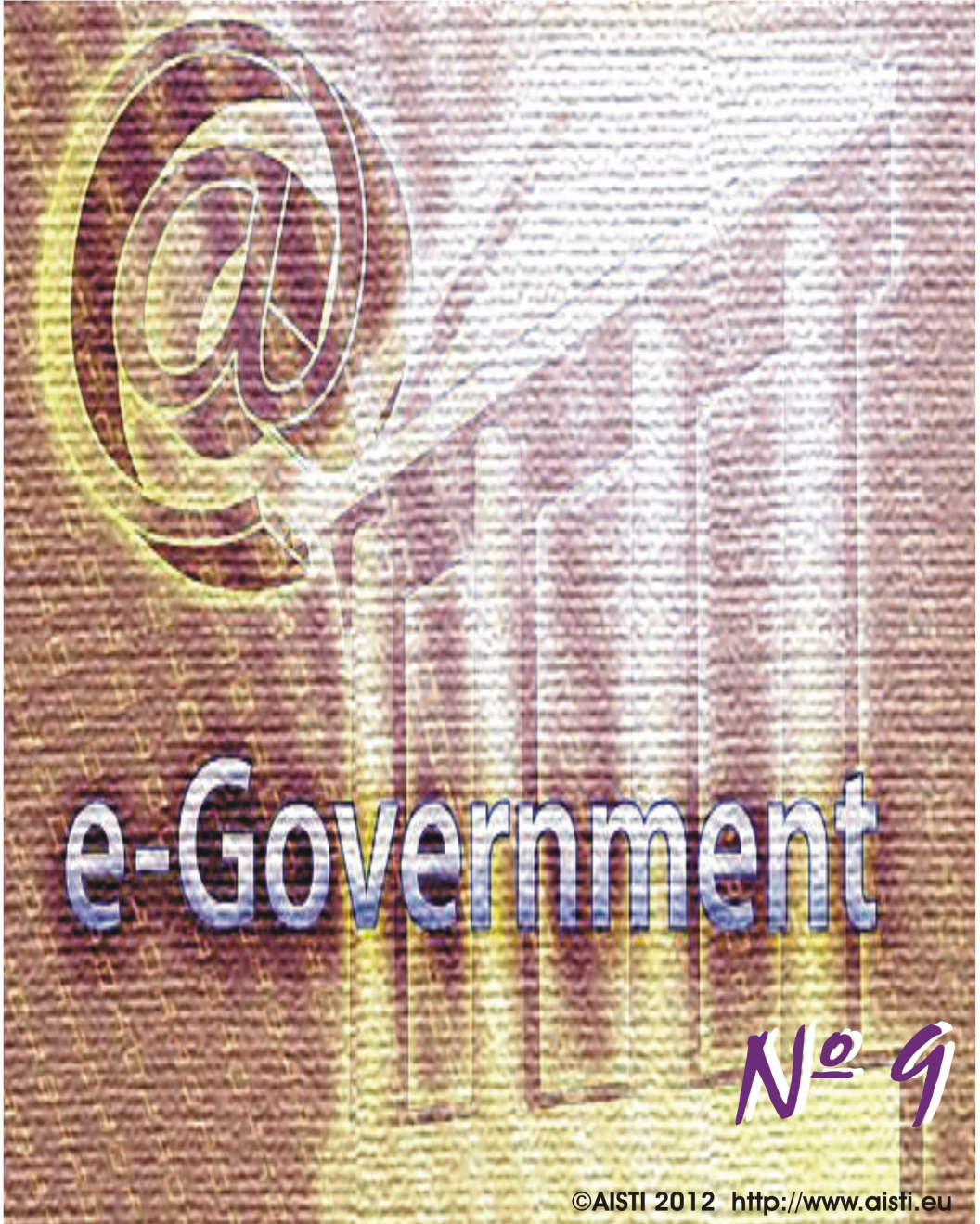




Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

J
U
N
H
O
2
0
1
2
.
J
U
N
I
O
2
0
1
2





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

Edição / Edición

Nº 9, 6/2012

Tiragem / Tirage: 500

Preço por número / Precio por número: 12,5€

Subscrição anual / Suscripción anual: 20€ (2 números)

ISSN: 1646-9895

Depósito legal:

Indexação / Indexación

Academic Journals Database, CrossRef, Dialnet, DOAJ, EBSCO, EI Compendex, GALE, IndexCopernicus, Index of Information Systems Journals, LatinIndex, ProQuest, SCOPUS, Scielo e Ulrich's.

Propriedade e Publicação / Propriedad y Publicación

AISTI – Associação Ibérica de Sistemas e Tecnologias de Informação

Rua de Lagares 523 - Silvares, 4620-646 Lousada, Portugal

E-mail: risti@aisti.eu

Web: <http://www.aisti.eu>

Parceiro / Socio

Academy Publisher: <http://www.academpublisher.com>

Ficha Técnica

Director

Álvaro Rocha, Universidade Fernando Pessoa

Coordenador da Edição / Coordinador de la Edición

Gonçalo Paiva Dias, Universidade de Aveiro

Conselho Editorial / Consejo Editorial

Carlos Ferrás Sexto, Universidad de Santiago de Compostela

Jose Antonio Calvo-Manzano Villalón, Universidad Politécnica de Madrid

Luís Borges Gouveia, Universidade Fernando Pessoa

Luís Paulo Reis, Universidade do Minho

Manuel Pérez Cota, Universidad de Vigo

Maria Manuela Cruz-Cunha, Instituto Politécnico do Cávado e do Ave

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

Secretariado Editorial

Avelino Victor, Instituto Superior da Maia e Instituto de Informática do Porto

Paulo Teixeira, Instituto Politécnico do Cávado e do Ave

Conselho Científico / Consejo Científico

Adolfo Lozano-Tello, Universidad de Extremadura, ES

Alberto Fernández, Universidad Rey Juan Carlos, ES

Aldemar Santos, Universidade Federal de Pernambuco, BR

Alejandro Peña, Escuela de Ingeniería de Antioquia, CO

Ana Maria Correia, Universidade Nova de Lisboa, PT

Ana Paula Afonso, Instituto Politécnico do Porto, PT

Angelica Caro, University of Bio Bio, CL

Antoni Lluís Mesquida Calafat, Universitat de les Illes Balears, ES

Antonia Mas Pichaco, Universitat de les Illes Balears, ES

António Godinho, ISLA-Gaia, PT

António Pereira, Instituto Politécnico de Leiria, PT

Armando Mendes, Universidade dos Açores, PT
Armando Sousa, Universidade do Porto, PT
Arturo J. Méndez, Universidad de Vigo, ES
Carlos Costa, Universidade de Aveiro, PT
Carlos Rabadão, Instituto Politécnico de Leiria, PT
Carlos Vaz de Carvalho, Instituto Politécnico do Porto, PT
Carmen Galvez, Universidad de Granada, ES
Ciro Martins, Universidade de Aveiro, PT
Daniel Castro Silva, Universidade de Coimbra, PT
Daniel Polónia, Universidade de Aveiro, PT
Didac Busquets, Imperial College London, UK
Eduardo Luís Cardoso, Universidade Católica Portuguesa - Porto, PT
Feliz Gouveia, Universidade Fernando Pessoa, PT
Fernando Bandeira, Universidade Fernando Pessoa, PT
Fernando Diaz, Universidad de Valladolid, ES
Francisco Restivo, Universidade Católica Portuguesa - Braga, PT
García Pérez-Schofield Baltasar, Universidad de Vigo, ES
Gonçalo Paiva Dias, Universidade de Aveiro, PT
Ivan Garcia, Universidad Tecnológica de la Mixteca, MX
Jaime S. Cardoso, Universidade do Porto, PT
Javier Garcia Tobio, CESGA-Centro de Supercomputacion de Galicia, ES
Jezreel Mejia, Centro de Investigación en Matemática, MX
João Paulo Costa, Universidade de Coimbra, PT
João Sarmento, Universidade do Minho, PT
João Tavares, Universidade do Porto, PT
Joana Maria Seguí Pons, Universitat de les Illes Balears, ES
Joaquim Reis, Instituto Superior de Ciências do Trabalho e da Empresa, PT
Jörg Thomaschewski, University of Applied Sciences OOW - Emden, DE
José Felipe Cocón Juárez, Universidad Autónoma del Carmen, MX
José Paulo Lousado, Instituto Politécnico de Viseu, PT
José Luis Pardo Díaz, Instituto Tecnológico Virtual de Educación, VE
Jose M Molina, Universidad Carlos III de Madrid, ES

José Silvestre Silva, Universidade de Coimbra, PT
Juan Carlos González Moreno, Universidad de Vigo, ES
Juan José de Benito Martín, Universidad de Valladolid, ES
Juan Manuel Fernández-Luna, Universidad de Granada, ES
Juan-Manuel Lopez-Zafra, Universidad Complutense de Madrid, ES
Luís Correia, Universidade de Lisboa, PT
Luis de Campos, Universidad de Granada, ES
Luis Fernandez-Sanz, Universidad de Alcalá, ES
Luisa María Romero-Moreno, Universidad de Sevilla, ES
Magdalena Arcilla Cobián, Universidade Nacional de Educação a Distância, ES
Marco Painho, Universidade Nova de Lisboa, PT
Maria Clara Silveira, Instituto Politécnico da Guarda, PT
Maria Helena Monteiro, Universidade Técnica de Lisboa, PT
María J. Lado, Universidad de Vigo, ES
Maria João Castro, Instituto Politécnico do Porto, PT
Martín Llamas Nistal, Universidad de Vigo, ES
Mercedes Ruiz, Universidad de Cádiz, ES
Miguel Castro Neto, Universidade Nova de Lisboa, PT
Mirna Ariadna Muñoz Mata, Centro de Investigación en Matemáticas (CIMAT) -
Unidad Zacatecas, MX
Nuno Lau, Universidade de Aveiro, PT
Nuno Ribeiro, Universidade Fernando Pessoa, PT
Orlando Belo, Universidade do Minho, PT
Paulo Pinto, Universidade Nova de Lisboa, PT
Pedro Abreu, Universidade de Coimbra, PT
Pedro Miguel Moreira, Instituto Politécnico de Viana do Castelo, PT
Pedro Nogueira Ramos, Instituto Superior de Ciências do Trabalho e da Empresa, PT
Pedro Pimenta, Universidade do Minho, PT
Pedro Sanz Angulo, Universidad de Valladolid, ES
Reinaldo Bianchi, Centro Universitário da FEI, BR
Santiago Gonzales Sánchez, Universidad Inca Garcilaso de la Vega, PE
Sergio Gálvez Rojas, Universidad de Málaga, ES
Tomás San Feliu Gilabert, Universidad Politécnica de Madrid, ES

Vitor Santos, Universidade de Trás-os-Montes e Alto Douro, PT
Xose A. Vila, Universidad de Vigo, ES

Editorial

A presente edição da RISTI é dedicada aos temas de *eGovernment*, *eDemocracy* e *eParticipation*. São temas abrangentes e claramente interdisciplinares. Mesmo do ponto de vista específico dos sistemas e tecnologias de informação, as possibilidades de contribuição científica são diversificadas, incluindo, entre outros aspetos, os modelos de desenvolvimento, as arquiteturas de suporte, a avaliação de impacto e as tecnologias de base. É ao nível destes aspetos que os seis artigos publicados no número 9 da RISTI se enquadram na temática proposta.

A seleção de artigos que se apresenta é o resultado de um exigente processo de avaliação das 33 propostas originalmente submetidas, provenientes de 10 países e de 3 continentes. Cada artigo foi avaliado por, pelo menos, três membros da Comissão Científica, resultando numa taxa de aceitação final de 18%. A qualidade evidenciada pelos seis artigos publicados é a face visível da exigência desse processo.

No primeiro artigo, propõe-se uma linguagem de modelação gráfica para a tramitação de procedimentos no domínio específico da administração eletrónica. A linguagem baseia-se na definição de um meta-modelo de administração pública, em que se definem as principais entidades que a compõe e as relações entre elas. Descreve-se ainda uma ferramenta gráfica de modelação e a sua validação usando casos reais.

O segundo artigo apresenta um modelo de segurança para uma arquitetura de interoperabilidade baseada em agentes autónomos que suporta a composição dinâmica de *workflows* na administração pública. O modelo suporta a identificação, autenticação, acreditação e autorização dos agentes e garante que os resultados produzidos apenas são entregues aos seus destinatários, mesmo que esses destinatários não sejam conhecidos na altura da produção do resultado.

No terceiro artigo, descreve-se o sistema de informação do Banco de Terras da Galiza, um organismo galego que atua como intermediário entre proprietários e agricultores para fomentar o arrendamento de terras e evitar o seu abandono. Detalham-se a arquitetura, componentes e funcionalidades do sistema e apresentam-se dados estatísticos da sua utilização.

O quarto artigo apresenta uma plataforma de mediação digital para a participação pública direta em períodos eleitorais. A aplicação foi especificamente desenhada para juntar, num único espaço neutro, regulado e deliberativo, os principais intervenientes numa eleição, promovendo a colaboração e a comunicação multidirecional entre eles. Apresentam-se as principais áreas funcionais da plataforma e os resultados de um caso de estudo sobre as últimas eleições legislativas em Portugal.

No quinto artigo, propõe-se um modelo de maturidade para a classificação do grau de proteção de privacidade em redes sociais. Este modelo é complementado por um quadro de análise, que padroniza a avaliação da privacidade, e por uma ferramenta na forma de *balanced scorecard*, que suporta auditorias de avaliação da privacidade.

O sexto artigo apresenta uma aplicação que permite aos utilizadores de dispositivos móveis recolher e preservar objetos digitais de forma contextualizada. Os autores argumentam que a aplicação permite colmatar o problema de obsolescência resultante da rápida evolução das tecnologias e do *software* usados nos dispositivos móveis.

Termino com uma palavra de agradecimento a todos os autores que submeteram o seu trabalho científico para ser avaliado para publicação nesta edição da RISTI; aos membros da Comissão Científica, pela criteriosa avaliação que fizeram dos artigos submetidos; e ao Conselho Editorial, pelo convite para editar este número da Revista. Foi com grande gosto que o fiz, ciente do percurso que tem sido feito pela mesma e da importância que já tem e, estou certo, se alargará, na consolidação de uma comunidade de expressão portuguesa e espanhola na área dos sistemas e tecnologias de informação.

Ainda uma palavra final para me congratular pelo facto de, a partir da presente edição, a RISTI passar a contar com o apoio da *Academy Publisher*, o que contribuirá certamente para uma maior divulgação da revista e permitirá que os artigos publicados passem a ser identificados através de DOI (*Digital Object Identifier*).

Gonçalo Paiva Dias

Universidade de Aveiro

Índice

Modelado específico de procedimientos en el dominio de la Administración Electrónica	1
<i>Guillermo Infante Hernández, Benjamín López Pérez, Aquilino Adolfo Juan Fuente</i>	
Modelo de segurança para a composição dinâmica de <i>workflows</i> em arquiteturas de <i>e-government</i>	15
<i>Fábio Marques, Gonçalo Paiva Dias, André Zúquete</i>	
Sistema de Información del Banco de Tierras de Galicia	27
<i>Juan Porta, Jorge Parapar, Paula García, Gracia Fernández, Juan Touriño, Francisco Ónega, Pablo Díaz, David Miranda, Rafael Crecente</i>	
iLeger: Uma proposta de Mediação Digital para Períodos Eleitorais	43
<i>Artur Afonso de Sousa, Luís Borges Gouveia</i>	
Evaluación de la Privacidad de una Red Social Virtual	59
<i>J. R. Coz Fernández, E. Fojón Chamorro, R. Heradio Gil, J. A. Cerrada Somolinos</i>	
Recolha, preservação e contextualização de objectos digitais para dispositivos móveis com <i>Android</i>	75
<i>Raquel Soares, Marco Pereira, Joaquim Arnaldo Martins</i>	

Modelado específico de procedimientos en el dominio de la Administración Electrónica

Guillermo Infante Hernández ¹, Benjamín López Pérez ¹, Aquilino Adolfo Juan Fuente ¹

infante@innova.uniovi.es, benja@uniovi.es, aajuan@uniovi.es

¹ Departamento de Informática, Universidad de Oviedo, 33007, Oviedo, España.

DOI: 10.4304/risti.9.1-14

Resumen: Debido a la complejidad que reviste el dominio de la Administración Electrónica (AE), las desarrolladas deberán ser capaces de integrarse con la multitud de plataformas y sistemas que componen dicho dominio. El impacto de esta integración además mejorar la tramitación de procedimientos. En el presente trabajo se propone un lenguaje de modelado gráfico (DSL) para la tramitación de procedimientos en el dominio específico de la AE. Este lenguaje parte de la definición de un metamodelo de AE que identifica sus principales entidades y define sus relaciones. Además se construyó una herramienta gráfica de modelado la cual fue probada con dos casos de estudio reales. aplicaciones

Palabras clave: Administración Electrónica; Metamodelo; DSL

Abstract: Due to the complexity involved in E-Government domain applications, the developed ones should be able to interoperate with the growing number of emerging management platforms. The impact of this integration has among its main goals to improve the procedure management task, which suffers an important lack of technological proposals. This work proposes a graphical domain specific language (DSL) for procedure management in E-Government domain. This language came from the definition of a metamodel that states the principle E-Government elements and defines its relations. A further graphical modeling tool was developed to implement the DSL and was tested with two actual case studies.

Keywords: E-Government; Metamodel; DSL

1. Introducción

El desarrollo de la AE particularmente en España ha venido acompañado de la aprobación de una normativa que lo regula y garantiza su evolución. Dentro de esta normativa se destaca la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP, Ley 11/2007, de 22 de junio) que se ha visto reforzada por medidas aprobadas por la Unión Europea como la Directiva de Servicios (DS 2006/123/CE). Para la puesta en marcha de la Directiva de Servicios, se solicita la aplicación de

medidas concretas, como las ventanillas únicas para prestadores de servicios, la puesta en marcha de procedimientos por vía electrónica y la cooperación administrativa entre los estados miembros. En este sentido ha quedado regulada la forma en la que llevar la administración electrónica a los ciudadanos pero aún existe la necesidad de propuestas tecnológicas concretas de cómo hacerlo.

La principal idea que abarca este trabajo está relacionada precisamente con una propuesta tecnológica para el modelado de procedimientos administrativos en el contexto de la Administración Electrónica. Partiendo de esta idea se hace a continuación una relación de las principales contribuciones aportadas:

- Se definió un metamodelo que integra las entidades principales identificadas en el dominio de la AE, el cual se encuentra descrito en la Sección 2.1. Hasta el momento no se había encontrado un metamodelo que identificase estas entidades y definiese sus relaciones. Éste constituye un paso fundamental para lograr consenso en lo que a tramitación por medios electrónicos se refiere.
- Se construyó una herramienta gráfica de modelado basada en el metamodelo creado, la cual contribuye a la integración de plataformas distintas de tramitación en el contexto de la Administración Electrónica. Esta integración puede ser alcanzada mediante la traducción de los modelos creados a ficheros XMI de intercambio (Specification, A. A., & Group, O. M., 2003), los cuales pueden ser transformados en código fuente de cualquier lenguaje. La construcción de esta herramienta se describe entre las secciones 2.1 y 2.5.
- Se modelaron dos procedimientos reales con la herramienta creada como caso de estudio descrito en la Sección 3 y se generó un sitio web de forma automática a partir de la información recogida en el modelado de dichos procedimientos.

1.1. Deficiencias en la tramitación de procedimientos

Se han analizado varias aproximaciones de solución a la tramitación electrónica de procedimientos en el contexto de la AE, por ejemplo (Beynon-Davies, P. 2007) define un metamodelo para la AE desde el punto de vista socio-tecnológico. Propone además una serie de modelos de negocio que podrían ser utilizados para el desarrollo de la AE. Este trabajo aunque ve la necesidad de modelar el dominio de la AE no propone soluciones concretas de cómo hacerlo. Por otro lado no utiliza tecnologías de modelado de procesos y carece de una propuesta de solución tecnológica para afrontar este problema.

Otro de los estudios revisados fue el de (Becker, J., Pfeiffer, D., & Räckers, M. ,2007). Este trabajo va un poco más lejos y ya introduce la propuesta de un método para el modelado de procesos de dominio específico en la AP. El enfoque de modelado de dominio específico se ha considerado en este trabajo como la solución al problema de la reorganización de las instituciones. Se ha creado un método que aplica el vocabulario del dominio de la AP para capturar de forma eficiente el mapa de procesos de una organización. Resulta interesante el enfoque de este trabajo ya que introduce el modelado de dominio específico y define un vocabulario para ese dominio. En este caso el objetivo del trabajo se centra en la reorganización administrativa y no en soluciones de tramitación electrónica.

Finalmente se analizó el Proyecto W@nda (2004). Este proyecto ha sido llevado a cabo por la Junta de Andalucía para la tramitación de expedientes de forma electrónica. Basa su solución en un tramitador electrónico y la definición de un dominio semántico. Para identificar las entidades principales se ha basado en los conceptos recogidos en Specification, W. M. (1999) y trata la tramitación de expedientes como una máquina de estados. Este trabajo aunque define un dominio común para la tramitación de expedientes, basa su solución en la aplicación de flujos de trabajo (workflows). Este enfoque formaliza la gestión de actividades y responsabilidades asignadas a cada tarea así como las transiciones entre las mismas, sin embargo restringe la tramitación a una tecnología concreta, lo cual dificulta la estandarización de este proceso.

No obstante, aunque la prestación de servicios a los ciudadanos con el uso de medios electrónicos ha avanzado notablemente, hecho que se ve reflejado en los enfoques analizados entre otros, aún quedan necesidades importantes por cubrir. Basándose en los estudios publicados por la Fundación Orange y La junta de Andalucía, eEspaña (2010) y el Proyecto W@nda (2004) respectivamente, se pueden identificar algunas de estas necesidades. Del total de requisitos posibles, en este trabajo se abarcan los siguientes:

- Debe existir una forma de tramitar común. Procedimientos similares se tramitarán de igual forma en diferentes organizaciones.
- Se debe simplificar la comunicación entre los entornos de tramitación existentes con la utilización de estándares y hacerlos independientes de los Sistemas de Información de los que proceden.

2. DSL para el modelado de procedimientos en AE

Analizados los requisitos e investigadas las propuestas tecnológicas de como satisfacerlos, se utiliza la ingeniería dirigida por modelos (MDE), la cual constituye una solución eficiente para esta tarea. En esta sección se profundiza en estas técnicas y especialmente en la propuesta de arquitectura dirigida por modelos MDA (Booch, G. et al, 2003) para el desarrollo de un lenguaje de dominio específico (DSL) para la tramitación de procedimientos electrónicos.

La elección del desarrollo de un DSL para el modelado de procedimientos en AE viene dado por la propia naturaleza de este dominio. El dominio de la AE está compuesto por un gran número de entidades relacionadas entre sí e interpretadas de forma distinta en diferentes escenarios. La manera en que se realiza la tramitación electrónica resulta una tarea compleja de implementar debido a la normativa que regula su funcionamiento y las variaciones que experimenta de una AP a otra. Es en este contexto surgen problemas de incompatibilidad e interoperabilidad entre las plataformas que componen la AE. A pesar de que la fase inicial del desarrollo de un DSL resulta un proceso costoso, a largo plazo reduce los costes del ciclo de vida de desarrollo debido al incremento de la productividad (Christensen, 2003), figura 1. Esto significa que si se contase con una solución que normalizara en alguna medida el desarrollo de aplicaciones para este dominio, la productividad en el desarrollo de las mismas crecería considerablemente.

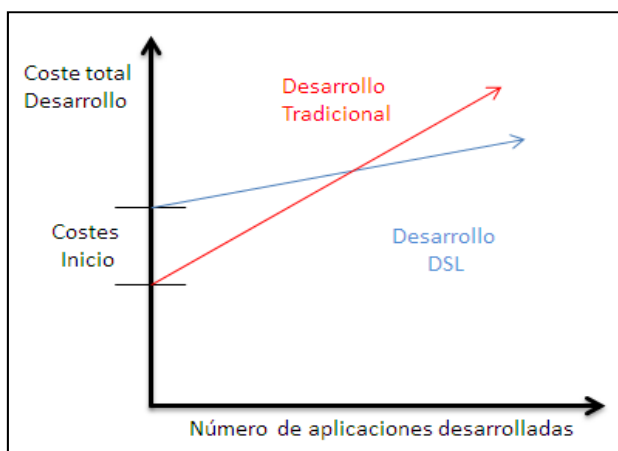


Figura 1 – Rentabilidad del Desarrollo DSL (Christensen, 2003)

El dominio de la AE como se ha mencionado está compuesto por un gran número de entidades. Para sacar verdadero provecho de un DSL, este debe ser diseñado como un lenguaje limitado y estrechamente enfocado a un problema en particular (Fowler, 2006). Por esta razón se han escogido las entidades más significativas que forman parte del proceso de tramitación electrónica para establecer un alcance razonable en el desarrollo de esta propuesta. En esta implementación se escogieron los entornos de GMF y EMF (Gronback, R. C., 2009) para la creación de una herramienta de modelado de procedimientos basada en un DSL. Esta elección está basada en la comparativa de (Pelechano et al, 2006) donde establece un análisis basado en criterios como: *el metamodelado, repositorio, transformaciones entre modelos y validaciones*. La tabla 1 muestra las entidades que forman el núcleo de la tramitación de procedimientos.

Se decidió que esta herramienta debería estar implementada en un entorno gráfico para permitir tanto a personal administrativo como técnico hacer sus desarrollos o modelados sin necesidad de un conocimiento técnico previo.

GMF establece un proceso muy específico para construir esta herramienta. Éste se compone de los siguientes subprocesos: **1.** definición del metamodelo, **2.** generación de código del modelo, **3.** definición de la metáfora gráfica, **4.** definición de las herramientas del modelo, **5.** especificación de la correspondencia entre los elementos del modelo y la metáfora gráfica, y **6.** generación del código de la herramienta. Estos subprocesos se detallan a continuación y se muestran en la figura 2.

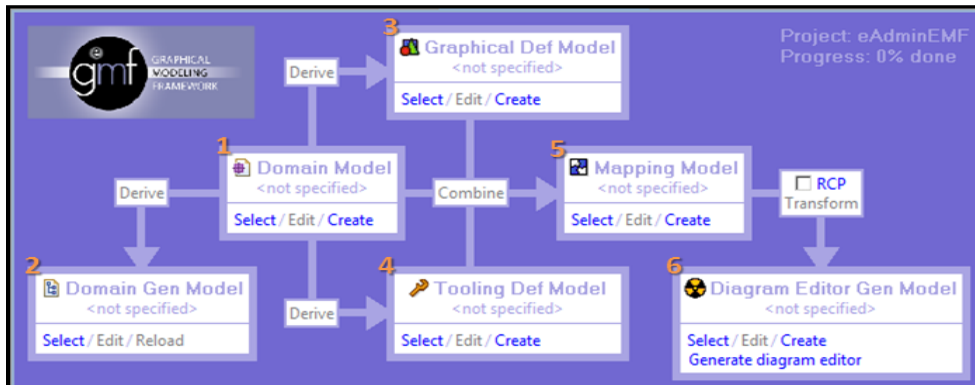


Figura 2 – Construcción de la herramienta DSL con EMF.

2.1. Definición del metamodelo

El metamodelo creado se basa en la definición del dominio específico de la Administración Electrónica definido en la tabla 1.

Tabla 1. Descripción de elementos principales del modelo.

Entidad	Descripción de Dominio
<i>Servicio</i>	"Cualquier actividad realizada por la Administración Pública dirigida a los ciudadanos para satisfacer sus necesidades, derechos u obligaciones".
<i>Procedimiento</i>	"Proceso de toma de decisiones en la Administración Pública".
<i>Trámite</i>	"Secuencia ordenada de tareas o actuaciones que representa la unidad básica de gestión dentro de un procedimiento.
<i>Interesado</i>	"Usuario participante en el procedimiento en el momento que forme parte activa en la tramitación del mismo".
<i>Expediente</i>	"Conjunto de documentos que integran un procedimiento administrativo".

GMF precisa de un metamodelo y para ello se sirve de EMF, el cual constituye un marco de modelado que soporta y genera documentos XMI con la especificación del dominio. El área de trabajo o modelado de EMF muestra parte del metamodelo creado en la figura 3.

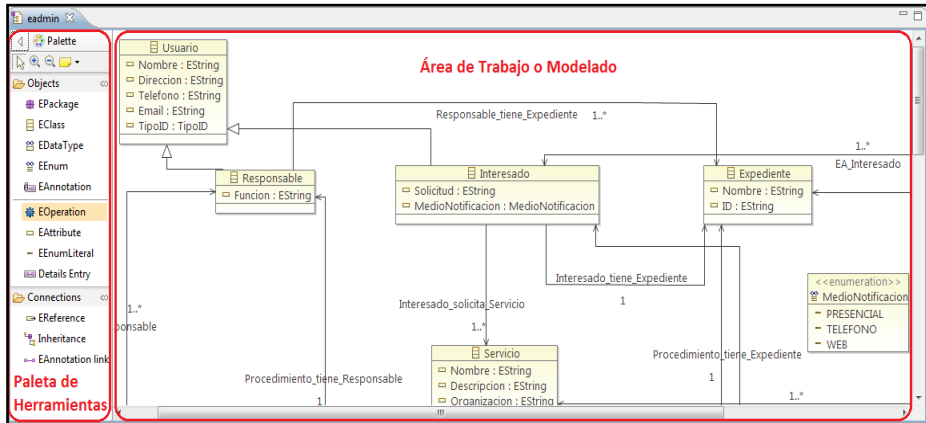


Figura 3 – Área de trabajo y paleta de herramientas EMF.

El árbol resultante con la totalidad de las entidades modeladas se muestra en la figura 4.

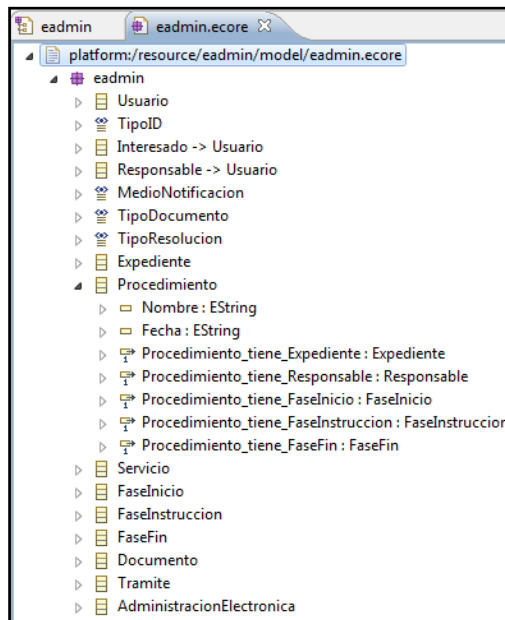


Figura 4 – Árbol del Metamodelo de Administración Electrónica.

2.2. Generación del código del modelo

El código del modelo se genera aplicando patrones de transformación. El resultado de la generación es un conjunto de clases e interfaces Java, que serán utilizadas más adelante en el proceso de creación de la herramienta de modelado específico de dominio. El objetivo de esta transformación es que todos los elementos que constituyen la herramienta se comporten tal y como el metamodelo creado lo establece. El código generado se muestra en la figura 5.

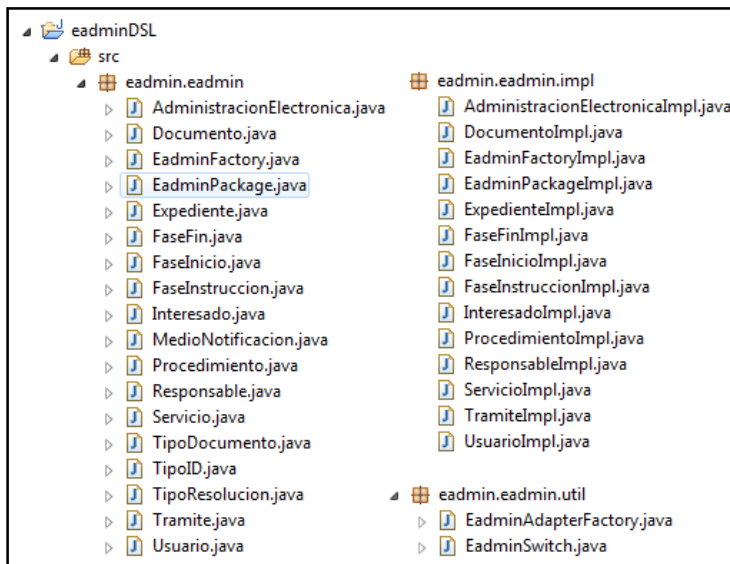


Figura 5 – Código Generado para el metamodelo de AE.

2.3. Definición de la metáfora gráfica y herramientas

La definición gráfica consiste en decidir qué primitivas de modelado harán la función de nodos (elementos de la herramienta de modelado que se desea construir), cuáles serán conectores (enlaces entre los nodos de la herramienta de modelado) y cuáles etiquetas (propiedades de los nodos y enlaces de la herramienta de modelado). En este paso además se define el panel de herramientas y el aspecto que tendrán todos los elementos gráficos del modelo tales como la iconografía de la paleta donde se representa cada nodo, enlace y propiedad.

2.4. Correspondencia entre los elementos del modelo y la metáfora gráfica

En este escenario todo lo creado anteriormente cobra sentido ya que se relacionan y asocian todos y cada uno de los elementos creados con anterioridad. El objetivo fundamental de este paso es el de asegurar que todas las anteriores especificaciones se han realizado correctamente y mantienen coherencia.

2.5. Generación del código de la herramienta

Una vez terminado el subproceso de mapeo, se completa el proceso de definición de la herramienta de modelado gráfico de procedimientos. El último paso para poder ejecutar la herramienta es la generación de su código, el cual se hace de forma totalmente automática. Una vez generado el código es posible ejecutar la herramienta como un plug-in de Eclipse¹. La figura 6 muestra la interfaz de la herramienta creada.

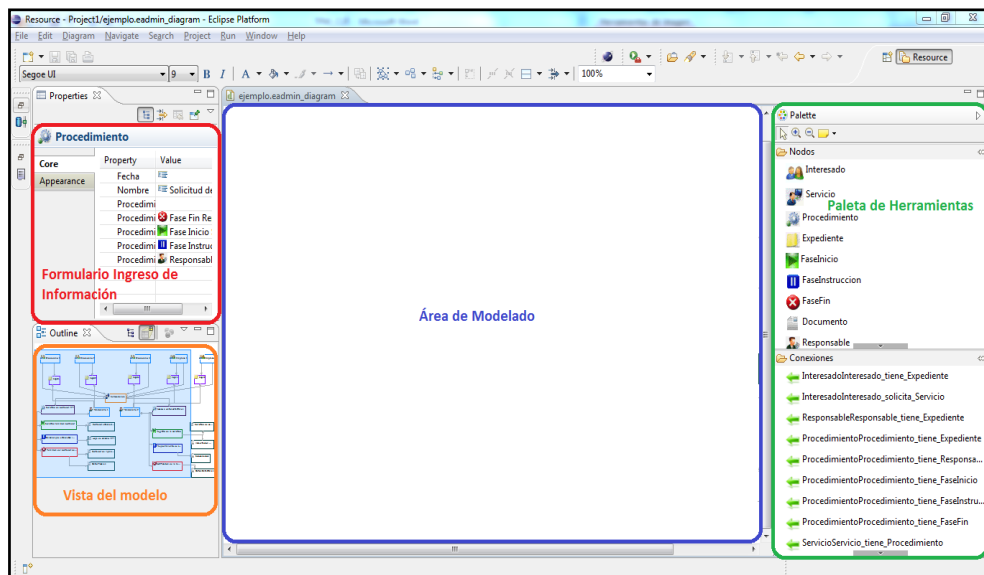


Figura 6 – Herramienta de modelado gráfico.

3. Caso de Estudio

En este caso en particular se modelaron dos procedimientos ofrecidos a través de los servicios del Ministerio de Hacienda (MEH²). La implementación de estos procedimientos no va más allá de los propósitos demostrativos que se persiguen para validar la herramienta con casos reales. El primero de ellos es el procedimiento de Solicitud de borrador de IRPF, el cual persigue el objetivo de facilitar la confección y presentación de la Declaración del Impuesto sobre la Renta de las Personas Físicas y cuyo órgano responsable es la Agencia Estatal de Administración Tributaria. El segundo de los procedimientos modelados fue el de Acceso a datos catastrales cuyo objetivo es facilitar la consulta y certificación de datos catastrales y la obtención de copias de documentos, su órgano responsable es la Dirección General del Catastro.

¹ Entorno de Desarrollo (IDE). <http://www.eclipse.org/>

² Ministerio de Economía y Hacienda. <http://www.meh.es/>

La descripción detallada de ambos procedimientos puede consultarse en el MEH. El modelado definido para ambos procedimientos con la herramienta creada puede visualizarse con más detalle en la figura 7.

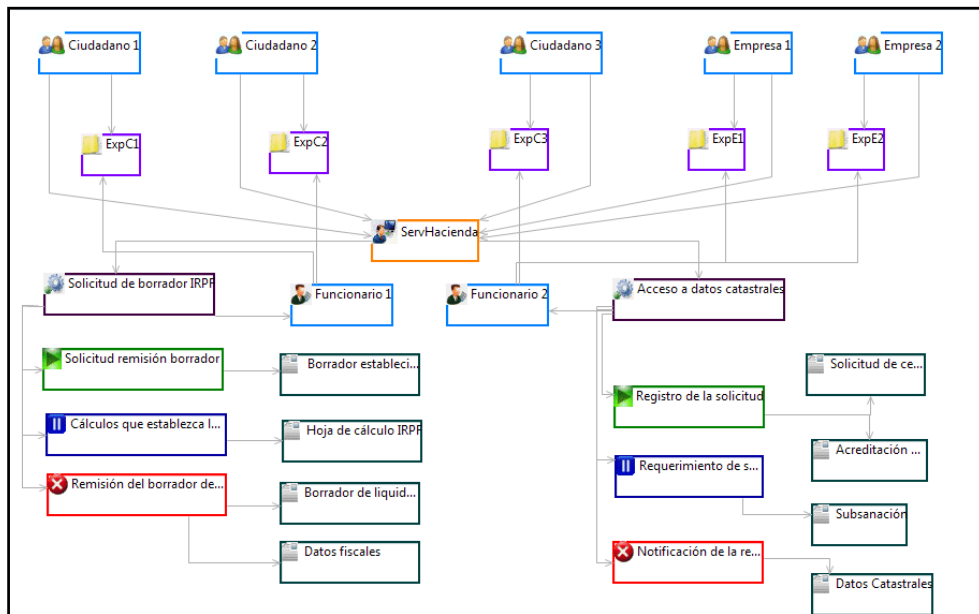


Figura 7 – Caso de estudio modelado con la herramienta creada.

El modelo creado es recogido en el formato XMI. Esta información recoge íntegramente el modelo creado con la herramienta y permite su posterior transformación a texto aplicando plantillas en lenguaje MOFScript (Oldevik et al., 2005), mediante las cuales es posible generar código a cualquier lenguaje de propósito general. Una vez transformado este fichero XMI al lenguaje que se desee, la aplicación resultante podrá ser desplegada en la plataforma escogida para su utilización.

Como se había planteado, este formato recoge toda la información del modelo creado: sus nodos, conexiones y datos introducidos. En el fragmento de la figura 8 se muestra el **Nodo** Procedimiento y los distintos componentes del modelo recogidos en XMI. En este caso el **Dato** que se muestra es el nombre del procedimiento en cuestión; las **Conexiones** representan los enlaces de este nodo a otros nodos o entidades previamente definidos en el metamodelo y las **Referencias** indican hacia donde apunta cada conexión, o sea el nodo destino de la conexión.

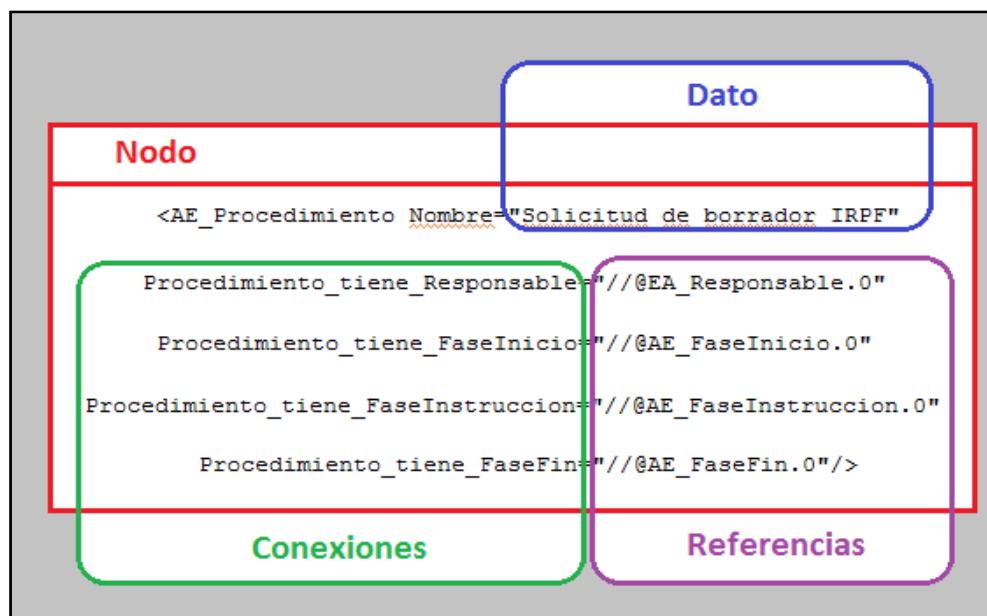
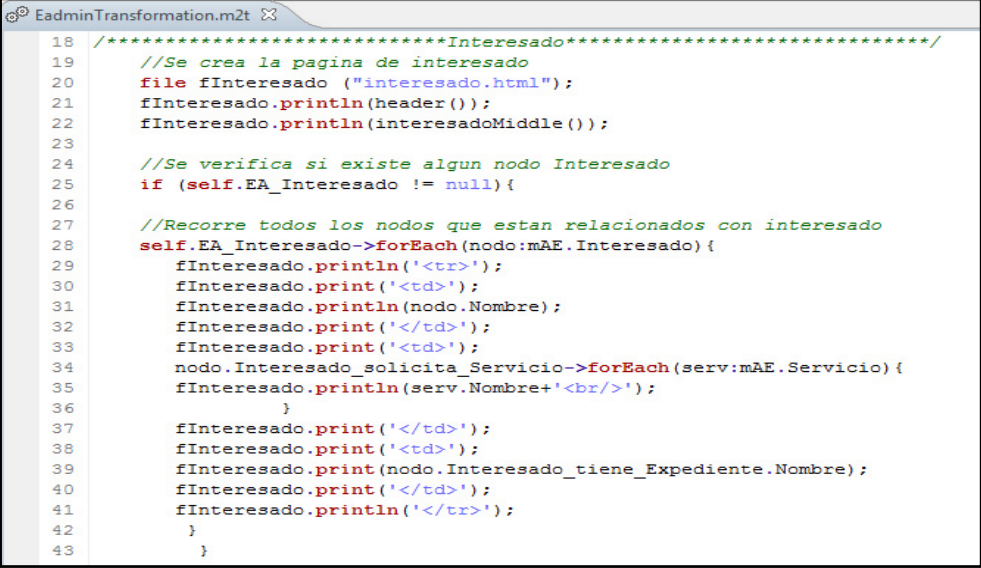


Figura 8 – Detalle XMI del modelo del caso de estudio.

4.1. Transformación y despliegue del modelo específico creado.

Una vez completado el modelado específico es posible transformar éste a código fuente de una aplicación web que muestre la información recogida en el modelo así como cualquier lógica que se desee implementar con el código generado. Esta transformación es llevada a cabo mediante el uso del lenguaje MOFScript. Se transforma el fichero XMI generado por la herramienta gráfica, el cual contiene un esquema de todos los datos contenidos en el modelo creado. La figura 9 muestra un fragmento del código creado con MOFScript. Se recorrieron todos los nodos del modelo creado de forma similar a un grafo dirigido y se fue extrayendo la información contenida en cada nodo.



```
18  //*****Interesado*****/
19  //Se crea la pagina de interesado
20  file fInteresado ("interesado.html");
21  fInteresado.println(header());
22  fInteresado.println(interésadoMiddle());
23
24  //Se verifica si existe algun nodo Interésado
25  if (self.EA_Interésado != null){
26
27  //Recorre todos los nodos que estan relacionados con interesado
28  self.EA_Interésado->forEach(nodo:mAE.Interésado){
29      fInterésado.println('<tr>');
30      fInterésado.print('<td>');
31      fInterésado.println(nodo.Nombre);
32      fInterésado.print('</td>');
33      fInterésado.print('<td>');
34      nodo.Interésado_solicita_Servicio->forEach(serv:mAE.Servicio){
35          fInterésado.println(serv.Nombre+'<br/>');
36      }
37      fInterésado.print('</td>');
38      fInterésado.print('<td>');
39      fInterésado.print(nodo.Interésado_tiene_Expediente.Nombre);
40      fInterésado.print('</td>');
41      fInterésado.println('</tr>');
42  }
43  }
```

Figura 9 – Fragmento de la plantilla MOFScript creada.

Se ha generado posteriormente un sitio web automáticamente a partir de la plantilla MOFScript creada. Todo el código HTML así como las hojas de estilo fueron generados por la herramienta. En esta etapa del trabajo se ha decidido implementar una representación tabulada de los datos obtenidos del modelo con el objetivo de demostrar la funcionalidad de la herramienta gráfica creada y el cierre del ciclo de vida de desarrollo del software mediante la aplicación de MDA. La figura 10 muestra una de las páginas del sitio generado.



Figura 10 – Página "Procedimientos" del sitio web generado.

5. Conclusiones

Se ha propuesto la integración de todos los conceptos identificados en la literatura para dar una visión más clara de cómo se relacionan los mismos en el contexto de la Administración Electrónica. Esto ha facilitado la creación de un metamodelo a partir de la definición del dominio de la misma.

A partir del metamodelo, se desarrolló un lenguaje de dominio específico para la Administración Electrónica donde se definió la semántica de dicho lenguaje en función del dominio y de las metáforas gráficas para su posterior implementación.

Se construyó una herramienta gráfica de modelado específico de procedimientos en el dominio de la Administración Electrónica.

Se modelaron dos casos de estudio reales generando a partir de los mismos un sitio web de forma automática con la información recogida en ambos modelos.

6. Trabajo Futuro

Toda investigación genera inquietudes y nuevas líneas por donde encaminar el trabajo futuro. A través del estudio de los conocimientos actuales en este campo y el análisis de los resultados obtenidos se pueden identificar algunas líneas futuras vinculadas con este tema. Una relación de estas líneas o posibles tareas a tener en cuenta para próximas intervenciones se propone a continuación.

- Realizar un estudio de arquitecturas existentes en la Administración Electrónica para identificar sus elementos comunes. Esto permitiría estandarizar los desarrollos y generar artefactos software con una ampliación de la herramienta creada para cada plataforma específica.
- Tomar una muestra de procedimientos de distintas administraciones y realizar su representación en la herramienta, contrastando posteriormente si se ha podido recoger toda la información de los distintos procedimientos en el modelo o si se detecta que existen carencias.

Referencias bibliográficas

- Beynon-Davies, P. (2007). Models for e-government. Transforming Government People Process and Policy, 1(1), 7-28. Retrieved from <http://www.emeraldinsight.com/10.1108/17506160710733670>
- Becker, J., Pfeiffer, D., & Räckers, M. (2007). Domain Specific Process Modelling in Public Administrations – The PICTURE-Approach. (M. A. Wimmer, J. Scholl, & A. Gronlund, Eds.)6th International Conference EGOV 2007. Springer Berlin/Heidelberg. Obtenido de <http://www.springerlink.com/content/umhvo013w7581p49/?p=e5a056cd4bc14422912773fca8776eec&pi=6>.
- BOE. (2007). Ley 11/2007, de 22 de junio, para el acceso electrónico de los ciudadanos a los Servicios Públicos, Obtenido de http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/12352
- Booch, G., Brown, A. W., Iyengar, S., Rumbaugh, J., & Selic, B. (2004). An MDA Manifesto. Business Process TrendsMDA Journal. Obtenido de <http://www.citeulike.org/group/2440/article/1271715>
- Christensen, N.H. (2003). Domain-Specific Languages in Software Development and the relation to partial evaluation, PhD thesis, DIKU, Dept. of Computer Science, University of Copenhagen, Denmark.
- eEspaña (2010). Madrid: Fundación Orange France Telecom. Obtenido de http://fundacionorange.es/fundacionorange/analisis/eespana/e_espana10_10.html
- Fowler M. (2006). DSL Boundary, Obtenido de <http://martinfowler.com/bliki/DslBoundary.html>
- Gronback, R. C. (2009). Eclipse Modeling Project: A Domain-Specific Language (DSL) Toolkit. (E. Gamma, L. Nackman, & John Wiegand, Eds.) Eclipse Series (p. 736). Addison-Wesley Professional. Obtenido de <http://www.amazon.com/Eclipse-Modeling-Project-Domain-Specific-Language/dp/0321534077>
- Oldevik, J., Neple, T., Grønmo, R., Aagedal, J., & Berre, A.-J. (2005). Toward Standardised Model to Text Transformations. In A. Hartman & D. Kreische (Eds.), European Conference on Modeldriven Architecture Foundation and Application ECMDAFA. Springer Berlin/Heidelberg. doi:10.1007/11581741_18

- Pelechano V., Albert M., Muñoz J., and Cetina C., Building Tools for Model Driven Development Comparing Microsoft DSL Tools and Eclipse Modeling Plug-ins, In Proceedings of the 11th Conference on Software Engineering and Database (JISBD'06), Barcelona, España, 2006.
- Specification, A. A., & Group, O. M. (2003). XML Metadata Interchange (XMI) Specification. Management, 01(May). Obtenido de <http://www.omg.org/spec/XMI/>
- Specification, W. M. (1999). Workflow Management Coalition Terminology & Glossary (Document No. WFMC-TC-1011). Workflow Management Coalition Specification. Obtenido de <http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20&path=ASIN/B002DJ1BEK>.
- W@nda (2004). Proyecto W@nda: WORKFLOW EN LA ADMINISTRACIÓN ANDALUZA. Domnio Semántico. ISBN: 84-688-7845-6 Obtenido de <https://wso24.juntadeandalucia.es/pluton/adminelec/ArTec/wanda.jsp>.

Modelo de segurança para a composição dinâmica de *workflows* em arquiteturas de *e-government*

Fábio Marques ^{1,4}, Gonçalo Paiva Dias ^{1,3}, André Zúquete ^{2,4}

fabio@ua.pt, gpd@ua.pt, andre.zuquete@ua.pt

¹ Escola Superior de Tecnologia e Gestão de Águeda da Universidade de Aveiro, Rua Comandante Pinho e Freitas, nº28, 3750-127, Águeda, Portugal

² Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro, Campus Universitário de Santiago, 3810-193, Aveiro, Portugal

³ Unidade de Investigação em Governança, Competitividade e Políticas Públicas, Campus Universitário de Santiago, 3810-193, Aveiro, Portugal

⁴ Instituto de Engenharia Eletrónica e Telemática de Aveiro, Campus Universitário de Santiago, 3810-193, Aveiro, Portugal

DOI: 10.4304/risti.9.15-26

Resumo: As arquiteturas de interoperabilidade permitem a criação de *workflows* transversais na administração pública e a integração de serviços na perspetiva dos cidadãos e empresas. Neste artigo apresentamos um modelo de segurança que visa as questões levantadas por arquiteturas de interoperabilidade baseadas em agentes autónomos que suportam a composição dinâmica de *workflows*. O modelo baseia-se numa infraestrutura de chave pública e num conjunto de estruturas de dados baseadas em normas bem conhecidas (X.509 V3 e WSDL). Este modelo de segurança suporta a identificação, autenticação, acreditação e autorização e garante que os resultados produzidos pelos agentes apenas são entregues aos seus destinatários, mesmo que estes destinatários não sejam conhecidos na altura da produção do resultado.

Palavras-chave: e-government; Segurança; Workflows dinâmicos; Privacidade; Interoperabilidade.

Abstract: Interoperability architectures allow the creation of transversal workflows in the public administration and the integration of services from the perspective of citizens and businesses. In this paper we present a security model to address the security issues that are raised by an interoperability architecture that supports the dynamic composition of e-government workflows by autonomous agents. The model is based in a Public Key Infrastructure and a set of data structures which are supported on well-known standards (X.509 V3 and WSDL). It addresses agent identification, authentication, accreditation and authorization and ensures that results produced by agents are privately delivered to their intended recipients even though those recipients may not be known when the results are produced.

Keywords: e-government; Security; Dynamic workflows; Privacy; Interoperability.

1. Introdução

A Organização para a Cooperação e Desenvolvimento Económico (OCDE) define e-government como “A utilização das Tecnologias da Informação e da Comunicação em atividades de governo” (OECD, 2001). As arquiteturas de interoperabilidade constituem uma das mais importantes aplicações das Tecnologias da Informação e da Comunicação (TIC) no governo. Estas arquiteturas suportam a partilha de informação entre ramos da administração pública, promovendo a eficiência e permitindo a integração de serviços na ótica dos cidadãos e empresas.

Em (Marques, Dias & Zúquete, 2011) foi apresentada uma arquitetura de interoperabilidade para e-government que segue a composição de serviços como abordagem, é mutável, adaptável, versátil e segura. Esta arquitetura é intrinsecamente dinâmica, permite a criação e remoção de novos serviços e de prestadores de serviço em qualquer altura. Devido ao seu dinamismo, não se aplica o paradigma comum de todos os prestadores de serviços serem confiáveis e autorizados para interagir com todos os restantes prestadores de serviços: um sistema de segurança dinâmico é essencial. Neste artigo apresentamos um modelo que, baseando-se na Tecnologia de Infraestrutura de Chave Pública (PKI), permite a criação dinâmica de esquemas de verificação de segurança no *e-government*.

O artigo está organizado da seguinte forma: começamos por introduzir o problema na presente secção; o trabalho relacionado é abordado na secção 2; na secção 3 fazemos uma breve introdução à arquitetura de interoperabilidade baseada em agentes; na secção 4 apresentamos o modelo de segurança; seguindo-se na secção 5 a discussão; o artigo é concluído na secção 6.

2. Trabalho Relacionado

A segurança tem sido uma das maiores preocupações no desenvolvimento de plataformas baseadas em agentes e em sistemas de *workflow*.

As características das plataformas de agentes e o seu cariz genérico conduziram ao desenvolvimento de vários modelos de segurança. Por exemplo, em (Stormer, Knorr & Eloff, 2000) os autores propuseram uma aproximação baseada em RBAC (*Role Based Access Control*) para autorização e em SoD (*Separation of Duties*) para a aplicação da integridade. Em (Savarimuthu, Purvis & Oliveira, 2004) os autores utilizaram uma PKI para suportar a autenticação de agentes e impuseram autorização RBAC através da utilização de hierarquias suportadas por PKI (cada Autoridade Certificadora pertence a uma sociedade diferente e cada sociedade representa uma função na plataforma). Em (Kannammal & Iyengar, 2008) é utilizado um *Key Server* que atua como um elemento de confiança comum para armazenar as chaves do *Launcher Agent* e dos agentes móveis. As chaves e o *Key Server* têm um papel central no modelo de segurança, permitindo autenticação aos agentes móveis, autenticação interdomínio e gestão da confiança do domínio.

Diversos modelos de segurança para *workflows* têm sido igualmente propostos ao longo dos anos e, como iremos ver, muitos deles são baseados em RBAC. No entanto isto não é o caso do modelo de autorização apresentado em (Hung & Karlapalem, 2003). Este modelo é suportado por um conjunto de funções de autorização que são executadas em diferentes camadas (*workflow*, controlo e dados) da máquina de estados multicamada que controla o modelo, disponibilizando ou negando o acesso aos diferentes recursos.

Em (Chou & Wu, 2004), Chou e Wu apresentaram um modelo de controlo de acesso baseado em RBAC – WfRBAC (*Role-based access control within workflows*) – que resolve algumas das limitações do modelo RBAC durante o tempo de execução do *workflow* (Chou & Wu, 2004): troca dinâmica de função, gestão de associação de função; e, prevenção indireta de fuga de informação. No modelo WfRBAC, para controlar o acesso à informação do *workflow* durante a sua execução, uma política de controlo de acesso é embutida no *workflow*. Isto aborda as limitações identificadas do modelo RBAC.

Dois modelos baseados em RBAC são apresentados em (Wainer, Barthelmess & Kumar, 2003), sendo ambos conhecidos por W-RBAC. O primeiro modelo, Wo-RBAC junta um serviço de permissões baseado em RBAC e uma componente *workflow*. O serviço de permissões providencia uma linguagem baseada em lógica que permite a definição de utilizadores que podem ser autorizados para realizar tarefas. O segundo modelo – W1-RBAC – adiciona a capacidade de tratamento de exceções ao primeiro modelo.

Em (Atluri & Huang, 1996), o WAM (*Workflow Authorization Model*) é apresentado. Este modelo suporta a especificação de políticas de autorização de acesso que permitem o acesso durante a execução de uma tarefa. A sincronização necessária do fluxo de autorização com o *workflow* é atingida através da utilização de um modelo de autorização que é associado a cada tarefa que integra o *workflow*.

Um modelo TBAC (*Task-Based Access Control*) foi apresentado em (Thomas & Sandhu, 1997). Este modelo associa autorização com tarefas. Todas as funções que são aceites para uma tarefa são reunidas num conjunto de confiança. De cada vez que um passo de autorização é executado uma função é escolhida deste conjunto de confiança.

3. A Arquitetura de Interoperabilidade Baseada em Agentes

Nesta secção apresentamos sucintamente a arquitetura baseada em agentes, de forma a contextualizar a nossa contribuição.

3.1. Visão Global

O conceito base da arquitetura é bastante simples: ela é composta por agentes que trabalham em conjunto para prestar serviços. Estes serviços estão registados num repositório de serviços e são publicados pelos agentes que os oferecem. Aplicam-se os seguintes pressupostos:

- A interoperabilidade é conseguida através da composição de serviços simples, que são fornecidos por autoridades públicas, para produzir serviços complexos, que são consumidos por outras autoridades públicas;
- Todos os serviços são prestados por agentes. Os serviços podem ser simples ou complexos. Serviços simples são prestados por agentes associados a um Sistema de Informação Local (SIL) das agências que efetivamente fornecem os serviços. Serviços complexos são prestados por agentes que compõem estes serviços simples;
- A gestão do *workflow* (i.e., o processo de prestação de um serviço) de um serviço complexo não está centralizada em nenhum agente. Os agentes têm a possibilidade de delegar a gestão de partes do *workflow* a outros agentes, invocando novos serviços. Isto implica que os *workflows* são estabelecidos dinamicamente, pelo que não existe um conhecimento prévio dos agentes que participam no *workflow* do serviço complexo;
- O resultado produzido por um agente no decorrer do *workflow* é mantido no agente até ser explicitamente requisitado por outro agente que necessita de o consumir. Este comportamento é imposto por requisitos de confidencialidade. Uma vez que os agentes que necessitam de consumir resultados podem não ser conhecidos na altura da sua produção, os resultados são mantidos pelos agentes que os produzem até que estes sejam requeridos por agentes autorizados para o fazer. De qualquer forma, os agentes têm conhecimento da localização dos resultados de que precisam, uma vez que a informação sobre a disponibilidade do resultado, mas não o seu valor, é transmitida através de todos os agentes que participam no *workflow*.

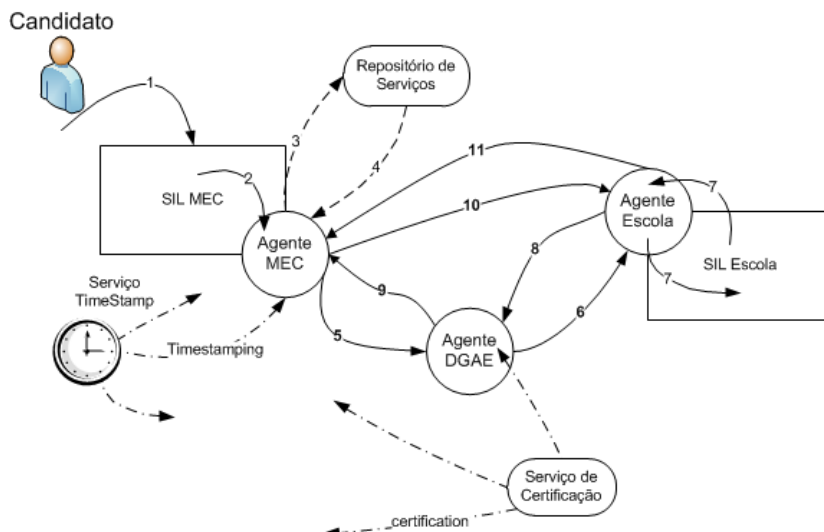


Figura 1 – Representação da arquitetura base e da prestação genérica de serviços

A Figura 1 fornece um exemplo da utilização da arquitetura: candidatura ao ensino superior em Portugal. Ocorrem as seguintes interações:

1. O candidato acede ao Ministério da Educação e Ciência (MEC) para fazer a sua candidatura ao ensino superior e seleciona os cursos e instituições para as quais se quer candidatar;
2. O Sistema de Informação Local do MEC solicita as notas do candidato ao agente que lhe está associado;
3. O agente encontra o serviço da Direção Geral da Administração Escolar (DGAE) que pode fornecer as notas dos alunos;
4. O agente obtém a informação de que necessita para solicitar o serviço;
5. O agente do MEC solicita o serviço ao agente da DGAE;
6. Por sua vez, o agente da DGAE, que não consegue responder diretamente ao serviço mas tem conhecimento do agente que lhe poderá responder, reencaminha o pedido (ou parte dele) para o agente da escola;
7. O agente da escola solicita as notas ao SIL a que está associado;
8. O agente da escola satisfaz o serviço enviando um URI que define a localização das notas do aluno para o agente da DGAE;
9. O agente da DGAE reencaminha a informação para o agente do MEC;
10. Uma vez que o MEC necessita do resultado para concluir o serviço inicialmente solicitado, envia um pedido para o agente da escola a pedir o resultado do serviço;
11. A satisfação deste último pedido conclui o serviço pedido originalmente. De notar que o agente da escola, aquando da produção do resultado, não sabe quem será o destinatário final das notas do aluno. Esse destinatário só fica a ser conhecido quando o agente do MEC solicita explicitamente o resultado produzido.

3.2. Mensagens

Durante a execução do *workflow* de um serviço, várias mensagens são trocadas entre os agentes que estão envolvidos no processo. Os tipos de mensagem são: *Service Request*; *Notification*; *Result Request*; *Result Delivery*.

Uma mensagem do tipo **Service Request** ((5) e (6) na Figura 1) é uma mensagem que suporta toda a informação necessária para solicitar um serviço. Consiste na descrição do serviço a ser pedido, na identificação do pedido, no timestamp correspondente à hora em que o serviço foi pedido, na assinatura do solicitador, da identificação do destinatário e da identificação do solicitador original. Em determinada altura no tempo, este tipo de mensagem pode conter blocos com o mesmo tipo dele próprio (correspondendo à composição do serviço), ou seja incluindo informação sobre todos os serviços mais simples que foram prestados (e dos agentes que os executaram) até àquele momento.

Toda e qualquer alteração no estado de uma prestação de serviço produz uma mensagem do tipo **Notification** ((8) e (9) na Figura 1). Deste modo, Notifications são enviadas dos agentes que executaram um serviço para os agentes que o tinham solicitado. A mensagem contém informação sobre o serviço que foi pedido, sobre o agente que está a prestar o serviço e sobre o novo estado da prestação do serviço (e.g. a conclusão da prestação do serviço com a produção de um resultado).

Uma mensagem do tipo **Result Request** ((10) na Figura 1) é utilizada quando um agente necessita de aceder a um resultado que foi previamente obtido por outro agente. O valor do resultado é identificado por um URI que foi gerado na altura pelo agente que produziu o resultado. O URI do valor do resultado e a Informação sobre o solicitador, nomeadamente os seus certificados, estão incluídos na mensagem.

Mensagens do tipo **Result Delivery** ((11) na Figura 1) são geradas como resposta ao Result Request. Para além do resultado, contém informação sobre o agente que entrega o resultado e os seus certificados.

3.3. Estruturas de Suporte

De forma a obter-se uma prestação de serviços segura e localizar os serviços disponibilizados, a arquitetura contém algumas infraestruturas de suporte, nomeadamente Repositórios de Serviços e uma Infraestrutura de Chave Pública.

Os Repositórios de Serviços respeitam o padrão *Universal Description, Discovery and Integration* (UDDI) (Clement, Hately, Riegen & Rogers, 2004). Estes repositórios armazenam informação sobre todos os serviços disponibilizados, incluindo a identificação do agente que realiza o serviço e os resultados produzidos. Esta informação é armazenada na estrutura (*Service Description*) baseada na linguagem *Web Services Description Language* (Christensen, Curbera, Meredith & Weerawarana, 2001) (WSDL).

A Infraestrutura de Chave Pública é utilizada para suportar a autorização de agentes (que exige a identificação e autenticação dos agentes), a acreditação dos pares do tipo {agente, serviço} e a assinatura digital das mensagens e dos resultados produzidos.

4. O Modelo de Segurança

Nesta secção identificamos as questões de segurança que resultam da arquitetura e apresentamos o modelo de segurança para os enfrentar.

4.1. Questões de Segurança na arquitetura

A arquitetura baseada em agentes tem um conjunto de questões de segurança que deve ser resolvido.

Primeiro, um agente, como um recetor de pedidos, é abordado de uma de duas formas: através de um *Service Request* ou através de um *Result Request* (ver Figura 2). Ambos os tipos de pedidos podem ser realizados por qualquer agente dentro da arquitetura. Uma vez que não existem restrições no que diz respeito ao acesso à arquitetura, estes pedidos podem também estar acessíveis a qualquer peça de *software* que consiga encontrar os *Web Services* do agente. De forma a proteger o SIL associado ao agente

que disponibiliza o serviço, o agente deve verificar a autorização do solicitador do serviço.

Segundo, o caminho do *workflow* pode forçar algumas limitações à prestação do serviço, por exemplo: conflitos de interesse entre duas entidades que estão envolvidas no mesmo processo de prestação do serviço. Os agentes devem estar preparados para atuar (verificar a autorização do *workflow*) de acordo com estes casos e responder de forma apropriada.

Terceiro, existem algumas preocupações que devem ser abordadas pelo solicitador do serviço ou resultado. Para pedir um serviço, é necessário verificar se o agente a quem o mesmo será solicitado está acreditado para o prestar (o que significa que uma terceira entidade de confiança confirma que um agente não só é capaz de prestar um serviço mas também tem a jurisdição/qualificação necessária para o fazer). Neste caso (solicitar um serviço), o agente solicitador deve ser capaz de identificar qualquer restrição ao nível do *workflow* que possa impedir a participação de outro agente no *workflow*.

Finalmente, devem ser tidas igualmente algumas precauções aquando da solicitação de um resultado. Uma vez que um agente não sabe para quem está a produzir um resultado no momento em que o produz, então ele é incapaz de explorar as transformações de cifragem/decifragem de forma a assegurar a confidencialidade e a privacidade do mesmo quando em trânsito por outros agentes. Uma vez que este é o caso por omissão na arquitetura, então o agente mantém o resultado produzido até este ser explicitamente requisitado pelo agente que necessita dele. Esta necessidade para solicitar o resultado adiciona algumas preocupações ao agente que dele necessita: primeiro, o resultado é válido? (que quer dizer: o autor do resultado tem jurisdição sobre aquele resultado? Está este agente acreditado para prestar o serviço que deu origem ao resultado?); segundo, se o agente que requer o resultado tem de produzir um novo resultado com base neste resultado anterior, então tem de identificar o agente que originalmente providencia o resultado (é importante para responsabilização).

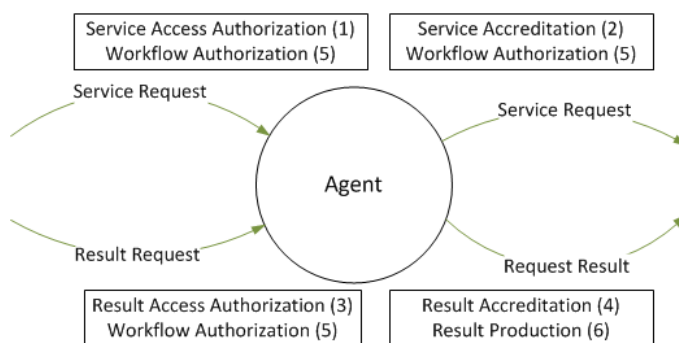


Figura 2 – Tipos de mensagens e preocupações de segurança relacionadas

Resumindo, deve-se assegurar que (ver Figura 2):

1. Um agente que solicita um serviço está autorizado para o fazer.
2. Um agente que disponibiliza um serviço está acreditado para o fazer.

3. Um agente que requer um resultado está autorizado para o obter.
4. Um agente que produz um resultado está acreditado para o oferecer.
5. Um agente que participa no *workflow* está autorizado para participar nesse mesmo *workflow*.
6. Um agente que disponibiliza um resultado é o mesmo agente que o produziu.

4.2. Estruturas de Suporte

A arquitetura deve conter estruturas de dados adequadas para suportar o modelo de segurança. As estruturas de dados seguintes são utilizadas para o efeito: *Certificate* e *Service Description*.

A estrutura **Certificate** baseia-se no RFC 5280. É utilizada com dois propósitos: identificar e autenticar agentes e determinar o nível de autorização para aceder aos serviços disponibilizados. O último é realizado através da utilização das extensões da versão 3 dos certificados X.509.

A estrutura dos certificados (ver Figura 3) contém informação sobre a entidade que certifica, sobre o próprio certificado e sobre todas as classificações de segurança, dado o agente e o tipo de certificado (autorização ou acreditação de serviço). Quando a acreditação do serviço está em causa, o certificado também contém a identificação do serviço.

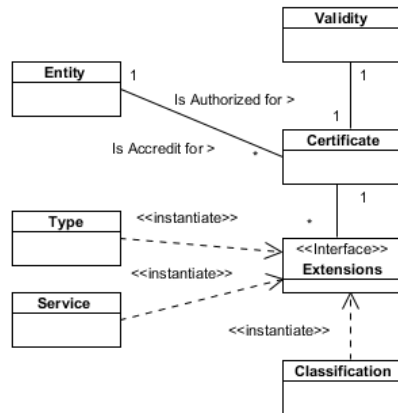


Figura 3 – Estrutura de dados do certificado

A classificação do serviço tem dois significados diferentes, dependendo do tipo de certificado. Nos certificados de autorização, que são utilizados para verificar a classificação de segurança possuída pelos agentes quando atuam como clientes, a classificação deve ser lida como o máximo de autorização que o agente detém. Nos certificados de acreditação de serviços, que são utilizados para acreditar pares {agente, serviço}, define o mínimo de classificação requerido para que um agente possa aceder ao serviço.

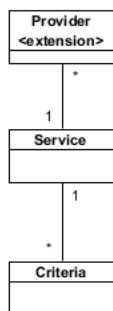


Figura 4 – Estrutura de dados da descrição do serviço

A estrutura **Service Description** baseia-se na especificação WSDL. O seu objetivo principal é disseminar informação sobre os serviços disponíveis na arquitetura. Inclui a descrição do serviço (ver Figura 4), informação sobre quem fornece o serviço (nomeadamente a localização e os seus certificados) e sobre um conjunto de características que são utilizadas pelos agentes para comparar os diferentes fornecedores do mesmo serviço (e.g.: custo; tempo de execução; necessidade de intervenção humana).

Na próxima subsecção expomos de que forma a combinação destas duas estruturas permitem abordar as questões de segurança identificadas.

4.3. A Mecânica do Modelo

Para abordar as questões de segurança identificadas na subsecção 4.1 os agentes utilizam o seguinte processo.

Após a receção de um *Service Request*, o agente que disponibiliza o serviço verifica se o agente que solicitou o serviço tem autorização suficiente para aceder ao serviço. Esta verificação é realizada através da comparação das classificações registadas no certificado de autorização do agente que solicita o serviço, que está disponível na mensagem recebida, com a classificação que é necessária para aceder ao serviço, que está disponível no certificado de acreditação do agente que fornece o serviço. Se o agente que solicita o serviço está autorizado a realizar o pedido, então o agente que fornece o serviço deve ser capaz de verificar se todos os agentes que participaram na prestação do serviço até àquele momento estão autorizados para o fazer de acordo com as políticas do agente que fornece o serviço. Isto é importante uma vez que podem existir políticas de autorização que impeçam que outros agentes participem no *workflow* (e.g.: conflitos de interesse; autorização baseadas no pedido original). Esta verificação também é realizada através da utilização da informação contida na mensagem do pedido do serviço, particularmente nos certificados de autorização e nos seus caminhos de certificação. Com este passo, os itens 1 e 5 estão verificados.

A receção do *Result Request* inicia ações que são similares àquelas que são iniciadas pela receção de um *Service Request*. Neste caso o agente deve verificar a autorização do

agente que solicita o resultado para aceder ao resultado pedido. Isto é feito através da utilização das classificações que estão presentes nos certificados de autorização do solicitador, permitindo que o fornecedor do resultado possa verificar se o agente solicitador está autorizado a aceder ao resultado e se pode participar no *workflow*, abordando os itens 3 e 5.

Para solicitar um serviço um agente deve escolher outro agente que possa fornecer os resultados necessários. Depois de o escolher, determina se este está acreditado para realizar o serviço, baseando-se, para isso, nos certificados e nos respetivos caminhos de certificação associados ao serviço, o que aborda os itens 2 e 5.

O último passo está relacionado com a solicitação de um resultado. Neste ponto, o agente tem um apontador em formato URI que indica a localização do resultado. Para além deste facto, tem também informação sobre o agente que produziu o resultado, nomeadamente os seus certificados. Com esta informação, o agente é capaz de verificar se o agente que fornece o resultado é o mesmo que o produziu, através da verificação da assinatura digital no URI, e de verificar se este está acreditado para produzir aquele resultado. Este passo aborda os itens 4 e 6.

5. Discussão

Como observámos na subsecção 4.1, a possibilidade de um agente delegar partes do *workflow* a outros agentes levanta um conjunto de preocupações de segurança. A nossa abordagem a estas preocupações baseia-se num conjunto de procedimentos, numa PKI e num conjunto de estruturas de dados de suporte.

A arquitetura de interoperabilidade que foi brevemente descrita na secção 3 levanta algumas preocupações de segurança, como mencionado previamente. Devido ao dinamismo da arquitetura, à capacidade que qualquer agente tem de realizar vários papéis simultaneamente e à gestão descentralizada do *workflow*, todos os modelos de segurança existentes se revelam inadequados. Para além disto, o modelo deve ter em consideração o facto de que a verificação da autorização deve ser realizada em diferentes contextos: *Service Request*; *Service Deliver*; e, *Result Request*.

O nosso modelo utiliza uma PKI de forma providenciar autenticação de agentes e acreditação de serviços e autorização.

Em termos de verificação de autorização, o objetivo do nosso modelo de segurança não é lidar com restrições de acesso específicas (que, argumentamos, são deveres do SIL) mas definir restrições de acesso gerais ao SIL. Com isto em mente, a nossa abordagem apenas requer a utilização das extensões de certificados apresentadas anteriormente. Mais, estas extensões e o conjunto de procedimentos que foram definidos permitem abordar todas as preocupações identificadas ao nível da autorização.

Mais, os modelos de segurança previamente referenciados definem uma função específica para cada agente, o que não se verifica na nossa arquitetura. Um agente pode prestar ou solicitar diversos serviços dentro do *workflow*, podendo, portanto, atuar com diferentes funções.

Então, para utilizar o RBAC seria necessário um grande número de funções e o necessário dinamismo para suportar a sua criação, manutenção e remoção em qualquer momento.

Finalmente, ao contrário de todos os outros trabalhos referenciados, a nossa proposta também aumenta a confidencialidade dos dados e a privacidade através da execução de *workflows*, impondo a solicitação obrigatória de resultados (que são mantidos pelos agentes que os produziram até serem explicitamente solicitados pelos seus destinatários finais).

6. Conclusões e trabalho futuro

Neste artigo apresentamos um modelo de segurança baseado em PKI para adicionar segurança a uma arquitetura de interoperabilidade baseada em agentes. Esta arquitetura foi igualmente sucintamente descrita, para apresentar as questões de segurança que levanta e que se devem essencialmente ao seu inerente dinamismo.

O modelo permite que agentes verifiquem as permissões de outros agentes para participar no *workflow* associado à prestação de um serviço, para verificar a autorização de outros agentes, para prestar e solicitar serviços e resultados e para verificar se os agentes que entregam resultados são os mesmos que originalmente os produzem. Mais, assegura a privacidade do conteúdo através da garantia de que os agentes solicitam explicitamente os resultados que lhes são destinados. A definição de políticas que possam lidar com restrições de acesso específicas ao SIL está fora do âmbito deste modelo.

No futuro é nossa intenção validar o modelo proposto através da exploração de um protótipo entretanto desenvolvido recorrendo a casos de utilização, os quais irão envolver o desenvolvimento de diversos tipos de agentes.

Referências

- Atluri, V., & Huang, W.-kuang. (1996). An authorization model for workflows. *Computer Security—ESORICS 96* (pp. 44–64). Springer.
- Chou, S. C., & Wu, C. J. (2004). An Access Control Model for Workflows Offering Dynamic Features and Interoperability Ability. *Int. Computer Symposium*, Dec (pp. 15–17).
- Christensen, E., Curbera, F., Meredith, G., & Weerawarana, S. (2001). *Web Services Description Language (WSDL) 1.1*.
- Clement, L., Hately, A., Riegen, C. von, & Rogers, T. (Eds.). (2004). *UDDI Version 3.0.2 Specification*. Retrieved from uddi.org/pubs/uddi_v3.htm
- Hung, P. C. K., & Karlapalem, K. (2003). A secure workflow model. *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21* (Vol. 21, pp. 33–41). Australian Computer Society, Inc.

- Kannammal, A., & Iyengar, N. C. S. N. (2008). A Framework for Mobile Agent Security in Distributed Agent Based E-Business Systems. *International Journal of Business and Information*, 3(1), 129-143.
- Marques, F., Dias, G. P., & Zúquete, A. (2011). A General Interoperability Architecture for e-Government based on Agents and Web Services. 6a Conferência Ibérica de Sistemas e Tecnologias de Informação (pp. 338-343).
- OECD. (2001). E-Government: Analysis Framework and Methodology. Group, (November), 1-10.
- Savarimuthu, B. T. R., Purvis, M., & De Oliveira, M. (2004). Towards Secure Interactions In Agent Societies. *Citeseer*, 143-148.
- Stormer, H., Knorr, K., & Eloff, J. (2000). A model for security in agent-based workflows. *Informatik Informatique*, 6, 24–29.
- Thomas, R., Sandhu, R. (1997). Task-Based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. *Proceedings of the IFIP WG11.3 Workshop on Database Security*, Lake Tahoe, California.
- Wainer, J., Barthelmeß, P., & Kumar, A. (2003). W-RBAC-a workflow security model incorporating controlled overriding of constraints. *International Journal of Cooperative Information Systems*, 12(4), 455–485. *Citeseer*.

Sistema de Información del Banco de Tierras de Galicia

Juan Porta ¹, Jorge Parapar ¹, Paula García ¹, Gracia Fernández ¹, Juan Touriño ¹,
Francisco Ónega ², Pablo Díaz ², David Miranda ², Rafael Crecente ²

juan.porta@udc.es, jparaparl@udc.es, pgarciab@udc.es, gfernandez@udc.es, juan@udc.es,
franciscojose.onega@usc.es, pablo.diaz.redondo@usc.es, david.miranda@usc.es,
rafael.crecente@usc.es

¹ Grupo de Arquitectura de Computadores, Universidad de A Coruña. España.

² Laboratorio del Territorio, Universidad de Santiago de Compostela. España.

DOI: 10.4304/risti.9.27-41

Resumen: Este artículo describe el desarrollo del sistema de información del Banco de Tierras de Galicia, organismo gallego que actúa de intermediario entre propietarios y agricultores para fomentar el arrendamiento de tierras y evitar su abandono. Sus objetivos son realizar la gestión interna del Banco, difundirlo entre el público y facilitar distintos tipos de tramitaciones a través de Internet. El sistema, disponible en <http://www.bantegal.com/sitegal>, está formado por una aplicación web con componentes SIG que ofrecen una mayor y mejor información sobre las parcelas y su entorno. El desarrollo se apoya en el uso de software libre y en la utilización de estándares para el manejo de la información geográfica. El artículo detalla la arquitectura, componentes y funcionalidades del sistema y ofrece datos estadísticos de su utilización.

Palabras clave: Banco de Tierras; SIG-Web; software libre; e-government

Abstract: This paper describes the information system of the Galician Land Bank. The Galician Land Bank is a public institution that aims to mitigate the land abandonment by promoting the rental of agricultural plots, acting as a mediator between owners and farmers. Within the objectives of the system are to do the internal management of the Bank, to disseminate it among the public and to enable the carrying out of procedures via Internet. The system, available at <http://www.bantegal.com/sitegal>, is formed by a web application with a GIS framework that offers better information about the plots and their environment. It has been developed using open source software and standards for the management of the geographic information. The paper describes the architecture of the system, its components and its functionalities and also gives some data about its usage.

Keywords: Land Bank, Web-GIS; open source software; e-government

1. Introducción

Desde hace años, muchos lugares de Europa están sufriendo procesos de abandono del ámbito rural debido principalmente a la disminución y cambios en la actividad agrícola (Keenleyside & Tucker, 2010). Este es el caso de Galicia, una comunidad autónoma situada al noroeste de España caracterizada por una estructura de la propiedad con parcelas muy pequeñas y por una tradición de minifundismo. Para frenar este abandono, las explotaciones agrícolas han de adaptarse a la agricultura moderna y tener tamaño suficiente para ser sostenibles. Es pues importante facilitar a los agricultores el acceso a la tierra, pero en algunos casos es complicado debido a que muchos propietarios han emigrado y son difíciles de localizar, y otros muchos tienen apego a sus propiedades, no desean venderlas y desconfían a la hora de arrendarlas. Además, muchas de las parcelas no tienen las condiciones necesarias para que su cultivo sea rentable.

Con el objetivo de mejorar esta situación, el gobierno gallego (Xunta de Galicia), puso en marcha el Banco de Tierras, un instrumento legal para intentar solucionar los problemas mencionados. Para gestionarlo y facilitar los trámites a través de Internet, la Consellería do Medio Rural firmó un convenio con el Laboratorio del Territorio, de la Universidad de Santiago de Compostela, y el Grupo de Arquitectura de Computadores, de la Universidad de A Coruña para la creación de un sistema de información basado en un prototipo desarrollado por ambos grupos en un proyecto previo que pretendía unos objetivos similares (Crecente, Doallo, Miranda, Ónega, Parapar, & Touriño, 2005). El sistema creado para el Banco de Tierras comparte muchas de las bases de dicho prototipo como son permitir la interacción de los usuarios del Banco, el uso de software libre para abaratar costes y facilitar su implantación y la inclusión de funcionalidades de los SIG para ofrecer una gestión más completa e integrada de las parcelas.

Considerando al Banco de Tierras como principal instrumento de movilidad, estudios recientes (Corbelle-Rico, Crecente-Maseda, & Santé-Riveira, 2012) indican que desde 1972 hasta 2001 se ha registrado un abandono en Galicia de 70.000 ha; que considerando una superficie media de 0.25 ha/parcela, resultarían unas 280.000 parcelas susceptibles de ser arrendadas.

En este artículo describimos el sistema desarrollado, el cual se encuentra en plena explotación por parte de la administración, y es de acceso público para propietarios, arrendatarios e interesados en general, a través de la dirección <http://www.bantegal.com/sitegal>. El artículo está estructurado de la siguiente manera: la sección 2 resume el funcionamiento del Banco de Tierras y hace referencia a algunas experiencias similares. La sección 3 proporciona una visión general de las funcionalidades desarrolladas, mientras que la sección 4 se dedica a describir la estructura interna del sistema. En la sección 5 se comentan los resultados obtenidos y se dan datos de uso del Banco de Tierras y del sistema. Finalmente, en la sección 6, se explica en que se está trabajando actualmente y se indican algunas ideas para la evolución del sistema.

2. Funcionamiento del Banco de Tierras de Galicia

El Banco de Tierras de Galicia, en funcionamiento desde noviembre de 2007, es un organismo público dependiente de la Consellería do Medio Rural e do Mar de la Xunta de Galicia. Para su funcionamiento dispone de una oficina central y cuenta con la colaboración de oficinas agrarias comarcales públicas repartidas por todo el territorio gallego, a las que pueden acudir los interesados a realizar los trámites pertinentes. El cometido del Banco es hacer de intermediario en el arrendamiento de parcelas entre propietarios y agricultores. El proceso se divide en dos fases: una fase de incorporación de la parcela al Banco y una fase de arrendamiento.

2.1. Proceso de incorporación de parcelas al Banco de Tierras

En principio, cualquier parcela agrícola es susceptible de ser incorporada al Banco. Las parcelas de particulares siguen perteneciendo a sus propietarios pero al incorporarlas, autorizan al Banco a arrendarlas a terceros para usos agrícolas. Mientras no son arrendadas, pueden seguir siendo utilizadas por sus propietarios. El periodo de permanencia en el Banco es indefinido, permanecerán hasta que el propietario solicite su retirada, lo que podrá hacer en cualquier momento salvo que la parcela esté ya arrendada, en cuyo caso deberá esperar a que finalice el contrato de arrendamiento.

Para incorporar una parcela al Banco, el propietario debe realizar una solicitud de incorporación y esta debe ser aceptada, en base a las características de la parcela. El precio de arrendamiento es fijado por el Banco, que establece anualmente unos precios de referencia por unidad de superficie dependiendo del tipo de terreno y de la parroquia en la que esté la parcela. El Banco no se compromete a arrendar las parcelas, dependerá de que existan agricultores interesados. Mientras las parcelas no se arrienden sus propietarios no reciben ningún pago. Si se arriendan, los propietarios recibirán el importe del arrendamiento salvo una comisión del 1% por gastos de gestión.

Además de las parcelas de particulares, el Banco posee parcelas de titularidad pública, mayoritariamente procedentes de terrenos sobrantes de procesos de concentraciones parcelarias (masas comunes).

2.2. Proceso de arrendamiento de parcelas del Banco de Tierras

Cualquier usuario puede consultar la lista de parcelas disponibles en el Banco y pedir su arrendamiento presentando para ello una solicitud oficial. Si sobre una parcela concurre más de una solicitud, la ley establece varios criterios para elegir cual será aceptada. El arrendatario firmará el contrato de arrendamiento con el Banco por una duración de cinco años, aunque si el propietario estuviese de acuerdo el arrendamiento podría durar más. El Banco garantiza al propietario el cobro del arrendamiento de la parcela mientras esta esté arrendada y que cuando finalice, la parcela será devuelta en las mismas condiciones que estaba antes de arrendarse. Una vez finalizado un arrendamiento, la parcela vuelve a estar disponible en el Banco o puede ser retirada por el propietario, si este lo desea.

2.3. Experiencias similares

Actualmente existen diversos lugares donde ya funcionan bancos de tierras, sin embargo, no se han encontrado aplicaciones SIG-Web públicas que permitan la interacción de usuarios con el Banco. Uno de estos casos es el del Banco de Tierras de Asturias, que dispone de una aplicación SIG (Carcedo, Fernández, & González, 1998) pero sólo para su gestión interna. Otro caso es el de la Diputación Foral de Vizcaya (País Vasco), que ha iniciado los pasos para crear un Fondo de Suelo Agrario. A nivel europeo, el banco de tierras más conocido es la sociedad SAFER, en Francia, que fue creada a principios de los años 60. Su gestión se basa en la compra-venta de propiedades, teniendo un derecho de tanteo sobre las tierras vendidas. Dispone de sitio web, <http://www.proprietes-rurales.com>, donde ofertan las propiedades disponibles, pero sin capacidades SIG.

Aparte de los bancos de tierras, existen sitios web desarrollados por iniciativas privadas como <http://www.turofincas.com>, <http://www.buscafincas.com> o <http://www.fincasysolares.com>, que se dedican al negocio de venta y alquiler de parcelas, construcciones y demás propiedades. Fuera de España, existen algunos especializados en las propiedades rurales como <http://www.fazonline.com.br>, o <http://www.landandranchsales.com>.

En general, en estos sitios web no se hace uso de entornos SIG para la localización y la consulta de información de las propiedades. Uno de los posibles motivos es el alto coste de obtención de las capas de información y otro es la complejidad de integración de los sistemas SIG en procesos como la compra-venta o el alquiler de tierras. No obstante, esto está cambiando gracias sobre todo a la popularización de servicios de mapas como Google Maps y cada vez son más los sitios que se apoyan en herramientas de terceros para mostrar los lugares en donde tienen sus ofertas. Ejemplos de esto son <http://www.housingmaps.com> y <http://www.farmseller.com>.

3. Visión general y funcionalidades

El sistema de información ha sido desarrollado para solucionar los problemas y alcanzar los objetivos descritos en las secciones anteriores y se ha convertido en pieza clave para el funcionamiento del Banco de Tierras. Desde su versión inicial, se le han ido añadiendo mejoras y nuevas funcionalidades. Otro de los objetivos que se pretendió desde el inicio fue el uso de software libre. Esto ha permitido un ahorro importante en costes de licencias, tanto para desarrollo como para producción, y también ha facilitado el trabajo al no tener que estar pendientes de las restricciones de instalación que imponen algunas licencias privativas.

El sistema está accesible para cualquier persona, distinguiéndose los siguientes tipos de usuarios:

Usuarios no registrados

Los usuarios no registrados pueden consultar las parcelas disponibles en el Banco de Tierras, tanto en forma de lista, como sobre un visor web de mapas interactivo (ver Figura 1) donde pueden visualizar la posición y forma exacta de cada parcela sobre una

ortofotografía de alta resolución. Las características técnicas del visor se detallan en la sección 4.2.

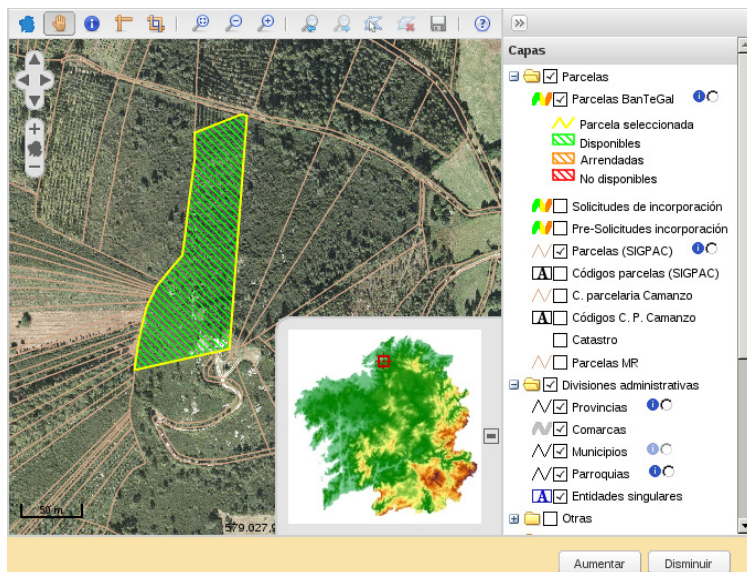


Figura 1 – Visor de mapas con una parcela seleccionada.

Mediante un buscador el usuario también puede buscar las parcelas que le interesen según criterios de superficie, situación, precio, etc. Cuando un usuario no encuentra parcelas que se ajusten a sus necesidades puede introducir en la aplicación las características de las parcelas que necesita y se le suministra un enlace personalizado para que en cualquier momento pueda consultar las que se adapten a sus necesidades. Además, el Banco le enviará un aviso por correo electrónico o SMS cuando se incorpore alguna parcela de su interés.

Usuarios registrados

Si un usuario desea solicitar el arrendamiento de una parcela del Banco o su incorporación al fondo de tierras, ha de registrarse en el sistema. Para solicitar una incorporación, el usuario puede identificar su parcela de dos modos: o bien moviéndose por el mapa hasta localizarla, o bien introduciendo el código catastral de la parcela y el sistema la buscará automáticamente. Si los límites de la parcela que figuran en el mapa no son correctos, el usuario puede dibujar él mismo la parcela sobre el visor. Para completar la incorporación también ha de introducir los datos de los propietarios. El precio de arrendamiento de la parcela es calculado automáticamente por el sistema en función de la zona en la que se encuentre y los usos a los que esté dedicada. A continuación, el sistema generará automáticamente el documento de solicitud (en formato PDF, DOC u ODT), el cual deberá ser impreso y firmado por los propietarios. Una vez firmado se entregará en alguna oficina junto con la documentación necesaria. Hecho esto, los gestores del Banco la estudiarán y decidirán sobre su aprobación o denegación.

Si un agricultor encuentra una parcela que le interesa, también puede introducir la solicitud a través de la aplicación, indicando qué condiciones cumple en relación a los distintos criterios que la ley contempla para la selección del arrendatario en caso de que existan varias solicitudes de arrendamiento sobre la misma parcela. El documento de solicitud que se genera también ha de ser firmado y entregado. Los usuarios pueden consultar el estado de sus solicitudes a través de la aplicación.

Gestores del Banco de Tierras

Los gestores del Banco de Tierras se encargan de estudiar las solicitudes y de aceptarlas o rechazarlas. Existen varios tipos de gestores (comarcales, centrales, administradores) con distintos permisos. Algunas de las funcionalidades a las que tienen acceso son las siguientes: introducción de datos de eventos relacionados con parcelas (visitas realizadas para comprobar su estado, peticiones recibidas para cambios de uso...); generación de estadísticas sobre las parcelas y solicitudes; importación de archivos shape para actualizar geometrías de parcelas; introducción de archivos adjuntos vinculados a solicitudes, parcelas y arrendamientos (contratos escaneados en formato PDF, fotografías, etc.); conexión con servicios web de la oficina del Catastro para la obtención de las geometrías actualizadas de las parcelas y las referencias catastrales.

El sistema también implementa la automatización de diversas tareas como: cálculo de los puntos asignados a las solicitudes de arrendamiento sobre una parcela en base a las características preferentes que reúnen los solicitantes; cálculos de los usos de una parcela mediante operaciones espaciales (intersección de la geometría de la parcela con la capa de usos); cálculo del precio de cada parcela en función de sus usos y situación; actualización de los importes de los arrendamientos de acuerdo con la variación del índice de precios al consumo (IPC) de España.

4. Implementación del sistema

Los detalles del sistema desarrollado, junto con sus componentes, fuentes de datos, e información sobre su despliegue son descritos a continuación.

4.1. Arquitectura global

En la Figura 2 se muestra un esquema de la arquitectura del sistema. El núcleo es una aplicación web Java que implementa la lógica de las funcionalidades relacionadas con las incorporaciones y arrendamientos de parcelas. Se encarga también de realizar el almacenamiento de la información en base de datos y de generar la interfaz de usuario mediante páginas web dinámicas, las cuales consultan los usuarios a través de sus navegadores. Esta aplicación accede a la información geográfica a través de un servidor de mapas, que es el otro pilar del sistema. El servidor de mapas es un proceso independiente que se encarga de generar los mapas que solicita el usuario y en general actúa de intermediario con la información geográfica, también para peticiones de atributos de los objetos. Así se independiza la aplicación de los orígenes de datos geográficos.

La aplicación Java se encarga de insertar el visor de mapas en aquellas páginas web en las que se usa, particularizándolo según los distintos casos de uso (introducción de

parcela, consulta de parcela, modificación de geometrías, etc.). Mediante JavaScript, el visor captura las acciones del usuario y las traduce en las correspondientes peticiones al servidor de mapas, con el que se comunica directamente usando técnicas AJAX (Asynchronous JavaScript and XML). Una vez que el servidor responde a una petición, el visor se encarga de actualizar aquellas partes de la página que sea necesario, de manera que al no recargar toda la página, se reduce el tiempo de carga y la interfaz de usuario se hace más amigable. Los mapas se generan en formato raster (JPEG o PNG) para que el tamaño de los archivos a descargar sea el menor posible.

Cuando el usuario selecciona una parcela para solicitar su incorporación al Banco, el visor comunica a la aplicación Java de qué parcela se trata, y la aplicación pide al servidor geográfico los atributos de dicho objeto (superficie, usos, situación...) y se los muestra al usuario en un formulario, pudiendo éste confirmarlos o corregirlos.

Consecuentemente con lo anterior, la información manejada por el sistema también está separada en dos grupos: la información relativa a las parcelas y usuarios del Banco de Tierras, y la información geográfica de referencia, creándose sendas bases de datos (a las que llamaremos base de datos del Banco y base de datos geográfica, respectivamente), ambas con soporte para información espacial. La aplicación Java gestiona la base de datos del Banco mientras que la base de datos geográfica es accedida por el servidor geográfico.

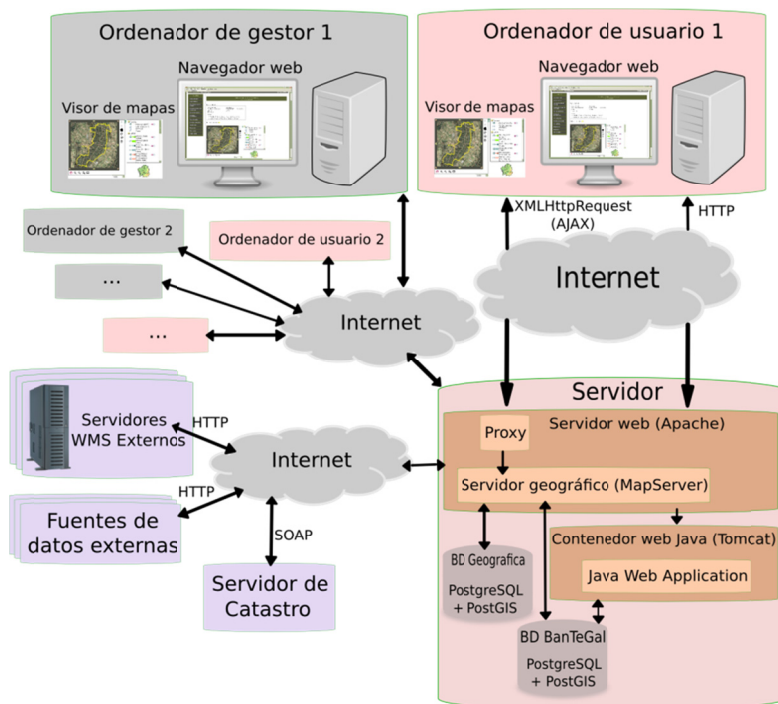


Figura 2 – Arquitectura del sistema.

Además de la base de datos geográfica, parte de la información geográfica procede de servicios externos a través de los protocolos WMS (Web Map Service) y WFS (Web Feature Service), ambos servicios definidos por el OGC (Open GeoSpatial Consortium), asociación internacional dedicada a la definición de estándares abiertos para la interoperabilidad de sistemas SIG. El WMS se usa para la obtención de mapas con distintas capas de información (normalmente en formato raster) y el WFS sirve para la obtención de datos en formato vectorial junto con los atributos alfanuméricos de los objetos (normalmente en formato GML). Este tipo de servicios encajan dentro de las Infraestructuras de Datos Espaciales (IDE).

4.2. Componentes del sistema

A continuación se describe con más detalle cada uno de los componentes del sistema y de las herramientas y librerías utilizadas.

Aplicación web Java

La aplicación web Java ha sido implementada utilizando herramientas software libre (Tabla 1) y haciendo uso de diversos patrones de diseño (Johnson, Singh, & Stearns, 2002) mostrados en la Figura 3. Como patrón arquitectónico se ha utilizado estructura en tres capas siguiendo el patrón Modelo-Vista-Controlador (MVC)

Tabla 1 – Herramientas utilizadas en la implementación de la aplicación web.

Nombre			Capa	Descripción
Hibernate			Modelo	Herramienta de transformación objeto-relacional utilizada para la lectura y escritura en base de datos.
Spring			Modelo	Entorno con numerosas funcionalidades para el desarrollo de aplicaciones web Java.
Apache Struts			Vista/Controlador	Framework para el desarrollo de aplicaciones web MVC.
JavaServer (JSP)	Pages	Vista		Tecnología Java para el desarrollo de páginas web con contenido dinámico.
AjaxTags			Vista	Librería JSP para implementar funcionalidades AJAX.
DisplayTag			Vista	Librería JSP que ayuda a la creación de tablas HTML con paginación.
JCaptcha			Vista	Implementación de los conocidos CAPTCHA.
JODReports			Controlador	Generador de informes basados en plantillas OpenOffice.
Quartz Scheduler			Modelo	Conjunto de librerías Java que permiten la ejecución de tareas de manera asíncrona, automática y programada.

ClamAV	Modelo	Antivirus que puede ser utilizado en aplicaciones web a través de su API.
Java Topology Suite	Modelo	Librería que implementa multitud de operaciones espaciales bidimensionales (insercciones, uniones...).
GeoTools	Modelo	Librería que ofrece diversos mecanismos para el manejo de datos espaciales. Es utilizada para la lectura de archivos de datos con formato SHP.

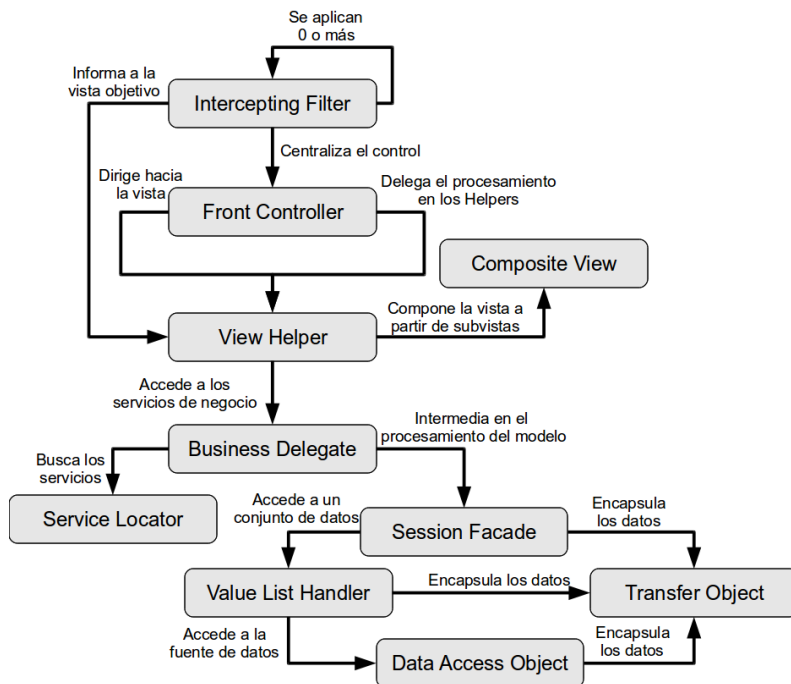


Figura 3 – Patrones de diseño utilizados.

Visor de mapas

El visor de mapas (ver Figura 1) está basado en OpenLayers. OpenLayers es el visor libre más popular en la actualidad. Se trata de una aplicación JavaScript que hace uso intensivo de AJAX y entre sus principales características están el que permite el acceso a muchos tipos de servicios de datos, tanto estándar (WMS, WFS, WMTS, KML, GML...) como no estándar (Google Maps, Yahoo Maps, OpenStreetMap...). Por contra, su interfaz de usuario es algo pobre, aunque gracias a las posibilidades de ampliación y personalización que ofrece existen complementos centrados en su mejora. En nuestro caso usamos GeoExt, basado en la librería Ext. Entre las funcionalidades del visor

están: desplazamiento por el mapa y zooms; medición de longitudes y áreas; consulta de información sobre los objetos visibles; selección y centrado de objetos; link para recuperar la situación actual del mapa en cualquier momento; digitalización y modificación de geometrías; etc.

Servidor de mapas

Como servidor de mapas se usa MapServer. Se trata de una de las aplicaciones SIG libres más veteranas y populares. Está programado en lenguaje C y funciona como un CGI acoplado al servidor web, aunque también ofrece APIs para numerosos lenguajes. Tiene un buen rendimiento y destaca por soportar numerosas fuentes de datos y estándares. En particular, permite el acceso en cascada a otros servidores WMS y WFS.

Almacenamiento

Como servidor de datos se usa PostgreSQL con su extensión espacial PostGIS. Su elección se debe a que PostGIS es el software libre que mejor soporta el estándar del OGC para bases de datos espaciales. De hecho está certificado por dicho organismo como acorde al perfil Types and Functions de la especificación Simple Features Specification for SQL. Posee una buena capacidad de indexación espacial y está soportado por la mayoría de servidores de mapas.

Integración de componentes

La conexión de la aplicación Java con la base de datos se hace mediante Hibernate e Hibernate Spatial los cuales soportan PostgreSQL y PostGIS. Una posible migración a cualquiera de los servidores de base de datos soportados por estas herramientas sería factible. De la conexión de MapServer con la base de datos se ocupa el propio MapServer, siendo también posible migrar a otra base de datos (MapServer soporta varios servidores de bases de datos espaciales) e incluso a otro servidor de mapas (PostgreSQL+PostGIS es soportado por la mayoría de servidores de mapas).

La comunicación entre el visor y la aplicación Java con el servidor de mapas es la parte que ha requerido mayor trabajo. Si bien la visualización de capas en el visor es una tarea sencilla, existen casos de uso que requieren una comunicación en varios pasos entre ambas partes. Por ejemplo, para introducir una solicitud de incorporación de una parcela los pasos son los siguientes: el usuario sitúa el mapa en la zona donde se encuentra la parcela (peticiones WMS GetMap para dibujar el mapa); selecciona una parcela y esta se resalta dibujando los bordes en otro color (petición WMS GetFeatureInfo para identificar qué parcela es y petición WMS GetMap para obtener el mapa con la parcela resaltada); y confirma que la parcela resaltada es la que quiere incorporar y esta se guarda en la base de datos (petición WFS GetFeature para obtener la geometría en formato vectorial y los atributos alfanuméricos de la parcela).

El diseño utilizado permite que todos los componentes del sistema sean independientes entre sí. Así, la sustitución de cualquiera de ellos sería transparente para el resto del sistema.

4.3. Fuentes de datos geográficos

Una de las cosas más importantes para que el sistema cumpla con los objetivos propuestos y tenga una buena acogida es que los datos geográficos utilizados posean suficiente calidad. En particular, hay tres capas de información que son básicas para el funcionamiento del sistema: ortofotografías del terreno, usos del suelo y la división parcelaria. En España, afortunadamente, se dispone de buenas fuentes de información para las tres.

Con respecto a las ortofotos, en el marco del Plan Nacional de Ortofografía Aérea, cada 2 años se vuela sobre toda España y se generan ortofotos con una resolución que alterna entre de 25 y 50 cm/píxel. Con respecto a las parcelas y a los usos del suelo, el SIGPAC (Sistema de Información de Parcelas Agrícolas), sistema encargado de la gestión de las ayudas agrícolas de la Unión Europea, dispone de ambas capas de información en formato vectorial para todo el país y las actualiza periódicamente. Para usar las capas de parcelario y los usos del suelo se han copiado los datos en la base de datos local debido a que no existen servidores WFS disponibles que permitan acceder a sus atributos. De las ortofotos no se tiene copia local, pues se usan únicamente como fondo del mapa y sí existen varios servidores WMS de acceso público que las suministran.

Otros datos usados son las divisiones administrativas, que proceden del Sistema de Información Territorial de Galicia (SITGA), y las zonas naturales protegidas que se obtiene del servidor WMS del Ministerio de Medio Ambiente.

Dada la estructura modular del sistema y gracias al uso de estándares, la incorporación al visor de mapas de nuevas capas de información disponibles vía WMS resulta muy sencilla.

4.4. Despliegue del sistema

El sistema es multiplataforma (Linux, Windows, Mac OS X) ya que todos sus componentes lo son (PostgreSQL, Java, MapServer). Actualmente se encuentra instalado en dos máquinas virtuales con sistema operativo SUSE Linux Enterprise Server 10 SP1, 4GB de RAM, y un procesador Intel Xeon X5450 a 3.00GHz con dos núcleos. En una de las máquinas está el servidor web (Apache), el servidor de mapas y la base de datos geográfica. En la otra se encuentra la aplicación web en un servidor Tomcat y la base de datos del Banco. Los usuarios acceden al servidor Apache de la primera máquina la cual redirige las peticiones correspondientes al servidor Tomcat de la segunda máquina, la cual sólo es accesible desde la red interna.

La tabla 2 resume las principales tecnologías utilizadas en el sistema.

Tabla 2 – Resumen de tecnologías utilizadas.

Elemento	Recurso	Breve descripción
Servidor web	Apache HTTP Server	Servidor HTTP.
Contenedor web	Apache Tomcat	Contenedor de aplicaciones web Java.
Servidor de mapas	MapServer	Servidor geográfico con soporte para servicios OGC.
Base de datos	PostgreSQL	Sistema gestor de bases de datos relacionales.
Extensión geográfica	PostGIS	Extensión con capacidades espaciales para PostgreSQL .
Estándares OGC	WMS	Web Map Service: servicio de imágenes georreferenciadas.
	WFS	Web Feature Service: servicio de datos geográficos.
	GML	Geography Markup Language: gramática XML para expresar datos y objetos geográficos.
	SLD	Styled Layer Descriptor: describe la apariencia de las capas de información.
Formato de datos geográficos	Shapefile	Formato de datos vectoriales.
	WKT	Well-Known Text: formato para representar la geometría de objetos en formato vectorial.
Fuentes de datos externos	SOAP DGC	Servicio web de la Dirección General de Catastro.
	WFS DGC	Servidor WFS de la Dirección General de Catastro.
	SIXPAC WMS	Servidor WMS del Sistema de Información de Parcelas Agrícolas de Galicia.
	SITGA WMS	Servidor WMS del Sistema de Información Territorial de Galicia.
	PNOA WMS	Servidor WMS del Plan Nacional de Ortografías Aéreas.

5. Resultados y discusión

El Banco de Tierras está operativo desde finales del año 2007. A fecha de diciembre de 2011, el número de parcelas disponibles en el Banco era de 7.160, las cuales suman un total de 3.049,36 hectáreas. De ellas, se encuentran arrendadas 1.404 parcelas sumando 1.359,80 hectáreas, es decir, un 44,59% de la superficie de parcelas del Banco está arrendada. Con respecto a los clientes del Banco, el 33,93% de las solicitudes de

arrendamiento y el 27,09% de las solicitudes de incorporación las inician a través del sistema vía Internet. Aunque sería deseable un porcentaje mayor, es un dato muy aceptable debido al perfil de los usuarios: gente de ámbito rural, de edad mediana o avanzada, con formación y experiencia informática reducida y con acceso a Internet de mala calidad, lo que ha sido identificado como una de las grandes dificultades en estas iniciativas rurales (Bayfield, y otros, 2005).

Las consultas espaciales suelen ser las operaciones más costosas en este tipo de sistemas. La tabla 3 muestra tiempos de ejecución medios de las peticiones más frecuentes sobre el servidor de mapas. Se ha probado con distinto número de peticiones por segundo y para cada caso se ha repetido la prueba varias veces (tandas) y se ha hecho la media. Las peticiones probadas han sido para zonas de 1000x1000 metros: consulta WMS GetMap sobre la capa de usos del suelo para un tamaño de mapa de 1024x1024 píxeles; consulta WMS GetFeatureInfo sobre la capa de parcelas para un tamaño de mapa de 1024x1024 píxeles; y consulta WFS GetFeature sobre la capa de usos del suelo utilizando un filtro de tipo bounding box (BBOX).

Tabla 3 – Tiempos medios de ejecución de consultas (en segundos).

Petición	Una petición	5 por seg.	10 por seg.	20 por seg.	50 por seg.
GetMap	1,10	2,21	3,76	6,38	13,81
GetFeatureInfo	0,64	1,46	2,53	4,31	10,14
GetFeature	1,18	2,12	3,31	5,85	11,81

Las parcelas y usos del suelo están almacenados en local y suman aproximadamente 12.000.000 y 16.000.000 registros respectivamente. Como se puede ver, para un número de usuarios moderado, los tiempos de ejecución son bastante buenos, dado el gran volumen de datos que involucran. En caso de necesitar más rendimiento, el sistema está diseñado para poder replicarse y utilizar balanceadores de carga sin necesidad de tocar el código fuente, sólo los archivos de configuración.

5.1. Experiencia con los usuarios

La comunicación permanente y directa entre los desarrolladores del sistema y los usuarios del Banco ha hecho que la aplicación esté en un ciclo de mejora continua y de ampliación de sus funcionalidades. Además, se han adaptado tecnologías y procedimientos para facilitar la usabilidad del sistema. Por ejemplo, en su momento se detectó que existían demandantes de parcelas que no encontraban en el Banco parcelas que se ajustasen a sus necesidades. Esto llevó a desarrollar una funcionalidad que permite al usuario introducir las características de las parcelas deseadas, y cuando se incorpore alguna parcela al Banco que cumpla con dichas características se avisa al demandante a través de SMS o correo electrónico.

Parte de los usuarios potenciales del sistema son gente escasos conocimientos en nuevas tecnologías e incluso un acceso limitado a Internet. Es por esto que los procesos de introducción y arrendamiento se han dividido en pasos guiados y detallados para

que resulte fácil e intuitivo realizarlos. Tampoco es necesaria la instalación de ningún plugin en el navegador del usuario (como puede suceder con otros visores geográficos) y se ha tratado de optimizar el sistema para que consuma poco ancho de banda.

La comunicación a través del sistema de información entre los gestores del Banco, sobre todo entre distintos roles (por ejemplo entre gestores centrales y gestores de las oficinas comarcales) es una necesidad que surgió cuando el Banco ya estaba en pleno funcionamiento. Por eso se ha creado un foro interno para gestores y un sistema de alertas y noticias. Con vistas a dinamizar el uso de la web, y en general del Banco, se está planteando la extensión de estas funcionalidades a todos los clientes y visitantes anónimos.

6. Conclusiones y trabajo futuro

El concepto de Banco de Tierras es novedoso. El desarrollo de su sistema de gestión, aquí explicado, es pues innovador y ha supuesto un reto ya que tanto el Banco como su aplicación SIG-Web han ido evolucionando conjuntamente. Los resultados obtenidos en estos ya más de cuatro años en funcionamiento, son muy satisfactorios. El sistema cumple con los objetivos para los que ha sido desarrollado y es la pieza clave para la gestión del Banco de Tierras. La gran cantidad de información manejada por el sistema está bien gestionada gracias a la utilización de estándares. El uso de software libre se ha mostrado suficientemente robusto, con buen rendimiento y ha ayudado a abaratar los costes. Además, ha tenido una acogida aceptable entre usuarios en principio poco habituados al uso de aplicaciones informáticas.

Algunas ideas para mejorar la aplicación son: opción para añadir al visor otras capas WMS y poder visualizarlas simultáneamente con el resto de capas; uso de *tiles* (división del mapa en celdas) para que las peticiones se hagan tile a tile y así la carga del mapa sea más dinámica; actualización del framework web utilizado (Struts) por uno más moderno (Wicket), cuya integración ya sería en sí un desafío interesante; implementación de opciones para introducción y arrendamiento agrupado de parcelas; integración con la gestión de concentraciones parcelarias; intermediación para el arrendamiento de explotaciones agrarias.

Agradecimientos

En este trabajo han colaborado y ha sido financiado por la Consellería do Medio Rural e do Mar de la Xunta de Galicia, la Sociedad Anónima Gestora Bantegal y la Agencia Gallega de Desarrollo Rural. También está incluido en el proyecto Sistema de Información Geográfico para la Planificación Urbanística y Ordenación del Territorio utilizando Técnicas de Optimización en Procesadores Multi-núcleo (ref. 08SIN011291PR).

Referencias bibliográficas

Bayfield, N. G., Conroy, J., Birnie, R. V., Geddes, A., Midgley, J. L., Shucksmith, M. D., et al. (2005). Current awareness, use and perceived priorities for rural databases in Scotland. *Land Use Policy*, 22(2), 153-162.

- Carcedo, L., Fernández, M. B., & González, V. (1998). Intergraph - Aplicación de tecnologías abiertas a la gestión territorial de la comisión regional del Banco de Tierras Principado de Asturias. *Mapping Interactivo*(49).
- Corbelle-Rico, E., Crecente-Maseda, R., & Santé-Riveira, I. (2012). Multi-scale assessment and spatial modelling of agricultural land abandonment in a European peripheral region: Galicia (Spain). *Land Use Policy*, 29(3), 493-501.
- Crecente, R., Doallo, R., Miranda, D., Ónega, F., Parapar, J., & Touriño, J. (2005). Tecnología SIG y web para la dinamización del mercado de tierras en Galicia. *III Jornadas Sindur. Sociedad de la Información en Espacios Periféricos, Nuevas Formas de Exclusión Social* (pp. 199-210). Servicio de Edición Digital de la Universidad de Santiago de Compostela.
- Johnson, M., Singh, I., & Stearns, B. (2002). *Designing Enterprise Applications with the J2EE Platform* (2nd ed.). Prentice Hall PTR.
- Keenleyside, C., & Tucker, G. (2010). Farmland Abandonment in the EU: an Assessment of Trends and Prospects. *Institute for European Environmental Policy, London*.

iLeger: Uma proposta de Mediação Digital para Períodos Eleitorais

Artur Afonso de Sousa ¹, Luís Borges Gouveia ²

ajas@di.estv.ipv.pt, lmbg@ufp.edu.pt

¹ Instituto Politécnico de Viseu, Campus Politécnico de Repeses, 3504-510, Viseu, Portugal

² Universidade Fernando Pessoa, Praça 9 de Abril n.º 349, 4249-004, Porto, Portugal

DOI: 10.4304/risti.9.43-57

Resumo: Neste artigo apresenta-se uma proposta de mediação digital para a participação pública direta em períodos eleitorais. A proposta assenta numa aplicação Web, designada *iLeger*, baseada nos princípios dos Media Sociais. Pretende-se, com esta proposta, contribuir para reduzir o fosso existente na comunicação entre a comunidade e os candidatos, tornar as campanhas mais abertas e estimular os cidadãos a envolverem-se e a participarem ativamente nos debates eleitorais. Apresentam-se as principais áreas funcionais do *iLeger*, assim como os resultados de um caso de estudo sobre as Eleições Legislativas Portuguesas de 2011.

Palavras-chave: Mediação digital; Eleições; eCampanha; eParticipação; Media Sociais.

Abstract: This paper presents a proposal for digital mediation for direct public participation during electoral periods. With this proposal, a Web application based on social media principles, it is intended to narrow the communication gap between voters and candidates, make campaigns more open and encourage citizens to become involved and participate in electoral debates. This paper also presents the main features of the proposed Web application and includes results from a case study about the Portuguese Parliamentary Elections held in 2011.

Keywords: Digital Mediation; Elections; eCampaigning; eParticipation; Social Media.

1. Introdução

A Internet é hoje uma ferramenta que molda a nossa vida em muitos aspetos. Para alguns é uma fonte inesgotável de informação e, para outros é um meio para gerir contas bancárias, fazer compras e utilizar os serviços públicos. Grande parte das

atividades da vida real tem já uma equivalente em linha. Seguindo essa tendência, também no campo da participação pública se tem verificado uma integração crescente das Tecnologias da Informação e Comunicação e da Internet, levando ao conceito de participação eletrónica - eParticipação (Stanford & Rose, 2007).

A utilização da Internet tem vindo a tornar-se relativamente mais interativa e orientada para o utilizador. A Web 2.0 e, mais recentemente o surgimento dos Media Sociais, não só criaram novas possibilidades para a comunicação, mas também novas formas de comportamento e envolvimento social e político (Kes-Erkul & Erdem-Erkul, 2009). Hoje, os *sites* de redes sociais como o Facebook, YouTube, Twitter, LinkedIn, Wikipedia e Flickr têm milhões de utilizadores ativos. Com os exemplos de mobilização de massas, como a Primavera Árabe e os movimentos de protesto contra a crise económica global, como o *Occupy Wall Street* (<http://occupywallst.org/>) e o *We Are the 99 Percent* (<http://wearethe99percent.tumblr.com/>), é seguro afirmar que os Media Sociais estão a transformar a sociedade e o jogo da política. Na revisão da literatura sobre Media Sociais e participação, Effing e os seus colegas alegam que o uso da Internet pelos cidadãos é cada vez mais social e participativo (Effing, Hillegersberg & Huibers, 2011). Eles ainda argumentam que um fator-chave da Web 2.0 e dos Media Sociais é a participação.

O acréscimo de interatividade torna a utilização da Internet num ambiente importante de comunicação em disputas eleitorais e acaba por diferenciar as campanhas *online* das campanhas empreendidas nos Media tradicionais. De acordo com (Bimber & Davis, 2003), a real contribuição democrática das campanhas em linha estaria na apropriação do potencial interativo da Internet para tirar os eleitores da função de meros espetadores.

No entanto, considerando, em campanhas eleitorais, ferramentas como blogues, *sites* de campanha dos partidos políticos, *e-mail*, boletins informativos, ou abordagens mais tradicionais que cobrem as transmissões de TV, debates, SMS (*Short Message Service*), contactos porta-a-porta ou discursos públicos, elas estão mais concentradas na comunicação unidirecional, como ilustra a Figura 1, e não suportam um eficiente processo de comunicação escalável baseado nos objetivos e necessidades de todas as partes interessadas.



Figura 1 – Comunicação unidirecional entre candidatos e cidadãos

Se considerarmos a perspetiva do cidadão e o processo de compilação de informação que precede a decisão de voto, temos duas grandes abordagens. A primeira, que pode ser denominada passiva, consiste em assistir a notícias, debates e discursos dos candidatos na televisão ou na rádio, assim como às análises dos comentadores políticos. Na segunda, a ativa, o cidadão consulta o programa eleitoral dos diferentes candidatos, tipicamente nos correspondentes sítios Web, ou eventualmente consulta outros sítios Web que agregam esta informação e providenciam uma comparação entre as posições dos diferentes candidatos sobre vários assuntos chave.

Depois de observar o tipo de comunicação política e de cobertura das campanhas eleitorais operado pelos órgãos de comunicação social tradicionais, surgiu uma pergunta de investigação preliminar importante: como estimular os cidadãos a envolverem-se e a participar ativamente nos debates eleitorais, através de mediação digital?

Neste contexto, acredita-se que pode ser útil e desejável ter uma solução que agregue num único local, neutro e regulado, os principais intervenientes num processo eleitoral e que possibilite uma comunicação multidirecional entre eles, como ilustrado na Figura 2. Isso permitiria que, por um lado, os cidadãos se esclarecessem acerca das questões e problemas mais importantes da sociedade e, por outro lado, que os candidatos tomassem conhecimento das principais ideias e problemas da comunidade sobre as diferentes áreas da governação (educação, saúde, economia, entre outras).

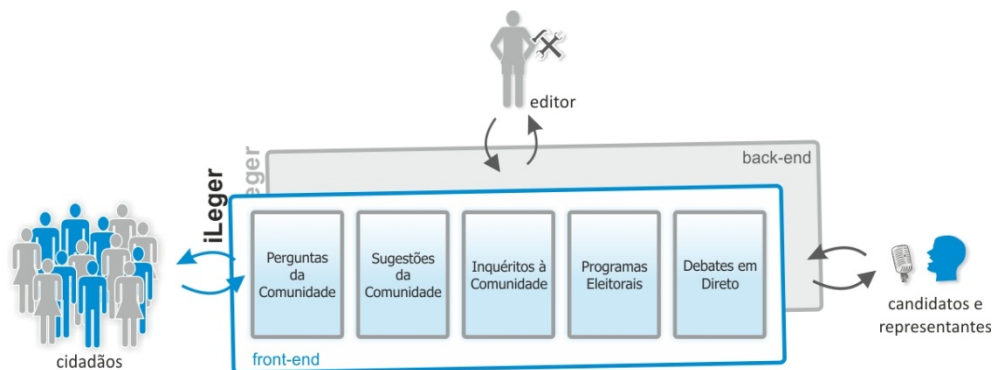


Figura 2 – Comunicação multidirecional entre cidadãos e candidatos

Assim, propõe-se uma aplicação Web, designada *iLeger*, especificamente concebida para reunir, durante o período eleitoral, os cidadãos e os candidatos a uma eleição num espaço deliberativo compartilhado. A interação e a colaboração são suportadas através de perguntas, respostas, sugestões, comentários, votações e debates em direto. Com esta aplicação pretende-se contribuir para colmatar a lacuna de comunicação identificada entre estes dois principais intervenientes, para tornar as campanhas mais abertas a discussões com o eleitorado e para converter o eleitor - que antes exercia a função de consumidor de informação - num agente com capacidade de intervir e de produzir informação.

A aplicação *iLeger* está integrada no projeto *Liberopinion* (<http://www.liberopinion.com>) que visa criar uma plataforma tecnológica na área dos

Media Sociais e da eParticipação, com ênfase na interação entre os utilizadores. Atualmente, a plataforma *Liberopinion* consiste em duas aplicações, a descrita neste artigo, *iLeger* e o *Governómetro* (Afonso de Sousa & Borges Gouveia, 2011), que visa monitorizar o desempenho da atividade governativa. Em síntese, o *Governómetro* é uma aplicação Web baseada nos princípios da eParticipação, especificamente projetada para monitorizar e discutir, de forma objetiva e independente, a atividade do governo e as novas leis a nível nacional, regional ou local. Numa primeira fase, o *Governómetro* foca três aspetos: a evolução dos indicadores de conjuntura, os objetivos do governo e as medidas de governação.

A aplicação *iLeger* foi recentemente testada na Eleição do Bastonário da Ordem dos Médicos de Portugal de 2010 (<http://om.ileger.sapo.pt>) e foi usada em parceria com o maior portal Web português (SAPO - <http://www.sapo.pt>), propriedade da Portugal Telecom, nas Eleições Presidenciais Portuguesas de 2011 (<http://presidenciais.ileger.sapo.pt>) e nas Eleições Legislativas Portuguesas de 2011 (<http://ileger.noticias.sapo.pt/legislativas/2011/>).

Este artigo está estruturado do seguinte modo: Na secção 2 apresentam-se algumas iniciativas de participação em linha em períodos eleitorais. Na secção 3 descrevem-se as principais áreas funcionais da aplicação *iLeger*. Na secção 4 são apresentados os resultados de um caso de estudo sobre as Eleições Legislativas Portuguesas de 2011. Finalmente, na secção 5 apresentam-se os comentários finais e abordam-se alguns tópicos para futura investigação.

2. Mediação digital e eleições

Têm sido levadas a cabo várias iniciativas em linha para ajudar os cidadãos a esclarecer as questões e as propostas eleitorais por parte dos diferentes candidatos. Uma abordagem conhecida apresenta um questionário aos cidadãos sobre vários assuntos, faz uma comparação estatística com as posições dos candidatos e obtém o candidato que melhor corresponde às respostas do utilizador (Smartvote, 2005). Todavia, isso não permite que o cidadão comunique e envie perguntas aos candidatos. Ademais, as perguntas formuladas são baseadas no programa eleitoral, tal como definido por cada candidato e não fornecem qualquer base para a interação. Também existem outros *sites* que comparam as propostas dos candidatos em vários tópicos (CNN Election Center, 2010).

Uma outra abordagem procura retificar a lacuna na comunicação entre os cidadãos e os políticos (Abgeordneten, 2010). Nessa iniciativa, é exibida a lista de representantes políticos, bem como dos candidatos às eleições, e os cidadãos podem enviar perguntas para os candidatos responderem. Porém, o *site* está desenhado em torno de cada representante político e não parece oferecer nem uma solução escalável quando o número de perguntas aumenta, nem uma comparação direta (lado a lado) das respostas dos candidatos para uma mesma pergunta, e nem a possibilidade de debater em torno da questão e das respetivas respostas.

Em (Aggio, Marques & Sampaio, 2011) descreve-se uma iniciativa de participação mantida pelo candidato José Serra às Eleições Presidenciais Brasileiras de 2010. Resumidamente, ao longo da primeira fase das eleições a campanha de José Serra

lançou uma plataforma Web de comunicação cujo objetivo era a construção de um plano de governação colaborativo, apto a agregar contribuições de cidadãos, especialistas e demais interessados em questões políticas relevantes para o Brasil. Para o efeito, foram criados fóruns temáticos classificados de acordo com a região do país ou com a natureza da questão abordada. Em (Talbot, 2008; Greengard, 2009) é analisada, a partir de uma perspectiva de eParticipação, a bem-sucedida campanha eleitoral de Barack Obama durante as Eleições Presidenciais de 2008. Todavia, essas abordagens servem essencialmente para envolver os cidadãos em torno de uma candidatura. Isto é, não juntam num único espaço os vários candidatos e os cidadãos para comunicarem e partilharem ideias e opiniões.

O espaço *U.S. Politics* no Facebook (<http://www.facebook.com/uspolitics>) destaca o uso desta rede social por políticos. Uma iniciativa interessante, levada a cabo por uma parceria entre o Facebook e a estação de televisão NBC, transmitiu ao vivo, em http://www.facebook.com/uspolitics?sk=app_201387976576727, o debate entre os candidatos presidenciais do Partido Republicano (Grand Old Party - GOP) realizado em 8 de Janeiro de 2012. Nesse espaço os cidadãos foram previamente convidados a submeter questões para os candidatos. Algumas dessas perguntas foram depois usadas durante o debate, juntamente com as perguntas do moderador, o jornalista David Gregory, e com mais algumas perguntas colocadas por cidadãos enquanto decorria o debate. Há, todavia, a questão sobre o modo de seleção das perguntas para o debate. Apesar de possuir uma premissa participativa, a iniciativa não é clara sobre as regras de seleção, não havendo qualquer referência ao modo de escolha das perguntas. Uma outra limitação da iniciativa diz respeito à organização da informação. Não existia nenhuma estrutura temática para a submissão de perguntas. Por outro lado, também não existiam áreas específicas para a submissão de sugestões, nem para realizar inquéritos aos cidadãos.

3. Estrutura funcional da aplicação *iLeger*

A plataforma *iLeger* foi projetada e desenvolvida de raiz para atender às necessidades e aos objetivos dos principais intervenientes no processo eleitoral, nomeadamente os cidadãos e os candidatos. Como ilustrado na Figura 3, a aplicação permite ao editor criar e gerir cinco tipos de iniciativas de participação em linha: perguntas dos cidadãos e respetivas respostas dos candidatos, sugestões e ideias da comunidade, inquéritos aos cidadãos, o programa eleitoral dos candidatos e, finalmente, debates em direto. A gestão da plataforma, dos utilizadores e dos eventos de participação, incluindo a sua moderação, é da responsabilidade do editor.

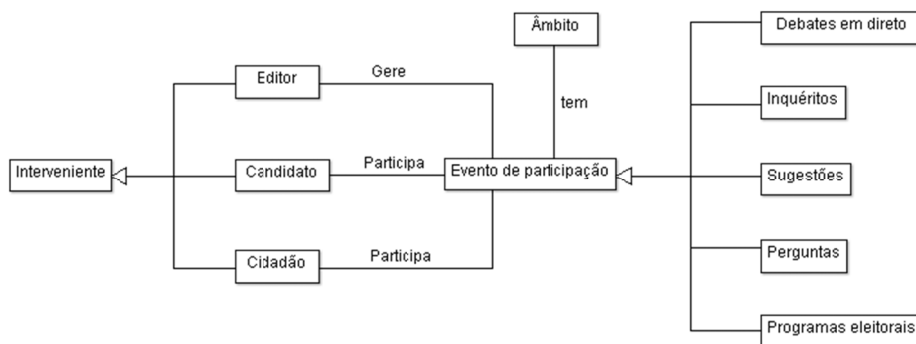


Figura 3 – Diagrama de classes UML simplificado da aplicação iLeger

Convém referir que, nas Eleições Legislativas Portuguesas de 2011, para poder usufruir das principais funcionalidades, tais como submeter perguntas, sugestões, comentários e votar, cada utilizador tinha que estar previamente registado na plataforma e tinha que efetuar o login. Por outro lado, caso não efetuasse o login, o utilizador apenas podia consultar os conteúdos da aplicação. No entanto, é possível configurar o iLeger para diferentes definições, de modo a permitir a interação por utilizadores não registados. Por exemplo, há um cenário em que utilizadores não registados podem votar, mas não podem introduzir conteúdos, e outro em que é permitida a votação e a introdução de conteúdos. Na última configuração, a única limitação para os utilizadores não registados é a falta de notificações por e-mail e dos recursos adicionais característicos das redes sociais, tais como seguir utilizador e acesso ao perfil público.

Todas as intervenções dos cidadãos foram alvo de moderação, de acordo com as regras de utilização da plataforma. Note-se que quando se registavam na plataforma, os utilizadores tinham que aceitar os termos de utilização. Por outro lado, as intervenções dos candidatos não foram moderadas. De modo a incentivar a participação, foi permitido aos cidadãos requerer o anonimato em todas as intervenções escritas submetidas na plataforma. Não obstante, a plataforma está desenhada para suportar diferentes configurações para a moderação. Por exemplo, é possível publicar diretamente todo o conteúdo, ou seja, desabilitar a moderação, ou moderar apenas as entradas denunciadas pelos utilizadores da plataforma.

Acredita-se que as redes sociais em linha serão cada vez mais importantes para as comunidades. Assim, considera-se muito importante munir a plataforma iLeger com recursos característicos das redes sociais. Por exemplo, um utilizador registado pode seguir outros utilizadores registados na plataforma. Todos os utilizadores registados possuem uma área de perfil onde podem colocar informação pessoal, nomeadamente dados de contacto, links para as suas páginas nas redes sociais e de blogues. Na área de perfil público de cada utilizador é também apresentada a sua atividade (as suas perguntas, sugestões e comentários) recente no iLeger, bem como a sua rede social.

A integração da plataforma com as redes sociais também é de suma importância. Por esse motivo, e como um passo inicial nessa direção, os utilizadores podem partilhar no Facebook e publicar diretamente no Twitter as perguntas e sugestões submetidas no iLeger. Deste modo, providencia-se uma interface mais aberta para promover a

participação e reforça-se a voz do cidadão, uma vez que se aumenta o alcance e o potencial impacto de participação de cada indivíduo. Note-se que a publicação nas redes sociais não depende da aprovação do moderador.

Atualmente, o iLeger pode também ser configurado em relação ao tipo de interação dos candidatos. Estão previstos dois cenários: com ou sem interação por parte dos candidatos. Com interação, os candidatos têm uma conta de acesso e são responsáveis pela introdução de conteúdos, permitindo a comunicação direta com os outros utilizadores. Na ausência de interação do candidato, o iLeger pode ser usado pelo editor para identificar as principais questões e sugestões dos eleitores, bem como as suas opiniões sobre as questões-chave sobre a eleição. O editor pode também colocar conteúdos sobre as candidaturas para que os cidadãos possam analisar e comentar. A seguir, apresentam-se as principais funcionalidades da aplicação, organizadas por ator.

3.1. Cidadãos

Resumidamente, como pode observar na Figura 4, os cidadãos podem submeter perguntas, sugestões e comentários, votar, participar em debates em direto, definir critérios para receber notificações (por exemplo: quando um candidato responde a uma pergunta ou comenta uma sugestão do utilizador, quando outro utilizador responde a um comentário do utilizador, entre outros), seguir ou deixar de seguir outros utilizadores e candidatos, editar o seu perfil público, propor sugestões para melhoria do iLeger.

Os cidadãos podem ainda visualizar um vasto conjunto de informação. Por exemplo, podem consultar e comparar as respostas dos candidatos; consultar, avaliar e comentar os programas eleitorais propostos por cada candidatura; consultar o perfil público dos outros utilizadores e dos candidatos, bem como a rede (seguidores) e a atividade do candidato na plataforma; consultar o arquivo; consultar resultados estatísticos; visualizar os TOPs das perguntas e das sugestões mais populares, etc.

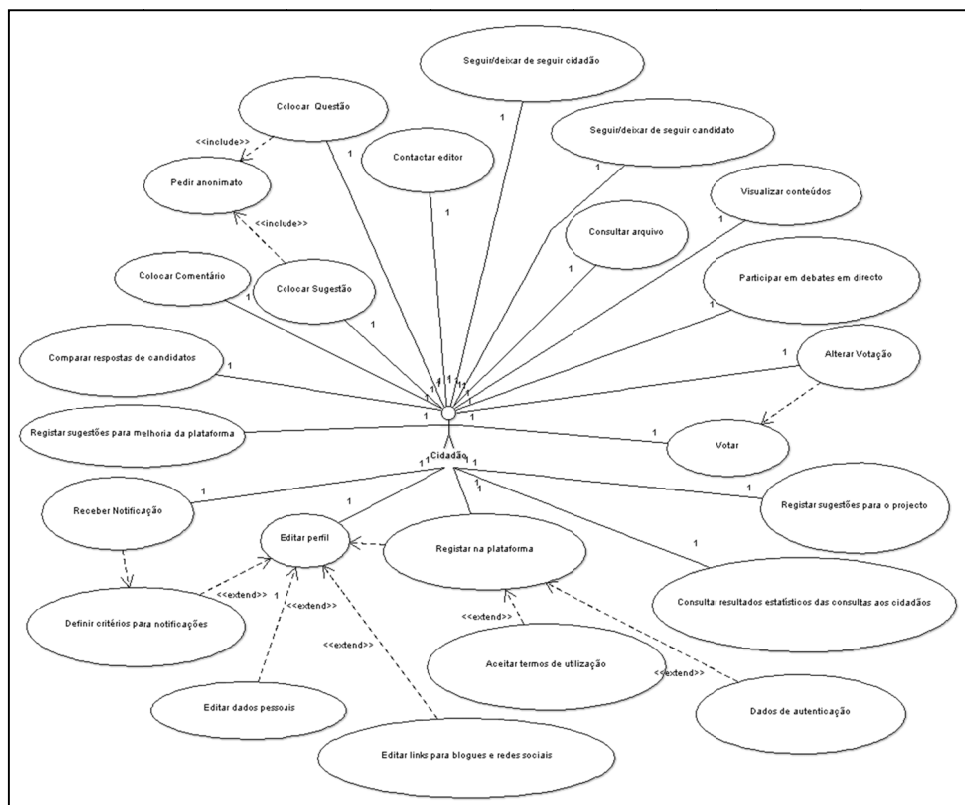


Figura 4 - Diagrama de casos de uso simplificado do ator cidadão

3.2. Candidatos e representantes

No caso de o iLeger estar configurado para haver interação direta dos candidatos, como pode observar na Figura 5, os candidatos e os seus representantes podem editar o seu perfil, responder a perguntas colocadas pelos cidadãos, comentar sugestões, marcar perguntas e sugestões para responder e comentar mais tarde, comentar respostas e comentários a sugestões de outros candidatos, participar em debates em direto, consultar dados estatísticos das consultas feitas aos cidadãos, definir critérios para receber notificações (por exemplo: quando outro candidato comenta uma resposta ou um comentário seu, quando outro candidato comenta uma proposta eleitoral sua, entre outros), apresentar o seu programa eleitoral (PE), incorporar sugestões dos cidadãos no PE, comentar os PE dos outros candidatos.

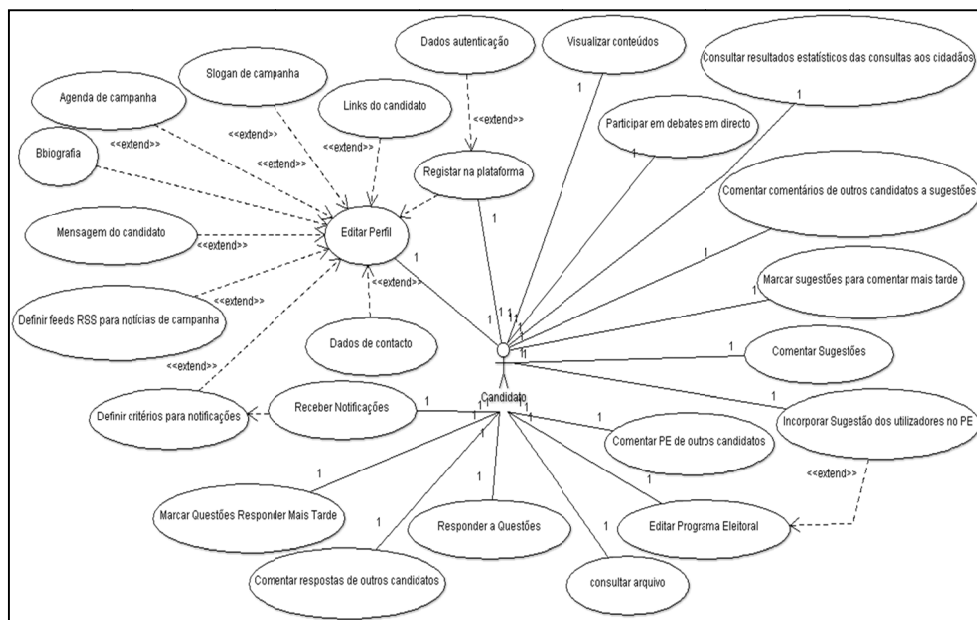


Figura 5 - Diagrama de casos de uso simplificado do ator candidato

O vasto conjunto de informação anteriormente referido para os cidadãos poderem visualizar está também, naturalmente, disponível para os candidatos. Destaca-se ainda a possibilidade de um candidato poder visualizar estatísticas sobre o seu desempenho, nomeadamente as votações às suas respostas e propostas eleitorais, a sua posição no ranking das melhores respostas, o seu nível de atividade, etc.

3.3. Editor da plataforma

A administração de utilizadores, a configuração da plataforma e a gestão dos eventos de participação e dos conteúdos editoriais é efetuada a partir de uma secção dedicada, o BackOffice. Como pode observar na Figura 6, o editor da plataforma pode criar eventos de participação para angariação de perguntas e de sugestões, para auscultação da opinião dos cidadãos (inquéritos) e debates em directo. O editor pode seleccionar as iniciativas de participação que quer destacar na respetiva secção (perguntas, sugestões e debates em directo), até a um máximo de quatro em simultâneo. O editor pode ainda definir o modo de moderação de cada evento de participação. Caso defina que o evento é moderado, todos os conteúdos escritos submetidos pelos cidadãos são alvo de moderação. O editor, no papel de moderador, deve fazer a moderação à luz dos termos de utilização do iLeger. O editor pode marcar/selecionar perguntas e sugestões colocadas pelos cidadãos, que considere pertinentes para incluir em TOPs editoriais.

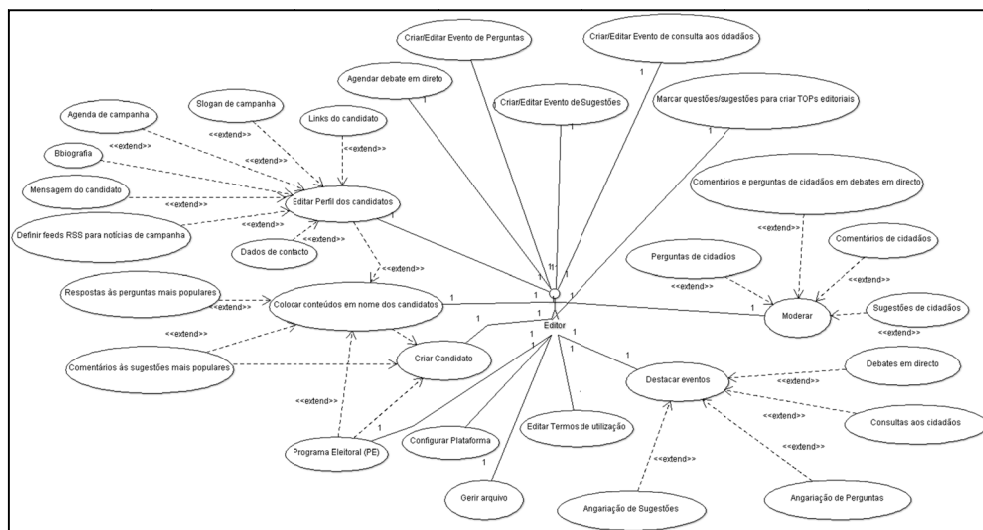


Figura 6 - Diagrama de casos de uso simplificado do ator editor

No caso de o iLeger estar configurado para não haver interação direta dos candidatos, o editor pode colocar informação sobre cada candidato: slogan de campanha, biografia, agenda de campanha, mensagem do candidato, notícias (texto ou através de um feed RSS), imagens e vídeos de campanha, links para o sítio Web e para as redes sociais da candidatura e o programa eleitoral. Neste cenário, o editor pode ainda usar o iLeger para identificar as melhores questões dos cidadãos eleitores. Depois, pode remetê-las a todos os candidatos para que possam responder. Finalmente, o editor publica no iLeger as respostas dos candidatos para que os cidadãos as possam comparar.

4. Caso de estudo: As Eleições Legislativas Portuguesas de 2011

A plataforma iLeger foi usada, em parceria com o maior portal Web de Portugal, o SAPO, propriedade da Portugal Telecom, durante a campanha para as Eleições Legislativas Portuguesas em Junho de 2011. Cobriu as duas últimas semanas antes das eleições, entre 20 de Maio e 3 Junho de 2011.

A versão do iLeger usada foi configurada para que os utilizadores tivessem que se registar para poderem submeter conteúdos (perguntas, sugestões e comentários) e votar. Todos os conteúdos escritos submetidos por cidadãos foram sujeitos a moderação e as várias candidaturas apenas participaram em debates em direto. Note-se, contudo, que para participar nos debates em direto não era necessário estar registado no iLeger.

Para o registo dos utilizadores foi usado o mecanismo de Single Sign On (SSO) do nosso parceiro. Desta forma, os utilizadores já registados no SAPO poderiam entrar no iLeger sem necessitarem de efetuar um novo registo. Foram contabilizados 290 utilizadores distintos que efetuaram o login no iLeger, ou seja, que ficaram habilitados para submeter conteúdos escritos e para votar. As estatísticas extraídas do Google

Analytics mostram que, durante as duas semanas, 21.486 utilizadores únicos visitaram o iLeger (perfazendo um total de 44.777 páginas vistas). Assim, apenas 1,3% dos visitantes distintos chegaram a efetuar login no iLeger.

Os cidadãos foram convidados a criar um top de 10 perguntas para ser, depois, apresentado simultaneamente às candidaturas durante um debate em direto realizado no dia 31 de Maio de 2011 no **Instituto Superior de Ciências Sociais e Políticas** (ISCSP). Sucintamente, foram criadas três iniciativas de participação. Cada iniciativa tinha a data limite de 30 de Maio de 2011 para a submissão de perguntas e tinha um tema associado, nomeadamente o crescimento da economia, o estado social e a ajuda externa. Convém referir que, dado o contexto económico e financeiro de Portugal nesse momento, esses foram os temas dominantes da campanha eleitoral. Para tal, os cidadãos inscritos enviaram perguntas e votaram, de acordo com a sua relevância. Nessa fase, foram aceites pelo moderador 107 das 116 perguntas submetidas pelos cidadãos, indicando uma taxa de rejeição de 8%.

O debate do ISCSP foi moderado pela diretora do canal de notícias do portal SAPO e, através de uma parceria entre a estação de televisão SIC Notícias e o portal SAPO, foi difundido em direto no iLeger, via streaming de vídeo. As 10 perguntas mais votadas no iLeger foram as únicas usadas no debate e foram respondidas por cada um dos políticos convidados. A Figura 7 ilustra a difusão do debate na área do iLeger destinada aos debates em direto.



Figura 7 - Debate em direto transmitido via *streaming* de vídeo no iLeger nas Eleições Legislativas 2011

Destaque-se o facto de terem aderido a esta iniciativa políticos conceituados, entre os quais líderes parlamentares e elementos que acabariam por vir a fazer parte do governo eleito como ministros.

Adicionalmente, na segunda semana foram realizados seis debates em direto, cada um com uma candidatura. Cada debate durou cerca de uma hora e meia. Ao longo dos seis debates houve 3779 entradas submetidas na forma de perguntas ou de comentários. No entanto, por restrições de tempo e de moderação, apenas 133 dessas entradas foram abordados pelas candidaturas. Para participar nos debates em direto os utilizadores não tinham que estar registados no iLeger. Para a realização dos debates em direto foi incorporado na plataforma iLeger o componente CoveritLive (www.coveritlive.com).

É importante notar que, segundo as estatísticas do Google Analytics, dos 21.486 visitantes únicos durante as duas semanas, 19.419 entraram pela primeira vez no iLeger durante os dias dos debates em direto, demonstrando o interesse dos cidadãos para participar em eventos ao vivo e de curta duração. Na Figura 8 ilustra-se a descrição geral dos visitantes do iLeger entre 20 Maio e 3 de Junho de 2011.



Figura 8- Descrição geral dos visitantes do iLeger entre 20 Maio e 3 de Junho de 2011

Os picos refletem os dias em que se realizaram debates em direto. Uma das possíveis razões para a grande adesão dos cidadãos nos dias dos debates em direto pode ser o facto de o nosso parceiro ter feito nesses dias maior divulgação da iniciativa na sua home page. Isto também demonstra a grande importância da divulgação das iniciativas de participação. Consideramos que os Media têm, a este nível, também um papel muito importante.

Durante as duas semanas os utilizadores registados submeteram um total de 50 sugestões, das quais 9 foram rejeitadas pelo moderador. Nesta secção do iLeger, o editor criou, em simultâneo, três iniciativas de angariação de sugestões; desafiou os cidadãos a dizer o que fariam se fossem a Chanceler Alemã Angela Merkel, o presidente do FMI (Fundo Monetário Internacional) e o presidente da União Europeia. Note-se que o editor assumiu que as personagens (tomadoras de decisão) consideradas nas três

iniciativas de recrutamento de ideias tinham um papel preponderante na eventual ajuda externa a Portugal.

No global, houve 299 votos em perguntas, 92 votos em sugestões e 1073 votos nas 15 questões do inquérito aos cidadãos.

É também pertinente notar que, se não se contabilizarem os debates em direto, dos 290 utilizadores únicos que efetuaram login, 156 submeteram conteúdos escritos (116 perguntas e 50 sugestões) ou votaram nas perguntas, nas sugestões e nos inquéritos. Isto indica que, como ilustrado na Figura 9, participaram ativamente no iLeger aproximadamente 54% dos utilizadores que efetuaram login.

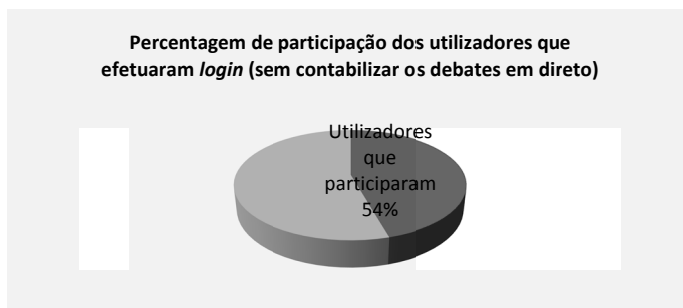


Figura 9 - Percentagem de participação dos utilizadores que efetuaram *login* (sem contabilizar os debates em direto)

Nestas eleições o iLeger foi usado principalmente para identificar as principais questões e sugestões dos cidadãos, bem como a sua opinião sobre os temas-chave da eleição. Através da realização dos debates em direto, foi também possível ficar com uma melhor perceção do ponto de vista dos representantes das candidaturas sobre as 10 perguntas mais votadas pelos cidadãos ao longo da primeira semana, bem como sobre outras perguntas colocadas em direto. Ao comparar os pontos de vista, os cidadãos ficam com informações adicionais sobre a posição dos candidatos acerca das principais questões, ajudando-os, eventualmente, a decidir pelo “melhor” candidato.

5. Comentários finais

Os partidos políticos e os candidatos a eleições têm vindo a realizar grandes investimentos (tempo, dinheiro e recursos humanos) em ferramentas de comunicação baseadas na Web, tais como as redes sociais (Facebook, Twitter, YouTube, Flickr, Myspace, entre outras), a blogosfera, e os Web sites de campanha, para transmitir as suas mensagens aos cidadãos eleitores.

Apesar de se acreditar fortemente que as ferramentas de participação baseadas na Internet, tais como as redes sociais e como a aplicação aqui apresentada, serão cada vez mais importantes em campanhas eleitorais, e que, se forem convenientemente usadas, elas têm potencial para contribuir significativamente para reverter o atual afastamento dos cidadãos dos debates eleitorais, defende-se que o foco tem que estar essencialmente na participação e nas pessoas (cidadãos e candidatos) e não tanto na tecnologia.

Perante as experiências de utilização do iLeger nas eleições do Bastonário da Ordem dos Médicos, Presidenciais e Legislativas Portuguesas de 2011 e à luz do feedback recebido de alguns atores envolvidos nessas eleições, quando se tentou responder à questão de investigação “Como estimular os cidadãos a envolverem-se e a participar ativamente nos debates eleitorais, através de mediação digital?”, alega-se que não se alcançou uma resposta conclusiva e completa. Todavia, tal como em (Moreira, Moller & Ladner, 2009; Stromer-Galley, 2000; Effing, Hillegersberg & Huibers, 2011) argumenta-se que o problema da eParticipação não é apenas uma questão de tecnologia, mas também sobre a mudança para uma cultura mais aberta e de colaboração.

Espera-se que os candidatos e os representantes democráticos aproveitem as características de ubiquidade da Internet e as oportunidades da Web colaborativa, emancipando-se dos Media tradicionais, em favor da Web 2.0 e dos Media Sociais, para as suas estratégias eleitorais e de comunicação e que, cada vez mais, promovam e participem em iniciativas de participação que os aproximem mais dos cidadãos.

Ainda em relação à experiência de utilização do iLeger, considera-se que a divulgação é um fator chave para o sucesso deste tipo de iniciativas de participação. Era claramente perceptível que sempre que havia divulgação na home page do nosso parceiro, aumentava consideravelmente o número de visitas no iLeger (cerca de 90%). A parceria com um dos principais órgãos de Media de Portugal também se revelou como um fator facilitador para atrair os políticos a participar. Portanto, entende-se que os Media podem desempenhar um papel muito relevante em iniciativas de eParticipação. Note-se que eles possuem já grandes comunidades de utilizadores com alguns hábitos de participação. Por outro lado, têm também um conjunto de comentadores e analistas que podem contribuir para a qualidade das discussões. A experiência jornalística que possuem pode também contribuir para uma melhor dinamização da plataforma e para garantir a qualidade dos conteúdos editoriais. É, no entanto, muito importante que tudo seja feito com absoluta neutralidade política. Outro contributo importante resultante das nossas experiências diz respeito à gestão editorial deste tipo de aplicações. Os utilizadores habituais da Internet gostam de novidade constante. Assim, entende-se que os cidadãos (e os políticos) devem ser convidados a participar em eventos de curta duração e sobre temas da atualidade. Considera-se que os Media estão numa posição privilegiada para desempenhar o papel de curador de informação (Rosembaum, 2011) de plataformas de eParticipação.

Como resultado da experiência obtida, surgem diversas possibilidades de exploração e aprofundamento dos dados obtidos. Em particular, torna-se pertinente colocar a questão para futuro trabalho: Qual o impacto dos mecanismos de mediação digital na participação?

Referências

- Abgeordneteten, <http://www.abgeordnetetenwatch.de/> (acedido em 20 de Maio, 2010)
- Afonso de Sousa, A., & Borges Gouveia, L. (2011). Governmeter: a Web Application for Monitoring Governmental Activity. Proceedings of 6th Iberian Conference on Information Systems and Technologies – CISTI2011. Chaves, Portugal.

- Aggio, C., Marques, J., & Sampaio, R. (2011). Campanhas Online, Participação Política e Esfera Pública: O Caso do Plano de Governo Colaborativo nas Eleições Brasileiras de 2010. *Public Sphere Reconsidered -Theories and Practices*, LabCom Books, pp. 3-21
- Bimber, B. & Davis, R. (2003). Campaigning Online: The Internet in U.S. Elections. *Oxford University Press*
- CNN ElectionCenter2008. (2008). <http://edition.cnn.com/ELECTION/2008/issues/> (acedido em 6 de Maio, 2010)
- Effing, R., Hillegersberg, J.V., & Huibers, T. (2011). Social Media and Political Participation: Are Facebook, Twitter and YouTube Democratizing Our Political Systems?, E. Tambouris, A. Macintosh, and H. de Bruijn (Eds.): ePart 2011, LNCS 6847, pp. 25-35
- Greengard, S. (2009). The First Internet President. *Communications of the ACM*, 52(2), pp.16--18
- Kes-Erkul, A. & Erdem-Erkul, R. (2009). Web 2.0 in the Process of e-participation: The Case of Organizing for America and the Obama Administration. National Center for Digital Government, Working paper No. 09-001
- Moreira, A.M., Moller, M., Gerhardt, G., & Ladner, A. (2009). E-Society and E-Democracy, eGovernment Symposium, Berne, Switzerland
- Rosembaum, S. (2011). Curation Nation: How to Win in a World Where Consumers are Creators. *McGraw-Hill*; 1st edition
- Sanford, C., & Rose, J. (2007). Characterizing eParticipation. *International Journal of Information Management*, vol. 27, pp. 406-421.
- SmartVote (2011). <http://www.smartvote.ch/> (acedido em 15 de Março, 2011)
- Stromer-Galley, J. (2000). On-Line Interaction and Why Candidates Avoid It. *Journal of Communication*, 50(4) pp. 111—132
- Talbot, D. (2008). How Obama Really Did It: The social-networking strategy that took an obscure senator to the doors of the White House. *Technology Review*, 9/10

Evaluación de la Privacidad de una Red Social Virtual

J. R. Coz Fernández ¹, E. Fojón Chamorro, R. Heradio Gil ¹, J. A. Cerrada Somolinos ¹

jrcozf@gmail.com, efojonc@gmail.com, rheradio@issi.uned.es, jcerrada@issi.uned.es

¹Departamento de Ingeniería de Software y Sistemas Informáticos. Universidad Nacional de Educación a Distancia. Ciudad Universitaria, Juan del Rosal 16, E-28040. Madrid, España.

DOI: 10.4304/risti.9.59-73

Resumen: Tanto para las organizaciones y empresas como para la Sociedad en su conjunto, la protección del ciberespacio constituye un aspecto crucial y la privacidad de la información es uno de los pilares sobre los que descansa esta protección. En el proceso de construcción del ciberespacio, las redes sociales virtuales se han convertido en uno de los elementos más relevantes para el intercambio de información, y su utilización de forma global y masiva pone de relevancia su gran importancia estratégica. En este artículo se propone la evaluación de la privacidad en las redes sociales virtuales, mediante un modelo de madurez, un marco para la evaluación y un cuadro integral de mandos.

Palabras clave: Privacidad, redes sociales virtuales, modelos de madurez, cuadro integral de mandos.

Abstract: For organizations, companies and society as a whole, the protection of cyberspace is a crucial aspect and privacy of information is one of the pillars on this protection. In the cyberspace construction process, virtual social networks have become one of the most important information exchange elements and its use in a comprehensive and massive manner has reinforced its strategic significance. This paper proposes the evaluation of privacy in virtual social networks through a maturity model, a framework for comprehensive assessment and a balanced scorecard.

Keywords: Privacy, social networks, maturity models, balanced scorecard.

1. Introducción

La sociedad de la información es definida como aquella en la cual la creación, distribución y manipulación de la información forman parte importante de las actividades culturales y económicas. El termino sociedad de la información fue acuñado por primera vez en 1962 por Fritz Machlup (1962), pero no es hasta la década de los 70 cuando se generaliza su uso, debido, fundamentalmente, a una evolución en los medios de generación de riquezas, pasando de los sectores industriales a los sectores de la tecnología de la información y las comunicaciones (TIC). Hoy en día la

economía globalizada contemporánea concede al sector de las TIC el papel de motor de la economía global. A pesar de encontrarnos aun en los albores de la sociedad de la información, el ciberespacio, y más concretamente internet, juega un papel vertebrador en la corriente globalizadora que está desarrollándose en los comienzos del siglo XXI.

Los seres humanos, por su naturaleza, son sociables, y la cotidianidad en el uso de internet ha provocado que exporten sus usos y costumbres desde un “*mundo real*” a un “*mundo virtual*”. En el caso específico de las redes sociales, su reciente virtualización ha permitido que las redes sociales convencionales sean más accesibles a todo el mundo, permitiendo a los seres humanos comunicarse de una manera global y dinámica. Uno de los grandes retos que se presentan relacionados con las redes sociales virtuales es la protección de la privacidad de sus miembros o usuarios tal y como lo describen Adrienne Felt y David Evans (2008). La privacidad la podemos definir como el ámbito de la vida personal de un individuo que se desarrolla en un espacio reservado, y que debe de mantenerse de forma confidencial. No existen en la actualidad modelos o estándares consolidados relacionados con la privacidad de la información en este tipo de redes.

Con estos antecedentes, se presenta este artículo, donde se exponen diversos modelos y herramientas que den soporte a la gestión de la privacidad de la información en las redes sociales virtuales. El artículo se estructura de la siguiente manera. En la sección 2 se profundiza sobre el concepto de red social virtual. Los ámbitos y principios de protección que cubre la privacidad de la información en las redes sociales virtuales son presentados en la sección 3. Los procesos relacionados con la gestión de la privacidad se detallan en la sección 4. La sección 5 ofrece un resumen de algunos modelos y herramientas que pueden dar soporte a una evaluación de la gestión de la privacidad en una red social virtual como un modelo de madurez, un framework de evaluación de la madurez o un cuadro integral de mandos. Finalmente, en la sección 6 se resumen las principales conclusiones del presente artículo. Se incluye también un breve glosario de términos.

2. Las Redes Sociales Virtuales

El concepto general de red social lo acuñó Lozares, C. (1996) que la definió como el conjunto delimitado de actores, incluyendo individuos, organizaciones, grupos, comunidades o sociedades vinculados unos con otros mediante una relación o conjunto de relaciones sociales. Algunos autores como Vázquez Barquero, A. (1999) delimitan este concepto a la red de relaciones entre empresas u organizaciones incluyendo en el concepto el sistema de relaciones que vinculan a las empresas o actores entre sí, respecto a un contenido (recursos, información o tecnología). Otros autores se refieren a las redes sociales en Internet, cubriendo la posibilidad de establecer relaciones personales o profesionales, con individuos a los que no conocemos y de tal manera, que la red se va construyendo con las aportaciones de todos y cada uno de sus miembros, González Gálvez, P y Rey Martín, C. (2009). Tapscot, D. y Williams, A. D. (2007) defienden esta nueva forma de trabajo en red, aunando esfuerzos y colaboraciones para conseguir innovación, creando valor y apoyando a la toma de decisiones en las organizaciones y empresas.

Para otros autores es importante el papel que juega la calidad de la información contenida en las redes sociales en las decisiones estratégicas de las organizaciones, Miralles, F. (1998). Pero casi todos los autores coinciden en que las nuevas tecnologías de la información y las comunicaciones ha acelerado todos estos cambios sociales, proporcionando velocidad en el acceso y la gestión de la información y permitiendo una comunicación global, Van Bavel, R. et al. (2004) y Quan Haase, A. et al. (2002).

Los sociólogos han identificado la existencia de diferentes maneras de observar el fenómeno de las redes sociales, atendiendo a una serie de circunstancias, diferenciando entre *redes sociales por filiación*, como aquellas que se generan de forma espontánea en los grupos y cuya presencia imprime un clima de camaradería e identificación, *redes sociales por conocimiento*, como aquellas redes sociales que responden a intereses propios de la organización pero con un alto grado de interés personal, se generan para agregar valor a los procesos, mejorarlos o crearlos y *redes por contexto* como aquellas que responden a las funciones propias vinculadas a un cargo o a un grupo de ellos, Durán Torres, K. (2010).

El carácter social de los seres humanos es inherente a casi todas las situaciones de la vida, la cotidianidad del mundo virtual ha provocado que exportemos nuestros usos y costumbres del mundo real al mundo virtual. En el caso de las redes sociales, su virtualización ha permitido aunar todos los tipos de redes sociales del mundo real en una única red social virtual, dotándola de un carácter tangible que, en muchas ocasiones, las redes sociales reales no tienen.

Las redes sociales virtuales permiten a los seres humanos comunicarse de una manera global y dinámica dando un carácter tangible a muchos de los aspectos intangibles de las redes sociales del mundo real, al apoyarse en complejos sistemas de información y en el uso de dispositivos. Por tanto, podemos concluir que una red social virtual, en adelante RSV, son servicios prestados a través de Internet que permiten a los usuarios generar un perfil, desde el que hacer públicos datos e información personal y que proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características publicadas en sus perfiles.

Las RSV, independientemente de la tipología a la que pertenezcan, comparten un conjunto de características como la conexión rápida y dinámica de los usuarios que forman parte de la RSV, la compartición de todo tipo de información entre los usuarios, la difusión viral a través de sus usuarios y los riesgos a los que se ven expuestos los usuarios. La clasificación tradicional de las RSV se realiza en relación a dos parámetros, la *temática* de la RSV y el *público objetivo* al que van dirigidas, Larissa A. (2002). Las *RSV horizontales* son aquellas cuya temática es generalista y está dirigida a todos los perfiles de usuarios y las *RSV verticales* son aquellas RSV cuya temática es definida y está dirigida a un determinado perfil de usuario. Dentro de este tipo se encuentran las *RSV profesionales*.

Las nuevas necesidades de los usuarios de las RSV está provocando, cada vez más, la creación de RSV que aúnan características de las RSV horizontales y verticales, dando lugar a las *RSV híbridas*. En lo que respecta al formato, la mayoría de las RSV se encuadran dentro de los tres siguientes:

1. Las plataformas de intercambio de contenidos e información permiten el alojamiento e contenidos con el objetivo de poder ser compartidos por el resto de usuarios. Este tipo de plataformas, en muchas ocasiones, no son consideradas RSV, debido a que la mayoría de los expertos en redes sociales consideran que las RSV se fundamentan en la teoría de “*los seis grados de separación*”, en virtud de la cual cualquier individuo puede estar conectado a otra persona en el planeta, a través de una cadena de conocidos con no más de cinco intermediarios (con un total de seis conexiones), Milgram S. (1967).
2. Por otro lado, las redes de blogging se basan en el blog como herramienta de comunicación. La mayoría de los usuarios de este formato de RSV actualizan periódicamente el contenido de su blog compartiendo vivencias, conocimientos o ideas personales o profesionales con el resto de los usuarios autorizados.
3. La mayoría de los usuarios de las RSV asocian el concepto de RSV con las redes sociales virtuales basadas en perfiles. Este hecho se debe, fundamentalmente, a que son el formato de RSV más numeroso, Alexa. (2012), y demandado por los usuarios de las redes sociales, Diogo T. & Isabel A. (2011). La popularidad de estas herramientas reside en su facilidad de uso, su diseño “user friendly”, el elevado número de servicios que ofrecen a sus usuarios y la teoría de los seis grados de separación, O'Connor, B. et al (2010). La búsqueda de antiguos amigos, compañeros o familiares y proporcionar un mecanismo para expresar la opinión sobre determinados asuntos son los usos más populares de las RSV, Ku, Ke, y Chen, (2009); Java, A. et al (2007).

3. Ámbitos y principios de protección

Cuando un usuario completa el proceso de alta en una RSV crea una identidad virtual. Este hecho, aparentemente cotidiano, constituye una de las mayores amenazas contra la privacidad. Esta nueva identidad será manejada por el usuario, que podrá optar por manejar una identidad virtual idéntica a su *identidad real* o, por el contrario, manejar una *identidad ficticia*, donde los datos del usuario sean ficticios. También podrá optar por el uso de *identidad virtual híbrida*, donde algunos de los datos de usuarios sean reales y otros ficticios. El usuario debe manejar la identidad virtual de un modo responsable con el objetivo de no comprometer la identidad real o la privacidad. A la hora de determinar qué tipo de identidad virtual debe utilizar, han de tenerse en cuenta varios factores:

- Por un lado, el tipo de usuario de la RSV. En caso que el usuario potencial de la RSV sea un menor de edad, pero mayor de 14 años, es aconsejable hacer uso de una identidad virtual ficticia a la hora de darse de alta en la RSV. En caso que el usuario potencial de la RSV sea un adulto deberá tener en cuenta los otros factores para poder realizar una correcta toma de decisión.
- Finalidad en el uso de la RSV solicitada. Si el propósito del alta del usuario a la RSV es profesional es aconsejable que el usuario haga uso de una identidad virtual real, ya que el objetivo suele ser la búsqueda de trabajo o el intercambio

de información profesional. En el resto de los casos es aconsejable hacer uso de las identidades virtuales ficticias o híbridas.

- Confiability de la RSV solicitada. Los usuarios, antes de completar el proceso de alta en una RSV deberían realizar un pequeño estudio de la citada RSV. Este estudio debería centrarse en recabar la opinión de conocidos y/o expertos que hagan uso de la citada RSV así como la lectura de las políticas de privacidad y las condiciones de uso. En el caso particular de las RSV basadas en perfiles, se constata que son el formato de RSV que gestionan identidades virtuales más extensas, debido a que son el formato que solicita a sus usuarios mayor número de datos. Es por ello, que este formato de RSV, de una manera especial, debe informar a sus usuarios de todos los procesos en los que se manejen los datos de su identidad virtual (alta, navegación, baja), así como de las consecuencias de un manejo inapropiado de los mismos.

Los usuarios de las RSV están expuestos a un conjunto de amenazas y riesgos que, en mayor o menor medida, pueden afectar a su privacidad. En la actualidad, las RSV basadas en perfiles son la tipología de RSV que exponen a sus usuarios a un mayor número de amenazas y riesgos. Esto se debe, fundamentalmente, a que se trata de la tipología que solicita y maneja mayor cantidad de datos de carácter personal. Acciones tan cotidianas, dentro de una RSV, como publicar datos de carácter personal, enviar mensajes privados, publicar fotos, etiquetar amigos, descargar aplicaciones, etc. llevan asociados un conjunto de amenazas y riesgos contra la privacidad. Algunos de los principales factores de riesgo para la privacidad de los usuarios de las RSV son:

1. La falta de concienciación de los usuarios de las RSV en las buenas prácticas en materia de privacidad. La gran mayoría de los usuarios confían en que su navegación a través de la RSV sea segura y exenta de todo riesgo. Esto se debe, fundamentalmente, a una falta de concienciación y educación en el correcto uso de las RSV, e Internet en general. La falta de concienciación no es solo un problema que puede comprometer la privacidad de los usuarios de las RSV, sino que puede comprometer la credibilidad de la RSV y su futura expansión. Por tanto, es tarea de los responsables de las RSV realizar una campaña de concienciación del futuro usuario durante el proceso del alta en la RSV, así como la de planificar un plan de formación continua durante todo el ciclo de vida del usuario en la RSV.
2. Falta de procedimientos y mecanismos de securización. Las RSV deben de funcionar sobre plataformas informáticas seguras que garanticen la salvaguarda de la privacidad de los usuarios que la utilizan. Del mismo modo, deben ponerse a disposición de los usuarios aquellas informaciones relacionadas con los mecanismos de seguridad de la RSV, así como cuáles son los procedimientos que permitan a los usuarios conocer sus derechos y ejercerlos en los momentos que consideren oportuno
3. Uso inadecuado de los datos de los usuarios por terceros. Es práctica común que las RSV suscriban con terceros (empresas de publicidad, marketing, etc.) acuerdos comerciales y/o de cesión de datos de los usuarios de la RSV sin el consentimiento informado del interesado. Estos acuerdos, en múltiples ocasiones, derivan en un uso incorrecto de los datos de los usuarios de las

RSV, pudiendo exponer al usuario en una situación de riesgo al desvelar información sensible del mismo, que en muchos casos excede la finalidad del marco de cesión de datos. Las RSV están obligadas a informar a sus usuarios sobre el uso que hará de los datos personales que aportan y/o publican en la RSV. Esta información debe ser aportada por la RSV en el proceso de alta del usuario y aceptada por él mismo antes de hacer uso de cualquier servicio proporcionado por la Red Social Virtual.

4. *Suplantación de identidad de los usuarios.* Las RSV permiten a los usuarios confeccionar su identidad digital. La falta de control en el registro de usuarios en la RSV permite suplantar la identidad de un usuario de manera sencilla, es decir, adoptar una identidad virtual ficticia a partir de la identidad real de un tercero. El principal riesgo de la suplantación de identidad son los daños irreparables a la privacidad del usuario suplantado. Hoy en día no existen mecanismos eficientes para evitar la suplantación de identidad, aunque las grandes RSV están trabajando en complejos sistemas de identificación que disminuyan el número de incidencias.

Las RSV deben salvaguardar y garantizar a sus usuarios el ejercicio de sus derechos al honor, vida personal y familiar y a la propia imagen. Los citados derechos consisten esencialmente en lo siguiente:

- ✓ *El derecho al honor* es aquel derecho a la protección de la imagen pública de una persona, de la consideración social en la que es tenido, de su nombre y su reputación, de tal forma que el resto de individuos lo respeten. Dicha protección, como excepción a lo usual en los derechos de la personalidad, se extiende más allá del fallecimiento por medio de acciones concedidas por el Ordenamiento a sus causahabientes.
- ✓ *El derecho a la propia imagen* atribuye al individuo la capacidad de ejercer un control sobre la captación, grabación, uso y difusión de su imagen, entendida como representación gráfica de la figura humana, y también de su voz.
- ✓ *El derecho a la intimidad* se entendió inicialmente por doctrina y jurisprudencia como un bien ordenado a la protección de lo más interno y reservado de las personas. Posteriormente la jurisprudencia y la evolución social han definido un derecho a la intimidad de contenido amplio y textura abierta, cuyas manifestaciones son múltiples.
- ✓ *La protección de datos personales.* El derecho a la protección de datos alcanza a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales. El que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima del usuario, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que, en determinadas circunstancias, constituya una amenaza para el individuo.

- ✓ Protección de consumidores y usuarios. La proliferación de RSV está modificando las prácticas comerciales. Este hecho se debe, en gran medida, a que los usuarios de las RSV son clientes potenciales de toda empresa, grande o PYME, que realice campañas de marketing o publicidad a través de las RSV. Comienza a ser una práctica común entre las grandes corporaciones, y cada vez más entre las PYMES, que destinen parte de su presupuesto de marketing y/o publicidad a campañas que usan a las RSV como plataforma. Este nuevo modelo, sin duda, es beneficioso para las empresas y usuarios ya que permiten realizar transacciones comerciales de manera más rápida y sencilla. Pero como ocurre siempre, todo beneficio tiene su riesgo, y en el caso de las transacciones comerciales se centran en la inseguridad de las transacciones electrónicas a través de la red, la validez de contratos, el derecho de los usuarios o la jurisdicción en caso de litigios.
- ✓ Protección de la propiedad intelectual. Otro de los grandes retos de la Sociedad de la Información es controlar el derecho a la propiedad intelectual de los contenidos que se intercambian a través de Internet. Con las premisas de que el autor es la persona física o jurídica que crea una obra, la propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el sólo hecho de su creación, los derechos de propiedad intelectual se componen tanto de derechos personales, como de los derechos de explotación sobre la obra y son consideradas obras de propiedad intelectual las obras literarias, artísticas o científicas, podemos concluir que la protección compromete, tanto a los derechos morales como patrimoniales. Los Derechos morales son derechos inherentes a la persona física y, por tanto, irrenunciables, encontrándose entre ellos la "paternidad" de la obra, la integridad de la misma, la decisión sobre su difusión y el reconocimiento de su autoría y los derechos patrimoniales son derechos cuantificables económicamente y que pueden ser dispuestos por los sujetos titulares (personas físicas y jurídicas). Estos derechos son los relativos a las actividades de reproducción, distribución, comunicación pública y transformación.
- ✓ La protección de los Menores. Los menores de edad conforman el segmento de usuario, de las RSV, más vulnerable. Los menores de edad son el segmento de la población que en mayor proporción hace uso de Internet y sus servicios. La curiosidad y falta de madurez son dos de los factores, que sin duda, provocan que los menores de edad estén expuestos a mayores riesgos que el resto de usuarios en el uso de Internet. La concienciación y educación de los menores permitirá minimizar los riesgos a los que se pueden ver expuestos cuando navegan por Internet, y en especial, cuando hacen uso de las RSV. El papel de los padres o tutores en la educación de los menores respecto al correcto uso de Internet es vital, pero, en muchas ocasiones, estos padres o tutores no disponen de la formación mínima necesaria para llevar a cabo esta tarea.

En la actualidad, hay vigentes una gran cantidad de legislaciones nacionales e internacionales relativas a la protección de datos. A pesar de esta diversidad, todas ellas tienen un conjunto de principios comunes. Estos son:

- i. Principio de calidad de los datos. Los datos que se recaben deben ser pertinentes, adecuados y no excesivos para la finalidad para la que son

recogidos. Las RSV, en la mayoría de los casos, vulneran este principio al no ser capaces de delimitar los límites de este principio.

- ii. Consentimiento previo e informado a los usuarios sobre el tratamiento de los datos y su cesión a terceros. Los usuarios de las RSV deben ser informados de la finalidad de la recogida de sus datos de carácter personal, así como el uso y posibles cesiones a terceros que se pudiesen llevar a cabo.
- iii. Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Los usuarios deberán tener la capacidad de ejercer sus derechos de acceso, rectificación, cancelación u oposición respecto a sus datos de carácter personal en cualquier momento y mediante medios gratuitos y de fácil acceso.
- iv. Garantía de confidencialidad. Se debe garantizar que los datos de carácter personal de los usuarios deberán ser manejados y gestionados de tal forma que solo sean accesibles por las personas autorizadas por el usuario.
- v. Regulación de la transferencia internacional de datos. Las RSV deben operar desde países confiables y que posean regulaciones en materia de protección de datos internacionalmente aceptadas.
- vi. Securización de los medios automatizados. Los responsables de las RSV deben implementar todas las medidas técnicas y procedimentales con el objetivo de securizar la plataforma en la que reside la RSV.

Tabla 1 – Resumen de riesgos, ambitos y principios de Protección de una RSV.

Riesgos	Ambitos de proteccion	Principios
✓ Falta de concienciación	✓ Derecho al honor	✓ Calidad de los datos
✓ Falta de mecanismos y procedimientos de securización	✓ Derecho a la propia imagen	✓ Consentimiento sobre el uso de datos
✓ Uso inadecuado de datos por terceros	✓ Derecho a la intimidad	✓ Derechos ARCO
✓ Suplantación de identidad	✓ Protección de datos personales	✓ Garantía de confidencialidad
	✓ Protección de consumidores	✓ Regulación de transferencia internacional de datos
	✓ Protección de la propiedad intelectual	✓ Securización de medios
	✓ Protección de menores	

4. Procesos de Gestión de la Privacidad

Para la gestión de la privacidad de una red social virtual (RSV), las fases más críticas son el proceso de alta del usuario en la RSV, el uso de determinados servicios de la RSV y el proceso de baja de los usuarios de la RSV:

- En el proceso de alta en la RSV los usuarios facilitan una cantidad importante de datos de carácter personal. En la mayoría de las ocasiones los datos son excesivos para la finalidad de su uso por parte de la RSV y, por tanto, en la mayoría de las ocasiones exponemos nuestra privacidad.
- La utilización de servicios que permiten la publicación de fotos, chatear con el resto de usuarios, enviar mensajes privados, etc. pueden comprometer la privacidad de los usuarios de la RSV, así como la de terceros, ya sean usuarios de la RSV o no.
- El proceso de baja de usuarios de la RSV es el último momento crítico, debido, fundamentalmente, a que la mayoría de las RSV no realizan un borrado efectivo de los datos facilitados por los usuarios a lo largo de su ciclo de vida en la RSV.

Los cinco procesos principales relacionados con la gestión de la privacidad en una red social virtual son:

1. La gestión de usuarios de la RSV. Este proceso incluye todas las actividades relacionadas con la gestión de usuarios de la RSV: el alta out-site e in-site de los usuarios, la gestión de los accesos a la RSV, la modificación de los datos de usuario, las diferentes modalidades de baja de usuarios, como la baja voluntaria, la baja tras la no confirmación en el proceso de alta, out-site, la baja promovida por los gestores de la RSV, las notificaciones de gestión de la RSV o las comunicaciones de tipo comercial.
2. La protección de los derechos de usuarios de la RSV. En este proceso se incluye la protección de los derechos ARCO, los procesos relacionados con la Agencia de Protección de Datos en España e incluidos en la Ley de Protección de Datos (LOPD), el movimiento internacional de los datos, la protección del derecho, el honor y la intimidad de los usuarios de la RSV, la propiedad intelectual y el derecho de los consumidores, los mecanismos de denuncia, el secreto de las comunicaciones y las herramientas de auto inspección.
3. La navegación de los usuarios en la RSV. El proceso de navegación abarca aspectos como la gestión de las sesiones de usuarios, los idiomas, el alta, modificación y borrado de contenidos de texto y multimedia y la gestión del almacenamiento de esta información.
4. La formación de los usuarios de la RSV. La formación tiene como objetivo la concienciación y la guía de los usuarios en el uso de la RSV. Este proceso incluye la segmentación de los tipos de usuarios en base a su grado de conocimiento técnico y de uso, la gestión de contenidos de tipo formativo, los planes de formación, los cursos y las notificaciones legales y técnicas en la RSV.
5. La seguridad de la plataforma de la RSV. La seguridad de la plataforma tecnológica sobre la que se soporta la RSV es el pilar básico sobre el que debe

sustentarse una RSV. Este proceso incluye multitud de aspectos tanto de seguridad lógica, de seguridad física, de continuidad como de procedimientos y técnicas de seguridad. También se incluyen todos los procesos relacionados con la auditoría de la plataforma y la organización responsable de su explotación y gestión.

5. Modelos y herramientas de evaluación

A continuación se muestran algunos modelos y herramientas que pueden dar soporte a la evaluación de la privacidad en una red social virtual.

5.1. El modelo de madurez

El primer modelo de madurez nace de las investigaciones realizadas en la década de los 80 por el Instituto de Ingeniería del Software de la Universidad Carnegie Mellon, junto con la MITRE Corporation, para la mejora del proceso de diseño y desarrollo del software. Fruto de estas investigaciones se desarrolla un marco de trabajo que se denominó Proceso de Madurez. Este marco de trabajo está relacionado con el concepto de la administración de la Calidad Total, TQM, (Ashley Rawlins, R. (2008)), y contaba con cinco niveles y una implementación de prácticas de calidad bien definidas.

Se puede considerar que el primero modelo de madurez fue una aplicación de TQM para el desarrollo de software. Pero no es hasta 1989 cuando se publica el libro titulado "*Managing the Software Process*", S. Humphrey, W (1989). En esta obra ya encontramos un marco de trabajo definido por cinco niveles de madurez. Este libro se puede considerar el primer modelo de madurez de la industria. Desde 1987 hasta 1997 este modelo ha ido evolucionando, pasando por las versiones 1.1., Beth Chrissis, M. et al. (2003), y 1.2., M. Ahern, D. et al (2008).

Además de este modelo, identificado como CMM, existen otros modelos de madurez ya consolidados en la industria, como por ejemplo, el Modelo de Madurez de la gestión de proyectos, portfolios y programas (P3M3), S. Bonham, S. (2008), de la Oficina de Comercio del Gobierno Británico (OGC), o el Modelo de Madurez de la Seguridad (SS-CMM), Abhijit Belapurkar A. et al. (2009).

En lo que se refiere a la gestión de la privacidad en redes sociales virtuales tenemos el modelo de madurez en materia de privacidad de una red social virtual, J.R. Coz and E. Fojón (2010), que está compuesto por una serie de componentes:

1. El análisis de las RSV. Incluye un estudio en profundidad del concepto de red social virtual. Este estudio incluye las diferentes tipologías de las RSV, se presentan los diferentes formatos en que se presentan las RSV, se analiza el concepto de "*identidad virtual*", la "*cadena de valor*" de las RSV y se ponen de manifiesto los principales riesgos a los que están expuestas estas redes. Por último, se realiza un resumen del "*modelo de negocio*" que las sustenta y se obtienen una serie de conclusiones sobre el futuro de este modelo.
2. Estudio de Privacidad. Este modelo de madurez detalla los diferentes ámbitos de protección de las RSV y para cada uno de estos ámbitos, se describen los

principios comunes, los riesgos a los que están sometidos y las medidas de protección, de carácter general, que pueden ser acometidas.

3. Resumen Ejecutivo. El resumen ejecutivo contiene los antecedentes y conceptos necesarios para entender el modelo, su estructura, los objetivos y beneficios que aporta el modelo y se organizan todos los Procesos de Gestión de la Privacidad y los Niveles de Madurez.
4. Modelo de Madurez, Procesos y Niveles. El Modelo está compuesto por cinco Niveles de Madurez (inicial, repetible, definido, gestionado y optimizado), cada uno de ellos se organiza en varios *procesos y subprocesos de gestión de la privacidad*. A su vez, cada subproceso contiene una serie de *áreas clave de procesos* y cada área se mide en *prácticas clave*. Además, cada Área Clave del Proceso, que puede ser evaluada por las diferentes Prácticas Clave, tiene una correspondencia con una serie de requisitos que deben de cumplirse. En total, hay 214 requisitos en todo el Modelo, que se encuentran organizados por Áreas Clave.

5.2. El framework de evaluación

El framework de evaluación complementa el modelo de madurez y permite normalizar el diagnóstico de cumplimiento del modelo en una organización responsable de la gestión de una RSV, J.R. Coz and E. Fojón (2010). Este framework hace uso de un “*cubo de gestión*”. Las dimensiones de este cubo representan todos los aspectos de gestión del framework. La primera dimensión del Framework de Evaluación son los Condicionantes (o requisitos previos) y los Objetivos. Existen una serie de condicionantes relativos a la Planificación, a la recogida de información, a las prácticas organizacionales, al equipo de trabajo, a la validación y a los informes de evaluación.

Estos condicionantes incluyen una serie de requisitos que deben de cumplirse con carácter previo al desarrollo de la evaluación. La segunda dimensión del cubo son los recursos, incluyendo roles y herramientas de evaluación, y las características de los informes de evaluación. Por último, la tercera de las dimensiones es el método de evaluación.

A continuación, en la figura 1, se muestra un gráfico muy resumido del método de evaluación que comienza con una primera fase de preparación, que incluye la planificación inicial y la recogida de datos, continua con una segunda fase de actividades sobre el terreno, que incluye una auditoria, entrevistas y análisis de datos y finaliza con la tercera y última fase de entrega de resultados, que incluye un informe final de la evaluación con las conclusiones y recomendaciones. Este informe final, describe el nivel de madurez en el que se ubica la organización y contiene recomendaciones para lograr alcanzar el siguiente nivel de madurez.

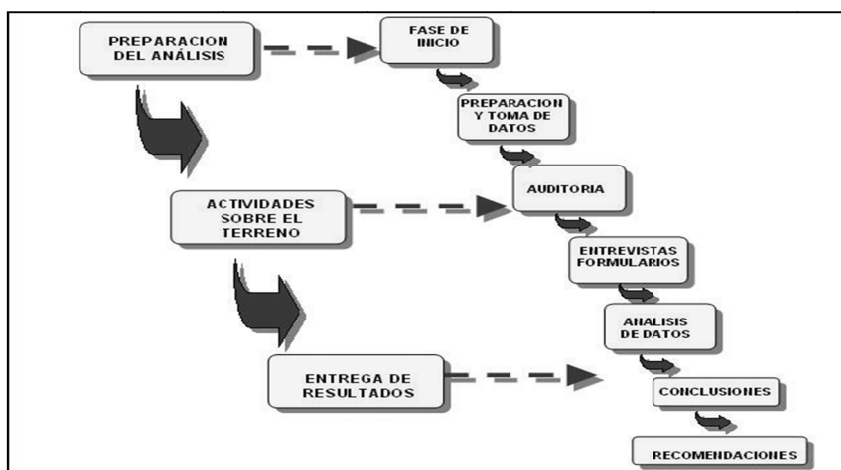


Figura 1 – Método de evaluación de la privacidad de una red social virtual.

5.3. Un Cuadro Integral de Mandos

El Cuadro Integral de Mandos (CIM) es un sistema de gestión propuesto por S. Kaplan, R. and P. Norton, D. (1996) y que va más allá de la perspectiva financiera con la que los gerentes evaluaban la marcha de una empresa u organización. Este sistema permite que veamos a la organización desde cuatro perspectivas: el desarrollo y aprendizaje, el cliente, la financiera y la interna del negocio. Tomando como referencia este concepto se ha desarrollado un CIM que da soporte a la realización de una auditoría de evaluación del modelo de madurez en materia de privacidad de una red social virtual, J. R. Coz et al. (2010). Este CIM propone esta evaluación desde las cuatro perspectivas:

1. Perspectiva de Desarrollo y Aprendizaje. Incluye todas aquellas prácticas clave y requisitos que se engloban dentro de la formación: la estrategia de la formación de los usuarios de la RSV, la segmentación de la formación, los contenidos de los cursos, los mecanismos de formación, el mantenimiento de las materias de formación, el plan de formación, los cursos de iniciación y la formación continua.
2. Perspectiva del Cliente. El rol del cliente lo asume el usuario de la RSV. La perspectiva del cliente incluye la gestión de los usuarios de la RSV (todos los procesos relacionados con las altas, modificaciones y bajas de usuarios) y la gestión de los derechos, que engloba: los procesos de gestión del derecho a la protección de datos de carácter personal, del derecho al honor, la intimidad personal y familiar y la propia imagen, del tratamiento para usos comerciales, del movimiento internacional de datos y de la propiedad intelectual.
3. Perspectiva Interna del Negocio. La perspectiva interna del negocio abarca todos los procesos relacionados con la gestión de la seguridad de la plataforma que da soporte a la RSV, incluyendo aspectos de seguridad lógica, como el control de accesos, la continuidad del servicio (copias de seguridad, recuperación, etc.), la gestión de incidencias, el cifrado de las comunicaciones,

el hacking ético, la gestión de cookies y web beacons, los permisos sobre el contenido publicado, la seguridad física y las auditorías.

4. Perspectiva Financiera. Incluye todas las cuestiones relacionadas con el comercio electrónico y las plataformas de pago de las RSV, en el caso de que incluyan este tipo de servicios.

La herramienta nos permite garantizar el cumplimiento de los requisitos expuestos en el Modelo de Madurez y en el Framework de Evaluación de la Madurez.

6. Conclusiones

En este artículo se analiza el concepto de red social virtual y los aspectos más relevantes relacionados con la gestión de la privacidad de la información, un asunto muy crítico y que constituye uno de los elementos básicos en la protección de la seguridad del ciberespacio.

En el presente artículo se han expuesto los principios y ámbitos de protección en las redes sociales virtuales y los principales procesos de gestión de la privacidad de la información. Además, en el artículo se describen varias propuestas para evaluar la gestión de la privacidad en las redes sociales virtuales como un modelo de madurez, que permite clasificar las redes en base a su nivel de protección, un marco de evaluación, que normaliza el proceso de evaluación de la privacidad y una herramienta en forma de cuadro integral de mandos, que da soporte a una auditoría de evaluación.

Todas estas propuestas ofrecen un marco de referencia sobre la privacidad de la información en las redes sociales virtuales que puede sentar las bases de una futura normalización en esta materia.

Glosario

- **Usuario:** persona física titular de los datos.
- **Bloqueo de datos:** la identificación y reserva de los datos con el fin de impedir su tratamiento.
- **Comunicación o cesión de datos:** toda revelación de datos realizada a una persona distinta del interesado o usuario.
- **Consentimiento del interesado:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- **Datos de carácter personal:** información concerniente a una persona física, que identifican la misma o permiten la identificación.
- **Fichero:** conjunto organizado de datos. Puede ser una base de datos estructurada, una hoja de cálculo o un documento electrónico cuyo el contenido sean datos de carácter personal.
- **Identificación del afectado:** cualquier elemento que permita determinar

directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona afectada.

- **Disociación:** todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
- **Transferencia de datos:** el transporte de los datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.
- **Tratamiento de datos:** operaciones y procedimientos técnicos de carácter automatizado o no, que permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Referencias bibliográficas

- Abhijit Belapurkar A. et al. (2009) *“Distributed Systems Security: Issues, Processes and Solutions”*. John Wiley and Sons, 2009.
- Adrienne Felt and David Evans (2008) *“Privacy Protection for Social Networking Platforms. Workshop on Web 2.0 Security and Privacy”*. Oakland, CA. 22 May 2008.
- Alexa. (2012) *“Alexa Top 500 Global Sites”*. Retrieved March 2012, from <http://www.alexacom/topsites>.
- Ashley Rawlins, R. (2008) *“Total Quality Management (TQM)”*. ISBN 1434372987, 9781434372987. AuthorHouse, 2008.
- Beth Chrissis, M. et al. (2003) *“CMMI: guidelines for process integration and product improvement”*. ISBN 0321154967, 9780321154965. Addison-Wesley, 2003.
- Diogo T. & Isabel A. (2011) *“Análise de opiniões expressas nas redes sociais”*. RISTI, Edición N.º 8, 12/2011.
- Durán Torres, K. (2010) *“Las Redes Sociales como estrategia competitiva para las PYMES: Caso de estudio empresas registradas en el Sistema Universitario de Mejora Empresarial (SUME)”*. Tesis presentada a la Facultad de Contaduría y Administración de la Universidad Veracruzana, Región Xalapa.
- Fritz Machlup (1962) *“The production and distribution of knowledge in the United States”*. Princeton University Press, 1962. ISBN 9780691003566.
- González Gálvez, P y Rey Martín, C. (2009) *“Redes sociales como fuente de capital social: una reflexión sobre la utilidad de los vínculos débiles”*. RISTI. Edición nº 3, 06/2009. ISSN: 1646-9895
- J. R. Coz et al. (2010) *“Cuadro Integral de Mandos como soporte al proceso de Evaluación de la Madurez de una Red Social Virtual en materia de Privacidad”*.

- V International Congress on IT Governance and Service Management: Proposals for Tough Economic Times. Alcalá de Henares, Junio 2010.
- J.R. Coz and E. Fojón (2010) "*Modelo de madurez para la privacidad de una red social virtual*". ISBN 1445720175, 9781445720173. Lulu Enterprises Inc., 2010.
- Java, A. et al (2007) "*Why We Twitter: Understanding Microblogging Usage and Communities*". Proceedings of the Joint 9th WEBKDD and 1st SNA-KDD Workshop 2007. San Jose, California , USA.
- Ku, L., Ke, K., & Chen, H. (2009) "*Opinion Analysis on CAW2.0 Datasets. Paper presented at the Content Analysis in Web 2.0*". Workshop, 21st April 2009, Madrid, Spain.
- Larissa A. (2002) "*Redes sociales y partidos políticos en Chile*". REDES- Revista hispana para el análisis de redes sociales". Vol.3,#2, sept-nov. 2002.
- Lozares, C. (1996) "*La teoría de redes sociales*". Papers, nº 48, pp. 103-126
- M. Ahern, D. et al (2008) "*CMMI Distilled: A Practical Introduction to Integrated Process Improvement*". ISBN 9780321461087. Addison-Wesley, 2008.
- Milgram S. (1967) "*The small world problem*". Psychology Today. 1967;1:61-7.
- Miralles, F. (1998) "*El saber de les organitzacions. Sistemes d'informació. Reptes per a les organitzacions*". Barcelona: Columna edicions, Edicions Proa. Pp 41-60.
- O'Connor, B. et al (2010) "*From Tweets to Polls: Linking Text Sentiment to Public Opinion Time Series*". The International AAAI Conference on Weblogs and Social Media, Washington DC.
- Quan Haase, A. et al. (2002) "*Capitalizing on the Net: Social Contact, Civic Engagement and Sense of Comunita*". In Barry Wellman and Carolyne Haythornthwaite (Eds.). The Internet in everyday life. Maryland: Blackwell Publishing.
- S. Bonham, S. (2008) "*Actionable Strategies Through Integrated Performance, Process, Project, and Risk Management*". ISBN 1596931191, 9781596931190. Artech House, 2008.
- S. Humphrey, W (1989) "*Managing the Software Process*". ISBN 0201180952, 9780201180954. Addison-Wesley, 1989.
- S. Kaplan, R. and P. Norton, D. (1996) "*The balanced scorecard: translating strategy into action*". ISBN 0875846513, 9780875846514. Harvard Business Press, 1996.
- Tapscot, D. y Williams, A. D. (2007) "*Wikinomics. la nueva economía de las multitudes inteligentes*". Barcelona: Ediciones Paidós.
- Van Bavel, R. et al. (2004) "*ICTs and Social Capital in the knowledge society*". Institute for prospective technological studies". Technical Report EUR 21064 EN.
- Vázquez Barquero, A. (1999) "*La Teoría del Desarrollo Endógeno*", Madrid: Pirámide.

Recolha, preservação e contextualização de objectos digitais para dispositivos móveis com *Android*

Raquel Soares ¹, Marco Pereira ¹, Joaquim Arnaldo Martins ¹

raquel.soares@ua.pt, marcopereira@ua.pt, jam@ua.pt

¹ DETI - Departamento de Electrónica, Telecomunicações e Informática,
IEETA - Instituto de Engenharia Electrónica e Telemática de Aveiro,
Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal.

DOI: 10.4304/risti.9.75-89

Resumo

Motivação: Com a crescente expansão e utilização de dispositivos móveis, emergiu rapidamente a necessidade de recolha e preservação de objectos digitais. Cada vez mais, é importante tornar a nossa informação persistente e acessível em qualquer momento e em qualquer lugar. E se, para além do acesso, existisse a possibilidade de contextualizar cada objecto digital? Desta forma, o utilizador poderia relembrar a origem e fundamento dos respectivos dados ao longo de toda a sua vida.

Resultados: A aplicação CoBy surge com o intuito de permitir ao utilizador recolher, preservar e contextualizar todos os objectos digitais que vão surgindo no seu dispositivo móvel com sistema operativo *Android*. A cada um deles vai sendo associada a respectiva geo-localização de onde ocorreram. Estão disponíveis também funcionalidades de *backup* e *restore* a partir do próprio dispositivo móvel ou da *Cloud*. Esta aplicação dará um forte contributo no que toca à preservação e contextualização do património digital pessoal.

Palavras-chave: Objecto digital; Contexto; Preservação digital; Geo-localização; Dispositivo móvel.

Abstract

Motivation: The increasing use and growth of mobile devices, spurred the need to collect and preserve digital objects. More and more, it is important ensure that our information becomes persistent and accessible anytime and anywhere. What if, besides access, there was the possibility of contextualize each digital object? If so, the user could recall how, what and why it stored that data, throughout their lives.

Results: The CoBy application was created in order to allow the user collect, preserve and contextualize all digital objects that will appear in mobile devices with Android as operating system. Each of them will be associated with place where they occurred (geo-location). The application includes other features, such as backup and restore from the mobile device or from the Cloud. This application

provides a strong contribute to the preservation and contextualization of a person's digital heritage.

Keywords: Digital object; Context; Digital preservation; Geo-location; Mobile device.

1. Introdução

A existência de objectos digitais no nosso dia-a-dia tem tido, ao longo dos últimos anos, um enorme crescimento. Estes podem ser concebidos como artefactos compostos tendo em conta três elementos essenciais: conteúdo, metadados e a sua relação com outros objectos (Saidis & Delis, 2007). Os objectos digitais podem assumir os mais variados tipos, retratando grande parte da nossa vida pessoal e profissional, e representam toda informação digital presente em dispositivos electrónicos como: computadores, telemóveis, *smartphones*, *tablets*, entre outros. Esta informação digital é extremamente importante, para as pessoas que utilizam estes dispositivos, e ao mesmo tempo muito delicada e frágil. Se não tomarmos as devidas precauções, a qualquer momento pode-se perdê-la, e em alguns casos nada se pode fazer para contrariar a situação. É extremamente importante permitir aos detentores (utilizadores) de objectos digitais formas de os preservar. Assim, o utilizador consegue não só manter todas as suas memórias de sempre e para sempre, mas também dar o seu contributo para a passagem de conhecimento de geração em geração. É humanamente impossível recordar todos os acontecimentos que vão emergindo ao longo da vida, e como “Sem memórias não há história”(da Costa, 2007), é crucial investir afincadamente nesta área. Com a sociedade maioritariamente digital em que vivemos hoje em dia, e a avançar a passos largos para se tornar inteiramente digital, é gritante a necessidade de preservar todo o material digital que dispomos, caso contrário, torna-se um pedaço da nossa história pessoal e universal que se perde.

Da necessidade de evitar a perda de informação digital surgiram os repositórios digitais (Heery & Anderson, 2005). Neles é possível armazenar colecções de objectos digitais, e que podem ser acedidos e recuperados para utilização imediata ou posterior. Um repositório digital suporta mecanismos de importação, exportação, identificação e armazenamento de objectos digitais. Para além disso, um repositório digital oferece ao utilizador uma interface permitindo-lhe aceder ao conteúdo que pretende. O uso de repositórios digitais traz benefícios a todos, até mesmo ao meio ambiente, evitando o consumo de alguns recursos naturais que tendem a escassear. A utilização vigorosa de repositórios digitais poderia contribuir para o atenuar deste problema, diminuindo a necessidade dos utilizadores preservarem os seus dados/conhecimentos em papel.

A necessidade de preservar a informação digital inerente à flexibilidade de armazenamento de qualquer tipo de objecto digital despoletou o aparecimento dos repositórios digitais pessoais. Estes permitem ao utilizador guardar os seus objectos digitais garantindo-lhe alguma capacidade de armazenamento e um controlo de acesso bastante prudente. Um utilizador quando recorre a este tipo de serviço pretende armazenar os seus dados para consulta e utilização a curto e longo prazo. Os repositórios digitais pessoais permitem a preservação controlada e persistente do nosso material digital, possibilitando o seu acesso em qualquer momento e em qualquer

lugar, por quem de direito. A segurança dos dados é inteiramente assegurada, dado que só terão acesso as pessoas que o utilizador permitir e os conteúdos que este definir.

Tendo a preservação dos nossos objectos digitais assegurada, levanta-se a questão: Será que conseguimos lembrar o seu contexto? O contexto, também designado como *Context Awareness* na literatura (Mehra, 2012), (Abowd, Ebling, Hung, Lei, & Gellersen, 2002), (Dey, 2001), (Pascoe, 1998), pode ser visto como uma análise ao contexto pessoal, social, histórico, físico, ambiental, posicional, etc., de um objecto digital. Resumidamente, o contexto de um objecto digital é tudo aquilo que fomenta o seu surgimento, a forma como é usado e interpretado, a que propósito foi concebido, o que influenciou a sua criação, local do evento, a sua relação com os outros objectos, entre outros. Segundo Arellano (Arellano, 2004) uma aplicação cuja finalidade recaia sobre a preservação de informação deve ter sempre presente o seu conteúdo, estrutura e contexto. É muito útil termos os nossos dados preservados, mas também é indispensável saber o seu contexto, para ao longo dos anos ser possível fazer a reconstrução da imagem mental do objecto digital.

Tal como é ilustrado na Figura 10, este projecto tem como principal objectivo recolher alguns objectos digitais e guardá-los num repositório digital pessoal presente na *Cloud*. Esta recolha é efectuada num dispositivo móvel com sistema operativo *Android*. Sempre que possível, é adicionada alguma informação que permita contextualizar cada objecto digital. É possível colocar no repositório os mais variados tipos de informação, como por exemplo: SMSs, contactos, histórico de chamadas, *bookmarks*, imagens, *emails*, páginas *Web* visitadas, lista de compromissos, entre muitos outros. Todo o material digital é preservado e sempre que o utilizador pretender tem total acesso a ele, independentemente do sítio, do tempo, do sistema operativo e do dispositivo de acesso. Existe ainda a liberdade de poder partilhar os seus conteúdos digitais com amigos, usando para isso as redes sociais (*Facebook*, *YouTube*, *Flickr*, *Linkedin*, entre outros), ou simplesmente permitir o acesso de determinada pessoa ao seu repositório digital pessoal.

Este projecto engloba diversas áreas de desenvolvimento, exigindo a integração de tecnologias bastante distintas. No entanto, a área móvel merece especial atenção, devido ao seu elevado crescimento e actual impacto na sociedade. Desta forma, este trabalho é desenvolvido a pensar nas pessoas e nos seus interesses, sendo que os dispositivos móveis contêm uma grande quantidade de informações pessoais altamente sensíveis. Então, neste contexto, deve-se desenvolver uma aplicação que tenha em conta esta delicadeza e ajude a preservar os conteúdos presentes nos dispositivos móveis. A aplicação CoBy (*Contextualized Backup and Restore*) foi desenvolvida para recolher alguns dos objectos digitais presentes em dispositivos móveis *Android* (*smartphone* ou *tablet*), contextualizá-los, e enviá-los para o repositório digital pessoal, tal como é exposto na Figura 11. Neste caso específico, e numa abordagem inicial, para além do contexto a que um objecto digital está sujeito, adicionou-se o contexto de geo-localização. A informação digital é guardada numa base de dados local (*backup*) no cartão de memória do dispositivo móvel e/ou enviada para o repositório, já devidamente contextualizada. Também é dada a possibilidade de restaurar (*restore*) os dados do repositório ou do cartão de memória de volta para o dispositivo móvel (Ottaviani, Lentini, Grillo, Di Cesare, & Italiano, 2011). Esta funcionalidade é extremamente importante caso haja uma mudança ou furto do *smartphone* ou *tablet*.

Desta forma, o utilizador pode voltar a ter todo o seu conteúdo digital de volta no dispositivo móvel. O repositório digital pessoal disponibiliza ainda, ao utilizador uma interface (página *Web*) para visualização do seu conteúdo. Este pode ser visto sobre a forma de *timeline* temporal, tendo capacidade de filtragem de informação usando alguns parâmetros, como por exemplo a geo-localização.



Figura 10 – Visualização e recolha de informação digital do utilizador.

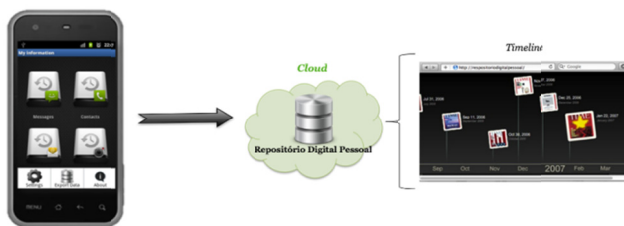


Figura 11 – Esquema ilustrativo da área móvel do projecto.

Desenvolveu-se a aplicação direccionada para dispositivos móveis com *Android*. Esta escolha deveu-se ao facto deste sistema operativo estar neste momento com a maior cota de mercado mundial (Gartner, 2012). E prevê-se que esse crescimento se acentue ainda mais (Darwin, 2012).

2. Trabalho relacionado

Ao longo da história o homem foi desenvolvendo formas de preservar a sua informação, recorrendo a pinturas, fotografias, manuscritos, livros, entre muitas outras coisas. Mas, devido à evolução da tecnologia, foi surgindo outro tipo de informação, que contribuiu para a sociedade da informação em que se vive actualmente, amplamente rodeada de conhecimento digital. Foi igualmente necessário o desenvolvimento de ferramentas de salvaguarda deste tipo de dados. Na área móvel esta preocupação torna-se acrescida devido à elevada vulnerabilidade dos seus objectos digitais. A pensar nesta questão, inúmeras aplicações foram desenvolvidas.

O sistema operativo *Android* disponibiliza uma aplicação designada *Play Store*, onde é possível obter todas as aplicações disponíveis no *Google Play*, a loja de aplicações do *Android*. Foi efectuada uma pesquisa usando a *Play Store* de um dispositivo móvel em busca de aplicações que permitissem efectuar *backup* e *restore* de dados. O resultado dessa pesquisa está ilustrada na Tabela 1 onde se encontram representadas as mais usadas. À semelhança da aplicação CoBy, todas elas disponibilizam funcionalidades de

backup e *restore* dos dados, à excepção da aplicação *Backup Contacts* que apenas permite fazer *backup*. A ausência da funcionalidade de *restore* torna esta aplicação limitada.

A capacidade de fazer *backups* automáticos é uma funcionalidade muito útil para este tipo de aplicações. Liberta o utilizador da necessidade de o realizar manualmente, que poderia conduzir a alguma perda de informação, caso o utilizador não se recordasse de o fazer com alguma regularidade. Esta funcionalidade está presente na aplicação CoBy, contrariamente ao que acontece por exemplo nas aplicações *Backup Contacts*, *Mobile Backup II* e *Super Backup*. Trata-se de uma funcionalidade que transmite uma maior confiança e segurança ao utilizador.

Analisando as aplicações retratadas na Tabela 1, observa-se a existência de duas abordagens distintas no que toca aos dados alvo. Existem aplicações que centram as suas atenções apenas num tipo específico de dados, como é o caso da *SMS Backup & Restore*, *Call Logs Backup & Restore*, *Backup Contacts*, etc. Assim como existem outras, que à semelhança da aplicação CoBy, são bastante mais abrangentes permitindo simultaneamente o *backup* e *restore* de objectos digitais distintos. Um bom exemplo disso são as aplicações: *SMS Backup +*, *JS Backup*, *Mobile Backup II* e *Backup Master*, etc. A capacidade de fazer *backup* e *restore* de vários objectos digitais, numa só aplicação, confere-lhe uma grande versatilidade, evitando a necessidade do utilizador instalar uma aplicação por cada tipo de dados.

Tabela 1 - Aplicações presentes no Google Play mais usadas para backup e restore (*Aplicações pagas).

Aplicações [Fabricante]	Backup	Backups automáticos	Restore	Destino dos dados	Dados alvo
App Backup & Restore [iNFOLIFE LLC]	■	■	■	Cartão memória	Aplicações
SMS Backup & Restore [RITESH SAHU]	■	■	■	Cartão memória, E-mail	SMS
Titanium Backup # root [Titanium Track] *	■	■	■	Cartão memória	Aplicações, dados associados à aplicação
SMS Backup + [Jan Berkel]	■	■	■	E-mail	SMS, MMS, Histórico chamadas
SMS Backup & Restore [iNFOLIFE LLC]	■	■	■	Cartão memória	SMS
Call logs Backup & Restore [Ritesh Sahu]	■	■	■	Cartão memória	Histórico chamadas
JS Backup [Johospace Co., Ltd.]	■	■	■	Cartão memória, DropBox, SugarSync, GoogleDocs	SMS, Contactos, <i>Bookmarks</i> , Histórico chamadas, Calendário, Aplicações, etc
Backup Contacts [Red Rock AS]	■	■	■	Cartão memória, DropBox, E-mail	Contactos
Mobile backup II [MobileHome Corp.]	■	■	■	Cartão memória	SMS, Contactos, Histórico chamadas, Eventos do calendário
Super Backup - SMS & Contacts [Mobileidea Studio]	■	■	■	Cartão memória	SMS, Contactos, Histórico chamadas
Bookmark Sort & Backup [happydroid]	■	■	■	Cartão memória	<i>Bookmarks</i>
Backup Master [Funny Android Games]	■	■	■	Cartão memória	Aplicações, SMS, MMS, <i>Bookmarks</i> , Histórico chamadas, Alarmes, etc
Backup and Share Backup Solution [Aress Software]	■	■	■	Servidores próprios	Contactos, Fotografias, Vídeos, Músicas, Imagens
MyBackup Pro [Rerware, LLC] *	■	■	■	Servidores próprios, Cartão memória	SMS, MMS, Histórico chamadas, Contactos, Fotografias, <i>Bookmarks</i> , Calendário
SMS BACKUP n2manager [n2manager]	■	■	■	Cartão memória	SMS

Dentro das aplicações estudadas, os dados de *backup* podem ser armazenados em locais distintos, sendo eles o cartão de memória do dispositivo móvel, um repositório pessoal e/ou uma conta de *e-mail*. O local de armazenamento de informação mais comum é o cartão de memória. Mas, se perdermos o dispositivo móvel, ou se houver um

furto do mesmo, o facto de termos um *backup* dos nossos dados no cartão de memória do dispositivo de nada serve, pois a informação perder-se-á. A salvaguarda de dados num repositório pessoal é indispensável e está presente nas aplicações *JS Backup* e *Backup Contacts*. A aplicação *CoBy* oferece um repositório semelhante, mas com funcionalidades acrescidas. Os ficheiros de *backup* são colocados no repositório pessoal não só para efectuar o *restore* posterior, mas também permite ter os dados permanentemente sincronizados. Os dados presentes no dispositivo móvel vão corresponder aos dados que estão armazenados no repositório pessoal. Esta funcionalidade permite que o repositório tenha sempre a versão mais actual do estado do dispositivo móvel. O acesso ao repositório pode ser feito em qualquer altura e em qualquer lugar, por qualquer sistema operativo.

A capacidade de preservar informação é evidente em todas as aplicações da Tabela 1, mas nenhuma delas proporciona ao utilizador a possibilidade de filtrar os dados que pretende conservar. Existem sempre objectos digitais que a sua preservação não é desejada. Esta funcionalidade encontra-se apenas presente na aplicação *CoBy*.

Contrariamente às restantes, a aplicação *CoBy*, permite recolher informações extras relativas ao contexto de um objecto. Para além do contexto comum usado (data, hora, destinatário, etc.), esta aplicação permite recolher o contexto geo-espacial do objecto. Trata-se também de uma característica única desta aplicação.

Naturalmente, todas as aplicações tem os seus pontos fracos e fortes. A aplicação *CoBy* distingue-se positivamente das restantes, sobretudo ao nível da geo-contextualização, filtragem de informação e a preservação da informação num repositório digital pessoal com funcionalidades acrescidas.

3. Modelo e arquitectura

Na Figura 12 está representado o modelo que pode ser usado para a criação de aplicações de recolha, preservação e contextualização de objectos digitais, no qual a aplicação *Coby* representa o seu protótipo.

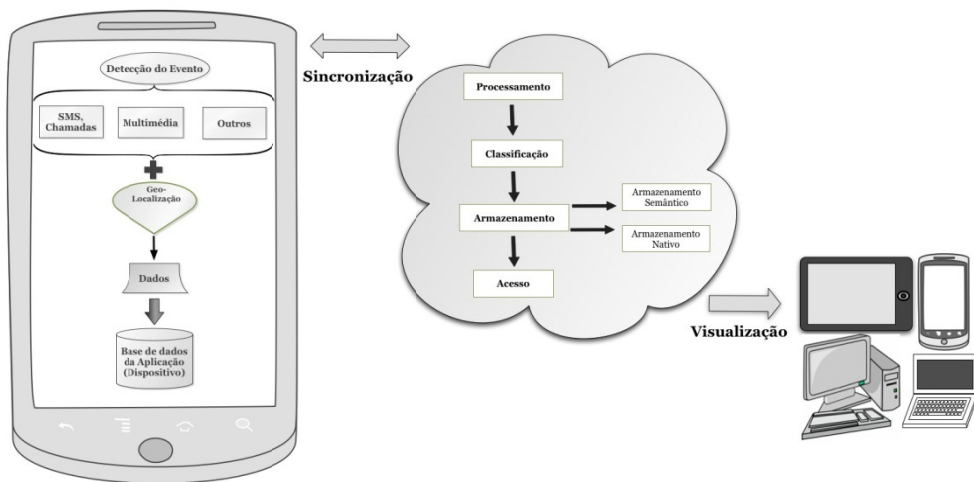


Figura 12 – Modelo genérico de recolha, preservação e contextualização de objectos digitais baseado no modelo OAIS (BOOK, 2002)

A aplicação CoBy tem a capacidade de recolher, preservar e contextualizar, numa fase inicial, objectos digitais do tipo SMSs (*Short Message Service*), chamadas e contactos. O utilizador tem a possibilidade de fazer *backups* automáticos para o cartão de memória (SD card, *Secure Digital Card*) do seu dispositivo móvel ou para o seu repositório digital pessoal presente na *Cloud* (Figura 13). Sempre que o utilizador pretender restaurar as suas SMSs, histórico de chamadas ou contactos de volta no dispositivo, pode fazê-lo não só a partir do *backup* existente no seu cartão SD, como também do repositório digital pessoal. Para o fazer a partir do repositório só precisa de uma ligação à Internet activa. Os dados enviados para o repositório ou guardados no cartão SD já se encontram devidamente contextualizados. Esta aplicação integra funcionalidades como obtenção da localização do utilizador, persistência de dados no dispositivo e consumo de *Web-services*.

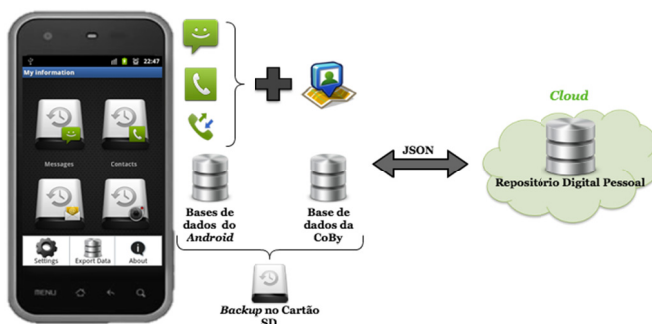


Figura 13 - CoBy (Contextualized Backup and Restore).

Para o sistema operativo *Android* existem algumas tecnologias que dão suporte à geo-

localização, sendo designadas por *Location Providers* (Zhuang, Kim, & Singh, 2010), (Meier, 2010), (Kumar, Qadeer, & Gupta, 2009). Nesta aplicação, a localização pode ser obtida usando três formas distintas: GPS (*Global Positioning System*); *Network Location Provider* (engloba Cell-ID e Wi-Fi); Triangulação por Cell-ID.

GPS (Kaplan & Hegarty, 2006), (Djuknic & Richton, 2001) é um sistema de navegação por satélite que permite fornecer algumas informações a um receptor, nomeadamente a sua posição geográfica. Este representa o método mais preciso de obtenção da localização. Usando *Network Location Provider*, a localização é obtida, não só, através da informação vinda das estações-base da operadora móvel, mas também dos pontos de acesso Wi-Fi aos quais o dispositivo se encontra ligado. Este representa o método mais rápido de obter a localização. O Cell-ID (Trevisani & Vitaletti, 2004) indica a posição da antena à qual o dispositivo se encontra ligado, e trata-se da forma de localização menos precisa.

Um objecto digital por si só já tem agregadas informações de contextualização, como é o caso da data, hora, destinatário, etc. Neste projecto, a contextualização adicional, consiste em associar informação de geo-localização ao objecto digital, no momento em que o utilizador o recebe, envia ou cria. Os parâmetros de informação de geo-localização usados para a contextualização são os seguintes: Latitude; Longitude; GSM Cell-ID; GSM *Area Code*; Morada. Para a localização do utilizador no momento em que recebeu, enviou ou criou um contacto, SMS ou chamada, é apurado se este possui o GPS activo. No caso afirmativo, é usado este sistema de geo-localização. No caso negativo, é investigado se tem o *Network Location Provider* activo. Se tiver, usa esse *provider* para se localizar. Se o GPS e *Network Location Provider* se encontrarem ambos inactivos é usada a localização por Cell-ID, que se encontra permanentemente activa, e permite saber aproximadamente a localização do utilizador. Se dispuser de todos os *providers* activos, é dado preferências ao de GPS, seguidamente do *Network Location Provider*, por questões de precisão. A geo-codificação (obtenção da morada a partir das coordenadas) só é obtida, imediatamente, se o utilizador tiver acesso à Internet (GSM ou Wi-Fi). Caso o utilizador não tenha uma ligação à Internet no momento em que surgiu o objecto digital, é guardado na base de dados da aplicação CoBy apenas as coordenadas (GSM Cell-ID + GSM *Area Code* e/ou latitude + longitude). A geo-codificação é conseguida posteriormente quando o utilizador já tiver oportunidade de se ligar a uma rede Wi-Fi ou GSM.

A duração da bateria dos dispositivos móveis é um dos grandes problemas com que os programadores e utilizadores se deparam. É essencial que se desenvolvam aplicações que de alguma forma, consumam menos recursos energéticos possíveis. No que toca à geo-localização é estabelecido um compromisso entre o consumo de bateria e a precisão de localização.

Outro aspecto que implicaria um consumo exaustivo dos recursos energéticos do dispositivo móvel seria a existência de um serviço para detectar a chegada de SMSs ou chamadas. Colmatou-se esse problema usando para isso o conceito de *Broadcast Receiver* para despoletar o serviço (Shu, Du, & Chen, 2009), e foi utilizado neste caso, a pensar nesta questão. Este activa o serviço só quando recebe um determinado evento,

neste caso a recepção de uma SMS ou uma chamada, evitando a necessidade de ter um serviço a correr permanentemente.

A detecção do envio, recepção ou criação de uma SMS, chamada, ou contacto é feito usando abordagens diferentes, tal como é ilustrado na Tabela 2. Sempre que, ao dispositivo móvel chega uma SMS ou uma chamada existe um *Broadcast Receiver* que detecta a sua chegada, usando o sistema de notificações do *Android*, e onde é possível aceder ao seu conteúdo. O *Broadcast Receiver* activa um serviço que irá obter a localização do utilizador usando os sistemas de geo-localização disponíveis no dispositivo móvel, no momento. Quando o utilizador, envia uma SMS, efectua uma chamada ou cria um contacto existe um *ContentObserver* que detecta esse acto. Assim que este é notado, o serviço responsável pela obtenção da geo-localização é activado e o utilizador é localizado.

Tabela 2 - Abordagem usada para envio/recepção de chamadas e SMSs.

Eventos	Abordagem usada
SM S enviada	<i>ContentObserver</i>
SM S recebida	<i>Broadcast Receiver</i>
Chamada efectuada	<i>ContentObserver</i>
Chamada recebida	<i>Broadcast Receiver</i>
Criação de contacto	<i>ContentObserver</i>

Seguidamente é guardado na base de dados da aplicação CoBy toda informação de geo-localização que se conseguir apurar. É criada uma tabela semelhante à ilustrada na Figura 14 por cada grupo de objectos digitais. Na base de dados da aplicação CoBy é unicamente guardada informação relativa à geo-localização. Todo o restante conteúdo da SMS, contacto ou chamada não está presente nesta base de dados, devido ao facto de se encontrarem acessíveis a partir das bases de dados do *Android*, evitando desta forma redundância de informação. Caso o utilizador apague um dos seus objectos digitais, a informação de geo-localização relativamente a esse objecto é mantida na base de dados da aplicação CoBy, mas com a indicação de que este foi apagado. Desta forma o utilizador sabe que apagou o objecto e tem acesso ao seu contexto, apenas desconhece qual o seu conteúdo. Tem também a possibilidade de não o fazer, e apagar toda a informação relativa ao objecto que previamente apagou na base de dados do *Android*.

_timestamp	Id	latitude	longitude	gsmCellId	gsmAreaCode	Deleted	DeletedTimestamp	Address	...
1331115608113	1	40.635007	-8.6765321	20504451	51	0	-	R. Banda da Amizade	...
1331216609113	3	40.935007	-8.5765321	20504451	51	1	1331219609113	R. Joaquim da Silva	
...	...	...	...	...	...	...	...	...	...

Figura 14 – Tabela da Base de dados da aplicação CoBy.

De forma a persistir os dados localmente no dispositivo móvel, a plataforma *Android* disponibiliza uma abstracção designada *Content Provider* (Hashimi, Komatineni, & MacLean, 2010), acedido através de cursores de uma forma espectacular e independentemente da fonte de dados utilizada. Para usar os padrões nativos deste

sistema operativo, foi utilizada uma base de dados SQLite¹ para guardar os dados localmente, construindo-se um *Content Provider* para facilitar o acesso aos mesmos (Owens, 2006). O *timestamp* que representa a data e o tempo de determinado evento, funciona como chave primária em todas as tabelas da base de dados da aplicação CoBy. Pois, dois objectos terão sempre *timestamps* diferentes. O ID do objecto só é obtido posteriormente, por pesquisa na base de dados do *Android*, e por comparação dos *timestamps*. Desta forma é possível identificar um objecto inequivocamente, nas duas bases de dados.

Na aplicação CoBy o utilizador tem total controlo sobre os seus dados. Existem opções que permitem uma vigilância afincada sobre aquilo que o utilizador pretende ou não enviar para o repositório digital pessoal, assim como aquilo que pretende ou não preservar no cartão SD do dispositivo móvel, como *backup*. A aplicação CoBy sincroniza-se com o repositório digital pessoal usando para isso um *Web-service REST* (Cobârzan, 2010), (He, 2003) que consome e produz dados no formato JSON (*JavaScript Object Notation*)². Na Figura 15 encontra-se representada a estrutura dos objectos JSON comum aos vários tipos de objectos digitais que são enviados para o *Web-service*. Consoante o tipo de objecto digital, existem alguns campos comuns e outros específicos de cada tipo de dados. A título de exemplo, na Figura 16 está ilustrado o formato completo de um objecto JSON do tipo SMS, constituído pelos seguintes campos:

- *Object Type*: identificador do objecto (SMS, Contactos, Chamadas, etc.);
- *Created Time*: identifica a data e hora da criação;
- *Address, longitude, latitude, Cell-ID*: informação de localização;
- *Own Contact*: identifica o número do cartão de onde surgiu o objecto;
- *Person Contact*: representa o número da pessoa com a qual se está a estabelecer contacto.
- *Source*: indica se a mensagem foi recebida ou enviada;
- *Body*: representa o corpo da SMS propriamente dito;

Object Type	Created Time	Address	Latitude	Longitude	Cell-ID	Own Contact	...
-------------	--------------	---------	----------	-----------	---------	-------------	-----

Figura 15 – Estrutura JSON comum a todos os objectos digitais.

¹ <http://www.sqlite.org/>

² <http://www.json.org/>

Caso o utilizador achar que não precisa de preservar os seus objectos no repositório digital pessoal, pode simplesmente usar esta aplicação para fazer *backup* e *restore* a partir do cartão SD do seu dispositivo móvel. Mas se houver uma perda ou furto do mesmo, toda a informação perder-se-á.

Object Type	Created Date	Address	Latitude	Longitude	Cell-ID	Own Contact	Person Contact	Source	Body
-------------	--------------	---------	----------	-----------	---------	-------------	----------------	--------	------

Figura 16 - Estrutura JSON para objectos digitais do tipo SMS.

A utilização de um repositório digital pessoal como plataforma de armazenamento remoto é um dos traços distintivos da aplicação CoBy. Um repositório digital pessoal, mais do que uma plataforma intermédia onde os objectos digitais ficam armazenados à espera de serem restaurados para um dispositivo móvel é uma plataforma que permite organizar e relacionar diferentes tipos de objectos digitais provenientes de várias plataformas e aplicações (Sousa, Pereira, & Martins, 2012). O repositório digital pessoal é responsável por interpretar as estruturas JSON utilizadas pela aplicação CoBy de forma a criar uma representação semântica dos objectos digitais recebidos, e de forma inversa é responsável por recriar as estruturas JSON a partir da representação semântica do objecto digital quando comunica com a aplicação CoBy. A representação semântica de um objecto digital é armazenada numa *embedded triple-store* (baseada na base de dados Neo4J³), e é determinada por uma ontologia (que se encontra em desenvolvimento de forma a ser capaz de lidar com tipos adicionais de objectos digitais). A ontologia que está a ser desenvolvida é fortemente influenciada pela ontologia CIDOC CRM (Group, 2011) com extensões para descrever eventos associados ao ciclo de vida dos objectos digitais, ao próprio repositório digital pessoal, e para descrever os vários tipos de objectos digitais que um utilizador pode armazenar no repositório digital pessoal. O uso desta ontologia permite classificar de forma consistente os objectos digitais, estabelecer as suas propriedades, e descobrir relações entre diferentes objectos digitais, tornado assim possível que o utilizador do repositório digital pessoal tenha a noção da forma como, por exemplo, uma determinada SMS se encaixa com outras formas de conversação digital (mensagens instantâneas, emails, etc.) mantidas com um contacto. Nem todos os objectos digitais podem ser armazenados de forma eficiente somente com recurso à sua descrição semântica. Objectos digitais com conteúdos binários, como por exemplo imagens ou músicas, são armazenados no seu formato binário nativo, tendo a sua representação semântica uma propriedade (URL para a representação nativa) que permite o acesso ao objecto digital no formato original.

As capacidades de classificação e organização de objectos digitais individuais distinguem um repositório digital pessoal das soluções de *backup* e *restore* com funcionalidades de armazenamento na *Cloud*, que normalmente criam arquivos com conjuntos de objectos digitais que têm de ser restaurados para um dispositivo compatível de forma a ficarem novamente acessíveis ao utilizador.

³ <http://neo4j.org/>

4. Análise da Aplicação

Subsistem muitas aplicações para *Android* que, tal como a aplicação CoBy, englobam funcionalidades de *backup* e *restore* de SMSs, contactos e histórico de chamadas. Na Tabela 3 encontra-se ilustrada a comparação entre a aplicação CoBy e as aplicações mais usadas no *Google Play*, e que de alguma forma dispõe de funcionalidades comuns. Será apenas sobre estas que será efectuado algum juízo de valor nesta secção.

Tabela 3 - Comparação entre a aplicação CoBy e as aplicações de backup e restore mais usadas no *Google Play* (* Apenas para e-mail).

Algumas funcionalidades	CoBy	SMS Backup & Restore (RITESH SAHU)	SMS Backup +	SMS Backup & Restore (INFOLIFE LLC)	Call logs Backup & Restore	JS Backup	Backup Contacts	Mobile backup II	Super Backup : SMS & Contactos	Backup Master	MyBackup Pro	SMS BACKUP n2manager
SMS	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Contactos	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Histórico de Chamadas	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Backup para SD Card	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Restore do SD Card	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Backup para repositório digital pessoal ou Cloud	☑	☑ *	☑ *	☑	☑	☑	☑	☑	☑ *	☑	☑	☑
Restore da repositório digital pessoal ou Cloud	☑	☑ *	☑ *	☑	☑	☑	☑	☑	☑ *	☑	☑	☑
Backups automáticos	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Capacidade de filtrar informação que pretende preservar	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Suporte repositório digital pessoal	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Geo-localização	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

A existência de aplicações que possibilitem *backup* e *restore* para e ou a partir do cartão de memória do dispositivo móvel já é uma realidade bastante clara, e é uma característica comum a todas as aplicações retratadas na Tabela 3, com a excepção das aplicações *SMS Backup+* e *Backup Contacts*. Os *backups* podem ser efectuados manualmente ou automaticamente. No caso em que esta tarefa é feita manualmente, pode existir alguma perda de informação. É bastante ineficaz para o utilizador ter de desencadear um *backup* sempre que recebe ou cria um objecto, ou quando achar que é necessário. Acabando por fazê-lo, mas com intervalos temporais muito espaçados, correndo o risco de perder informação nesse período de tempo. Os *backups* automáticos são bastante mais eficazes, libertando o utilizador da preocupação de salvarguardar os seus dados periodicamente, tendo neste caso, a possibilidade de definir na aplicação quando e de quanto em quanto tempo o pretende fazer. Esta funcionalidade está presente não só na aplicação CoBy, como também em todas as restante, com a excepção das aplicações *Backup Contacts*, *Mobile Backup II* e *Super Backup: SMS & Contacts*.

Tudo aquilo que é guardado com o objectivo de ser preservado deve sofrer um controlo integral por parte do utilizador. Existem sempre objectos digitais em que a sua preservação pode não ser desejada. A aplicação CoBy fornece ao utilizador este

controlo bastante pormenorizado, permitindo-lhe preservar unicamente aquilo que pretender. Trata-se de uma funcionalidade única da aplicação CoBy.

Já existem aplicações que de alguma forma permitem o armazenamento e a preservação de dados na *Cloud*. Algumas delas só disponibilizam essa funcionalidade para o *e-mail*. Três bons exemplos disso são as aplicações *SMS Backup & Restore* desenvolvido por *RITESH SAHU*, *Super Backup* e *SMS Backup +* que permitem a exportação dos dados para uma conta de e-mail. Tornando-se confuso e pouco objectivo para o utilizador. As aplicações CoBy, *JS Backup*, *Backup Contacts* e *MyBackup Pro* são bastante mais inovadoras neste aspecto, pois permitem a ligação a um repositório digital pessoal onde a informação se encontra organizada, estruturada e privada. Os repositórios usados por estas aplicações são: *DropBox*, *SugarSync* ou *Google Docs*.

Nenhuma das aplicações ilustrada na Tabela 3 permite qualquer tipo de geo-contextualização de informação. Trata-se de uma funcionalidade única da aplicação CoBy, permitindo ao utilizador preservar não só o conteúdo mas também o local em que os objectos digitais surgiram.

A aplicação CoBy consegue englobar funcionalidades como: recolha, preservação e contextualização de vários tipos de objectos digitais (SMSs, contactos, histórico de chamadas); geo-localização dos objectos; armazenamento da informação em locais distintos (cartão SD e repositório pessoal); sincronismo dos dados com o repositório; *backups* automáticos e *restore* para/do cartão SD e repositório pessoal; preservar apenas objectos digitais do interesse do utilizador; interface gráfica de acesso aos dados no dispositivo móvel e no repositório. Nenhuma das restantes conseguem integrar na sua totalidade as funcionalidades presentes na aplicação CoBy. Mas aquilo que de facto, se pode considerar inovador, é a geo-contextualização dos objectos, possibilitando ao utilizador legitimar o surgimento dos mesmos, bem como a possibilidade de garantir a sua preservação num repositório digital pessoal.

5. Conclusões

Neste artigo apresentou-se a aplicação CoBy como protótipo de um modelo de recolha, preservação e contextualização de informação. Esta aplicação demonstra uma elevada utilidade para utilizadores de dispositivos móveis. Trata-se de uma aplicação com capacidade de *backup* automático e *restore* de SMSs, contactos e histórico de chamadas, devidamente contextualizados. O utilizador pode fazer uma cópia de segurança e restauro não só para o seu repositório digital com também para cartão de memória do seu dispositivo. A sua ligação a um repositório digital pessoal permite colmatar o problema da acelerada obsolescência inerente às diversas tecnologias e *softwares* que vão surgindo. Assim, vê-se garantida a preservação persistente e continuada do material digital, sem receio de perda, detioração ou corrupção dos mesmos. A contextualização permite ao utilizador a criação de uma imagem mental inteligível de tudo aquilo que o rodeava quando recebeu, criou ou enviou o objecto digital. Permitindo, desta forma não só preservar o conteúdo propriamente dito, mas também a imagem mental circundante. Com esta aplicação, o utilizador consegue salvarguardar as SMSs, contactos e/ou chamadas que achar que tem relevância para tal

e dar um grande contributo para a escrita da sua própria história, não só pessoal mas também profissional.

Com um método semelhante ao descrito para as SMSs, contactos e chamadas, a aplicação CoBy irá permitir não só a recolha, preservação e contextualização destes objectos, mas também de imagens, emails, fotos, *bookmarks*, músicas, calendário, etc. Em suma, todo o material digital disponível no dispositivo móvel e que seja do interesse do utilizador preservar. Serão também efectuados testes de usabilidade de forma a tornar a aplicação mais robusta. Futuramente, a aplicação CoBy será extensível a outros sistemas operativos móveis.

Agradecimentos: Este trabalho foi financiado em parte pela bolsa SFRH/BD/62554/2009 da Fundação Portuguesa para a Ciência e Tecnologia.

6. Referências

- Abowd, G. D., Ebling, M., Hung, G., Lei, H., & Gellersen, H. W. (2002). Context-aware computing. *Pervasive Computing, IEEE*, 99(3), 22-23.
- Arellano, M. A. (2004). Preservation of digital documents. *Ciência da Informação*, 33(2), 15-27.
- BOOK, B. (2002). Reference Model for an Open Archival Information System (OAIS).
- Cobârzan, A. (2010). Consuming Web Services on Mobile Platforms. *Informatica Economica*, 14(3), 1453-1305.
- da Costa, R. (2007). História e Memória: a importância da preservação e da recordação do passado. *SINAIS - Revista Eletrônica - Ciências Sociais*, 1, 02-15.
- Darwin, I. F. (2012). *Android Cookbook* (First Edition ed.): O'Reilly Media.
- Dey, A. K. (2001). Understanding and using context. *Personal and ubiquitous computing*, 5(1), 4-7.
- Djuknic, G. M., & Richton, R. E. (2001). Geolocation and assisted GPS. *Computer*, 34(2), 123-125.
- Gartner. (2012). Worldwide Mobile Device Sales to End Users Retrieved 05-06-2012, from <http://www.gartner.com/technology/home.jsp>
- Group, C. C. S. I. (2011). The CIDOC Conceptual Reference Model Retrieved 05-06-2012, from <http://www.cidoc-crm.org/>
- Hashimi, S. Y., Komatineni, S., & MacLean, D. (2010). *Pro Android 2*: Springer.
- He, H. (2003). What is service-oriented architecture. *Publicação eletrônica* 30.
- Heery, R., & Anderson, S. (2005). Digital repositories review. *Joint Information Systems Committee*.
- Kaplan, E. D., & Hegarty, C. J. (2006). *Understanding GPS principles and applications*. Norwood: Artech House Publishers.

- Kumar, S., Qadeer, M. A., & Gupta, A. (2009). *Location based services using android (LBSOID)*. Paper presented at the Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference, Bangalore.
- Mehra, P. (2012). Context-Aware Computing: Beyond Search and Location-Based Services. *Internet Computing, IEEE*, 16(2), 12-16.
- Meier, R. (2010). *Professional Android 2 application development*. USA: Wiley Publishing, Inc.
- Ottaviani, V., Lentini, A., Grillo, A., Di Cesare, S., & Italiano, G. F. (2011). *Shared Backup & Restore: Save, Recover and Share Personal Information into Closed Groups of Smartphones*. Paper presented at the New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference.
- Owens, M. (2006). *The definitive guide to SQLite*: Apress.
- Pascoe, J. (1998). *Adding generic contextual capabilities to wearable computers*. Paper presented at the Wearable Computers, 1998. Digest of Papers. Second International Symposium.
- Saidis, K., & Delis, A. (2007). Type-consistent digital objects. *D-Lib Magazine*, 13(5), 4.
- Shu, X., Du, Z., & Chen, R. (2009). *Research on mobile location service design based on Android*. Paper presented at the Proceedings - 5th Int. Conf, WiCOM 2009.
- Sousa, J., Pereira, M., & Martins, J. A. (2012). Improving Browser History Using Semantic Information. *ICEIS 2012 - 14th International Conference on Enterprise Information Systems*.
- Trevisani, E., & Vitaletti, A. (2004). *Cell-ID location technique, limits and benefits: an experimental study*. Paper presented at the Mobile Computing Systems and Applications.
- Zhuang, Z., Kim, K. H., & Singh, J. P. (2010). *Improving energy efficiency of location sensing on smartphones*. Paper presented at the Proceedings of the 8th international conference on Mobile systems, applications, and services (MobiSys '10), ACM, New York, NY, USA.

CrITÉrios 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.aisti.eu>).

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.

Lo envío de artículos para publicación en la RISTI debe hacerse de conformidad con las llamadas de los artículos y las instrucciones y normas establecidas en el sitio Web de la revista (<http://www.aisti.eu>).

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.

Chamada de Artigos

Encontra-se aberto até 19 de Outubro de 2012 o período de envio de artigos para o décimo número da RISTI (Revista Ibérica de Sistemas e Tecnologias de Informação), o qual será publicado durante o próximo mês de Dezembro de 2012.

Este número é dedicado à Engenharia e Gestão de Sistemas de Informação e pretende integrar contribuições originais e relevantes nas diferentes dimensões e vertentes destas temáticas. Os tópicos recomendados incluem os listados abaixo. No entanto, também serão bem-vindos outros tópicos relacionados com estas temáticas mas aqui não incluídos:

- Abordagens Teóricas e Metodológicas
- Planeamento Estratégico de SI
- Criatividade em SI
- Arquitecturas de SI
- Práticas de Governação de SI
- Gestão da Informação
- Auditoria a SI
- Gestão do Conhecimento
- Modelos de Maturidade e Benchmarking.
- Qualidade em SI
- Integração de SI
- Segurança em SI
- Análise de Requisitos
- Metodologias de Desenvolvimento de Software

Os artigos devem ser escritos em Português ou Espanhol. Para informações sobre dimensão, normas de formatação e processo de submissão, agradecemos a consulta do Portal da RISTI: <http://www.aisti.eu>

Llamada de Artículos

Se encuentra abierto hasta al día 19 de Octubre de 2012 el período de envío de artículos para el decimo número de la RISTI (Revista Ibérica de Sistemas y Tecnologías de la Información), el cual será publicado durante el próximo mes de Diciembre de 2012.

Este número se dedica a las temáticas de Ingeniería y Gestión de Sistemas de Información. Pretende integrar contribuciones originales y relevantes en las diferentes dimensiones y aspectos de estos temas. Los asuntos recomendados incluyen los abajo listados, pero también serán bienvenidos otros asuntos relacionados con la temática y aquí no incluidos:

- Enfoques Teóricos y Metodológicos
- Planificación Estratégica de SI
- Creatividad en SI
- Arquitecturas de SI
- Prácticas de Gobierno de SI
- Gestión de la Información
- Auditoría de SI
- Gestión del Conocimiento
- Modelos de Madurez y *Benchmarking*
- Calidad en SI
- Integración de SI
- Seguridad en SI
- Análisis de Requisitos
- Metodologías de Desarrollo de Software

Los artículos deben ser escritos en portugués o español. Para obtener información sobre longitud, reglas de formato y proceso de envío, por favor consulte el Portal de la RISTI: <http://www.aisti.eu>

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 aisti@aisti.eu

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 aisti@aisti.eu



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 - 25€

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

☐ Outro (Empresa, etc.) - 500€

NIF/CIF: _____

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



Associação Ibérica de Sistemas e Tecnologias de Informação



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

Apoio



ACADEMY PUBLISHER

<http://www.academpublisher.com/>

FCT Fundação para a Ciência e a Tecnologia

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR