EC
Dora Simões, Universidade de Aveiro, PT
Eduardo Sánchez Vila, Universidad de Santiago de Compostela, ES
Emiliano Reynares, CIDISI - UTN FRSF - CONICET, AR
Enric Mor, Universitat Oberta de Catalunya, ES
Eusébio Ferreira da Costa, Escola Superior de Tecnologias de Fafe, PT
Fábio Magalhães, Universidade Nove de Julho, BR
Feliz Gouveia, Universidade Fernando Pessoa, PT
Fernando Bandeira, Universidade Fernando Pessoa, PT
Fernando Moreira, Universidade Portucalense, PT
Francisco Restivo, Universidade Católica Portuguesa, PT
Frederico Branco, Universidade de Trás-os-Montes e Alto Douro, PT
Gerardo Gonzalez Filgueira, Universidad da Coruña, ES
Germano Montejano, Universidad Nacional de San Luis, AR
Guilhermina Lobato Miranda, Universidade de Lisboa, PT
Hélder Zagalo, Universidade de Aveiro, PT
Hélia Guerra, Universidade dos Açores, PT
Henrique Santos, Universidade do Minho, PT
Higino Ramos, Universidad de Salamanca, ES

Isabel Pedrosa, Instituto Politécnico de Coimbra, PT
Isaura Ribeiro, Universidade dos Açores, PT
Isidro Calvo, Universidad del País Vasco (UPV/EHU), ES
Ismael Etxeberria-Agiriano, Universidad del País Vasco (UPV/EHU), ES
Ivan Garcia, Universidad Tecnológica de la Mixteca, MX
Javier Garcia Tobio, CESGA-Centro de Supercomputacion de Galicia, ES
Jeimy Cano, Universidad de los Andes, CO
Jezreel Mejia, Centro de Investigación en Matemática (CIMAT), MX
João Pascual Faria, FEUP, Universidade do Porto, PT
João Paulo Costa, Universidade de Coimbra, PT
João Tavares, FEUP, Universidade do Porto, PT
Joaquim José Gonçalves, Instituto Politécnico do Cávado e do Ave, PT
Joaquim Madeira, Universidade de Aveiro, PT
Joaquim Reis, ISCTE - Instituto Universitário de Lisboa, PT
Jörg Thomaschewski, University of Applied Sciences OOW - Emden, DE
Jorge Dias Villegas, Universidad de la Frontera, CL
Jose Alfonso Aguilar, Universidad Autonoma de Sinaloa, MX
José Braga de Vasconcelos, Universidade Atlântica, PT
José Cascalho, Universidade dos Açores, PT
José Felipe Cocón Juárez, Universidad Autónoma del Carmen, MX
Jose J. Pazos-Arias, Universidad de Vigo, ES
José Luís Silva, Instituto Universitário de Lisboa (ISCTE-IUL), PT
José Paulo Lousado, Instituto Politécnico de Viseu, PT
José Luis Pestrana Brincones, Universidad de Málaga
José Luís Reis, ISMAI - Instituto Superior da Maia, PT
Jose M Molina, Universidad Carlos III de Madrid, ES
José Martins, Universidade de Trás-os-Montes e Alto Douro, PT
Jose Maria de Fuentes, Universidad Carlos III de Madrid, ES
Jose R. R. Viqueira, Universidade de Santiago de Compostela, ES
José Silvestre Silva, Academia Militar, PT
Josep M. Marco-Simó, Universitat Oberta de Catalunya, ES
Juan D'Amato, PLADEMA-UNCPBA-CONICET, AR
Juan M. Santos Gago, Universidad de Vigo, ES
Juan Manuel Fernández-Luna, Universidad de Granada, ES

Leonardo Bermon, Universidad Nacional de Colombia, CO
Leila Weitzel, Universidade Federal Fluminense, BR
Luis Alvarez Sabucedo, Universidad de Vigo, ES
Luis de Campos, Universidad de Granada, ES
Luis Fernandez-Sanz, Universidad de Alcalá, ES
Luís Ferreira, Instituto Politécnico do Cávado e do Ave, PT
Luis Vilán-Crespo, Universidad de Vigo, ES
Luisa María Romero-Moreno, Universidad de Sevilla, ES
Luisa Miranda, Instituto Politécnico de Bragança, PT
Lus Sussy Bayona Ore, Universidad Nacional Mayor de San Marcos, PE
Magdalena Arcilla Cobián, Universidade Nacional de Educación a Distancia, ES
Manuel Jose Fernandez Iglesias, Universidad de Vigo, ES
Marco Painho, ISEGI, Universidade Nova de Lisboa, PT
Maria Hallo, Escuela Politécnica Nacional, EC
María J. Lado, Universidad de Vigo, ES
Maria João Castro, Instituto Politécnico do Porto, PT
Maria João Ferreira, Universidade Portucalense, PT
Maria João Gomes, Universidade do Minho, PT
Maria José Angélico, Instituto Politécnico do Porto, PT
Maria José Marcelino, Universidade de Coimbra, PT
Maria José Sousa, Universidade Europeia, PT
Marisol B. Correia, Universidade do Algarve, PT
Maristela Holanda, Universidade de Brasília, BR
Martín Llamas Nistal, Universidad de Vigo, ES
Matías García Rivera, Universidad de Vigo, ES
Mercedes Ruiz, Universidad de Cádiz, ES
Miguel A. Brito, Universidade do Minho, PT
Miguel Bugalho, Universidade Europeia, PT
Miguel Casquilho, IST, Universidade de Lisboa, PT
Mirna Ariadna Muñoz Mata, Centro de Investigación en Matemáticas (CIMAT), MX
Nelson Rocha, Universidade de Aveiro, PT
Nuno Lau, Universidade de Aveiro, PT
Nuno Ribeiro, Universidade Fernando Pessoa, PT
Oscar Mealha, Universidade de Aveiro, PT

Paula Prata, Universidade da Beira Interior, PT
Paulo Martins, Universidade de Trás-os-Montes e Alto Douro, PT
Paulo Pinto, FCT, Universidade Nova de Lisboa, PT
Pedro Miguel Moreira, Instituto Politécnico de Viana do Castelo, PT
Pedro Nogueira Ramos, ISCTE - Instituto Universitário de Lisboa, PT
Pedro Sánchez Palma, Universidad Politécnica de Cartagena, ES
Pedro Sanz Angulo, Universidad de Valladolid, ES
Pilar Mareca Lopez, Universidad Politécnica de Madrid, ES
Raul Laureano, ISCTE - Instituto Universitário de Lisboa, PT
Reinaldo Bianchi, Centro Universitário da FEI, BR
Rita Santos, Universidade de Aveiro, PT
Rodolfo Miranda Barros, Universidade Estadual de Londrina, BR
Rubén González Crespo, Universidad Internacional de La Rioja, ES
Rui Cruz, IST, Universidade de Lisboa, PT
Rui José, Universidade do Minho, PT
Rui Pedro Marques, Universidade de Aveiro, PT
Santiago Gonzales Sánchez, Universidad Inca Garcilaso de la Vega, PE
Sergio Gálvez Rojas, Universidad de Málaga, ES
Sérgio Guerreiro, Universidade Lusófona de Humanidades e Tecnologias, PT
Silvia Fernandes, Universidade do Algarve, PT
Solange N Alves de Souza, Universidade de São Paulo, BR
Tomás San Feliu Gilabert, Universidad Politécnica de Madrid, ES
Valéria Farinazzo Martins, Universidade Presbiteriana Mackenzie, BR
Victor Hugo Medina Garcia, Universidad Distrital Francisco José de Caldas, CO
Vitor Carvalho, Instituto Politécnico do Cávado e do Ave, PT
Vitor Santos, ISEGI, Universidade Nova de Lisboa, PT
Wagner Tanaka Botelho, Universidade Federal do ABC, BR
Xose A. Vila, Universidad de Vigo, ES

Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital

Cybersecurity and cyberdefense. Challenges and perspectives in a digital world

Jeimy J. Cano M.¹, Alvaro Rocha²

jcano@uniandes.edu.co, amrocha@dei.uc.pt

¹ Facultad de Derecho, Universidad de los Andes, Bogotá, Cra 1E No. 18A-10, Bogotá, Colombia.

² Universidade de Coimbra, Departamento de Engenharia Informática, Pólo II - Pinhal de Marrocos, 3030-290 Coimbra, Portugal.

DOI: 10.17013/risti.32.0

1. Introducción

La acelerada evolución de la convergencia tecnológica, el aumento de la densidad digital y la asimetría de la información en una sociedad cada vez más digital y tecnológicamente modificada, establece un escenario de análisis más elaborado y complejo, que exige de parte de los analistas de negocio, de seguridad de la información y de ciberseguridad, una vista mucho más holística y el entendimiento de relaciones emergentes antes ignoradas por los saberes disciplinares y segmentados.

En este sentido, se establecen nuevos retos en el contexto de la ciberseguridad y ciberdefensa, donde ya no es suficiente conocer y entender las amenazas conocidas del entorno, sino configurar propuestas actualizadas o novedosas que permitan, no solo proteger y asegurar los activos de información, sino defender y anticipar escenarios desconocidos o inciertos, que habiliten a las organizaciones y a los países para identificar y gestionar riesgos latentes y emergentes con una vista más sistémica.

En este marco, la trigésima segunda edición de la RISTI (Revista Ibérica de Sistemas y Tecnologías de la Información) se centra en las reflexiones, propuestas y avances en los temas de seguridad de la información, ciberseguridad y ciberdefensa, que busca conectar las realidades digitales de las organizaciones y las naciones, con las disrupciones, amenazas y riesgos derivados de un escenario cada vez más volátil, incierto, complejo y ambiguo.

El conjunto de ocho artículos publicados en este número de RISTI fue el resultado de un exigente proceso de evaluación por parte de los miembros del comité científico de los treinta y cinco trabajos presentados por los autores, procedentes de una colaboración entre España y México, tres de Argentina, un trabajo conjunto entre Colombia y España, Ecuador, Cuba y Chile, lo que corresponde a una tasa de aceptación del 22%.

2. Estructura

El primer artículo, con el título “Validación del contenido de un guion de entrevista sobre la competencia digital docente en Educación Superior”, presenta un estudio para obtener evidencias de validez del contenido de un guión de entrevista en profundidad, en el marco de una investigación sobre el desarrollo de la competencia digital de profesores universitarios. Como resultado se obtuvo una versión acotada del guión propuesto y se identificaron aspectos en debate sobre la conceptualización de esta competencia docente en la Educación Superior.

El segundo artículo, con el título “Herramienta para el Análisis Forense de Correos Electrónicos”, introduce una herramienta para el análisis forense de correos electrónicos a partir de la cabecera de los mismos y la utiliza para instanciar una ontología definida para responder a los puntos de pericia solicitados sobre éstos correos. El documento detalla cada componente de la herramienta y se ejemplifica su uso mediante un caso de estudio sobre análisis forense de un correo electrónico.

El tercer artículo, con el título “Auditorías en Ciberseguridad. Un modelo de aplicación general para empresas y naciones”, detalla los resultados de un estudio de implementación y validación del Modelo de Auditoría de Ciberseguridad (CSAM), en un ejercicio de casos múltiples en una universidad canadiense. El artículo concluye ilustrando los resultados de la aplicación del modelo en sus diferentes vistas, con información relevante para la toma de decisiones futuras, que permita ajustar las limitaciones de ciberseguridad identificadas, mejorar sus dominios y controles, y de esta manera, implementar y probar de manera eficiente este modelo en cualquier organización o país.

El cuarto artículo, con el título “Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada”, aborda del reto de repensar la estructura jerárquica y centralizada de una infraestructura de llave pública (en inglés Public Key Infrastructure) hacia una propuesta descentralizada y distribuida basada en tecnología de cadena de bloques (en inglés blockchain) que permita mayor transparencia en la emisión de certificados, disminución del riesgo y aumento de la confiabilidad. Como resultado, la arquitectura propuesta proporciona a los usuarios mayor eficiencia en el proceso de gestión de certificados, con ahorro de tiempo y simplificación de trámites y configuraciones vigentes en el modelo tradicional.

El quinto artículo, con el título “Balanceo De Carga Basado En Criterios Combinados, Para Servidores, Utilizando Tecnologías De Redes Definidas Por Software”, ilustra un algoritmo de balanceo de carga basado en un sistema de criterios combinados, que utiliza tecnologías de redes definidas por software para obtener en tiempo de ejecución, parámetros desde distintos puntos de la red y seleccionar el servidor con las mejores condiciones para responder. Los resultados del experimento utilizando la herramienta

Mininet, demuestran que el balanceador de carga basado en criterios combinados, reduce, hasta en un 50%, el tiempo de respuesta del servidor en comparación con el método tradicional Round Robin.

El sexto artículo, con el título “Ciberseguridad del Sistema de Control Industrial de la Planta Cloro-Sosa ELQUIM”, desarrolla la implementación de una estrategia de defensa en profundidad para la protección del sistema de control industrial de la planta de producción de Cloro-Sosa de la empresa ELQUIM. Para ello, se sigue la aplicación de la guía de seguridad para sistemas de control industrial del NIST, articulando sus resultados con software hecho en el país y software para asegurar la soberanía tecnológica de la solución.

El séptimo artículo, con el título “KE-SER: Un sistema basado en el conocimiento y la experiencia para dar soporte a arquitectos de software en aspectos de seguridad”, propone un sistema experto, denominado KE-SER (por sus siglas en inglés *Knowledge & Experience – SEcurity Recommendations*) para brindar apoyo, desde el punto de vista de la seguridad, a los arquitectos de software para que puedan tomar decisiones durante el diseño arquitectónico de forma consciente e informada. En este trabajo, se describe un sistema capaz de realizar recomendaciones para satisfacer los requerimientos de seguridad de los sistemas a construir. Las recomendaciones pueden estar basadas en el conocimiento capturado de expertos en seguridad o en experiencias pasadas de arquitectos que diseñaron arquitecturas de sistemas con requerimientos similares.

Finalmente, el último artículo, con el título “Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información”, detalla una nueva versión del enfoque de programación de conjunto de respuestas (en inglés ASP - *Answer Set Programming*) para tomar una decisión sobre inversiones en seguridad de la información en un escenario con restricciones presupuestarias. La propuesta se compara con el desarrollo del problema utilizando programación lineal (LP), ilustrando la fase de modelado y el rendimiento computacional de ambas soluciones. El modelo ASP presenta tiempos de resolución del tipo exponencial a medida que aumenta el número de controles sobre los que debe decidirse, lo que implica que si se quieren respuestas rápidas, se debe usar una baja cantidad de controles.

3. Agradecimientos

Esta introducción termina expresando nuestra gratitud a todos los autores y revisores involucrados en esta edición, esperando que este número de RISTI sea una lectura interesante para todos aquellos que se movilizan en torno a los retos de la ciberseguridad y la ciberdefensa. Un agradecimiento especial a AISTI, propietaria y promotora de RISTI, así como a las Bases de Datos de Revistas Académicas como CiteFactor, Compendex, Dialnet, DOAJ, DOI, EBSCO, GALE, IndexCopernicus, Index of Information Systems Journals, ISI Web of Knowledge, Latindex, ProQuest, QUALIS, SciELO, SCImago y Scopus, entidades que han contribuido a convertir a RISTI en un referente en este competitivo mercado de revistas científicas.

Índice / Index

EDITORIAL

Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital	ix
<i>Jeimy J. Cano M., Alvaro Rocha</i>	

ARTIGOS / ARTICULOS / ARTICLES

Validación del contenido de un guion de entrevista sobre la competencia digital docente en Educación Superior.....	1
<i>Angelina Lorelí Padilla-Hernández, Vanesa M.^a Gámiz-Sánchez, M.^a Asunción Romero-López</i>	
OntoFoCE: Herramienta para el Análisis Forense de Correos Electrónicos	17
<i>Enzo Notario, Beatriz Parra de Gallo, Marcela Vegetti, Horacio Leone</i>	
Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones.....	33
<i>Régner Sabillón, Jeimy J. Cano M.</i>	
Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada	49
<i>Ignacio Gallardo, Patricia Bazan, Paula Venosa</i>	
Aplicación de Balanceo De Carga Dinámico Para Servidores, Basada En Redes Definidas Por Software.	67
<i>Carlos Enrique MINDA GILCES, Rubén PACHECO VILLAMAR</i>	
Ciberseguridad del Sistema de Control Industrial de la Planta Cloro-Sosa ELQUIM.	83
<i>Héctor Enrique Socarrás, Ivan Santana</i>	
KE-SER: Un sistema basado en el conocimiento y la experiencia para dar soporte a arquitectos de software en aspectos de seguridad	97
<i>María Celeste Carignano, Silvio Gonnet, Horacio Leone</i>	
Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información	113
<i>Mauricio Diéguez, Carlos Cares</i>	

Validación del contenido de un guion de entrevista sobre la competencia digital docente en Educación Superior

Angelina Lorelí Padilla-Hernández¹, Vanesa M.^a Gámiz-Sánchez², M.^a Asunción Romero-López²

angelina.lorelí@gmail.com, vanesa@ugr.es, romerol@ugr.es

¹ Becaria CONACYT-México y doctoranda en la Universidad de Granada, Campus Cartuja s/n, 18011, Granada, España.

² Universidad de Granada, Facultad de Ciencias de la Educación, Campus Cartuja s/n, 18011, Granada, España.

DOI: 10.17013/risti.32.1-16

Resumen: Este artículo presenta un estudio para obtener evidencias de validez del contenido de un guion de entrevista en profundidad, en el marco de una investigación sobre el desarrollo de la competencia digital de profesores universitarios. La técnica utilizada fue la evaluación por juicio de expertos, que se centró en los criterios: claridad, pertinencia e importancia, y contó con la participación de docentes investigadores de México, España y Chile. La revisión integradora de la evaluación incluyó el análisis cuantitativo de las calificaciones de los jueces, mediante el Índice de Validez de Contenido y los estadísticos Kappa de Cohen y Kappa de Fleiss, así como el análisis de contenido de los comentarios. Como resultado se obtuvo una versión acotada del guion de entrevista, incluido como anexo. Además, se identificaron aspectos en debate sobre la conceptualización de esta competencia docente en la Educación Superior.

Palabras-clave: Competencia digital; Docente; Educación Superior; Validación; Entrevista.

Content validity study of an interview guide about teachers' digital competence in Higher Education

Abstract: This paper presents a study to obtain content validity evidence of an in-depth interview guide, in the context of a research about the development of digital competence in Higher Education teachers. The technique used was the expert judgment panel, focused on the following criteria: clarity, relevance and importance. Professors from Mexico, Spain and Chile participated as experts. The integrative review of the evaluation included statistical analysis, using the Content Validity Index and the Kappa of Cohen and Kappa de Fleiss indexes, as well as the content analysis of the comments made by the judges. As a result, a more focused version

of the interview guide was obtained, included as an annex. Furthermore, aspects in debate about the conceptualization of this teachers' competence were compiled.

Keywords: Digital competence; Teacher; Higher Education; Validity; Interview.

1. Introducción

La participación del profesorado universitario es fundamental para enfrentar el desafío de la integración crítica de las Tecnologías de Información y Comunicación (TIC) en la Educación Superior. Los docentes, con su conocimiento, experiencia y visión, toman decisiones sobre la manera de aprovechar las posibilidades y enfrentar las limitaciones de prácticas y recursos digitales para apoyar el aprendizaje de los estudiantes y su propio desarrollo profesional. De hecho, el rol docente ha sido uno de los temas de interés de la Tecnología Educativa en los últimos 20 años (Prendes, 2018).

En esta línea, el concepto de competencia digital docente (CDD) ayuda a comprender la competencia profesional del perfil del profesorado universitario, necesaria para la integración adecuada de las TIC (Prendes, Martínez & Gutiérrez, 2018; Tejada & Pozos, 2018; Zabalza, 2003). En el contexto actual se espera que los docentes aprovechen una amplia gama de herramientas digitales con propósitos de innovación y de mejora educativa (Adams Becker et al., 2017; UNESCO, 2011). Sin embargo, el foco principal de la CDD no está en la tecnología, sino en las competencias movilizadas y las decisiones reflexivas que los profesores toman para incorporar las tecnologías digitales de manera estratégica y pedagógica (Pozos, 2013) y su influencia en la competencia digital de los estudiantes (Redecker, 2017).

Aunque existen avances en la conceptualización de la CDD, resulta complejo delimitar su significado. La propia definición de competencia digital es plural, multifacética y contextual (Ala-Mutka, 2011; Gallardo-Echenique, Minelli, Marqués-Molias & Esteve-Mon, 2015; Janssen et al., 2013). Además, se vincula a la influencia del ámbito familiar, al capital cultural y al logro de la inclusión digital (Martínez-Piñeiro, Vila & Grewerc, 2018). Por otra parte, es necesario considerar los rasgos específicos de la docencia universitaria, como los ejes de actuación profesional (docencia, investigación, gestión, transferencia de conocimiento), los enfoques metodológicos y didácticos, el campo disciplinar, las estrategias y recursos digitales empleados, y los contextos institucionales y sociales que podrían variar los atributos de esta competencia. En el contexto iberoamericano existen propuestas para caracterizar la CDD del profesorado universitario, por ejemplo, la síntesis de Carrera & Coiduras (2012), el perfil propuesto por Rangel (2016), los modelos de Prendes et al. (2018) y Tejada & Pozos (2018), así como numerosos estudios e instrumentos para su diagnóstico, evaluación y certificación.

En general, la revisión de literatura muestra una tendencia deductiva y cuantitativa para evaluar la CDD, es decir, a partir del uso de cuestionarios, encuestas y declaraciones de desempeños. Aún son pocas las aproximaciones cualitativas y enfocadas en el carácter dinámico de la CDD. Si partimos de la comprensión de competencia desde el enfoque socioconstructivista, sería necesario reconocer su carácter procesual y cualitativo (Díaz-Barriga, 2011). Por lo tanto, existe la oportunidad de contribuir en esta línea al considerar el carácter evolutivo de la CDD como foco principal de estudio, anclado en el desarrollo profesional docente.

La investigación más amplia a la que pertenece este estudio tiene como propósito caracterizar la adquisición y el desarrollo en la práctica de la CDD de docentes universitarios de México y España, desde una perspectiva cualitativa y mediante el enfoque biográfico narrativo. Como parte del diseño metodológico surgió la necesidad de revisar el diseño del instrumento principal: una entrevista en profundidad de tipo biográfico, organizada en varias sesiones (Fernández, 2006; Kelchtermans, 1999). Se requería que esta mantuviera un carácter abierto y a la vez común entre los relatos de vida de los participantes, a partir de líneas cronológicas y temáticas (Bolívar, Domingo & Fernández, 2001). De la revisión de literatura especializada se obtuvo un listado amplio de dimensiones, categorías e indicadores, por lo que fue necesario realizar un estudio de obtención de evidencias de validez de contenido.

En síntesis, la validez se entiende como el grado en que la teoría y la evidencia son un sustento para la interpretación de los datos que se obtienen mediante un instrumento, en concordancia con los objetivos del mismo (Bandalos, 2018; Pedrosa, Suárez-Álvarez & García-Cueto, 2013). Según Cabero & Llorente (2013) el juicio de expertos se utiliza en el ámbito de la educación y las tecnologías como técnica para evaluar instrumentos, recursos educativos y propuestas de aprendizaje, por ejemplo, para revisar su adecuación a la población objetivo (Rodrigues, Martins, Pinto & Teixeira, 2018).

Además, el juicio de expertos tiene la ventaja de generar información detallada acerca de “(...) contenidos y temáticas difíciles, complejas y novedosas o poco estudiadas” (Cabero & Llorente, 2013: 14), como es el caso de la CDD en términos de su evolución. Algunos estudios sobre la CDD de profesores universitarios han utilizado esta técnica para evaluar los instrumentos de investigación empleados (Cejas-León & Navío, 2016; Rangel, 2016). A continuación, se comparte el método seguido para la realización de este estudio.

2. Método

El juicio de expertos se considera una fuente de evidencias de validez del contenido puesto que las evaluaciones de los jueces ayudan a revisar la relevancia y representatividad de los ítems, así como su relación con los propósitos del instrumento y con el dominio de interés (Escobar-Pérez & Cuervo-Martínez, 2008; Pedrosa et al., 2013; Sireci, 1998). Forma parte de la búsqueda continua de la validez y del rigor en la investigación (Bandalos, 2018; Hernández-Sampieri, Fernández & Baptista, 2014). En otras palabras, esta técnica proporciona una base para la toma de decisiones a fin de mejorar el diseño de los instrumentos de investigación.

El objetivo del presente estudio fue obtener evidencias de la validez de contenido de las dimensiones e indicadores sobre la evolución de la competencia digital docente del profesorado universitario, mediante la evaluación por juicio de expertos, a fin de mejorar el guion de entrevista en profundidad. Los objetivos específicos fueron:

- Valorar la pertinencia de las dimensiones e indicadores para caracterizar la evolución de la CDD del docente universitario.
- Identificar aspectos por añadir o eliminar para cubrir el dominio de interés.
- Recopilar observaciones para la mejora del instrumento.

En cuanto al desarrollo del estudio, este se organizó en tres fases: preparatoria, desarrollo de la evaluación y toma de decisiones. Como parte de la fase preparatoria, se seleccionaron los temas para el guion de entrevista de acuerdo a la revisión de literatura especializada (estudios del ámbito e instrumentos de investigación) y su análisis descriptivo (Padilla-Hernández, Gámiz-Sánchez & Romero-López, 2018). Las cuatro dimensiones identificadas se desglosaron en 17 categorías y 65 indicadores que representan los temas sugeridos para la entrevista.

Se construyeron los criterios de evaluación con sus respectivos límites de aceptación y revisión a partir del cálculo de medidas de dispersión (ver tabla 1). Para el criterio de pertinencia se utilizó el Índice de Validez de Contenido (IVC) (Lawshe, 1975) para valorar el grado de acuerdo o consenso entre los expertos sobre la adecuación de los ítems y de las dimensiones del instrumento (Delgado-Rico, Carretero-Dios & Ruch, 2012; Pedrosa et al., 2013; Polit, Beck & Owen, 2007).

Criterio	Descripción	Escala	Límite para su revisión/ aceptación
Claridad	La redacción del ítem es clara y su significado se comprende sin ambigüedad.	Dicotómica: Sí, No.	Porcentaje de respuestas afirmativas: 80% (Escobar-Pérez & Cuervo-Martínez, 2008).
Pertinencia	El indicador es adecuado para el objetivo del estudio.	Dicotómica: Sí, No.	Promedio del IVC por dimensión: 0.80 (Delgado-Rico et al., 2012). IVC de los indicadores: 0.67 (Polit et al., 2007).
Importancia	Grado de importancia y significatividad del indicador para la dimensión.	Tipo Likert: 1: Muy poca 2: Poca 3: Bastante 4: Mucha	Media (M): menos de 3. Desviación estándar (DE) como información adicional.

Tabla 1 – Criterios de evaluación

Como el IVC no excluye la posibilidad de acuerdo debida al azar se recurrió a medidas complementarias de estimación de la consistencia entre las evaluaciones, como el índice Kappa de Cohen (porcentaje de acuerdo entre pares y promedio de pares) y el Kappa de Fleiss, específico para múltiples evaluadores (Delgado-Rico et al., 2012; Wynd, Schmidt & Atkins, 2003). Estos índices se emplearon para la revisión general de las dimensiones del instrumento. El límite para un acuerdo moderado y aceptable fue de 0.41 para el promedio del Kappa de Cohen y para el resultado del índice Kappa de Fleiss (Delgado-Rico et al., 2012; López de Ullibarri & Pita, 1999).

Se diseñó una planilla como instrumento para la evaluación, con los criterios de evaluación y con espacio para los comentarios de los jueces. Además, se elaboró una carta de invitación con el contexto de la investigación.

Seleccionamos a los profesores e investigadores participantes según el procedimiento del biograma (Cabero & Llorente, 2013), de acuerdo a la revisión de su trayectoria profesional. Los criterios de inclusión fueron: conocimiento y experiencia investigadora

en el tema y el enfoque metodológico a fin de obtener una retroalimentación pertinente para el instrumento (Davis, 1992), amplia experiencia como docentes universitarios por la empatía con el perfil y la experiencia profesional (Hynes, Richard & Kubany, 1995), Iberoamérica como ubicación geográfica debido al contexto del estudio, equidad de género y disposición para participar. A partir de estos criterios se construyó una muestra intencional de especialistas.

Seis profesores investigadores aceptaron la invitación, cada uno de ellos reúne más de 20 años de trayectoria profesional en la docencia universitaria y son expertos en las líneas de investigación (Tecnología educativa, Aprendizaje en red, Competencia digital, Desarrollo profesional docente) o en el enfoque biográfico-narrativo. Una de las profesoras reside en Chile (Profesora A), dos docentes en México (Profesor B y Profesora E) y tres en España (Profesora D, Profesores C y F).

En la fase de desarrollo se llevó a cabo el contacto con los docentes investigadores y la recogida de datos. Los materiales se recopilaron vía correo electrónico de forma individual, aunque también se desarrollaron conversaciones personales para profundizar en algunos aspectos de las sugerencias. Las calificaciones se registraron en una hoja de datos. Los cálculos de las medidas de dispersión y del IVC fueron realizados con apoyo de fórmulas en la hoja de datos. Para el cálculo de los índices Kappa se utilizó la herramienta en línea ReCal3 (Freelon, 2010, 2017), cuyos resultados se verificaron con el programa IBM SPSS Statistics (versión 24.0).

La fase de toma de decisiones sobre los cambios al instrumento se basó en el análisis cualitativo de las calificaciones, según los límites expresados en la tabla 1, y en la interpretación cualitativa de las observaciones. Como sugieren Polit et al. (2007) se identificaron los ítems que requerían revisión o descarte, para luego contrastar esta revisión con los comentarios de los jueces. La valoración cualitativa de los comentarios se realizó mediante el análisis de contenido. Las aportaciones se codificaron según los temas de la entrevista como categorías previamente establecidas (Bardin, 1996). Una categoría nueva emergió del conjunto de comentarios: recomendaciones generales para la investigación. Finalmente, una vez que el guion fue corregido según los resultados de la evaluación del juicio de expertos, se desarrolló un ejercicio piloto de entrevista con dos docentes.

3. Resultados

3.1. Índices generales por dimensión

En la tabla 2 se presentan los índices obtenidos sobre la concordancia entre evaluadores y el promedio de IVC por dimensión.

En términos generales, los índices de concordancia manifestaron un acuerdo moderado entre los evaluadores, no existiendo evidencias empíricas de inconsistencia entre las evaluaciones de los jueces. El promedio del IVC de las dos últimas dimensiones se presentó ligeramente por debajo del 0.80, por lo tanto, fue necesario revisar su construcción. A continuación, se detalla la evaluación para cada dimensión y sus indicadores.

Dimensión	Pertinencia, promedio del IVC	Porcentaje de acuerdo por pares Kappa de Cohen	Promedio del Kappa de Cohen por pares	Índice Kappa de Fleiss
<i>Desarrollo profesional docente</i>	0.81	68.64%	0.497	0.473
<i>Evolución de la CDD</i>	0.84	75.29%	0.574	0.563
<i>Áreas de la CDD</i>	0.75	75.29%	0.566	0.553
<i>Valoración crítica del uso de TIC en Educación Superior</i>	0.72	68.33%	0.508	0.473
Promedio general	0.78	72.65%	0.542	0.529

Tabla 2 – Índices por dimensión y promedio general

3.2. Desarrollo profesional docente

En esta dimensión (D1), el criterio de pertinencia tuvo un mayor grado de concordancia entre evaluadores, con un porcentaje de acuerdo entre pares de un 84.44%, en contraste con la claridad (67.4%) y la importancia de sus ítems (54.07%). La tabla 3 muestra las puntuaciones de los indicadores de la D1:

Categoría	Indicador	Claridad (%Sí)	Pertinencia (IVC)	Importancia	
				(M)	(DE)
<i>Trayectoria profesional</i>	Razones para elegir la docencia como profesión	100	1	3.3	0.82
	Evolución de la carrera profesional	83.3	1	3.7	0.52
	Incidentes críticos	50*	0.33*	2.7*	0
<i>Perfil profesional</i>	Autopercepción y motivaciones profesionales	100	1	4	0
	Rasgos del conocimiento pedagógico y disciplinar	83.3	0.67*	3.7	0.52
	Entorno socio-profesional	83.3	1	3.8	0.41
<i>Perspectiva de futuro</i>	Valoración del momento presente	66.7*	0.33*	3	1.26
	Metas de desarrollo profesional	83.3	1	3.8	0.41
	Prospectiva de la universidad, la sociedad y las TIC	83.3	1	3.8	0.41

Nota: Con asterisco (*) se marcan los resultados de los ítems a revisar.

Tabla 3 – Cálculos e IVC para los indicadores de la D1: Desarrollo profesional docente

Se eliminaron los ítems que obtuvieron un IVC bajo por su ambigüedad o carácter analítico, según las observaciones de los jueces. Los temas agrupados en las categorías “Perfil profesional” y “Perspectiva de futuro” se reorganizaron para evitar su solapamiento con otros ítems.

Se añadieron temas relacionados con: “(...) experiencias formativas tempranas: antecedentes relacionados con la docencia; antecedentes relacionados con las TIC; experiencia en la Educación Secundaria y Preparatoria en relación con las TIC”, según lo sugirió el Profesor F. Otra observación de los jueces fue destacar el carácter reflexivo de la docencia dado que resulta transversal en el ejercicio de relatar las experiencias relacionadas con la CDD.

3.3. Evolución de la competencia digital docente

En esta dimensión (D2), los promedios de acuerdo entre pares de los criterios claridad y pertinencia presentaron una consistencia alta (81.24% y 86.28% respectivamente), mientras que el de importancia obtuvo un porcentaje del 57.65%. La tabla 4 presenta la calificación de los indicadores de la D2.

Categoría	Indicador	Claridad (%Sí)	Pertinencia (IVC)	Importancia	
				(M)	(DE)
<i>Desarrollo de la CDD</i>	Primeras experiencias para la adquisición de la CDD	100	1	4	0
	Hitos para el desarrollo de la CDD	66.7*	1	4	0
	Dificultades en relación con la competencia digital	100	1	4	0
	Influencia de otros ámbitos (familiar, social, laboral)	100	1	3.7	0.52
<i>Uso de TIC en los ejes de la docencia universitaria</i>	Docencia	100	1	3.8	0.41
	Investigación	100	1	3.5	0.84
	Gestión	100	1	3.5	0.84
<i>Aprendizaje continuo</i>	Exploración sobre educación y TIC	50*	0.67*	3.7	0.52
	Formación continua	100	1	3.7	0.52
	Colaboración (docentes, estudiantes, comunidad)	83.3	1	3.8	0.41
	Proyectos de investigación o de innovación	100	1	3.3	0.82
<i>Rutinas, espacios de trabajo y recursos digitales</i>	Actividades y uso del tiempo en la jornada laboral	83.3	0.67*	3.3	0.82
	Espacios de trabajo	100	0.67*	3.5	0.84
	Recursos digitales	100	1	4	0
	Emociones de las experiencias en red	83.3	1	3.8	0.41
<i>Uso de TIC en la vida cotidiana</i>	Finalidades	50*	0.00*	2.7*	1.3
	Relación con su competencia digital docente	83.3	0.33*	3.7	0.52

Nota: Con asterisco (*) se marcan los resultados de los ítems a revisar.

Tabla 4 – Cálculos e IVC para los indicadores de la D2: Evolución de la CDD

Esta dimensión presentó varios puntos a revisar. Por un lado, fueron eliminados los ítems que obtuvieron un IVC bajo debido a la falta de claridad, ambigüedad o amplitud. Como ejemplo está la categoría “Uso de TIC en la vida cotidiana” que fue eliminada porque el foco de la investigación es en la CDD y los relatos de los docentes podrían expresar la influencia de otros ámbitos en el desarrollo de esta competencia.

Los jueces sugirieron añadir la vinculación o transferencia de conocimiento a los ejes de la docencia universitaria como parte del trabajo académico. También se incluyeron los proyectos de innovación y de investigación relacionados con el aprovechamiento de las TIC. Se renombraron ciertos ítems para hacerlos más claros y diferenciados, como el caso de “Exploración sobre educación y TIC” renombrado como: “Estrategias para actualizar su CDD”.

3.4. Áreas de la competencia digital docente

La tercera dimensión (D3) mostró el mayor porcentaje de acuerdo entre pares en cuanto a la claridad (81.24%), mantuvo un buen nivel de concordancia en el criterio de pertinencia (73.89%) y presentó el grado más alto de acuerdo sobre el criterio de importancia (63.7%). La tabla 5 reúne las calificaciones de los ítems de la D3.

El panel de expertos señaló ítems cuya formulación resultó menos clara para abordar la CDD. La categoría “Pedagogía” recibió una crítica debido a su enfoque, que según varios jueces resultaba poco actual, tradicional o difícil de abordar. Algunos ítems fueron eliminados por su formulación poco clara, entre ellos la “Generación de conocimiento” y “Adecuación de recursos digitales”. También se descartaron los siguientes indicadores por su bajo IVC y por las observaciones de los jueces: “Netiqueta”, “Programación” y “Participación ciudadana”. Por ejemplo, el profesor C señaló: “(...) la “Programación” no debe contemplarse como objetivo (y por tanto pongo en cuestión el área) en la CDD.”

Varios jueces coincidieron en el poco nivel de concreción de la categoría “Ética, salud y seguridad”, como detalla la profesora D: “Aprecio cierto solapamiento [entre varias] cuestiones de este mismo apartado (...)”. Así, revisamos de nuevo la literatura e identificamos dos ejes generales: “Implicaciones éticas y uso responsable de tecnologías digitales”, y “Salud, seguridad y prevención de riesgos”. Éstos se incluyeron como indicadores de una nueva categoría: “Reflexiones sobre su CDD”.

Finalmente, esta dimensión se transformó en una categoría de la D2 con el propósito de acotar el acercamiento al problema de investigación. En este cambio las áreas de la CDD pasaron a ser indicadores, dotando a los ítems de un carácter más inductivo y abierto al contenido de los relatos de los docentes. En el caso del área pedagógica, se valorarán los aspectos concretos que surjan en la conversación con los docentes.

3.5. Valoración crítica del uso de TIC en Educación Superior

En términos generales esta dimensión (D4) reunió el menor porcentaje de acuerdo entre pares, sobre todo en el criterio de importancia (55.56%). Los porcentajes de la pertinencia (80.21%) y la claridad (78.84%) presentaron una diferencia menor. En la tabla 6 se encuentran las puntuaciones de los ítems de la D4.

Categoría	Indicador	Claridad (%Sí)	Pertinencia (IVC)	Importancia	
				(M)	(DE)
<i>Pedagógica</i>	Planificación de experiencias de aprendizaje	100	0.33*	3	0.55
	Desarrollo de experiencias de aprendizaje	100	0.67*	3.3	0
	Evaluación	100	0.67*	3.2	0.45
	Valoración del potencial del uso de TIC en educación	83.3	0.33*	2.3*	0.84
<i>Informacional</i>	Fuentes de información y recursos para la docencia	100	1	4	0
	Búsqueda y selección de información	100	1	4	0
	Organización y recuperación de información	100	1	4	0
	Generación de conocimiento	66.7*	0.67*	3.3	0
<i>Comunicativo-colaborativa</i>	Comunicación en red	100	1	3.3	0
	Colaboración en red	100	1	3.3	0
	Netiqueta	83.3	0.33*	2.8*	0.98
	Participación ciudadana	83.3	0.00*	3.5	0.84
	Gestión de la identidad digital	83.3	0.67*	3.8	0.41
<i>Creación de contenido digital</i>	Creación de material digital (propio, integración)	100	1	4	0
	Uso de licencias y derechos de autor	83.3	0.67*	3.5	0.84
	Adecuación de recursos digitales	83.3	0.67*	3.3	0
	Programación	100	0.33*	3.3	1.03
<i>Ética, salud y seguridad</i>	Valores en las prácticas digitales	83.3	0.67*	3.3	0
	Equidad de acceso y uso de TIC	83.3	1	4	0
	Hábitos saludables y sostenibles de uso de TIC	83.3	0.67*	3	0.89
	Protección de datos y dispositivos	100	1	3.7	0.82
	Protección del medio ambiente	100	1	3.7	0.82
	Relación entre sociedad y TIC	66.7*	1	3.5	0.55
<i>Técnica</i>	Comprensión a nivel usuario de software, hardware y dispositivos externos	83.3	1	4	0
	Comprensión de las funciones y la estructura de Internet	83.3	1	4	0
	Identificación de la infraestructura de los recursos digitales	83.3	0.67*	3.3	0
	Resolución de problemas técnicos	100	1	3.5	0.84

Nota: Con asterisco (*) se marcan los resultados de los ítems a revisar.

Tabla 5 – Cálculos e IVC para los indicadores de la D3: Áreas de la CDD

Categoría	Indicador	Claridad (%Sí)	Pertinencia (IVC)	Importancia	
				(M)	(DE)
<i>Cambios y reflexiones en su docencia</i>	Cambios en el perfil docente	66.7*	1	3.7	0.52
	Problemáticas del uso de TIC	66.7*	0.33*	3.2	0.45
	Reflexiones para el uso crítico de TIC	83.3	0.67*	3.3	0
	Vías para compartir su experiencia	83.3	1	3.8	0.41
	Necesidades de aprendizaje en relación con la CDD	100	1	3.7	0.52
<i>La competencia digital de los estudiantes</i>	Importancia en su formación	83.3	0.67*	3.3	0
	Desarrollo de la CDD en la universidad	100	0.67*	3.3	0
	Necesidades de aprendizaje	83.3	0.67*	3.3	0
<i>Educación Superior y cultura digital</i>	Influencia de la política educativa en su práctica	66.7*	0.33*	3	0.89
	Percepción de la competencia digital en su institución	100	0.67*	3.7	0.52
	Impacto de la cultura digital en la Educación Superior y viceversa	100	1	3.7	0.82
	Desafíos para el uso crítico de TIC en la Educación Superior	100	0.67*	3.8	0.41

Nota: Con asterisco (*) se marcan los resultados de los ítems a revisar.

Tabla 6 – Cálculos e IVC para los indicadores de la D4: Valoración crítica del uso de TIC en Educación Superior

Entre las modificaciones a esta dimensión, se destaca la reorganización de la categoría “Cambios y reflexiones sobre su docencia”. Se renombró para distinguir la percepción sobre cambios en la docencia y las reflexiones sobre el desarrollo de la CDD. Una jueza observó la relación directa del contenido de la categoría con la dimensión sobre la evolución de la CDD. Por esto, se añadió una nueva categoría en la segunda dimensión, titulada “Reflexiones sobre su CDD”, que integró nuevos ítems por sugerencia de los jueces: la percepción de beneficios asociados a su CDD y la influencia de las prácticas digitales en la mejora educativa. Cabe destacar el comentario de la profesora D acerca de la conveniencia de tratar: “(...) la influencia de la competencia digital en la mejora de los resultados de aprendizaje o en la mejora de la calidad de la enseñanza universitaria”.

Luego, se amplió la sección dedicada al perfil de los estudiantes o jóvenes universitarios, pues como señaló la profesora E, además del centro en la persona del profesor, sería necesario considerar: “(...) dos elementos que me parecen muy relevantes: (1) los retos para los entornos universitarios; (2) ese otro, el aprendiz”. En cuanto al segundo punto, el profesor B comentó que: “(...) alguna cuestión relacionada con cómo los profesores valoran (o evaden) las competencias digitales de los estudiantes puede ayudar a explicar alguna parte de la evolución del profesor en esas competencias”. Además, se incluyó

una categoría sobre los grupos docentes donde participa el profesorado por su posible influencia en la CDD.

Fue necesario renombrar esta dimensión como: “Contexto: Educación Superior y cultura digital”, en sintonía con el comentario de la Profesora A sobre la importancia del contexto pues: “(...) según lo que conozco en diferentes instituciones no siempre las competencias digitales pueden explicarse a partir de la voluntad del profesor(a)”.

Esta aportación formó parte de las recomendaciones sobre la investigación en general, entre las que destacan el analizar los relatos de vida tanto en el plano personal como contextual y procurar el carácter abierto de la entrevista a partir de la profundización en las narraciones.

Por último, se realizó un ejercicio piloto del guion de entrevista modificado en el que se confirmó el carácter abierto de los ítems para profundizar en las vivencias de los docentes. Preparativos como la consulta del currículum vitae de los profesores y la conversación informal sobre la investigación favorecieron el desarrollo de la entrevista.

4. Discusión y conclusiones

La estrategia de evaluación por juicio de expertos permitió reunir evidencias de validez del contenido del guion de entrevista en profundidad y, a partir de su análisis, tomar decisiones para la mejora del instrumento. La pertinencia e importancia de varios indicadores fueron confirmadas. A partir de la síntesis de su contenido y de la adición de ítems el instrumento adquirió mayor consistencia al estar más acotado, mejorar su fundamentación y reducir posibles sesgos en la etapa preparatoria de la investigación. El guion definitivo se compone de tres dimensiones, diez categorías y 40 indicadores, y puede consultarse en el anexo 1. Constatamos con este estudio la valiosa ayuda del juicio de expertos para la evaluación del diseño de instrumentos de corte cualitativo.

Además, los propósitos de cada dimensión obtuvieron más claridad. La primera de ellas, “Desarrollo profesional docente”, tiene un carácter transversal y secundario pues es el hilo para relatar el proceso de aprendizaje en relación con la CDD. El foco central de la investigación es la dimensión “Evolución de la CDD” porque abarca el recorrido cronológico y narrativo en torno a la adquisición y el desarrollo de la CDD; en este sentido, sus indicadores son ayudas para evocar relatos y reflexiones del profesorado. La dimensión “Contexto: Educación superior y cultura digital” trata del contexto institucional y sociocultural de las experiencias del profesorado universitario, por lo que sitúa el desarrollo de la CDD.

Es importante señalar que un relato puede presentar uno o más aspectos de la CDD o de ítems del guion. Por ejemplo, el manejo de información digital está presente en varios de los ejes de la docencia universitaria y es probable que implique reflexiones sobre el uso responsable y ético de las TIC. Así, los relatos de vida de los docentes serán una oportunidad para caracterizar la CDD en sus distintas manifestaciones y en su complejidad.

En cuanto a la comprensión de esta competencia, surgieron varios puntos para el debate. En primer lugar, se sugirió integrar la transferencia del conocimiento o vinculación

como otro eje fundamental de la labor docente. En segundo lugar, la programación informática como área de la CDD fue cuestionada; ésta podría resultar pertinente según el perfil y el campo disciplinar del profesorado. Tercero, las áreas pedagógica y ética resultaron difíciles de concretar; respecto del área ética, algunas propuestas la consideran un aspecto transversal a los ejes de la labor docente (Prendes et al., 2018; Rangel, 2016). Por último, fue llamativo el énfasis de algunos jueces en el perfil digital de los estudiantes debido a su influencia en el desarrollo de la CDD, observación que resulta congruente con el planteamiento del modelo DigCompEdu (Redecker, 2017). En consecuencia, se tendrán presentes estos puntos para el análisis de los relatos.

Finalmente, el guion anexo constituye un material que podría ser retomado por futuras investigaciones desde una perspectiva complementaria a la tendencia mayormente cuantitativa en el campo. Así mismo, puede ser un recurso de apoyo para proyectos de formación docente e innovación educativa a fin de profundizar en las vivencias y reflexiones del profesorado sobre el desafío de la integración de TIC a la Educación Superior.

Agradecimientos

Agradecemos la colaboración de los jueces expertos en esta línea de debate. La estancia de investigación cuenta con el apoyo del Programa de Becas en el Extranjero del Consejo Nacional de Ciencia y Tecnología (CONACYT), México.

Referencias

- Adams Becker, S., Cummins, M., Davis, A., Freeman, A., Hall Giesinger, C., & Ananthanarayanan, V. (2017). *The NMC Horizon Report: 2017 Higher Education Edition*. Texas: The New Media Consortium. Recuperado de: <https://www.nmc.org/publication/nmc-horizon-report-2017-higher-education-edition/>
- Ala-Mutka, K. (2011). *Mapping digital competence: towards a conceptual understanding*. Sevilla: Joint Research Centre. Recuperado de: http://ftp.jrc.es/EURdoc/JRC67075_TN.pdf
- Bandalos, D. (2018). Validity. En *Measurement Theory and Applications for the Social Sciences* (pp. 254-297). Nueva York-London: The Guilford Press.
- Bardin, L. (1996). *Análisis de contenido*. Madrid: Ediciones Akal.
- Bolívar, A., Domingo, J., & Fernández, M. (2001). *La investigación biográfico-narrativa en educación: Enfoque y metodología*. España: La Muralla.
- Cabero, J., & Llorente, M. C. (2013). La aplicación del juicio de experto como técnica de evaluación de las Tecnologías de Información y Comunicación (TIC). *Revista de Tecnología de Información y Comunicación en Educación*, 7(2), 11–22.
- Carrera, F. X., & Coiduras, J. L. (2012). Identificación de la competencia digital del profesor universitario: un estudio exploratorio en el ámbito de las Ciencias Sociales. *REDU Revista de Docencia Universitaria*, 10(2), 273–298.

- Cejas-León, R., & Navío, A. (2016). El modelo TPACK competencial. Elaboración de un cuestionario para el profesorado universitario [CD]. En J. Gairín. (Ed.), *Aprendizaje situado y aprendizaje conectado: Implicaciones para el trabajo*. Madrid: Wolters Kluwers.
- Davis, L. (1992). Instrument review: Getting the most from a panel of experts: *Applied Nursing Research. Clinical Methods*, 5(4), 194–197.
- Delgado-Rico, E., Carretero-Dios, H., & Ruch, W. (2012). Content validity evidences in test development: An applied perspective. *International Journal of Clinical and Health Psychology*, 12(3), 449–460.
- Díaz-Barriga, A. (2011). Competencias en educación. Corrientes de pensamiento e implicaciones para el currículo y el trabajo en el aula. *Revista Iberoamericana de Educación Superior (RIES)*, 5(2), 3–24.
- Escobar-Pérez, J., & Cuervo-Martínez, Á. (2008). Validez de contenido y juicio de expertos: una aproximación a su utilización. *Avances en medición*, 6(1), 27–36.
- Fernández, M. (2006). *Desarrollo profesional docente*. Granada: Grupo Editorial Universitario.
- Freelon, D. (2010). ReCal: Intercoder reliability calculation as a web service. *International Journal of Internet Science*, 5(1), 20–33.
- Freelon, D. (2017). ReCal3: Reliability for 3+ Coders [en línea]. Recuperado de: <http://dfreelon.org/utis/recalfront/recal3/>
- Gallardo-Echenique, E., Minelli, J., Marqués-Molias, L., & Esteve-Mon, F. (2015). Digital competence in Knowledge Society. *Journal of Online Learning and Teaching*, 11(1), 1–16.
- Hernández-Sampieri, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación*. Madrid: McGraw-Hill.
- Hynes, S. N., Richard, D. C. S., & Kubany, E. S. (1995). Content Validity in Psychological Assessment: A Functional Approach to Concepts and Methods. *Psychological Assessment*, 7(3), 238–247. doi: 1040-3590/95/\$3.00
- Janssen, J., Stoyanov, S., Ferrari, A., Punie, Y., Pannekeet, K., & Sloep, P. (2013). Experts' views on digital competence: Commonalities and differences. *Computers & Education*, 68, 473–481. doi: 10.1016/j.compedu.2013.06.008
- Kelchtermans, G. (1999). Narrative-Biographical Research on Teachers' Professional Development: Exemplifying a Methodological Research Procedure. En *On the Threshold of the 21st Century: Challenges and Opportunities. Annual Meeting of the American Educational Research Association (AERA-symposium)*, (pp. 2-22). Montreal: n/d.
- Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel Psychology*, 28(4), 563–575. doi: 10.1111/j.1744-6570.1975.tb01393.x

- López de Ullibarri, I., & Pita, S. (1999). Medidas de concordancia: el índice Kappa. *Cadernos de atención primaria*, 6(4), 223–226.
- Martínez-Piñeiro, E., Vila, E., & Grewerc, A. (2018). El papel de la familia en la construcción de la competencia digital. *RISTI: Revista Ibérica de Sistemas e Tecnologías de Informação*, (28), 2–13. doi: 10.17013/risti.28.1–13
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2011). *UNESCO ICT competency framework for teachers*. París: UNESCO.
- Padilla-Hernández, A. L., Gámiz-Sánchez, V. M., & Romero-López, M. A. (2018). Selección de categorías para el estudio de la evolución de la competencia digital docente del profesorado en Educación Superior. *RIITE Revista Interuniversitaria de Investigación en Tecnología Educativa*, (4), 55–67. doi: 10.6018/riite/2018/327881
- Pedrosa, I., Suárez-Álvarez, J., & García-Cueto, E. (2013). Evidencias sobre la validez de contenido: avances teóricos y métodos para su estimulación. *Acción Psicológica*, 10(2), 3–20. doi: 10.5944/ap.10.2.11820
- Polit, D. F., Beck, C. T., & Owen, S. V. (2007). Is the CVI an acceptable indicator of content validity?: Appraisal and recommendations. *Research in Nursing and Health*, 30(4), 459–467. doi: 10.1002/nur.20199
- Pozos, K. V. (2013). Digital competence of higher education teachers for the knowledge society: a preliminary approach of a need assessment study in mexican universities. En *6th International Conference of Education, Research and Innovation (ICERI 2013)*, (pp. 5533–5543). Sevilla: IATED.
- Prendes, M. P. (2018). La Tecnología Educativa en la Pedagogía del siglo XXI: una visión en 3D. *RIITE Revista Interuniversitaria de Investigación en Tecnología Educativa*, (4), 6–16. doi: 10.6018/riite/2018/335131
- Prendes, M. P., Martínez, F., & Gutiérrez, I. (2018). Competencia digital: una necesidad del profesorado universitario en el siglo XXI. *RED Revista de Educación a Distancia*, año XVI (56), 1–22. doi: 10.6018/red/56/7
- Rangel, A. (2016). Competencias docentes digitales. Propuesta de un perfil. *Píxel-Bit. Revista de Medios y Educación*, (46), 235–248. doi: 10.12795/pixelbit.2015.146.15
- Redecker, C. (2017). *European Framework for the Digital Competence of Educators: DigCompEdu*. Sevilla: Joint Research Centre.
- Rodrigues, L., Martins, M., Pinto, C.C., & Teixeira, E. (2018). Tecnología educacional para mediar prácticas educativas sobre alimentação complementar na Amazônia: estudo de validação. *RISTI: Revista Ibérica de Sistemas e Tecnologías de Informação*, (28), 29–40. doi: 10.17013/risti.28.29–40
- Sireci, S. G. (1998). The construct of content validity. *Social Indicators Research*, 45(1–3), 83–117.
- Tejada, J., & Pozos, K. V. (2018). Nuevos escenarios y competencias digitales docentes: Hacia la profesionalización docente con TIC. *Profesorado, Revista de Currículum y Formación del Profesorado*, 22(1), 41–67.

Wynd, C., Schmidt, B., & Atkins, M. (2003). Two quantitative approaches for estimating content validity. *Western Journal of Nursing Research*, 25(5), 508–518. doi: 10.1177/0193945903252998

Zabalza, M. Á. (2003). *Competencias docentes del profesorado universitario: calidad y desarrollo profesional*. Madrid: Narcea.

Anexo: Guion de entrevista en profundidad sobre la evolución de la CDD de profesores universitarios

1. Desarrollo profesional docente
 - 1.1. Trayectoria profesional
 - Antecedentes relacionados con la docencia
 - Razones para elegir la docencia como profesión
 - Evolución de la carrera profesional: primera etapa, desarrollo y momento actual
 - 1.2. Perfil profesional
 - Autopercepción y motivaciones profesionales
 - Perspectiva de futuro
2. Evolución de la competencia digital docente (CDD)
 - 2.1. Adquisición y desarrollo de la CDD
 - Antecedentes en relación con las TIC
 - Experiencia en educación básica, profesional y universitaria relacionada con las TIC
 - Primeras experiencias para la adquisición de la CDD
 - Experiencias significativas para desarrollar la CDD
 - Dificultades en relación con el desarrollo de la CDD
 - Recursos digitales
 - Influencia de ámbitos familiar, social y laboral
 - 2.2. Los ejes de la docencia universitaria y áreas de la CDD
 - Pedagógica
 - Informacional
 - Comunicativo-colaborativa
 - Técnica
 - *Ejes*: docencia, investigación, gestión, y transferencia de conocimiento o vinculación.
 - 2.3. Aprendizaje continuo
 - Estrategias para actualizar su CDD
 - Formación continua sistematizada o formal
 - Colaboración (docentes, estudiantes, comunidad)
 - Proyectos de investigación y de innovación
 - Vías para compartir su experiencia
 - Necesidades de aprendizaje para la CDD
 - 2.4. *Reflexiones sobre su CDD*
 - Cambios en el perfil docente
 - Beneficios asociados a su CDD
 - Problemáticas en relación con el uso de TIC

- Implicaciones éticas y uso responsable de TIC
- Salud, seguridad y prevención de riesgos
- 3. Contexto: Educación Superior y cultura digital
 - 3.1. *Perfil digital de los estudiantes universitarios*
 - Percepción de la competencia digital de los estudiantes universitarios
 - Oportunidades de desarrollo de la competencia digital en la universidad
 - Necesidades de aprendizaje en relación con la competencia digital
 - 3.2. *Competencia digital de los equipos docentes*
 - Coordinación docente
 - Grupos de investigación
 - Grupos de innovación
 - 3.3. *Valoración del contexto institucional*
 - Conocimiento y participación en la política educativa sobre TIC
 - Apoyo y recursos técnicos en su universidad
 - Percepción de la influencia de las TIC en la mejora educativa
 - Desafíos para la alfabetización digital crítica en su universidad
 - 3.4. *Valoración del contexto socio-cultural*
 - Impacto de la cultura digital en la Educación Superior y viceversa
 - Reflexiones sobre las TIC y la digitalización en general en la sociedad

OntoFoCE: Herramienta para el Análisis Forense de Correos Electrónicos

Enzo Notario¹, Beatriz Parra de Gallo¹, Marcela Vegetti², Horacio Leone²

ernotario@ucasal.edu.ar, bgallo@ucasal.edu.ar, mvegetti@santafe-conicet.gov.ar, hleone@santafe-conicet.gov.ar

¹ IESIng – Facultad de Ingeniería, Universidad Católica de Salta, Salta, Argentina,

² INGAR – Instituto de Desarrollo y Diseño (Conicet/UTN), Santa Fe, Santa Fe, Argentina

DOI: 10.17013/risti.32.17–32

Resumen: Este trabajo tiene como objetivo presentar una herramienta para el análisis forense de correos electrónicos a partir de la cabecera de los mismos y la utiliza para instanciar una ontología definida para responder a los puntos de pericia solicitados sobre el correo electrónico. La herramienta consta de cuatro componentes que permiten la obtención de las cabeceras de los correos a peritar, la instanciación de la ontología con los datos obtenidos de las cabeceras y la obtención de respuestas a los puntos de pericia a partir de las preguntas de competencia definidas para la ontología. Se describe cada componente y se ejemplifica el uso de la herramienta mediante un caso de estudio sobre análisis forense de un correo electrónico.

Palabras-clave: Ontología; cabecera de correo; forensia digital.

OntoFoCE: A Framework for the Forensic Analysis of Electronic Mail based on an ontology

Abstract: The purpose of this work is to present a tool for the forensic analysis of emails from their headers. The tool is used to generate a defined ontology, in order to respond to the points of expertise requested about the email. It consists of four components which allow us to obtain the headers of the mails to be analyzed, to generate the ontology with the data acquired from those headers, and to give an answer to the points of expertise produced by the competency questions defined for the ontology. Each component is described and the use of the tool is exemplified through a case study on forensic analysis of an email.

Keywords: Ontology; mail header; digital forensia

1. Introducción

El análisis forense de correos electrónicos se realiza a partir de los datos que residen en su *cabecera*. Allí constan las cuentas, direcciones IP, fechas y demás elementos que permiten validar un correo electrónico cuando es propuesto como prueba en un juicio.

Un correo electrónico se compone de una cabecera y un cuerpo presentados según el formato definido por la norma RFC 822¹. Los datos de la cabecera necesarios para el análisis forense deben ser identificados y tratados individualmente durante la pericia.

La pericia de correos electrónicos puede suponer dos escenarios de trabajo distintos: a) el análisis de un correo en particular, cuando se trata de un único documento; y b) el análisis de un conjunto de correos que deben considerarse en su totalidad. Ambos casos suponen métodos y herramientas diferentes. En el primero, los datos se obtienen directamente de la revisión visual de la cabecera, pero en el segundo caso, se requiere procesos automáticos de extracción por el volumen de datos a considerar.

Teniendo en cuenta esta necesidad de extraer de manera automática datos de la cabecera de varios correos, este trabajo propone el framework OntoFoCE. Este framework, que tiene como componente principal una ontología, asiste al perito informático en el análisis forense de un conjunto de correos electrónicos, brindando soporte desde la preparación de los datos e instanciación de la ontología mediante un proceso automático, hasta la obtención de las respuestas a los puntos de pericia.

Estos trabajos han contribuido a la investigación en curso con un aporte particular en cada caso. Los trabajos (Flores & Hadfeg, 2017), (Tolaba, Caliusco, & Galli, 2015) y (Sarli, Leone, & Gutierrez, 2019) muestran distintos enfoques de aplicación de las ontologías útiles para definir cómo aplicar las ontología en el análisis forense. Los trabajos (Kota, 2012), (Brady, Overill, & Keppens, 2015), (Ovens & Morison, 2016), (Xie, Liu, & Chen, 2016) y (Stadlinger & Dewald, 2017) ayudaron en la definición del procesamiento interno de los datos, atendiendo al volumen y diversidad de formatos que se utilizan en la forensia de correos electrónicos. Las propuestas de (Rueda-rueda, Rico-bautista, & Guerrero, 2018) y de (Di Ioro et al., 2017) se tuvieron en cuenta para definir el método más adecuado para el análisis forense de correos electrónicos. Los criterios de calidad para que las herramientas forenses permitan la reconstrucción de la prueba digital, bajo cánones de reproducibilidad, integridad y credibilidad propuestos por (Chabot, Bertaux, Nicolle, & Kechadi, 2015) y los criterios de evaluación de herramientas propuestos por (David, Parra, Rico-bautista, Medina-cárdenas, & Sanchez-ortiz, 2018) resultaron de interés para aplicar a la herramienta de soporte aquí presentada. El trabajo (Chhabra & Bajwa, 2012) que revisa integralmente el tema del análisis forense de correos electrónicos, se tomó como estructura formal para la descripción ordenada del objeto de estudio, mientras que los trabajos (Devendran, Shahriar, & Clincy, 2015) y (Youn, 2014) permitieron ajustar la ontología al modelo requerido para representar la trazabilidad y las preguntas de competencia. Los trabajos sobre trazabilidad de (Selamat, Shahrin, Hafeizah, Yusof, & Abdollah, 2013), (Morgan, 2017a) y (Morgan, 2017b), (Ya'u, Nordin, & Salleh, 2017) y (Noll & Ribeiro, 2007) sustentan la aplicación de la trazabilidad como camino válido para modelar el proceso de transmisión del correo electrónico, y particularmente el trabajo de (Yubao, 2015) en el que propone el uso de la trazabilidad como componente de confianza para generar la evidencia digital. Los aportes de (Blandón Andrade, 2018), (Arcila-Calderón, Barbosa-

¹ Se puede consultar en: <https://www.ietf.org/rfc/rfc822.txt>

Caro, & Cabezuelo-Lorenzo, 2016) y (Faria, Serra, & Girardi, 2014) sirvieron como punto de inicio en el proceso de instanciación incluido en OntoFoCE.

La estructura del trabajo es la siguiente: la sección 2 describe el proceso de transmisión y trazabilidad del correo electrónico y su representación mediante una ontología. La sección 3 describe OntoFoCE mientras que en la sección 4 se muestra un ejemplo de aplicación de la misma. En la sección 5 se compara OntoFoCE con otras herramientas forenses de correos electrónicos y la sección 6 describe las conclusiones del trabajo.

2. Representación ontológica de la trazabilidad del proceso de transmisión de un correo electrónico

La pericia de correos electrónicos se efectúa sobre la cabecera del mismo, pues allí están los datos de la emisión, transmisión y recepción del mismo y siempre sobre *cabeceras de correos recibidos*, ya que los correos emitidos solo contienen datos referidos al envío del mismo, mientras que las cabeceras de correos recibidos tienen todos los datos requeridos para establecer la trazabilidad de la transmisión.

Considerando el proceso de transmisión de un correo electrónico desde su emisión hasta la recepción, ocurren diferentes procesos que se van ejecutando. De éstos, interesan en particular aquellos que pueden impactar en la *modificación del paquete de datos* que circula. Un correo electrónico es manejado por un mínimo de 4 equipos: el emisor, el servidor de correo del remitente, el servidor de correo del receptor y el equipo receptor. En todos ellos, se añade a la *cabecera del correo* una etiqueta de identificación cada vez que pasa por un servidor, y finalmente se agregan los datos del equipo y cuenta receptora una vez que el correo electrónico llega a su destino.

Así, se puede establecer la *trazabilidad* de un correo electrónico a partir de la cabecera. La trazabilidad permite conocer con certeza la procedencia y la historia de un objeto. La necesidad de reconstruir el camino inverso de un correo electrónico recibido se sustenta en que así se puede probar su existencia, avalando el carácter probatorio de esa evidencia.

Durante la transmisión el correo va residiendo en diferentes dispositivos, así, es posible tomar cada archivo almacenado en éstos y verificar si el paquete de datos *original* fue modificado en algún punto de la transmisión. La comprobación de la inalterabilidad del correo se realiza probando que éste es el mismo en cada equipo en que se almacena durante la transmisión. Esto es en cuanto al *cuerpo del mensaje*, que debería estar sin cambios mientras la *cabecera* se va extendiendo a medida que va pasando por los dispositivos durante la transmisión. Así, se puede establecer la trazabilidad de la transmisión, a partir de estos criterios: a) el correo se representa mediante *ocurrencias*, tantas como veces se almacena éste en los distintos dispositivos durante la transmisión. Una ocurrencia es una copia exacta del correo (en cuanto al contenido), con el agregado en la cabecera de la identificación del dispositivo actuante; b) existen tres tipos de ocurrencias: de emisión, de transmisión y de recepción; mientras que las ocurrencias de emisión y recepción son únicas, las de transmisión serán tantas como servidores intervienen en el proceso de envío; d) las ocurrencias se asocian en hilos que señalan el recorrido del correo desde el equipo emisor hasta el equipo receptor, así, habrá tantos hilos como receptores tenga el correo; y e) una secuencia relaciona los distintos hilos que

conforman el correo. La Figura 1 ejemplifica las ocurrencias, hilos y secuencia del envío de un correo desde una cuenta dirigida a dos remitentes.

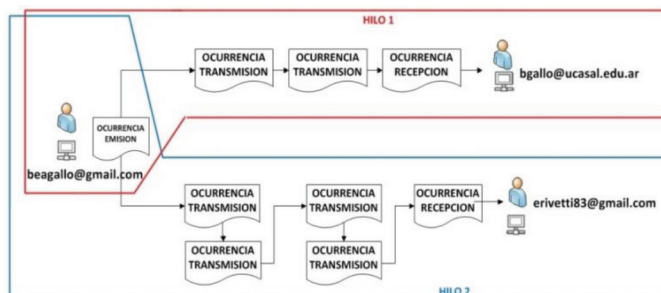


Figura 1 – Ocurrencias del correo electrónico

El envío del correo se realiza en una *SECUENCIA* que contiene dos *HILOS*. Existe una única *OCURRENCIA DE EMISION*, correspondiente a la cuenta beagallo@gmail.com, que a través del *HILO_1*, contiene dos *OCURRENCIAS DE TRANSMISION*, que llegan a la *OCURRENCIA DE RECEPCION* correspondiente a la cuenta receptora bgallo@ucasal.edu.ar. De igual modo, desde esa única *OCURRENCIA DE EMISION* se genera el *HILO_2* con 4 *OCURRENCIAS DE TRANSMISION* hasta llegar a la *OCURRENCIA DE RECEPCION* de la cuenta erivetti@gmail.com.

La ontología definida en (Gallo & Leone, 2016) representa el correo electrónico y la trazabilidad del proceso de transmisión, y responde a los puntos de pericia a partir de las preguntas de competencia. Durante la especificación de la ontología se conformó un banco de puntos de pericias, expresados en lenguaje natural, del cual se extrajeron las preguntas de competencia. Para esto, se encuestó a peritos informáticos sobre pericias realizadas sobre correos electrónicos, obteniéndose 151 puntos de pericia que se clasificaron, ordenaron y asociaron por similitud de datos requeridos, y se usaron para definir las 21 preguntas de competencia que responde OntoFoCE:

1. ¿Cuál es la fecha, hora y dirección IP de emisión del correo electrónico?
2. ¿Cuál es la fecha, hora y dirección IP de recepción del correo electrónico?
3. ¿Cuántos receptores tiene el correo?
4. ¿Cuál es el nombre de usuario y dirección de e-mail del Emisor?
5. ¿Cuál es el nombre de usuario y dirección de e-mail del Receptor?
6. ¿Cuál fue el cliente de correo utilizado por cada usuario?
7. ¿Cuál fue el equipo desde el cual se emitió el correo?
8. ¿Cuál fue el equipo en el que se recibió el correo?
9. Dado una cuenta ¿cuáles son los correos que emitió?
10. Dado una cuenta ¿cuáles son los correos que recibió?
11. Dado un correo, un emisor y un receptor ¿cuáles son los servidores de paso del correo?
12. Dado una cuenta C1 ¿se ha emitido un correo hacia la cuenta C2?
13. Dado una cuenta C1 ¿se ha recibido un correo desde la cuenta C2?
14. Dada una dirección IP ¿cuál sería la localización geográfica del mismo?

15. ¿Cuáles son los correos que han pasado por el dispositivo que posee una IP dada?
16. ¿Cuáles son los mails enviados desde una determinada cuenta en una fecha dada?
17. ¿Cuáles son los mails recibidos por una determinada cuenta en una fecha dada?
18. Dada una palabra clave ¿Figura en el asunto de un correo?
19. Dada una palabra clave ¿Figura en el cuerpo de un correo?
20. Dada una palabra clave ¿Figura en el adjunto de un correo?
21. ¿Cuáles son los correos intercambiados entre las cuentas C1 y C2 en un rango de fechas dado?

A partir de las preguntas de competencia, se derivaron los conceptos, objetos, sus clases y relaciones, así como los axiomas que permiten modelar el correo electrónico desde varios enfoques: la estructura interna, la trazabilidad del proceso de transmisión, y los criterios de validez del documento digital como prueba no repudiable.

A continuación, se detallan algunos aspectos de la ontología que interesan para el presente trabajo. La taxonomía define los conceptos necesarios para representar la trazabilidad del correo electrónico sobre la cual se basa el análisis pericial.

Correo representa el correo electrónico que es objeto de la pericia, e incluye la subclase *CorreoValido* que representa un correo que cumple con los criterios de mínima para que pueda ser analizado por la herramienta. *CabeceraDeCorreo* representa la parte del correo que se toma para el análisis. *Cuenta* es la clase que representa las cuentas de correo que intervienen en el envío/recepción del mismo. Se descompone en dos subclases: *CuentaEmisor* que representa la cuenta desde la cual se emite el correo, y *CuentaReceptor* que representa la cuenta destinataria. *Ocurrencia* representa la copia del correo que reside en los dispositivos utilizados durante el proceso de transmisión. Esta clase se descompone en tres subclases: *OcurrenciaDeEmision*, *OcurrenciaDe Transmision* y *OcurrenciaDeRecepcion* que representan respectivamente la copia del correo emitido, las copias generadas durante la transmisión y la copia del correo recibido. *Hilo* representa la asociación de las ocurrencias relacionadas a cada cuenta receptora, o sea, vincula una *OcurrenciaDeEmisión* con una o más *OcurrenciaDe Transmisión* y una *OcurrenciaDeRecepcion*; existiendo tantas instancias de *Hilo* como cuentas receptoras haya. *Secuencia* representa el conjunto de *Hilos* que se generan para las cuentas receptoras del correo. También se han definido otras clases para representar los conceptos necesarios para que la ontología modele cabalmente el análisis forense: *Equipo*; *IdentificaciónEquipo* (con las subclases *IP* y *HostName*), *ClienteCorreo*, *Adjunto*, *Asunto*, *CuerpoCorreo*, *Expediente* y *PalabraClave*.

La clase *Correo* se asocia a las clases *CuentaEmisor* y *CuentaReceptor* mediante las relaciones de *cuentaEmisorEmiteCorreo* y *cuentaReceptorRecibeCorreo* respectivamente. La trazabilidad del proceso de transmisión se representa con las relaciones que vincula las clases *Secuencia*, *Hilo* y *Ocurrencias*. En particular, interesa las relaciones *esAnteriorA* que representan el orden de aparición de las ocurrencias en cada *Hilo*.

La ontología propuesta incluye además un axioma que sustenta la validez del análisis forense de correos electrónicos, referido a la *existencia* de un correo electrónico, que

se puede verificar mediante 3 elementos: a) los datos del remitente (cuenta de correo y dirección IP); b) la trazabilidad del mismo (datos de los dispositivos que intervienen en la transmisión); y c) los datos del destinatario (cuenta de correo y dirección IP).

En (Gallo & Leone, 2016), (Gallo, Vegetti, & Leone, 2015) y (Gallo, Vegetti, & Leone, 2017) se pueden encontrar más detalles acerca de la ontología propuesta.

La implementación de la ontología es el componente destacable del framework *OntoFoCE*, que toma como entrada las cabeceras de los correos a analizar, instancia los datos en la ontología y genera como resultado las respuestas a las preguntas de competencia, que a su vez, permiten responder a los puntos de pericia solicitados.

3. Framework para el Análisis Forense de Correos Electrónicos

Si el análisis forense debe hacerse sobre un único correo, es sencillo revisar visualmente la cabecera para responder a los puntos de pericia. Cuando se trata de un conjunto de correos, el análisis se complica por el volumen de datos que se deben trabajar, a lo que se suma la dificultad para obtener las cabeceras de correos mediante procesos automáticos. Si bien hay herramientas para forensia de correos que resuelven en parte los problemas derivados del volumen de datos, usualmente no cuentan con procesos automáticos para extraerlos. Y principalmente, no responden de manera directa a los puntos de pericia. Por ello, se propone un framework que permita obtener la cabecera del correo de manera automática, instancie los datos en la ontología y permita responder los puntos de pericia. El Framework *OntoFoCE* está integrado por cuatro componentes (Figura 2): Extractor de Cabeceras, Gestor de Instancias de la Ontología, Analizador de Puntos de Pericia y la ontología, que trabajan sobre un servicio SPARQL Endpoint que las consultas sobre la ontología.

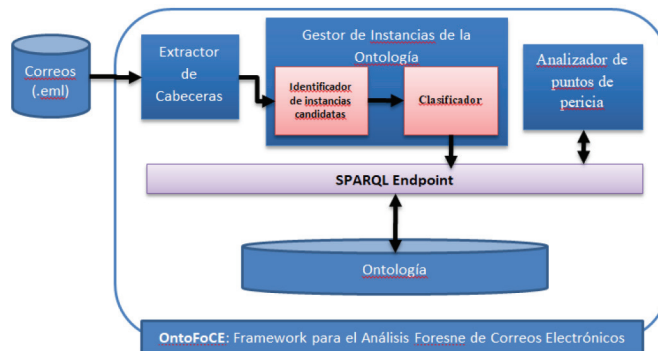


Figura 2 – OntoFoCE Framework para el Análisis Forense de Correos Electrónicos

En la sección 2 se describió la ontología que sirve de base para la herramienta. Seguidamente, se describen los objetivos y funcionalidad de los restantes componentes.

3.1. Extractor de las Cabeceras de Correos

Este componente obtiene las cabeceras de los correos, mediante un proceso automático que evite una tarea manual engorrosa y sujeta a errores. Para ello se accede al cliente de correo de la cuenta y se exportan los correos en un archivo con formato de texto plano. Si el cliente de correo no cuente con funciones de exportación, se debe recurrir a un cliente de correo multiplataforma, con capacidad de importación/exportación de cuentas de otros clientes de correo, para obtener los correos en formato de texto plano.

3.2. Gestor de Instancias de la Ontología

Este proceso toma el archivo en texto plano de la cabecera del correo y descompone los datos en elementos mínimos adecuados para la instanciación de los conceptos y relaciones de la ontología. Este proceso incluye los pasos para cargar la ontología con los datos de la cabecera: a) seleccionar los datos provenientes de la cabecera; b) realizar un proceso ETL (extracción, transformación y carga) para compatibilizarlos con la ontología; c) identificar cuáles son los conceptos y relaciones de la ontología que se corresponden con esos datos, y d) instanciarlos en la ontología.

Se propone un método propio para el proceso ETL de las cabeceras, considerando algunos de los criterios vistos en las diversas técnicas de instanciación estudiadas. Así, se requiere del análisis morfológico de la cabecera del correo, aunque no enfocado en el *significado* de las palabras, sino más bien de la *ubicación* en el texto respecto de la estructura señalada por la norma RFC 822. Y se debe dotar al procedimiento de la máxima automatización, en virtud del volumen de datos que puedan considerarse durante el análisis forense de una cuenta de correo electrónico.

En esta fase se identifican las instancias de las clases de la ontología (*Correo*, *CuentaEmisor*, *Ocurrencias*, etc.) y las relaciones correspondientes, que se insertarán en la base de tripletas TCB a la cual se accede luego mediante *Apache Fuseki*². Este proceso consta de dos sub-componentes: el *Identificador de Instancias Candidatas*, que detecta los datos relevantes en el archivo de texto plano y el *Clasificador de Instancias* que lleva adelante la instanciación en la ontología. Se describe a continuación cada una de éstas.

Identificador de Instancias Candidatas

En esta etapa la aplicación informática recibe un archivo en texto plano con la cabecera y el cuerpo del correo electrónico. Según la norma RFC 822, la cabecera y el cuerpo están separados por una línea en blanco, así, se lee el contenido línea por línea hasta hallar la primera línea en blanco, almacenando todo lo anterior como la cabecera del correo y el resto como el cuerpo. Luego, siguiendo la estructura de esa norma, se procesa la

² Apache Fuseki es un servidor SPARQL que proporciona una API sobre HTTP, permitiendo realizar inserciones y consultas de manera fácil y desde cualquier lenguaje de programación (se puede consultar en la siguiente página. <https://jena.apache.org/documentation/fuseki2/>).

cabecera seleccionando los datos para armar la base de conocimiento con los atributos y valores hallados. Previo, se verifica que la cabecera cumpla con los criterios mínimos exigidos para la pericia: a) el correo tiene un único emisor; b) se identifica la dirección IP del emisor, y c) se identifica la dirección IP del receptor.

Clasificador de Instancias

El Clasificador es un algoritmo que analiza la cabecera de correo en búsqueda de los atributos relevantes, los cuales están representados según el formato definido por la RFC 822. El algoritmo extrae los atributos relevantes de la cabecera y establece las relaciones para instanciar las clases necesarias para conformar una instancia de correo, por último, inserta las tripletas en la base que almacena la ontología.

A continuación, se describe el algoritmo utilizado y las detalles a considerar para analizar la cabecera de un correo electrónico. Cabe mencionar que durante las pruebas se encontraron casos en donde la cabecera no sigue el formato preestablecido por el RFC 822. Además, se ha tenido en cuenta lo descrito por (Darahuge & Arellano González, 2016) acerca del proceso de análisis forense de correos electrónicos.

Lectura de la cabecera

Palabra clave	Descripción	Clase	Atributo
Subject	Resumen del contenido del mensaje.	Asunto	contenidoAsunto
Message-ID	Identificador único del correo.	CorreoValido	idCorreo
Date	Fecha y hora de envío del mensaje.	OcurrenciaDeEmision	fechaHoraOcurrencia
From	Cuenta de correo electrónico del emisor y dirección IP del equipo emisor	CuentaEmisor	cuentaCorreo
To	Cuenta de correo electrónico del Receptor	CuentaReceptor	cuentaCorreo
Delivered-To			
X-Original-To	Atributo insertado por cada equipo que interviene en la transmisión (incluyendo las máquinas del remitente, servidores y el destinatario), se obtiene la fecha y hora de la ocurrencia y la dirección IP del equipo (servidor o receptor).	OcurrenciaDeEmision	fechaHoraOcurrencia
Received o X-Received		IP / HostName	IdentificadorEquipo
		OcurrenciaDeTransmision	fechaHoraOcurrencia
		IP / HostName	IdentificadorEquipo
		OcurrenciaDeEmisión	fechaHoraOcurrencia
		IP / HostName	IdentificadorEquipo

Tabla 1 – Palabras claves de una cabecera y clases que representan

La cabecera del correo se lee de abajo hacia arriba, ya que a medida que ésta va circulando, el proceso de transmisión añade datos al inicio de la cabecera. Cada línea define un atributo junto con su valor mediante el formato {Palabra clave}: {Valor}. A veces el valor ocupa varias líneas, y es necesario concatenar las líneas que en realidad son continuación de una anterior. Durante las pruebas realizadas se observó que éstas comienzan con al menos un espacio en blanco, así, aquellas que cumplen esa condición

son concatenadas al valor de la línea anterior (recursivamente). Luego que se obtienen todas las líneas concatenadas, cada una es leída en búsqueda del patrón {Palabra clave}: {Valor}. Las palabras claves que se buscan en la cabecera se resumen en la Tabla 1, indicando además el atributo de la clase que la representa en la ontología.

3.3. Analizador de los Puntos de Pericia

Este es el tercer componente de OntoFoCE, y su objetivo es responder las preguntas de competencia que sean pertinentes al punto de pericia requerido. El conjunto de preguntas de competencia a las que la ontología propuesta puede responder han sido descriptas en la sección 2, y se formalizan mediante consultas SPARQL, que son implementadas en la herramienta propuesta.

4. Caso Ejemplo

Para mostrar el uso de OntoFoCE como soporte para la forensia de correos electrónicos, se propone un caso ejemplo. Supongamos una causa en la que el juez formule al perito este punto de pericia: “... *Informe si durante la relación contractual (01/05/2017 al 01/01/2018) las partes se enviaron mensajes de correo electrónico desde la cuenta beatriz@empresa.com hacia la cuenta jose@empresa.com ...*”, ordenando la pericia sobre la cuenta beatriz@empresa.com.

El perito accede a dicha cuenta y normalmente desde el equipo desde el cual se gestiona dicha cuenta. Es en este momento cuando se obtiene los datos auxiliares para el informe pericial: dirección física del equipo, cliente de correo utilizado y otra información relevante para el informe pericial.

Se debe destacar que, para no acceder a correos no vinculados a lo indicado por el juez en los puntos de pericia e incurrir en el delito de acceso no autorizado a datos privados, el perito debe acceder a la cuenta teniendo cuidado de identificar y separar solo los correos requeridos. Ubicado ya en la cuenta de correo para realizar el análisis, se observa que la misma tiene un total de 31784 correos, de éstos, se busca y selecciona los 774 correos enviados/recibidos desde la cuenta beatriz@empresa.com a la cuenta jose@empresa.com, se asocian a una carpeta particular y se exportan en un archivo de texto plano. Se debe mantener la cadena de custodia de la prueba digital obtenida, para eso el perito aplica una función *hash* al archivo antes de grabarlo en el dispositivo externo protegido contra escritura, dejando constancia del número de encriptación del hash en el acta que registra todo el procedimiento pericial. Con ese conjunto de 774 correos, el perito responderá los puntos de pericia solicitados. Necesita recurrir a una herramienta que automatice la tarea de analizar esa cantidad de correos permitiéndole seleccionar los correos intercambiados en un rango de fechas. Puede realizar esto de varias formas, accediendo a distintas herramientas que le permitan procesar los correos, trabajando con cada uno por separado según la funcionalidad ofrecida y obtener los datos que luego deberá interpretar para responder a los puntos de pericia.

OntoFoCe integra en un mismo entorno todas las funcionalidades requeridas, incluidas las respuestas a los puntos de pericia mediante las 21 preguntas de competencia contenidas en la ontología.

Una vez cargados los 774 correos en la aplicación, se inicia el proceso de identificación de los pares atributo valor para instanciarlos y representar la trazabilidad de cada correo. Tomando la cabecera de un correo de este ejemplo, en la Figura 3 se señalan las ocurrencias con sus correspondientes valores de fecha y dirección IP de los dispositivos en las que se almacenaron a cada paso de la transmisión.

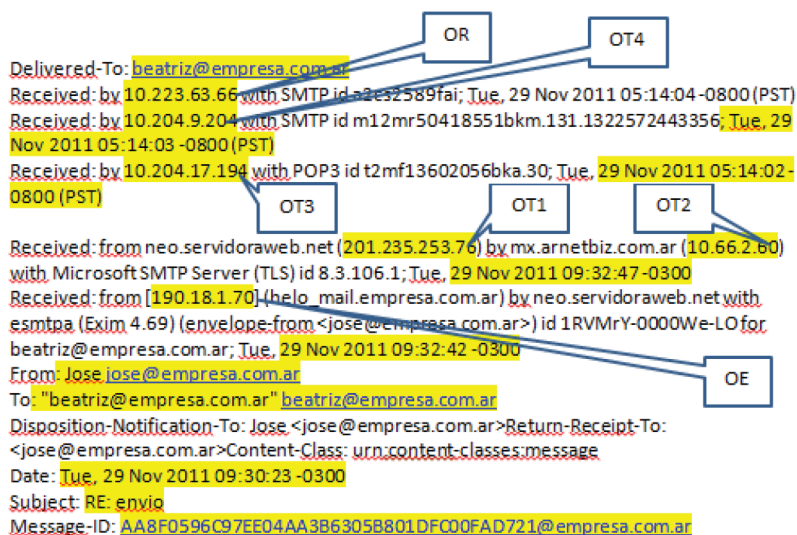


Figura 3 – Ejemplo de correo analizado con identificación de las ocurrencias

Y para el ejemplo de la Figura 3, en la Figura 4 se ilustra cómo muestra OntoFoCE las ocurrencias obtenidas a partir de la instanciación de la cabecera. Se observa en dicha figura que para el correo cuya cabecera se ilustra en la Figura 4, hay 1 ocurrencia de emisión y 1 de recepción que muestran el paso del correo por los equipos cuyas direcciones IP son 190.18.1.70 y 10.223.63.66, respectivamente. Asimismo, se observa los cinco equipos por los que pasó el correo electrónico en su camino desde el equipo emisor hasta el equipo receptor. Cada uno de estos equipos son identificados con un nombre, como en el caso de la ocurrencia de transmisión 1 o con su dirección IP, como ocurre con las otras 4 ocurrencias de transmisión. Para cada ocurrencia, se muestra también la fecha y hora en que el correo pasó por el equipo.

Considerando el requerimiento del punto de pericia, se puede responder al mismo mediante las preguntas de competencia 12, 13 y 21 (ver sección 2), cuyos resultados se muestran en la Figura 5. La respuesta a la pregunta 12 muestra los correos emitidos desde la cuenta beatriz@empresa.com a la cuenta jose@empresa.com; mientras que la respuesta a la pregunta 13 muestra los correos recibidos en la cuenta beatriz@empresa.com, constatando así que efectivamente hubo intercambio epistolar entre ambas cuentas. Por otra parte, la pregunta 21 muestra todos los correos intercambiados entre ambas cuentas en el período 01/05/2017 al 01/01/2018. Así, el perito puede adjuntar un impreso de los resultados de estas preguntas de competencia como base del informe pericial que debe entregar.

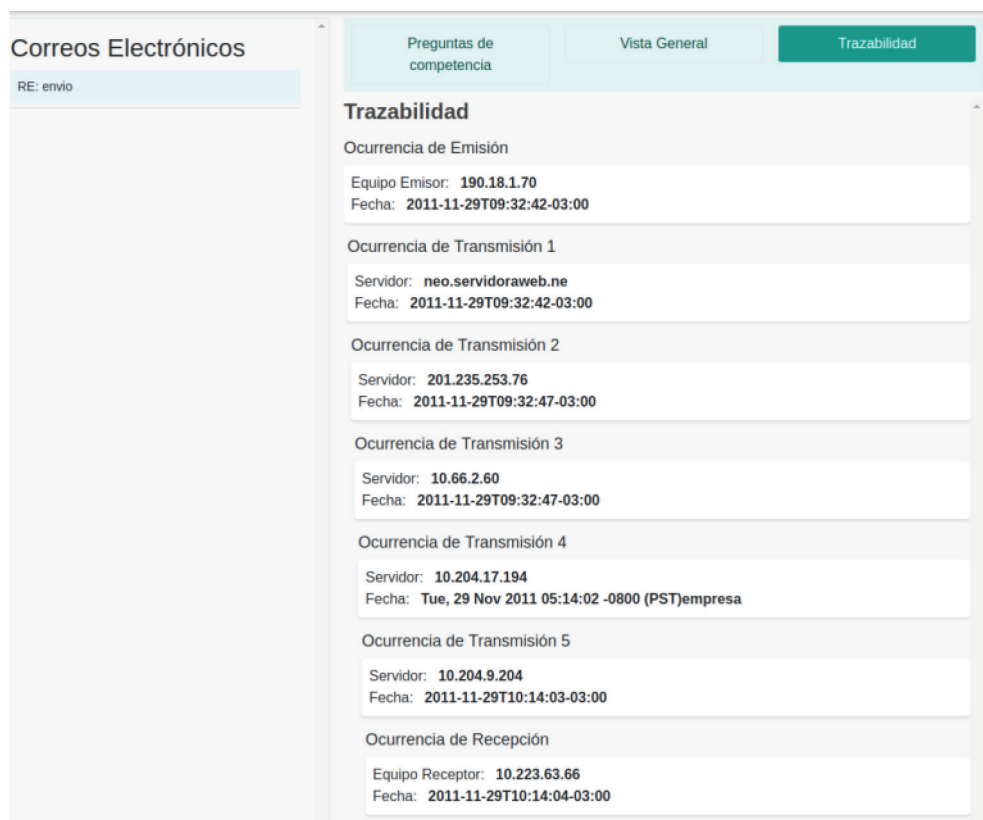


Figura 4 – Trazabilidad de un correo analizado

5. Discusión

A continuación, se describe el marco teórico considerado para definir el framework OntoFoCE propuesto para el análisis forense de correos electrónicos a partir de la ontología desarrollada.

Respecto de las herramientas disponibles para analizar un correo electrónico, se citan aquellas de más interés para la presente investigación.

Aid4Mail, utilizado para la migración y conversión de correos de/a diversos formatos, soporta más de 40 formatos de correo electrónico y programas de cliente de correo, así como muchos servicios populares de correo web y cuentas remotas. Respecto de esta herramienta, OntoFoCE es superadora en cuanto que acepta archivos con formato plano, el modelo ontológico utilizado como soporte para el análisis forense brinda información más completa y se enfoca en dar una respuesta a los puntos de pericia.

EmailTrackerPro no sólo ofrece la capacidad de rastrear un correo electrónico usando su encabezado, sino que también permite filtrar spam, escaneando cada correo a medida

12) Dado una cuenta C1 ¿se ha emitido un correo hacia la cuenta C2?

C1: beatriz@empresa.com.ar
 C2: jose@empresa.com.ar

Emisor: jose@empresa.com.ar
 Receptor: beatriz@empresa.com.ar
 Asunto: =?iso-8859-1?Q?RV_Env=EDo_formularios_de_Orden_de_Pago?=
 Fecha de emisión: Thu, 1 Mar 2018 17:07:34 -0300 (-03)

Emisor: jose@empresa.com.ar
 Receptor: beatriz@empresa.com.ar
 Asunto: RV: BANCO .
 Fecha de emisión: Wed, 13 Sep 2017 16:13:27 -0300 (-03)

13) Dado una cuenta C1 ¿se ha recibido un correo desde la cuenta C2?

C1: beatriz@empresa.com.ar
 C2: jose@empresa.com.ar

Emisor: jose@empresa.com.ar
 Receptor: beatriz@empresa.com.ar
 Asunto: =?iso-8859-1?Q?RV_Env=EDo_formularios_de_Orden_de_Pago?=
 Fecha de emisión: Thu, 1 Mar 2018 17:07:34 -0300 (-03)

Emisor: jose@empresa.com.ar
 Receptor: beatriz@empresa.com.ar
 Asunto: RV: BANCO .
 Fecha de emisión: Wed, 13 Sep 2017 16:13:27 -0300 (-03)

Correos intercambiados entre 2017-05-01 - 2018-01-01 por jose@empresa.com.ar y beatriz@empresa.com.ar

Emisor: jose@empresa.com.ar
 Receptor: beatriz@empresa.com.ar
 Asunto: RE: Mantenimiento de UPSs
 Fecha de emisión: 2017-08-11T11:36:40-03:00

Emisor: jose@empresa.com.ar
 Receptor: beatriz@empresa.com.ar
 Asunto: RV: INVITACION PARA CLIENTES FINALES SEMINARIO SIEMON DIA 21
 Fecha de emisión: 2017-09-14T11:26:33-03:00

Figura 5 – Resultados de la pregunta de competencia N° 12, 13 y 21

que llega y advierte al usuario si se sospecha de spam. La característica más valiosa de *EmailTrackerPro* es la capacidad de rastrear más de una dirección IP a la vez. Se puede trazar tantas direcciones IP y nombres de dominio como sea necesario y se envían los resultados a una nueva pestaña o un archivo Excel / HTML. Si se compara esta herramienta con OntoFoCE, se observa la coincidencia en el enfoque de la trazabilidad

del proceso de transmisión, a lo que OntoFoCE agrega por su parte las preguntas de competencia para responder a los puntos de pericia.

Existen frameworks integrados para el análisis forense de correos electrónicos, tales como el *Integrated E-mail Análisis Forense Framework (IEFAF)*, propuesto por (Hadjidj et al., 2009), que consta de 5 módulos: Navegador Interbase de datos, Explorador de estadísticas, Explorador de minería de datos, submódulo Weka y Explorador de E-mail. Consta además de una interfase gráfica con 5 visores (detalles del e-mail, ubicación geográfica de las IP, estadísticas; red social que vincula las IP con cuentas de correo; y minería de datos). No fue posible obtener una versión de esta herramienta para realizar un estudio comparativo sobre su funcionalidad versus las que ofrece OntoFoCE, pero de lo investigado se observa que, si bien el análisis apoyado en la minería de datos es lo más poderoso en esta herramienta, no se deduce que genere resultados directamente orientados a responder los puntos de pericia.

EnCase Forensic es una poderosa plataforma de investigación que recolecta datos digitales, realiza análisis, informa sobre descubrimientos y los preserva en un formato válido a efectos legales, en el caso de correos electrónicos cuenta con una amplia compatibilidad con los distintos formatos de archivos de correos y permite obtener un archivo imagen del mismo con el objeto de preservar la prueba original libre de manipulación. Aquí también es distintiva la funcionalidad de la herramienta para el análisis forense de correos electrónicos, y los informes de resultados que muestran los datos desde varias ópticas, pero dejando a consideración del perito la selección de los resultados que le permitan responder a los puntos de pericia.

En el trabajo (Rivetti & Gallo, 2017) se realizó un estudio comparativo de algunas herramientas de uso libre, disponibles en la web para el análisis de estos casos, encontrándose que *MailXaminer* es la más eficiente cuando se trata de un conjunto masivo de cabeceras de correos electrónicos. Con la aplicación informática que aquí se presenta se realizó el análisis forense de 774 correos con un tiempo de procesamiento total de 22 segundos, incluyendo la extracción de los datos, clasificación e instanciación correspondiente en la ontología. Este mismo conjunto de datos, analizados con las herramientas *MailXaminer* insumió un tiempo de 83 segundos, lo que muestra la eficiencia del algoritmo para procesar grandes volúmenes de datos.

Respecto del Framework OntoFoCE, se puede decir que es posible encontrar herramientas disponibles para el análisis forense de correos electrónicos que permiten procesar un conjunto de cabeceras de correos electrónicos, pero la mayoría de ellas se agotan en mostrar los datos de la cabecera, que permiten responder puntos de pericia simples (como por ejemplo cuales son los datos de emisión/recepción del correo), dejando a consideración del perito la respuesta a los *puntos periciales complejos* como por ejemplo, establecer la trazabilidad del correo, identificar correos enviados y recibidos en rangos de fechas, o buscar información de correos asociadas entre un conjunto de cuentas de correo, entre otros. Una particularidad de la aplicación es la posibilidad de incrementar el banco de preguntas de competencia, en caso de encontrar un punto de pericia que no pueda responderse desde las preguntas existentes. Esto es posible debido a que una nueva pregunta de competencia se formaliza e integra en la aplicación mediante una consulta SPARQL.

6. Conclusiones

Considerando el conjunto de herramientas analizadas, ninguna de ellas cumple integralmente con el cometido final de dar respuesta a los puntos de pericia de manera directa e inmediata, en todos los casos, corre a cargo del perito la identificación de aquellos datos que le son de utilidad para responder a los puntos de pericia. Ello es así porque no se consideran a estos últimos, los puntos de pericia, como elementos expresados en lenguaje natural que luego se representan mediante preguntas de competencia de una ontología. Se considera que ésta es la principal ventaja de OntoFoCE frente a otras herramientas.

Otra cuestión propia de la herramienta desarrollada, es la generación de un marco integral para el procesamiento automático de las cabeceras, cuando la cantidad de correos a analizar significa un volumen importante de datos, con el consiguiente esfuerzo en tiempo y dedicación que implicaría revisar una a una las cabeceras de correo o trabajando separadamente con herramientas de forensia e integrar luego los resultados obtenidos. El Framework OntoFoCE contempla el proceso ETL completo de las cabeceras de correos electrónicos, así como los procesos para instanciar la ontología, y realizar el análisis forense permitiendo contestar los puntos de pericia.

Cabe destacar que la aplicación se construyó utilizando tecnologías web, lo que permite disponer de una herramienta en línea accesible desde cualquier dispositivo con conexión a internet a través de un navegador web, considerando además los criterios y políticas de seguridad necesarias para el análisis forense.

Referencias

- Arcila-Calderón, C., Barbosa-Caro, E., & Cabezuelo-Lorenzo, F. (2016). Técnicas big data: análisis de textos a gran escala para la investigación científica y periodística. *El Profesional de La Información*, 25(4), 623. <https://doi.org/10.3145/epi.2016.jul.12>
- Blandón Andrade, J. C. (2018). A State-of-the-art Review About Ontology Population. *Ingeniería y Desarrollo*, 36(1), 259–284. <https://doi.org/10.14482/inde.36.1.10949>
- Brady, O., Overill, R., & Keppens, J. (2015). DESO: Addressing volume and variety in large-scale criminal cases. *Digital Investigation*, 15, 72–82. <https://doi.org/10.1016/j.diin.2015.10.002>
- Chabot, Y., Bertaux, A., Nicolle, C., & Kechadi, T. (2015). An ontology-based approach for the reconstruction and analysis of digital incidents timelines. *Digital Investigation*, 15, 83–100. <https://doi.org/10.1016/j.diin.2015.07.005>
- Chhabra, G. S., & Bajwa, D. S. (2012). Review of E-mail System, Security Protocols and Email Forensics. *International Journal of Computer Science & Communication Networks*, 5(3), 201–211.
- Darahuge, M. E., & Arellano González, L. E. (2016). *Manual de Informática Forense III*.
- David, L., Parra, L., Rico-bautista, D., Medina-cárdenas, Y., & Sanchez-Ortiz, A. (2018). Definición de una metodología práctica para la adquisición y análisis de evidencia digital en el contexto de una investigación post mortem, 369–384.

- Devendran, V. K., Shahriar, H., & Clincy, V. (2015). A Comparative Study of Email Forensic Tools. *Journal of Information Security*, 06(02), 111–117. <https://doi.org/10.4236/jis.2015.62012>
- Di Ioro, A. H., Castellote, M. A., Constanzo, B., Curti, H., Waimann, J., Lamperti, S. B., ... & Nuñez, L. (2017). El rastro digital del delito Aspectos técnicos , legales y estratégicos de la Informática Forense. Mar del Plata: Esitorial UFASTA.
- Faria, C., Serra, I., & Girardi, R. (2014). A domain-independent process for automatic ontology population from text. *Science of Computer Programming*, 95(P1), 26–43. <https://doi.org/10.1016/j.scico.2013.12.005>
- Flores, V., & Hadfeg, Y. (2017). Un método para generar explicaciones de resultados de un Sistema Experto, usando Patrones de discurso y Ontología. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, (21), 99–114. <https://doi.org/10.17013/risti.21.99-114>
- Gallo, B. P. de, & Leone, H. (2016). Aplicación de la Ingeniería Ontológica para representar la trazabilidad de un Correo Electrónico. In: 2º Simposio Argentino de Ontologías y Sus Aplicaciones (SAOA 2016), 108–121.
- Gallo, B. P. de, Vegetti, M., & Leone, H. (2015). Población de ontologías con datos no estructurados utilizando herramientas de minería de datos. In Congreso Nacional de Ingeniería Informática / Sistemas de Información - CONAIISI 2015, Buenos Aires, Argentina.
- Gallo, B. P. de, Vegetti, M., & Leone, H. (2017). Hacia una Ontología para el soporte de la trazabilidad del correo electrónico en la Forensia Digital. In V Congreso Iberoamericano de Docentes e Investigadores de Derecho e Informática (CIIDDI 2017), Habana, Cuba.
- Hadjidi, R., Debbabi, M., Lounis, H., Iqbal, F., Szporer, A., & Benredjem, D. (2009). Towards an integrated e-mail forensic analysis framework. *Digital Investigation*, 5(3–4), 124–137. <https://doi.org/10.1016/j.diin.2009.01.004>
- Kota, V. K. (2012). An Ontological Approach for Digital Evidence Search. *International Journal of Scientific and Research Publications*, 2(12), 409–414. <https://doi.org/10.1.1.642.3055>
- Morgan, R. M. (2017a). Science and Justice Conceptualising forensic science and forensic reconstruction. Part I: A conceptual model. *Science & Justice*, 57(6), 455–459. <https://doi.org/10.1016/j.scijus.2017.06.002>
- Morgan, R. M. (2017b). Science and Justice Conceptualising forensic science and forensic reconstruction. Part II: The critical interaction between research, policy / law and practice. *Science & Justice*, 57(6), 460–467. <https://doi.org/10.1016/j.scijus.2017.06.003>
- Noll, R. P., & Ribeiro, M. B. (2007). Enhancing traceability using ontologies. In *Proceedings of the 2007 ACM Symposium on Applied Computing*, 1496–1497. <https://doi.org/10.1145/1244002.1244322>

- Ovens, K. M., & Morison, G. (2016). Identification and analysis of email and contacts artefacts on iOS and OSX. In *Proceedings of 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, (October 2017), 321–327. <https://doi.org/10.1109/ARES.2016.56>
- Rivetti, E. A., & Gallo, B. P. de. (2017). Estudio comparativo de desempeño de herramientas para el Análisis Forense de Correos Electrónicos. In *Congreso Nacional de Ingeniería Informática / Sistemas de Información - CONAIISI 2017* (pp. 46–51).
- Rueda-Rueda, J. S., Rico-Bautista, D., & Guerrero, C. D. (2018). Guía práctica abierta para el análisis forense digital en dispositivos Android, 442–457.
- Sarli, J. L., Leone, H., & Gutierrez, M. (2019). SCFHLA: Un Modelo de Interoperabilidad Semántica para Simulación Distribuida de Cadenas de Suministro. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (30), 34–50. <https://doi.org/10.17013/risti.30.34-50>
- Selamat, S. R., Shahrin, S., Hafeizah, N., Yusof, R., & Abdollah, M. F. (2013). A Forensic Traceability Index in Digital Forensic Investigation. *Journal of Information Security*, 04(01), 19–32. <https://doi.org/10.4236/jis.2013.41004>
- Stadlinger, J., & Dewald, A. (2017). A Forensic Email Analysis Tool Using Dynamic Visualization. *The Journal of Digital Forensics, Security and Law*, 12(1), 3–31. <https://doi.org/https://doi.org/10.15394/jdfsl.2017.1413>
- Tolaba, A. C., Caliusco, M. L., & Galli, M. R. (2015). Representación del Conocimiento de la Información Geográfica siguiendo un Enfoque basado en Ontologías. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, (14), 101–116. <https://doi.org/10.17013/risti.14.101-116>
- Xie, L., Liu, Y., & Chen, G. (2016). A forensic analysis solution of the email network based on email contents. In *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2015*, 1613–1619. <https://doi.org/10.1109/FSKD.2015.7382186>
- Ya'u, B. I., Nordin, A., & Salleh, N. (2017). Software requirements patterns and meta model: A strategy for enhancing requirements reuse (RR). In *Proceedings of 6th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2016*, 188–193. <https://doi.org/10.1109/ICT4M.2016.42>
- Youn, S. (2014). SPONGY (SPam ONtology): Email classification using two-level dynamic ontology. *Scientific World Journal*, 2014. <https://doi.org/10.1155/2014/414583>
- Yubao, W. U. (2015). Research on Electronic Data Tracing Method Based on Trusted Forensics. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (16a), 204–213. <https://doi.org/10.17013/risti.16a.204-213>

Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones

Régner Sabillón¹, Jeimy J. Cano M.²

regners@athabascau.ca , jcano@uniandes.edu.co

¹ Universitat Oberta de Catalunya, Internet Interdisciplinary Institute (IN3), Parc Mediterrani de la Tecnologia (Edifici B3), Av. Carl Friedrich Gauss, 5, 08860 Castelldefels, Barcelona, España.

² Universidad de los Andes, Bogotá, Facultad de Derecho, Cra 1E No. 18ª-10, Bogotá, Colombia.

DOI: 10.17013/risti.32.33-48

Resumen: Este artículo presenta los resultados de un estudio de implementación y validación del Modelo de Auditoría de Ciberseguridad (CSAM), en un estudio de casos múltiples en una universidad canadiense. Se propone que el modelo se utilice para adelantar auditorías de ciberseguridad en cualquier organización o nación, y así evaluar la seguridad, su madurez y la preparación frente a la seguridad cibernética. De igual forma, detectar las necesidades para acrecentar la conciencia cibernética a nivel organizacional y personal. CSAM se ha probado, implementado y validado en tres escenarios de investigación (1) Auditoría de todos los dominios del modelo, (2) Auditoría de varios dominios y (3) una auditoría de un único dominio. El artículo concluye detallando información relevante para la toma de decisiones futuras con el fin de ajustar las limitaciones de ciberseguridad identificadas, mejorar sus dominios y controles, y de esta manera, implementar y probar de manera eficiente este modelo en cualquier organización o país.

Palabras-clave: Ciberseguridad; modelos de auditoría de ciberseguridad; auditorías en ciberseguridad; controles en ciberseguridad; aseguramiento en ciberseguridad.

Audits in Cybersecurity: A model of general application for companies and nations

Abstract: This article presents the results of an implementation and validation study of the Cybersecurity Audit Model (CSAM), in a multiple case study at a Canadian university. It is proposed that the model be used to advance cybersecurity audits in any organization or nation to assess security, its maturity, and preparedness for cybersecurity. Similarly, identify needs to increase cybersecurity awareness at the organizational and personal levels. CSAM has been tested, implemented and validated in three investigation scenarios (1) Audit of all model domains, (2) Audit of several domains and (3) an audit of a single domain. The article concludes by detailing relevant information for future decision making in order to adjust the identified cybersecurity limitations, improve their domains and controls, and thus efficiently implement and test this model in any organization or country.

Keywords: Cybersecurity; cybersecurity audit models; cybersecurity audits; cybersecurity controls; cybersecurity assurance

1. Introducción

Las organizaciones tratan de proteger los activos cibernéticos e implementar medidas y programas de ciberseguridad, pero a pesar de este esfuerzo continuo, es inevitable que se presenten las violaciones de la ciberseguridad y se materialicen ataques cibernéticos.

Un estudio reciente (Hiscox, 2017) destaca que la incidencia de ataques cibernéticos es alta en compañías británicas, estadounidenses y alemanas de diferentes industrias y sectores, incluyendo tecnología, finanzas, servicios empresariales, manufactura, servicios profesionales, comercio minorista, construcción, transporte, alimentos y bebidas, salud, ocio, telecomunicaciones, bienes raíces, medios de comunicación, energía y productos farmacéuticos, desde pequeñas empresas hasta grandes corporaciones. El 57% de las empresas han experimentado al menos uno y el 42% de esas organizaciones se han ocupado de dos o más ataques cibernéticos en el último año. La mayoría de las empresas (62%) generalmente se recuperan de un incidente cibernético en menos de 24 horas; un cuarto (26%) generalmente toma menos de una hora para volver a los negocios, mientras que algunas compañías pasan dos días o más para recuperarse de un ataque cibernético. El análisis de brechas sugiere que invertir dinero o tener grandes presupuestos de seguridad cibernética no ayuda a las empresas a alcanzar el nivel de “Expertos en Internet”. Por el contrario, un importante desembolso financiero no es la solución sino la implementación de otras medidas de estrategia y proceso, como la participación de la alta gerencia, la capacitación en concientización sobre la seguridad cibernética, el seguimiento sistemático y la documentación. Los costos de un ataque cibernético varían según las zonas geográficas, por ejemplo, con las empresas con más de 1.000 empleados, el impacto financiero costaría \$ 53,131 en Alemania, \$ 84,045 en el Reino Unido y \$ 102,314 en los Estados Unidos (Hiscox, 2017).

Las auditorías de TI se están redefiniendo para incluir la ciberseguridad, sin que a la fecha existan pautas claras o consenso sobre qué áreas, subáreas, dominios o subdominios se incluirán en una auditoría de ciberseguridad. El modelo propuesto de auditoría de seguridad cibernética (CSAM), detallado en este artículo, ha sido diseñado para abordar las limitaciones y la inexistencia de controles de seguridad cibernética con el fin de materializar un programa de ciberseguridad o desarrollar auditorías de ciberseguridad específicas de dominio. Por tanto, un modelo extenso de auditoría de ciberseguridad puede apoyar la función de seguridad de la información y al mismo tiempo establecer un marco de trabajo para la concientización en seguridad de la información basada en los roles de la empresa.

Portanto, se presentan los resultados de un estudio empírico que evaluó la implementación y validación del CSAM a través de una extensa auditoría de ciberseguridad. Este estudio fue motivado por la falta de directrices generales para llevar a cabo auditorías exhaustivas de ciberseguridad y las debilidades existentes de los programas disponibles a la fecha para impartir entrenamiento en concientización sobre la ciberseguridad.

Esta investigación se realizó con el propósito de dar respuesta a las siguientes interrogantes:

¿Cómo podemos evaluar y medir el nivel aseguramiento de la ciberseguridad, la madurez y la ciberpreparación en cualquier organización o Nación?

¿Por qué es necesario aumentar la ciberconciencia a nivel organizacional y personal?

2. Metodología

El objetivo de este estudio es investigar y proporcionar modelos integrales para los desafíos que puedan surgir al planificar y realizar auditorías de ciberseguridad, así como la implementación de la capacitación propia de la concientización sobre ciberseguridad. Entre los casos de estudio se consideran los más relevantes los estudios observacionales; los resultados de cualquier caso de estudio son limitados en generalización y aplicaciones más amplias (Edgard & Manz, 2017). Algunos autores prefieren diseñar sus casos de estudio utilizando la metodología de investigación de Yin (2009). Bartnes & Brede (2016) presentaron su investigación utilizando la recopilación de datos, el análisis de datos, las secciones de escenarios y contenido de casos. Meszaros & Buchalcevova (2016) diseñaron el Marco de Seguridad de Servicios Online (OSSF) y sus métodos de investigación se organizaron en un proceso con las siguientes actividades:

1. Identificación del problema y motivación.
2. Definición de objetivos para una solución.
3. Diseño y desarrollo.
4. Demostración
5. Evaluación
6. Comunicación

Luego de esta declaración, se ha diseñado, implementado y validado un estudio de casos múltiples basado en Yin (2018) de dos ejercicios: una auditoría de ciberseguridad y una capacitación de concientización sobre la ciberseguridad en una institución de educación superior canadiense. No es posible revelar más detalles de la organización objetivo por los acuerdos de confidencialidad establecidos. Se ha realizado este estudio de casos múltiples siguiendo la metodología de investigación propuesta por Yin (2018).

La motivación de este estudio tuvo como objetivo diseñar un modelo que incluyera un enfoque completo para planificar y realizar auditorías de ciberseguridad en cualquier organización con la capacidad para evaluar igualmente, las estrategias nacionales de ciberseguridad. Además, se identificó que era necesario lidiar con la falta de conocimiento para enfrentar los ataques y las amenazas cibernéticas, y como resultado, se diseñó un modelo organizacional de capacitación para la concientización sobre ciberseguridad que se puede implementar para fundar los elementos de cualquier programa de concientización sobre ciberseguridad.

3. Marco General de Gestión de Riesgos

Los modelos vigentes de ciberseguridad o de auditoría de ciberseguridad, responden por lo general a una gestión de riesgos conocidos. Las organizaciones basadas en sus

experiencias previas, resultados de ejercicios anteriores y revisiones de terceros, establecen un marco general de riesgos que terminan articulando en las ya conocidas matrices de riesgo-control, las cuales son revisadas y validadas en última instancia por los ejecutivos de las empresas (Cano, 2018).

En este contexto, las prácticas comunes de riesgo, generalmente articuladas desde el ISO 31000 e ISO 27005, establecen una serie de pasos que buscan explorar de forma eficiente la manera como la organización se puede enfrentar a aquellas amenazas y actividades no deseadas previamente establecidas en el entorno (Díaz & Muñoz, 2018), dejando posiblemente fuera del radar aquellas que pueden afectarla gravemente por lo incierto de su manifestación.

De acuerdo con lo anterior, se hace necesario introducir un marco de trabajo de riesgos que actualice las prácticas actuales de su gestión, con el fin de ir más allá de los riesgos conocidos, y establecer un escenario extendido de revisión y análisis que dé cuenta tanto de las posibilidades como de las probabilidades. La ventana de AREM (Cano, 2014) es un marco de trabajo estratégico y táctico que no solo incluye los riesgos conocidos, sino que desarrolla aquellos que son propios del sector de la empresa que hace el ejercicio (riesgos focales), los latentes y los emergentes. Este instrumento, que ha sido probado en grandes empresas de energía como en el sector financiero, así como en la identificación y gestión de los riesgos de la infraestructura crítica de un país, permite a los auditores de ciberseguridad, movilizar sus reflexiones más allá del cuadrante de riesgos conocidos, para motivar conversaciones con las empresas para ver escenarios ampliados de amenazas, las cuales pueden no ser visibles desde el uso tradicional de los estándares.

Basado en lo anterior, la aplicación del Modelo de Auditoría de Ciberseguridad (CSAM), fundado en la gestión de riesgos usando la ventana de AREM, permite a los auditores mantener una sensibilidad concreta del entorno, que habilita una vista sistémica de los riesgos, para explorar en profundidad los diferentes dominios del modelo mencionado y buscar alternativas de aseguramiento que aumentan la confiabilidad de las prácticas de ciberseguridad de las empresas evaluadas.

4. El Modelo de Auditoría de CiberSeguridad (CSAM)

El Modelo de Auditoría de Ciberseguridad (CSAM) es un modelo innovador y exhaustivo que incluye la evaluación óptima de la ciberseguridad en cualquier organización y puede verificar pautas específicas para las naciones que planean implementar una estrategia nacional de seguridad cibernética o desean evaluar la efectividad de su Estrategia o Política Nacional de Ciberseguridad ya en vigor. El CSAM se puede implementar para llevar a cabo auditorías internas o externas de ciberseguridad, este modelo se puede usar para realizar auditorías de ciberseguridad individuales o puede ser parte de cualquier programa de auditoría corporativa para mejorar los controles de ciberseguridad. Cualquier equipo de auditoría tiene las opciones de realizar una auditoría completa para todos los dominios de ciberseguridad o simplemente seleccionando dominios específicos para auditar ciertas áreas que necesiten verificación de control y fortalecimiento. El CSAM tiene 18 dominios; el dominio 1 es específico para las Naciones y los dominios 2-18 se pueden implementar

en cualquier organización. La organización puede ser cualquier empresa pequeña, mediana o grande, el modelo también es aplicable a cualquier organización sin fines de lucro.

El objetivo de este trabajo es introducir un modelo de auditoría de ciberseguridad que incluya todas las áreas funcionales, a fin de asegurar una evaluación efectiva de ciberseguridad, su madurez y preparación cibernética en cualquier organización o Nación que esté auditando su Estrategia Nacional de Ciberseguridad. Esta propuesta se concibió como un modelo de auditoría de ciberseguridad integrado para evaluar y medir el nivel de madurez de la ciberseguridad y la preparación cibernética en cualquier tipo de organización, sin importar en qué industria o sector esté posicionada la organización. Muchos marcos de seguridad cibernética están orientados principalmente hacia una industria específica como el “PCI DSS” para la seguridad de las tarjetas de crédito, el “NERC CIP Cyber Security” para el sistema de energía eléctrica o el “Marco de seguridad cibernética del NIST” para proteger la infraestructura crítica nacional.

Sin embargo, los marcos existentes no proporcionan una vista unificada para la planificación y la realización de auditorías de ciberseguridad. La necesidad de alinear los marcos de seguridad cibernética específicos se debe a los requisitos regulatorios propios de las industrias, con el fin de cumplir con las auditorías internas o externas, y así satisfacer los propósitos comerciales y los requisitos del cliente o simplemente mejorar la estrategia de ciberseguridad de la empresa.

El Modelo de Auditoría de Ciberseguridad (CSAM) contiene información general, recursos, 18 dominios, 26 subdominios, 87 listas de verificación, 169 controles, 429 subcontroles, 80 evaluación de pautas y un cuadro de evaluación que se muestra en la Figura 1.



Figura 1 – Modelo de Auditoría de Ciberseguridad (CSAM)

4.1. Información General

Esta sección presenta la estructura del modelo, la metodología de trabajo y las posibles opciones de implementación.

4.2. Recursos

Este componente proporciona enlaces a recursos adicionales para ayudar a comprender los temas de ciberseguridad:

Ciberseguridad: Centro de Recursos de Seguridad Informática del Instituto Nacional de Estándares y Tecnología (NIST), prácticas de ciberseguridad de la Autoridad Reguladora de la Industria Financiera (FINRA) y ciberseguridad de la Seguridad Nacional (USA Homeland Security).

Estrategia nacional de ciberseguridad: Estrategia de ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN), estrategia de ciberseguridad de la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA) y análisis comparativo de la Organización para la Cooperación y el Desarrollo Económico (OCDE) de las estrategias nacionales de ciberseguridad.

Gobernanza: Junta de Gobernanza de Ciberseguridad en PricewaterhouseCoopers y ciberseguridad de MITRE Corporation.

Activos cibernéticos: activos cibernéticos críticos de NERC (North American Electric Reliability Corporation).

Marcos: Marcos comunes de ciberseguridad de Foresite, el marco del Equipo de Preparación para Emergencias Informáticas de los EE.UU. (US-CERT) y el de ISACA (Information Systems Audit and Control Association) implementando el marco de ciberseguridad del NIST.

Arquitectura: Guía de arquitectos del TCG (Trusted Computer Group) y la arquitectura de seguridad de TI del Departamento de Energía de EE. UU.

Gestión de vulnerabilidades: Evaluación de vulnerabilidad SANS, evaluación y gestión de la seguridad nacional.

Inteligencia de amenazas cibernéticas: SANS (SysAdmin, Audit, Network and Security Institute): ¿Quién usa la inteligencia de amenazas cibernéticas y cómo?

Respuesta a incidentes: Preguntas frecuentes sobre el Equipo de respuesta a incidentes de seguridad informática (CSIRT – Computer Security Incident Response Team).

Análisis forense digital: Libros blancos de análisis forense SANS.

Conocimiento: NCSA (National Cyber Security Alliance) - Manténgase seguro online y PCI DSS (Payment Card Industry Data Security Standard): Mejores prácticas para implementar el programa de conocimiento de seguridad.

Defensa cibernética: SANS- La escala móvil de la ciberseguridad.

Recuperación ante desastres: FEI (Financial Executives International) Canadá - Ciberseguridad y continuidad de negocios.

Personal: Kaspersky - Los 10 mejores consejos para educar a los empleados sobre la ciberseguridad.

4.3. Dominios

El CSAM contiene 18 dominios. El dominio 1 ha sido diseñado exclusivamente para Naciones y los dominios 2-18 son aplicables a cualquier organización.

4.4. Subdominios

Todos los dominios tienen al menos un subdominio, pero en ciertos casos pueden existir varios subdominios por dominio.

Los subdominios son Ciberespacio, Gobernanza, Estrategia, Legal y Regulatorio, Gestión de Activos Cibernéticos, Riesgos Cibernéticos, Marcos y Regulaciones, Arquitectura, Redes, Información, Sistemas, Aplicaciones, Gestión de Vulnerabilidad, Inteligencia de Amenazas, Administración de Incidentes, Forensia Digital, Programa de Cibereducación Seguro Cibernético, Defensa Cibernética Activa, Tecnologías en Evolución, Recuperación de desastres, Contratación, Recursos Humanos, Habilidades, Capacitación y Despidos/ Renuncias.

4.5. Controles

Cada dominio tiene subdominios que tienen asignado un número de referencia. Los controles se identifican mediante números de cláusula y una lista de verificación asignada. Para verificar la evaluación de control, el control de ciberseguridad está definido o es inexistente.

4.6. Listas de Verificación

Cada lista de verificación está vinculada a un dominio específico y al subdominio subordinado. La lista de verificación verifica la validez de los subcontroles de ciberseguridad alineados con una cláusula de control. Los auditores de ciberseguridad tienen la opción de recopilar evidencia para verificar el cumplimiento del control secundario.

4.7. Evaluación de Directrices

La evaluación de la guía solo se aplica al dominio de las Naciones. Las directrices se evalúan para determinar la cultura de ciberseguridad, la Estrategia Nacional de Ciberseguridad (ENC), las operaciones cibernéticas, las infraestructuras críticas, la inteligencia cibernética, la guerra cibernética, la ciberdelincuencia y la diplomacia cibernética.

4.8. Cuadro de Evaluación

La evaluación de control, directriz y subcontrol se calcula después de que se haya completado la auditoría. La evaluación consiste en asignar puntajes y calificaciones para cada control, directriz y control secundario.

Se calcula la clasificación final de la madurez de la ciberseguridad del dominio de las Naciones utilizando los siguientes criterios. La puntuación se puede asignar a un nivel de madurez específico:

Inmaduro (I): 0-30

La Nación no tiene planes para administrar su ciberespacio. Una Estrategia o Política Nacional de Ciberseguridad (ENC) es inexistente.

En desarrollo (D): 31-70

La Nación está empezando a centrarse en la ciberseguridad nacional. Si las tecnologías están en su lugar, la Nación debe centrarse en áreas clave para proteger el ciberespacio.

Maduro (M): 71-90

Mientras que la Nación tiene un ambiente maduro. Se requieren mejoras en áreas claves que se han identificado con debilidades.

Avanzado (A): 91-100

La Nación se ha destacado en la ciberseguridad nacional y en las prácticas del ciberespacio. Siempre hay espacio para mejorar. La Nación podría convertirse en un líder internacional y ayudar a otros Estados en temas de ciberseguridad y ciberespacio.

Y para los dominios 2-18, calculamos la calificación final de madurez de la ciberseguridad de cualquier organización utilizando los siguientes criterios:

La puntuación se puede asignar a un nivel de madurez específico:

Inmaduro (I): 0-30

La organización no tiene planes para gestionar su ciberseguridad. Los controles para las áreas críticas de ciberseguridad son inexistentes o muy débiles. La organización no ha implementado un programa integral de ciberseguridad.

En desarrollo (D): 31-70

La organización está empezando a centrarse en asuntos de ciberseguridad. Si las tecnologías están en su lugar, la organización debe centrarse en áreas clave para proteger los activos cibernéticos. La atención debe estar enfocada hacia el personal, procesos, controles y regulaciones.

Maduro (M): 71-90

Mientras que la organización tiene un ambiente maduro. Se requieren mejoras en las áreas claves que se han identificado con debilidades.

Avanzado (A): 91-100

La organización ha destacado en la implementación de las mejores prácticas de ciberseguridad. Siempre existen posibilidades para la mejora continua. Se debe mantener la documentación correspondiente actualizada y revisar continuamente los procesos de ciberseguridad a través de auditorías y basado en el marco general de riesgos latentes y emergentes.

5. Resultados

El CSAM se implementó y validó utilizando tres escenarios diferentes en la institución de educación superior canadiense. Para implementar y validar el CSAM, también diseñamos el CATRAM que se implementó simultáneamente junto con el CSAM. Nuestras preguntas de investigación se abordaron adecuadamente mediante la creación y validación de dos modelos de ciberseguridad en las áreas de auditoría y concientización. La organización objetivo consideró los tres escenarios como realistas para su evaluación, capacitación de sensibilización, aseguramiento y auditoría de ciberseguridad. Se concluye que los dos modelos de ciberseguridad son funcionales y útiles según se observa en los resultados de la validación (Tabla 1). Por lo tanto, los modelos de ciberseguridad son susceptibles de implementar y probar en cualquier organización. Blokdyk (2018) utiliza un enfoque similar para presentar los resultados del cuadro de mando de ciberseguridad. Esta autoevaluación de la ciberseguridad presenta el cuadro de mando ilustrado en un gráfico de radar, que destaca un sistema de puntaje de siete criterios que incluye el reconocimiento, la definición, la medición, el análisis, la mejora, el control y el mantenimiento de los asuntos de ciberseguridad con un enfoque en la gestión de riesgos.

No.	Ciberdominios	Resultados
2	Gobernanza y Estrategia	35%
3	Marco Legal y Conformidad	90%
4	Activos Cibernéticos	30%
5	Riesgos Cibernéticos	60%
6	Marcos y Regulaciones	30%
7	Arquitectura y Redes	67%
8	Información, Sistemas y Aplicaciones	55%
9	Identificación de Vulnerabilidades	30%
10	Inteligencia de Amenazas	60%
11	Gestión de Incidentes	10%
12	Análisis Forense Digital	30%
13	Educación de Concientización	60%
14	Ciberseguros	90%
15	Defensa Cibernética Activa	5%
16	Tecnologías Evolutivas	100%
17	Recuperación ante Desastres	30%
18	Gestión de Recursos Humanos	77%
Nivel de Madurez en Ciberseguridad		51%

Tabla 1 – Nivel de Madurez basado en múltiples ciberdominios

El siguiente resumen presenta oportunidades al mejorar y fortalecer las medidas de seguridad cibernética en nuestra organización objetivo.

Dominios de ciberseguridad que necesitan atención inmediata basada en la auditoría CSAM:

Marcos y regulaciones (30%): La organización necesita seleccionar un marco o componentes de seguridad específicos de varios marcos de seguridad de la información para implementar los marcos deseados. Se debe seleccionar un marco de ciberseguridad para garantizar la protección de las áreas funcionales, la gestión de riesgos, los controles de seguridad y la auditoría.

Identificación de vulnerabilidades (30%): La organización necesita implementar un plan de evaluación de vulnerabilidad. Se requiere un plan para implementar el escaneo continuo, las pruebas de penetración, la evaluación de vulnerabilidades, las medidas de corrección de vulnerabilidades y buscar la alineación con el panorama actual de amenazas cibernéticas y los riesgos existentes.

Gestión de incidentes (10%): La organización necesita saber cómo afrontar los ataques cibernéticos. Un plan de acción es urgente. La organización necesita un plan de acción para implementar la gestión de respuesta a incidentes, establecer niveles de escalamiento y comunicación, educación y concientización de incidentes, una política corporativa de gestión de incidentes y definir el procedimiento para todas las fases de respuesta a incidentes cibernéticos.

Análisis forense digital (30%): Ya sea para contratar consultores externos o capacitar a su personal de TI, la organización debe tener un plan que debe formar parte de la gestión de incidentes cibernéticos de su organización. La organización no está familiarizada con los procedimientos de investigación digital, los procedimientos de cadena de custodia y las investigaciones de descubrimiento electrónico.

Defensa cibernética activa (5%): La organización necesita implementar controles de ciberseguridad para todas las áreas de negocios. La organización no ha implementado controles críticos para aplicar la defensa cibernética activa, detectar y analizar ataques cibernéticos, mitigar daños cibernéticos y contramedidas externas fuera de sus redes.

Recuperación ante desastres (30%): La organización necesita agregar e integrar la ciberseguridad para su Recuperación ante desastres (DR) y su Plan de continuidad comercial (BCP). Si bien se han tomado algunas medidas para la recuperación general de desastres, la ciberseguridad no se ha considerado en ningún caso de interrupciones, ni en las evaluaciones para los escenarios posteriores a la reanudación.

Gobernanza y estrategia (35%): La organización debe definir su estrategia de seguridad cibernética e implementar un programa de ciberseguridad organizacional que esté alineado con la estrategia, misión, visión, metas y objetivos de la institución.

Dominios de ciberseguridad que necesitan mejoras en función de la auditoría CSAM:

Riesgos cibernéticos (60%): La organización necesita diseñar, implementar y revisar regularmente un plan de administración de riesgos cibernéticos. Se requiere una clara clasificación de los activos de información. Además, se necesita una política de gestión de riesgos cibernéticos bien definida, que incluya metas y objetivos junto con una matriz para aceptar, mitigar o transferir riesgos cibernéticos.

Activos cibernéticos (60%): Los activos cibernéticos deben identificarse y protegerse. Se requieren auditorías de inventario para identificar los activos cibernéticos y se requieren propietarios dentro de la organización.

Arquitectura y redes (67%): La organización necesita implementar controles adicionales para fortalecer la arquitectura y la seguridad de las redes. Las áreas que necesitan mejoras son defensa en profundidad, seguridad física, seguridad para productos y servicios de terceros, marcos de arquitectura, encriptación, pruebas de penetración, gestión de cuentas de usuarios y gestión del rendimiento.

Información, sistemas y aplicaciones (55%): La organización necesita implementar controles adicionales para reforzar la seguridad de la información, los sistemas y las aplicaciones. Las áreas que necesitan mejoras son la gestión de proyectos, la gestión de cambios, la gestión de registros, los controles y evaluaciones de auditoría, la gestión web, la planificación de recursos empresariales (ERP), la seguridad de las aplicaciones, los controles de salida de aplicaciones, los controles de seguimiento de auditoría de aplicaciones y los controles de correo electrónico.

Inteligencia de amenazas (60%): La organización necesita comenzar a recopilar y procesar información sobre posibles amenazas cibernéticas, vulnerabilidades cibernéticas y posibles ataques cibernéticos que pueden afectar sus operaciones. La organización debe dedicar recursos y equipos para mejorar la recopilación de inteligencia sobre amenazas y para implementar las políticas de respuesta requeridas.

Educación de concientización (60%): La organización necesita implementar un programa completo de concientización y capacitación sobre ciberseguridad para todas las partes interesadas. El entrenamiento parcial de concientización es ineficaz. Si bien CATRAM se implementó por completo como punto de partida para desarrollar el programa corporativo de concientización y capacitación sobre ciberseguridad, se

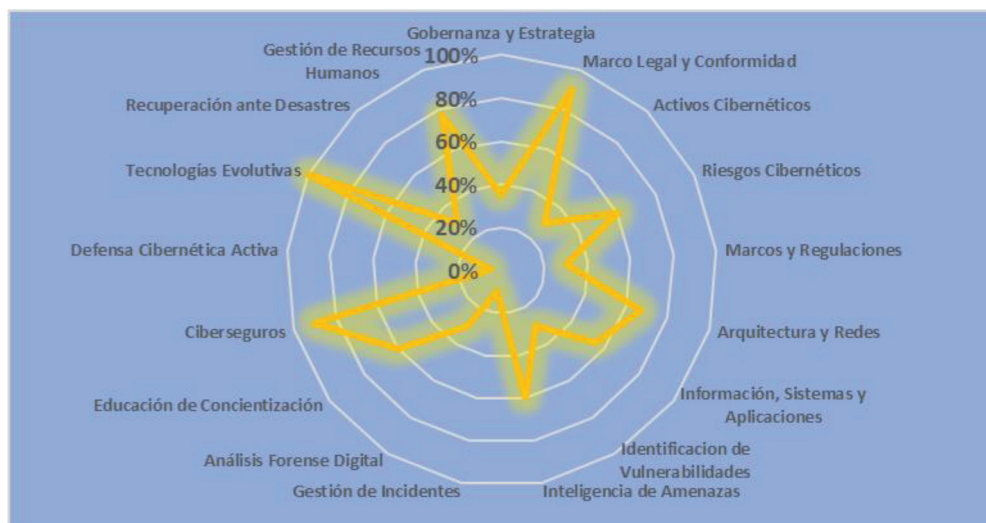


Figura 2 – Gráfico de Radar del estudio CSAM

recomienda particularmente realizar revisiones anuales para enfrentar las nuevas amenazas cibernéticas.

El estudio del caso demostró que el alcance de la investigación se logró según lo establecido. La evidencia para esta conclusión se presenta en la Figura 2.

6. Conclusiones

El objetivo principal de esta investigación fue diseñar y validar el Modelo de Auditoría de Ciberseguridad (CSAM) para enfrentar los desafíos al realizar auditorías de ciberseguridad integrales. El modelo de ciberseguridad que incluye todos sus componentes, fue validado satisfactoriamente por un caso de estudio realizado en una institución de educación superior canadiense.

El CSAM no es exclusivo para una industria, sector u organización. Por el contrario, el modelo se puede utilizar para planificar, realizar y verificar auditorías de ciberseguridad en cualquier organización o país. El CSAM ha sido diseñado para realizar auditorías de ciberseguridad parciales o completas para un dominio específico, varios dominios o para la auditoría integral de todos los dominios.

Los resultados de este estudio muestran que las auditorías de ciberseguridad realizadas por dominios pueden ser muy efectivas para evaluar los controles y las respuestas a las amenazas cibernéticas.

La limitación de nuestro estudio es que el modelo se validó en una sola organización, las limitaciones de tiempo, la falta de interés por los temas y la falta de compromiso fueron algunos de los desafíos que tuvimos que superar por parte de los participantes e investigadores. Por lo tanto, actualmente estamos realizando una segunda validación en una universidad canadiense diferente y más grande, que permita comprobar con nuevos datos de investigación científica el diseño y la efectividad del CSAM.

Los resultados de la investigación tienen implicaciones para nuestra organización objetivo, pero al mismo tiempo, implicaciones para futuras investigaciones en las que se pueda revisar y ampliar los modelos de ciberseguridad propuestos, integrando dentro de la dinámica de aplicación de éstos, la ventana de AREM, como soporte estratégico de riesgos y amenazas emergentes para los auditores de ciberseguridad (Cano, 2017).

Referencias

- Bartnes, M., Brede, N., & Heegaard, P.E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*. (61). 32–45. doi: 10.1016/j.cose.2016.05.004
- Bartnes, M., & Moe, N.B. (2017). Challenges in IT security preparedness exercises: A case study. *Computers and Security*. (67). 280–290. doi: 10.1016/j.cose.2016.11.017
- Blokdyk, G. (2018). *Cyber Security Risk Management: Complete Self-Assessment Guide*. Brisbane: Emereo Publishing.

- Cano, J. (2014). La ventana de AREM. Una herramienta estratégica y táctica para visualizar la incertidumbre. *Actas de la XIII Reunión Española de Criptología y Seguridad de la Información*. Alicante, España. Septiembre 2 al 5. Recuperado de: <http://web.ua.es/es/recsi2014/documentos/papers/la-ventana-de-arem-una-herramienta-estrategica-y-tactica-para-visualizar-la-incertidumbre.pdf>
- Cano, J. (2017). The AREM Window: A Strategy to Anticipate Risk and Threats to Enterprise Cyber Security. *ISACA Journal*. 5 (2017).
- Cano, J. (2018). Repensando los fundamentos de la gestión de riesgos. Una propuesta conceptual desde la incertidumbre y la complejidad. *Revista Ibérica de Tecnología y Sistemas de la Información*. (E15). Abril. 76–87.
- Center for Audit Quality – CAQ (2017). The CPA's Role in Addressing Cybersecurity Risk: How the Auditing Profession Promotes Cybersecurity Resilience. Washington, DC: CAQ-AICPA.
- CERT Division (2017). CSIRT Frequently Asked Questions. Pittsburgh, PA: Carnegie Mellon University. Recuperado de <https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm>
- Deloitte University Press (2016). Deloitte-NASCIO Cybersecurity Study- State governments at risk: Turning strategy and awareness into progress. Deloitte Development LLC. Recuperado de: <https://www.nascio.org/Portals/o/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf>
- Díaz, O. & Muñoz, M. (2018). Implementación de un enfoque DevSecOps + Risk Management en un Centro de Datos de una organización Mexicana. *RISTI - Revista Ibérica de Tecnología y Sistemas de la Información*. (26) 43–53. Doi: 10.17013/risti.26.
- Donaldson, S., Siegel, S., Williams, C., & Aslam, C. (2015). *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats* (pp 201-204). New York, USA.: Apress.
- Edgar, T., & Manz, D. (2017). *Research Methods for Cyber Security* (pp 143-144). Cambridge: Elsevier.
- Financial Executives International (2014). Financial Executives, Cyber Security & Business Continuity. Toronto, Ontario: Canadian Executives Research Foundation. Recuperado de: <https://www.feicanada.org/enews/file/CFERF%20studies/2013-2014/IBM%20Cyber%20Security%20final3%202014.pdf>
- Financial Industry Regulatory Authority (2015). Report on Cybersecurity Practices: February (pp 1- 46). Recuperado de: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_o.pdf
- Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index. Arlington: Potomac Institute for Policy Studies. Recuperado de: <http://www.potomacinstitute.org/images/CRIndex2.0.pdf>

- Hiscox (2017). Hiscox Cyber Readiness Report. London: Forrester Consulting. Recuperado de: <https://www.hiscox.com/documents/brokers/cyber-readiness-report.pdf>
- ISACA (2014). Implementing the NIST Cybersecurity Framework. Rolling Meadows: ISACA.
- ISACA (2016). IS Audit/Assurance Program – Cybersecurity: Based on the NIST Cybersecurity Framework. Rolling Meadows: ISACA.
- Kaspersky Lab (2015). Top 10 Tips for Educating Employees about Cybersecurity. AO Kaspersky Lab. Recuperado de: http://go.kaspersky.com/rs/kaspersky1/images/Top_10_Tips_For_Educating_Employees_About_Cybersecurity_eBook.pdf
- Khan, M. (2016). Managing Data Protection and Cybersecurity-Audit's Role. *ISACA Journal*, 1(2016).
- Leidos (2017). Core Security Framework Assessment. Recuperado de: <https://cyber.leidos.com/services/core-security-framework-assessment>
- Leidos (2017). Cyber Defense Maturity Scorecard: Defining Cybersecurity Maturity Across Key Domains. Recuperado de: https://www.leidos.com/sites/g/files/zoouby166/files/2018-08/CDMEScorecard_Digital.pdf
- Messier, R. (2016). *Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems*. New York: Apress. ISBN 978-1-4842-1856-3.
- Meszaros, J., & Buchalcevoa, A. (2016). Introducing OSSF: A framework for online service cybersecurity risk management. *Computers & Security*. (65). 300–313.
- Ministry of Economic Affairs and Communication (2017). 2014-2017 Estonia Cybersecurity Strategy. Iráklío, Greece : ENISA. Recuperado de https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf
- National Association of State Chief Information Officers (NASCIO), Grant Thornton & CompTIA (2017). The 2017 State CIO Survey. Recuperado de: <https://www.comptia.org/communities/resources/2017-state-cio-survey>
- National Cyber Security Alliance (2017). Stay Safe Online. NCS. Recuperado de: <https://staysafeonline.org/ncsam/>
- National Institute of Standards and Technology (2017). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1, January.
- National Institute of Standards and Technology (2017). NIST Special Publications SP. Recuperado de: <http://csrc.nist.gov/publications/PubsSPs.html>
- North Atlantic Treaty Organization. Cooperative Cyber Defence Centre of Excellence (2015). Cyber Security Strategy Documents. August. Recuperado de: <https://ccdcoe.org/strategies-policies.html>

- North American Electric Reliability Corporation (2010). Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets. NERC. Recuperado de: www.nerc.com/docs/cip/sgwg/Critical_Cyber_Asset_ID_V1_Final.pdf
- Organisation for Economic Co-Operation and Development (2012). Cybersecurity Policy Making at a Turning Point. OECD. Recuperado de: <http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf>
- Payment Card Industry. Security Standards Council (2014). Best Practices for implementing a Security Awareness Program. PCI DSS, October. Recuperado de: https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf
- Pricewaterhouse Coopers (2016). PwC's Board Cybersecurity Governance Framework. PwC. Recuperado de: <https://www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf>
- Protiviti (2017). A Global Look at IT Audit Best Practices: Assessing the International Leaders in an Annual ISACA/Protiviti Survey. Protiviti Inc.
- Protiviti (2017). Board Perspectives: Risk Oversight. Protiviti Inc. Recuperado de <https://www.protiviti.com/US-en/taxonomy/term/3566>
- Ross, S. (2015). Cybersecurity for a "Simple" Auditor. *ISACA Journal*. 6(2018).
- Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits. *Enfoque UTE*, 9(1), 127 - 137. doi: <https://doi.org/10.29019/enfoqueute.v9n1.214>
- Sabillon, R., Serra, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). In: *Proceedings of the 2nd International Conference on Information Systems and Computer Science (INCISCOS)*. IEEE Xplore Digital Library, 253-259. doi: <https://doi.org/10.1109/INCISCOS.2017.20>
- Sabillon, R., Serra, J., Cavaller, V., & Cano, J. (2018). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRaining Model (CATRAM). In: *Proceedings of the 1st International Conference on Information Systems and Management Science (ISMS)*. University of Malta, Misida, Malta.
- SANS Institute (2017). SANS Forensics Whitepapers. SANS Institute. Recuperado de <https://digital-forensics.sans.org/community/whitepapers>
- United States Computer Emergency Readiness Team (2017). Cybersecurity Framework. US-CERT. Recuperado de <https://www.us-cert.gov/ccubedvp/cybersecurity-framework>
- U.S. Department of Homeland Security (2016). Cybersecurity. September. Recuperado de <https://www.dhs.gov/topic/cybersecurity>

- Yin, R.K. (2009). *Case Study Research: Design and Methods*. 4th ed. Los Angeles, CA: Sage Publications.
- Yin, R.K. (2014). *Case Study Research: Design and Methods*. 5th ed. Thousand Oaks, CA: Sage Publications.
- Yin, R.K. (2018). *Case Study Research and Applications*. 6th ed. Thousand Oaks, CA: Sage Publications.

Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada

Ignacio Gallardo^{1,2}, Patricia Bazan², Paula Venosa²

igallardo@est.iue.edu.ar, pbaz@info.unlp.edu.ar, pvenosa@info.unlp.edu.ar

¹ Universidad de la Defensa Nacional - Facultad de Ingeniería, Palermo, CABA, Argentina.

² Universidad Nacional de la Plata - Facultad de Informática - Laboratorio de Investigación de Nuevas Tecnologías Informáticas, La Plata, Argentina.

DOI: 10.17013/risti.32.49-66

Resumen: Los principales esfuerzos de los últimos años se han concentrado en el problema de asignar de forma segura nombres a claves públicas, de hecho, la comunidad científica adoptó progresivamente el uso de sistemas basados en Public Key Infrastructure (PKI) con el fin de proporcionar servicios de seguridad a los sistemas, los cuales dependen de la existencia de una arquitectura centralizada y jerárquica. Esta misma problemática se traspola a la gestión del comercio electrónico, donde en el modelo inicial se requería de una entidad central que debía emitir divisa electrónica a los diferentes usuarios, no obstante, en 2009, Satoshi Nakamoto crea Bitcoin: una criptomoneda con tecnología peer-to-peer para operar sin una autoridad central o bancos. En esta investigación se aplica en PKI lo mismo que logró Nakamoto en el comercio electrónico, una reingeniería, migrando una arquitectura centralizada y jerárquica a una completamente descentralizada por medio de su innovación tecnológica llamada Blockchain.

Palabras-clave: PKI; certificados digitales; blockchain; bitcoin, ciberseguridad.

Architecture of Certificates: form a hierarchical architecture and centralized to a distributed and decentralized

Abstract: The main efforts of recent years have focused on the problem of set a name securely to public keys, in fact, the scientific community has been gradually adopting the use of systems based in Public Key Infrastructure (PKI) in order to provide security services. However, that systems depend on the existence of a centralized and hierarchical method. This same problem is translated into the management of electronic commerce, which presents a central entity that must issue electronic currency to different users. In 2009, Satoshi Nakamoto creates Bitcoin: a peer-to-peer technology to operate without a central authority or banks. This investigation applies in PKI the same concepts that Nakamoto applied in the electronic commerce, a reengineering and a paradigm shift, a migration from a

centralized and hierarchical architecture to a decentralized and not hierarchical through the innovative technology called Blockchain.

Keywords: PKI; digital certificates; blockchain; bitcoin; cybersecurity.

1. Introducción

Una forma de entender qué es una **blockchain** (Bahga, A., & Madiseti, V., 2017) es antes comprender qué es una **criptomoneda** con sus diferencias respecto del dinero electrónico, y para comprender fácilmente estos conceptos, primero hay que definir qué es una moneda fiduciaria (Adams, M., 2016).

Moneda fiduciaria es toda moneda de curso legal designada y emitida por una **autoridad central** que las personas están dispuestas a aceptar a cambio de productos o servicios porque está respaldada por la regulación vigente y por la **confianza** en dicha autoridad central.

El dinero fiduciario es similar al dinero respaldado por los productos básicos en apariencia y uso, pero no puede ser canjeado por uno de esos productos, como por ejemplo la plata y/o el oro.

Por el contrario, una **moneda virtual** es un tipo de **dinero digital** no regulado que emiten y controlan sus creadores, y que se utilizan y aceptan entre miembros de la comunidad virtual (Capoti, D., Colacchi, E., & Maggioni, M., 2015).

La criptodivisa **Bitcoin** (Capoti, D., Colacchi, E., & Maggioni, M. 2015) surgió en el año 2009 como una alternativa a la moneda fiduciaria, con la diferencia que éstos no se emiten como este último, sino que se “extraen” mediante un procedimiento denominado “minería de bitcoins” utilizando la capacidad de una inmensa red de cómputo conectada y distribuida a través de todo el mundo. Esta tecnología surge con el objetivo de **descentralizar** los pagos entre usuarios, eliminando la necesidad de la **presencia de instituciones** financieras en las transacciones. Para llevar a cabo estos requerimientos, bitcoin se despliega en una **red P2P** (Peer to Peer) (Steinmetz, R., Wehrle, K., 2005). por la cual se mantienen, distribuyen y coexisten todas las transacciones asegurando la **no alteración** de las mismas sin tener que realizar operaciones demasiadas exigentes desde el punto de vista computacional para converger todo el sistema (Nakamoto, S., 2009).

Esencialmente, no solo Bitcoin sino las demás criptomonedas como Ethereum, Litecoin, Ripple, etc. son nada más ni menos que un archivo digital donde se enumeran todas las transacciones de la red al mejor estilo “libro de contabilidad”, con la peculiaridad que este mismo, se encuentra presente en todos los participantes del juego y no puede ser alterado.

Aparte del formato digital, son mínimas las similitudes entre el dinero electrónico y las criptomonedas. El dinero electrónico, como muchos otros formatos digitales de la moneda fiduciaria —como las tarjetas de crédito y débito, PayPal y las transferencias electrónicas—, es simplemente un mecanismo mediante el cual se interactúa con esa moneda fiduciaria. Para mitigar riesgos sistémicos y de protección del consumidor, el efectivo que respalda el dinero electrónico emitido habitualmente se deposita en

instituciones financieras que siguen todas las regulaciones prudenciales. A diferencia de la moneda criptográfica, el dinero electrónico no es una moneda individual y está supervisado por la misma autoridad central que controla la moneda nacional que lo respalda.

Este sistema inicialmente aplicado a las criptomonedas es el primer ejemplo de una creciente revolución teleinformática, potencialmente aplicable a infinitas áreas de conocimiento, en la que mediante software de código abierto se resuelven **sincronizadamente** cálculos matemáticos para **validar todas las operaciones** realizadas por cada individuo perteneciente a la red sin necesidad de ser comandados y regulados por un **ente central**, y no obstante, **manteniendo la integridad, máxima disponibilidad** del historial de las transacciones, y **desconcentrando** no solo la confianza en esta única autoridad central, sino también la información y los procesos, lo cual proporciona una ventaja a la hora de la existencia de una violación a la seguridad.

De todo este procedimiento descrito surge el término **cadena de bloques** o **blockchain** —mecanismo utilizado por Bitcoin— ya que todas las operaciones de la red se acumulan en bloques de transacciones y estos mismos se van adjuntando entre sí formando una cadena y aplicando los conceptos de un árbol de **Merkle**, no obstante, existe una réplica irrevocable de este árbol —archivo digital— en todos los integrantes del sistema mantenido a la orden del día (Nakamoto, S., 2009).

Resulta llamativo pensar que una tecnología implementada hace menos de nueve años y desarrollada por una persona desconocida podría pasar a ser más eficiente, confiable y popular que ya varias décadas de la vigencia del dinero electrónico, pero la realidad es que toda su arquitectura y diseño contempla hasta el último detalle a la hora de pensar en confiabilidad, robustez y seguridad.

El objetivo general de este trabajo consiste en analizar y seleccionar los conceptos de descentralización, distribución, validación masiva y comunitaria, sincronismo, integridad, transparencia, escalabilidad, redundancia y confiabilidad presentes en **blockchain** o **cadena de bloques**, para poder extraerlos y aplicarlos en una propuesta de rediseño y mejora a otro ámbito que ya lleva bastante tiempo de estudio desde el punto de vista no solo de la seguridad sino también de la ingeniería de software llamado: Arquitectura de **Certificados Digitales** o **Infraestructura de clave pública** (Vimercati, S. D., & Mitchell, C., 2013). Estas ventajas serán aprovechadas volcando de forma teórica en la modificación del diseño y arquitectura existente en los **certificados digitales** (Thomas, S. A., 2000).

Este trabajo integra conocimientos avanzados de Seguridad en Teleinformática, Criptografía, **Criptodivisas**, Arquitectura de **certificados digitales**, Arquitectura de sistemas distribuidos, **Blockchain** (Gallardo, I., 2018).

2. Motivación y Estado del Arte

Las redes P2P (Steinmetz, R.; Wehrle, K., 2005.) presentan características que las convierten en un activo para el que es difícil encontrar comparación en el mundo real. En primer lugar, porque las conforman sistemas distribuidos y vivos que no presentan un único punto de fallo y que toleran la desconexión de algunos de ellos de forma flexible

y sin dejar que el funcionamiento de la red en su conjunto se vea comprometida. Se trata de organismos cuya robustez radica precisamente en el número de nodos que las componen y en cómo estos están conectados unos a otros.

Con esto, se puede afirmar que la aparición de los métodos de pago modernos que exploten la potencia de estas tecnologías es el fruto de la evolución natural del marco tecnológico reciente.

La materialización de las criptomonedas como fenómeno contemporáneo tiene un trasfondo ideológico muy ligado a conceptos que forman parte de la cultura *hacker* tradicional: evitar la hasta ahora necesaria presencia de un organismo central de control financiero que es considerado como poco democrático y potencialmente corrompible. Aunque las implicaciones de una economía desregulada y el reparto de divisas son materias controvertidas que se han afrontado desde cada comunidad con puntos de vistas diferentes, la consecución de estos objetivos requiere, desde un punto de vista técnico, la colaboración de distintas entidades que asuman aunadas ese rol de organismo central multifacético. Si a su naturaleza descentralizada (Shane, P. M., & Hunker, J. A., 2013) se le suma que los nodos que forman parte de la red no tienen por qué ser conocidos entre sí y que, aun así, tienen que ser capaces de seguir funcionando de forma consensuada incluso en un escenario en el que hay que dar por supuesta la presencia de agentes no confiables, permite toparse con un escenario real del conocido *problema de los generales bizantinos de tolerancia a fallos* (Byzantine Fault Tolerance o BFT).

El libro mayor de contabilidad distribuido **blockchain** (basado en una arquitectura de comunicaciones P2P) (Steinmetz, R.; Wehrle, K., 2005), fue creado, para registrar, organizar y sostener la más importante criptomoneda, el Bitcoin, pero eso no quiere decir que esta tecnología pueda utilizarse sólo para ello. De hecho, ahora es cuando la **blockchain** tiene casi ilimitadas puertas por abrir: si ella es capaz de registrar digitalmente, de forma segura y pública a la vez, todo el ciclo de vida de cada bitcoin; en teoría, también puede registrar todo el ciclo de vida de cualquier otra cosa (desde facturas de hospital, hasta diamantes).

En contraste a esto, y polarizando los mismos conceptos, la idea de descartar la estructura jerárquica en la que se basa hoy en día la infraestructura PKI (Nash, A., 2002), logra no sólo una total transparencia en la emisión de certificados sino también se disipa el riesgo y aumenta la confiabilidad, ya que no existe una entidad central de gestión. Por otro lado, la arquitectura **propuesta** proporcionará a los usuarios eficiencia total en el proceso de gestión de certificados, ya que ahorrará tiempo (eliminando las cuestiones burocráticas de papelerías), tediosas configuraciones y dinero (Gallardo, I., 2018).

2.1. Propuestas Similares

Existen varias propuestas de investigación y desarrollo o implementaciones que abordan problemáticas similares a la de promover una reingeniería y rediseño de la infraestructura de clave pública actual. Entre estas, algunas abordan extendiendo funcionalidades, otra reemplazando la arquitectura actual y desde distintos puntos de vista, por ejemplo:

- Certificate Transparency Using Blockchain: Es una propuesta realizada por estudiantes de la Universidad de Ashoka que pretende implementar una PKI distribuida utilizando una plataforma de IBM para interactuar con una

blockchain de negocios open source (Jhanwar, M. P., Chattopadhyay, A., Madala, D. S. V., 2018).

- BlockPGP, a Blockchain-based Framework for PGP Key Servers: Es un proyecto presentado por la Universidad de Luxemburgo, en donde se pretende reemplazar los servidores de claves PGP por un repositorio de claves PGP distribuidas sobre blockchain, en particular, la cadena de bloques de Ethereum (Yakubov, A., Shbair, W. M., State, R., 2018).
- CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections: Es una solución de auditoría de gestión de certificados digitales de la PKI sobre blockchain presentado en un congreso en Honolulu, HI, USA (Chen, J., Yao, S., Yuan, Q., He, K, Ji, S., Du, R., 2018).
- Decentralized Public Key Infrastructure for Internet-of-Things: Es la solución que estratégicamente se parece más a la presentada en este trabajo de investigación, pero con la diferencia de que se aplica para dispositivos IoT y presenta un proceso diferente de validación de identidades. Este trabajo fué presentado en Washington, USA (Won, J., Singla, A., Bertino, E., Bollella, G., 2018).
- PTAS, Privacy-preserving Thin-client Authentication Scheme in Blockchain-based PKI: Es una implementación presentada por investigadores Chinos, que aborda un proceso de autenticación innovador vía blockchain para seguridad en dispositivos de IoT (Jiang, W., Li, H., Xu et al, G., 2019).
- BlockPKI, an Automated, Resilient, and Transparent Public-Key Infrastructure: En este trabajo, investigadores singapurenses agregan a la PKI un tercero de confianza, el cual, este último se materializa en una blockchain (Dykcik, L., Chuat, L., Szalachowski, P., Perring, A., 2018).

Como se puede ver en la breve descripción de cada solución propuesta, al igual que la presentada en este trabajo, todas abordan la problemática que existe a la hora de confiar en un ente central y jerárquico, no obstante, presentan implementaciones montadas sobre blockchain con el fin de disipar este potencial riesgo de seguridad, descansando en una arquitectura descentralizada y no jerárquica. Como se pueden apreciar en las diferentes publicaciones, esta problemática es tan amplia que es abordada por investigadores de diferentes partes del mundo.

Lo que sí debe quedar claro es que la diferencia principal y totalmente innovadora que presenta este trabajo presentado por investigadores argentinos, llamado “Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada” es que se realiza una reingeniería y rediseño, migrando totalmente la PKI a una arquitectura de certificados digitales sobre blockchain, presentando nuevos procedimientos e innovadores en cada etapa existente en la infraestructura de clave pública, aplicado específicamente para servicios HTTPs y finalmente soportando la integración con la arquitectura actual PKI.

3. Metodología

Se realizó un estudio en profundidad de la tecnología **blockchain** evaluando sus fortalezas y debilidades para luego realizar una propuesta utilizando su esencia y procedimientos de aseguramiento y confiabilidad en las transacciones para aplicar

en el campo de la emisión, validación y manejo de **certificados digitales** de clave pública/privada. **Blockchain**, entre unas de sus funcionalidades, logra validar de forma distribuida y así determinar del lado del receptor si el emisor de la transacción es quien dice ser. Con la aplicación de esta característica sumada a otros procedimientos implementados en otras tecnologías como ser: Criptografía Contemporánea (Blake, I. F., Seroussi, G., & Smart, N. P., 1999), Arquitecturas Distribuidas (Zhao, W., 2014), **Certificados Digitales** (Leuf, B., 2002) y Conceptos de Seguridad Informática (Vacca, J. R., & Vacca, J. R., 2013), se logró eliminar las jerarquías de autoridades certificadoras, descentralizando la arquitectura. Para que dicha propuesta haya funcionado se debió cumplir tres características importantes. La primera y como se mencionó antes, debió ser descentralizada -al no existir un ente centralizador para emitir **certificados digitales**, esta actividad será realizada de forma repartida entre los participantes de la red-. También debió ser distribuida, ya que cada nodo funcionará como cliente/servidor y teniendo una copia de la base de datos de todo el sistema. Por último, el sistema fué totalmente auditable por cualquier nodo para así poder determinar anomalías en la red.

Para enriquecer el estudio exclusivo de esta tecnología, se abordó un análisis cualitativo de la arquitectura de gestión de certificados digitales vigente a fin de detectar y exponer las debilidades. En base a ello se elaboró una propuesta de rediseño de la arquitectura para así cubrir dicha endeblez. Finalmente se implementó un prototipo que permitió validar dicha propuesta (Gallardo, I., 2018).

4. Desarrollo Experimental

Para validar la propuesta y probar los flujos propuestos en su funcionamiento se desarrolló un componente de software que está compuesto por cuatro módulos e interactúa con otros dos. El componente fue desarrollado en Java (Lafosse, J., 2009) y Typescript (Pardi, P., 2015).

El módulo de software número uno (denominado **PkChain**) se encarga de la columna vertebral de esta propuesta, es decir, realiza una simulación del funcionamiento de **blockchain** que permitirá utilizar su "API" (Masse', M., 2012) para luego incorporar las siguientes funcionalidades.

El segundo módulo emula a la arquitectura de comunicación peer-to-peer (denominado **Gestor de Servicios**) para así poder tener este tipo de conectividad entre los diferentes nodos **blockchain** como propone el protocolo de Bitcoin.

El tercer componente de software agrega a la **cadena de bloques** la inteligencia propuesta en este trabajo. Esta inteligencia tiene el rol de un plugin/librería para la **PkChain**, y se denominará **LibCerts**.

El cuarto módulo es un **Cliente PkChain**, que básicamente consume la red **blockchain** como un nodo de la red.

Finalmente, para lograr la prueba de todo el procedimiento de verificación, validación, emisión y revocación de certificados se crea un **Cliente Web** que realiza consultas a un **Servidor Web** que también se lo implementó (Gallardo, I., 2018).

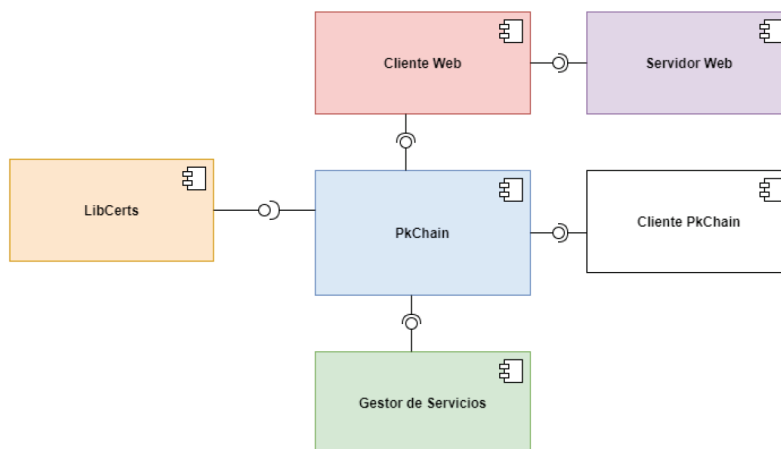


Figura 1 – Diagrama de Componentes de la Propuesta

4.1. Procesos y Operaciones de la Arquitectura Propuesta

Las operaciones y procesos que la arquitectura contempla son: gestión de claves, emisión, distribución, revocación, renovación y validación (Nash, A., 2002).

4.1.1. Proceso de Gestión de Claves

Este proceso queda tal cual funciona en la arquitectura PKI vigente, ya que bajo cuestiones de gestión/generación de claves la solución se encuentra compatible e interoperable a la actual, y desde el punto de vista técnico no se detectaron contramedidas en esta etapa, no obstante, se decidió no modificar el mismo.

4.1.2. Proceso de Emisión de Certificados

Al igual que la arquitectura PKI vigente, este proceso se encarga de aceptar la petición de emisión de certificados digitales de los diferentes usuarios.

En consiguiente, una vez generado el par de claves, el portador de las mismas expone la clave pública en formato Base58 Check en el servidor web, en la dirección “URL-RAÍZ/emit/pk”, por ejemplo: “www.prueba-clave-publica.com/emit/pk”. Es decir, si un usuario realiza una petición web GET de ese recurso, obtendría la clave pública expuesta anteriormente en formato Base58 Check.

Ya generado esto, se crea una **transacción** de emisión de certificados que lleva dentro:

- Como **dirección**: el hash de la misma.
- La **clave pública** del servidor (clave pública a dar de alta).
- El **dominio** portador de la clave pública (URL-RAÍZ).
- La ruta donde buscarla (/emit/pk).

Luego se disemina esta transacción por la red *peer to peer* y el portador de la clave pública aguarda su confirmación.

Todos los nodos que reciban dicha transacción, verificarán su integridad y realizarán una petición web GET hacia el recurso expuesto en la misma. Ya recibida la respuesta de la petición, se compara el resultado con la clave pública del servidor contenida dentro de la transacción y en caso afirmativo se retransmite a los demás nodos y se encola para realizar el proceso de minado, en su defecto la misma se descarta.

Una vez minada y confirmada la transacción (al igual que en Bitcoin, para la confirmación se aconsejan 10 bloques por delante del bloque en donde se encuentra la transacción), el creador de la transacción debe generar un certificado x.509 autofirmado o firmado por una Autoridad Certificante propia, desconocida por los demás o incluso conocida. Este certificado contendrá los diferentes campos correspondientes al estándar y a la configuración que se desee, salvo la particularidad de que en el campo opcional **issuerUniqueID** se dejará asentado el identificador de la **transacción** confirmada. Ya a esta altura el usuario se encuentra en condiciones de agregarlo a la configuración HTTPS del servidor con su dominio en cuestión y/o firmar otros certificados digitales.

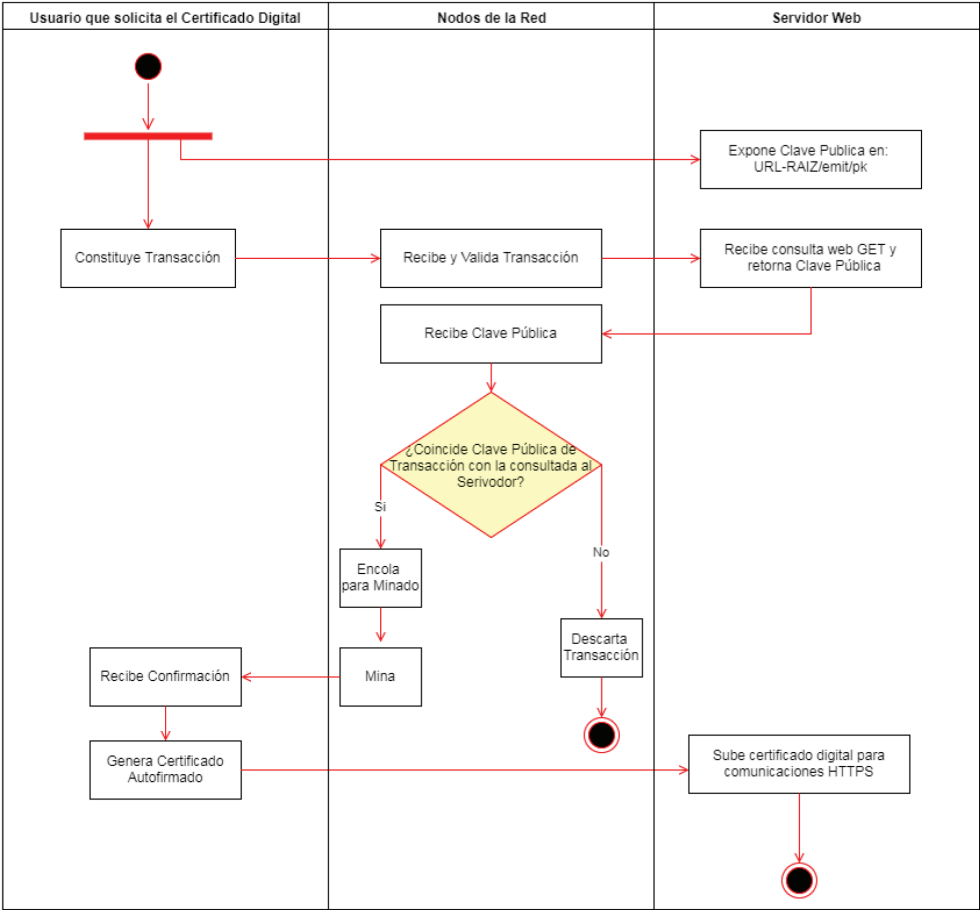


Figura 2 – Diagrama de Actividades del Proceso de Emisión

4.1.2. Proceso de Distribución de Certificados

El método utilizado para la distribución de los certificados es el basado **blockchain**, es decir, distribuido en la totalidad de los nodos en la red. Tanto para operaciones de verificación de firmas o de cifrado, el acceso a los certificados se lleva a cabo mediante consultas a la **cadena de bloques** donde las claves públicas emitidas, renovadas o revocadas se encuentran disponibles gracias a la convergencia y consenso de la red. Esta base de datos pública además proporciona información extra que resulta útil a la hora de realizar el proceso de validación, como ser, información del dominio en donde validar las mismas. Esto es debido a que (como visto en el proceso anterior) cada usuario que desea emitir, renovar o revocar un certificado digital debe agregar su clave pública a modo de recurso web, donde cada nodo de la red accede a la misma para poder validarla y converger en la emisión, renovación o revocación del mismo.

4.1.2. Proceso de Revocación de Certificados

Este proceso se lleva a cabo con el fin de dar de baja o declararlo como no confiable a un certificado digital, por consiguiente y al igual que el proceso de emisión, al momento de generar una revocación, el usuario deberá exponer la clave a revocar en el servidor web para que sea accesible por los nodos que la validan, luego generar una transacción y diseminarse por la red.

Dicho ésto, el usuario portador de la clave pública del servidor expone la misma en “URL-RAÍZ/revoke/pk” y genera una transacción con las siguientes características:

- Como **dirección**: el hash de la misma.
- La **clave pública** del servidor (clave pública a revocar).
- El **dominio** portador de la clave pública.
- La ruta donde buscarla (/revoke/pk).
- La **dirección** de la transacción de emisión o de renovación (transacción anterior).

Todos los nodos que reciban dicha transacción verificarán su integridad y realizarán una petición web GET hacia el recurso expuesto (por medio de la ruta proporcionada en la transacción de revocación o en la indicada en la transacción de emisión o renovación anterior). Ya recibida la respuesta de la petición, se compara el resultado con la clave pública del servidor contenida dentro de la **transacción de emisión o renovación** y en caso afirmativo se retransmite a los demás nodos y se encola para realizar el proceso de minado, en su defecto la misma se descarta.

Una vez minada y confirmada la transacción (al igual que en Bitcoin, para la confirmación se aconsejan 10 bloques por delante del bloque en donde se encuentra la transacción), el creador de la transacción ya da la clave por revocada.

4.1.3. Proceso de Renovación de Certificados

En esta etapa usuario portador de la clave pública del servidor debe exponer la **nueva** clave pública en “URL-RAÍZ/renovate/pk” y genera una transacción con las siguientes características:

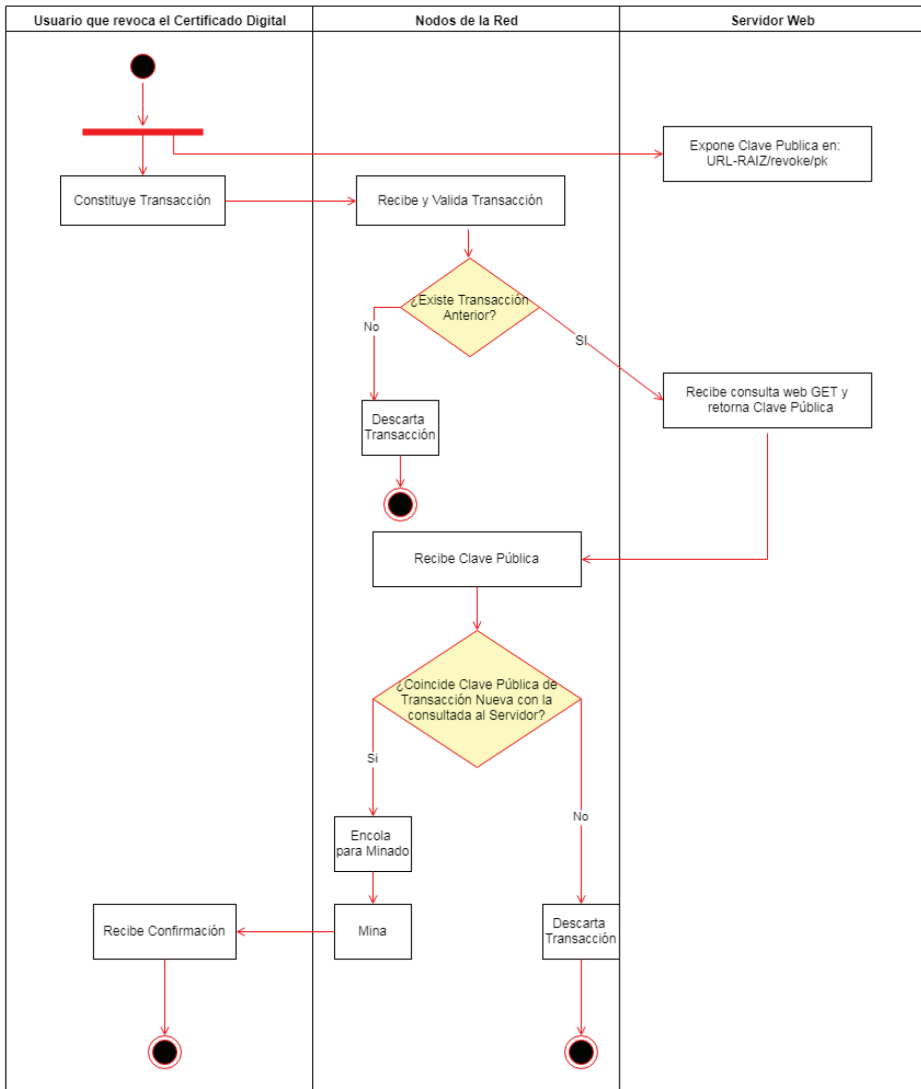


Figura 3 – Diagrama de Actividades del Proceso de Revocación

- Como **dirección**: el hash de la misma.
- Nueva **clave pública** del servidor.
- El **dominio** portador de la clave pública.
- La ruta donde buscarla (/renovate/pk).
- La **dirección** de la transacción de emisión o renovación (transacción anterior).

Todos los nodos que reciban dicha transacción verificarán su integridad y realizarán una petición web GET hacia el recurso expuesto (por medio de la ruta proporcionada en la transacción de revocación o en la indicada en la transacción de emisión o renovación

anterior). Ya recibida la respuesta de la petición, se compara el resultado con la clave pública del servidor contenida dentro de la **transacción** realizada recientemente y en caso afirmativo se retransmite a los demás nodos y se encola para realizar el proceso de minado, en su defecto la misma se descarta.

Una vez minada y confirmada la transacción (al igual que en Bitcoin, para la confirmación se aconsejan 10 bloques por delante del bloque en donde se encuentra la transacción), el creador de la transacción debe generar un certificado x.509. Este certificado al igual que en el proceso de emisión deberá rellenar en el campo opcional **issuerUniqueID** (Identificador único del emisor) con el identificador de la **transacción** confirmada. Ya a esta altura el usuario se encuentra en condiciones de agregarlo a la configuración HTTPS del servidor con su dominio en cuestión y/o firmar otros certificados digitales.

4.2. Transacciones.

Las transacciones al igual que en Bitcoin son estructuras de datos firmadas digitalmente, pero que en vez de cambiar el propietario de un bitcoin, realizan una acción de emisión, revocación o renovación de certificados digitales.

La estructura de datos es la siguiente (*Ilustración 13, Ilustración 14 e Ilustración 15*):

- **Transacción anterior:** registro que referencia a una transacción previa. Para transacciones de **emisión** este campo se lo fija en 0, ya que no posee transacciones anteriores, y para transacciones de **renovación** o **revocación** se referencia a la transacción anterior.
- **Dominio del servidor:** portador del certificado a emitir, renovar o revocar.
- **Clave pública del servidor:** que se quiere dar de alta, relacionada a ese dominio.
- **Dirección (path/url):** en donde encontrar la **clave pública del servidor** para cotejar con la contenida en la transacción. Para transacciones de emisión se completa el campo “emit”, para renovación el “renovate” y para revocación el “revoke”.
- **Hash de transacción (identificador):** resumen de toda la estructura de datos.
- **Firma digital del emisor:** encriptación del **hash de la transacción** con la clave privada del nodo emisor.

Por ejemplo, si **A** desea **emitir** un certificado digital para el dominio “www.prueba-pkchain.com”, entonces se genera el par de claves para su servidor, expone la clave pública en “www.prueba-pkchain.com/emit/pk”, y genera la transacción con los siguientes campos:

- **server domain:** “www.prueba-pkchain.com”
- **emit:** “/emit/pk”
- **revoke:** “” (Vacío, ya que es una transacción de emisión)
- **renovate:** “” (Vacío, ya que es una transacción de emisión)
- **server public key:** “clave pública perteneciente al par de clave generado”
- **previous transaction:** “” (Vacío, ya una transacción de emisión no posee transacción anterior).

Si **A** desea **renovar** esta emisión, deberá generar el nuevo par de claves, publicar la nueva clave en la dirección de “renovate” declarada en esta nueva transacción. La transacción contendrá los siguientes campos:

- **server domain:** “www.prueba-pkchain.com”
- **emit:** “” (Vacío, ya que es una transacción de renovación)
- **revoke:** “”(Vacío, ya que es una transacción de renovación)
- **renovate:** “/renovate/pk”
- **server public key:** “clave pública perteneciente al nuevo par de clave generado”.
- **previous transaction:** Identificador de transacción anterior.

```
{
  "id": "f1b7fed773accafad5088eb4c3957cb050912535a4ce2ed81b0781ea69ba4669",
  "libCert": {
    "serverDomain": "http://www.prueba-pkchain.com",
    "emit": "/emit/pk",
    "revoke": "",
    "renovate": "",
    "serverPublicKey": "04d50ce5ff067e2dbb28f197ff05ab3a4d363227f169da5dd821d821...",
    "previousTx": ""
  }
}
```

Figura 2 – Transacción de Emisión en formato JSON

```
{
  "id": "abc1345fdf2e75064b1559e5520a51f896c7f28c8576d68205e326a8d3dee873",
  "libCert": {
    "serverDomain": "http://www.prueba-pkchain.com",
    "emit": "",
    "revoke": "",
    "renovate": "/renovate/pk",
    "serverPublicKey": "04fe71e62fc22b20e3473a90b3d1005d49f9d0c0aab69cfb7dd99122...",
    "previousTx": "f1b7fed773accafad5088eb4c3957cb050912535a4ce2ed81b0781ea69ba4669"
  }
}
```

Figura 3 – Transacción de Renovación en formato JSON.

Por último, si **A** desea **revocar** un certificado, deberá publicar la clave a revocar en la dirección de “revoke” declarada en la transacción nueva. La estructura de datos contendrá los siguientes campos:

- **server domain:** “www.prueba-pkchain.com”
- **emit:** “” (Vacío, ya que es una transacción de revocación)
- **revoke:** “/revoke/pk”
- **renovate:** “” (Vacío, ya que es una transacción de revocación)
- **server public key:** clave pública que se quiere revocar.
- **previous transaction:** Identificador de transacción anterior.

Cada transacción excepto las de “emisión”, poseen referencias o “punteros” a anteriores que se encuentran reconocidas por toda la red y almacenada en la base de datos distribuida, no obstante, se encuentran disponibles para que todos los nodos puedan consultarlas.

```
{
  "id": "zf11345fdf2e75064b1559e5520a51f896c7f28c8576d68205e326a8d3deeds3",
  "libCert": {
    "serverDomain": "http://www.prueba-pkchain.com",
    "emit": "",
    "revoke": "/revoke/pk",
    "renovate": "",
    "serverPublicKey": "04fe71e62fc22b20e3473a90b3d1005d49f9d0c0aab69cfb7dd99122...",
    "previousTx": "abc1345fdf2e75064b1559e5520a51f896c7f28c8576d68205e326a8d3dee873"
  }
}
```

Figura 4 – Transacción de Revocación en formato JSON.

4.3. Construcción del Camino a la Certificación.

Si un **cliente pkchain** se conecta a un servidor web, este último retorna el certificado digital. El cliente, accede al campo “*issuerUniqueID*” y con el identificador de transacción contenido dentro busca en toda la blockchain hacia atrás. Si este no se encuentra como entrada de una transacción de revocación, la transacción existe contenida dentro de un bloque de la *blockchain*, y la información contenida dentro de la transacción coincide con la del certificado digital enviado por el servidor (dominio y clave pública), entonces se da luz verde y el mismo se acepta, de lo contrario se lo rechaza.

4.4. Consideraciones Generales.

Desde el punto de vista de la convergencia de la red a nivel blockchain, se intentó emular el proceso idéntico al implementado en Bitcoin, es decir, en cuestiones de minería, pruebas de trabajo, estructura de datos de bloques, tiempos entre bloques, criptografía utilizada y ajustes de dificultad se realizó una copia de la lógica vigente de la *blockchain* de Bitcoin.

5. Trabajos Futuros

Blockchain pone sobre la mesa la posibilidad de realizar transacciones entre entidades (personas u organizaciones) de manera distribuida, segura y sin necesidad de intermediarios, donde las reglas del juego están definidas por medio de algoritmos computacionales.

Llegar a tener una sociedad más distribuida y autónoma en cuanto a su estructura, sus redes y transacciones es algo que podría venir de la mano de esta tecnología y que podría cambiar la forma en que muchas cosas están pensadas hoy.

De la misma manera que **internet** cambió para siempre los modelos de negocio de miles de industrias y empresas, la **blockchain** o **cadena de bloques** está dando lugar

a una nueva revolución, proponiendo nuevas formas de optimizar las relaciones entre usuarios, ahorrar costes administrativos, favorecer cooperaciones y comprender todas las posibilidades imaginables que ofrecía el internet de la información en una segunda ola tecnológica de cambio.

Blockchain es la verdadera innovación que hizo posible la existencia de **Bitcoin** (su primer uso de esa tecnología) y eso le permitió ser, hasta el día de hoy, la más popular de todas, al punto de ser más popular en el consciente colectivo que **Blockchain** en sí, no obstante, lo más importante que se extrae de esta gran solución es la posibilidad de utilizar la **cadena de bloques** en otros ámbitos, como por ejemplo, su incorporación en la propuesta abordada en esta investigación.

En este trabajo se abordó una propuesta de reingeniería y migración de la arquitectura de certificados digitales vigente a una montada sobre **blockchain**, sería interesante analizar una propuesta de implementación que se monte sobre su alternativa: **hashgraph**.

En esta propuesta se ha desarrollado un prototipo a modo de validar el modelo, no obstante, la implementación real junto con la apertura de un proyecto **open source** para que la comunidad pueda realizar sus aportes invocando a la inteligencia colectiva, es el principal trabajo que queda pendiente por realizar.

Esta arquitectura de certificados digitales distribuida y descentralizada tiene un enfoque orientado a arquitecturas web, por lo tanto, realizar un análisis de viabilidad de implementación en diferentes ámbitos como ser firma digital de expedientes o en voto electrónico sería de gran interés.

Sería muy interesante poder también lograr la interoperabilidad entre la propuesta de esta investigación y la lógica de negocios de **Bitcoin**, de modo de integrar las dos soluciones para que puedan convivir al mismo tiempo en la misma **cadena de bloques**. Para lograr esto, en vez de quitar la lógica de negocios de **Bitcoin** (como se planteó en este trabajo), se deberá realizar una modificación en la misma para agregar la lógica de negocios de esta propuesta.

Por último, visto y considerando que la solución planteada en esta investigación descansa sobre **blockchain**, también acarrea sus mismas debilidades, no obstante, es motivo de trabajo a futuro contemplar mejoras en este sentido.

6. Conclusiones

Dada la gran frecuencia en la que surgen proyectos montados sobre **blockchain**, y no solo eso, sino la cantidad de criptomonedas vigentes y por aparecer que están revolucionando la economía mundial, es necesario conocer los fundamentos que se hacen del núcleo de esta área de conocimiento de forma tal de dominar la tecnología, conocer sus posibles vulnerabilidades, y mejoras.

Ha habido gran cantidad de propuestas para lograr una formalización de la ingeniería en seguridad de **Blockchain**, pero la mayoría tienen un alcance limitado. Resulta totalmente relevante incursionar en el tema ya que hasta el momento no se ha podido

probar de manera exhaustiva si la arquitectura de **Blockchain** sea totalmente segura o no, o más aún, si es tan útil como se dice o no.

Dentro de la filosofía **Blockchain** existen muy pocas obras que realicen una utilización en serio de sus funcionalidades, y de las pocas que existen, la mayor parte la aborda con un enfoque indiscreto e irreal sobre cómo descentralizar en dos pasos al mundo.

Cabe destacar que en la actualidad casi no existe bibliografía seria y en español que aborde y exponga una detallada descripción de los procesos internos, arquitecturas y operaciones tanto de **Bitcoin** como de **Blockchain**. La escasa bibliografía existente brinda diferentes análisis y proyecciones genéricas más inclinadas a puntos de vistas de las ciencias económicas que técnicas de la ingeniería.

En este trabajo se puede apreciar una detallada descripción en español de todos los conocimientos que se encuentran detrás de este telón, comenzando por los fundamentos básicos, hasta entrando en las entrañas matemáticas que dirigen la orquesta. No obstante, se hace mención a una necesidad contemporánea muy importante, básica y colectiva, que obliga a enfocarse hacia un cambio de paradigma en la arquitectura de certificados digitales vigente. En consiguiente, se presenta una propuesta que integra conocimientos y funcionalidades provenientes de tecnologías de punta como es la implementación de diferentes sistemas sobre **Blockchain**.

Para ir finalizando, como conclusión no solo personal, sino de la comunidad informática en general, es que el aporte más grande que ha dado Satoshi Nakamoto (Nakamoto, S., 2009) con su publicación en 2009 no fue **Bitcoin**, sino su columna vertebral, es decir, **Blockchain**. Una tecnología que tiene características ilimitadas tanto desde el punto de vista técnico como económico, que permite abordar investigaciones, realizar propuestas innovadoras y simples implementaciones como la presentada en esta investigación.

Por último, este rediseño de la arquitectura plasmado en este trabajo de investigación fue llevado a cabo y probado experimentalmente, en donde para mayor detalle de esta propuesta de reingeniería e implementación se dejan referencias de la tesis¹ que extiende en detalle todos estos conceptos junto al repositorio² correspondiente.

Referencias

- Adams, M. (2016). *Blockchain: The history, mechanics, technical implementation and powerful uses of blockchain technology*. CreateSpace Independent Publishing Platform.
- Allison, I. (2010). *Organizational factors shaping software process improvement in small-medium sized software teams: A multi-case analysis*. In *Proceedings - 7th International Conference on the Quality of Information and Communications Technology, QUATIC 2010* (pp. 418–423). Porto, Portugal: IEEE. <https://doi.org/10.1109/QUATIC.2010.81>

¹ Tesis de maestría: <http://sedici.unlp.edu.ar/handle/10915/72076>

² Repositorio del código de la Tesis de maestría: <https://gitlab.com/ignaciomgu/pkchain>

- Antonopoulos, A. M. (2018). *Mastering bitcoin: Programming the open blockchain*. Sebastopol, CA: O'Reilly media.
- Bahga, A., & Madiseti, V. (2017). *Blockchain applications a hands-on approach*. Vpt.
- Blake, I. F., Seroussi, G., & Smart, N. P. (1999). *Elliptic curves in cryptography*. Cambridge : Cambridge University Press.
- Capoti, D., Colacchi, E., & Maggioni, M. (2015). *Bitcoin revolution: La moneta digitale alla conquista del mondo*. Milano: U. Hoepli.
- Chen, J., Yao, S., Yuan, Q., He, K, Ji, S., Du, R. (2018). CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections. In Proceedings of the IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, (pp. 2060-2068). Honolulu, HI, USA. Doi: 10.1109/INFOCOM.2018.8486344.
- Diffie, W.; & Hellman, M. (1976). "New directions in cryptography". *IEEE Transactions on Information Theory*. 22 (6): 644–654. Doi: 10.1.1.37.9720. doi:10.1109/TIT.1976.1055638.
- Doglio, F. (2018). *REST API Development with Node.js: Manage and Understand the Full Capabilities of Successful REST Development*. New York: Apress LP.
- Dykcik, L., Chuat, L., Szalachowski, P., & Perring, A. (2018). BlockPKI: An Automated, Resilient, and Transparent Public-Key Infrastructure. In Proceedings of the Workshop on Blockchain and Sharing Economy Applications, (pp. 316-322). Singapore. doi: 10.1109-ICDMW.2018.00022.
- Finch, V. (2017). *Bitcoin: The only complete quick & easy guide to mastering Bitcoin and digital currencies*. Auva Press.
- Friedman, W. F. (1922). "The index of coincidence and its applications in cryptology". *Department of Ciphers. Publ 22*. Geneva, Illinois, USA: Riverbank Laboratories.
- Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge: Cambridge University Press.
- Gallardo, I. (2018). *Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada*. (Master Thesis in Data Networks), University of La Plata, Argentina.
- Hoffman, N. (2017). *Blockchain: The insider's guide to Blockchain technology, Bitcoin mining, investing and trading cryptocurrencie*. Blockchain, cryptocurrency.
- Hoskinson, C. (2013), "The Mathematician's Defense of Bitcoin: It's Just Another Option". PBS News Hour.
- Housley, R., & Polk, T. (2001). *Planning for PKI: Best practices guide for deploying public key infrastructure*. Hoboken: Wiley.
- Jenkins, Y., & Jenkins, Y. (2015). *Bitcoin: Millionaire maker or monopoly money?* Publisher not identified.

- Jiang, W., Li, H., ...& Xu, G. (2019). PTAS: Privacy-preserving Thin-client Authentication Scheme in Blockchain-based PKI. January 2019 Future Generation Computer Systems 96. doi: 10.1016/j.future.2019.01.026
- Johnson, E. C. (2017). *Cryptocurrency: The beginner's guide to investing and trading in cryptocurrency*. Scotts Valley, CA: CreateSpace Independent Publishing Platform.
- Jhanwar, M. P., Chattopadhyay, A., & Madala, D. S. V. (2018). Certificate Transparency Using Blockchain. In Proceedings of the 2018 IEEE International Conference on Data Mining Workshops (ICDMW), (pp. 71-80). Singapore. from: <https://eprint.iacr.org/2018/1232.pdf>
- Kohnfelder, L. M. (1978). "On the Signature Reblocking Problem in Public Key Cryptography". *Communications of the ACM*. 21 (2): 179.
- Lafosse, J. (2009). *Java EE: Guide de développement d'applications web en Java*. Epsilon
- Leuf, B. (2002). *Peer to peer: Collaboration and sharing over the Internet*. Boston: Addison-Wesley.
- Massé, M. (2012). *REST API design rulebook*. Sebastopol, CA: O'Reilly media.
- Mohanty, H., & Pattnaik, P. K. (2019). *Webservices: Theory and practice*. Berlin: Springer.
- Mudunuri, S. (2013). *Spring Framework: A step by step approach for learning Spring framework*. Scotts Valley, CA: CreateSpace.
- Nash, A. (2002). *PKI: Infraestructura de claves públicas: La mejor tecnología para implementar y administrar la seguridad electrónica de su negocio*. New York: McGraw-Hill.
- Pathak, N., & Bhandari, A. (2018). *IOT, AI, and Blockchain for .NET: Building a next -generation application from the ground up*. New York: Apress.
- Pardi, P. (2015). *The TypeScript programming language*. Microsoft.
- Prieto, A. & Piattini, M. (2015). Propuesta de marco de mejora continua de gobierno TI en entidades financieras. RISTI - Revista ibérica de Sistemas y Tecnologías de Información RISTI, (15), pp. 51–67. DOI: 10.17013/risti.15.51-67.
- Satoshi, Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from <https://bitcoin.org/bitcoin.pdf>.
- Shane, P. M., & Hunker, J. A. (2013). *Cybersecurity: Shared risks, shared responsibilities*. Durham: Carolina Academic Press.
- Springer, S. (2018). *Node.js das umfassende Handbuch*. Bonn: Rheinwerk Verlag.
- Steinmetz, R.; Wehrle, K (2005). 2. What Is This "Peer-to-Peer" About?. pp. 9-16. Berlin Heidelberg: Springer..

- Thomas, S. A. (2000). *SSL & TLS essentials: Securing the Web*. Hoboken: Wiley.
- Vacca, J. R. (2002). *Public key infrastructure*. Boca Raton, FL: Auerbach.
- Vacca, J. R. (2013). *Computer and information security handbook*. Morgan Kaufmann.
- Vigna, P., & Casey, M. (2015). *The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order*.
- Vimercati, S. D., & Mitchell, C. (2013). *Public key infrastructures, services and applications*. In *9th European Workshop, EuroPKI 2012, Pisa, Italy, September 13-14, 2012: Revised selected papers*. Berlin: Springer.
- Won, J., Singla, A., Bertino, E., & Bollella, G. (2018). Decentralized Public Key Infrastructure for Internet-of-Things. In *Milcom 2018 Track 5 - Big Data and Machine Learning*, (pp. 907-913). Washington, USA. doi: 10.1109/MILCOM.2018.8599710.
- Yakubov, A., Shbair, W. M., & State, R. (2018). BlockPGP: A Blockchain-based Framework for PGP Key Servers. In *Proceedings of the 6th International Symposium on Computing and Networking Workshop*, (pp. 316-322). Hida Takayama, Japan.
- Zhao, W. (2014). *Building dependable distributed systems*. Scrivener Publishing/Wiley.

Aplicación de Balanceo De Carga Dinámico Para Servidores, Basada En Redes Definidas Por Software.

Carlos Enrique MINDA GILCES¹, Rubén PACHECO VILLAMAR²

cminda@uees.edu.ec, rpachevov@uees.edu.ec

^{1,2} Universidad de Especialidades Espíritu Santo, Samborondón, Guayas, Ecuador.

DOI: 10.17013/risti.n32.67-82

Resumen: Un aspecto relevante en investigación a nivel de redes de datos es la optimización de recursos. Las redes deben gestionar grandes volúmenes de tráfico sin introducir tiempos de espera innecesarios y garantizar la disponibilidad de servicios. Este artículo propone un algoritmo de balanceo de carga basado en un sistema de criterios combinados que utiliza tecnologías de redes definidas por *software* para obtener en tiempo de ejecución, parámetros desde distintos puntos de la red y seleccionar el servidor con las mejores condiciones para responder. La aplicación propuesta está escrita en lenguaje Python utilizando el controlador Ryu; la implementación de este programa en un *switch*, lo convierte en un balanceador de carga. Se utilizó la herramienta de simulación Mininet para la evaluación resultados; el experimento demuestra que el balanceador de carga basado en criterios combinados, reduce, hasta en un 50%, el tiempo de respuesta del servidor en comparación con el método tradicional *Round Robin*.

Palabras-clave: SDN; balanceo de carga; redes; servidores; OpenFlow.

Dynamic Load Balancing Application for Servers, Based on Software Defined Networking.

Abstract: A relevant topic in current data network research is network resource optimization. Networks must cope with large volumes of traffic and ensure the availability of services without introducing unnecessary timeouts. This article presents a load balance algorithm based on *software* defined networks; it uses combined criteria to obtain at runtime, parameters from different nodes in the network to select the server with the best capability to deliver services. The proposed load balancer is written in Python language using the Ryu controller. The implementation of the python code on a *switch* allows it to act as a network load balancer. Mininet simulation tool was used in the experiment. Results demonstrate that the SDN load balancer obtains a response time up to 50% lower than *Round Robin* algorithm.

Keywords: SDN; load balancing; networks; servers; OpenFlow.

1. Introducción

La navegación web emplea un modelo cliente-servidor en donde un cliente solicita datos y el servidor responde. Dependiendo del tipo de servicio, pueden existir millones de conexiones al servidor, en un mismo instante. De acuerdo a (KLEINER PERKINS, 2018) hasta julio del 2018 se registraron 4,119 millones de usuarios de Internet. Esta creciente demanda genera sobrecarga; los aumentos repentinos de tráfico en la red ocasionan congestión en los enlaces, lo que a su vez compromete el despliegue de las aplicaciones y los servicios ofrecidos por los proveedores. Un estudio empírico de Kandula, Sengupta, Greenberg, Patel, y Chaiken (2009) demuestra que el 15% de la congestión en una red de centro de datos conformada por 150 *switches* y 1500 servidores dura más de 100 segundos, aun cuando muchos de los enlaces se encuentran subutilizados; esto implica una necesidad considerable de optimizar la asignación de recursos de red.

La mayoría de centros de datos opta por la implementación de un balanceador de carga con el fin de satisfacer el gran número de usuarios y los requerimientos que estos generan (Chen, Shang, Tian, & Li, 2015). Usualmente, las estrategias de balanceo implementadas a los servicios web (HTTP) suelen basarse en las métricas de enlace proporcionadas al momento de la instalación y no consideran las condiciones de red dinámicas relativas a la utilización del ancho de banda, la pérdida de paquetes y los retrasos, por lo tanto carecen de flexibilidad para ajustarse a los distintos requerimientos de la red, o del tráfico o de las aplicaciones que operan sobre ésta (Qilin & Weikang, 2015).

La problemática recae en que al momento de aplicar el balanceo, los elementos de juicio disponibles para la toma de decisiones no contemplan parámetros variantes de la red que también influyen en el desempeño y pueden ser medidos dinámicamente (Kanungo, 2013), tales como la latencia, la variación de la latencia y las rutas alternas disponibles desde el punto de vista de procesos estocásticos. Como respuesta al requerimiento de alta disponibilidad, surgieron las Redes Definidas por *Software* (SDN, por sus siglas en inglés), que controlan la red de forma central o “programada” mediante aplicaciones de *software*. (Fernandez & L.Muñoz, 2016). Al implementar SDN, equipos de red de funcionalidad básica como los *switches*, son capaces de realizar funciones avanzadas.

Este artículo propone una solución de balanceo de carga que utiliza tecnologías de redes definidas por *software*. El mecanismo de balanceo de carga es aplicado a un grupo de servidores y está basado en criterios combinados, calculados a partir de la monitorización de múltiples parámetros de desempeño del servicio, que de acuerdo a estudios previos influyen en la calidad percibida por el usuario. El estudio está estructurado de la siguiente forma: La primera parte describe los Antecedentes y trabajos relacionados y la segunda el desarrollo de la investigación.

2. Antecedentes y Trabajos Relacionados

En lugar de utilizar un algoritmo estático como el *Round Robin*, los estudios de (Qilin, 2015);(Cui & Xu, 2016; Zhang & Guo, 2014) proponen a las redes definidas por *software* (SDN) como un nuevo acercamiento al balanceo de carga a través de un controlador de red centralizado. El trabajo de Fernandez & L. Muñoz (2016) menciona que existen dos métodos por los cuales se pueden agregar entradas a una tabla de flujos. La primera es de forma proactiva, esto se refiere a que la tabla es poblada por entradas mucho antes de

que los paquetes transiten por la red. El segundo método es el reactivo, en este método el dispositivo de red se inicializa sin ninguna regla de flujo preestablecida. Todo paquete entrante es enviado al controlador y posterior a tomar la decisión de qué hacer con el paquete, actualiza la tabla de flujo con la regla respectiva en el *switch*. La segunda vez que un paquete perteneciente al mismo flujo ingrese al dispositivo de red, este ya conocerá que acción debe realizar.

Por lo tanto, existen dos tipos de balanceadores de carga SDN que pueden ser desarrollados (Golinelli, 2015). La diferencia está en la manera en que el controlador aplica las reglas de flujo en el *switch*. En el método proactivo se establece previamente una división de las distintas direcciones IP que harán los requerimientos y dependiendo de la fuente se selecciona el servidor. En el método reactivo, la selección del servidor que atenderá el requerimiento es tomada cada vez que un paquete entra al *switch* y es enviado al controlador.

3. Métricas de Calidad

Según la investigación de Changhui (2016), el uso efectivo de los limitados recursos de red para satisfacer las necesidades de Calidad de Servicio de los negocios es un problema clave en el desarrollo de Internet. Conforme a las investigaciones de Kandula et al., (2009); Tashtarian, Erfanian, & Varasteh, (2018) los parámetros con mayor influencia en el establecimiento de niveles satisfactorios de QoE y QoS en una red de datos se reducen a: la capacidad de la red para acomodar el tráfico (rendimiento de procesamiento o throughput), la latencia o retraso que existe en la transferencia de

E estándar de Ancho de Banda (Throughput Standards)	Categoría	Ancho de Banda Disponible (%)
	Excelente	100
	Medio	75
	Bueno	50
	Pobre	<25
E estándar Pérdida de Paquetes (ETSI)	Categoría	Pérdida de Paquetes (%)
	Excelente	0
	Bueno	3
	Medio	15
	Pobre	> 25
E estándar Latencia (ITU-T-G.114)	Categoría	Intervalos (ms)
	Bueno	0-5
	Medio	150 – 400
	Pobre	> 400
E estándar Jitter (ITU-T-G.114)	Categoría	Intervalos (ms)
	Bueno	0-20
	Medio	20 – 50
	Pobre	> 50

Tabla 1 – Valores Basados en los Estándares revisados para Ancho de Banda, Pérdida de Paquetes, Latencia y Jitter.

datos de un punto a otro, el jitter, la variación en un periodo de tiempo que tiene la latencia y la pérdida de paquetes ocasionada por fallas en la transmisión de paquetes IP de un nodo a otro. Los estudios de (Tashtarian et al., 2018; Wawge & Tijare, 2014) expanden estas investigaciones y correlacionan el nivel de los parámetros medidos con el nivel de satisfacción que se genera en el usuario en referencia (TIPHON, 2002) como se detalla en la tabla 1.

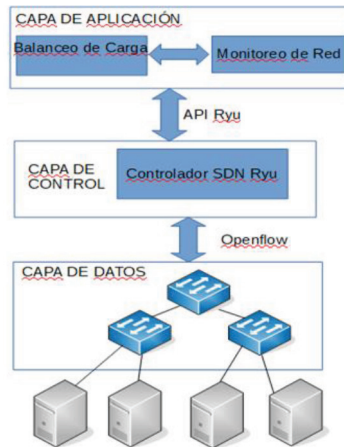


Figura 1 – Diagrama esquemático de los componentes lógicos. Fuente: Autores.

La figura 2 muestra la separación en capas en una arquitectura SDN, como se explica en el trabajo de Barrientos, Rico, Coronel y Cuesta(2019) estas capas se comunican por medio de una interfaz de programación de aplicaciones API lo cual brinda a las nuevas redes emergentes una mayor flexibilidad, fiabilidad y seguridad.

3. Desarrollo

Las métricas a tomar en consideración para el diseño de sistemas combinados son las de: latencia (ms) y ancho de banda disponible (kb/s), por la facilidad que se tiene para monitorizarlos desde el controlador. Adicional a estos parámetros de red se considera el consumo de CPU y memoria del servidor, debido a que, de acuerdo a Tashtarian et al., (2018) y Wawge & Tijare, (2014) estos afectan directamente al tiempo de respuesta del servicio, por el hecho de que de ellos depende la capacidad del servidor de procesar y atender los requerimientos. Estas métricas tienen un mayor peso en consideración con los parámetros medibles en red, ya que su influencia decrece directamente con la capacidad de la red de entregar correctamente un paquete. Para establecer los rangos permitidos para los valores medidos se hace referencia a estándares revisados. Utilizando estos estándares, los rangos y pesos para el sistema de criterios combinados escogidos se muestran en la tabla 2.

Sistema de <u>Criterios Combinados</u>				
	Parámetro	Valor Óptimo	Valor No Óptimo	Incidencia en Calificación
Servidor				
	CPU	0%	90%	50
	Memoria	0%	90%	30
Red				
	Latencia	0 ms	400 ms	10
	Ancho de Banda Disponible	100 %	50 %	10

Tabla 2 – Sistema de Criterios Combinados

3.1. Descubrimiento de equipos

Para relacionar las direcciones físicas e IP de los equipos se implementó dentro del controlador una tabla ARP. El controlador genera paquetes ARP que llevan un ARP REQUEST a todas las direcciones especificadas en la configuración. Al recibir un ARP_REPLY se agrega en un diccionario la dirección IP y su correspondiente dirección física. La figura 3 muestra una captura del intercambio de paquetes ARP.

No.	Time	Source	Destination	Protocol	Length	Info
26	1.388584467	00:00:00_00:00:03	aa:bb:cc:dd:00:11	ARP	42	Who has 10.0.0.10? Tell 10.0.0.3
28	1.386518612	00:00:00_00:00:03	aa:bb:cc:dd:00:11	ARP	42	Who has 10.0.0.10? Tell 10.0.0.3
29	1.388603851	aa:bb:cc:dd:00:11	00:00:00_00:00:03	ARP	60	10.0.0.10 is at aa:bb:cc:dd:00:11
31	1.388579712	00:00:00_00:00:03	aa:bb:cc:dd:00:11	ARP	42	Who has 10.0.0.10? Tell 10.0.0.3
84	3.692158397	00:00:00_00:00:04	aa:bb:cc:dd:00:11	ARP	42	Who has 10.0.0.10? Tell 10.0.0.4
90	3.692162622	00:00:00_00:00:04	aa:bb:cc:dd:00:11	ARP	42	Who has 10.0.0.10? Tell 10.0.0.4
91	3.690274314	00:00:00_00:00:04	aa:bb:cc:dd:00:11	ARP	42	Who has 10.0.0.10? Tell 10.0.0.4
92	3.692187604	aa:bb:cc:dd:00:11	00:00:00_00:00:04	ARP	60	10.0.0.10 is at aa:bb:cc:dd:00:11

Figura 2 – Intercambio de Mensajes ARP. Fuente: Autores.

3.2. Cálculo de Ancho de Banda Disponible

Se utiliza una aplicación de monitoreo de tráfico desarrollada por Machi y Cheng(2018). La obtención del ancho de banda disponible se calcula en base a los valores de la capacidad de ancho de banda del *switch* y la tasa de transferencia del puerto. La capacidad de ancho de banda es consultada directamente al *switch* por el controlador por medio del mensaje OFPPORT_FEATURES. La tasa de transferencia del puerto se calcula por medio de la variación de paquetes transmitidos en un periodo de tiempo determinado, la fórmula es la siguiente:

$$Ttp = \frac{Pq_t - Pq_{t-1}}{1/t} \quad (1)$$

Donde Pq es el número de paquetes transmitidos y Ttp la tasa de Transferencia del Puerto. Luego, el ancho de banda disponible se calcula a partir de (2), donde Cp representa la capacidad del puerto. El ancho de banda queda expresado en las unidades de kb/s.

$$B = \frac{(Cp - Ttp) 8}{100} \tag{2}$$

3.3. Cálculo de Latencia

Para el cálculo de latencia se desarrolló un módulo dentro de la aplicación de balanceo de carga que construye y envía paquetes *ICMP* hacia cada dirección IP definida en el archivo de configuración del balanceador. Este cálculo se realiza desde el punto de vista del balanceador hacia los servidores, utilizando el tiempo de ida y vuelta (RTT) provisto por la aplicación PING (*ICMP*).

La Latencia, se calcula determinando el lapso transcurrido desde que el balanceador envió el paquete de prueba *ICMP* (tiempo de envío paquete), hasta el momento en que le llega la respuesta correspondiente (tiempo actual). Se adjunta fórmula utilizada:

$$l = T_{actual} - T_{ICMP} \tag{3}$$

3.4. Datos del Servidor

Con el objetivo de simplificar el diseño y evitar el uso de herramientas adicionales para la medición de las métricas del servidor se implementó una pequeña aplicación en Python. Esta aplicación utiliza la librería *psutil* para consultar los porcentajes de consumo de CPU y memoria del servidor y es compatible con sistemas operativos Windows o Linux (Rodola, 2018). Luego de consultar las métricas el controlador construye un paquete UDP con la información requerida, el cual es enviado a la dirección IP virtual designada para el balanceador de carga. Cuando este paquete llega al controlador la información de las métricas es almacenada. La figura 4 muestra una captura de tráfico en el que se verifica el envío de los paquetes hacia la dirección IP del balanceador.

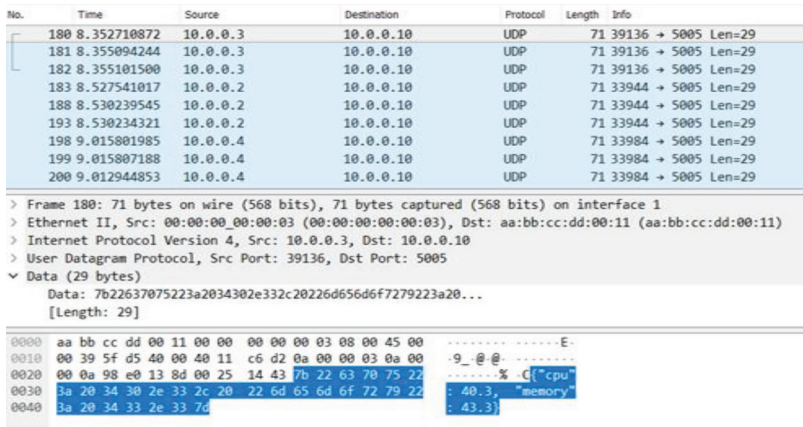


Figura 3 – Captura de tráfico UDP de los servidores al controlador. Fuente: Autores.

3.5. Normalización de datos

Debido a que las métricas que conforman el sistema de criterios combinados poseen unidades y rangos de valores distintos es necesario realizar la normalización de los datos previo a realizar el cálculo del peso de cada servidor. La función implementada dentro de la aplicación de balanceo de carga para normalizar los datos está dada por (4):

$$V_N = \left(\frac{V_M - V_{min}}{V_{max} - V_{min}} \right) 100 \quad (4)$$

Donde V_{min} y V_{max} son los valores mínimos y máximos respectivamente, V_M el valor medido y V_N el valor normalizado. De este modo, de cada métrica se obtiene una calificación sobre 100 puntos, como se muestra en la Tabla 3.

Parámetro	Valor Medido	Valor Mínimo	Valor Máximo	Valor Normalizado
Latencia (ms)	20	400	0	95.00
Latencia (ms)	50	400	0	87.50
Ancho de Banda Disponible (%)	80	50	100	60.00
CPU (%)	10	90	0	88.89
Memoria (%)	40	90	0	55.56

Tabla 3 – Ejemplo de normalización de datos medidos.

Dado que cada parámetro medido, por su nivel de importancia en el tiempo de respuesta, debe tener el peso específico que le corresponde en la determinación de la métrica combinada (peso), se utilizó una escala basada en la experiencia y el criterio de expertos, desarrollada a través de encuestas e investigaciones predecesoras, y se determinó la ponderación de acuerdo a la fórmula (5) donde W representa el Peso, C_{cpu} el consumo de cpu, M la memoria, l la latencia y B el ancho de banda.

$$W = 0.50C_{cpu} + 0.30M + 10l + 10B \quad (5)$$

3.6. Aplicación de Balanceo de Carga

La aplicación de balanceo de carga es de tipo reactivo. Todos los paquetes entrantes al *switch* son enviados al controlador para la selección del servidor. Los paquetes entrantes levantan un evento del tipo OFPPacketIn. Si la dirección de destino coincide con la del servicio, el paquete pasa a ser procesado, caso contrario el paquete es ignorado y no se realiza ninguna acción.

El controlador verifica que el paquete corresponda a un paquete TCP y en ese momento realiza la selección del servidor. El destino escogido se decanta por el servidor que posee la mejor calificación, basado en el sistema de criterios combinados, calculado en ese instante de tiempo. Una vez seleccionado el servidor el controlador construye dos entradas con las que actualiza la tabla de flujo del *switch* utilizando la dirección IP y

dirección física del servidor seleccionado y del cliente. Una entrada corresponde al flujo cliente-servidor para los requerimientos entrantes. La segunda entrada corresponde al flujo servidor-cliente para la entrega de las respuestas del servidor.

Como se visualiza en la Figura 5, una vez establecida la conexión con el *switch*, para la monitorización de las estadísticas del equipo de red, el controlador genera un paquete del tipo *OFPPortStatsRequest*. La respuesta, un paquete *OFPPortStatsReply*, es enviada por el *switch* al controlador y contiene información de los puertos como: la capacidad de ancho de banda, velocidad de transmisión, paquetes transmitidos y recibidos.

La información del uso de CPU y memoria llegan al controlador por medio de un paquete UDP generado por el servidor. En este caso, el evento *OFPPacketIn* inicia el gestor de paquetes UDP implementado en la aplicación del balanceo de carga y extrae de la trama UDP la información y la dirección IP de origen.

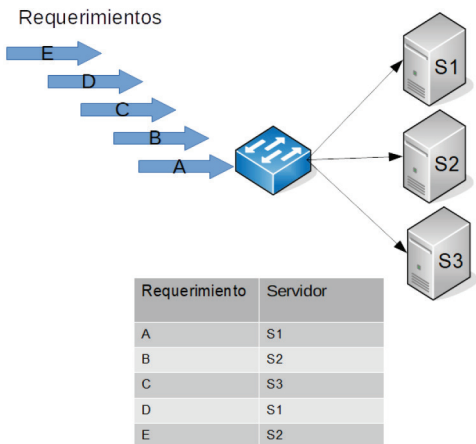


Figura 4 – Intercambio de mensajes Openflow. Fuente: Autores.

La actualización de la tabla de flujos es realizada por medio del paquete *OFPFLOWMod* enviado desde el controlador hacia el *switch*. Una vez ingresadas las entradas en la tabla de flujo del *switch* el paquete es enviado al destino seleccionado y se establece la conexión TCP. Una vez establecida la conexión, se realiza el intercambio de información por medio del protocolo HTTP.

3.7. Ambiente de pruebas

La aplicación de balanceo de carga fue desarrollada e implementada sobre una red virtualizada en *Mininet*,¹ utilizando *OpenVswitch* y el controlador *Ryu*. Se escogió este

¹ Mininet es un *software* de código abierto que permite la virtualización de redes y hosts para la simulación de distintas topologías de red. Esta herramienta le provee al desarrollador un ambiente de pruebas para todo tipo de aplicaciones. *Mininet* permite describir y levantar topologías de manera programática.

controlador porque de acuerdo a (Shah, Faiz, Farooq, Shafi, & Mehdi 2013) es el que cubre un mayor número de especificaciones técnicas para el desarrollo de aplicaciones. La figura 6 denota la topología del entorno de pruebas, el *OVS* actúa como balanceador de carga y se conecta a los servidores S1, S2, S3. El equipo H1 funciona como cliente. Para la implementación del balanceador de carga se desarrolló el archivo *lb-topology.py* para automatizar el despliegue de los servidores, los enlaces y la inicialización del módulo de estadísticas del servidor y el servicio web.

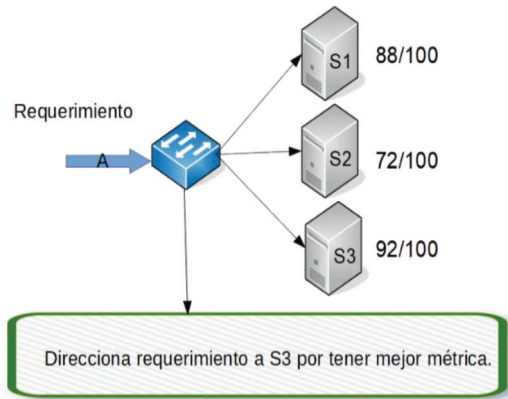


Figura 5 – Topología de Red Virtualizada en *Mininet* para entorno de pruebas. Fuente: Autores.

3.8. HTTPPerf

Para la generación de tráfico se optó por utilizar la herramienta *httperf*, un *software* de código abierto que permite realizar pruebas de servicios *HTTP*. Con *httperf* se realiza

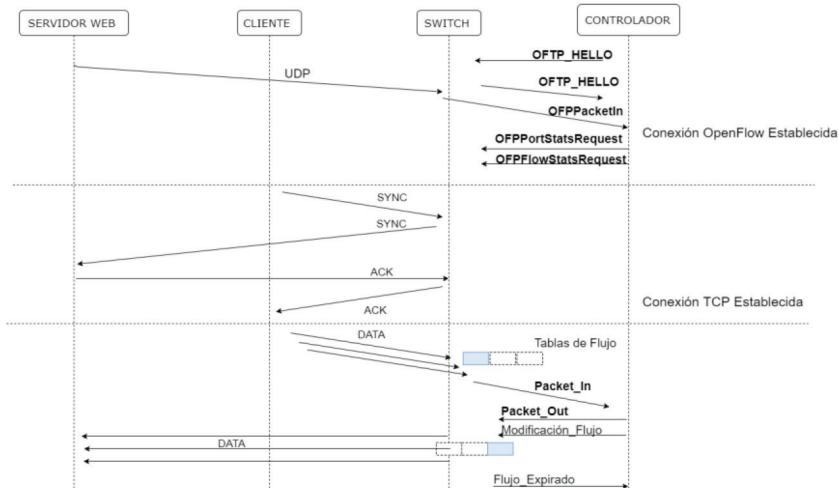


Figura 6 – Método Round Robin. Fuente: Autores.

la medición del tiempo de respuesta promedio de un servidor web y el número de requerimientos exitosos y fallidos.

El objetivo de las pruebas es constatar el funcionamiento y medir los tiempos de respuesta del balanceo de carga basado en criterios combinados. Para este efecto, se ejecutó la virtualización del balanceador y se obtuvieron varias mediciones del tiempo de respuesta bajo diferentes condiciones. Luego se implementó el método de balanceo de carga, *Round Robin*, para comparar los resultados de rendimiento de éste versus el balanceo de carga basado en criterios combinados sobre el mismo ambiente. En las figuras 7 y 8, se muestra el proceso de selección con cada técnica de balanceo.

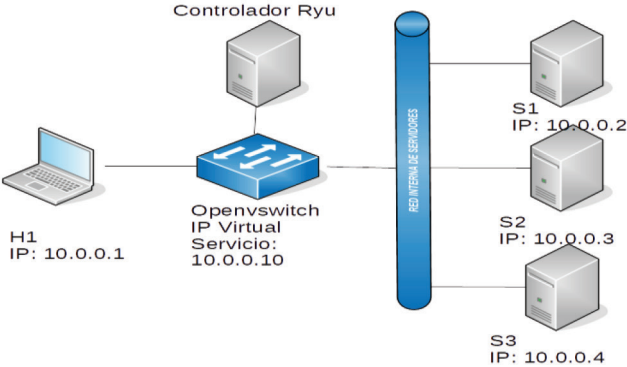


Figura 7 – Método de selección basado en el sistema de criterios combinados. Fuente: Autores.

4. Resultados

Para confirmar el funcionamiento del balanceo de carga, dentro de la etapa de implementación, se capturó el tráfico generado dentro de *Mininet* con la herramienta

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000380361	127.0.0.1	127.0.0.1	OpenFL	208	Type: OFPT_PACKET_IN
3	0.001138020	127.0.0.1	127.0.0.1	OpenFL	206	Type: OFPT_PACKET_OUT
7	0.002323224	127.0.0.1	127.0.0.1	OpenFL	208	Type: OFPT_PACKET_IN
8	0.002337498	127.0.0.1	127.0.0.1	OpenFL	209	Type: OFPT_PACKET_IN
13	0.003346844	127.0.0.1	127.0.0.1	OpenFL	206	Type: OFPT_PACKET_OUT
14	0.003368116	127.0.0.1	127.0.0.1	OpenFL	207	Type: OFPT_PACKET_OUT
22	0.395649823	127.0.0.1	127.0.0.1	OpenFL	178	Type: OFPT_PACKET_OUT
25	0.396019504	127.0.0.1	127.0.0.1	OpenFL	180	Type: OFPT_PACKET_IN
26	0.396682754	127.0.0.1	127.0.0.1	OpenFL	178	Type: OFPT_PACKET_OUT
33	1.004266277	127.0.0.1	127.0.0.1	OpenFL	208	Type: OFPT_PACKET_IN
34	1.005127995	127.0.0.1	127.0.0.1	OpenFL	209	Type: OFPT_PACKET_IN
36	1.006247755	127.0.0.1	127.0.0.1	OpenFL	208	Type: OFPT_PACKET_IN
38	1.007550168	127.0.0.1	127.0.0.1	OpenFL	206	Type: OFPT_PACKET_OUT
40	1.007589421	127.0.0.1	127.0.0.1	OpenFL	207	Type: OFPT_PACKET_OUT
> Frame 40: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits) on interface 0						
> Linux cooked capture						
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1						
> Transmission Control Protocol, Src Port: 6633, Dst Port: 44018, Seq: 774, Ack: 955, Len: 139						
> OpenFlow 1.3						

Figura 8 – Captura de tráfico demostrando el intercambio de paquetes Openflow. Fuente: Autores.

Wireshark. En la figura 9, se visualiza el intercambio de mensajes del Protocolo Openflow. Se muestran los paquetes que corresponden a los eventos de *OFPT_PACKET_IN* y *OFPT_PACKET_OUT* que confirman que los paquetes entrantes al *switch* están siendo enviados hacia el controlador. Adicionalmente, se verificó que al enviar un paquete hacia la dirección virtual, este sea redirigido hacia uno de los servidores.

La figura 10 muestra una captura de pantalla de la secuencia de eventos en ese caso. Aquí se verifica que al realizar un requerimiento desde el cliente a la dirección del servicio posteriormente se selecciona uno de los servidores para atender el requerimiento. También se puede observar el status de respuesta del paquete.

7384	41.114166826	10.0.0.1	10.0.0.10	HTTP	130	GET / HTTP/1.1
7385	41.114175455	10.0.0.1	10.0.0.4	HTTP	130	GET / HTTP/1.1
7418	41.150411539	10.0.0.4	10.0.0.1	HTTP	964	HTTP/1.0 200 OK (text/html)
7419	41.150412901	10.0.0.10	10.0.0.1	HTTP	964	HTTP/1.0 200 OK (text/html)
7451	41.178113746	10.0.0.1	10.0.0.10	HTTP	130	GET / HTTP/1.1
7452	41.178117618	10.0.0.1	10.0.0.2	HTTP	130	GET / HTTP/1.1
7479	41.187233542	10.0.0.4	10.0.0.1	HTTP	964	HTTP/1.0 200 OK (text/html)
7480	41.187234745	10.0.0.10	10.0.0.1	HTTP	964	HTTP/1.0 200 OK (text/html)
7509	41.192723219	10.0.0.2	10.0.0.1	HTTP	964	HTTP/1.0 200 OK (text/html)
7510	41.192724385	10.0.0.10	10.0.0.1	HTTP	964	HTTP/1.0 200 OK (text/html)
7539	41.205187451	10.0.0.4	10.0.0.1	HTTP	964	HTTP/1.0 200 OK (text/html)
7540	41.205188547	10.0.0.10	10.0.0.1	HTTP	964	HTTP/1.0 200 OK (text/html)


```

[Stream index: 2]
[TCP Segment Len: 62]
Sequence number: 1 (relative sequence number)
[Next sequence number: 63 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x018 (PSH, ACK)
Window size value: 16060
[Calculated window size: 16060]
[Window size scaling factor: 1]
Checksum: 0x146f [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (62 bytes)
▼ Hypertext Transfer Protocol
> GET / HTTP/1.1\r\n
User-Agent: httpperf/0.9.0\r\n
Host: 10.0.0.10\r\n
\r\n
[Full request URI: http://10.0.0.10/]
[HTTP request 1/1]
[Response in frame: 2647]

```

Figura 9 – Redirección de paquetes HTTP. Fuente: Autores.

4.1. Resultados Rendimiento de balanceo de carga

Con el propósito de realizar pruebas de rendimiento del balanceo de carga sobre la topología previamente establecida, se utilizó la herramienta *httpperf* para generar tráfico HTTP hacia la dirección virtual del servicio. Para el primer conjunto de pruebas todos los enlaces están virtualizados bajo condiciones ideales, es decir con latencia mínima y cero pérdida de paquetes. En el segundo conjunto de pruebas se agrega latencia a dos de los enlaces que se conectan del *switch* al servidor.

Previo a la ejecución de cada una de las pruebas se reinició la aplicación de balanceo de carga, y la de la topología virtualizada en *Mininet* para evitar que datos residuales en memoria afecten el rendimiento de los algoritmos del balanceo de carga. Así mismo, previo a iniciar la herramienta *HTTPPerf* se ejecutó un comando *pingall* en la línea de comando de *Mininet* para confirmar que todos los hosts virtualizados fueron alcanzados.

Los dos conjuntos de pruebas consisten de un número total de conexiones (100, 200 y 300) a establecerse. Para cada caso se varía la cantidad de conexiones que se establecen

por segundo. Por último se limita de manera equitativa el porcentaje de CPU al que pueden acceder los servidores para evitar que el host se saturé. HTTPerf calcula un promedio del tiempo de respuesta para cada requerimiento y nos muestra una estadística del tiempo de respuesta promedio para cada prueba. Con estas estadísticas, se calculó la disminución porcentual, es decir, la proporción de la cantidad por la cual el tiempo de respuesta se ha reducido al emplear el sistema de criterios combinados en comparación con el tiempo del sistema *Round Robin*. Cuando el valor de disminución porcentual es positivo, implica que el tiempo de respuesta se ha reducido en dicho porcentaje. Cuando el valor es negativo se debe entender que ha habido un incremento en el tiempo de respuesta en dicho porcentaje. La Tabla 4 y el Gráfico 1 resumen los resultados obtenidos para el primer conjunto de pruebas en condiciones ideales.

En cualquiera de los tres escenarios (100, 200 o 300 conexiones) se puede observar que el balanceo de carga basado en el sistema de criterios combinados (línea naranja) obtiene un menor tiempo de respuesta comparado con el método *Round Robin* (línea azul) para la mayoría de tasas de conexión. Así mismo, la disminución porcentual es positiva para la mayoría de casos, indicando que el tiempo de respuesta se reduce con la aplicación del sistema de criterios combinados. En promedio, el tiempo de respuesta se reduce en un rango del 20 hasta 50% utilizando el sistema de criterios combinados. La única excepción se da cuando la tasa de conexiones por segundo es de 50. Esto puede ser atribuido al hecho de que en el ambiente de pruebas los recursos de CPU y memoria son limitados por la máquina host.

Total de Conexiones	Tasa de Conexiones por Segundo	Sistema de Criterios		Disminución porcentual
		Round Robin	Combinados	
		Tiempo de Respuesta (ms)	Tiempo de Respuesta (ms)	
100	5	73.7	54.5	26.05
	10	70.8	31.5	55.51
	15	51.8	25	51.74
	20	65.6	40.5	38.26
	50	44	63.5	-44.32
200	5	61.9	56.2	9.21
	10	70.2	45	35.90
	15	58.6	29.7	49.32
	20	54	54.1	-0.19
	50	38.7	66.5	-71.83
300	5	59.9	48.8	18.53
	10	68.7	28.3	58.81
	15	61.5	32.7	46.83
	20	73.7	49.2	33.24
	50	49.7	68.2	-37.22

Tabla 4 – Comparativo Condiciones Ideales

El método *Round Robin* es un método simple el cuál utiliza poco recursos del controlador a diferencia del sistema de criterios combinados. Esto se debe a que a una mayor cantidad de conexiones por segundo, decrece la efectividad del algoritmo de selección propuesto ya que el ambiente sobre el cuál se está realizando la simulación debe hacer uso de tiempos de CPU y memoria del host para la virtualización de los elementos, la creación de la carga o conexiones y en generar la respuesta de los servidores.

La aplicación de balanceo de carga basado en criterios combinados, al monitorear en tiempo real las estadísticas de la red y los servidores y realizar el cálculo con las métricas obtenidas hace fuerte uso de estos recursos, y el tiempo de respuesta del servidor sufre un incremento debido al tiempo que le toma al controlador realizar los cálculos, el cual aumenta al existir menor cantidad de recursos disponibles.

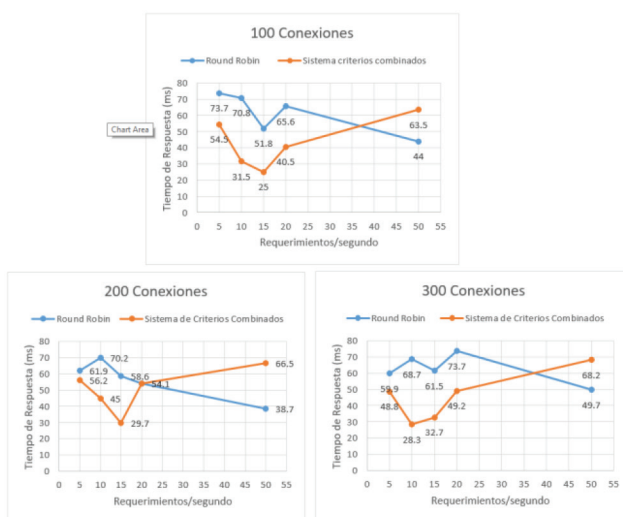


Gráfico 1 – Tiempo de Respuesta vs Requerimientos/Segundos del primer set de pruebas.
Fuente: Autores.

En el segundo conjunto de pruebas se aprovechó la flexibilidad que brinda la herramienta de Mininet para agregar latencia en los enlaces que conectan al dispositivo de red, el OVS *switch*, con los servidores. En estas pruebas a dos de los enlaces se les agregó una latencia correspondiente a 50 ms y 80ms, mientras que el enlace restante no es afectado por latencia. En la Tabla 5 y Gráfico 2 se puede observar los tiempos de respuesta obtenidos para ambos algoritmos de selección. Nuevamente se observa una disminución en el tiempo de respuesta al utilizar el sistema de criterios combinados. Incluso agregando la latencia, la disminución porcentual es positiva para casi todos los casos a excepción del de 5 conexiones por segundo, en el grupal de 100 conexiones. La tabla denota una mejora general en los tiempos de respuesta en todos los casos, reduciéndolo hasta en más del 50% del tiempo de respuesta obtenido por el método *Round Robin*.

También se observa que cuando existe una gran cantidad de conexiones por segundo el tiempo de respuesta del sistema de criterios combinados tiende a aumentar con respecto

a los casos anteriores. Aún cuando existe latencia en los enlaces el algoritmo propuesto demuestra un mejor desempeño comparado al *Round Robin*. Esto se debe, en gran parte a que, cuando se incluye latencia en los enlaces, el balanceo de carga propuesto tenderá a escoger el enlace que presente menor latencia hasta que la carga sobre este servidor cause que el consumo de CPU y memoria aumenten y reduzcan la calificación de este servidor bajo el sistema de criterios combinados, pasando a seleccionar uno de los enlaces restantes.

		Sistema de Criterios		
		Round Robin	Combinados	
Total de Conexiones	Tasa de Conexiones por Segundo	Tiempo de Respuesta (ms)	Tiempo de Respuesta (ms)	Disminución Porcentual
100	5	72.4	74.3	-2.62
	10	147.2	92.2	37.36
	15	146.1	86.7	40.66
	20	132.3	116.1	12.24
	50	123.7	65.1	47.37
200	5	96.1	90	6.35
	10	147	93.6	36.33
	15	58.6	29.7	49.32
	20	134.6	82.4	38.78
	50	122.3	100.5	17.83
300	5	149.5	109.4	26.82
	10	154.8	80.3	48.13
	15	137.4	91.1	33.70
	20	137.3	65.9	52.00
	50	126.4	116.9	7.52

Tabla 5 – Comparativo con latencia en enlaces

5. Conclusiones y recomendaciones

El experimento demostró que el algoritmo de selección que toma en consideración parámetros de la red y servidores para la técnica de balanceo de carga permite obtener un menor tiempo de respuesta y en consecuencia, incrementa el rendimiento de los servicios web. Al comparar el sistema de criterios combinados versus el algoritmo *Round Robin*, se concluye que para entornos de red en los que existe latencia en los enlaces, el balanceador de carga basado en criterios combinados funciona mejor, con un tiempo de respuesta hasta 50% menor que el obtenido en comparación con la estrategia *Round Robin*. Adicionalmente, los tiempos de respuesta obtenidos usando el sistema de criterios combinados van desde valores de 25 a 68.2 ms en el caso de enlaces sin latencia y 29.7 a 116.9 ms en los enlaces con latencia. Valores que se encuentran por debajo al límite recomendado por Google de los 200ms para tiempo de respuesta de un servidor. Basado en esto se puede concluir que la implementación del balanceo de carga basado en criterios combinados ayuda a mejorar la experiencia de usuario al utilizar un servicio web.

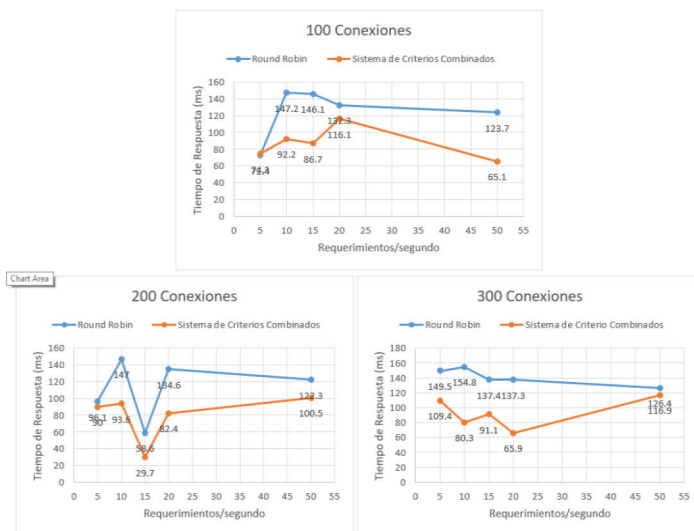


Gráfico 2 – Tiempo de respuesta vs Requerimientos/Segundos. Resultados obtenidos pruebas que incluyen latencia en los enlaces. Fuente: Autores.

El algoritmo propuesto en este documento, además de disminuir los tiempos de respuesta para proporcionar una mejor experiencia de usuario, permite también una utilización más eficiente del CPU y la memoria del servidor y por lo tanto ofrece un método de balanceo de carga más eficaz en comparación a las estrategias tradicionales.

La implementación actual del balanceo de carga basado en un sistema de criterios combinados recolecta y procesa datos utilizando la memoria del equipo en el que corre el controlador, esta configuración puede ser mejorada almacenando los parámetros monitoreados en una base de datos y no en memoria. La arquitectura SDN presenta un punto de fallo en el controlador, si éste falla, la red quedaría incapacitada, debido a esto las aplicaciones que se ejecuten dentro del controlador deben de ser eficientes en cuanto al consumo de CPU y memoria. Una solución a este problema es utilizar dos controladores dentro de la arquitectura de la red. La primera etapa de balanceo determinaría el controlador que realiza la segunda etapa de balanceo correspondiente a las aplicaciones del usuario. En trabajos futuros se sugiere modificar el esquema empleando dos controladores.

Experimentar sobre otro tipo de servicios, como FTP o flujo (streaming) de video, para comparar el desempeño del algoritmo de selección propuesto son sugerencias para trabajos de investigación futuros.

Referencias

- Barrientos-Avendaño, E., Rico-Bautista, D., Coronel-Rojas, L. A., & Cuesta-Quintero, F. R. (2019). Granja inteligente: Definición de infraestructura basada en internet de las cosas, IPv6 y redes definidas por software. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (E17), 183-197.

- Changhui, C. (2016). Research on QoS flow control method based on OpenFlow technology. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (17B), 14. DOI:10.17013/risti.17B.14-26
- Chen, W., Shang, Z., Tian, X., & Li, H. (2015). Dynamic Server Cluster Load Balancing in Virtualization Environment with OpenFlow. *International Journal of Distributed Sensor Networks*, July 2015. <https://doi.org/10.1155/2015/531538>
- Cui, C. X., & Xu, Y. Bin. (2016). Research on load balance method in SDN. *International Journal of Grid and Distributed Computing*, 9(1), 25–36. <https://doi.org/10.14257/ijgdc.2016.9.1.03>
- Fernandez, C.L., & Muñoz, J. (2016). Software Defined Networking (SDN) with OpenFlow 1.3, Open vSwitch and Ryu, (June 2010), 183.
- Golinelli, E. S. (2015). A Software Defined Networking evaluation approach to distributing load. Retrieved from <https://www.duo.uio.no/bitstream/handle/10852/45126/Golinelli-master.pdf>
- Ikram, A., Arif, S., Ayub, N., & Arif, W. (2018). Load Balancing In Software Defined Networking (SDN).
- Kandula, S., Sengupta, S., Greenberg, A., Patel, P., & Chaiken, R. (2009). The Nature of Datacenter Traffic : Measurements & Analysis. Provider. (pp 202–208). Microsoft Research. <https://doi.org/10.1145/1644893.1644918>
- Kanungo, P. (2013). Study of Server Load Balancing Techniques. *International Journal of Computer Science & Engineering Technology*, 4(11), 1383–1389.
- Kleiner, P. (2018). Internet Trends. Kpcb.
- Machi, H., & Cheng, L. (2018). PureSDN. Github.Com.
- Qilin, M., & Weikang, S. (2015). A Load Balancing Method Based on SDN. In *Proceedings - 2015 7th International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2015*. <https://doi.org/10.1109/ICMTMA.2015.13>
- Rodola, G. (2018). Psutil. Github.Com.
- Shah, S. A., Faiz, J., Farooq, M., Shafi, A., & Mehdi, S. A. (2013). An architectural evaluation of SDN controllers. In *IEEE International Conference on Communications*, 1, 3504–3508. <https://doi.org/10.1109/ICC.2013.6655093>
- Tashtarian, F., Erfanian, A., & Varasteh, A. (2018). S2VC: An SDN-based framework for maximizing QoE in SVC-based HTTP adaptive streaming. *Computer Networks*, 146, 33–46. <https://doi.org/10.1016/j.comnet.2018.09.007>
- TIPHON. (2002). Etsi tr 101 329-7 Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to end Quality of Service in TIPHON systems; Part 7: Design guide for elements of a TIPHON connection from an end-to-end speech transmission per. *Intellectual Property*, 1, 1–72.
- Wawge, P., & Tijare, P. (2014). Implementing Parameterized Dynamic Load Balancing Algorithm Using CPU and Memory, 3(5), 12828–12834.

Ciberseguridad del Sistema de Control Industrial de la Planta Cloro-Sosa ELQUIM.

Héctor Enrique Socarrás¹, Ivan Santana²

hector@cedai.com.cu, ching@uclv.edu.cu

¹ Empresa de Automatización Integral CEDAI, División Villa Clara, Calle 4ta no 7, C.P. 50100, Santa Clara, Villa Clara, Cuba.

² Universidad Central “Marta Abreu” de las Villas, Facultad de Ingeniería Eléctrica, Departamento de Automática, Carretera a Camajuaní Km. 5 y 1/2, C.P. 50100, Santa Clara, Villa Clara, Cuba.

DOI: 10.17013/risti.32.83–96

Resumen: Después de Stuxnet la protección de los Sistemas de Control Industrial, en especial aquellos que controlan procesos de infraestructuras críticas, ha tomado vital importancia para los gobiernos. Ya solo no basta la protección física de estas instalaciones, sino una amenaza como los ciberataques deben ser tenidas en cuenta. Es en este escenario que la implementación de medidas de ciberseguridad para el sistema de control industrial (SCI) de la nueva planta de Cloro-Sosa de la empresa ELQUIM es un requerimiento de las autoridades nacionales. En este artículo se presenta la implementación de una estrategia de defensa en profundidad para la protección de este SCI siguiendo las reglas internacionales y nacionales lo cual es definitorio para el arranque de la nueva planta.

Palabras-clave: Ciberseguridad; Infraestructura Crítica; Sistemas de Control Industrial.

Cyber Security for the Industrial Control System of the ELQUIM's Chlorine Plant.

Abstract: After Stuxnet, the protection of Industrial Control Systems, especially those that control critical infrastructure processes, has taken vital importance for governments. The physical protection of these facilities alone is not enough, but a threat such as cyber-attacks must be taken into account. It is in this scenario that the implementation of cybersecurity measures for the industrial control system (ICS) of the new ELQUIM company's chlorine plant is a requirement of the national authorities. In this article we present the implementation of a defense in depth strategy for the protection of this ICS.

Keywords: Cyber Security; Critical Infrastructure; Industrial Control Systems.

1. Introducción

Las Infraestructuras Críticas son aquellas instalaciones y sistemas sobre los que recaen servicios esenciales cuyo funcionamiento no permite soluciones alternativas, por lo que

su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales prestados a la sociedad. (CCN-CERT, 2016). La planta de producción de Cloro-Sosa de la empresa ELQUIM, única de su tipo en Cuba, es responsable de suplir la demanda de Cloro líquido e hipoclorito de sodio para la potabilizar el agua suministrada a la población.

La planta actual, con más de 35 años de explotación y tecnología de celdas electrolíticas de mercurio, se encuentra al final de su ciclo de vida y fue reemplazada por una moderna planta con tecnología de membranas, más amigable con el medio ambiente. La nueva planta cuenta con un sistema de control industrial compuesto por un sistema de control distribuido (DCS), un sistema de apagado de emergencia (ESD) y controladores lógicos programables (PLC) en unidades auxiliares.

Muchos de los Sistemas de Control Industrial de hoy evolucionaron desde la inserción de las capacidades de tecnologías de la información en los sistemas físicos existentes, a menudo reemplazando o complementando los mecanismos de control físico. Las mejoras en el costo y el rendimiento han fomentado esta evolución, dando como resultado muchas de las tecnologías “inteligentes” de hoy en día, como la red eléctrica inteligente, el transporte inteligente, los edificios inteligentes y la fabricación inteligente. Si bien esto aumenta la conectividad y la criticidad de estos sistemas, también crea una mayor necesidad de adaptabilidad, resiliencia y seguridad (Stouffer et al, 2015).

Para utilizar los recursos y los activos del SCI de manera eficiente, este debe estar bajo el control de una administración de seguridad y gobernanza adecuada. La gobernanza se refiere al conjunto de controles de seguridad que se utilizan para gobernar una organización (Alcaraz, C. et al, 2015).

Para fortalecer la seguridad de los SCI, una solución es implementar una defensa en profundidad mediante la combinación de controles de seguridad para reducir el riesgo para los activos que se están protegiendo. Al aplicar múltiples controles sobre el SCI se introducen otras barreras, que un atacante debe superar (Maglaras, L. A. et al, 2018).

Este trabajo tuvo como objetivo la implementación de una estrategia de defensa en profundidad para la protección del SCI de la planta de producción de Cloro-Sosa de la empresa ELQUIM. En la sección 2 se describe el SCI de la planta, la sección 3 presenta los aspectos fundamentales de la estrategia de defensa en profundidad y describe la implementación de la misma, finalmente se presentan las conclusiones.

2. Descripción del Sistema de Control Industrial

2.1. DCS

El DCS de la planta está implementado sobre la solución CENTUM VP de Yokogawa (Yokogawa Electric Corporation, 2015).

Este sistema está compuesto en la planta, por 3 estaciones de control de campo o (FCS), las cuales son controladores con una alta fiabilidad, realizan funciones de control y de entrada/salida al proceso, formadas por una Unidad de Control de Campo y varias

unidades de nodos para el montaje de módulos de entrada/salida; 2 estaciones de interface humana (HIS) que son PC con los paquetes de software de funciones de operación y monitoreo instalados a través de las cuales los operadores interactúan con el proceso; una estación de Ingeniería, que es un PC con los paquetes de software necesarios para la configuración, programación y administración del sistema; todo esto interconectado a través de una red de control Vnet/IP, que es una red ethernet redundante a 1Gbps.

Adicionalmente la red ethernet estándar de las estaciones HIS es utilizada para la comunicación con las impresoras de alarmas y la comunicación con la red de gestión empresarial a través de un servidor de datos OPC DA y AE.

2.2. Sistema de Apagado de Emergencia. (ESD)

La protección contra eventos peligrosos como explosiones, escapes de productos tóxicos etc., se realiza a través de un esquema de protección por capas Figura 1, en la cual los ESD se encuentran en la capa de prevención y mitigación de eventos peligrosos.

El ESD fue implementado utilizando el sistema instrumentado de seguridad de Yokogawa ProSafe-RS el cual está certificado por TUV Rheinland, logra un nivel de integración de seguridad (SIL) 3 y se integra fácilmente con el DCS Centum VP (Yokogawa Electric Corporation, 2016).

Está compuesto por la estación de ingeniería de seguridad (SENG) compartida con la estación de ingeniería del DCS y 2 estaciones de control de seguridad (SCS).

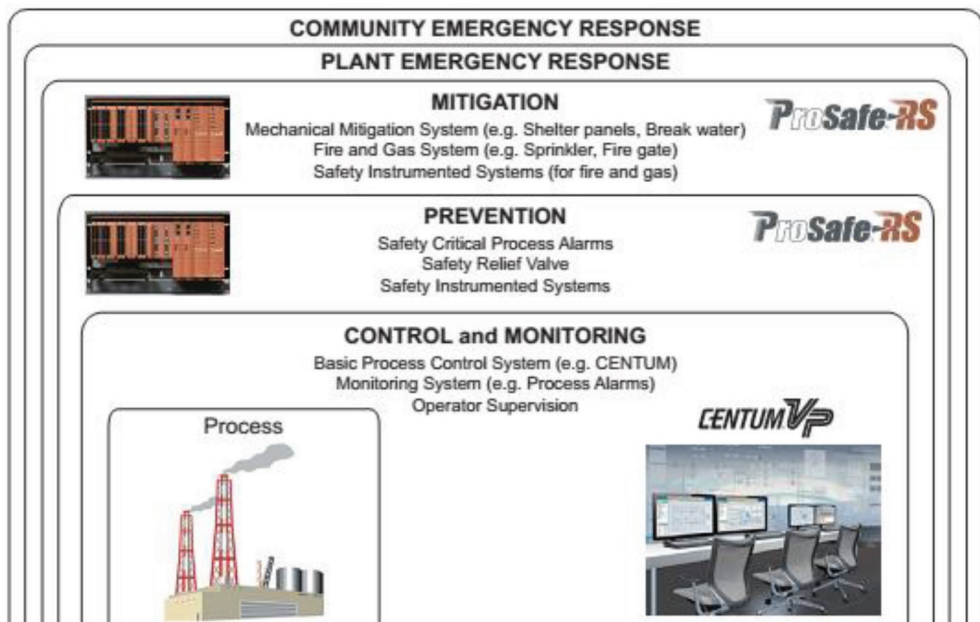


Figura 1 – Seguridad funcional. Protección por capas (Yokogawa Electric Corporation, 2016).

3. Estrategia de Ciberseguridad

Para la protección del SCI de la planta Cloro-Sosa se determina seguir las recomendaciones del Instituto nacional de estándares y tecnologías (NIST) (Stouffer et al., 2015) implementando una estrategia de defensa en profundidad con los siguientes elementos claves:

1. Evaluación de riesgos.
2. Protección Física.
3. Separación de redes.
4. Protección del Perímetro.
5. Endurecimiento de los dispositivos.
6. Monitoreo y Actualizaciones.
7. Manejo de Vendedores.
8. Factor Humano. Entrenamiento y Capacitación.

3.1. Evaluación de riesgos.

El riesgo, es un valor que combina el impacto (Consecuencia) que produciría el deterioro o pérdida de un activo (o grupo de activos), junto con la probabilidad de que una vulnerabilidad existente en el activo sea explotada por una amenaza (Centro de Ciberseguridad Industrial, 2016).

Activos

Primeramente, se realiza un levantamiento detallado de los activos del Sistema de Control, considerándose como activos los siguientes elementos:

- Instrumentos y actuadores de campo. Transmisores de presión, flujo, etc., así como válvulas de control y variadores de frecuencia.
- Controladores. PLC, RTU o dispositivos electrónicos inteligentes.
- Interfaces Hombre-Máquina. Paneles de operación y consolas de operación.
- Lógica en ejecución en los controladores. Programas de usuario de los PLC.
- Equipos del proceso.
- Información del proceso. Planos eléctricos, diagramas de instrumentación y tuberías, etc.
- Elementos de redes y comunicación.
- Personal.

Evaluación de Vulnerabilidades

Las vulnerabilidades son evaluadas para cada activo del SCI. Se tienen en cuenta factores físicos, como el grado de protección IP, si están expuesto a los elementos naturales, el acceso a la manipulación del activo o cuestiones desde el punto de vista de software.

Las vulnerabilidades se pueden agrupar en las siguientes categorías (Stouffer et al, 2015):

- Políticas y Procedimientos
- Arquitectura y Diseño.
- Configuración y Mantenimiento.
- Físicas.

- Software
- Redes y Comunicaciones.

Las vulnerabilidades específicas de diferentes fabricantes se pueden encontrar en sus sitios oficiales o en sitios de los diferentes CERT de seguridad industrial.

Yokogawa:

<https://www.yokogawa.com/library/resources/white-papers/yokogawa-security-advisory-report-list/>

ICS-CERT Estados Unidos: <https://ics-cert.us-cert.gov/advisories>

La evaluación de la probabilidad de que la vulnerabilidad sea explotada se calcula de acuerdo a la Tabla 1 (Centro de Ciberseguridad Industrial, 2016).

Nivel	Descripcion
<i>Alta</i>	Es probable que la amenaza explote la vulnerabilidad durante el próximo año.
<i>Media</i>	Es probable que la amenaza explote la vulnerabilidad durante los próximos diez años.
<i>Baja</i>	Es poco probable que la amenaza explote la vulnerabilidad y no existen datos históricos de su ocurrencia.

Tabla 1 – Evaluación de probabilidad de ocurrencia

Evaluación de Consecuencias

Las consecuencias pueden dividirse en cuatro categorías principales (U.S. Department of Homeland Security, 2009b).

- Seguridad y Salud: Efecto sobre la vida humana y bienestar. Ejemplo fatalidades, heridas, lesiones etc.
- Económicas: Pérdidas económicas directas e indirectas. Ejemplo pérdidas de producción, reconstrucción de algún activo.
- Psicológicas: Efectos en la moral pública y en la confianza en las instituciones estatales.
- Gobierno/Misión: Impactos en la habilidad del gobierno o la industria de mantener el orden, suministrar servicios públicos esenciales, garantizar la salud pública y realizar misiones relacionadas con la seguridad nacional.

Se evalúan de acuerdo a la siguiente tabla.

Escenarios de Riesgo

Todos los riesgos son evaluados respecto a un escenario específico o grupo de escenarios. El escenario de riesgo debe responder a la pregunta: ¿El riesgo de qué? Todas las consecuencias, vulnerabilidades y amenazas estimadas son específicas al escenario de riesgo. El riesgo puede ser evaluado a un activo, red, sistema o una combinación de estos (U.S. Department of Homeland Security, 2009b).

Se crea una plantilla por cada escenario de riesgo que incluye el nombre del escenario, descripción, activos involucrados, probabilidad de ocurrencia de acuerdo a la Tabla 2

Categoría	Impacto Bajo	Impacto Medio	Impacto Alto
<i>Pérdidas Financieras</i>	Más de 10000 USD	Más de 100000 USD	Más de 1000000 USD
<i>Medio Ambiente</i>	Daño pequeño y contenido	Daño pequeño sin contención	Impacto severo a largo plazo en el entorno
<i>Interrupción de la producción</i>	más de 1 hora	más de 1 día	más de 7 días
<i>Imagen Pública</i>	N/A	Pérdida de confianza de los clientes	Daño a la Imagen de la Empresa
<i>Impacto nacional</i>	Pequeño impacto a un sector o servicios públicos	Impacto severo a un sector o servicios públicos	Impacto a múltiples sectores o interrupción grave de servicios público

Tabla 2 – Evaluación de Impacto o Consecuencia

aplicada a las vulnerabilidades identificadas en los activos involucrados en el escenario de riesgo, amenazas, evaluación del impacto de materializarse el escenario de acuerdo con la tabla 1, y por último una clasificación del riesgo de acuerdo a la tabla 3 (Centro de Ciberseguridad Industrial, 2016).

Categoría del Impacto			
Probabilidad	Alta	Media	Baja
Alta	Riesgo Alto	Riesgo Alto	Riesgo Medio
Media	Riesgo Alto	Riesgo Medio	Riesgo Bajo
Baja	Riesgo Medio	Riesgo Bajo	Riesgo Bajo

Tabla 3 – Evaluación del Escenario de Riesgo

Una vez identificados los escenarios de riesgos se procede a priorizar los esfuerzos de gestión de riesgos con respecto a los activos más significativos, para enfocar la planificación, aumentar la coordinación, la asignación efectiva de recursos y mejorar la gestión de incidentes, respuesta y restauración (U.S. Department of Homeland Security, 2009b).

Se definieron los siguientes órdenes de prioridades:

1. Seguridad funcional de la planta.
2. Continuidad del Proceso Productivo.
3. Servicios Auxiliares.

Equipo de respuesta a incidentes de seguridad (CSIRT)

Las acciones para mitigar el riesgo involucran medidas diseñadas a prevenir, determinar y mitigar las amenazas, reducir las vulnerabilidades, minimizar las consecuencias y habilitar una respuesta eficiente y restauración posterior a la ocurrencia de un incidente.

La capacidad de respuesta a incidentes debe incluir varios elementos proactivos como la prevención (U.S. Department of Homeland Security, 2009) y otros centrados en la gestión de los mismos, (contención, corrección, restauración y recuperación)

El primer paso es crear un equipo interno de respuesta a incidentes de seguridad, siguiendo las recomendaciones de (U.S. Department of Homeland Security, 2009) y los resultados de los análisis de (Muñoz et al, 2015).

El CSIRT de la planta tendrá el propósito de responder a la ocurrencia de un incidente, identificar impactos operacionales para la planta, reportar la ocurrencia de un incidente a los organismos de control, recopilar información forense para asistir análisis y acciones legales, restaurar el SCI después del incidente y crear y mantener un plan de respuesta incidentes.

El equipo debe estar compuesto por:

- Ingeniero en control de procesos: Es el experto en la arquitectura de control. Es capaz de determinar el impacto potencial de sacar un componente del SCI fuera de servicio.
- Administrador de red del SCI: Es una persona clave si el incidente involucra un ataque cibernético.
- Administrador del DCS: Es la persona que conoce los permisos de acceso al SCI de los diferentes usuarios, se encarga de servir de interface con los vendedores del DCS.
- Jefe de Seguridad y Protección de la empresa.
- Jefe de planta: Está facultado en la toma de decisiones involucradas en la interrupción de la producción de ser necesario como respuesta a un incidente.
- Especialista Legal: Es opcional, la asesoría legal es necesaria en varias áreas asegurando el cumplimiento con leyes y regulaciones nacionales.
- Especialista en Recursos Humanos: Tiene un papel en este equipo cuando un incidente involucra a un trabajador de la planta, y es el encargado de las medidas disciplinarias a aplicar.

3.2. Protección Física

Las medidas de protección físicas están encaminadas a prevenir impactos indeseados en el SCI tales como:

- Acceso no autorizado a locales sensibles.
- Modificación, manipulación, robo o destrucción de dispositivos, interfaces de comunicación u otros activos.
- Observación no autorizada de documentación sensible, toma de fotografías, notas, etc.
- Introducción no autorizadas de nuevo hardware, como puntos de acceso inalámbricos y memorias USB.

Primeramente, se clasifican los locales con equipamiento del SCI en Áreas Limitadas, Restringidas o Estratégicas de acuerdo a la resolución 127/2007 del Ministerio de la Informática y las Comunicaciones y se implementan las medidas indicadas en esta resolución.

Áreas Limitadas:

- Sala de Control.
- Cuarto de Armarios del Rectificador.

- Cuarto de Racks de la planta de tratamiento de Agua.
- Subestación eléctrica media tensión.
- Subestación eléctrica baja tensión.

Áreas Restringidas:

- Sala de gabinetes del DCS/ESD.
- Armario del controlador de seguridad SCS0105 en la sala de celdas.
- Oficina de Estación de Ingeniería.

3.3.Separación de redes

La separación de la red de control con la red administrativa se realiza a través de una zona desmilitarizada (DMZ) implementada con dos cortafuegos de acuerdo a la Figura 2.

Los dispositivos compartidos se ubican en la DMZ, en el caso de la planta de ELQUIM están el servidor de datos históricos y un servidor ftp para la realización de salvadas de respaldo. El cortafuegos 2 protege tanto la DMZ como la red de control, mientras que el cortafuegos 1 protege la red de control de alguna estación comprometida de la DMZ.

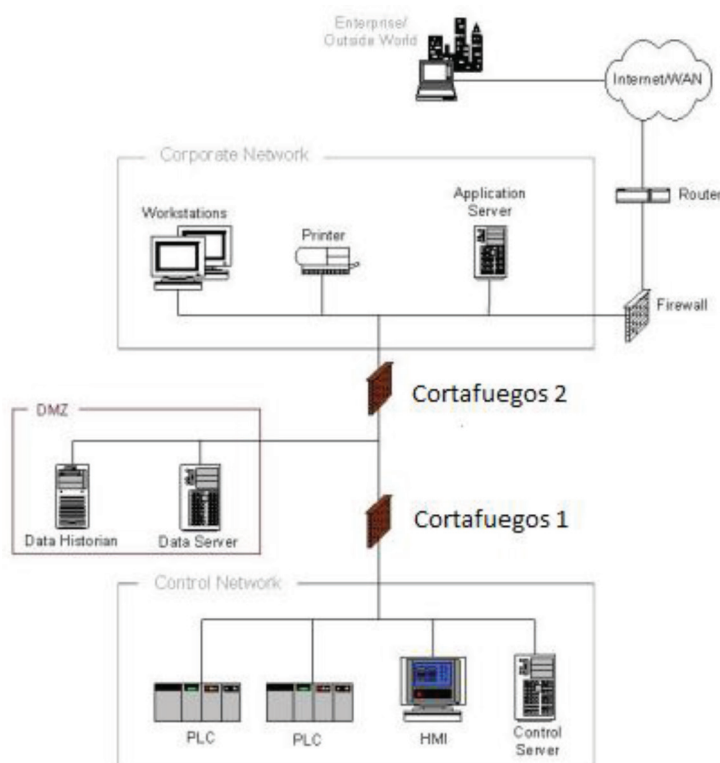


Figura 2 – Arquitectura de la DMZ entre la red de control y la red corporativa del ELQUIM

Esta configuración hace uso de cortafuegos de diferentes fabricantes, el cortafuegos 1 fue desarrollado por la empresa XETID y es administrado exclusivamente por esta, se instaló en el local de Racks del SCI.

El cortafuegos 2 fue implementado con un “dual-homed” PC y la distribución de Linux IPFire, fue configurado igualmente por la empresa XETID, pero su administración es asumida por el grupo de informática de la empresa ELQUIM.

3.4. Protección del Perímetro

La protección del perímetro del SCI incluye tanto la protección física, como la protección lógica para la protección de los activos. La protección lógica, incluye controles como mecanismos de autenticación, sistemas de detección y prevención de intrusos, listas de control de acceso y otros medios para proteger el sistema desde un punto de vista cibernético (ICS-CERT, 2016).

Reglas Generales para los cortafuegos

Un cortafuegos es solo tan efectivo, como la precisión de las reglas con las que está configurado (ICS-CERT, 2016). Las reglas de los cortafuegos 1 y 2 deben cumplir con las siguientes políticas generales.

- El tráfico de administración de los cortafuegos deberá realizarse sobre una conexión encriptada. El tráfico también deberá ser restringido por direcciones IP de estaciones específicas de administración. Cualquier otro tráfico dirigido al cortafuegos será bloqueado sin notificación. (Evita que el cortafuegos sea visible al escáner atacante).
- Bloquear cualquier tráfico de salida originado en el cortafuegos. (El cortafuegos no debe establecer ninguna conexión directa)
- Todo tráfico debe terminar en la DMZ.
- Todas las reglas de permitir, deben configurarse por dirección IP y puerto.
- Todo tráfico debe estar basado en protocolos enrutables TCP/IP o UDP/IP.
- Todo protocolo no IP deberá ser descartado.
- Todo protocolo permitido entre la red de control y la DMZ deberá estar denegado entre la DMZ y la red corporativa y viceversa.
- Los dispositivos de la red de control no deberán tener acceso a internet.
- La última regla es la regla por defecto y es siempre bloquear/denegar sin notificación cualquier tráfico que no esté explícitamente permitido por las reglas precedentes.

Cortafuegos 1.

El cortafuegos 1 además de cumplir con las políticas generales fue configurado teniendo en cuenta las siguientes reglas específicas:

Debe permitir la conexión del servidor de datos históricos en la DMZ hacia la estación de ingeniería, solamente a los puertos destinados para los servicios del DCOM especificados en la guía de seguridad de CENTUM VP, necesarios para la comunicación OPC.

El tráfico FTP estará restringido por el cortafuegos, solamente deberá permitir conexiones a los puertos configurados en el servidor FTP para el modo pasivo.

Los registros de este cortafuegos pueden ser auditados desde la estación de ingeniería por parte del equipo de administradores del SCI

Cortafuegos 2

Este cortafuegos solo permite el tráfico desde el servidor de datos de la red de gestión con destino al servidor de datos históricos que utiliza PostgreSQL.

Adicionalmente permite la administración remota desde la estación del especialista de seguridad informática de la empresa.

Sistema de detección y prevención de intrusos

Un IDS (Intrusion Detection System), es una herramienta de seguridad que actúa como un monitor del tráfico de red, describiendo y analizando ahora el contenido de los paquetes que ingresan a la organización. Sus principales funcionalidades son las siguientes (Miranda et al, 2016):

- Detectar ataques y otras violaciones de seguridad.
- Implementar calidad de control para eventos de seguridad y administración.
- Proporciona información acerca de los intrusos que intentan acceder a la red o sistemas.
- Previene problemas de comportamiento de abusos en el sistema o red.

Los IDS aportan a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa. Los SCI proveen una oportunidad única cuando se considera utilizar un IDS/IPS en la red, ya que, a pesar del tráfico considerable, este tráfico es muy predecible (ICS-CERT, 2016).

Se utiliza el IDS Snort que trae consigo la distribución de IPFire instalada en la estación del cortafuegos 2 para monitorear todo el tráfico dirigido a la DMZ desde la red de gestión.

3.5. Endurecimiento de los dispositivos

El endurecimiento de las medidas de seguridad para cada activo constituye una capa más en la estrategia de defensa en profundidad conocida como “device hardening”.

En las estaciones de trabajo por ejemplo deberán tomarse las siguientes medidas:

- Instalar y configurar un cortafuegos personal.
- Contraseñas personales e intransferibles con un mínimo de 8 o más caracteres, utilizando caracteres alfanuméricos y signos especiales.
- Configurar los registros de eventos.
- Software Antivirus
- Software de Lista Blanca.
- Deshabilitar cuentas de usuarios y servicios que no se utilizan, como email, multimedia, juegos.
- Reemplazar servicios inseguros como telnet por alternativas seguras como SSH.
- Inhabilitar puertos USB y torres de discos flexibles si existieran.

Endurecimiento de OPC

La comunicación con la red de gestión empresarial por parte del SCI se realiza a través de un servidor de datos OPC DA instalado en la estación de ingeniería.

A lo largo de su historia las implementaciones de llamadas de procedimientos remotos (Remote Procedure Call o RPC) han tenido pobres antecedentes relacionados con la seguridad. Dado que OPC está basado en la tecnología de DCOM de Microsoft y esta a su vez está basada en RPC, las estaciones con OPC son vulnerables a todas las banderas de pre-autenticación de RPC como las explotadas por el gusano Blaster en 2003. (Byres and Peterson, 2007a).

OPC DA le permite a un atacante no solo ganar acceso a datos de control del proceso, sino también modificar parámetros de ajustes en los controladores, valores de alarmas u otros parámetros de control.

Solo un parche agresivo de las estaciones OPC o el bloqueo de todo el tráfico OPC en el cortafuegos pueden mitigar el riesgo de estas vulnerabilidades (Byres and Peterson, 2007b).

Para manejar los riesgos asociados a OPC es necesaria una configuración cuidadosa de las cuentas de usuarios y poner restricciones en la configuración del DCOM. Primeramente, es necesario dar solo los permisos imprescindibles para los usuarios por cada objeto DCOM. Por ejemplo, si en una misma estación hay varios servidores OPC, pero solo uno necesita ser accedido remotamente, permitir entonces acceso únicamente a ese servidor, si todos los servidores y clientes OPC se encuentran en la misma estación entonces se inhabilita el acceso remoto en el DCOM (Byres and Peterson, 2007b).

En segundo lugar, es necesario el uso de diferentes cuentas de usuarios con diferentes privilegios. Solamente el usuario Ingeniero con privilegios de administración en la estación, será el único capaz de arrancar y configurar las aplicaciones OPC. La cuenta de Process_logger puede ser usada por usuarios que solamente necesitan conectarse y acceder a servidores OPC.

La configuración del DCOM, así como del cortafuegos personal de las estaciones de ingeniería y de operación se realiza a través de la herramienta IT Security Tools del propio Centum VP, evitando que se tenga que realizar de manera manual.

Adicionalmente a las medidas de fortalecimiento del DCOM, se configura en el DCS el usuario correspondiente a la conexión OPC, en función de los privilegios de este usuario es posible comandar la planta a través de OPC, o incluso pasar a manual lógicas de enclavamientos para que no se ejecuten.

Se configura por tanto el usuario OPC con el mismo nivel de seguridad que el usuario OFFUSER que es el usuario por defecto y tiene privilegios mínimos.

3.6.Actualizaciones

Aplicar los parches a un componente de SCI es un desafío para los administradores, debido a que los parches y actualizaciones pueden interferir con el funcionamiento del SCI (ICS-CERT, 2016).

La aplicación de parches solo deberá realizarse durante las paradas de plantas. No se realizará ninguna actualización del sistema operativo, solo se realizarán actualizaciones indicadas por el vendedor del SCI, de ser posible deberán probarse en una estación de prueba.

3.7. Manejo de Vendedores

Los vendedores presentan un caso especial de la estrategia de Defensa en Profundidad. En los últimos años los vendedores han tomado conciencia de la importancia de la ciberseguridad en las soluciones de control industrial y en muchos casos han incorporado seguridad en el ciclo de vida de sus productos.

Cadena de suministro

La cadena de suministro representa un riesgo significativo en los SCI; incluye inserción de falsificaciones o equipamiento no genuino, sabotajes e inserción de software malicioso (Boyens et al., 2015).

Se establece un programa de manejo de vendedores incluyendo por ejemplo reglas para solamente comprar directamente de fabricantes o sus distribuidores oficiales en Cuba.

Servicios Subcontratados

Es común que las organizaciones subcontraten servicios altamente especializados que utilizan poco frecuente o de los que carecen de personal calificado. Cuando se contrate a terceros para la realización de servicios, ambas partes deberán establecer y acordar reglas de contratación.

Las tareas de mantenimiento preventivo y correctivo por terceros al SCI siguen las siguientes reglas:

- Se deberán especificar cuáles actividades se van a realizar, en que sistema y quien va ser el encargado de realizarla.
- Solo se utilizarán los programadores de campo suministrado por ELQUIM. Bajo ningún concepto se utilizarán los dispositivos de terceros para conectarse con ningún activo de la red de control.

3.8. Factor Humano. Entrenamiento y Capacitación.

El manejo de recursos humanos dentro de los SCI presenta desafíos para la organización. Los SCI grandes y complejos son susceptibles a errores cometidos por personal inexperto y falta de entrenamiento, así como de actividades de personal malicioso dentro del SCI. Se deben diseñar procedimientos para establecer como el personal debe conducirse en un proceso particular o configurar un sistema, dichos procedimientos deberán servir para rápidamente entrenar al personal nuevo asegurándose que ellos siguen todas las regulaciones y estándares de operación del SCI. Los administradores del SCI se entrenarán en la instalación desde cero del sistema valiéndose de máquinas virtuales y ejercitándolo con una periodicidad de al menos una vez al año.

4. Conclusiones

El número de potenciales problemas de seguridad y sus riesgos asociados, aumenta con el crecimiento de la complejidad y la conectividad de los SCI con redes externas. La seguridad de los mismos debe ser tenida en cuenta durante la etapa de proyecto y deben ser utilizadas las soluciones tanto de hardware como de software del vendedor del SCI.

La estrategia implementada para la defensa en profundidad es de diseño inédito en el sector industrial cubano por lo que puede servir como guía para otras soluciones con sistemas similares.

En la estrategia se empleó hardware estándar de tecnologías de la información, así como software de producción nacional de la empresa XETID para la comunicación con el servidor OPC y software libre como Snort y PostgreSQL, todo esto permite asegurar la soberanía tecnológica de la solución.

Referencias

- Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8 53-66.
- Boyens, J., Moorthy, R., & Bartol, N. (2015). Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Special Publication 800-161. [Internet]. Retrieved from: <http://dx.doi.org/10.6028/NIST.SP.800-161>
- Byres, E., & Peterson, D. (2007a). OPC Security White Paper #2 OPC Exposed. Lantzville: Byres Research
- Byres, E., & Peterson, D. (2007b). OPC Security White Paper #3 Hardening Guidelines for OPC Hosts. Lantzville: Byres Research
- CCN-CERT (2016). Amenazas y análisis de riesgos en Sistemas de Control Industrial (ICS). [Internet]. Retrieved from: <https://www.ccn-cert.cni.es/gl/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-publicos/1381-ccn-cert-ia-04-16-amenazas-y-analisis-de-riesgos-en-sistemas-de-control-industrial-ics/file.html>
- Centro de Ciberseguridad Industrial. (2016). Guía para la construcción de un sgci. Sistema de gestión de la ciberseguridad industrial. Madrid: Centro de Ciberseguridad Industrial. 1ra edición. ISBN: 978-84-942379-8-0
- ICS-CERT. (2016). Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability. [Internet]. Retrieved from: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICSCERT_Defense_in_Depth_2016_S508C.pdf
- Maglaras, L.A., Kim, K.-H., Janicke, H., Ferrag, M.A., Rallis, S., Fragkou, P., ...& Cruz, T.J. (2018). Cyber security of critical infrastructures. *ICT Express* 4(1) 42-45.
- Ministerio de la Informática y la Comunicaciones (2007). Resolución No 127/2007. Gaceta Oficial de la República de Cuba 57, 899 – 910.

- Miranda, J.M., & Ramirez, H. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (17), 1-15. doi: 10.17013/risti.17.1-15
- Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (E3), 1-15. doi: 10.17013/risti.e3.1-15
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82. [Internet]. Retrieved from: <http://dx.doi.org/10.6028/NIST.SP.800-82r2>
- U.S. Department of Homeland Security. (2009). Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability. [Internet]. Retrieved from: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf
- U.S. Department of Homeland Security. (2009b). National Infrastructure Protection Plan: Partnering to enhance protection and resiliency. [Internet]. Retrieved from: https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
- Yokogawa Electric Corporation. (2015). Integrated Production Control System CENTUM VP System Overview (General Overview). Tokyo: Yokogawa Electric Corporation.
- Yokogawa Electric Corporation. (2016). Safety Instrumented System ProSafe-RS System Overview. Tokyo: Yokogawa Electric Corporation.

KE-SER: Un sistema basado en el conocimiento y la experiencia para dar soporte a arquitectos de software en aspectos de seguridad

María Celeste Carignano¹, Silvio Gonnet^{1,2}, Horacio Leone^{1,2}

mcarigna@frsf.utn.edu.ar, sgonnet@santafe-conicet.gov.ar, hleone@santafe-conicet.gov.ar

¹ Universidad Tecnológica Nacional – Facultad Regional Santa Fe, Santa Fe, CP: 3000, Santa Fe, Argentina.

² INGAR – Instituto de Desarrollo y Diseño, CONICET-UTN, Santa Fe, CP: 3000, Santa Fe, Argentina.

DOI: 10.17013/risti.32.97–112

Resumen: En la actualidad, las organizaciones están expuestas a ataques cada vez más sofisticados, cuyo objetivo es comprometer o corromper la integridad, confidencialidad y disponibilidad de la información que manejan. La mayoría de los ataques, internos o externos, explotan vulnerabilidades de seguridad, las cuales pueden tener su origen en el desarrollo de los sistemas de software que emplean las organizaciones. Desarrollar sistemas que contemplen aspectos de seguridad es fundamental para disminuir las vulnerabilidades que exponen a las organizaciones. Sin embargo, las compañías de software pocas veces cuentan con expertos en seguridad que las asesoren a lo largo del ciclo de vida del desarrollo de software. En este trabajo se propone un sistema experto para brindar apoyo, desde el punto de vista de la seguridad, en una de las principales actividades del desarrollo como es el diseño arquitectónico.

Palabras-clave: sistema experto, seguridad, arquitectura de software, diseño, conocimiento.

KE-SER: A system based on knowledge and experience to support software architects in security aspects

Abstract: Nowadays, the organizations are exposed to increasingly sophisticated attacks, whose objective is to compromise or corrupt the integrity, confidentiality and availability of the information they handle. Most attacks exploit security vulnerabilities. The origin of these vulnerabilities can be in the development of the software systems that organizations employ. In order to reduce these vulnerabilities, it is fundamental to develop systems dealing with security aspects. However, software companies rarely have security experts to advise them throughout the software development life cycle. This paper proposes an expert system to provide support, from the point of view of security, in one of the main development activities such as architectural design.

Keywords: expert systems, security, software architecture, design, knowledge.

1. Introducción

La información siempre ha sido un recurso valioso para las organizaciones. En las últimas décadas, los avances tecnológicos han revolucionado la forma en la que se obtiene, procesa, comunica y almacena la información dentro y fuera de las organizaciones, generando ventajas competitivas y numerosos beneficios (Mejía & Muñoz, 2017). Sin embargo, estos avances también han colaborado con la aparición de ataques cada vez más sofisticados, cuyo objetivo es comprometer o corromper la integridad, confidencialidad y disponibilidad de la información que manejan dichas organizaciones.

La mayoría de los ataques, internos o externos, explotan vulnerabilidades de seguridad (Zambrano, Guarda, Valenzuela, & Quiña, 2019). La base de datos “*Common Vulnerabilities and Exposures*” (CVE, 2019) es una lista de vulnerabilidades y exposiciones de ciberseguridad divulgadas públicamente, ampliamente reconocida por la comunidad internacional de ciberseguridad, que define a una vulnerabilidad como:

una debilidad en la lógica computacional (por ejemplo, el código) que se encuentra en el software y algunos componentes de hardware (por ejemplo, el firmware) que, cuando se explota, produce un impacto negativo en la confidencialidad, la integridad o la disponibilidad. La mitigación de las vulnerabilidades en este contexto implica cambios en la codificación, pero también podría incluir cambios en las especificaciones o incluso la eliminación de las especificaciones (por ejemplo, la eliminación de los protocolos o la funcionalidad afectados en su totalidad).

Teniendo en cuenta esto, resulta evidente la importancia de contemplar aspectos de seguridad durante el ciclo de vida del desarrollo de software (SDLC por sus siglas en inglés: “*Software Development Life Cycle*”) con el objetivo de eliminar o disminuir las vulnerabilidades que podrían ser aprovechadas durante su ejecución. Cuanto más tarde se detecte el origen de una vulnerabilidad, mayor será el costo de su corrección y las consecuencias pueden llegar a ser catastróficas. Ejemplos de ello son los problemas ocasionados por los ataques “*Ransomware*” en la actualidad (Winkler & Treu Gomes, 2017).

Las mejores prácticas de desarrollo de software sugieren integrar los aspectos de seguridad en cada fase del SDLC. Existen varios enfoques que así lo proponen, como ser: Software Assurance Maturity Model (SAMM, 2019) de la organización Open Web Application Security Project (OWASP, 2019), Touchpoints de McGraw (MacGraw, 2006) y Security Development Lifecycle (SDL, 2019) de Microsoft, entre otros. Análisis comparativos de algunos de estos enfoques, o, en el caso de SAAM de su predecesor, pueden encontrarse en los trabajos de: De Win, Scandariato, Buyens, Grégoire, & Joosen (2009) y Mohammad, Alqatawna, & Abushariah (2017).

Sin embargo, las compañías de desarrollo de software no suelen contemplar la seguridad en el SDLC debido a que consideran que es muy costosa, que requiere de mucho tiempo y que no están suficientemente capacitadas para su realización, ya que, generalmente, no cuentan con expertos en seguridad entre sus miembros (Mohammad, Alqatawna, & Abushariah, 2017). En este contexto surge la motivación que da origen a la propuesta presentada en este trabajo.

Durante el diseño arquitectónico se toman las primeras decisiones de diseño que permiten establecer las bases para construir una solución de software que satisfaga los requerimientos de los stakeholders de un sistema (Bass, Clements, & Kazman, 2013; Clements, et al., 2010). Entre los requerimientos a satisfacer, se encuentran los requerimientos de seguridad. Estas decisiones tempranas son las más difíciles de corregir, las más difíciles de cambiar posteriormente en el SDLC, y tienen los efectos de mayor alcance (Bass, Clements, & Kazman, 2013). Por consiguiente, si los requerimientos de seguridad no son tenidos en cuenta de manera apropiada durante el diseño arquitectónico, el sistema resultante puede presentar vulnerabilidades que pongan en riesgo la seguridad del sistema desarrollado y la información de la organización que lo ejecuta.

Es por este motivo que se considera necesario brindar apoyo a los arquitectos de software para que puedan tomar decisiones durante el diseño arquitectónico de forma consciente e informada. En este trabajo, se describe un sistema capaz de realizar recomendaciones para satisfacer los requerimientos de seguridad de los sistemas a construir. Las recomendaciones pueden estar basadas en el conocimiento capturado de expertos en seguridad o en experiencias pasadas de arquitectos que diseñaron arquitecturas de sistemas con requerimientos similares.

A continuación, se presenta la propuesta con mayor nivel de detalle. En la sección 2, se describen las principales características del sistema experto, llamado KE-SER por sus siglas en inglés: “*Knowledge & Experience – SEcurity Recommendations*”. En la sección 3, se profundizan los principales componentes de KE-SER. Luego, en la sección 4, se analizan los resultados de una evaluación del sistema experto propuesto. En la sección 6, se contextualiza la propuesta con referencia a trabajos relacionados. Finalmente, en la sección 5, se presentan las conclusiones y trabajos futuros.

2. KE-SER: conocimiento y experiencia

Los sistemas expertos cobran importancia y utilidad en aquellos dominios en los que resulta difícil y costoso disponer de expertos humanos para realizar consultas de manera personal, ilimitada e instantánea (Gupta & Singhal, 2013). Las compañías de desarrollo de software generalmente no cuentan con expertos en seguridad entre sus miembros (Mohammad, Alqatawna, & Abushariah, 2017), por lo que KE-SER puede ser de gran valor.

KE-SER es un sistema basado en el conocimiento y la experiencia que tiene como objetivo brindar soporte a los arquitectos de software en el proceso de diseño arquitectónico contemplando aspectos de seguridad. Los componentes de este sistema se presentan en la Fig. 1.

Los objetivos de KE-SER incluyen:

- responder a las consultas que podría realizar un arquitecto de software a un experto en seguridad para resolver los requerimientos de los stakeholders de los sistemas de software que deben ser construidos; y
- recordar las soluciones empleadas en el pasado para poder aplicarlas en el diseño de nuevas arquitecturas.

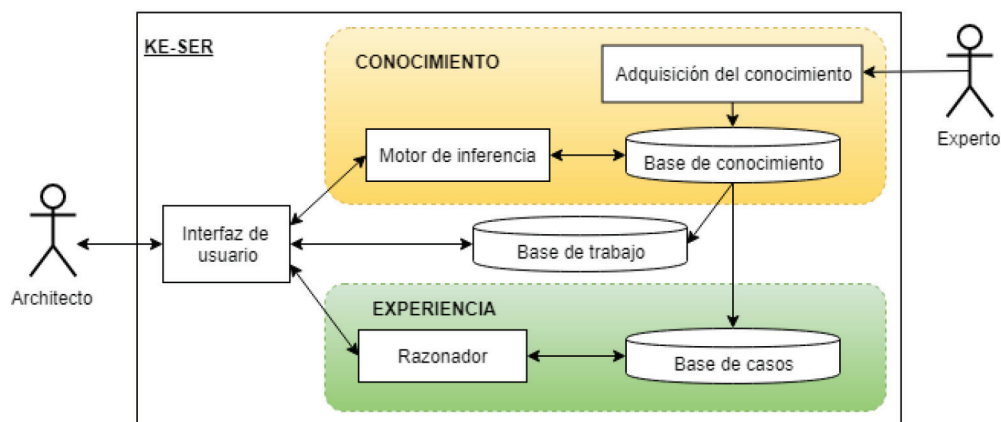


Figura 1 – Componentes de KE-SER

Para cumplir con el objetivo *I*) KE-SER emplea los componentes asociados al *CONOCIMIENTO* (en Fig. 1), y para cumplir con el objetivo *II*) KE-SER utiliza los componentes asociados a la *EXPERIENCIA* (en Fig. 1).

El sistema intenta ofrecer recomendaciones o consejos sobre seguridad ante preguntas como las siguientes: ¿Cuáles serían los aspectos a tener en cuenta para evitar el acceso no autorizado de individuos? ¿Cómo evitar que usuarios sin privilegios modifiquen los datos? ¿Cómo almacenar los datos para que no puedan ser leídos por personas ajenas al sistema? ¿Cuáles son los aspectos de seguridad que deberían ser tenidos en cuenta en aplicaciones como la que se está diseñando? ¿Cómo se diseñó la solución para un requerimiento de autenticación en aplicaciones anteriores?

Cabe destacar que KE-SER solo ofrece recomendaciones, con el objetivo de brindar información a los arquitectos de software para que tomen mejores decisiones durante el diseño arquitectónico, pero no ejecuta o genera ninguna decisión de manera automática.

La información que gestiona KE-SER está distribuida en tres bases de datos:

- La **Base de Conocimiento**, la cual contiene el conocimiento de los expertos en seguridad. El conocimiento está distribuido en objetos y su estructura se describe, mediante un diagrama de clases, en la sección 2.1.
- La **Base de trabajo**, la cual contiene la información de los sistemas que se están diseñando. En la sección 2.2 se describe la información que almacena esta base de datos.
- La **Base de Casos**, la cual contiene información sobre experiencias de diseño arquitectónico pasadas. Estas experiencias están representadas por casos y su estructura se describe, mediante diagramas de clases, en la sección 2.3.

El experto interactúa con KE-SER mediante el componente de **Adquisición de conocimiento**, el cual permite que el experto vuelque sus conocimientos en el sistema.

Para responder consultas tomando como base el conocimiento, se emplea el **Motor de Inferencia**, el cual simula, mediante un conjunto de algoritmos, la estrategia de resolución de problemas de un experto. En cambio, para responder consultas tomando como base la experiencia, se utiliza el **Razonador**, el cual utiliza razonamiento basado en casos para proponer estrategias de resolución basadas en el recuerdo de experiencias pasadas similares.

A partir del sistema experto propuesto, se ha construido una versión prototípica de una herramienta, llamada KE-T. KE-T ha sido implementada en JAVA (JAVA, 2019) como un complemento (*plug-in*) de Eclipse (Eclipse, 2019) utilizando SWT (siglas en inglés de Standard Widget Toolkit (SWT, 2019)) para construir la interfaz gráfica de la aplicación. Por restricciones en la longitud del trabajo no se presentará una descripción detallada de la misma. Pero resulta importante destacar, que ni el sistema experto, ni la herramienta presentada, pretenden automatizar el trabajo de los arquitectos, sino que el objetivo es brindar información que les permita tomar mejores decisiones durante el diseño de una arquitectura.

3. KE-SER: componentes

A continuación, se describen con mayor profundidad cada uno de estos componentes del sistema experto KE-SER.

3.1. Componentes asociados al conocimiento.

Los componentes asociados al conocimiento tienen como responsabilidad ofrecer recomendaciones a los arquitectos para que puedan resolver los requerimientos de seguridad de un sistema en particular. Con este fin, KE-SER mantiene una base de conocimiento (ver Fig. 1) que contiene el conocimiento volcado previamente por expertos en seguridad. La representación del conocimiento de los expertos se muestra en el diagrama de clases de la Fig. 2.

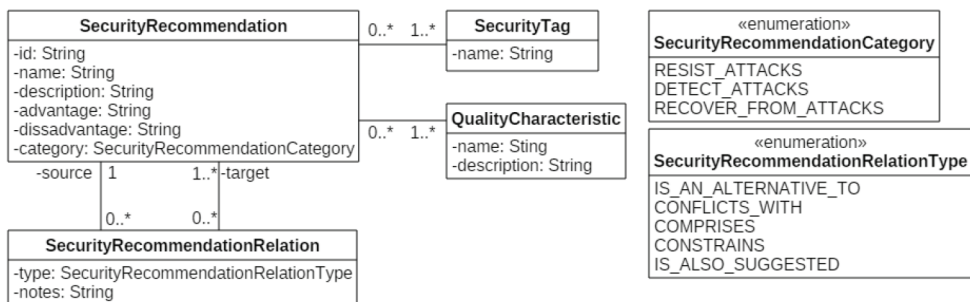


Figura 2 – Base de conocimiento de KE-SER

Las instancias de la clase *SecurityRecommendation* (ver Fig. 2) describen recomendaciones de seguridad que pueden ser útiles durante el diseño arquitectónico de un sistema. Ejemplos de recomendaciones son tácticas arquitectónicas, algoritmos específicos, o componentes arquitectónicos.

En general, las recomendaciones persiguen un objetivo específico, el cual puede ser resistir ataques de terceros, detectar ataques o recuperarse de ataques efectuados. La categoría de las recomendaciones (atributo *category* de *SecurityRecommendation* en Fig. 2) permite establecer los objetivos de cada recomendación documentada.

Además, los expertos deben proporcionar datos sobre las recomendaciones documentadas que permitan clasificarlas y recuperarlas. Un dato necesario es la característica de calidad que puede asociarse a cada recomendación (instancia de *QualityCharacteristic* en Fig. 2). Ejemplos de características de calidad están dados en la norma ISO/IEC 25010 (ISO 25010, 2011), como ser: confidencialidad, integridad, no-repudio, responsabilidad, y autenticidad; o en el trabajo de Bass, Clements & Kazman (2013): no-repudio, confidencialidad, integridad, garantía, disponibilidad, y auditoría. La restante información de clasificación puede ser documentada como etiquetas de la recomendación (instancias de *SecurityTag* en Fig. 2).

Un ejemplo de recomendación de seguridad podría ser el siguiente:

- **ID:** SR-AIC
- **Name:** Autenticar usuarios por medio de identificador y contraseña
- **Description:** La autenticación es el proceso de validar la identidad de un usuario, en este caso, mediante un ID de usuario y una contraseña.
- **Advantage:** Fácil de implementar. Bajo costo. Fácil de utilizar
- **Dissadvantage:** El nivel de seguridad depende directamente de la complejidad de la contraseña. Contraseñas simples o débiles son fáciles de adivinar o inventar. Contraseñas demasiado complejas conducen a los usuarios a aplicar estrategias para gestionarlas que no siempre son correctas. Proporcionar una contraseña correcta no prueba que una persona es quien dice ser.
- **Quality Characteristic:** Autenticidad
- **Category:** RESIST ATTACKS
- **Security Tags:** Autenticación, Usuario, Password, Contraseña, Identificador, Nombre de usuario

Otros ejemplos de recomendaciones pueden observarse en la Tabla 1.

Las recomendaciones presentadas en la Tabla 1 forman parte de una vista parcial de una base de conocimiento construida con fines prácticos. Algunas de las fuentes de información formales consultadas para confeccionar la base de conocimiento fueron: Bass, Clements & Kazman (2013) y Johnsson, Deogun, & Sawano (2019). También fueron consultados sitios web y expertos en seguridad. Por cuestiones de extensión no se detalla la descripción, ventajas y desventajas de las recomendaciones presentadas.

Finalmente, los expertos pueden indicar si existe algún tipo de relación que vincula varias recomendaciones (*SecurityRecommendationRelation* en Fig. 2). Sin embargo, por limitaciones en la extensión del trabajo no serán abordadas en esta presentación.

3.2. Soluciones en producción

En el presente trabajo no se prescribe cómo debe ser documentada la arquitectura de software a diseñar. Solo se establece la necesidad de capturar información de dos

ID	Name	Quality Characteristic	Category	SecurityTag
SR-AIC	<i>Autenticar usuarios por medio de identificador y contraseña</i>	Autenticidad	RESIST ATTACKS	Autenticación, Usuario, Password, Contraseña, Identificador, Nombre de usuario
SR-AIB	<i>Autenticar usuarios por medio de identificaciones biométricas</i>	Autenticidad	RESIST ATTACKS	Autenticación, Usuario, Biométricas, Biometría
SR-AMF	<i>Autenticar usuarios por medio de múltiples factores</i>	Autenticidad	RESIST ATTACKS	Autenticación, Usuario, Biométricas, Biometría, Password, Contraseña, Identificador
SR-AT	<i>Mantener un “audit trail”.</i>	Disponibilidad Auditoría No-repudio	RECOVER FROM ATTACKS	Audit trail, Log
SR-CD	<i>Mantener la confidencialidad de los datos</i>	Confidencialidad	RESIST ATTACKS	Datos, Protección, Acceso, Encriptar, Encriptación, Canales de comunicación, VPN, SSL

Tabla 1 – Ejemplos de recomendaciones

elementos: los intereses de los stakeholders y las decisiones de diseño de los arquitectos, ambos referidos con aspectos de seguridad de los sistemas de software a diseñar.

La información de seguridad relacionada con los sistemas que se están diseñando es almacenada en la **base de trabajo**. En la Fig. 3 se presenta la estructura de los conceptos involucrados en el diseño arquitectónico desde la perspectiva de la seguridad.

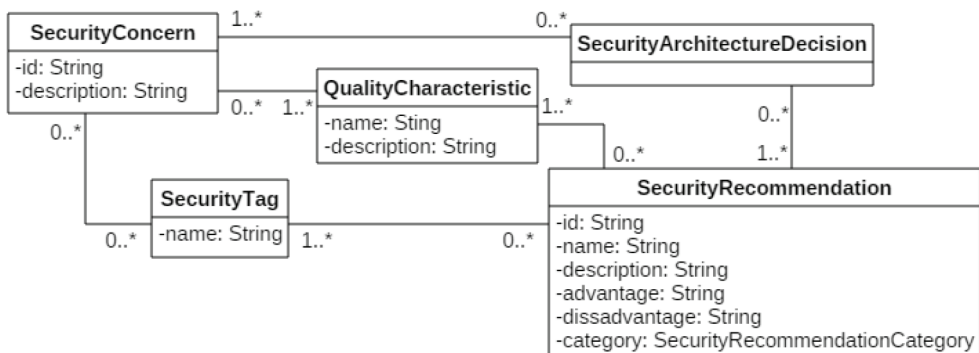


Figura 3 – Conceptos de KE-SER

Los intereses de los stakeholders referidos a seguridad están representados mediante la clase *SecurityConcern* (ver Fig. 3). Cada interés de seguridad se categoriza mediante las características de seguridad asociadas y las etiquetas de seguridad identificadas.

De esta forma, si un *stakeholder* expresa un interés expresado de la siguiente forma: “Se deberá dejar registrado todo intento de acceder al sistema con un nombre de usuario no existente”, puede ser documentado como se muestra en la Tabla 2.

Las decisiones tomadas por los arquitectos, para satisfacer los intereses de seguridad, son documentadas mediante objetos de tipo *SecurityArchitectureDecision* (ver Fig. 3). Dichas decisiones pueden involucrar la adopción de una o más recomendaciones brindadas por el sistema experto (*SecurityRecommendation* en Fig. 3).

ID	Description	Quality Characteristic	SecurityTag
SC01	Se deberá dejar registrado todo intento de acceder al sistema con un nombre de usuario no existente	Autenticidad Auditoría	Autenticación. Usuario no autorizado, Nombre de usuario, Audit trail, Log

Tabla 2 – Ejemplo de instancia de *SecurityConcern*

Teniendo en cuenta las recomendaciones presentadas en la Tabla 1, y el interés de seguridad descrito en la Tabla 2, las decisiones de diseño tomadas podrían ser las mostradas en la Tabla 3.

SecurityConcern		SecurityRecommendation	
ID	Description	ID	Description
SC01	Se deberá dejar registrado todo intento de acceder al sistema por parte de un usuario no autorizado	SR-AIC	Autenticar usuarios por medio de identificador y contraseña
		SR-AT	Mantener un “audit trail”

Tabla 3 – Ejemplo de instancia de *SecurityArchitectureDecision*

3.3. Componentes asociados a la experiencia

Los componentes asociados a la experiencia tienen como responsabilidad recuperar las soluciones de seguridad empleadas en el pasado para proponerlas a los arquitectos durante el diseño de nuevas arquitecturas. Para ello KE-SER aplica razonamiento basado en casos (CBR, por sus siglas en inglés *Case-based reasoning*). Razonamiento Basado en Casos es un paradigma de resolución de problemas (Aamodt & Plaza, 1994) que involucra el uso de experiencias pasadas para comprender y resolver nuevas situaciones (Kolodner, 1992). Un **caso** denota una situación experimentada previamente, que ha sido capturada y aprendida de forma tal que puede ser reutilizada en la resolución de problemas futuros (Aamodt & Plaza, 1994). Suele estar compuesto por el *problema*, que describe el estado del mundo cuando ocurre el caso; y la *solución*, que establece la solución encontrada (Watson & Marir, 1994).

En el contexto de este trabajo, un caso describe las decisiones de diseño tomadas durante la definición de una arquitectura de software que involucran aspectos de seguridad y es llamado **caso arquitectónico de seguridad**. En la Fig. 4 se presenta la estructura definida para los casos *arquitectónicos de seguridad*.

Un *caso arquitectónico de seguridad* es representado mediante la clase *SecurityArchitectureCase* (ver Fig. 4). El *problema* (*ProblemDescription* en Fig. 4) está definido en función de los intereses de seguridad de los stakeholders (*SecurityConcern*

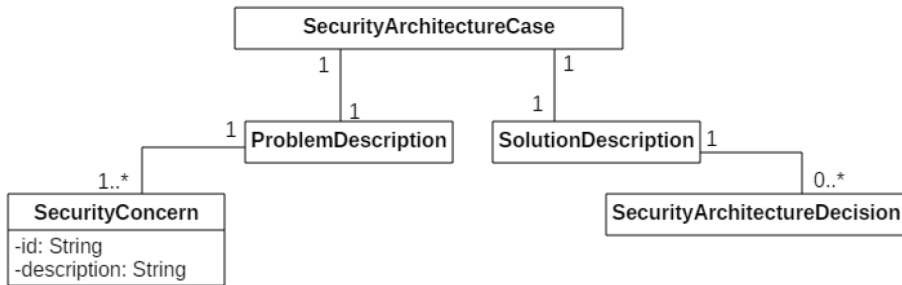


Figura 4 – Estructura de un caso arquitectónico

en Fig. 4) y la solución (*SolutionDescription* en Fig. 4) se compone de decisiones de diseño (*SecurityArchitectureDecision* en Fig. 4) tomadas por los arquitectos de software aceptando recomendaciones de diseño propuestas.

Los *casos arquitectónicos de seguridad* se almacenan en la base de casos (ver Fig. 1) y contienen la información de los sistemas que se encontraban en la base de trabajo, una vez que se finaliza con el diseño de su arquitectura.

3.4. Motor de inferencia

El motor de inferencia simula la estrategia de resolución de problemas de un experto. Para ello ejecuta un proceso que tiene como entrada un conjunto de intereses de seguridad (instancias de *SecurityConcern*) del sistema a construir y como salida cero o más recomendaciones de seguridad (instancias de *SecurityRecommendation*) para cada uno de los intereses de entrada. La cantidad de recomendaciones propuestas dependerá de la información almacenada en la base de conocimiento y de la calidad descriptiva de las etiquetas de seguridad empleadas en la definición de los intereses de seguridad y las recomendaciones de seguridad.

El proceso de inferencia analiza cada uno de los intereses de seguridad de entrada (llamado *ISE*) aplicando la siguiente regla:

SI (existe un conjunto de recomendaciones de seguridad, llamado *CR*, que poseen características de calidad (instancias de *QualityCharacteristic*) comunes con *ISE* y también poseen etiquetas de seguridad (instancias de *SecurityTag*) comunes con *ISE*) **ENTONCES** proponer las recomendaciones del conjunto *CR* para el interés de seguridad *ISE*.

Una vez finalizado el procesamiento de todos los intereses de seguridad del conjunto de entrada, se presentan al arquitecto las recomendaciones de seguridad obtenidas para cada uno de ellos.

Para determinar si una recomendación de seguridad (llamada *RS*) posee características de calidad comunes con un interés de seguridad (llamado *IS*), el sistema experto realiza el siguiente cálculo (I):

$ \begin{aligned} &CIS = \text{características de calidad de } \mathbf{IS} \\ &CR = \text{características de calidad asociadas a } \mathbf{RS} \\ &IC = \text{intersección de } CIS \text{ y } CR \\ &X = \text{cantidad de características en } IC / \text{cantidad de características en } CIS \end{aligned} $	(I)
---	-----

Si $X > U_C$ entonces se considera que **RS** posee características de calidad comunes con **IS**, en donde U_C es un valor umbral previamente establecido que indica un límite inferior de inclusión de las recomendaciones.

Por otro lado, para determinar si una recomendación de seguridad (llamada **RS**) posee etiquetas de seguridad comunes con un interés de seguridad (llamado **IS**), el sistema experto realiza el siguiente cálculo (II):

$ \begin{aligned} &EIS = \text{etiquetas de seguridad de } \mathbf{IS} \\ &ER = \text{etiquetas de seguridad asociadas a } \mathbf{RS} \\ &IE = \text{intersección de } EIS \text{ y } ER \\ &Y = \text{cantidad de etiquetas en } IE / \text{cantidad de etiquetas de } EIS \end{aligned} $	(II)
---	------

Si $Y > U_E$ entonces se considera que **RS** posee etiquetas de seguridad comunes con **IS**, en donde U_E es un valor umbral previamente establecido que indica un límite inferior de inclusión de las recomendaciones.

3.5. Razonador

El **Razonador** utiliza razonamiento basado en casos para proponer recomendaciones de seguridad basadas en el recuerdo de experiencias pasadas similares. Ante la descripción de los intereses de seguridad (instancias *SecurityConcern*) del sistema a ser diseñado, se recuperan de la base de casos aquellos *casos arquitectónicos de seguridad* (instancias de *SecurityArchitectureCase*) que tienen intereses similares y se proponen para el nuevo diseño arquitectónico las recomendaciones de seguridad consideradas en dichos casos.

Para esto, KE-SER recorre todos los casos de la *base de casos*, calculando para cada uno de ellos el porcentaje de intereses de seguridad del sistema a construir que tienen similitud con los intereses del caso que está siendo analizado. Aquellos casos, cuyo porcentaje supera un valor umbral previamente establecido (llamado U_I), pasan a formar parte del conjunto de casos recuperados.

Como resultado, el arquitecto puede consultar para cada uno de los casos recuperados cuáles fueron las recomendaciones que se siguieron para satisfacer los intereses de seguridad que son similares a los intereses del sistema a construir.

Para establecer si dos intereses de seguridad son similares (llamando **ISS** al interés de seguridad del sistema a construir y **ISC** al interés de seguridad del caso de seguridad arquitectónico), se tienen en cuenta los siguientes aspectos:

Por un lado, las características de calidad de ambos intereses, realizando el cálculo presentado en (III):

CIS_1 = características de calidad de ISS CIS_2 = características de calidad de ISC IC = intersección de CIS_1 y CIS_2 X = cantidad de características en IC /cantidad de características de CIS_1	(III)
--	-------

Por el otro, las etiquetas de seguridad de ambos intereses, realizando el cálculo presentado en (IV):

EIS_1 = etiquetas de seguridad de ISS EIS_2 = etiquetas de seguridad de ISC IE = intersección de EIS_1 y EIS_2 Y = cantidad de etiquetas en IE /cantidad de etiquetas de EIS_1	(IV)
--	------

De esta forma, si **ISC** cumple con la restricción presentada en (V) pasa a ser considerado por KE-SER como similar a **ISS**, por lo que las recomendaciones de seguridad contempladas al momento de resolver a **ISC** serán propuestas al arquitecto para resolver a **ISS**.

$X > U_IC \ \& \ Y > U_IE$	(V)
------------------------------	-----

En donde U_IC y U_IE son valores umbrales previamente establecidos.

4. Evaluación y resultados

Para realizar la evaluación del modelo propuesto se utilizó un dataset público llamado PROMISE (PROMISE, 2019). Este dataset consta de 625 sentencias de requerimientos que pertenecen a 15 proyectos de desarrollo, de las cuales 66 corresponden a requerimientos de seguridad. En la evaluación se tuvieron en cuenta 57 sentencias de requerimientos de seguridad, debido a que 9 fueron descartadas por considerarse mal clasificadas o por carecer de suficiente información como para trabajar con ellas. Las sentencias de requerimientos de seguridad fueron consideradas como intereses de seguridad (instancias de *SecurityConcern* en Fig. 3).

La evaluación se llevó a cabo en tres pasos: 1) se clasificaron los intereses de calidad (asociándolos a instancias de *QualityCharacteristic*); 2) se etiquetaron los intereses de seguridad (asociándolos a instancias de *SecurityTag*); y 3) se empleó KE-SER para recuperar recomendaciones de seguridad.

En la Tabla 4 se presentan los resultados del primer paso discriminando los intereses de seguridad por proyecto.

Durante el segundo paso se asignaron etiquetas de seguridad a los intereses de seguridad analizados. Las etiquetas utilizadas se mencionan a continuación, indicándose entre paréntesis la cantidad de intereses de seguridad a las que fueron asignadas: Acceso (9), Usuario autenticado (9), Autorización (9), Rol usuario (18), Usuario autorizado (34), Autorización (34), Datos (7), Datos correctos (7), Datos válidos (7), Integridad (10), Acceso información (17), Acceso servicios (16), Nivel de acceso (1), Informe de usuario (2), Auditoría (4), Nombre de usuario (2), Contraseña (3), Acceso subsistemas (1),

Características de calidad	Proyectos															Total
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Confidencialidad	0	0	6	7	4	1	2	7	0	1	3	0	0	1	2	34
Autenticidad	1	1	0	1	0	1	0	0	0	0	0	0	2	1	0	7
Integridad	0	1	1	0	1	2	0	3	0	0	0	1	0	0	0	9
Auditoría	0	0	0	2	0	0	0	1	0	0	0	1	0	0	0	4
Confidencialidad + Autenticidad	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	2
Confidencialidad + integridad	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
TOTAL	1	3	7	10	5	4	2	12	0	1	3	3	2	2	2	57

Tabla 4 – Métricas de intereses de seguridad según características de calidad asociadas

Encriptación (3), Detección ataques (2), Notificaciones (1), Verificación integridad (1), Seguimiento transacciones (1), No cookies (1), Archivos de datos (2), Base de datos (2).

Durante el tercer paso, se llevaron a cabo distintas consultas al sistema experto KE-SER.

Por un lado, se realizaron consultas individuales al sistema experto para obtener recomendaciones basadas en el conocimiento. Para ello se llevaron a cabo 15 consultas. En cada i -ésima consulta se le solicitó a KE-SER conocer las recomendaciones basadas en el conocimiento para los intereses de seguridad del i -ésimo proyecto. Debido a que la Base de Conocimiento había sido nutrida con suficiente conocimiento, se obtuvieron recomendaciones para todas las sentencias de seguridad de todos los proyectos consultados. Por restricciones en la longitud del trabajo no se presentan detalles de la Base de conocimiento empleada para realizar la evaluación.

Los resultados de este tipo de consultas a KE-SER dependen del conocimiento volcado en la base de conocimiento. Si el conocimiento y la clasificación de las etiquetas es escaso, es poco probable que se obtengan respuestas útiles del sistema experto. Este hecho es análogo a las respuestas que se podrían obtener de expertos humanos, si no tienen mucho conocimiento no pueden realizar recomendaciones útiles y de calidad.

Por otro lado, se realizaron consultas al sistema experto para obtener recomendaciones basadas en la experiencia. Para ello, se llevaron a cabo 15 iteraciones. En cada i -ésima iteración se realizaron las siguientes actividades:

- consulta a KE-SER de las recomendaciones basadas en la experiencia para los intereses de seguridad del i -ésimo proyecto;
- creación del correspondiente caso arquitectónico de seguridad (*SecurityArchitectureCase* en Fig. 4) con la información del problema (dado por las sentencias de seguridad del i -ésimo proyecto) y de la solución, basada en las recomendaciones recibidas. En aquellos casos en los que no se obtuvieron recomendaciones útiles para un interés de seguridad, se crearon recomendaciones basadas en el conocimiento para dar solución a dichos intereses y poder continuar con el proceso;
- almacenamiento del i -ésimo caso arquitectónico en la base de casos.

Los resultados obtenidos se presentan en la Tabla 5. Como puede observarse en la Tabla, un 79% de los intereses de seguridad planteados como consulta obtuvieron recomendaciones basadas en la experiencia. Los resultados de este tipo de consulta a KE-SER dependen de la experiencia que tenga el sistema experto, es decir, de la cantidad de casos en la Base de Casos.

	Proyectos															Total
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
<i>Casos en la Base de casos al momento de consultar por proyecto</i>	Ø	1	1-2	1-3	1-4	1-5	1-6	1-7	1-8	1-9	1-10	1-11	1-12	1-13	1-14	
<i>Intereses de seguridad</i>	1	3	7	10	5	4	2	12	0	1	3	3	2	2	2	57
<i>Intereses de seguridad con recomendaciones aplicadas surgidas de la experiencia</i>	0	2	4	6	5	4	2	9	0	1	3	3	2	2	2	45

Tabla 5 – Métricas de sentencias de seguridad con recomendaciones basadas en la experiencia según proyecto

Los primeros proyectos analizados (como ser 1, 2 y 3) obtuvieron peores resultados que los últimos, debido a que al momento de ser tratados la base de casos no contaba con experiencias pasadas para recuperar. Este comportamiento también es análogo al de expertos humanos, aquellos expertos que cuentan con más experiencia tienen más probabilidades de responder consultas con recomendaciones útiles y de calidad.

5. Trabajos relacionados

En la actualidad, en el contexto del diseño arquitectónico existen varias herramientas que brindan asistencia a los arquitectos de software para la realización de sus tareas. En Rodríguez, Díaz Pace, & Soria (2018) y Vazquez, Díaz Pace, & Campo (2010) se describen enfoques que emplean en CBR para explorar alternativas de diseño de arquitecturas orientadas al servicio (SOA) y arquitecturas a nivel general, respectivamente. En ambos trabajos los requerimientos de calidad toman un papel importante, pero el objetivo es dar soporte al diseño detallado o implementación de las arquitecturas de entrada.

En Carignano, Gonnet, & Leone (2016) se describe una herramienta que utiliza CBR para dar soporte al diseño de arquitecturas de software, a partir de un conjunto de requerimientos de calidad y restricciones de diseño. Esta herramienta contempla todo tipo de requerimiento de calidad de manera general.

En Gomes & Leitão (2006) también se propone una herramienta que aplica CBR para reutilizar conocimiento de diseño de software, empleando diagramas de clases UML para describir el sistema a diseñar.

Las herramientas y enfoques mencionados hasta aquí contemplan los requerimientos de calidad de manera general, siendo la seguridad una parte más de ellos. La diferencia con el enfoque propuesto se puede describir con base en dos pilares. Por un lado, el enfoque propuesto está especializado en los requerimientos de calidad de seguridad, por lo que puede ser abordado con mayor nivel de detalle. Por el otro, KE-SER no solo trabaja desde la perspectiva de la experiencia, como las herramientas previamente mencionadas, sino que también integra la perspectiva del conocimiento proveyendo los beneficios de contar con un experto con el conocimiento necesario para resolver problemas cuando la experiencia no es suficiente.

En el ámbito de seguridad, varios trabajos han propuesto el empleo de sistemas expertos, por ejemplo: Yang, Hu, and Chen (2004), o Rani and Goel (2015). Sin embargo, no se han encontrado trabajos relacionados a la utilización de sistemas expertos para dar soporte al diseño de arquitecturas de software.

6. Conclusiones y trabajos futuros

Las mejores prácticas de desarrollo de software sugieren integrar los aspectos de seguridad en cada fase del SDLC. Por lo que en este trabajo se presentaron las características generales de un sistema experto, llamado KE-SER, cuyo objetivo es dar soporte a los arquitectos de software en sus tareas en aspectos relacionados con seguridad.

El sistema experto KE-SER cuenta con la posibilidad de ofrecer recomendaciones de seguridad desde el punto de vista de información experta o de la experiencia. De forma tal que el arquitecto pueda seleccionar aquellas que considere más adecuadas para su aplicación. Además, en este trabajo se describió brevemente una herramienta que permite materializar el sistema experto propuesto, llamada KE-T.

Como trabajo futuro, se plantea el enriquecimiento de las etiquetas de seguridad (*SecurityTag*) para que reconozca sinónimos, antónimos y homónimos. Las etiquetas de seguridad son conceptos muy importantes, en el contexto de KE-SER y una definición detallada y rica de ellas permite un mejor funcionamiento del sistema experto.

Referencias

- Aamodt, A., & Plaza, P. (1994). Case-based reasoning: Foundational issues, methodological variations, and system approaches. *AI Communications*. IOS Press, 7(1):39–59, 1994.
- Bass, L., Clements, P., & Kazman, R. (2013). *Software Architecture in Practice*, 3rd Edition. Boston: Addison-Wesley. DOI: 10.1145/2693208.2693252
- Carignano, M.C., Gonnet, S., & Leone, H. (2016). RADS: una herramienta para reutilizar estrategias en diseños de arquitecturas de software. In *Simposio Argentino de Ingeniería de Software (ASSE 2016) - JAIIO 45*. SSN: 2451–7593, pp. 147-158
- Clements, P., Bachmann, F., Bass, L., Garlan, D., Ivers, J., Little, R., Merson, P., Nord, R., & Stafford, J. (2010). *Documenting Software Architectures: Views and Beyond* (2nd Edition). Boston: Addison-Wesley.

- CVE (2019). Common Vulnerabilities and Exposures. Recuperado de: cve.mitre.org/about Accedido: 02/2019.
- Yang, D., Hu, C., & Chen, Y. (2004). A framework of cooperating intrusion detection based on clustering analysis and expert system. In Proceedings of the 3rd international conference on Information security (InfoSecu '04). ACM, New York, NY, USA, 150–154. DOI: 10.1145/1046290.1046321
- De Win, B., Scandariato, R., Buyens, K., Grégoire, J., & Joosen, W. (2009). On the secure software development process: CLASP, SDL and Touchpoints compared. *Information and Software Technology*, 51(7), 1152–1171. DOI: 10.1016/j.infsof.2008.01.010.
- Eclipse (2019). Eclipse Foundation. Eclipse. Recuperado de: www.eclipse.org. Accedido: 22-02-2019.
- Gomes, P., & Leitão, A. (2006). A tool for management and reuse of software design knowledge. In: Staab S., Svátek V. (eds) Managing Knowledge in a World of Networks. EKAW 2006. Lecture Notes in Computer Science, vol 4248. Berlin, Heidelberg: Springer. DOI: 10.1007/11891451_3
- Gupta, S., & Singhal, R. (2013). Fundamentals and Characteristics of an Expert System. *International Journal on Recent and Innovation Trends in Computing and Communication*, 1(3), 110–113.
- ISO 25010 (2011). ISO/IEC 25010:2011 - Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models. International Organization for Standardization/ International Electrotechnical Commission.
- ISO 42010 (2011). ISO/IEC/IEEE 42010: International Organization for Standardization and International Electrotechnical Commission. Systems and software engineering - architecture description. Edition 01-12-2011.
- Java (2019). Oracle Corporation. Java. Recuperado de: www.oracle.com/technetwork/java/index.html. Accedido: 22-02-2019.
- Johnsson, D., Deogun, D., & Sawano, D. (2019). Secure by Design. Shelter Island, NY: Manning Publications
- Kolodner, J. (1992). An introduction to case-based reasoning. *Artificial Intelligence Review*, 6, 3–34. DOI: 10.1007/BF00155578
- MacGraw, G. (2006). Software security: building security in. Boston: Addison-Wesley.
- Mejía, J., & Muñoz, M. (2017). Tendencias en Tecnologías de Información y Comunicación. RISTI - Revista Ibérica de Sistemas y Tecnología de información, (21), 51–66. Doi: 10.17013/risti.21.51-66.
- Mohammad, A., Alqatawna, J., & Abushariah, M. (2017). Secure Software Engineering: Evaluation of Emerging Trends. 8th International Conference on Information Technology (ICIT), 814–818, DOI:10.1109/ICITECH.2017.8079952

- OWASP (2019). The OWASP Foundation. Recuperado de: www.owasp.org. Accedido: 02/2019
- PROMISE (2019). PROMISE Software Engineering Repository. Recuperado de: promise.site.uottawa.ca/SERepository/. Accedido: 05/2019.
- Rani C., & Goel, S. (2015). CSAAES: An expert system for cyber security attack awareness. In *International Conference on Computing, Communication & Automation*, Noida, 2015, pp. 242–245. DOI: 10.1109/CCAA.2015.7148381
- Rodríguez, G., Díaz-Pace, J. A., & Soria, A. (2018). A case-based reasoning approach to reuse quality-driven designs in service-oriented architectures. *Information Systems*, 77(2018), 167–189. DOI: 10.1016/j.is.2018.06.003.
- SAMM (2019). Software Assurance Maturity Model. Recuperado de: www.owasp.org/index.php/OWASP_SAMM_Project. Accedido: 22-02-2019.
- SDL (2019). Microsoft Security Development Lifecycle, Microsoft. Recuperado de: www.microsoft.com/en-us/sdl. Accedido: 22-02-2019.
- SWT (2019). Eclipse Foundation. Standard widget toolkit. Recuperado de: www.eclipse.org/swt. Accedido: 22-02-2019.
- Watson, I., & Marir, F. (1994). Case-based reasoning: A review. *The Knowledge Engineering Review*, 9(4), 327–354.
- Winkler, I. & Treu Gomes, A. (2017). Chapter 7 - Adversary Infrastructure. In I. Winkler & A. Treu Gomes (Eds.). *Advanced Persistent Security*, (pp. 67 – 79). Rockland, MA: Syngress. DOI: 10.1016/B978-0-12-809316-0.00007-5
- Zambrano, A., Guarda, T., Valenzuela, E.V.H., & Quiña, G. N. (2019). Técnicas de mitigación para principales vulnerabilidades de seguridad en aplicaciones web. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, (E17), 299-308.

Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información

Mauricio Diéguez^{1,2}, Carlos Cares^{1,3}

mauricio.dieguez@ufrontera.cl, carlos.cares@ceisufro.cl

¹ Departamento de Ciencias de la Computación e Informática, Universidad de La Frontera, 4811230, Temuco, Chile.

² Grupo de Ciberseguridad, Centro de Excelencia de Modelación y Computación Científica, Universidad de La Frontera, 4811230, Temuco, Chile.

³ Centro de Estudios de Ingeniería de Software, Universidad de La Frontera, 4811230, Temuco, Chile.

DOI: 10.17013/risti.32.113–128

Resumen: Proporcionar procesos y herramientas sistemáticos para tomar una decisión sobre inversiones en seguridad en un escenario con restricciones presupuestarias, es de suma importancia para asegurar que dichas decisiones se tomen adecuadamente. Presentamos un enfoque de programación de conjunto de respuestas (ASP) para resolver este problema. Nuestra propuesta se compara con el desarrollo del problema utilizando programación lineal (PL). Ilustramos la fase de modelado y el rendimiento computacional de ambas soluciones. El modelo ASP presenta tiempos de resolución del tipo exponencial a medida que aumenta el número de controles sobre los que debe decidirse. Por otro lado, el modelo basado en PL no presenta variaciones importantes en sus tiempos de resolución de problemas. Sin embargo, el problema es más fácil de modelar en ASP. Luego, esta propuesta tiene ventajas para modelar y resolver problemas específicos en los que se requiere una respuesta rápida con una baja cantidad de controles.

Palabras-clave: Answer set programming; Programación lineal; Optimización; Controles de seguridad de la información; Sistema de gestión de seguridad de la información.

Comparing Two Quantitative Approaches to Select Information Security Controls

Abstract: Provide systematic processes and tools to make a decision about security investments under a scenario of budget constraints, is of paramount importance to assure that such decisions are soundly made. We present a answer set programming (ASP) approach to solve this problem. Our proposal is then compared against a traditional linear programming (LP) operational research technique. We illustrate the modeling phase and computational performance of both solutions. The model based on ASP presents resolution times of the exponential type as the number of controls over which it must be decided increases. On the other hand, the model based on LP does not present important variations in its problem resolution times.

However, the problem is easier to model in ASP. Then, this proposal has advantages for modeling and solving specific problems in which a rapid response is required and which do not require many controls.

Keywords: Answer set programming; linear programming; optimization; information security controls; information security management systems.

1. Introducción

El actual escenario en ciberseguridad, ha obligado a las organizaciones a incorporar un conjunto de buenas prácticas de seguridad en sus sistemas de gestión de la información. Estas prácticas de protección se han extendido por todo el mundo y han llevado a diferentes organizaciones a definir e implementar estándares de seguridad de la información (Tofan, 2011).

Un estándar para la seguridad de la información consiste en un conjunto de reglas que tienen como objetivo regular las operaciones de una empresa, con un énfasis especial en la gestión y el aseguramiento de la información. En términos generales, el cumplimiento de algún estándar de seguridad de la información implica el logro de un conjunto de objetivos, la adquisición de recursos o la implementación de acciones regulares que se definen en el estándar (Pereira & Santos, 2014). Todos estos elementos se conocen como controles de seguridad de la información (ISC por sus siglas en inglés) (Yau, 2014) y pueden agruparse por dimensiones.

El mapa de controles implementados-no implementados se convierte en una herramienta de administración para avanzar en la seguridad de la información. En este contexto, es necesario definir un programa de selección de controles que proponga un camino hacia el logro de la norma y que pueda evaluarse continuamente a través de un programa de auditoría. Sin embargo, la limitación de recursos y la existencia de dependencias entre ellos pueden impedir que algunos de los controles se implementen juntos. Por lo tanto, la progresión hacia un cumplimiento total de un estándar definido, viene a menudo a través de múltiples avances parciales. En este escenario, la selección del subconjunto de controles de seguridad que debe implementarse, debe ser tal que maximice el progreso, minimice los riesgos y optimice los recursos.

El enfoque tradicional para enfrentar esta situación, ha sido la gestión del riesgo mediante el uso de instrumentos cualitativos y juicios de expertos (Cano, 2018). Sin embargo, algunos autores consideran que dichos enfoques cualitativos son subjetivos y están incompletos (A. Otero, Otero, & Qureshi, 2010), que deben ir acompañados de algún tipo de enfoque cuantitativo y objetivo. Se han propuesto varias técnicas con el objetivo de formalizar el proceso de selección del ISC, sin embargo, estas propuestas mantienen un grado de subjetividad (A. R. Otero, 2015).

Una solución cuantitativa para la selección de ISC se considera un problema NP-Hard (Tosatto, Governatori, & Kelsen, 2015). Existen propuestas que apuntan al uso de métodos matemáticos para apoyar la selección del ISC -ver por ejemplo (Breier & Hudec, 2013b; Cuihua & Jiajun, 2009; J. Lv, Zhou, & Wang, 2011; Yang, Shieh, Leu, & Tzeng, 2009) -. Sin embargo, agregar variables y restricciones reales al considerar casos específicos hace que sea más compleja la etapa de modelado, y transforma

esta etapa en una barrera difícil de cruzar para alcanzar una solución cuantitativa al problema.

En un trabajo anterior, hemos tratado de superar este problema proponiendo un enfoque basado en “Answer Set Programming” (ASP) (Cares & Diéguez, 2017). ASP es un área de investigación basada en la representación del conocimiento, la programación lógica y la satisfacción de restricciones diseñada para hacer frente principalmente a los problemas de NP-Hard (Brewka, Eiter, & Truszczyński, 2011). Hoy en día, hay herramientas que permiten la especificación y solución de estos modelos, tales como Clingo (Gebser et al., 2011).

Otra forma propuesta para resolver la selección de ISC es aplicar un enfoque de Programación Lineal (PL). La programación lineal es un producto de investigación que proviene de la disciplina de Investigación de Operaciones (OR). La programación lineal es parte del cuerpo de conocimientos de OR y también requiere una etapa de modelado. Existen varias herramientas para implementar estos algoritmos. Ilustramos esta solución específica utilizando NEOS Server (NEOS, 2018), una herramienta web para resolver problemas de optimización.

El objetivo de este documento es doble: por un lado, presentamos una versión ampliada del enfoque ASP, que mejora la versión anterior en (Cares & Diéguez, 2017). Por otro lado, para validar esta propuesta, la comparamos con el enfoque de PL, que se ha propuesto como un enfoque cuantitativo para la selección óptima de controles de seguridad (Kawasaki & Hiromatsu, 2014; Sawik, 2013; Yevseyeva, Fernandes, Van Moorsel, Janicke, & Emmerich, 2016). El aporte de este trabajo radica en presentar la aplicación de modelos de optimización y restricciones de operación que no habían sido consideradas en el dominio de la seguridad de la información. Además se proporciona un estudio respecto de la medición del desempeño de ambas técnicas, lo cual no se ha tratado con anterioridad.

El documento está organizado de la siguiente manera: en la sección 2, se presenta una búsqueda bibliográfica basada en un mapeo sistemático de los métodos actuales que tratan la gestión del ISC. En la Sección 3, el problema de la selección de controles se modela utilizando los dos enfoques en revisión, es decir, ASP y PL, e ilustramos cómo se implementa el modelo propuesto en dos plataformas tecnológicas diferentes. En la Sección 4, se realiza una prueba de concepto utilizando datos extraídos de un caso real para comparar el desempeño de ambas propuestas. Finalmente, la Sección 5 presenta las conclusiones del estudio.

2. Gestión de los Controles de Seguridad de la Información

La gestión de la seguridad de la información en una organización se realiza mediante la implementación y operación de un Sistema de Gestión de Seguridad de la Información (SGSI). Estos sistemas están orientados a identificar e implementar controles de seguridad para reducir el riesgo en el manejo de la información (Saint-Germain, 2005).

Actualmente, existen varios estándares de seguridad de la información que guían la implementación, operación, monitoreo, revisión, mantenimiento y mejora de un SGSI

(Tofan, 2011). En particular, uno de los estándares de seguridad más conocidos es ISO/IEC 27001: 2013 (International Organization for Standardization, 2013).

Es importante tener en cuenta que el enfoque de la selección de ISC no es solo la cantidad de controles que se deben implementar para lograr un nivel de seguridad, sino también la idoneidad del conjunto de controles (A. Otero et al., 2010).

Sin embargo, se ha reconocido que los intereses propios del administrador de seguridad pueden influir en el conjunto resultante de controles para implementar (Bachlechner, Maier, Innerhofer-Oberperfler, & Demetz, 2011), lo que hace que el proceso sea subjetivo. Este hecho se explica por la teoría de la agencia (Jensen & Meckling, 1976), que reconoce que un objetivo organizativo, como el objetivo de reducir el riesgo organizativo, no está necesariamente alineado con el objetivo de quien lo administre. Esta teoría señala que los intereses entre una organización (principal) y un administrador (agente) pueden divergir y que es necesario incurrir en lo que se conoce como costos de vinculación para lograr cierta alineación de objetivos y comportamientos. Si bien la Teoría de la Agencia reconoce que el mercado tiende a eliminar estas diferencias, una extensión de esta teoría ilustra cómo las anomalías del mercado pueden retrasar considerablemente el proceso de ajuste. Como ejemplo de lo anterior, es posible pensar en términos de un caso en el que un gerente de seguridad desea mostrar un aumento considerable en el porcentaje de controles implementados, como un indicador de su éxito en la gestión, aunque esto no necesariamente signifique una reducción significativa de los riesgos de seguridad de la información. Estos diferentes objetivos aumentan la complejidad del problema, ya que, bajo numerosas opciones de seguridad, las organizaciones buscarían elegir e implementar el conjunto óptimo de controles que reducen el riesgo y aumentan la rentabilidad, mientras que los administradores buscarían mejorar su propia posición como agentes de la organización.

Además, se debe considerar el caso en el que una organización desea cumplir con más de una norma de seguridad, como las organizaciones públicas, que, además de intentar lograr una norma internacional, debe cumplir con las normas locales regulaciones y políticas gubernamentales (Diéguez, Cares, & Sepúlveda, 2012).

Para identificar los estudios que han abordado el problema, hemos llevado a cabo una búsqueda bibliográfica basada en un protocolo de mapeo sistemático (Petersen, Vakkalanka, & Kuzniarz, 2015). En nuestro caso, el objetivo fue identificar qué métodos o técnicas se han propuesto para la selección de ISC. La pregunta que guió a los hallazgos principales fue: “¿Qué métodos o técnicas se han propuesto para resolver el problema de la selección y programación de un conjunto de controles de un estándar de seguridad de la información que permite la evaluación del riesgo en una organización?”

Para definir la cadena de búsqueda, se definieron los conceptos clave, que fueron: (“Evaluación de seguridad” O “Selección de controles” O “Soluciones de seguridad”) Y “Cumplimiento de la seguridad de la información”).

Para las búsquedas utilizamos los principales repositorios bibliográficos digitales de informática y disciplinas relacionadas: IEEE Xplore, Biblioteca Digital ACM, Springer Link y Science Direct. Además, se realizó una búsqueda manual en las actas de las principales conferencias del área.

Los artículos encontrados fueron evaluados por tres revisores para decidir su inclusión o exclusión, de acuerdo a los criterios descritos en la tabla 1. En la tabla 2, se muestra la lista con los artículos encontrados, después de filtrar respecto de los criterios de inclusión y exclusión.

De los 35 artículos seleccionados, cinco se refieren a investigaciones que incluyen modelos de optimización cuantitativos para la selección de ISC (Almeida & Respício, 2018; Kawasaki & Hiromatsu, 2014; Sawik, 2013; Yevseyeva, Basto-Fernandes, Emmerich, & van Moorsel, 2015; Zhang, Chari, & Agrawal, 2018). Estos enfoques proponen un modelo de selección de controles mediante la aplicación de un modelo de optimización de multi-objetivos, en el que relacionan los controles con sus riesgos asociados y su distribución de costos, para obtener una solución óptima. Sin embargo, no consideran la dependencia entre los controles de seguridad. En estas propuestas, la programación lineal se utiliza como la técnica principal de modelado y solución.

En un artículo anterior (Diéguez et al., 2012), propusimos un método de selección de ISC. Nuestro modelo, al igual que los cinco seleccionados, puede considerarse como un problema de optimización multi-objetivos, pero, a diferencia de los anteriores, considera las dependencias entre los controles. Además, el modelo se puede codificar según diferentes enfoques, como Answer Set Programming (ASP) y programación lineal (PL).

Criterios de Inclusión	Criterios de Exclusión
1. Artículos que presentan propuestas, modelos teóricos, ejemplos teóricos o casos de estudio, respecto de la selección y/o programación de controles de un estándar de seguridad de la información o que abordan el problema de selección de medidas de seguridad de la información.	1. Artículos que no presentan propuestas, modelos teóricos, ejemplos teóricos o casos de estudio, respecto de la selección y/o programación de controles de un estándar de seguridad de la información o que abordan el problema de selección de medidas de seguridad de la información. 2. Libros y Reportes Técnicos. 3. Documentos de tesis. 4. Trabajos duplicados del mismo estudio en diferentes fuentes. 5. Documentos de discusión o revisiones bibliográficas. 6. Artículos que no son accesibles. 7. Artículos que no están escritos en inglés.

Tabla 1 – Criterios de inclusión y exclusión del protocolo de mapeo sistemático

3. Descripción de las propuestas para la selección de controles de seguridad

En esta sección, presentamos dos enfoques alternativos para resolver el problema de optimización. El primer enfoque consiste en resolver el problema utilizando ASP, mientras que el segundo enfoque resuelve el problema utilizando PL.

Dado que puede haber múltiples combinaciones de controles que cumplan con un presupuesto determinado, se esperaría que los modelos presentados pudieran determinar el conjunto de controles que optimiza el presupuesto de una organización.

3.1. Modelado del problema con el enfoque ASP

ASP es un lenguaje de programación declarativo flexible, que se enfoca en resolver problemas combinatorios difíciles. Como tal, es una herramienta poderosa para la representación y razonamiento del conocimiento (Bonatti, Calimeri, Leone, & Ricca, 2010), y se puede usar para resolver problemas de tipo NP. Por lo tanto, encaja bien con los problemas de optimización y la programación de restricciones (Hooker, 2002), en la cual la función objetivo debe ser maximizada o minimizada, sujeta a algunas restricciones (Gebser et al., 2011).

Referencia	Año	Referencia	Año
(Bistarelli, Fioravanti, & Peretti, 2007)	2007	(Kiesling, Ekelhart, Grill, Straub, & Stummer, 2013)	2013
(Ojamaa, Tyugu, & Kivimaa, 2008)	2008	(Kiesling, Strauss, Ekelhart, Grill, & Stummer, 2013)	2013
(Yang et al., 2009)	2009	(Yang, Shieh, & Tzeng, 2013)	2013
(Gao, Li, & Song, 2009)	2009	(Sawik, 2013)	2013
(Cuihua & Jiajun, 2009)	2009	(Breier & Hudec, 2013b)	2013
(Chen, Li, Hu, & Lian, 2009)	2009	(Breier & Hudec, 2013a)	2013
(Nagata, Amagasa, Kigawa, & Cui, 2009)	2009	(Breier, 2014)	2014
(A. Otero et al., 2010)	2010	(Choo, Mubarak, Mani, & others, 2014)	2014
(J.-J. Lv & Wang, 2010)	2010	(Al-Safwani, Hassan, & Katuk, 2014)	2014
(Angel Otero, Ejnoui, Otero, & Tejay, 2011)	2011	(Kawasaki & Hiromatsu, 2014)	2014
(Yameng, Yulong, Jianfeng, Xining, & Yahui, 2011)	2011	(Meng & Liu, 2015)	2015
(J. Lv et al., 2011)	2011	(Shahpasand, Shajari, Golpaygani, & Ghavamipoor, 2015)	2015
(Rees, Deane, Rakes, & Wade H. Baker, 2011)	2011	(Yevseyeva et al., 2015)	2015
(Angel Otero, Tejay, Otero, & Ruiz-Torres, 2012)	2012	(Sarala, Zayaraz, & Vijayalakshmi, 2015)	2015
(Ejnoui, Otero, Tejay, Otero, & Qureshi, 2012)	2012	(Jiménez-Martín, Vicente, & Mateos, 2015)	2015
(Breier & Hudec, 2012)	2012	(Khajouei, Kazemi, & Moosavirad, 2017)	2017
(Viduto, Maple, Huang, & López-Peréz, 2012)	2012	(Almeida & Respício, 2018)	2018
(Kiesling, Strauss, & Stummer, 2012)	2012	(Zhang et al., 2018)	2018

Tabla 2 – Lista de artículos encontrados en Mapeo Sistemático

La figura 1 muestra un extracto de la formulación de este problema utilizando ASP, de acuerdo con la formulación presentada en (Cares & Diéguez, 2017). El modelo, es decir, predicados, reglas y restricciones de este caso se puede descargar desde <http://dci.ufro.cl/fileadmin/Software/OptimalSecurityControls-OSCUFRO.zip>.

<pre>#show planned/1. #show totalCost/1. #show totalProfit/1. %controls control(c6_1; c6_1_1; c6_1_2; c6_1_3; c6_1_3_1; c6_2; c6_2_1; c6_2_2; %Implementation of %controls implies costs cost(c6_1,4800000). cost(c6_1_1,800000). cost(c6_1_2,160000). cost(c6_1_3,220000). cost(c6_1_3_1,100000). %Implementation of controls %implies security profits profit(c6_1,1). profit(c6_1_1,1). profit(c6_1_2,1). profit(c6_1_3,1). profit(c6_1_3_1,1). profit(c6_2,1). profit(c6_2_1,1). profit(c6_2_2,1).</pre>	<pre>%some controls requires %other controls require(c6_1,(c6_1_1;c6_1_2;c6_1_3)). require(c6_1_3,(c6_1_3_1)). require(c6_2,(c6_2_1;c6_2_2;c6_2_3;c6_2_4;c6_2_5)). budget(4000000). %Generate 0 { planned(Y) } 1 :- terminal(Y). 0 { planned(X) } 1 :- totalRequired(X,D), totalIncluded(X,W), D=W. %Define totalRequired(X,D):- control(X), D = #count {Z:require(X,Z),control(Z)}. totalIncluded(X,D):- control(X), D = #count {Z:require(X,Z),planned(Z)}. totalProfit(Y):- Y = #sum {D,X: planned(X),profit(X,D)}. totalCost(N) :- N = #sum {D,X: planned(X),cost(X,D)}. terminal(X):-control(X), not require(X,_). %Test :- totalCost(N), budget(T), N>T. %Optimization #maximize { I:totalProfit(I) }.</pre>
--	--

(a) Configuración de Variables

(b) Definición de ecuaciones

Figura 1 – Codificación de Clingo del modelo ASP.

3.2. Modelación del problema con el enfoque PL

La formulación para el problema presentado, considerando las restricciones de presupuesto, las dependencias de control y los beneficios de la implementación, se describe en la ecuación 1. La ecuación 2, es el costo de la restricción de implementación, donde la suma de estos costos no puede exceder el presupuesto disponible para la implementación. La ecuación 3 representa el anidamiento de primer nivel y la ecuación 5 el anidamiento de segundo nivel.

Para formular el problema, utilizamos el Sistema de modelado algebraico general (GAMS) (GAMS, 2018), un sistema de modelado de alto nivel para programación y optimización matemática. Para resolver el problema, utilizamos el portal web NEOS Server (NEOS, 2018), un sitio web gratuito para resolver problemas de optimización. En el Servidor NEOS, el problema se modeló como Programación lineal de enteros mixtos, utilizando la entrada GAMS.

En la Figura 2, se muestra un extracto de la configuración de las variables y la definición de las ecuaciones, en lenguaje GAMS.

$$\text{Max (} \sum_{i>0, j>0, j \neq k, j=l} P_{ij} X_{ij} + \sum_{i>0, j>0, k \in A_{ij}} P_{ijk} X_{ijk} + \sum_{i>0, j>0, k \in A_{ij}, l \in A_{ijk}} P_{ijkl} X_{ijkl}) \quad (1)$$

s.t.

$$\left(\sum_{i>0, j>0, j \neq k, j=l} C_{ij} X_{ij} + \sum_{i>0, j>0, k \in A_{ij}} C_{ijk} X_{ijk} + \sum_{i>0, j>0, k \in A_{ij}, l \in A_{ijk}} C_{ijkl} X_{ijkl} \right) - B \leq 0 \quad (2)$$

$$\begin{aligned} X_{ij} - X_{ijk} &\leq 0 \\ i > 0, j > 0, k &\in A_{ij}, A_{ij} \neq \emptyset \end{aligned} \quad (3)$$

$$X_{ijk} - X_{ijkl} \leq 0$$

$$i > 0, j > 0, k \in A_{ij}, l \in A_{ijk}, A_{ij} \neq \emptyset, A_{ijk} \neq \emptyset$$
(4)

Donde,

P: Beneficio de implementar cada control

i: Dimensión desde el estándar de seguridad multidimensional.

j: Identificación del control en la dimensión.

k: Primer nivel de anidamiento para el control j-ésimo

l: Segundo nivel de anidamiento para el control jk-ésimo

B: Presupuesto disponible

A_{ij}: Conjunto de controles anidados de primer nivel

A_{ijk}: Conjunto de anidado de controles de segundo nivel

4. Comparación de los enfoques en una situación industrial: Prueba de concepto.

Como ya se mencionó, se utilizaron los datos de una auditoría informática realizada en una organización gubernamental chilena. En este caso, la organización debe cumplir con dos regulaciones de seguridad de la información establecidas por el Gobierno de Chile: (i) Decreto Supremo 83 (DS83) (Gobierno de Chile, 2005), una norma de seguridad para oficinas públicas; y (ii) la guía metodológica para la seguridad de la información (GUI) (Gobierno de Chile, 2011), que describe los requisitos técnicos asociados con el diagnóstico, la planificación y la implementación de un sistema de seguridad de la información. Además, la organización decidió evaluar su cumplimiento con la norma internacional ISO 27001, en su versión 2005. A los efectos de la prueba, solo presentaremos la dimensión referente a la seguridad de las instalaciones, ya que fue el principal foco de evaluación después del terremoto del año 2010 en Chile.

```
SOFFSYNDKREF
SOFFSYMLIST

option limrow=0;
option limcol=0;
option solprint=on;
option sysout=off;

option LP=CPLEX;
option MIP=CPLEX;
option NLP=CONOPT;
option MINLP=DICOPT;
option OPTCR=0;

$TITLE Ejercicio de Prueba

VARIABLES

F, ppto ;

POSITIVE VARIABLES

ppto ;

BINARY VARIABLES

X1, X2, X3, X4, X5, X6, X7, X8, X9, X10 ;
```

(a) Configuración de Variables

```
EQUATIONS

funcObj, R1, R2, R3, R4, R5, R6, R7, R8, R9, R10 ;

funcObj.. F =E= 3*X1 + 5*X2 + 3*X3 + 2*X4 + 2*X5 +
5*X6 + 6*X7 + 2*X8 + 5*X9 + 1*X10 ;

R1.. 120*X1 + 202*X2 + 150*X3 + 120*X4 + 202*X5 +
171*X6 + 230*X7 + 100*X8 + 100*X9 + 140*X10 - ppto =L= 0;

R2.. ppto =L= 900 ;
R3.. X5 - X1 =L= 0;
R4.. X5 - X2 =L= 0;
R5.. X8 - X3 =L= 0;
R6.. X9 - X4 =L= 0;
R7.. X9 - X5 =L= 0;
R8.. X9 - X6 =L= 0;
R9.. X10 - X7 =L= 0;
R10.. X10 - X8 =L= 0;

MODEL optTotal /ALL / ;

SOLVE optTotal using MIP maximizing F ;
```

(b) Definición de ecuaciones

Figura 2 – Configuración del modelo en lenguaje GAMS

La tabla 3 muestra un resumen de los beneficios y costos (en miles de pesos chilenos) asociados con la implementación de cada control.

Para esta prueba de concepto, ambos modelos se ejecutaron en tres escenarios, en los que el número de controles se incrementó en una magnitud de diez en diez con un máximo de 31 controles; en el primer caso se evaluaron un total de 11 controles, en el segundo caso se evaluaron un total de 22 controles y en el tercer caso se evaluaron 31 controles.

Los beneficios asociados con cada control se establecieron considerando el estándar al que pertenecen. Se otorgó una puntuación más alta a los controles que cumplieran con las reglas específicas del gobierno de Chile y aquellos que cumplieran con más de una norma. Los costos de implementación de cada control se estimaron según las condiciones operativas de la organización. El presupuesto considerado para el ejemplo es \$ 4.000.000 (en pesos chilenos).

La tabla 4, muestra un resumen de los resultados óptimos obtenidos con ambos modelos, destacando los costos, beneficios, controles propuestos y tiempos de procesamiento.

Como se observa, en los tres casos, los resultados, desde el punto de vista de los beneficios logrados por la implementación del conjunto de controles propuestos, son iguales, es decir, ambos modelos maximizan el beneficio.

Para el caso de 22 controles, hay una diferencia con respecto al conjunto de controles que se seleccionaron y, por lo tanto, los costos asociados con el conjunto mencionado anteriormente. Sin embargo, el beneficio es el mismo para ambos modelos.

Control	Beneficio	Costo	Dependencia	Control	Beneficio	Costo	Dependencia
C1	1	480	-	C7	1	480	-
C1-1	1	800	C1	C7-1	1	120	C7
C1-2	1	160	C1	C7-2	1	50	C7
C1-3	1	220	C1	C7-3	1	50	C7
C1-3-1	1	100	C1-3	C7-4	1	50	C7
C2	1	800	-	C7-5	1	50	C7
C2-1	1	80	C2	C8	1	200	-
C2-2	1	160	C2	C9	1	1.480	-
C2-3	1	920	C2	C9-1	1	80	C9
C2-4	1	120	C2	C9-2	1	80	C9
C2-5	1	160	C2	C9-3	1	80	C9
C3	2	290	-	C9-4	1	1.080	C9
C3-1	3	50	C3	C9-4-1	1	80	C9-4
C4	1	120	-	C9-4-2	1	800	C9-4
C5	1	320	-	C9-4-3	1	120	C9-4
C6	1	600	-				

Tabla 3 – Costos y beneficios de implementar cada control.

Modelo ASP	Modelo PL
Universo de Controles: 11 Tiempo de ejecución: 0,109 seg. Número de controles seleccionados: 11 Costo: 4.000 (Miles de pesos) Beneficio: 11	Universo de Controles: 11 Tiempo de ejecución: 0,006 seg. Número de controles seleccionados: 11 Costo: 4.000 (Miles de pesos) Beneficio: 11
C1; C1-1; C1-2; C1-3; C1-3-1; C2; C2-1; C2-2; C2-3; C2-4; C2-5.	C1; C1-1; C1-2; C1-3; C1-3-1; C2; C2-1; C2-2; C2-3; C2-4; C2-5.
Universo de Controles: 22 Tiempo de ejecución: 12,016 seg. Número de controles seleccionados: 19 Costo: 3.980 (Miles de pesos) Beneficio: 22	Universo de Controles: 22 Tiempo de ejecución: 0,01 seg. Número de controles seleccionados: 19 Costo: 3.980 (Miles de pesos) Beneficio: 22
C1; C1-1; C1-2; C1-3; C1-3-1; C2; C2-1; C2-2; C2-4; C2-5; C3; C3-1; C4; C5; C7; C7-1; C7-2; C7-3; C7-4; C7-5.	C1; C1-1; C1-2; C1-3; C1-3-1; C2; C2-1; C2-2; C2-4; C2-5; C3; C3-1; C4; C5; C6; C7-1; C7-2; C7-3; C7-4; C7-5.
Universo de Controles: 31 Tiempo de ejecución: 9.744,287 seg. Número de controles seleccionados: 24 Costo: 3.820 (Miles de pesos) Beneficio: 27	Universo de Controles: 31 Tiempo de ejecución: 0,019 seg. Número de controles seleccionados: 24 Costo: 3.820 (Miles de pesos) Beneficio: 27
C1-2; C1-3; C1-3-1; C2-1; C2-2; C2-4; C2-5; C3; C3-1; C4; C5; C6; C7; C7-1; C7-2; C7-3; C7-4; C7-5; C8; C9-1; C9-2; C9-3; C9-4-1; C9-4-3.	C1-2; C1-3; C1-3-1; C2-1; C2-2; C2-4; C2-5; C3; C3-1; C4; C5; C6; C7; C7-1; C7-2; C7-3; C7-4; C7-5; C8; C9-1; C9-2; C9-3; C9-4-1; C9-4-3.

Tabla 4 – Resultados de la ejecución de los modelos.

A partir de esta prueba de concepto, se observa que ambos modelos pueden maximizar el beneficio de acuerdo con las restricciones presupuestarias y las dependencias entre controles.

La gran diferencia se da en la velocidad de ejecución de ambos modelos. Si bien el modelo PL presenta tiempos de procesamiento muy bajos e incrementos pequeños a medida que se consideran más controles, el modelo ASP, aunque comienza con un tiempo de configuración muy bajo, aumenta su tiempo de ejecución de manera exponencial con respecto al número de controles. Esto implica que el modelo ASP se vuelve poco práctico al evaluar un gran número de controles, a pesar de su facilidad de modelado.

5. Conclusiones

Un enfoque contemporáneo para administrar la seguridad de la información en las organizaciones, es cumplir con los estándares basados en procesos, que se basan en la implementación de un conjunto de buenas prácticas denominados controles de seguridad. La primera etapa requiere una evaluación de la seguridad de la información que produzca, como resultado relevante, un conjunto de controles ya implementados y otro conjunto de controles a implementar. Tomar una decisión acerca de la próxima implementación de ISC no es una respuesta trivial, ya que implica diferentes escenarios de riesgo alternativos, restricciones presupuestarias y objetivos comerciales, lo que genera un problema de optimización combinatoria del tipo np-hard.

Para obtener una visión de las actuales soluciones, hemos llevado a cabo una búsqueda bibliográfica basada en un protocolo de revisión de mapeo sistemático, el cual ha dado como resultado 35 artículos que abordan el problema de selección de ISC. De este conjunto, solo 5 abordaron el problema desde una perspectiva cuantitativa bajo un conjunto limitado de restricciones.

Para agregar nuevas restricciones, hemos presentado dos enfoques cuantitativos: uno basado en Answer Set Programming y otro basado en la Programación lineal. Hemos utilizado un ejemplo con tres tipos de restricciones: dependencias temporales entre controles, un presupuesto limitado y diferentes beneficios de seguridad de la información dados por los diferentes controles a implementar. La solución ASP resulta simple e ilustrativa. En primer lugar, hemos demostrado que una solución cuantitativa no es difícil de modelar; en segundo lugar, se puede extender fácilmente para admitir controles adicionales (hechos) y restricciones. Sin embargo, el rendimiento de ASP fue lento, con un rendimiento aceptable hasta un espacio de búsqueda de 30 controles en máquinas secuenciales y 40 en máquinas paralelas. Por lo tanto, este tipo de solución es muy adecuado para realizar diagnósticos limitados con respecto al estándar, por ejemplo, sobre algún dominio específico, donde se desea obtener resultados rápidamente a un bajo costo de modelado.

Por otro lado, el enfoque PL resulta en una etapa de modelado más compleja, sin embargo, su rendimiento fue completamente satisfactorio. En las diferentes soluciones, incluso considerando la cantidad total de controles involucrados, el tiempo de procesamiento, incluido el tiempo de proceso web, no alcanzó 30 segundos.

Por lo tanto, hemos propuesto dos enfoques cuantitativos basados en la tecnología existente y abierta para abordar el problema de seleccionar ISC. Uno de ellos, basado en ASP, resulta adecuado para unos pocos controles que facilitan la etapa de modelado debido al alto nivel de abstracciones de su lenguaje de programación. El segundo, basado en PL, presenta un excelente rendimiento, aunque su formulación algebraica resulta un poco más complejo de especificar que ASP.

En términos de trabajo futuro, experimentaremos sobre el desempeño de enfoques más complejos, principalmente en soluciones no lineales e incluyendo el riesgo como variables estocásticas. Mantendremos el enfoque en la dualidad de la evaluación que requiere mucho tiempo considerando tanto el tiempo de modelado como el tiempo de cálculo, ya que ambos factores forman parte del esfuerzo total necesario para resolver el problema presentado.

Agradecimientos

Trabajo financiado por la Universidad de La Frontera, Proyecto DI19-0116.

Referencias

- Al-Safwani, N., Hassan, S., & Katuk, N. (2014). A multiple attribute decision making for improving information security control assessment. *International Journal of Computer Applications*, 89(3).

- Almeida, L., & Respício, A. (2018). Decision support for selecting information security controls. *Journal of Decision Systems*, 0125(May), 1–8. <https://doi.org/10.1080/12460125.2018.1468177>
- Bachlechner, D., Maier, R., Innerhofer-Oberperfler, F., & Demetz, L. (2011). Understanding the management of information security controls in practice. In *Proceedings of the 9th Australian Information Security Management Conference*. Perth Western Australia: Edith Cowan University.
- Bistarelli, S., Fioravanti, F., & Peretti, P. (2007). Using CP-nets as a guide for countermeasure selection. In *Proceedings of the 2007 ACM symposium on Applied computing*. <https://doi.org/10.1145/12444002.12444073>
- Bonatti, P., Calimeri, F., Leone, N., & Ricca, F. (2010). Answer set programming. In *A 25-year perspective on logic programming* (pp. 159–182). Berlin: Springer.
- Breier, J. (2014). Security Evaluation Model based on the Score of Security Mechanisms. *Information Sciences and Technologies Bulletin of the ACM*, 6(1), 19–27.
- Breier, J., & Hudec, L. (2012). New approach in information system security evaluation. In *IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)* (pp. 1–6). IEEE. <https://doi.org/10.1109/estel.2012.6400145>
- Breier, J., & Hudec, L. (2013a). On Identifying Proper Security Mechanisms. *Information and Communicatiaon Technology*, 285–294.
- Breier, J., & Hudec, L. (2013b). On Selecting Critical Security Controls. In *International Conference on Availability, Reliability and Security* (pp. 582–588).
- Brewka, G., Eiter, T., & Truszczyński, M. (2011). Answer set programming at a glance. *Communications of the ACM*, 54(12), 92–103.
- Cano, J. J. M. (2018). Repensando los fundamentos de la gestión de riesgos. Una propuesta conceptual desde la incertidumbre y la complejidad. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (E15), 76–87.
- Cares, C., & Diéguez, M. (2017). An Answer Set Solution for Information Security Management. In *proceedings of the Eighth International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking* (pp. 11–15).
- Chen, L., Li, L., Hu, Y., & Lian, K. (2009). Information Security Solution Decision-Making Based on Entropy Weight and Gray Situation Decision. In *2009 Fifth International Conference on Information Assurance and Security* (Vol. 2, pp. 7–10). IEEE. <https://doi.org/10.1109/IAS.2009.9>
- Choo, K. K., Mubarak, S.,...& Mani, D. (2014). Selection of information security controls based on AHP and GRA. *Pacific Asia Conference on Information Systems*.
- Cuihua, X., & Jiajun, L. (2009). An Information System Security Evaluation Model Based on AHP and GRAP. *International Conference on Web Information Systems and Mining*, 493–496.

- Diéguez, M., Cares, C., & Sepúlveda, S. (2012). On Optimizing the Path to Information Security Compliance. In 8th International Conference on the Quality of Information and Communications Technology (QUATIC'12) (pp. 182–185).
- Ejnioui, A., Otero, A., Tejay, G., Otero, C., & Qureshi, A. (2012). A Multi-attribute Evaluation of Information Security Controls in Organizations Using Grey Systems Theory. In Proceedings of the International Conference on Security and Management (p. 1).
- GAMS. (2018). General Algebraic Modeling System. Retrieved from: <https://www.gams.com/>
- Gao, C., Li, Z., & Song, H. (2009). Security Evaluation Method Based on Host Resource Availability. In Multimedia and Ubiquitous Engineering, 2009. MUE'09. Third International Conference on (pp. 499–504).
- Gebser, M., Kaufmann, B., Kaminski, R., Ostrowski, M., Schaub, T., & Schneider, M. (2011). Potassco: The Potsdam answer set solving collection. *Ai Communications*, 24(2), 107–124.
- Gobierno de Chile. (2005). Decreto 83: Norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Gobierno de Chile, G. U. I. (2011). Programa de mejoramiento de la gestión sistema de seguridad de la información: Versión 2011.
- Hooker, J. N. (2002). Logic, optimization, and constraint programming. *INFORMS Journal on Computing*, 14(4), 295–321.
- International Organization for Standardization. (2013). ISO 27001:2013 - Information security management. Retrieved from <https://www.iso.org/standard/54534.html>
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360.
- Jiménez-Martín, A., Vicente, E., & Mateos, A. (2015). Selección de salvaguardas en gestión del riesgo en sistemas de la información: un enfoque borroso. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (15), 83–100. <https://doi.org/10.17013/risti.15.83-100>
- Kawasaki, R., & Hiromatsu, T. (2014). Proposal of a model supporting decision-making on information security risk treatment. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 8(4), 583–589.
- Khajouei, H., Kazemi, M., & Moosavirad, S. H. (2017). Ranking information security controls by using fuzzy analytic hierarchy process. *Information Systems and E-Business Management*, 15(1), 1–19. <https://doi.org/10.1007/s10257-016-0306-y>
- Kiesling, E., Ekelhart, A., Grill, B., Straub, C., & Stummer, C. (2013). Simulation-based optimization of IT security controls: Initial experiences with meta-heuristic solution procedures. In Proceedings of 14th EUME Workshop.

- Kiesling, E., Strauss, C., Ekelhart, A., Grill, B., & Stummer, C. (2013). Simulation-based optimization of information security controls: An adversary-centric approach. In *Proceedings of Winter Simulations Conference (WSC)*.
- Kiesling, E., Strauss, C., & Stummer, C. (2012). A Multi-objective Decision Support Framework for Simulation-Based Security Control Selection. In *Seventh International Conference on Availability, Reliability and Security*, 454–462. <https://doi.org/10.1109/ares.2012.70>
- Lv, J.-J., & Wang, Y.-Z. (2010). A ranking method for information security risk management based on ahp and promethee. In *Management and Service Science (MASS), 2010 International Conference on* (pp. 1–4).
- Lv, J., Zhou, Y., & Wang, Y. (2011). A Multi-criteria Evaluation Method of Information Security Controls. In *Fourth International Joint Conference on Computational Sciences and Optimization*, 190–194.
- Meng, M., & Liu, E. (2015). The Application Research of Information Security Risk Assessment Model Based on AHP Method. *Journal of Advances in Information Technology*, 6(4).
- Nagata, K., Amagasa, M., Kigawa, Y., & Cui, D. (2009). Method to Select Effective Risk Mitigation Controls Using Fuzzy Outranking. In *2009 Ninth International Conference on Intelligent Systems Design and Applications*. <https://doi.org/10.1109/isda.2009.186>
- NEOS. (2018). NEOS Server web portal. Retrieved from <https://neos-server.org/neos/>
- Ojamaa, A., Tyugu, E., & Kivimaa, J. (2008). Pareto-optimal situation analysis for selection of security measures. In *MILCOM 2008 - 2008 IEEE Military Communications Conference*. IEEE. <https://doi.org/10.1109/milcom.2008.4753520>
- Otero, A., Ejnoui, A., Otero, C., & Tejay, G. (2011). Evaluation of information security controls in organizations by grey relational analysis. *International Journal of Dependable and Trustworthy Information Systems*, 2(3), 36–54.
- Otero, A., Otero, C., & Qureshi, A. (2010). A Multi-Criteria Evaluation of Information Security Controls Using Boolean Features. *International Journal of Network Security & Its Applications*, 2(4), 1–11. <https://doi.org/10.5121/ijnsa.2010.2401>
- Otero, A. R. (2015). An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems*, 18, 26–45. <https://doi.org/https://doi.org/10.1016/j.accinf.2015.06.001>
- Otero, A., Tejay, G., Otero, D., & Ruiz-Torres, A. (2012). A fuzzy logic-based information security control assessment for organizations. In *Open Systems (ICOS), 2012 IEEE Conference* (pp. 1–6).
- Pereira, T., & Santos, H. (2014). Challenges in Information Security Protection. In *Proceedings 13th European Conference on Cyber Warfare and Security* (pp. 160–166).

- Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, 64, 1–18. <https://doi.org/10.1016/j.infsof.2015.03.007>
- Rees, L. P., Deane, J. K., Rakes, T. R., & Wade, H. (2011). Decision support for Cybersecurity risk planning. *Decision Support Systems*, 51(3), 493–505. <https://doi.org/10.1016/j.dss.2011.02.013>
- Saint-Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. *The Information Management Journal*, (July/August), 60–66.
- Sarala, R., Zayaraz, G., & Vijayalakshmi, V. (2015). Optimal Selection of Security Countermeasures for Effective Information Security. In *Proceedings of the International Conference on Soft Computing Systems* (pp. 345–353). Springer. https://doi.org/10.1007/978-81-322-2674-1_33
- Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems*, 55(1), 156–164. <https://doi.org/10.1016/j.dss.2013.01.001>
- Shahpasand, M., Shajari, M., Golpaygani, S. A. H., & Ghavamipoor, H. (2015). A comprehensive security control selection model for inter-dependent organizational assets structure. *Information and Computer Security*, 23(2), 218–242. <https://doi.org/10.1108/ics-12-2013-0090>
- Tofan, D. (2011). Information Security Standards. *Journal of Mobile, Embedded and Distributed Systems*, 3(3), 128–135.
- Tosatto, S. C., Governatori, G., & Kelsen, P. (2015). Business process regulatory compliance is hard. *IEEE Transactions on Services Computing*, 8(6), 958–970. <https://doi.org/10.1109/TSC.2014.2341236>
- Viduto, V., Maple, C., Huang, W., & López-Peréz, D. (2012). A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. *Decision Support Systems*, 53(3), 599–610. <https://doi.org/10.1016/j.dss.2012.04.001>
- Yameng, C., Yulong, S., Jianfeng, M., Xining, C., & Yahui, L. (2011). AHP-GRAP Based Security Evaluation Method for MILS System within CC Framework. In *Seventh International Conference on Computational Intelligence and Security*.
- Yang, Y., Shieh, H., Leu, J., & Tzeng, G. (2009). A VIKOR-based multiple criteria decision method for improving information security risk. *International Journal of Information Technology & Decision Making*, 8(2), 267–287.
- Yang, Y., Shieh, H., & Tzeng, G. (2013). A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. *Information Sciences*, 232, 482–500.
- Yau, H. (2014). Information Security Controls. *Advances in Robotics & Automation*, 3(2), e118. <https://doi.org/doi:10.4172/2168-9695.1000e118>

- Yevseyeva, I., Basto-Fernandes, V., Emmerich, M., & Van Moorsel, A. (2015). Selecting optimal subset of security controls. *Procedia Computer Science*, 64, 1035–1042. <https://doi.org/10.1016/j.procs.2015.08.625>
- Yevseyeva, I., Fernandes, V. B., Van Moorsel, A., Janicke, H., & Emmerich, M. (2016). Two-stage Security Controls Selection. *Procedia Computer Science*, 100, 971–978. <https://doi.org/10.1016/j.procs.2016.09.261>
- Zhang, H., Chari, K., & Agrawal, M. (2018). Decision support for the optimal allocation of security controls. *Decision Support Systems*, 115, 92-104. <https://doi.org/10.1016/j.dss.2018.10.001>

Crítérios Editoriais

A RISTI (Revista Ibérica de Sistemas e Tecnologias de Informação) é um periódico científico, propriedade da AISTI (Associação Ibérica de Sistemas e Tecnologias de Informação), 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, propiedad de la AISTI (Asociación Ibérica de Sistemas y Tecnologías de la Información), 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.

El 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.

Os asociados da AISTI recebem a RISTI gratuitamente, por correio postal. Torne-se associado da AISTI. Preencha o formulário abaixo e envie-o para o e-mail aistic@gmail.com

Los asociados de la AISTI reciben la RISTI por correo, sin costo alguno. Hazte miembro de la AISTI. Rellena el siguiente formulario y remítelo al e-mail aistic@gmail.com



Formulário de Associado / Formulario de Asociado

Nome/Nombre: _____

Instituição/Institución: _____

Departamento: _____

Morada/Dirección: _____

Código Postal: _____ Localidade/Localidad: _____

País: _____

Telefone/Teléfono: _____

E-mail: _____ Web: _____

Tipo de Associado e valor da anuidade:

☐ Individual - 35€

☐ Instituição de Ensino ou I&D/Institución de Educación o I&D - 250€

☐ Outro (Empresa, etc.) - 500€

NIF/CIF: _____

Data/Fecha: __/__/____ Assinatura/Firma: _____



Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

©AISTI 2019 <http://www.aisti.eu>

