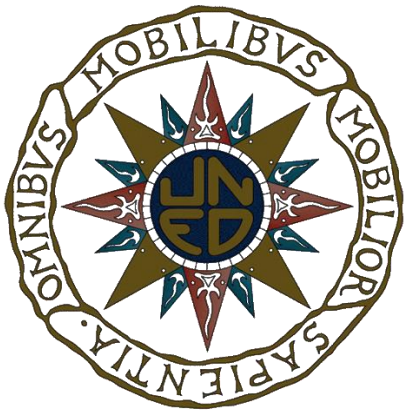
UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES

DEPARTAMENTO DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA

Y DE CONTROL



TESIS DOCTORAL

ARQUITECTURAS DISTRIBUIDAS DE GOBIERNO ELECTRÓNICO CON CIBERSEGURIDAD CRÍTICA

JESUS SALVADOR CANO CARRILLO

MÁSTER EN COMUNICACIÓN, REDES Y GESTIÓN DE CONTENIDOS

INGENIERO EN INFORMÁTICA

MADRID, 2015

UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA
ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES

TESIS DOCTORAL

ARQUITECTURAS DISTRIBUIDAS DE GOBIERNO ELECTRÓNICO CON CIBERSEGURIDAD CRÍTICA

Autor:
JESUS SALVADOR CANO CARRILLO
MÁSTER EN COMUNICACIÓN, REDES Y GESTIÓN DE CONTENIDOS
INGENIERO EN INFORMÁTICA

Director:

Dr. D. ROBERTO HERNÁNDEZ BERLINCHES

Dedico esta tesis a mi cariñosa
esposa, y a mis adorables e
incansables hijas.

AGRADECIMIENTOS

Este trabajo no hubiera sido posible sin el seguimiento y apoyo de mi maestro Dr. Roberto Hernández que me ha guiado con perseverancia. Su dirección, tutorización y la elección de los temas que componen hoy este conjunto de resultados científico-técnicos han sido trazados con un mapa de ruta exigente y con un plan de trabajo constante e intenso, gracias por todo.

Es imposible conseguirlo sin el cariño y el apoyo de toda mi familia, en especial a los que han sufrido la falta de tiempo y las noches en vela.

Quiero acordarme especialmente de aquellos maestros del Colegio Público San Agustín, que me imprimieron esta ilusión por el estudio desde pequeño. A la Guardia Civil y al Tribunal Constitucional: militares, funcionarios civiles, letrados, jueces, policías y todo el personal con los que comparto trabajo, espíritu y tecnología. A IEEE y especialmente a IEEE eGovernment por su apoyo y confianza.

A aquellos profesores míos de la Universidad que ahora me llaman colega, mil gracias por enseñarme a ser humilde. A los amigos y compañeros que con este hito tendrán una excusa más para celebrarlo.

SÍNTESIS DE LA TESIS

La sociedad digital se encuentra en un punto de inflexión caracterizado por la revolución tecnológica y la ebullición de sistemas de la información y el conocimiento que están cambiando el mundo. Como consecuencia, el ecosistema de relaciones sociales reconoce a los ciudadanos la naturaleza digital y exigen a los gobiernos el ejercicio de sus nuevos derechos y libertades.

El desarrollo y puesta en marcha de arquitecturas ingenieriles de Gobierno Electrónico que den respuesta a este nuevo impulso tecnológico es un reto ineludible que necesita desarrollarse a partir del esfuerzo de la comunidad científica y la innovación. Hoy en día es una realidad que desde las administraciones públicas se han desarrollado importantes pasos con el fin de mejorar la atención y el servicio al ciudadano, pero a menudo se ven superados por la ola de los cambios.

Los sistemas distribuidos se implementan a través de una amplia gama de redes y entornos, bajo requisitos significativos de rendimiento y seguridad, con un ingente paquete de políticas e inversiones públicas. Las arquitecturas gubernamentales se caracterizan en la realidad por grandes cuotas de complejidad, heterogeneidad y uso a gran escala. El desarrollo de soluciones de Administración electrónica se convierte en una tarea delicada y la ciberseguridad en un reto de dimensión especial. La relación con los ciudadanos y con la industria hace que el

sector público pueda ser considerado la mayor de las empresas, no sólo cuantitativa sino también cualitativamente. Por consiguiente, el gobierno electrónico es un contexto en el que resulta inherente su carácter interdisciplinar, lo que añade una visión poliédrica de las arquitecturas tecnológicas.

Los sistemas de información viven en un continuado movimiento innovador, lo que supone una constante presión para ajustar la demanda de servicios hacia el ciudadano. Los modelos tradicionales de arquitecturas, desarrollo y despliegue no ofrecen fácilmente los resultados con la inmediatez que las expectativas de la alta dirección y los ciudadanos esperan. Los esfuerzos en la comunidad científica por abordar estas problemáticas han sido especialmente emergentes en relación a la evolución de las arquitecturas orientadas a servicios, Web-escalables, en la nube, la computación ubicua-pervasiva y las redes sociales.

El objetivo fundamental de la tesis doctoral es proponer una nueva visión de las arquitecturas tecnológicas que permitan avanzar en el gobierno electrónico e inteligente cuyos dominios de negocio presentan necesidades críticas de ciberseguridad. La aplicación de nuevas estrategias tecnológicas aplicadas al Gobierno Electrónico es una de las aportaciones de este trabajo, especialmente en sectores relacionados con la seguridad, la defensa, la justicia, la educación y la democracia. En este contexto, tanto los desarrollos técnicos como la necesidad de que los sistemas sean gestionables de forma interdisciplinar adquieren especial relevancia.

Por ello, es importante aportar metodologías y contenidos que faciliten la formación tanto del personal técnico en computación como de otras áreas de conocimiento como profesionales del ámbito del derecho y de la gestión, tanto pública como privada, consecuencia de la propia naturaleza multidisciplinar del e-Gobierno. Como consecuencia se comprueba que mediante arquitecturas ágiles altamente distribuidas se consigue una alternativa, optimizada, para las arquitecturas tradicionales que se están viendo superadas por las innovaciones actuales; a través de las plataformas elásticas, las web escalables, la computación en la nube, las metodologías iterativas e incrementales, la integración continua, la virtualización, tanto de maquina como de comunicaciones o las redes sociales.

A lo largo de la tesis se han investigado un conjunto de áreas clave de los sistemas gubernamentales, se han desarrollado sistemas distribuidos y se ha evaluado la experiencia de su puesta en marcha. Los trabajos han servido de base para ofrecer una visión ágil cuya aplicación supone innovaciones tanto en los sectores de seguridad y defensa, en prevención de atentados terroristas, como en el sector de la democracia y participación, como es las iniciativas ciudadanas en ecosistemas de gobernanza relacionadas con las Smart Cities, pasando por arquitecturas de Open/e-Justicia y e-Educación. No se trata pues de una investigación especulativa ni de arquitecturas en sentido abstracto, sino que se han desarrollado, desplegado, explotado y gestionado.

Definitivamente esta tesis doctoral sigue un enfoque metodológico de investigación basado en el diseño que ha permitido contribuir al conocimiento de la ingeniería con la puesta en marcha de sistemas en su contexto natural bajo criterios arquitectónicos de eficiencia y seguridad.

THESIS ABSTRACT

The digital society is at a turning point, characterized by a technological revolution and the boiling of information systems and knowledge that are changing the world. As a result, the ecosystem of social relations gives citizens the digital nature and require governments to exercise their new rights and freedoms.

The development and implementation of e-government engineering architectures that respond to this new technological pull is an unavoidable challenge that needs to be developed from the efforts of the scientific community and innovation. Today it is a reality that the public administrations have developed important steps in order to improve care and service to the citizen, but often are overwhelmed by the wave of change.

Distributed systems are implemented through a wide range of networks and environments under significant performance and safety requirements, with an enormous package of policies and public investments. Government architectures are really characterized by large shares of complexity, heterogeneity and large-scale use. The development of e-government solutions becomes a delicate task; and cybersecurity is a challenge with special dimension. The relationship with the citizens and the industry makes public sector can be considered the largest of the

companies, not only quantitatively but also qualitatively. Therefore, e-government is a context that is inherent in its interdisciplinary character, which adds a multifaceted vision of technology architectures.

Information systems live in a continuous innovative movement, which is a constant pressure to adjust the demand for services to the citizen. Traditional models of architectures, development and deployment not easily provide immediate results with the expectations of top management and citizens expect. Efforts in the scientific community to address these issues have been especially emerging in relation to the evolution of service-oriented architecture, Web-scalable, cloud, ubiquitous-pervasive computing and social networks.

The main objective of this dissertation is to propose a new vision of technology architectures that advance electronic and smart government whose business domains have critical needs of cybersecurity. The application of new technological strategies implemented Electronic Government is one of the contributions of this work, especially in areas related to security, defense, justice, education and democracy. In this context, both technical developments and the need for systems that are manageable in an interdisciplinary are particularly important.

Thus it is important to provide methodologies and content to facilitate training both computer technicians as other areas of expertise as professionals in the field of law and both public and private management, due to the multidisciplinary nature itself of e-Government . Consequently it is found that using agile highly distributed architectures an alternative, optimized for traditional

architectures that are being overtaken by current innovations is achieved; through elastic platforms, scalable web, cloud computing, iterative and incremental methodology, continuous integration, virtualization, both machine as communications or social networks.

Throughout the thesis have been researched a group of key areas of government systems, distributed systems have been developed and has been assessed the experience of its implementation. The work has provided the basis for lively vision whose implementation involves innovations in the areas of security and defense in prevention of terrorist attacks, including in the field of democracy and participation, such as the citizens' initiative ecosystem of smart governance related to Smart cities, through architectures Open / e-Justice and e-Education. It is not merely a speculative research and architectures in an abstract sense, but have been developed, deployed, operated and managed.

Definitely, this PhD follows a methodological research approach based on design has allowed contributing to knowledge of engineering with the implementation of systems in their natural context under architectural criteria of efficiency and safety.

ÍNDICE GENERAL

LISTA DE ABREVIATURAS Y SIGLAS

ABP	APRENDIZAJE BASADO EN PROBLEMAS
ABC	APRENDIZAJE BASADO EN CASOS
ACM	ASSOCIATION FOR COMPUTING MACHINERY
AGIS	PROGRAMA EUROPEO PARA LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL
API	APPLICATION PROGRAMMING INTERFACE
ASP	ACTIVE SERVER PAGES
BOE	BOLETÍN OFICIAL DEL ESTADO
BPR	BUSINESS PROCESS REENGINEERING
BYOD	BRING YOUR OWN DEVICE
CAdES	CMS ADVANCED ELECTRONIC SIGNATURES
CCA	CLINGER-COHEN ACT
CCS	CACHE-BASED CONTENT SYSTEM
CDS&E	COMPUTATIONAL AND DATA-ENABLED SCIENCE AND ENGINEERING
CEO	CHIEF EXECUTIVE OFFICER
CERT	COMPUTER EMERGENCY RESPONSE TEAM
CIA	CONFIDENTIALITY, INTEGRITY, AVAILABILITY
CIBEV	CITIZEN INITIATIVE BASED ON ELECTRONIC VOTING
CcSM	CLOUD COMPUTING STORAGE MODULE
CIO	CHIEF INFORMATION OFFICER
CIS	CENTRO DE INVESTIGACIONES SOCIOLÓGICAS
CISS	CENTRAL INFORMATION SOFTWARE SYSTEM
CISP	PROGRAMA EUROPEO FRENTE AL TERRORISMO Y OTROS RIESGOS DE SEGURIDAD
CGRIP	CITIZEN GOVERNMENT RELASHIONSHIP INTERNET PROTOCOL
CMS	CRYPTOGRAPHIC MESSAGE SYNTAX
CN	COLLABORATIVE NETWORKS
CPS	CYBER PHYSICAL SYSTEM

CS	COMPETENT SIGNATURE
CSM	CITIZEN-SENSORS MODULE
CVM	CENSUS-VALIDATION MODULE
CVS	CÓDIGO DE VALIDACIÓN SEGURA
DBR	DESIGN-BASED RESEARCH
DBSM	DATABASE STORAGE MODULE
DMPC	DECISION-MAKING PROCESS CONTROL
DNI	DOCUMENTO NACIONAL DE IDENTIDAD
DNIE	DNI ELECTRÓNICO
DNS	DOMAIN NAME SYSTEM
DMZ	DEMILITARIZED ZONE
ECTS	EUROPEAN CREDIT TRANSFER SYSTEM
EE	ENTERPRISE EDITION, JAVA PLATFORM
EEES	ESPACIO EUROPEO DE EDUCACIÓN SUPERIOR
EGB	E-GOVERNMENT BACKSTAGE
EGDI	E-GOVERNMENT READINESS INDEX
E-ID	ELECTRONIC IDENTIFICATION
ERP	ENTERPRISE RESOURCE PLANNING
ETSI	EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE
EUPL	EUROPEAN UNION PUBLIC LICENCE
FNMT	FÁBRICA NACIONAL DE MONEDA Y TIMBRE
FPDF	FREE PDF, LIBRERÍA PHP
FSSM	FILESYSTEM STORAGE MODULE
GBL	GAME-BASED LEARNING
GCIO	GOVERNMENT CHIEF INFORMATION OFFICER
GPL	GNU GENERAL PUBLIC LICENSE
HCI	HUMAN–COMPUTER INTERACTION
HDI	HUMAN DEVELOPMENT INDEX
HPC	HIGH PERFORMANCE COMPUTING
HTML	HYPERTEXT MARKUP LANGUAGE
HTML5	HTML VERSIÓN 5

ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communications technology
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
IDE	Integrated development environment
IDS	Intrusion detection system
IEEE	Instituto de Ingenieros de Electricidad y Electrónica
IEC	International Electrotechnical Commission
IGF	Internet Governance Forum
IIS	Internet Information Server
ILP	Iniciativa Legislativa Popular
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ISIS-MTT	Industrial Signature Interoperability and Mailtrust Specification
ISMS	Information security management system
ITU	International Telecommunication Union
JCA	Java Cryptography Architecture
JCE	Java Cryptographic Extensions
JDK	Java Development Kit
JEC	Junta Electoral Central
JSON	JavaScript Object Notation
JSP	JavaServer Pages
JSPF	Fragmento JSP
JVM	Java Virtual Machine
KDJ	Knowledge database of Jurisprudence
LAN	Local Area Network
LLL	Life Long Learning
LM	Location Module
LOPD	Ley orgánica de protección de datos
MVC	Modelo Vista Controlador
NLP	Natural language processing
OAS	Oracle Application Server

ONU	Organización de las Naciones Unidas
OpenXML	Formato basado en XML para documentos ofimáticos
OWL	Web Ontology Language
P3	Public–private partnership, PPP
PAdES	PDF Advanced Electronic Signatures
PBL	Problem-Based Learning
PDF	Portable Document Format
PDO	PHP Data Objects
PERT	Program Evaluation and Review Technique
PIC	Protección de Infraestructuras Críticas
PKI	Infraestructura de clave pública
PKCS#7	Estándar de sintaxis de mensajes criptográficos
PMM	Process Management Module
PPP	Public–private partnership
RAID	Redundant array of independent disks
RDF	Resource Description Framework
REST	Representational State Transfer, estilo arquitectura web
RFC	Request for Comments
SARA	Sistemas de Aplicaciones y Redes para las Administraciones
SCEPYLT	Sistema de Control de Explosivos para la Prevención y Lucha contra el Terrorismo
SEO	Security Engineeer Officer
SM	Storage Module
SNA	Social Network Analysis
SVM	Signature-Verify Module
SOA	Service-oriented architecture
SOAP	Simple Object Access Protocol
SOC	Security operations center
SQuaRE	System and Software Quality Requirements and Evaluation
SSL	Secure Sockets Layer
SSM	Signature-Subscription Module
sTESTA	Secure TESTA

T1UL	Token de uso limitativo o un solo uso
TCP	Transmission Control Protocol
TEIF	Trazabilidad electrónica independiente del formato
TESTA	Trans European Services for Telematics between Administrations
TI	Tecnología de la información
TIC	Tecnologías de la información y las comunicaciones
TLS	Transport Layer Security
TSA	Time Stamping Authority
UE	Unión Europea
UML	Unified Modeling Language
UNDP	United Nations Development Programme
UNED	Universidad Nacional de Educación a Distancia
UOC	Universitat Oberta de Catalunya
URI	Uniform resource identifier
URL	Uniform Resource Locator
USA	United States of America
VAA	Módulo de verificación abierta basada autenticada
VPN	Virtual private network
W3C	World Wide Web Consortium
WAN	Wide Area Network
WSS	Web Software System
XAdES	XML Advanced Electronic Signatures
XML	Extensible Markup Language
XSS	Cross-site scripting

LISTA DE FIGURAS

TABLAS

Capítulo 1.

INTRODUCCIÓN

En este capítulo se introduce la perspectiva general, las motivaciones y el alcance de esta tesis doctoral, que utiliza una visión intensiva de la computación distribuida aplicada a dominios críticos en sistemas de gobierno electrónico en los que la aplicación de técnicas de protección y ciberseguridad son esenciales. Se presenta concisamente el enfoque actual de la disciplina tratada y se explica la necesidad que ésta supone sobre el estado del conocimiento.

1.1. MOTIVACIÓN

La transformación actual sobre la revolución tecnológica de la Sociedad de la Información y el Conocimiento está poniendo al alcance de los ciudadanos nuevas fórmulas de relación con la Administración Pública. A través de una Internet única, la gobernanza electrónica, la colaboración público-privada, los nuevos sistemas de participación y democracia, las plataformas de seguridad ciudadana, salud, justicia, defensa y educación se concentran en dominios críticos basados en TI que emergen

con fuerza impulsados por los cambios sociales, tanto de pensamiento como de innovación científica.

Con la extraordinaria evolución de las tecnologías de las comunicaciones, las arquitecturas centralizadas de los sistemas de información están dejando paso a los sistemas masivamente distribuidos. Su impacto en la vida diaria de las personas define la sociedad del futuro. Algunas instantáneas en este nuevo panorama social son las redes sociales, las tecnologías móviles, los sistemas Web escalables, el almacenamiento y análisis de grandes volúmenes de datos y los vehículos inteligentes.

El gobierno electrónico y las relaciones clásicas derivadas del paradigma burocrático tienen grandes retos a través de las arquitecturas distribuidas de información en el ámbito público. La evolución del *Open Government* y la gobernanza inteligente incorpora la eficiencia y la eficacia junto a altas exigencias de transparencia y participación ciudadana.

La ciberseguridad toma una extremada importancia en el ejercicio de los derechos y libertades digitales que el gobierno electrónico ofrece. De la misma manera que la seguridad ciudadana es fundamental para la convivencia de una sociedad democrática, la seguridad cibernética aspira alcanzar esos valores que habilite el desarrollo de la ciudadanía digital.

1.2. OBJETIVOS

Esta tesis doctoral propone una serie de arquitecturas de gobierno electrónico abarcando dominios intrínsecamente públicos, críticos y con necesidades de ciberseguridad por diseño. Para ello se desarrollan y se pone en marcha experiencias sobre democracia y participación, seguridad pública y terrorismo, justicia y educación en el marco de la e-Sociedad. La aplicación de ingeniería de la seguridad por defecto desde fases tempranas de la arquitectura es un objetivo primordial en el modelo de construcción de sistemas para un gobierno electrónico óptimo, así como las tecnologías orientadas al ciudadano.

1.3. INVESTIGACIÓN

Una de las primeras observaciones que se ha podido constatar en el campo de investigación sobre tecnologías ciudadanas es que no está suficientemente tratada en la literatura técnica, al menos en comparación con otras áreas. Este hecho puede explicarse en gran medida por el carácter multidisciplinar del Gobierno Electrónico, transversal con otras ramas del conocimiento científico, como las ciencias jurídicas y humanistas.

Esta tesis ha seguido un proceso de investigación basado en diseño (DBR, Design-Based Research), con elementos metodológicos cuantitativos y cualitativos. La investigación en diseño es un tipo de metodología que representa un paradigma alternativo a la investigación clásica positivista (esquema sistemático de problemas-hipótesis-métodos-demostración). Se ha extendido en los últimos años

especialmente aplicada a entornos complejos, donde los investigadores tratan de comprender y mejorar la realidad [1] y especialmente en dominios de la Sociedad del Conocimiento y de la Información. Esto se traduce en una forma de investigar donde se conoce a través del hacer y a partir de ahí se busca generar nuevo conocimiento y aplicaciones prácticas, como por ejemplo en computación componentes software, infraestructuras, marcos de trabajo o protocolos de TI. Estos mecanismos incorporan aspectos ágiles de investigación y un proceso iterativo para desde la práctica realimentar el conocimiento y mejorar su formulación. Así el fenómeno es explicado, no sólo desde la teoría, sino también como el resultado de un proceso de diseño. Para más detalle se puede consultar algunos autores en un repaso general desde los primeras teorías en los año 90 en [2], así como en [3] aplicada a la investigación de sistemas de información y en [4] en otros entornos.

En tanto que esta metodología de investigación sugiere la creación de un artefacto innovador, en cada una de las partes de esta tesis se sigue esta idea y se desarrollan varios artefactos (aplicaciones web-escalables, diseños distribuidos, frameworks, modelos de TI, protocolos y arquitecturas) en el dominio crítico objeto de la investigación que permiten la contribución al conocimiento científico aplicado en ingeniería.

1.4. ESTRUCTURA DE LA TESIS

Esta tesis está organizada en 7 capítulos. El primero de ellos presenta los principios de la investigación realizada, el segundo un repaso conceptual de arquitecturas distribuidas, gobierno electrónico, ciberseguridad, ingeniería de la seguridad y ciber-ética. Desde el capítulo 3 al 6 se expone el núcleo de la investigación en distintos dominios críticos de eGovernment.

- En el capítulo 2, se describen los fundamentos de la computación distribuida, haciendo un estudio de la situación actual, una prospección de evolución así como los modelos de solución distribuida. En este sentido, se aporta un análisis comparativo de las leyes de Moore y Gilder para ilustrar el balance entre rendimiento máquina y progreso en telecomunicaciones. En la sección 2 se describen los conceptos básicos de gobierno electrónico y gobernanza. A continuación se sitúa la temática de ciberseguridad e ingeniería de la seguridad, resaltando la protección de infraestructuras críticas. Además, se debate sobre el derecho a la información de seguridad, los servicios privados de ciberseguridad y el fenómeno de la ciberdelincuencia. Para terminar con el capítulo se tratan asuntos de ciber-ética, educación y concienciación.

- En el capítulo 3, se presenta el dominio de la participación y la democracia electrónica mediante el diseño de un framework para eDemocracia aplicable a Smart Cities. Para ello se construye una arquitectura distribuida con uso extensivo de mecanismos criptográficos y se desarrolla una aplicación software. Para ello, en primer lugar se introducen los conceptos básicos y el

estado del conocimiento sobre eDemocracia. A continuación, se expone la concepción del framework, con una descripción de los actores, del proceso, una arquitectura dual, consistente en una plataforma ciudadana y otra gubernamental, y se anticipa un protocolo susceptible de estandarización para eDemocracia de carácter universal. La siguiente sección trata del proyecto OpenILP (aplicación para iniciativas legislativas populares electrónicas), sus consideraciones funcionales y técnicas, los criterios de interoperabilidad, integridad y compatibilidad del software y detalles sobre los procesos criptográficos. La siguiente sección presenta un modelo conceptual para iniciativas ciudadanas basadas en esquemas de voto electrónico (CIBEV) para extender el proyecto. Al final se expone la experiencia, haciendo hincapié en la repercusión política, social y en los medios de comunicación que ha tenido dentro y fuera de España.

- En el capítulo 4, se investiga sobre eJusticia. Se presenta el estado actual de las tendencias en este dominio, particularmente sobre Justicia Abierta, donde se discute sobre los dilemas, la elección y la participación ciudadana, la justicia en red, la transparencia y los aspectos tecnológicos. Cabe resaltar la propuesta que se hace de *Amicus curiae digital* (participación ciudadana en el ámbito de la justicia) como solución intermedia de incorporación de la ciudadanía a la toma de decisiones judiciales, inspirándonos en un concepto del derecho clásico romano. Además en la sección 2 se expone la concepción

de nuevas arquitecturas, los factores importantes y la evolución tecnológica en relación a este sector. Finalmente, se presenta un framework para Open Justice, con determinación de sus parámetros constructivos, y la implementación de una aplicación software basada en este modelo que da soporte a la formulación.

- El capítulo 5 versa sobre dominios críticos de seguridad, criminalidad y terrorismo. Comienza con una revisión de la literatura y el estado del arte. Se repasa el concepto de CIO gubernamental o GCIO, el equipo humano, los factores críticos y tendencias, así como se ejemplifica con alguno de los sistemas de información representativos de índole internacional en este ámbito. En la sección 3 se expone el tema de la gestión de este tipo de sistemas críticos de seguridad internacional. A continuación se desarrolla un catálogo de lecciones y principios aprendidos que pueden servir de modelo para proyectos de esta naturaleza. En la última sección se presenta un framework de gobierno electrónico aplicado a terrorismo y una aplicación software sobre bases de datos distribuidas implantada a nivel europeo. Para ello se motiva y contextualiza el proyecto, se expresan los principios básicos para el diseño, el modelo arquitectónico completamente distribuido, la estructura de un nodo, los algoritmos para transacciones y consultas distribuidas, la implantación cifrada de redes y detalles de implementación.

- En el capítulo 6 se trabaja sobre el dominio crítico de e-Educación en el contexto de la sociedad de la información y el conocimiento desde dos planos

bien conocidos. En primer lugar desde el plano de la gestión educativa, se determina el contexto de la investigación, se hace un análisis de la situación actual de los sistemas educativos en relación al desarrollo de gobierno electrónico y se introduce conceptualmente la arquitectura. En esta sección se expone un framework de acreditaciones y diplomas basado en sistema de arquitectura de seguridad, verificación, trazabilidad y clasificación, mencionando especialmente la aparición del término firma competente y el diseño de la estrategia de token de uso limitativo T1UL. Se realiza el desarrollo software de un artefacto basado en Web escalable, denominado Opendiploma, y se evalúa la experiencia. En el segundo plano se trata la e-Educación desde el punto de vista de utilizar recursos tecnológicos para el proceso de enseñanza. Para ello se realiza una motivación científica y la definición de un proyecto didáctico de interés para la investigación que ha tenido cierta repercusión académica y profesional para la implantación de un Laboratorio de Ciberseguridad basado en recursos online y gamificación. Se describe la metodología de la investigación y un diseño en dos fases donde la primera es la fase de ideas previas, mientras que la segunda trata del diseño instruccional del laboratorio. La sección 4 ofrece algunas extensiones sobre el proyecto anterior para otras ramas del conocimiento y la inclusión de algunas técnicas de tipo constructivista. Se finaliza con una propuesta de adaptación curricular.

1.5. CONTRIBUCIONES Y TRABAJOS PUBLICADOS

En este apartado se resumen las contribuciones técnicas y la lista de artículos del autor motivados y relacionados con alguna parte de esta tesis. Es significativo señalar que los artículos publicados han pasado una revisión ciega por pares sobre revistas científicas con factor de impacto.

1.5.1. ARTÍCULOS

- Cano, J.; Hernandez, R.; Ros, S., "Distributed Framework for Electronic Democracy in Smart Cities," **Computer** , vol.47, no.10, pp.65,71, Oct. 2014 doi: 10.1109/MC.2014.280

- Cano, J.; Hernandez, R., "SCEPYLT: An Information System for Fighting Terrorism," ***Software, IEEE*** , vol.30, no.3, pp.73,79, May-June 2013 doi: 10.1109/MS.2013.23

- Cano, J.; Hernández, R.; Ros, S., "Bringing an engineering lab into social sciences: didactic approach and an experiential evaluation," ***Communications Magazine, IEEE*** , vol.52, no.12, pp.101,107, December 2014 doi: 10.1109/MCOM.2014.6979960

- Cano, J.; Jimenez, C.E.; Hernandez, R.; Ros, S., "New tools for e-justice: legal research available to any citizen," *eDemocracy & eGovernment*

(ICEDEG), 2015 Second International Conference on , vol., no., pp.108,111, 8-10 April 2015 doi: 10.1109/ICEDEG.2015.7114455

- Jimenez, C.E.; Cano, J.; Hernandez, "Emerging trends in engineering applied to e-Government and e-Justice" – HICSS Hawaii International Conference on System Sciences.

1.5.2. PARTICIPACIÓN EN CONFERENCIAS

- Madrid, España. I Jornada sobre calidad del producto software. Noviembre 21-22, 2013 (http://calidaddelproductosoftware.com/2013/programa)
- Quito, Ecuador. 2nd International Conference on eDemocracy & eGovernment. Abril 8-10, 2015 (https://edem-egov.org/ICEDEG-2015)
- Guadalajara, Mexico. First IEEE International Smart Cities Conference. Octubre 25-28, 2015. - Program Committee. (http://sites.ieee.org/isc2)
- Hawai, Estados Unidos. 49th Hawaii International Conference on System Sciences. HICSS. Enero 5-8, 2016. (http://www.hicss.org)

1.5.3. CAPÍTULOS DE LIBRO

- Cano, J., Hernandez, R. "Managing Software Architecture in Domains of Security-Critical Systems: Multifaceted Collaborative eGovernment Projects". Capitulo del libro "Securing Government Information and Data in Developing Countries". Editado por Dr. Saleem Zoughbi. **IGI-Global**. Serie: Advances in Information Security, Privacy, & Ethics (AISPE) Book Series. ISSN: 1948-9730

- Cano, J.; Hernandez, R.; Jimenez, C.E.; Pomed, L.; "Open justice in constitutional courts: securing Networked Constitution, challenges of electronic justice, transparency and citizen participation". Capítulo del libro "Achieving Open Justice through Citizen Participation and Transparency". Editado por: Jiménez, C.E. & Gascó, M. **IGI-Global**. Serie: Advances in Public Policy and Administration (APPA) Book Series.

- Carpio Cámara, M.; León, A.; Cano Carrillo, J.; Jiménez, C.E. "Regulación y ciberseguridad. Contribuciones al modelo de Gobernanza" Edita: **IGF Forum Spain**. 2015. [Disponible online] http://igfspain.com/doc/archivos/Gobernanza_Internet_Spain_2015.pdf [Accedido: 2015]

Capítulo 2.

COMPUTACIÓN DISTRIBUIDA, GOBIERNO ELECTRÓNICO Y CIBERSEGURIDAD

En este capítulo se introducen los conceptos arquitectónicos básicos de computación distribuida que se utilizan en el desarrollo de esta tesis. Se describen las arquitecturas, su caracterización y diseño, especialmente los aspectos relacionados con la escalabilidad, heterogeneidad, seguridad y fallos. El hecho de adoptar aproximaciones modernas de arquitecturas distribuidas tiene relevancia no sólo en el modelo de objetos y componentes, servicios web, soluciones de comunicaciones y sistemas de información, sino también en las metodologías de desarrollo, integración y producción así como en la gestión del cambio y la formación.

Por otro lado, se expone la visión actual de los principios del Gobierno Electrónico como articulador del conocimiento de los procesos gubernamentales a través del uso de tecnologías de la información que ofrecen servicios a los ciudadanos y a la industria. Se introducen como ámbito de aplicación de las

contribuciones presentadas en este trabajo las principales tendencias relacionadas con los dominios de defensa, seguridad interior, democracia y participación, justicia electrónica y educación.

Finalmente, se describe la ciberseguridad desde un punto de vista organizativo, metodológico y práctico sobre el que se fundamentan las decisiones arquitectónicas de esta tesis.

2.1. ARQUITECTURAS DE COMPUTACIÓN DISTRIBUIDA

La computación distribuida consiste en solucionar problemas complejos de la realidad mediante la organización en partes más pequeñas sobre un ecosistema de tecnología de la información y las comunicaciones. Para ello se diseña una arquitectura hardware y software capaz de maximizar el rendimiento de todos los componentes, interconectando usuarios y recursos de ingeniería de forma fiable, tolerante a fallos, accesible, transparente y a un coste determinado.

2.1.1. ASPECTOS GENERALES Y SITUACIÓN ACTUAL

Con la evolución de las arquitecturas y el avance en su capacidad de comunicación por red, la distancia tradicional entre la computación paralela y los sistemas distribuidos van difuminándose, configurándose en dos perspectivas para solucionar problemas complejos convergentes. De hecho gran parte de la literatura y las líneas de investigación comparten escenario y ha sido objeto de un importante

desarrollo durante los últimos años. Tanto el paralelismo como los sistemas distribuidos son clásicos en el currículum de las ciencias de la computación. En este sentido es interesante destacar todas las ediciones del texto clásico sobre Arquitectura del profesor Coulouris [5] en las que al compararlas se observa la rápida evolución en los sistemas distribuidos.

Otros autores siguen el enfoque clásico de recorrer las arquitecturas multiprocesador, pasando por los sistemas de paso de mensajes hasta las estructuras de red distribuidas, como en [6].

A la ciencia e ingeniería computacional relacionada con la explotación de datos (*Computational and Data-Enabled Science and Engineering*, CDS&E) hay que atribuirle gran parte del desarrollo y explotación de los métodos avanzados en procesamiento de la información, minería de datos, simulaciones y análisis de información que se pueden realizar hoy día. Además hay que añadir las infraestructuras de Grid computing, la computación de alta capacidad (HPC), las nuevas generaciones de informática ubicua sobre telefonía móvil, las aplicaciones de Big data, el análisis de redes sociales (SNA), el Cloud computing, o las redes de alta velocidad. Con todo ello se presenta un panorama de ciber infraestructuras avanzadas que permiten abrir nuevas posibilidades en la innovación científica y en la educación en áreas relacionadas con la computación que facilite el trabajo multidisciplinar de técnicos y no-técnicos para formar grupos de trabajo más productivos.

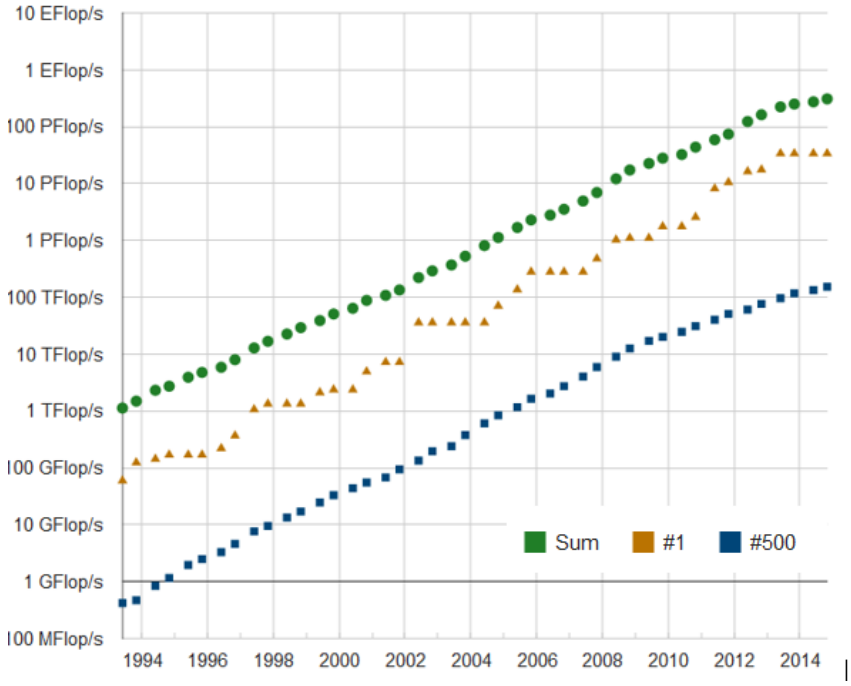
Otras áreas interesantes de la computación distribuida corresponde a crowdsourcing paralelo, las aplicaciones científicas y biomédicas, los sistemas wearables (sistemas

microelectrónicos distribuidos para llevar puesto en la ropa o en el cuerpo) y sistemas ciber-físicos (CPS) sobre los que se apoya la Internet de las Cosas [9].

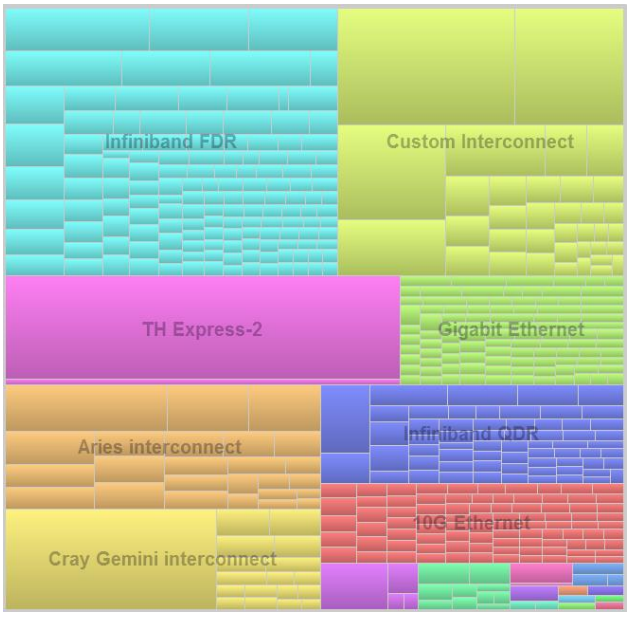
Las arquitecturas basadas en paralelismo incluyen desde estructuras a nivel de instrucción hasta niveles de proceso-hilo de ejecución, sistemas multiprocesadores cuyo diseño, análisis, rendimiento y tolerancia a fallos son especialmente relevantes, sistemas multicore, grandes sistemas de alto rendimiento Pentaescalares y Hexaescalares [10]. En la Figura 1 puede observarse por un lado la evolución del rendimiento de procesamiento de los conforme a la estadística del top 500 de supercomputación, mientras que la Figura 1.b ilustra la cuota de tipos de interconexión usado por los grandes sistemas de computación.

En su conjunto todo ello constituye un área de interés de propósito especial con respecto al manejo de Big data, de procesamiento y aceleración gráfica, procesamiento de señales, sistemas de almacenamiento masivo, arquitecturas aplicadas al Green Computing o aplicaciones hacia la seguridad de los datos.

En el ámbito de desarrollo software, las principales áreas de investigación se enfocan hacia lenguajes que aprovechen las capacidades distribuidas y de paralelismo, tanto en sistemas operativos como en computación sobre Internet y servicios para la web.



a)



b)

Figura 1. Evolución en supercomputación. a) Rendimiento b) Tecnología de interconexión

(Fuente: top500.org)

2.1.2. PROSPECTIVA DE LA EVOLUCIÓN TECNOLÓGICA

La reducción de costes en tecnología microelectrónica junto con el avance en la complejidad de los dispositivos se ha justificado por la conocida Ley de Moore. Antes de fundar la multinacional Intel, Gordon Moore enunció que la complejidad se duplicaría cada año y medio, si bien luego la reformuló a dos años. El fenómeno ha identificado la evolución comercial de los últimos 50 años en microprocesadores, computadores industriales, equipos personales y últimamente en tecnología móvil [7].

En esta inquietud prospectiva se ha intentado estudiar el impacto de los avances en las redes de comunicaciones. De hecho el ancho de banda ha ido creciendo de forma importante hasta nuestros días, de tal manera que se ha llegado a enunciar que el back-bone (redes principales) de Internet viene doblando su velocidad cada 6 meses, lo que se conoce como Ley de Gilder.

Sin embargo, hay otra regla para evolución de las conexiones de usuario final, que desde finales de los 90 viene enunciando que cada año aumentaría un 50% el ancho de banda según la Ley de Nielsen. Ciertamente una de sus afirmaciones fue que en 2015 se alcanzarían 100 Mbps de velocidad de Internet ofertado, cosa que ya ha ocurrido con la incorporación de la fibra óptica, y en 2020 se llegarían a 1Gbps, con un retraso de puesta en el mercado real de dos o tres años.

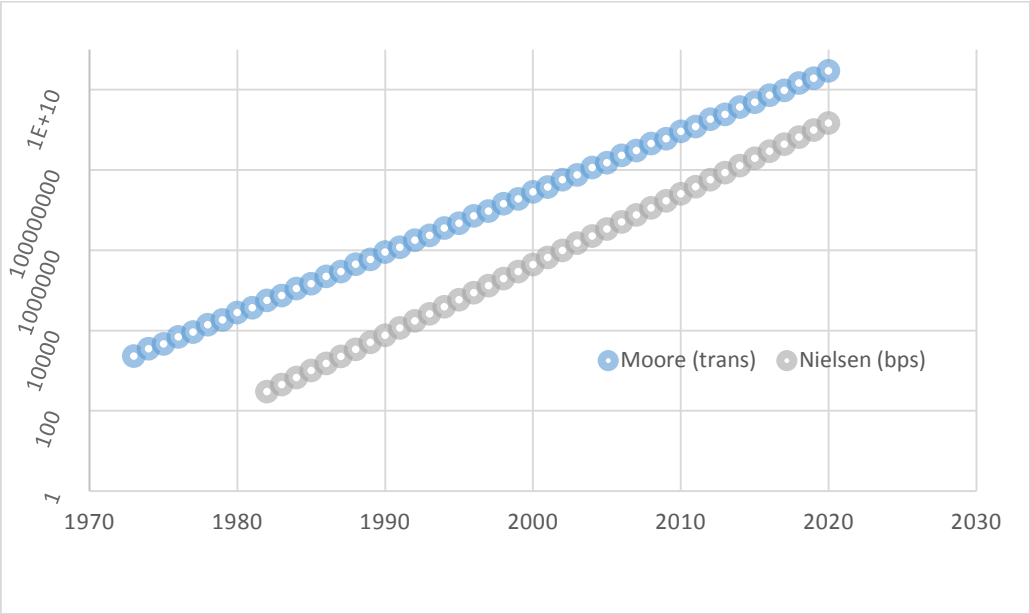


Figura 2. Análisis gráfico de las leyes de Moore y Nielsen

Como consecuencia, si evaluamos estas tendencias se puede discutir que la evolución de las tecnologías de comunicación ha crecido más que la potencia de computación y por ende que el intercambio de datos resulta algo más barato comparativamente. La Figura 2 muestra un análisis gráfico comparativo entre la línea teórica de Moore y de Nielsen.

Pero hay que tener en cuenta que si bien estas expresiones son predicciones teóricas que se han visto corroboradas con la realidad empírica, e intentan predecir el futuro cercano, si consideramos la realidad vemos cómo de buena ha sido esta predicción. De esta manera, al hacer un análisis relacionado con la capacidad de los microprocesadores reales observamos un desfase preocupante que pudiera prevenir de un nuevo ciclo evolutivo en microelectrónica.

Se han tomado las características de 92 microprocesadores, expuestas en [11], para confeccionar el siguiente gráfico, que ilustra por un lado la evolución de la capacidad real de los microprocesadores, en cantidad de integración de transistores, frente a su valor esperado conforme a la Ley de Moore. Con todo ello hemos obtenido los resultados que se muestran en la Figura 3.

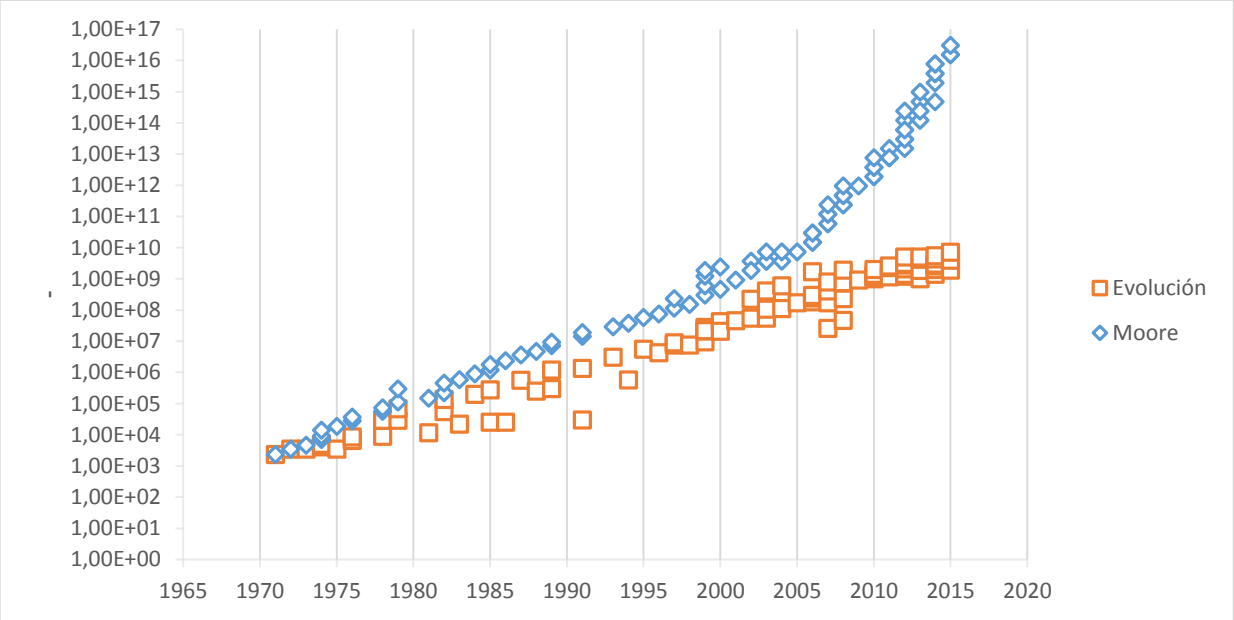


Figura 3. Análisis de evolución real frente a Moore

Vemos pues que desde finales de la primera década del 2000 el comportamiento de la ley de Moore empieza a desviarse, si bien la capacidad de velocidad ofertada por Internet sigue la dinámica de Nielsen, hecho que apoya la inversión y el despegue de tecnologías emergentes que se apoyan en el intercambio de información para su procesamiento distribuido.

En consecuencia, esto hace posible que el paralelismo y la computación distribuida basada en la conexión de procesadores sobre una red de datos, que ya venía utilizándose a través de LAN mediante los clusters, abra paso cada vez más a un modelo de aplicaciones distribuidas sobre redes WAN en la línea de la computación en Grid o en Cloud.

2.1.3. MODELOS DE SOLUCIÓN DISTRIBUIDA

En general los modelos distribuidos persiguen solucionar el intercambio de información entre los distintos procesos y nodos, la carga de procesamiento y balanceo, la escalabilidad y los asuntos relacionados con la seguridad en un entorno de red. Para ello han ido apareciendo distintos paradigmas o modelos de computación distribuida. Cabe mencionar el clásico modelo Cliente/Servidor, las arquitecturas Web, los modelos descentralizados P2P, la abstracción del modelo en Grid, los modelos en Cloud, la computación ubicua, el Internet de las Cosas (IoT), entre otras como hemos venido ya mencionando.

El modelo clásico Cliente/Servidor sirve de base para la intercomunicación entre procesos remotos, donde una parte asume el rol de proveedor de recursos y otro de consumidor de servicios.

Derivado del modelo anterior surgen las arquitecturas Web. Es un modelo extenso basado en una gran variedad de tecnologías sobre un esquema básico de relación entre servidor web y cliente navegador, donde existe un espacio de información (ciberespacio) en los que los recursos se identifican mediante identificadores (URI).

El organismo de estandarización W3C trabaja en la normalización y definición técnica de los protocolos de información [11], donde la extensión denominada Web Semántica toma un especial protagonismo (Web 3.0). Así, se promueven estándares para el formato de datos y protocolos de intercambio de información desde el punto de vista del significado, con el objeto de facilitar la reutilización de la información entre sistemas heterogéneos. Para ello se utilizan lenguajes de marcado y añadidos, como por ejemplo RDF para la descripción de recursos, OWL para definición de ontologías para la web o XML que extienda el marcado basado en HTML. En la Figura 4 se puede ver la relación entre algunos estándares que componen la web semántica del Consorcio W3C.

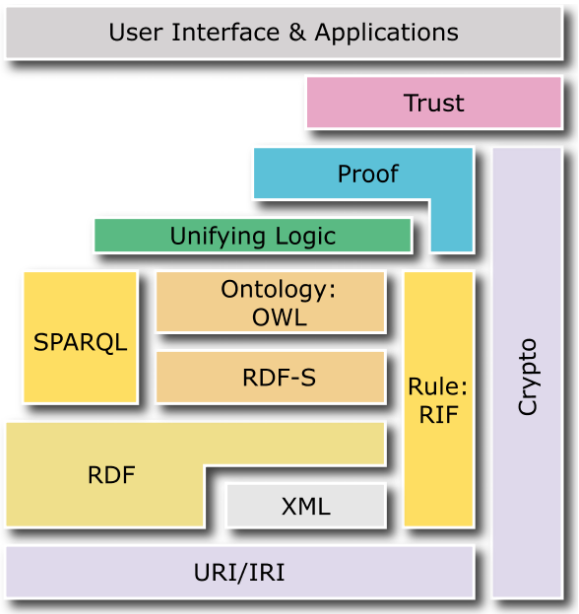


Figura 4. Actividades de la web semántica

(Fuente: W3C Linked Data on the Web)

Los modelos distribuidos en malla P2P se basan en la interconexión de cualquier proceso con cualquier otro a través de la red en sistemas que requieren una alta escalabilidad y descentralización. En esta tesis hacemos una contribución mediante el diseño de un sistema completamente descentralizado de datos.

En cuanto a los modelos basados en Grid, se tiene una gestión virtual de recursos y procesos remotos descentralizados con el objetivo de reducción de costes, en la línea de mejorar la escalabilidad y disponibilidad. De forma similar encontramos el paradigma de Cloud computing, donde interesa la compartición de recursos bajo criterios de economía y prestaciones basadas en servicios.

Por su impacto social las arquitecturas ubicuas, basadas en tecnologías móviles y tablets con permanencia continua de conexión del usuario, están formando parte del estilo de vida de la sociedad. La irrupción de las tecnologías invisibles y dispositivos para llevar puesto como los weareables, vienen a completar el panorama de transformación social.

Simultáneamente las tecnologías del Internet de las Cosas (IoT), los sensores conectados y los primeros pasos en las redes vehiculares están empezando a tomar las calles de las denominadas ciudades inteligentes (Smart Cities).

2.2. GOBIERNO ELECTRÓNICO

2.2.1. CONCEPTOS Y ASPECTOS GENERALES

El Gobierno electrónico consiste en el uso de sistemas de información y comunicaciones para mejorar los servicios públicos. Las definiciones dadas en la literatura al respecto implican esta idea, como la visión global planteada en [16], si bien pueden existir diversos matices. Las Naciones Unidas en su página web lo presenta ligeramente en relación a las TIC. Algunos estudios tratan el tema de la definición en función de la evolución de la sociedad, como en [12], o bien aportan una definición adjetivada como la de la Comisión Europea "eGovernment se define como la utilización de las tecnologías de la información y la comunicación (TIC) en las administraciones públicas, asociada a cambios en la organización y nuevas aptitudes del personal" [13]. Además se incluye en el término la mejora en la calidad y la accesibilidad a los recursos ofrecidos, la reducción de costes en las relaciones empresa-administración y la de hacer más fácil las transacciones ciudadano-administración.

Otros autores resaltan con claridad que eGovernment es algo más que un sitio web, un correo electrónico o procesar transacciones por Internet [14] y lo consideran una extensión de la revolución tecnológica que acompaña a la sociedad del conocimiento.

A pesar de las iniciativas puestas en marcha ha sido una constante, al menos en las declaraciones políticas, la intención de utilizar el gobierno electrónico como

una oportunidad de apertura, transparencia, gobernanza más entendible y auditable por los ciudadanos.

2.2.2. GOBERNANZA ELECTRÓNICA

Un tema que parece relevante, que no se ha tratado suficientemente en España, es la importancia cada vez mayor que tiene el hecho de buscar exigencia para seguir los estándares de la ingeniería del software en productos software que se construyan para las Administraciones Públicas, de manera que permitirían un mayor nivel de corrección y calidad de producto a nivel técnico. Además de otras consideraciones, esto tendría implicaciones a nivel preventivo en cuanto a la seguridad. Con la interconexión de redes cada vez más generalizada, muchos de los requisitos técnicos que se asociaban especialmente para sistemas críticos son cada vez más necesarios en la construcción de aplicaciones e infraestructuras públicas. En el tema de la gobernanza, la inclusión y colaboración contando con organizaciones neutrales como IEEE en organismos y comisiones supervisoras a nivel oficial, junto con el gobierno y otros actores, podría suponer un incremento en las garantías.

Cabe destacar, además, el papel creciente que se vislumbra para la administración electrónica, en el marco de implantación y diseño del paradigma de Internet de las Cosas (IoT) y su expresión más cercana de cara a los ciudadanos, como entornos contextuales y Ciudades Inteligentes. En este contexto, en el cual se potencia un intercambio masivo de datos, así como la automatización de los mismos, se abren nuevas oportunidades de interacción entre los ciudadanos, así como con diversos estratos de las administraciones. Todo ello es factible si se

analiza de manera detallada el reto de interoperabilidad y procesamiento masivo de datos.

La especificación de requisitos de calidad y su evaluación sigue siendo una tarea pendiente en nuestros esquemas de contratación, tanto pública como privada. En esta línea van estándares como SQuaRE ISO/IEC 25000 (*Software Product Quality Requirements and Evaluation*) que pretenden organizar y enriquecer este planteamiento respecto del propio producto software y no sólo del proceso de construcción. Para más información sobre este estándar aplicado a eGovernment se puede ver [15] donde se presenta una comparativa con modelos anteriores.

La iniciativa del IEEE Computer Society, la principal asociación internacional de profesionales de tecnologías de la información compuesta por miles de ingenieros de todo el mundo, para el diseño seguro y la identificación de defectos de diseño comunes [17] es significativa como una aproximación práctica a esta problemática que nos enlaza con las vulnerabilidades y nos introduce también en el área temática de la ciberseguridad.

2.3. CIBERSEGURIDAD E INGENIERÍA DE LA SEGURIDAD

En general la ciberseguridad es una preocupación social, pero especialmente se agudiza en épocas de recesión económica en parte consecuencia de que la industria mantiene importantes gastos relacionados con la seguridad de la información mientras que la ciberdelincuencia sigue aumentando [20]. Evitar

ataques continuos es un reto para el esquema clásico de negocios, especialmente en empresas encargadas de servicios e infraestructuras críticas como las relacionadas con energía, defensa o sanidad. Por ello, el modelo de organización empresarial actual debe incorporar la gestión de riesgos y controlar el balance de riesgo a asumir, lo que se traduce en poner límites a la hora de asumir riesgos para conseguir retornos beneficiosos. La ciberseguridad influye en esta falta de concienciación con respecto del riesgo que las empresas aceptan a fin de alcanzar sus objetivos económicos [24].

En el ámbito gubernamental la ingeniería de la seguridad está surgiendo como un perfil profesional que está empezando a normalizarse como consecuencia de la necesidad de administrar y gestionar la seguridad de la información. Por ello, el SEO, en su terminología en inglés (Security Engineeer Officer), es un rol con responsabilidades asociadas a la ciberseguridad, a la ingeniería y tecnología de la información que toma especial relevancia, como puede verse, por poner un ejemplo de tantos, en vacantes públicas en US [19]. Junto a los responsables de los sistemas de información (CIO) y la colaboración de los agentes sociales, especialmente asociaciones y organizaciones profesionales en áreas de ingeniería, el derecho o la criminología, se enfrentan a problemas de seguridad cada vez más persistentes y complejos. De hecho, se vienen sucediendo ciberataques sobre infraestructuras civiles y militares, incluido el Pentágono, que han hecho saltar todas las alarmas en Estados Unidos, siendo una dinámica en los últimos años que puede poner en jaque la estabilidad mundial [18].

Esto es parte también de la cultura de la ética cibernética y la ciberseguridad. No sólo en las instituciones públicas sino en las privadas, además, es necesario cambiar el modelo organizativo de tal manera que el riesgo cibernético sea considerado como parte del modelo de negocio. La ausencia de gestión de riesgos de los sistemas de información puede hacer que peligre la subsistencia de una empresa e incluso abre la puerta a nuevas empresas más ágiles en el entorno de la sociedad digital.

La globalización ha puesto de relieve el cambio de comportamiento de las personas en un entorno como Internet y en un mercado online abierto y cercano. Si bien la visión tradicional estaba centrada en los productos, este movimiento ha supuesto un acercamiento de la empresa a los consumidores y poner el foco en las personas. En lo público la demanda de atención de los ciudadanos cuestiona la efectividad de los mecanismos tradicionales de tipo burocráticos y en este caso abre paso a los sistemas basados en una mayor participación y centrados en el ciudadano.

En consecuencia, los avances en la sociedad de la información y el conocimiento que influyen en el comportamiento de las personas son realimentados por las nuevas demandas de servicios electrónicos y de los nuevos modelos de negocio. En las administraciones públicas destaca como resultado de este fenómeno la exigencia de una mayor transparencia a través de información de mayor calidad y formato de presentación de datos tratable por los usuarios finales. Con todo ello, las plataformas digitales de servicios online, la nube, la tecnología móvil, las redes

sociales y el Big data son el panorama de tendencias que se introduce en la ecuación sin resolver de la confianza digital.

2.3.1. PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

El mantenimiento de servicios considerados esenciales para la sociedad es una prioridad para muchos países. Fruto del libre mercado muchos sectores críticos de servicios públicos, universales y de interés general, están gestionados por empresas privadas. Esto se ha materializado en muchos países en desarrollos reguladores relacionados con estrategias de seguridad. En Europa la Directiva 2008/114 del Consejo de la Unión, pone la base para que cada país incorpore a su normativa nacional una serie de instrumentos de control y de gestión de las infraestructuras críticas. España concretó esta estrategia en la denominada Ley PIC (Protección de Infraestructuras Críticas, Ley 8/2011) y en un reglamento derivado (Real Decreto 704/2011). Los parámetros clave consisten en la integridad, bajo un punto de vista global, físico y lógico; la responsabilidad compartida entre lo público y lo privado; y una regulación eficiente que evite disfunciones entre los actores intervienes en la protección global y sectorial.

Pero a pesar del sistema garantista que la legislación pretende poner en marcha, la diligencia de las empresas va más allá de la normativa y parece claro que la implantación de una Cultura de la Protección de Infraestructuras esenciales para la sociedad es una actividad imprescindible para que el modelo PIC tenga éxito. De hecho, el Centro Nacional de Infraestructuras Críticas del Gobierno de España participa de numeras jornadas de intercambio y difusión de información de las

tecnologías que dan soporte a los servicios esenciales. En definitiva, las empresas deben utilizar todos los medios necesarios para solucionar y prevenir sus incidencias de seguridad, de tal manera que lo contrario, es decir, no tomar iniciativas de gestión de la seguridad, de evaluación del riesgo y salvaguardas, podría suponer una negligencia. Así aparece en la sombra el concepto jurídico de la "culpa in vigilando" donde los actores que participan en la sociedad digital para la prestación de servicios deben asumir las responsabilidades que de esa prestación corresponde ante una indisponibilidad o ataque externo aunque no sea consecuencia de una actuación dolosa.

Para evitar esto, una de las primeras medidas debe ser compartir las buenas prácticas y las lecciones aprendidas, así como el intercambio de información sobre amenazas, vulnerabilidades y respuestas ante incidentes.

Los principios básicos para una estrategia de ciberseguridad consisten en una fluida colaboración público-privada. Generalmente los sectores más delicados son los organismos públicos básicos, las tecnologías de la información y las comunicaciones, las centrales y redes de energía, el sistema bancario-financiero, el sector sanitario, la alimentación de la población y la red de abastecimiento de agua, el transporte y la seguridad vial, o la industria química y nuclear. Los recursos críticos además se miden por su impacto económico o social y la potencialidad de víctimas. De ahí que la colaboración sea fundamental en la consecución de los objetivos de seguridad global, incluyendo además a otros agentes como las organizaciones, colegios y asociaciones profesionales y el mundo académico.

2.3.2. DERECHO A LA INFORMACIÓN DE SEGURIDAD

Para contribuir a la cultura de la protección cibernética es apropiado establecer un estatuto de derechos de la ciudadanía y de las empresas para el acceso a la información sobre vulnerabilidades e incidentes de seguridad que abunde en la confianza en la e-Sociedad. Este derecho de acceso a la información de ciberseguridad se convierte en fundamental desde el mismo momento en que pasa a ser relevante para la protección de otros derechos, como la intimidad, la protección de datos personales o la defensa frente la ciberdelincuencia. Una de las dificultades extra que aparece es la de coordinar esfuerzos en armonizar el marco jurídico y las líneas de acción concretas para que la información sobre ciberseguridad esté accesible por los ciudadanos como un derecho en sí. Sin embargo, la interoperabilidad en ciberseguridad para estandarizar protocolos de comunicación organizativa y técnica en cuanto a incidentes es un reto atrevido, especialmente, por la publicidad y la proyección de la imagen corporativa que se imprime al delatar estos problemas, por muy buena intención que tenga.

La legislación española sobre Seguridad Privada reformada en 2014 (Ley 5/2014) disciplina como novedad una obligación de comunicar las incidencias de seguridad. Si bien el alcance del término seguridad es global, la norma incluye la seguridad cibernética por primera vez en este sector y la industria de consultoría informática deberá asumir esta responsabilidad adicional relacionada con el control público de la ciberseguridad. En consecuencia, las empresas cuyas actividades estén

relacionadas con la seguridad informática tendrán reglamentariamente requisitos específicos para garantizar la calidad de sus servicios.

2.3.3. DATOS PERSONALES

No obstante, hay otros aspectos impuestos por otras leyes que entran en juego, como por ejemplo en el orden de la privacidad de las personas con la Ley LOPD (Ley 15/1999) y el Reglamento Europeo de Protección de Datos, de cumplimiento directo, que ha sido aprobado por la Comisión Europea en junio de 2015. Entre los aspectos más relevantes de la norma supranacional está la regulación del derecho al olvido, mayores garantías de acceso a la información de los datos propios, el derecho a conocer cuando los datos personales han sido hackeados y la introducción del "principio de protección por diseño" donde se señala que la protección de datos debe venir por defecto en productos y servicios en los estadios tempranos de su desarrollo. Para ampliar información se puede consultar la base de legislación europea y otros detalles en [21].

2.3.4. SERVICIOS PRIVADOS DE CIBERSEGURIDAD

Los centros de operación de ciberseguridad (SOC) consisten en la prestación de servicios privados relacionados con la seguridad de redes y activos de clientes, en una funcionalidad equivalente en parte al de los equipos de respuestas ante incidentes CERT. La coordinación entre estos equipos nos sugiere que se debe

encontrar una sinergia entre ambos tipos de organismos que permitan mitigar las crisis cibernéticas de amplio espectro y que pueden afectar a un determinado sector del tejido empresarial o ciudadano.

2.3.5. CIBERDELINCUENCIA

La necesidad de una regulación relevante en materia de delincuencia en el ciberespacio, en el sentido de bien común de la Humanidad, pasa por el consenso internacional. Si bien los ciber-ataques se muestran globales en toda su potencia, las respuestas se realizan de forma fragmentada, a una escala estatal o nacional, cuya eficacia es excesivamente limitada. Como resultado, se observa un incremento de la ciberdelincuencia, el ciberespionaje, ciberterrorismo y las actividades antisociales. La persecusión de estos ilícitos se unen a los relacionados con los tipos penales tradicionales y la problemática de la regulación particular y el marco competencial de cada uno de los países que forman Internet. Esta contradicción deriva del axioma de la existencia de una sola Internet, o de que Internet es única pero hay cientos de legislaciones diferentes que la regulan según la ubicación, lagunas jurídicas y consecuencias negativas en la persecución de los delincuentes y la prevención de los delitos. La lucha contra la ciberdelincuencia necesita avanzar partiendo de la línea de consenso establecida en el Convenio de Budapest, suscrito por España en 2010 [18]. Esto queda patente con los datos presentados por el informe de 2014 sobre cibercriminalidad durante el año anterior elaborado por la Secretaría de Estado de Seguridad del Ministerio del Interior, que señala que apenas un 5% de los delitos cibernéticos pudieron esclarecerse [19].

2.4. CIBER-ÉTICA, EDUCACIÓN Y CONCIENCIACIÓN

La ciber-ética es una disciplina filosófico-técnica relacionada con los ordenadores y el comportamiento programado de éstos. Los códigos ciber-éticos más conocidos, como el RFC 1087 de los años 80 y el código de buenas prácticas del Departamento de Salud, Educación y Bienestar de Estados Unidos (1973), tienen bastantes años. La explosión tecnológica actual ha cambiado radicalmente el panorama de la ética en el ciberespacio.

La cultura de fomentar la ciber-ética va de la mano de la formación y la conciencia social en el ciberespacio, pero particularmente de la Educación para la Ciber-Paz. Los riesgos que afectan al factor humano, como es el caso de la ingeniería social, se abordan primordialmente con medidas educativas.

El modelo actual de sistema educativo debería incluir la urbanidad cibernética y la cultura de la ciber-ética y la ciberseguridad en todas las etapas educativas desde la educación infantil, primaria, secundaria, formación profesional hasta universitaria, adaptando los contenidos y procedimientos curriculares.

A nivel universitario las ingenierías necesitan fortalecerse con contenidos curriculares que resalten la calidad para asegurar los diseños y arquitecturas hardware y software de una forma trasversal durante la titulación. En las ciencias jurídicas, humanidades y sociales, incluso en otras ramas del conocimiento, debería añadirse la ciberseguridad y la filosofía del ciberespacio como una materia propia.

La educación secundaria, la formación profesional, la formación continua, los estudios de posgrados, la investigación y el desarrollo, las prácticas en empresas y las becas de formación deberían tener en cuenta también estos aspectos.

Al fin y al cabo la conciencia social no se hace en un momento, requiere un proceso y una madurez que sólo se obtiene si se prepara con antelación. Pero una manera flexible de ir creando esta conciencia social, a distintos niveles tanto técnicos como no técnicos, consiste en la creación de seminarios, jornadas de debate, talleres prácticos y conferencias que permitan la discusión y el contraste crítico de ideas.

Capítulo 3.

UN FRAMEWORK DISTRIBUIDO DE DEMOCRACIA ELECTRÓNICA

Internet ha revolucionado las formas de comunicación social y ha influido drásticamente en los canales tradicionales de socialización, en la producción literaria, prensa, radio y televisión. El número de usuarios conectado a la gran red mantiene una aceleración constante alcanzando prácticamente a la mitad de la población mundial a día de hoy.

Abordar el gobierno electrónico como herramienta real válida de gobierno democrático cobra relevancia, esencialmente en cuanto a legalidad, seguridad y fiabilidad. En este trabajo se presenta un framework distribuido de gobierno electrónico para dominios críticos de democracia y participación, con una clara intención de e-democracy escalable y que se adapte a la naturaleza de la participación ciudadana en las Smart Cities. En las secciones siguientes se expone un análisis sobre el fenómeno de la participación online (sección 3.1), los objetivos planteados (sección 3.2), el estado del conocimiento en e-democracia (secciones 3.3), la concepción del framework de e-democracia (sección 3.4), el desarrollo y experiencia un proyecto de investigación basado en arquitecturas desarrolladas (3.5), la investigación relacionada con extensiones del framework basada en e-voting (sección 3.6), así como la repercusión social de esta investigación y su evaluación empírica (sección 3.7).

3.1. ANÁLISIS GENERAL DEL FENÓMENO PARTICIPATORIO

Prácticamente el 40 por ciento de la población mundial, casi tres mil millones de habitantes, están usando Internet [25], de los cuales más de dos tercios corresponden a países desarrollados frente a una tercera parte de países en vías de desarrollo. Esta realidad refuerza la tendencia del incremento de la participación ciudadana en las decisiones públicas. Conforme a los datos agregados proporcionados por el organismo de la Naciones Unidas especializado en tecnologías de la información y las comunicaciones, conocido como la International Telecommunication Union (ITU), se ha elaborado en la Figura 5 una representación del crecimiento de la cantidad de internautas a nivel mundial a lo largo de los últimos años, con la especificidad de España, cuya tendencia se constata en consonancia con los países de su entorno. Los datos recogidos del último año son estimativos, obtenidos tanto del portal estadístico de la ITU [26] como, para el caso español, de [27].

El volumen y la influencia de Internet sobre los aspectos sociales, económicos y políticos internacionales tiene un gran impacto en la humanidad y en la vida de las personas, fenómeno que seguirá siendo indisoluble de la Sociedad de la Información y del Conocimiento de las próximas generaciones.

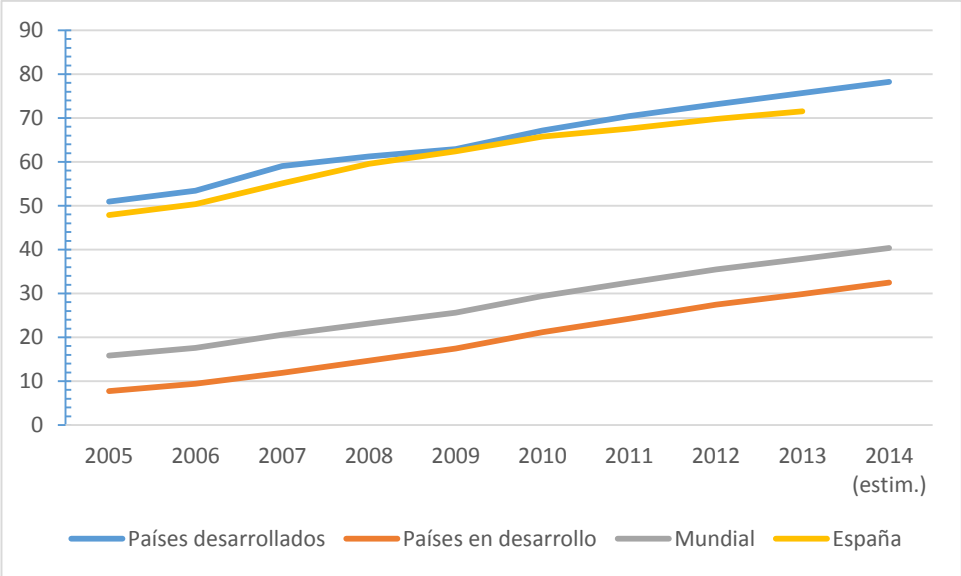


Figura 5. Porcentaje de internautas a nivel mundial

Sin embargo, hoy día la gobernanza de Internet no está centralizada, ni siquiera sigue criterios homogéneos en cuanto a implementaciones tecnológicas, normativa de uso, políticas de acceso o consideraciones de ética en el ciberespacio. No obstante, es cierto que Internet se sustenta en unos acuerdos básicos para el espacio de direcciones IP y el sistema de nombres de dominio (DNS) coordinada por el organismo internacional ICANN (Internet Corporation for Assigned Names and Numbers). Pero en el centro de estas preocupaciones trascendentes sobre el gobierno de Internet las Naciones Unidas consensuó la creación de un foro denominado Internet Governance Forum (IGF) que se reúne anualmente desde finales de 2006 y que viene organizándose en capítulos por países. En lo concerniente a IGF Spain, uno de sus objetivos principales es definir el papel de España en la gobernanza de Internet, incluyendo áreas como la regulación y tendencias en ciberseguridad y los recursos críticos para 2015, en la línea de trabajo de esta tesis, donde participan expertos de

distintas Universidades, Administraciones Públicas, empresas privadas y asociaciones profesionales [28].

Las redes sociales como elemento de opinión pública es una realidad de movimiento abierto en Internet. La tendencia de los últimos años posiciona el volumen de usuarios de redes sociales del orden de miles de millones, con una estimación lineal previsible de crecimiento en los próximos años. En la Figura 6 puede verse, en base a información estadística y prospectiva [29] dicha tendencia.

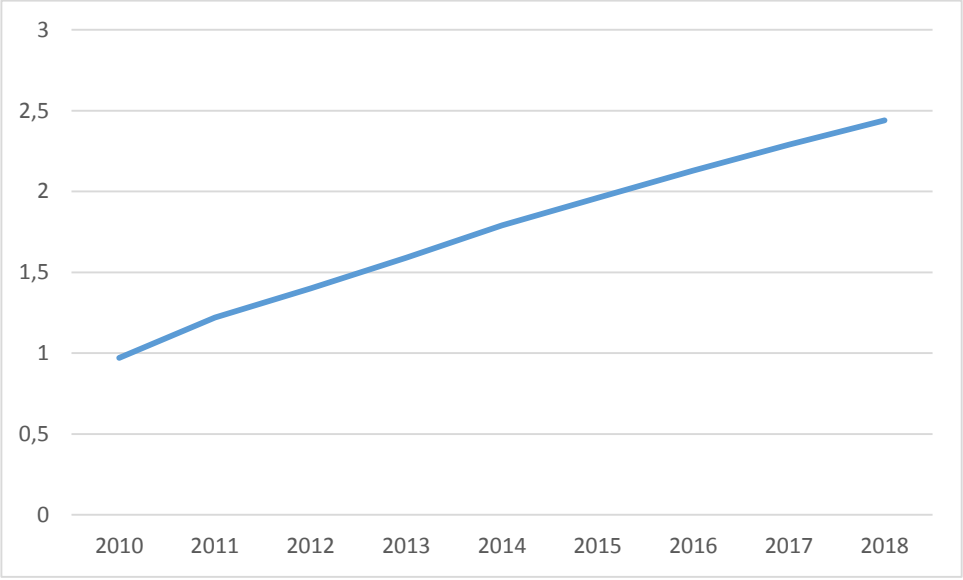


Figura 6. Volumen de usuarios de redes sociales a nivel mundial

Como consecuencia las redes sociales son un hervidero de opiniones y una fuente de influencia para los procesos de decisiones de políticas públicas. La valoración de los movimientos participatorios en la red choca en muchas ocasiones con la

representatividad derivada de las urnas y las decisiones de los políticos. Las redes sociales se están constituyendo en un factor importante a considerar en las campañas electorales, en la cercanía al ciudadano de a pie y en sondear sus preocupaciones de una manera relativa. Sin embargo, dicha valoración entra en la estrategia de decisión pública de una manera informal, cuando lo hace, y en gran medida depende de la sensibilidad política.

Las redes sociales como mecanismos de opinión contrastan radicalmente con la visión de las encuestas sociológicas institucionales, que reflejan de forma globalizada determinados barómetros sobre asuntos de actualidad sobre una muestra, son una herramienta tradicional que ha venido ilustrando a los núcleos de decisión durante las últimas décadas. Este es el caso español del Centro de Investigaciones Sociológicas (CIS) donde cuatro veces al año hacen una valoración de la opinión política, la intención de voto y estudios sociales [30] que vienen realizando desde su creación en 1963. Véase por su relación con lo que se viene argumentando la encuesta del CIS de 2014 a la pregunta "¿Con qué frecuencia suele conectarse a las redes sociales?" sobre una muestra de población N=1142 española y mayor de edad en la Figura 7.

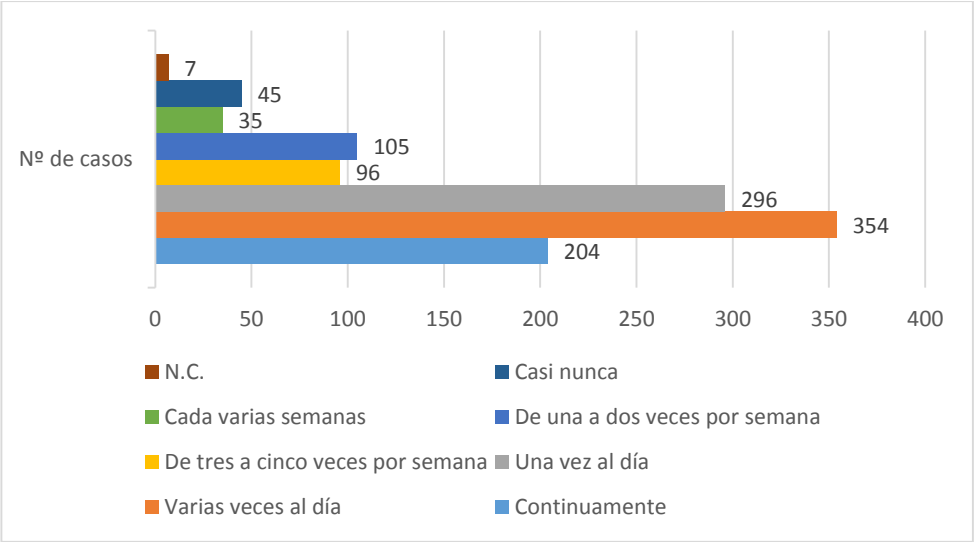


Figura 7. Encuesta CIS sobre frecuencia de uso de redes sociales

N=1142, España, 18+ años

Sin entrar en la metodología científica en sí, la visión tradicional del sistema de encuestas cumple un objetivo específico muy meritorio pero a veces limitado por su propia naturaleza. Los nuevos espacios de investigación sociológica necesitarán acoger las técnicas informáticas de análisis relacionadas con redes sociales y gestión del conocimiento.

Desde el punto de vista del proceso de decisión política, los propios movimientos ciudadanos online están exigiendo que la participación sea más directa y así lo están entendiendo con mayor o menor acierto los poderes públicos y los diferentes interlocutores políticos.

Por otro lado, el ciberactivismo como fenómeno de masas en Internet siente la necesidad de formalizar las opiniones online. Para ello surgen plataformas de adhesión,

semiencuestas o peticiones con el propósito de recopilar un número de apoyos de tal manera que puedan ponerse en conocimiento de alguna persona responsable, organismo o empresa. Ejemplo de ello son los portales de peticiones Change.org, DemocraciarealYA.es o Avaaz.org, de carácter independiente, e incluso otras con apoyo gubernamental como el caso británico de ePetitions (epetitions.direct.gov.uk). Las peticiones participativas se cumplimentan mediante suscripción online, es decir, escribiendo nombre y dirección postal, entre otros datos personales, y una mención de aceptación. Este mecanismo viene mencionado en ocasiones como firma online, si bien no debe confundirse con mecanismos de firma electrónica o procedimientos criptográficos de seguridad, ya que la confianza de la validación reside en la veracidad presupuesta del usuario y la responsabilidad de comprobación del destinatario.

La participación en el entorno de la democracia electrónica objeto de esta tesis no está orientada a la mera expresión de opiniones sino que tiene como objetivo que esta participación sea eficaz y tenga consecuencias reales en la actividad política a través de procesos de ingeniería. Para ello se organiza el framework en módulos arquitectónicos basados en dos tipos de plataformas. La primera orientada a la promoción de iniciativas legislativas ciudadanas directas para obligar al debate parlamentario y a la toma de decisiones políticas. La segunda plataforma modela los componentes tecnológicos que intervienen en el lado de la Administración Pública y el resultado del proceso de la toma de decisiones políticas de los gobernantes locales. Además se plantea la necesidad de establecer un protocolo de Internet para el intercambio de información de e-democracy que sirva para estandarizar y normalizar este dominio. El framework es suficientemente versátil para ser escalable, tanto a nivel

de servicio como funcional, en un entorno económicamente viable. Como resultado empírico, se presenta un proyecto de desarrollo que se ha puesto en marcha en un caso real de relevancia. Se muestra la experiencia de uso del proyecto sobre una iniciativa legislativa popular de interés cultural y con polémica social, con el que por primera vez el Parlamento español ha recibido firmas electrónicas como parte de un proceso de e-democracy, dando validez legal a la metodología y la tecnología en general para las iniciativas ciudadanas. Todo ello ha servido para llevar a la práctica el modelo propuesto.

3.2. OBJETIVOS Y ALCANCE

Con la aparición de las Smart Cities y las tecnologías ubicuas, el uso de Internet se postula como el canal de liberación de las preocupaciones sociales más cercana al ciudadano y un elemento de democratización en sí. Los ciudadanos y movimientos sociales demandan el derecho a poder expresarse y hacer oír su opinión con respecto a la vida pública y la situación política.

En este capítulo se verán los retos, las dificultades, las lecciones que se pueden aprender sobre estos puntos, a través de una aplicación desarrollada y puesta en producción, así como las inminentes necesidades de investigación en esta línea. Pero es obvio que cualquier investigación de esta naturaleza, inevitablemente, debe tener en cuenta la legislación del Estado. Sin embargo, la tendencia fáctica de las modernas naciones democráticas es impulsar la participación de personas y grupos en la vida

pública, a través de alguna forma de participación popular, incluida la elaboración de leyes y otras normas o impulsar referendos.

En muchas partes del mundo han regulado y por lo general se reconoce la autoridad de algún tipo de iniciativa ciudadana, y dependiendo del tipo de regulación, es de un carácter más o menos vinculante para el Gobierno en cuestión. Además, las iniciativas populares pueden aplicar a nivel local, regional o estatal.

En el ámbito de la democracia local ya en el siglo XIX las primeras comunidades rurales de Estados Unidos mantenían reuniones anuales donde todas las personas con derecho a voto tomaron parte directa en la toma de decisiones ("town-meetings"). Hoy día, con el avance tecnológico, no es necesario reunirse en un espacio físico, ni restringirse a sólo una vez al año, ni siquiera ser una pequeña comunidad. A través de redes sociales, los entornos de trabajo cooperativo, la ubicuidad y dispositivos móviles, el ciudadano digital se vuelve omnipresente y se convierte en un sensor muy valioso de la vida pública, de la generación de opiniones y de influencia en la toma de decisiones de los gobernantes.

El concepto del ciudadano-sensor es una tendencia relacionada con las tecnologías y el ejercicio de la ciudadanía responsable, donde junto con los sistemas de sensores que configuran las nuevas ciudades inteligentes para la medición de la actividad diaria [31]. El propio ciudadano ayuda al resto de la comunidad a formar opinión sobre las decisiones públicas. Las experiencias y el estudio sobre sensores-ciudadanos se utilizan en conjunto con líneas de investigación relacionados con "Living labs" o tecno-laboratorios ciudadanos [32].

En este sentido, se puede pensar en una forma de expresión de la democracia directa basada en las opiniones sociales electrónicas, ámbito que puede entrar dentro de la visión de la Internet of Things como una especie de "Internet of political things".

En definitiva, emerge con fuerza una nueva forma de gobernanza, íntimamente ligada a las tecnologías, con las oportunidades de acción de la ciudadanía y los aspectos sociales de la Smart City. La investigación y el desarrollo sobre la e-democracia es exigente principalmente porque debe tener en cuenta todos los fenómenos sociales innovadores y por otro todo el nivel tecnológico disponible y previsible.

3.3. ESTADO DEL CONOCIMIENTO SOBRE E-DEMOCRACIA

El fomento de la administración electrónica está en la agenda de todos los países, como puede verse en el informe bianual de las Naciones Unidas sobre e-Government [33]. La importancia y el impacto social y económico de las herramientas TIC gubernamentales hacen que sea imperativo invertir en investigación sobre arquitecturas tecnológicas y desarrollo de software orientada a contextos interoperables y reutilizables.

Por un lado, se define la democracia electrónica como una nueva forma de democracia donde se utiliza las tecnologías de la información y las comunicaciones para hacer más directa y extensiva la participación ciudadana en los asuntos públicos

y en los procesos de decisiones de los poderes gubernamentales. Esto incluye la elaboración de normas legales y las decisiones basadas en referéndum, fórmulas usadas en los países donde tienen un mayor implante los mecanismos de democracia directa.

Por otro lado, la participación electrónica se refiere al uso de tecnologías para facilitar la participación ciudadana en las actividades de las Administraciones Públicas en general [34]. Esto hace que a veces se aplique a la democracia electrónica sin olvidar su concepción más amplia.

En la literatura tanto tecnológica como de ciencias sociales, se ha realizado un esfuerzo por modelar el dominio de la e-democracia especialmente desde los inicios de la globalización de Internet. No obstante, el punto de partida surge de la visión clásica de la democracia en la antigua Grecia, si bien hay actualmente un interés emergente, sin obviar la retrospectiva histórica, para el estudio del papel de las TIC en relación a la participación ciudadana. Conforme a la filosofía de Platón la forma de gobierno se organiza en monarquía, aristocracia o democracia, en función de si gobierna uno, unos pocos o la multitud. Por un lado, la democracia es indirecta o representativa cuando las decisiones políticas se toman por personas que representan a los demás. Por otro lado, la democracia se considera directa cuando todos los miembros de la ciudadanía pueden participar directamente la toma de decisiones. Un concepto relacionado a mitad de camino es la democracia participativa o semidirecta que viene a referirse a los mecanismos de participación directa mediante alguna forma de plebiscito, referéndum, votaciones o iniciativas legislativas populares.

Con la llegada de la revolución de la Sociedad de la Información, los estudiosos de las ciencias sociales y políticas han vigorizado las ideas de democracia digital, proponiendo variantes del concepto de democracia derivado del uso de Internet y de la universalización de la tecnología informática. Un ejemplo de ello son las ideas de democracia líquida donde se intenta insertar dentro del esquema de representación parlamentaria la votación digital individual de los ciudadanos. Otra corriente de gran interés es la teoría de la" Strong Democracy", también llamada democracia ciudadana, de Benjamin Barber [35] donde incluye muchas de las ideas actuales para la regeneración democrática donde pone en un primer plano al activismo político personal, la participación, solidaridad social y altruista frente al liberalismo de un grupo representativo denominado como clase política. Esto ha derivado en intentos de diseñar y por ello construir marcos tecnológicos para la democracia fuerte ha preocupado y ocupado a ingenieros en los años recientes [36].

En 2000 Gross [37] desde un punto puramente técnico nos plantea un punto de partida determinando las capacidades básicas necesarias para desarrollar la democracia electrónica: el acceso a la información, la apertura al diálogo de asuntos políticos y el voto electrónico. El acceso a la información implica ciudadanos mejor formados, lo que permite un proceso con mayores garantías. La apertura supone la interlocución directa entre los ciudadanos y los políticos que toman las decisiones. Y el voto electrónico culmina este conjunto de requisitos con las ventajas temporales y espaciales que supone, a pesar de que siguen perdurando retos para su puesta en marcha efectiva, como la gestión del cambio social y la seguridad de la información,

especialmente la autenticación y la confidencialidad. Pero no sólo estas características de seguridad convierten en inusual la práctica efectiva del voto electrónico, también está la disponibilidad que se enfrenta a fallos, accidentales o intencionales, vulnerabilidades y el avance sofisticado del malware.

Del estudio de los proyectos TIC en relación a la e-participación se aprecia que resulta más complicado abordar proyectos con parámetros de seguridad de identificación robusta de los usuarios. En [38] se presenta un inventario de herramientas que advierte de estas dificultades, así como de la tendencia diáfana de la computación móvil para articular la participación ciudadana.

La aportación de Kalampokis y colaboradores por evaluar el dominio de e-participation [39] para la caracterización de herramientas TIC, realizada mediante lenguaje de modelado UML, deja claro que intervienen tres grandes paquetes abstractos de funcionalidades: las relacionadas con las partes intervininentes (stakeholders), las propias del proceso y las herramientas informáticas. Aunque este trabajo de 2008 ha quedado superado por la irrupción de otros canales, como redes sociales, cloud computing o Smart cities, el propósito sigue siendo útil desde el punto de vista conceptual.

Como consecuencia de la puesta en marcha de diferentes soluciones de e-Government, en general, y de e-partipación en particular, surge la necesidad de poder establecer características que sirvan para realizar comparativas entre ellas y evaluar el éxito de las iniciativas, lo que da lugar a una productiva línea de investigación como la propuesta en [40], donde se sugieren la accesibilidad, la información relevante y la calidad relacionados con la comunicación con los ciudadanos. En [41], Macintosh

sugiere diez dimensiones clave para caracterizar la participación, lo que a la postre supone un decálogo de buenas prácticas tecnológicas para la e-participación. Las dimensiones son: nivel de participación, el escenario de la decisión, los actores involucrados, las tecnologías utilizadas, las reglas para recopilar la información personal, la duración y sostenibilidad, la accesibilidad de los ciudadanos, los recursos y promoción publicitaria, la evaluación de los resultados y los factores críticos políticos, legales, culturales, económicos y tecnológicos.

A nivel municipal se ha pretendido contextualizar la democracia electrónica [42], el uso de tecnología móvil [43] y su influencia en el cambio social [44]. Otros casos de estudio buscan poder contribuir con soluciones específicas para los procesos de participación, como en [45]. Como se puede ver en la literatura, aparentemente, establecer un modelo global no es fácil; de hecho, la investigación sobre e-participación sigue evolucionando rápidamente en los últimos años.

Pero a la vez que el uso de herramientas informáticas para la participación electrónica va tomando madurez, han venido irrumpiendo recientemente el despliegue de tecnologías relacionadas con las Smart Cities [46]. Ello provoca un nuevo panorama y un cuestionamiento de las relaciones sociales alrededor de la tecnificación de las ciudades y por tanto en la propia participación ciudadana. Las ciudades inteligentes parten de la visión de una compleja infraestructura de Smart Grid con un sistema de monitorización de grano fino, con cierto nivel de detalle, y el control de los dispositivos sensores y actuadores físicos con el objetivo de conseguir mayor eficiencia y mejor servicio a la ciudadanía. Ejemplo de ello son los sensores medio ambientales, de

polución, los de control de tráfico, consumo de energía, etc. Pero también uno de los parámetros principales que se evalúa para medir las Smart Cities es su nivel de gobernanza participativa.

En esencia las ideas de la participación política y la ayuda a la toma de decisiones cambia desde el momento en que la tecnología se vuelve omnipresente (pervasive) en la vida de los ciudadanos. La literatura refleja un interés alto por el desarrollo tecnológico relacionado con el *Urban Computing*, especialmente con aspectos que pueden ser aplicados a la vida diaria de las personas [47]. Algunos autores consideran que a pesar de la complejidad, se trata de un fenómeno de masas que ha redefinido el espacio urbano, los aspectos físicos, estéticos y funcionales. Además, esto afecta a la mitad de la población mundial, que reside en núcleos urbanos, que tiene una mejor capacidad de conectividad y un creciente número de dispositivos móviles e infraestructura relacionada. Sin embargo, los pensamientos o las opiniones ciudadanas, la participación y los procesos de toma de decisiones no han sido suficientemente investigados desde esta perspectiva. En este sentido, se encuentran trabajos que muestran la complejidad de tratar esta información, como puede verse en [48] donde el prof. Carenini, y otros, nos presenta el reto de usar técnicas de procesamiento del lenguaje natural (NLP) para la comunicación entre el ciudadano y las Administraciones Públicas. Ciertamente esto es una muestra de la prolijidad de esta área y la necesidad de buscar soluciones ingenieriles para la realidad social [49].

Uno de los vértices de esta tesis está en la participación de los ciudadanos para la toma de decisiones en relación la gobernanza electrónica. Como ya se ha presentado, la interoperabilidad juega un papel importante, pero no sólo en lo que concierne a las TIC. Se entiende el concepto de interoperabilidad como un principio

fundamental que va más allá de la implementación técnica. La gobernanza está íntimamente relacionada con la visión moderna de interoperabilidad, como se puede observar en trabajos recientes sobre eGovernment. Siguiendo con el tema la investigadora social Mila Gascó [50] y tecnólogos como Jimenez [51] que han estudiado la interoperabilidad desde distintos puntos de vista, se concluye que la interoperabilidad en el gobierno electrónico es un concepto cuyo eje no es sólo tecnológico sino que intervienen aspectos de relaciones institucionales internacionales. En un primer lugar la interoperabilidad técnica se alcanza especialmente a través de estándares y protocolos, canales y mecanismos de comunicación entre sistemas de información, congeniándose en un conjunto de características y elementos físicos de interconexión. En un segundo lugar, la interoperabilidad semántica orientada a la interpretación adecuada de los significados objeto de comunicación, para lo que se utilizan sistemas de clasificación, tesauros, metadatos y ontologías.

La necesidad de interoperabilidad llega a ser evidente en el informe de e-Government que la Organización de las Naciones Unidas publica en años alternos. Si bien en 2012 se subrayó la necesidad de estándares comunes a través tecnologías interoperables para habilitar la posibilidad de compartir e integrar la información en el sector público, en el siguiente informe de 2014 las Naciones Unidas menciona como uno de los grandes retos la gobernanza colaborativa y la interoperabilidad en el ámbito del e-Government, cuestión reconocida que va más allá de lo puramente tecnológico [33]. Esto supone la asunción de facto de que el papel de las herramientas informáticas como elemento clave para el Gobierno electrónico ha perdido su posición de liderazgo

tradicional. El foco de interés de la comunidad científica se apoya en la idea de que la tecnología es importante pero no es eficiente ni efectiva sin ponderar a un nivel suficiente otros factores que tienen significación: las personas, las leyes, los recursos y las condiciones sociales.

Así como en los aspectos tecnológicos de interoperabilidad, visto desde la perspectiva general de e-Government, es esencial establecer mecanismos para resolver los problemas comunes, como arquitecturas y protocolos, no es menos cierto que cada país puede tener implementaciones que pueden hacer inviable la gobernanza colaborativa. Por consiguiente un modelo relevante debería considerar la eficiencia de la implementación o un diseño detallado de la interoperabilidad, una idea que se sigue en esta tesis en relación con la democracia ciudadana.

En otro orden de cosas, la concepción de la colaboración público-privada (PPP) favorece el crecimiento económico y el enriquecimiento. Es importante dentro de la gobernanza electrónica, tanto en las Smart Cities [52] como en zonas territoriales más amplias, alcanzar un fuerte compromiso con la participación pública, como demuestran los baremos de evaluación de Smart Cities [53]. Esto último determina el acuñamiento de un concepto más adjetivado como es el de gobernanza inteligente.

De hecho en 2014 la Unión Europea en relación a la actividad de las ciudades inteligentes europeas [54], hace un estudio donde sobresalen aquellas ciudades que buscan dirigir sus asuntos públicos a través de soluciones informáticas, dando la oportunidad de intervenir a distintas partes interesadas. El trabajo presenta información del análisis de 468 grandes ciudades y clasificadas en función de un ranking establecido. Las conclusiones de la UE apuntan a encontrar soluciones que

sean más escalables, que permitan propagar y reproducir los proyectos TIC en otros lugares y crear una postura común para el desarrollo de las Smart Cities.

La brecha digital sigue siendo uno de los grandes retos para el gobierno electrónico. Sin embargo, el interés de los gobiernos por la e-participación y el crecimiento de los canales ubicuos a través de telefonía móvil han hecho mejorar algo la situación.

Entre las tendencias mundiales a destacar está la de considerar la posición de los ciudadanos centrada respecto de todo el proceso de participación electrónica, pasando de un status pasivo tradicional a otro claramente activo. De esta manera se ha consolidado un esquema general de clasificación de soluciones TIC según la posición del ciudadano, a tres niveles: e-información, e-consulta y e-decisión. La referencia al último nivel demuestra alguna capacidad significativa de participación en la política pública y en la posibilidad de co-producir servicios públicos. Una estrategia efectiva para mejorar la e-participación es la desconcentración y descentralización de la gobernanza, facilitando a los ciudadanos y sus comunidades el acceso a la información y una mayor calidad en la respuesta a las necesidades sociales.

En definitiva, el núcleo de este trabajo de investigación se centra en poder definir un modelo de dominio de la democracia electrónica, que incluya el entorno de las Smart Cities. De ahí se necesita determinar si es preciso un nuevo modelo de participación política, básico para el apoyo a la toma de decisiones, pragmático, versátil y económicamente viable. Esto es, establecer un framework donde las opiniones

ciudadanas sean parte del "Internet of Thing" de las cosas en el plano político, una especie de "Internet of Thoughts".

3.4. LA CONCEPCIÓN DEL FRAMEWORK

En gran medida los sistemas de e-democracy investigados se conciben como herramientas TIC de una capa plana, donde funcionalmente la Administración Pública proporciona todo el ciclo de vida de la participación a nivel técnico. Esto supone un esfuerzo de eGovernment y un liderazgo tecnológico de la propia entidad pública. Consecuentemente, las iniciativas de los grupos sociales y de los ciudadanos dependen del nivel de gobernanza y recursos públicos, especialmente económicos.

La idea que se presenta trata de investigar qué parte tecnológica de la Smart Governance es esencialmente responsabilidad de la parte pública y, por otro lado, qué pueden asumir las entidades no públicas: movimientos o grupos de ciudadanos, asociados o no en entidades privadas. Es necesario definir un framework donde se puedan estandarizar los servicios electrónicos de e-democracy. Por un lado, los imprescindibles para el funcionamiento de la labor asociada a validez y verificación de los requisitos gubernamentales y, por otro, las competencias que pueden ser atribuidas a iniciativas ciudadanas.

De ahí que el marco de trabajo se define por las partes interesadas (stakeholder), el proceso de participación y por una arquitectura distribuida organizada en una plataforma dual, como se explica a continuación tras la identificación de las partes interesadas y del proceso participativo. La primera parte de la plataforma tiene por objeto la promoción de iniciativas ciudadanas directas para fomentar la discusión y elaboración de políticas. La segunda describe un modelo de componentes que

intervienen en el lado tecnológico de la Administración Pública y el resultado del proceso de toma de decisiones políticas de los gobernantes.

3.4.1. LOS ACTORES

Los actores representan en el framework las partes interesadas que participan del sistema: el actor ciudadano (Citizen Stakeholder), el grupo de ciudadanos o promotores sociales (Citizens' group – sponsoring) y el actor de gobernanza electrónica que representa las partes interesadas con responsabilidad pública.

Citizen Stakeholder: Los ciudadanos dan su opinión subscribiendo una iniciativa que se formaliza mediante un texto de propuesta.

Citizens' group / Sponsoring Stakeholder: Los movimientos sociales y los ciudadanos son protagonistas principales y activos. Así una iniciativa de opinión se promueve y se enfrenta al juicio del resto de ciudadanos, y cuyo resultado refleja la opinión colectiva.

Governance Stakeholder: Los responsables políticos son la otra parte a tener en cuenta, ya que recogen las opiniones colectivas de una forma cuantitativa y fiable.

3.4.2. EL PROCESO

El proceso debe cumplir con los siguientes requisitos: estar preparado para que los ciudadanos puedan firmar electrónicamente, mediante criptografía robusta, la

propuesta de un proyecto de ley privado; almacenar las suscripciones; facilitar la presentación de ellos, y proporcionar una solución de servicio para la validación.

Por lo tanto, la iniciativa de participación se pone en movimiento mediante la presentación de un texto a un Comité de Gobierno, Asamblea o Parlamento, el ejemplo de un grupo de ciudadanos que es un Comité de Patrocinio.

Por lo general, un órgano de gobierno considera si acepta o no la propuesta, con el fin de comprobar los requisitos previos. Una vez que se ha dado permiso para proceder, se comienza a recolectar suscriptores. La Figura 8 muestra un diagrama conceptual del proceso.

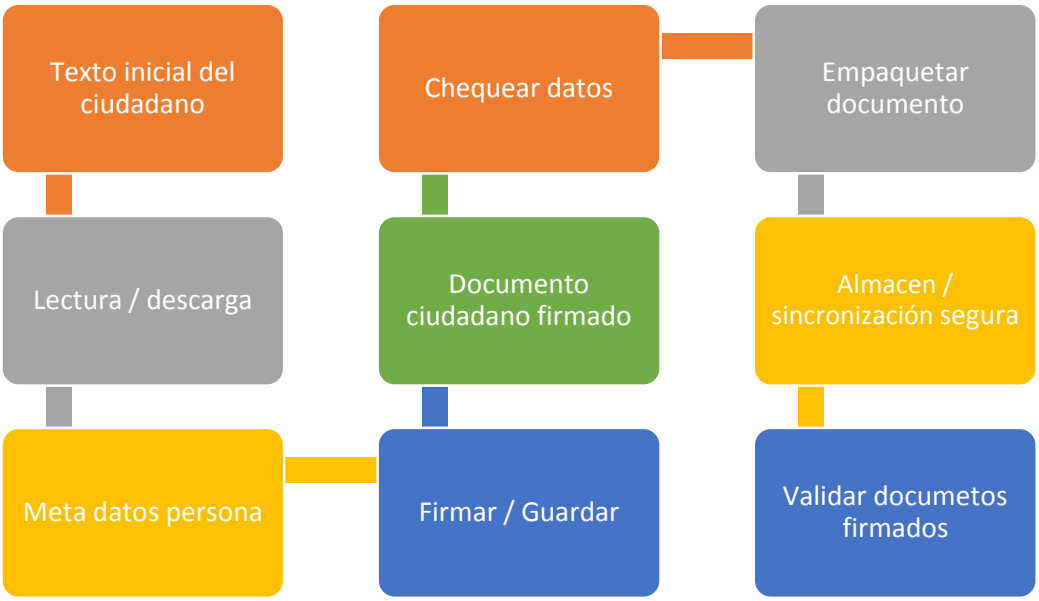


Figura 8. Diagrama conceptual del proceso

En consecuencia, el marco debe presentar un sistema de firma digital y un sistema para verificar las firmas digitales u organismos gubernamentales que proporcionan un estándar.

Para ello se requiere garantizar que el proceso se ajusta a unos criterios básicos de seguridad. Se considera de aplicación directa el modelo del triángulo CIA: confidencialidad, integridad y autenticidad.

En la Figura 9 se presenta un modelo de arquitectura para el marco y los módulos significativos implicados. Se muestra una plataforma de ingeniería distribuida basada en la integración de sistemas, en dos partes: promoción de los ciudadanos y arquitectura de e-Government.

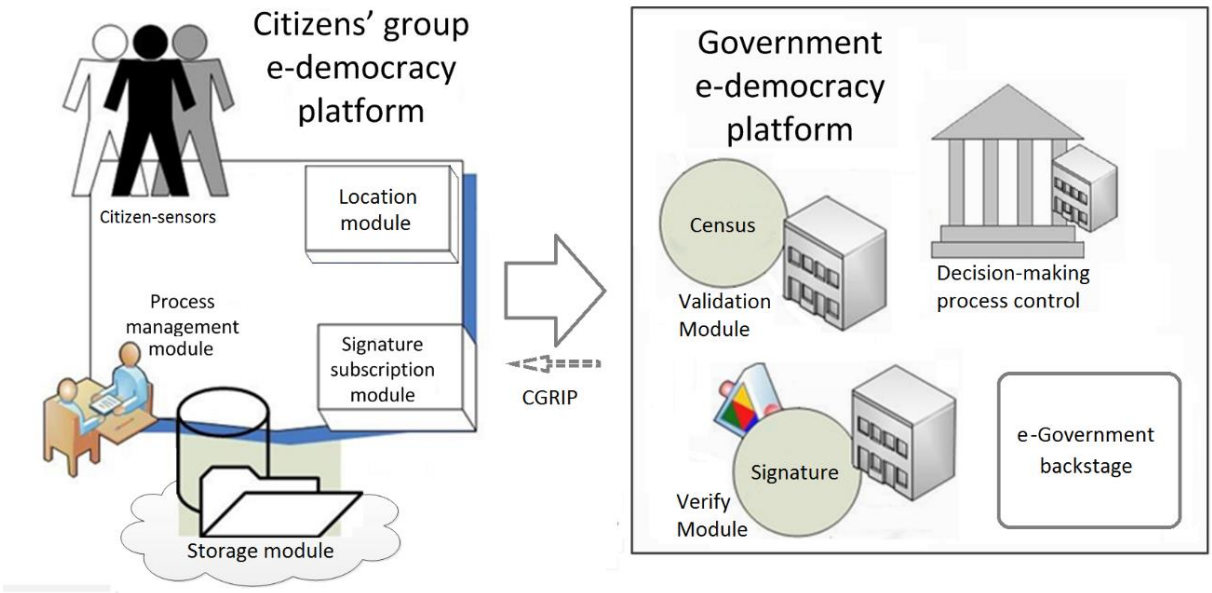


Figura 9. Visión arquitectónica del framework

3.4.3. PLATAFORMA PARA LA CIUDADANÍA

Esta plataforma de e-democracia de grupo de ciudadanía (Citizens' group e-democracy platform) contiene los módulos necesarios para que los ciudadanos o grupos de ciudadanos desplieguen las operaciones de participación democrática necesarias para recoger todas las adhesiones, subscripciones o firmas en apoyo de iniciativas políticas de su propio interés. Esta plataforma va a consistir principalmente de los componentes software:

Citizen-Sensors Module (CSM): Son los actores principales de la participación ciudadana. Se presenta en el sentido de ciudadanos como sensores de la opinión política plasmada a través de una iniciativa democrática directa y en el entorno de las Smart cities esta percepción toma mayor protagonismo, gracias a la computación ubicua y onmipresente (pervasive).

Process Management Module (PMM): Es el motor de flujos de tareas que define el proceso de participación ciudadana. Implementa funcionalmente la definición de actividades necesarias para llevar a cabo la elaboración, publicación y puesta a disposición de las propuestas políticas, conforme se modela en la Figura 9.

Storage Module (SM): Este subsistema responde a la abstracción de la necesidad de almacenamiento de todo el proceso, especialmente el almacén de firmas digitales. Conceptualmente es un almacén flexible relacionado con sistemas de ficheros (Filesystems Storage Module – FsSM), de bases datos (Databases Storage Module - DbSM), sincronizadas o centralizadas de forma distribuida, y/o en la nube (Cloud computing Storage Module – CcSM) .

Cuando el módulo de almacenamiento está en la nube (CcSM) se debe contemplar en especial, además del enfoque técnico, los reglamentos y las necesidades de la administración pública, así como por otro lado las cláusulas de los contratos de los proveedores de servicios de cloud. Esta idea está relacionada con el concepto de gobernanza en la nube y el gobierno como plataforma [55], un paradigma que puede ser aplicado en función del nivel de los requisitos de servicio y de gobierno.

Signature-Subscription Module (SSM): Consiste en un componente concebido como un elemento público cuyo desarrollo debe abordarse de forma independiente del módulo de verificación de la firma electrónica. El módulo de firma-suscripción digital sobre esta arquitectura se basa en la firma robusta que garantiza unívocamente a un ciudadano. Un ejemplo que se puede anticipar puede ser el uso de certificados digitales X.509v3, en concordancia con el estándar RFC 3280, sin necesidad de que la clave privada asociada con el certificado salga del contenedor del cliente. Además algunas consideraciones sobre formatos de firma pueden incluir: PKCS#7, CMS en el sentido del RFC 3852, el estándar ETSI XAdES, el estándar de firma XML W3C de XMLDsig, PAdES para firma PDF y firma para documentos ofimáticos, entre otros.

Location Module (LM): Es una abstracción de un componente que describe una ubicación sobre la que se podría aplicar la participación ciudadana. Es un concepto versátil, que debe adaptarse a los requerimientos específicos del proceso de participación. Puede concretarse en un cliente de geo-posicionamiento, una interacción del usuario-ciudadano, o cualquier otro mecanismo de delimitación del alcance.

3.4.5. PLATAFORMA GUBERNAMENTAL DE E-DEMOCRACIA

Esta segunda plataforma de e-democracia de gobierno electrónico (Government e-democracy Platform) contiene los módulos necesarios para que las agencias gubernamentales desplieguen las operaciones de democracia electrónica necesarias para mantener el censo ciudadano y las funcionalidades de validación relacionadas, la firma electrónica y su verificación, el control del proceso de decisión y la integración con el backstage. Los componentes de la arquitectura fundamentales de la plataforma son:

Census-Validation Module (CVM): Este es un componente que modela las reglas funcionales propias en el dominio del proceso de participación. El objeto principal que se gestiona es el censo de población sobre el que se interactúa. Son reglas del dominio la residencia, edad, estar en plenas facultades civiles y mentales, la localización geográfica requerida en el ejercicio de la opinión, etc. La validación de estos requisitos para la participación definen el alcance en la toma de decisiones y, por consiguiente, su validez para los responsables políticos.

Signature-Verify Module (SVM): Este componente verifica el ejercicio de la participación digital, la subscripción, adhesión o firma electrónica de una persona. La verificación depende de la política establecida de autenticación para la participación y de los criterios de seguridad para comprobar la identidad de los ciudadanos por vía telemática. Un criterio de autenticación fuerte podría consistir en la identificación mediante firma electrónica con certificado digital. En cambio, un criterio de

autenticación débil sería mediante desafío y comprobación de datos personales que razonablemente debe conocer el sujeto. Pero hay más formulas, como la autenticación del terminal o dispositivo ubicuo desde el que se conecta o la verificación de la geo-posición.

Decision-Making Process Control (DMPC): Es el núcleo del sistema en la parte gubernamental, aglutina el conjunto de funcionalidades necesarias para la gestión y el control del proceso de participación. Coordina la validación de los participantes y la verificación de las participaciones.

e-Government Backstage (eGB): Es un conjunto de componentes que abstrae los sistemas de información previos o heredados (legacy) de los organismos públicos. Típicamente pueden incluir otros sistemas de gestión, ERP, otras bases de datos o repositorios de almacenamiento de apoyo o subsidiarios que forman parte de la infraestructura general de gobierno electrónico.

3.4.6. PROTOCOLO DE INTERNET DE RELACIÓN CIUDADANÍA Y GOBIERNO ELECTRÓNICO

Esta investigación introduce un protocolo de intercambio de información CGRIP (Citizen Government Relashionship Internet Protocol), necesario para la escalabilidad y operatividad real de la arquitectura de e-democracia propuesta. Las dos partes bien diferenciadas, grupo de ciudadanos y administración gubernamental, constituyen un

par de interlocutores. Cada par necesita definir algún tipo de reglas de comunicación, para el intercambio de información sobre el proceso de participación ciudadana. El fundamento principal de esta definición se basaría en acordar un protocolo de comunicaciones por Internet sobre la capa de red de aplicación. Un aspecto importante sería el uso de formatos interoperables (XML, JSON), ontologías semánticas y conectores basados en servicios web.

Un aspecto trascendente resulta de considerar la escalabilidad del sistema. Cuando las plataformas electrónicas de movimientos sociales aumentan sobre la misma plataforma de e-Government el volumen de reglas de comunicación puede hacerse difícil de manejar. Mucho más si las plataformas son heterogéneas.

La Figura 10 muestra una instanciación del modelo para una Smart City que nos sirve de esquema para visualizar el framework con tres plataformas ciudadanas, cada una puede corresponder a una implementación tecnológica heterogénea o no. De esta manera, definiendo el protocolo el intercambio de información se estandariza.

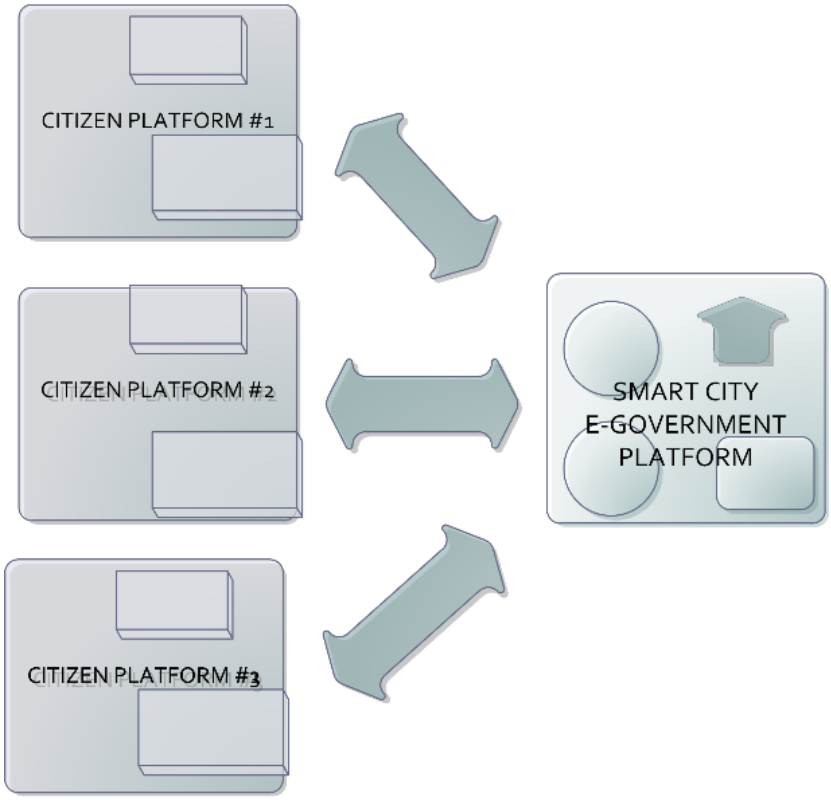


Figura 10. Instancia del framework en grado 3

Este protocolo de intercambio de información es necesario para la escalabilidad, interoperabilidad y la eficacia real de la arquitectura propuesta e-democracia. Las dos partes bien diferenciadas, el grupo de los ciudadanos y la administración del gobierno, constituyen un par de interlocutores.

Cada pareja tiene que definir algún tipo de regla de comunicación para el intercambio de información sobre el proceso de participación. Al margen de su concreción la definición del protocolo consiste en una especificación formal para la interoperabilidad de las soluciones de e-democracia sobre la capa de Aplicación en la pila de red (capa superior de la pila de red, ISO / IEC 7498-1 o TCP / IP). Esto supone

en sí una investigación con una diáfana visión de estandarización en el entorno de organismos de normalización como puede ser el Instituto de Ingeniería Eléctrica y Electrónica (IEEE).

La interoperabilidad del sistema es una característica fundamental que debe tomar consideraciones globales, multistakeholder y multidisciplinares.

La Figura 11 muestra un diseño del modelo de un ecosistema Smart City que serviría como un ejemplo para la visualización de la estructura con tres plataformas ciudadanas y tres niveles de gobierno electrónico. En este tipo de ecosistemas se ha definido los conceptos de grado y nivel como se expresa a continuación:

Grado.- Valor que representa la cantidad de plataformas ciudadanas diferentes que interactúan con una plataforma gubernamental dentro de la arquitectura.

Nivel.- Valor que representa la cantidad de plataformas de gobierno electrónico diferentes que intervienen en el dominio de la realidad.

Cada plataforma ciudadana y gubernamental puede o no haber sido desarrollado con una tecnología de aplicación heterogénea. De esta manera, mediante la definición del protocolo de intercambio de información (CGRIP), el sistema se puede presentar de forma estandarizada.

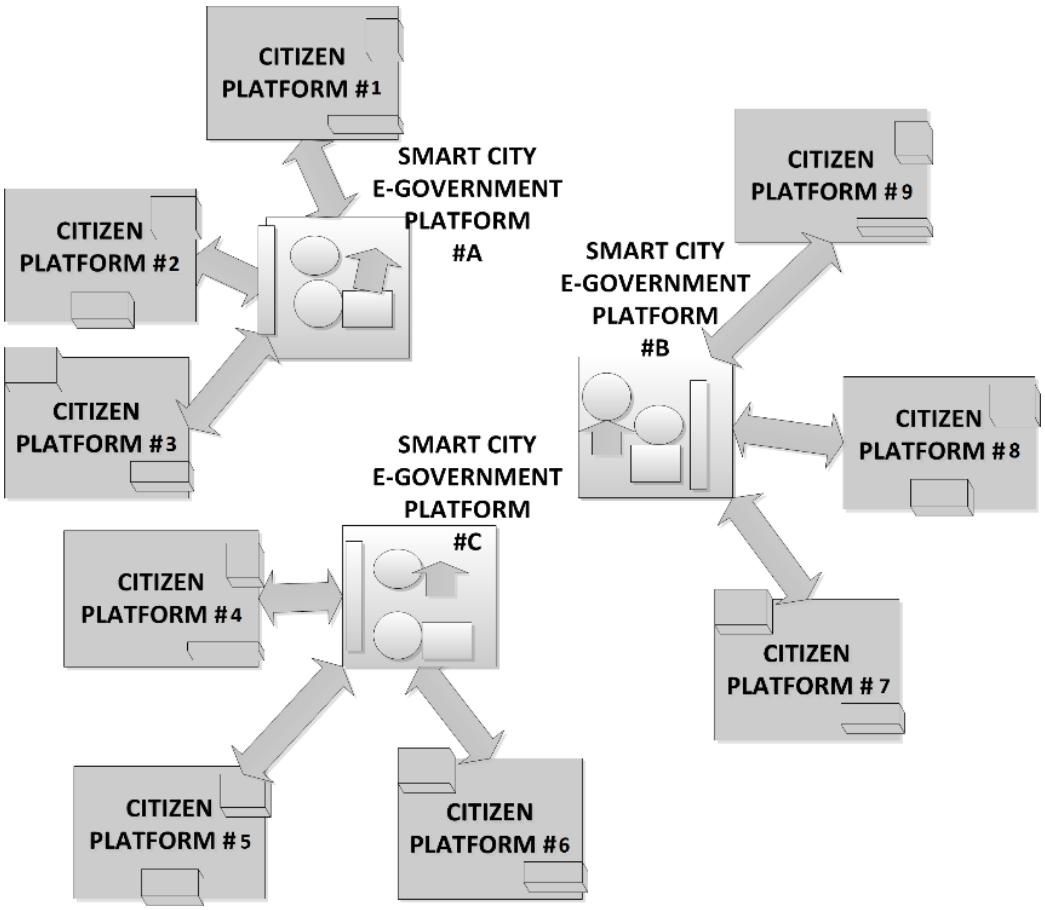


Figura 11. Un ecosistema de e-democracia de nivel 3 y grado 3

Esta arquitectura de sistemas distribuidos conduce a la interoperabilidad entre plataformas ciudadanas, incluso a través de diferentes ciudades inteligentes. Su versatilidad se revela en la mancomunidad de servicios donde algún módulo se puede ampliar para dar servicio a varios módulos cuyo servicio puede ser en común. La Figura 12 ilustra un ejemplo de esta posibilidad tomando el ecosistema de ejemplo.

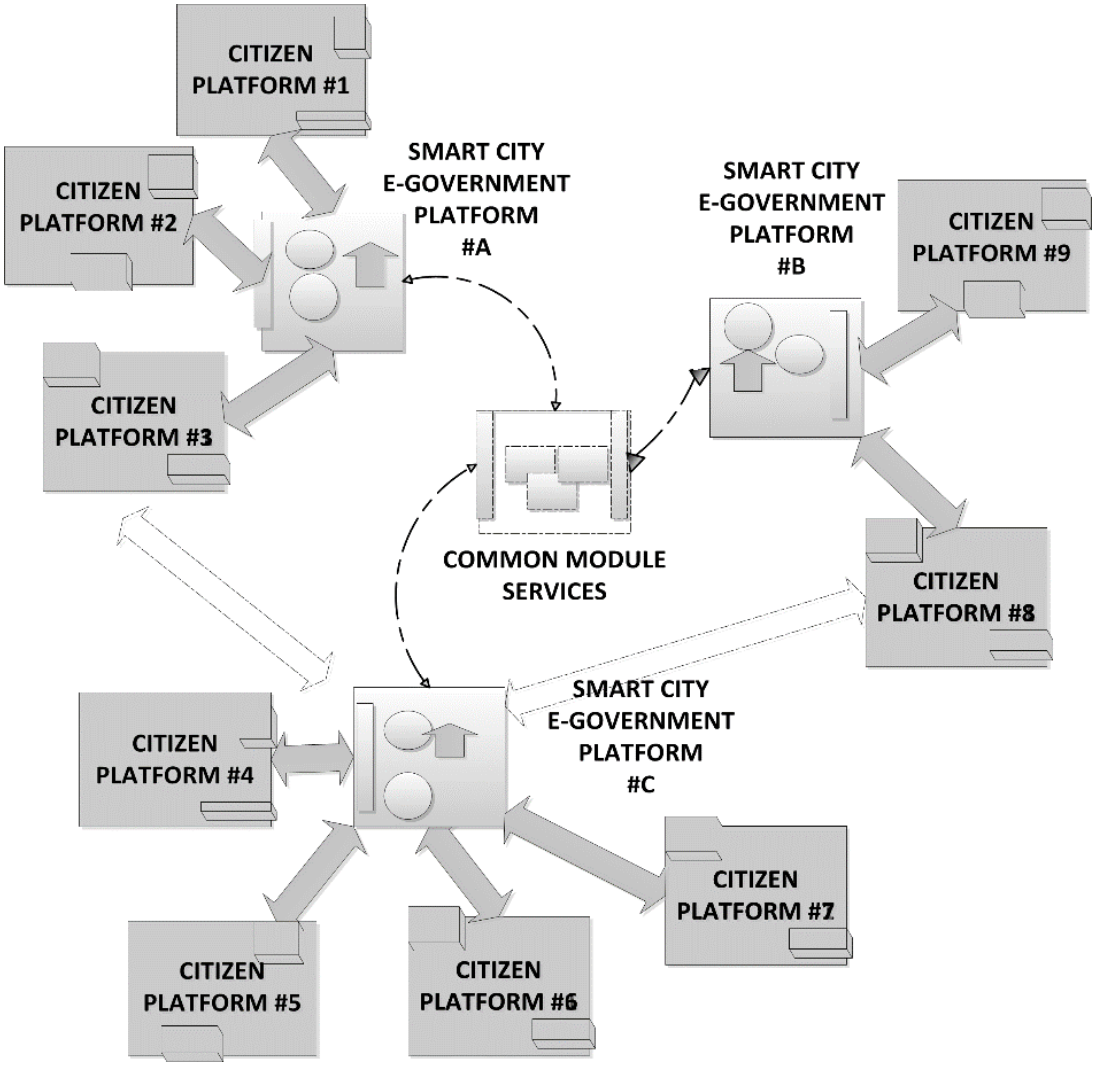


Figura 12. Ecosistema de e-democracia, nivel 3 interrelacionados

3.5. DESARROLLO DEL PROYECTO OPENILP

El proyecto OpenILP es un ejemplo de solución de ingeniería informática para el marco propuesto y, específicamente, una implementación del Grupo de Plataformas e-Democracia de Ciudadanos. Está enfocado a la iniciativa popular. El objetivo de este trabajo es dar a conocer este proyecto como software libre con el propósito de "liberar" a las personas en el poder promover iniciativas desde el salto tecnológico necesario.

Con todo ello el software completo fue depositado en [sourceforge.net /projects/openilp] para su libre uso.

Si bien es una aplicación de ingeniería web se hace un uso prioritario de recursos criptográficos, especialmente para la firma directa de los ciudadanos. Se tienen en cuenta las arquitecturas software interoperables y las buenas prácticas de Administración electrónica y ajustado a estándares tecnológicos internacionales. Es un proyecto que propone potenciar la participación cívica y libre, como alternativa al cauce tradicional de tramitación parlamentaria de las normas legislativas.

La mayoría de los estados democráticos disponen de medios para considerar esta participación social, mediante recogida de firmas. Por ejemplo, gran parte de los estados de USA, la mitad de los países europeos, como Alemania, Italia, Austria o Suiza, la mayoría de América Latina. En el caso concreto de España la participación directa de los ciudadanos para hacer una ley que propondrán al Parlamento para que se tramite requiere 500.000 firmas.

El proyecto tiene una visión práctica sobre la Administración Electrónica y la integración de software con otros sistemas gubernamentales es una parte relevante del diseño. Para ello se pueden utilizar varios formatos, modos y certificados válidos. En el caso de España son por ejemplo el DNI[1]electrónico, los certificados personales

[1]El DNI electrónico, también denotado DNIe, es el Documento Nacional de Identidad que identifica a cada persona en España y que desde el año 2007 tiene un nuevo formato para permitir almacenar un certificado digital personal.

expedidos por organismos oficiales (como los de la FNMT[2]) y aquellos otros de organismos privados admitidos legalmente.

Este proyecto puede ponerse a disposición de todos aquellos promotores que deseen ofrecer esta herramienta de iniciativa legislativa electrónica a sus conciudadanos y tiene vocación de utilidad pública. Para ello, el proyecto openILP se define como herramienta de software libre, gratuito y accesible a cualquier iniciativa popular.

3.5.1. INGENIERÍA SOFTWARE

El entorno de desarrollo está basado en el lenguaje Java para aplicaciones profesionales centrado en la Web: Java EE. Además se han utilizado para este proyecto herramientas de desarrollo libres, tanto IDE de código abierto como servidores y librerías de código. La implementación realizada utiliza el modelo de aplicación con el patrón Modelo Vista Controlador (MVC) en los componentes de Apache Struts y una reutilización del código Web sobre el marco Tiles. La Figura 13 muestra un esquema básico basado en MVC.

[2]Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, abreviado FNMT, es el organismo del Ministerio de Economía y Hacienda encargado en España de la fabricación desde hace más de un siglo de productos timbrados, moneda y, más recientemente, de certificados digitales para personas y empresas.

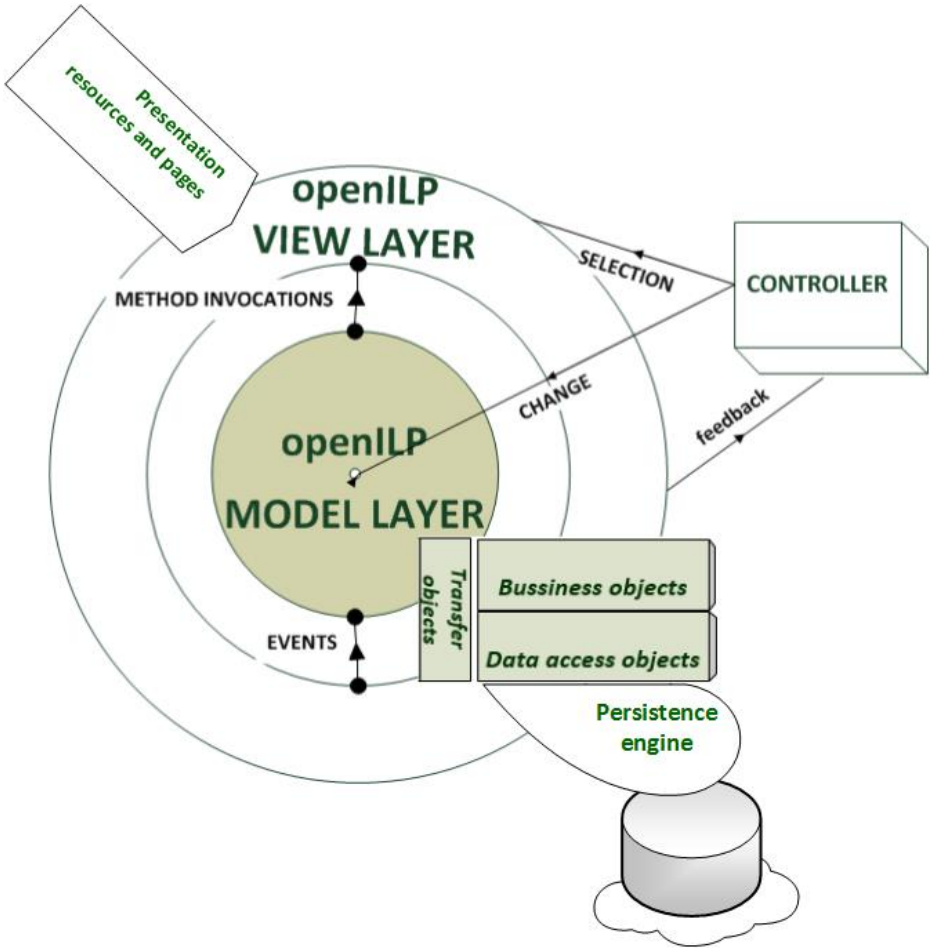


Figura 13. Representación esquemática del software

En la estructura de Modelo se incluye la parte de almacenamiento, firma digital en sistema de archivos y en base de datos que puede configurarse desde los archivos de configuración. Esta solución propuesta tiene la flexibilidad de ser capaz de situar el sistema de almacenamiento o su sincronización segura de una manera distribuida o en nube.

Los detalles más importantes de la implementación del proyecto subrayan el uso de buenas prácticas tecnológicas como la utilización del patrón de arquitectura

Modelo Vista Controlador, el de reutilización de objetos, la abstracción del acceso a datos y de objetos de negocio y la ingeniería de funciones criptográficas.

Diseño del modelo de aplicación partiendo de los dos modelos tradicionales de ingeniería web para aplicaciones Java empresariales: modelo de aplicación tipo 1, que consiste en aplicación en tres capas con componentes JSP/Servlets, y modelo de aplicación 2, donde en la aplicación se establecen múltiples capas. Se opta por el uso de marcos de trabajo que demuestran patrones de diseño con buenas prácticas de desarrollo, como por ejemplo MVC (Modelo-Vista-Controlador). Dentro de las implementaciones de estos marcos destacan Apache Struts, Spring y JSF de Oracle-Sun. La implementación OpenILP liberada que se ha realizado utiliza el modelo de aplicación con el patrón MVC y una reutilización de código web sobre el framework Tiles. Además incorpora el almacenamiento de las firmas digitales sobre Filesystem y sobre base de datos, configurable desde ficheros de configuración. La propuesta de solución permite la flexibilidad de poder ubicar de forma distribuida el sistema de almacenamiento o su sincronización segura.

Patrón MVC, basado en la implementación de Apache, se trata de un patrón de arquitectura que utiliza como esqueleto de aplicación para múltiples capas con el objetivo de separar la lógica de datos y la lógica de negocio de la presentación de usuario. Esta estrategia facilita habilitar el principio básico de separación de conceptos de forma modular en ingeniería del software, la reutilización de código y su posterior mantenimiento. La capa del controlador corresponde con la distribución de las acciones y su correspondiente información. Mientras que la capa Vista es donde se hacen distinciones entre los contenidos de la Web, como páginas HTML, páginas Java para

la reutilización de fragmentos de código (jspf), scripts de presentación en cliente y diseño basado en hojas de estilo.

Patrón Composite, basado en la implementación Apache Tiles, que consiste en código que se ha reutilizado usando las directivas de creación de objetos complejos a partir de objetos más simples y su definición mediante archivo XML. El patrón Composite permite una solución elegante de implementación, reutilización de código similar, facilita el seguimiento y mantenimiento del software.

Estrategia de persistencia de datos, que consiste en una capa software que abstrae los accesos a los sistemas de almacenamiento, como es el caso de sistema de archivos, base de datos y otras arquitecturas de almacenaje como Cloud.

Abstracción de entidades del modelo, basada en objetos transferibles entre capas.

Encapsulamiento de objetos de negocio, para la lógica propia de la aplicación.

Desarrollo de funciones criptográficas basada en librerías y clases propias de la Arquitectura Criptográfica Java (JCA) de las que vienen en el kit de desarrollo de Java (JDK), los del servidor de contenedor que se utilizarán en el medio ambiente y las bibliotecas criptográficas libres.

3.5.2. CONSIDERACIONES FUNCIONALES

El desarrollo del Proyecto ha estado dirigido por casos de uso, como técnica relevante que ha sido utilizada ampliamente en la moderna ingeniería del software y forma parte de multitud de metodologías tradicionales e incluso de las ágiles. La naturaleza del desarrollo de nuestro proyecto ha seguido una estrategia iterativa e incremental, lo que casa bien con estrategias ágiles y tecnologías web.

En el caso de las firmas digitales, la Junta Electoral Central (JEC) no dispone de infraestructura tecnológica para recibir vía telemática las mismas, ni para ofrecer un servicio de suscripción a las iniciativas legislativas populares por Internet de cara a los ciudadanos.

El organismo público sobre el que recae la garantía de procedimiento es la Junta Electoral Central, dependiente del Congreso, que sellará y numerará los pliegos en papel para las firmas manuscritas y autorizará el sistema de firma digital en caso de utilizarse.

Por ello, la promotora de la iniciativa debe facilitar el sistema de firma, en base a la existencia de la ley 59/2003 de firma electrónica, si bien no se proporcionan unas especificaciones técnicas por parte de la Administración Pública encargada, la Junta Electoral Central.

Teniendo en cuenta el Acuerdo de la Junta Electoral Central, de 17 de septiembre de 2009, para establecer el procedimiento legal para la incorporación de firma electrónica en iniciativas legislativas populares, se identifican cinco requisitos

formales que suponen una serie de decisiones de diseño que deben enmarcarse en la arquitectura software del proyecto.

- RF01.- Cumplimiento de la ley 59/2003 de firma electrónica
- RF02.- Certificados de la Fábrica de Moneda y Timbre (FNMT) o autorizada al efecto.
- RF03.- Garantías de identificación personal en la iniciativa popular (artículos 9 y 10 de la ley de iniciativa popular)
- RF04.- Comunicación a la JEC del sistema de firma electrónica a utilizar.
- RF05.- Facilitar un sistema de verificación de firmas electrónicas.

Sin embargo, hemos de considerar que la función primordial que afecta al proyecto y que realiza de forma directa la Junta, es la validación formal de las firmas electrónicas. Para ello, la Administración General del Estado en España dispone de utilidades relacionadas con certificados digitales a través de su red intranet administrativa, denominada Red SARA. La Red SARA interconecta las administraciones públicas, tanto las administraciones estatales como las regionales y locales. Es más, la gran intranet administrativa española se interconecta con una mayor propia de la Unión Europea, denominada Red TESTA [56].

Los escenarios de uso del proyecto consisten en los siguientes casos:

- Caso de uso de lectura del texto de la iniciativa legislativa popular.

- Debe opcionalmente permitir asimismo la descarga del texto en formato documento PDF.

- Rellenar los datos personales del firmante, que consistirán en:
  - Nombre
  - Primer apellido
  - Segundo apellido
  - Documento nacional de identidad con letra, verificando que el cálculo de la letra es correcta.
  - Fecha de nacimiento, permitiendo sólo mayores de edad.
  - Localidad y provincia de nacimiento.
  - Domicilio donde esté censado
  - Municipio de residencia
  - Provincia
  - Código postal, sería recomendable una ayuda para cumplimentar el código postal.
- Firma digital, consiste en la firma con certificado digital y su procesamiento.
  - Incluye el procesamiento de la firma, guardando el documento de firma en el servidor, opcionalmente el tratamiento de los errores y guardar el documento en el ordenador del usuario.
- Validación, consiste en cómo realizar la comprobación de la validez del documento firmado y/o el certificado digital utilizado.

Teniendo en cuenta las anteriores consideraciones la Figura 14 muestra el diagrama UML de casos de uso. Entre los escenarios contemplados cabe destacar la consulta de los textos que se presentan para constituirse en iniciativa popular, la gestión de los detalles de la persona que subscribe, la gestión específica de la firma digital basada es mecanismos robustos sobre certificados electrónicos y su procesamiento criptográfico y la información relacionada con las plataforma de verificación tanto de lo firmado como de la validez del certificado.

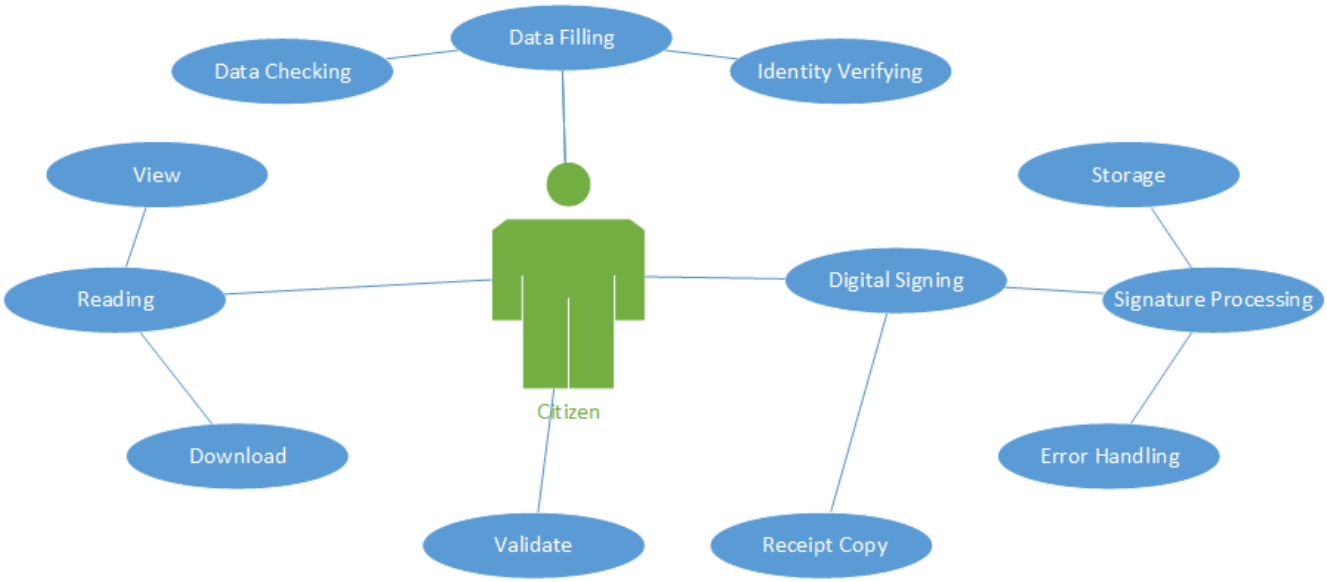


Figura 14. Diagrama de escenarios de uso del ciudadano en OpenILP

En la Tabla 1 se muestra una lista de datos de referencia utilizados en el proyecto.

Datos del firmante	Nombre
	Apellidos
	Número de identificación (DNI)
	Lugar de nacimiento
	Fecha de nacimiento/Edad
Datos censales	Domicilio de registro para votar
	Lugar de residencia

	Código postal
Datos de la firma digital	Identificación certificado
	Algoritmo criptográfico
	Estándar firma documento
	Fecha de firma
	Localización

Tabla 1. Datos de referencia utilizados en OpenILP

Teniendo en cuenta estas consideraciones en mente la Figura 14 muestra un diagrama que representa los escenarios sobre los que puede interactuar el ciudadano sobre OpenILP.

Se muestra asimismo una visión esquemática de la funcionalidad que representa en la Figura 15: la vista de interfaz de usuario diseñada siguiendo criterios de facilidad de uso, accesibilidad y apariencia intuitiva.

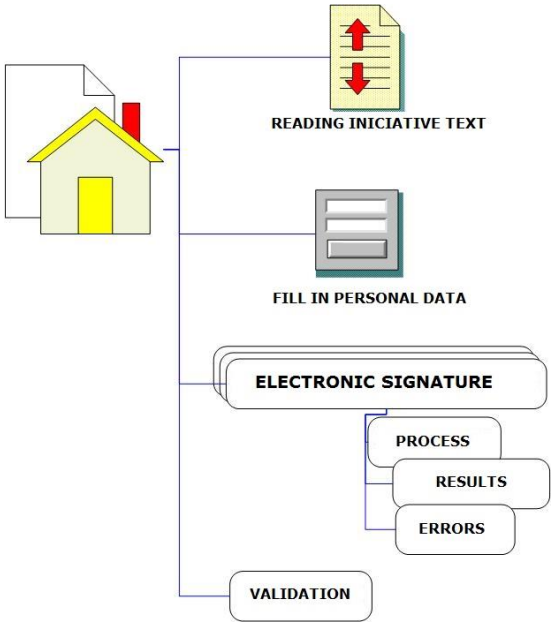


Figura 15. Diagrama esquemático de la vista de usuario

3.5.3. REQUISITOS TÉCNICOS, SOCIO-POLÍTICOS Y LEGALES

Evidentemente cualquier proyecto de estas características debe considerar de forma inexcusable la legislación del Estado, incluyendo la producción legislativa, la propuesta de leyes o la de referendos.

Sin que haya un criterio uniforme, numerosos países tienen regulada la iniciativa legislativa popular, concediendo en la mayoría de casos la facultad de iniciar el procedimiento legislativo y, en función de esta regulación, añadiendo un carácter más o menos vinculante para el Parlamento respectivo. Además, las iniciativas populares pueden ser de aplicación local, regional o nacional. En países con gran tradición democrática como Estados Unidos se incorpora la iniciativa popular directa a finales del siglo XIX, como ya hemos mencionado con respecto a los "town-meeting". Todo esto influye en que la iniciativa popular exista desde hace muchos años en numerosas regiones de USA, como son, por orden de aparición desde 1898 en adelante: Dakota del Sur, Utah, Oregón, Nevada, Montana, Oklahoma, Missouri, Maine, Michigan, Arkansas, Colorado, Arizona, California, Washington, Nebraska, Idaho, Ohio, Dakota del Norte, Massachusetts, siguiendo más tarde Alaska, Wyoming, Illinois, Florida y el Distrito de Columbia. La incorporación de la institución de iniciativa popular, con mayor o menor alcance político, se extiende también a numerosos países europeos: Italia, Austria, Alemania, España, entre otros; en casi una docena de países de América latina,

como Uruguay, Venezuela, Brasil o Argentina; e incluso en otros continentes cabe mencionar Filipinas, Mongolia o Taiwan [57].

Fruto de esta inquietud la Unión Europea, como organismo supranacional, en 2011 reguló por primera vez la iniciativa legislativa a nivel comunitario mediante un reglamento como marco general de la iniciativa, pendiente de su desarrollo normativo completo [58].

Someramente sin intención de realizar un análisis jurídico a continuación se repasan los aspectos legales más relevantes en la legislación española.

La Iniciativa Legislativa Popular está regulada por ley en España desde el año 1984, concretamente por la Ley 3/1984, como puede verse en [59], que posteriormente fue modificada por la Ley 4/2006. La Ley necesitó actualizarse en el año 2006, después de 22 años, entre otras cosas para permitir el uso de la firma electrónica. Con esto se regula la posibilidad de participación directa de los ciudadanos para hacer una ley que propondrán al Parlamento para que se tramite, en la línea de la mayoría de estados democráticos modernos. Para ello, es necesario el aval de 500.000 firmas de ciudadanos españoles, mayores de edad y con plena facultad para ejercer sus derechos civiles.

La iniciativa popular se inicia mediante la presentación de un texto a la Mesa del Congreso a propuesta de un grupo de ciudadanos, denominado Comisión Promotora. La Mesa del Congreso estudia la propuesta para su admisión, con el visto bueno previo del Senado. Una vez admitido a trámite, se inicia un período de recogida de firmas de 9 meses, ampliable a 3 meses más.

Para recoger firmas es necesario autenticar a la persona firmante, para ello se permite la designación de Fedatarios Especiales, que son personas determinadas que darán fe pública de la validez de las firmas recogidas.

Entre las normas jurídicas que se deben mencionar en relación con el proyecto, se ha de considerar lo expresado en la Constitución Española, *Artículo 87, apartado 3:*

> "*Una Ley orgánica regulará las formas de ejercicio y requisitos de la iniciativa popular para la presentación de proposiciones de Ley. En todo caso se exigirán no menos de 500.000 firmas acreditadas. No procederá dicha iniciativa en materias propias de Ley orgánica, tributarias o de carácter internacional, ni en lo relativo a la prerrogativa de gracia*."

En su desarrollo normativo, debe considerarse la Ley Orgánica 3/1984, que regula la iniciativa legislativa popular que debió ser modificada posteriormente por la Ley Orgánica 4/2006, para permitir la firma electrónica. Después de 22 años a la Ley se incorpora un nuevo apartado al articulado: "*Las firmas se podrán recoger también como firma electrónica conforme a lo que establezca la legislación correspondiente*".

Sin embargo, hasta 2009 no se habían detallado unas instrucciones claras sobre cómo realizar la iniciativa de forma electrónica. Es el Acuerdo de la Junta Electoral Central, de 17 de septiembre de 2009, donde se indica que "*el uso de la firma electrónica para la recogida de firmas a efectos de la presentación de una iniciativa*

legislativa popular debe entenderse válida siempre que se ajuste a lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica".

Asimismo, se menciona expresamente que se acompañe de certificado válidamente proporcionado por la Fábrica Nacional de Moneda y Timbre (FNMT) o por otra entidad autorizada al efecto. Se permiten más entidades proveedoras de certificación digital en España siempre que estén acreditadas y cumplan con unos estrictos requisitos establecidos por Ley. Pero la información contenida en el certificado digital de una persona no es suficiente para poder adherirse a una proposición popular de ley, se exigen además los datos del lugar de nacimiento, el lugar de residencia y la fecha de nacimiento, datos todos ellos que no suelen acompañar a un certificado digital.

Como consecuencia, la Comisión Promotora deberá comunicar al Congreso, a través de la Junta Electoral Central, un sistema de firma electrónica y un sistema de verificación de las firmas electrónicas.

En el ámbito legal sobre la firma electrónica se debe considerar la norma principal en Europa: la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica [60], que ha sido trasladado a todos los países de la Unión Europea. El objetivo principal de esta directiva fue dar confianza a las transacciones electrónicas dentro del ámbito de los países europeos y favorecer así el mercado económico interior.

De esta manera, en Europa queda armonizada la firma electrónica y se sientan las bases de su validez jurídica. La directiva europea distingue entre tres tipos de

firmas: 1) la firma simple, a efectos de identidad, como puede ser la firma textual de un correo electrónico; 2) la firma avanzada, que debe cumplir unos requisitos técnicos y que corresponden con una firma electrónica basada en infraestructura de clave pública (PKI); y 3) firma reconocida, que cumple con mayores requisitos técnicos, corresponde con una firma avanzada, con un certificado reconocido y creada mediante un dispositivo seguro de creación de firmas. Esto supone que la firma electrónica reconocida tiene a nivel europeo la misma validez que la firma manuscrita. La directiva europea se concreta en el caso de España en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

La experiencia sobre el uso de la firma electrónica tanto a nivel europeo como a nivel nacional, deja en evidencia que, pese a haber un marco común, la implantación del uso de la firma necesita avanzar en la interoperabilidad técnica, tanto a nivel nacional como transfronterizo, como a veces se ha venido reconociendo por la propia Comisión Europea [61].

De ahí, como medida complementaria para mejorar el marco de la Administración Electrónica, es necesario mejorar la interoperabilidad, con normativa de rango inferior, como son por ejemplo en España el Esquema Nacional de Seguridad [62], el Esquema Nacional de Interoperabilidad [63] y la regulación del certificado digital del DNI electrónico [64] o, en otros países, por poner algún ejemplo la serie de especificaciones técnicas alemanas ISIS-MTT para la interoperabilidad entre productos de firma electrónica [65].

3.5.4. INTEROPERABILIDAD E INTEGRACIÓN DE SOFTWARE

El impulso de la Administración Electrónica va en consonancia con la tendencia supranacional de los países de nuestro entorno, especialmente la Unión Europea (UE). En este ámbito se realizó una Conferencia de Administración Electrónica en diciembre de 2010, denominada "LIff-off to Open Government". En este evento, además, se presentó un "Plan de Acción de Administración Electrónica" [66] para el lustro 2011-2015, fruto de los acuerdos directivos alcanzados en la Declaración Ministerial de Malmö de noviembre de 2009.

A nivel nacional, tanto las administraciones locales como regionales, en consonancia con la estatal, vienen ofreciendo cada vez más servicios directos a los ciudadanos. Entre los más demandados podemos mencionar la declaración de la Renta, relativo a impuesto directo aplicado sobre los ingresos de los individuos y empresas para costear los servicios públicos del país, solicitudes de beca y ayudas o matriculación en la Universidad. Especialmente, se debe resaltar el portal www.060.es, uno de los más visibles ejemplos de la e-Administración, destacado por interés por la accesibilidad y usabilidad, desde el que se puede acceder a los servicios mencionados anteriormente.

Desde el punto de vista legislativo la situación puede considerarse madura. Por otro lado, desde el punto de vista tecnológico un factor clave ha sido la liberalización del cliente @firma en 2011 como software libre GPL y que es la implementación estándar en las administraciones españolas.

El sistema @firma es una plataforma tecnológica realizada para impulsar la Administración Electrónica facilitando una serie de servicios para el uso de la firma electrónica a los organismos gubernamentales españoles. Con esto se pretende conseguir una capa de abstracción de seguridad que evite a las Administraciones Públicas la complejidad asociada a las infraestructuras de clave pública relacionada con los servicios de certificación digital. Para ello, desde el Ministerio de Política Territorial y Administraciones Públicas, de forma centralizada, se ofrecen una serie de servicios mediante la RedSara. Entre los servicios más destacados que presta destacan la comprobación de la validez de un certificado, la generación y validación de firmas en servidor, la auditoría de las transacciones, sellados de tiempo y la generación de firmas en cliente. Este último componente ha sido objeto de liberación GPL, motivo que ha permitido su integración en este proyecto y que permiten extender a la iniciativa ciudadana las bondades de @firma, entre las que destaca su apoyo y soporte gubernamental.

Además, cabe mencionar la plataforma pública VALIDE del Ministerio de Industria, Turismo y Comercio, otro organismo gubernamental que pretende hacer más accesible los servicios de validación de las firmas digitales desde Internet para las firmas generadas con el sistema @firma. Dicho organismo es a su vez competente para establecer y acreditar los Prestadores de Servicios de Certificación. Dado su vocación de servicio pública, la plataforma VALIDE se integra dentro de nuestro proyecto como garantía de transparencia al ser una validación de acceso universal y público.

Como sistema principal y alternativo al anterior, las Administraciones Públicas tienen la posibilidad de utilizar el servicio de validación de @firma, restringido a organismos públicos y accesible desde su propia Intranet administrativa, lo que permite dar una doble garantía en la validación.

Teniendo en cuenta las anteriores consideraciones, el proyecto OpenILP no debe entenderse como una aplicación ad hoc sino como un ejemplo de integración de aplicaciones para la participación ciudadana cívica, integrando los servicios de generación de firmas y de validación. El objetivo de este trabajo es difundir como software libre este proyecto con el fin de "liberalizar" a los promotores de las iniciativas legislativas del salto tecnológico necesario y ponerlo al alcance de cualquier persona interesada.

3.5.5. DISEÑO Y COMPATIBILIDAD

Como punto de partida debe considerarse la doctrina jurídica definida en el Acuerdo de 17 de septiembre de 2009 de la Junta Electoral Central [67]. Así, el sistema deberá cumplir los siguientes requisitos:

- Estar preparado para que los ciudadanos puedan firmar electrónicamente una proposición de ley
- Almacenar las firmas
- Facilitar la entrega de firmas a la Junta Electoral.
- Dar una solución de servicio para la validación de las firmas.

Como plataforma tecnológica se propone un entorno profesional en Java, sobre tecnología web, compatible con los sistemas de firma electrónica válidos en la

Administración General del Estado (Figura). Para ello se tomarán como referencia los certificados de la FNMT (Fábrica Nacional de Moneda y Timbre), el DNI electrónico, el sistema @firma, la herramienta VALIDE de la red Intranet administrativa y la disponibilidad de la verificación de la firma de la Administración.

En la arquitectura del sistema es de especial interés la interoperabilidad y la integración óptima de módulos ya existentes. Principalmente estos sistemas son gubernamentales e incluso privadas de los propios organismos. Diseñar una solución que tenga en cuenta estos mecanismos y estándares facilita la interoperabilidad, la facilidad en la implantación, la fiabilidad y, en esencia, la confianza. Los componentes que se articulan alrededor de OpenILP son:

Red Sara.- Intranet que concentra las distintas subredes de los organismos públicos nacionales, regionales y locales, así como con otras redes de Instituciones europeas, facilitando el intercambio de información y la cooperación entre ellas.

Plataforma @firma.- Plataforma común dentro de la gran Intranet de la Administración Pública, creada para ayudar e impulsar el uso de la firma electrónica en los organismos públicos. Ha sido desarrollada por el Ministerio de Política Territorial y Administración Pública español. Como parte destacada, se trata de una implementación de servicios web, pero no están directamente accesibles desde Internet, ya que son de uso exclusivo de los órganos gubernamentales. Dentro de este conjunto de servicios, se debe destacar el servicio de verificación de certificados, el

servicio de verificación de firmas electrónicas y el servicio de generación de firmas, tanto en servidor como en cliente.

Plataforma VALIDE.- Es una aplicación del Ministerio de Industria, Turismo y Comercio como medida para impulsar la Administración Electrónica, para facilitar el uso de la firma electrónica desde Internet. De forma transparente para el usuario, VALIDE interacciona con @firma con lo que es coherente con los tipos de certificados y formatos de firma. La parte más interesante es que ofrece un servicio de verificación de firma electrónica, lo que puede ser utilizado por agentes externos no gubernamentales. Recordemos que los organismos públicos pueden utilizar la Validación directamente accediendo desde su Intranet administrativa. El Ministerio de Industria, Turismo y Comercio es el encargado de acreditar los prestadores de certificación, lo que a la postre supone determinar los certificados que se van a permitir para operar legalmente.

STESTA.- Intranet europea que interconecta las redes nacionales de los países miembros de la Unión Europea, para facilitar servicios de carácter internacional. La Red Sara se conecta mediante una pasarela que gestiona el Ministerio de Política Territorial y Administraciones Públicas.

Subsistema de almacenamiento de firmas.- El almacenamiento de las firmas digitales se plantea de forma flexible, tanto sobre sistemas de ficheros como sobre base de datos, que pueden estar sincronizadas u hospedadas de forma distribuida. Esto permite la integración con otros sistemas empresariales, propios de los promotores de la iniciativa legislativa, por ejemplo, a los efectos de reutilizar un

sistema "legacy" con unos criterios de seguridad concretos para el manejo de datos de carácter personal.

Subsistema Cliente @firma.- Se libera el código fuente del cliente @firma para firma electrónica, que consiste en un componente Java que puede ser reutilizado bajo licencia GPL versión 2 y EUPL versión 1.1, constituyéndose como un componente público de fuentes abiertas cuyo desarrollo se mantiene aparte de la plataforma de servicios @firma.

3.5.6. PROCESO CRIPTOGRÁFICO DE FIRMA

El proceso de firma sobre esta arquitecta se ejecuta en el ordenador del usuario haciendo uso de certificados digitales X.509 version 3, según la RFC 3280 [68], sin que la clave privada asociada al certificado tenga que salir del contenedor del cliente. Además, se permite seleccionar entre cuatro tipos de formatos de firma disponibles: 1) CMS, para firma según el RFC 3852, compatible con PKCS#7; 2) XAdES, para firma electrónica avanzada XML, según el estándar ETSI (European Telecommunications Standards Institute); 3) XAdES Enveloping, donde la firma avanzada XML contiene la información firmada; 4) XMLDsig, según el popular estándar de firma XML del W3C, denominado "IETF/W3C XML-Signature Syntax and Processing specification" (junto a Internet Engineering Task Force). La Figura 16 muestra los formatos disponibles.

Figura 16. Formatos de firma implementados en OpenILP

La Firma Avanzada XAdES significa "XML Advanced Electronic Signatures", un estándar europeo del ETSI (Instituto Europeo de Estándares de Telecomunicaciones), que extiende las recomendaciones internacionales XMLDSig del organismo W3C. Surge por la necesidad de dar una respuesta técnica a los cambios legales de la Directiva Europea de firma electrónica que hemos mencionado anteriormente, para guardar documentos firmados durante mucho tiempo, independientemente de los algoritmos criptográficos subyacentes. El estándar XAdES se denota ETSI TS 101 903.

En este estándar se permiten variantes para la firma electrónica avanzada en XML. Destacan, la firma electrónica básica: XAdES-BES, formato que cumple suficientemente con criterios legales; la firma electrónica basada en política explícita: XAdES-EPES, formato básico con información de la política de firma; firma electrónica con datos de sellado seguro de tiempo: XAdES-T; variante XAdES-C, que añade referencias completas para certificados y listas de revocación, que permitiría ser usado a largo tiempo en modo off-line. Otros formatos como XAdES-X, que añade sellos de

tiempo a la información de certificados; XAdES-X-L, que añade los propios certificados y listas de revocación, para permitir la verificación aun cuando no existan estos certificados o listas en el futuro; o bien XAdES-A, que añade un sellado de tiempo periódico para archivado durante largos períodos de tiempo, típicamente usado para aplicaciones de archivística.

En esencia, para el propósito de nuestro proyecto la firma XAdES-BES es suficiente para establecer un formato de firma XML para las Iniciativas Legislativas Populares. No se considera la firma con sellado de tiempo porque funcionalmente no es necesario, ya que la normativa sobre iniciativa ciudadana tiene un plazo establecido en su normativa específica y un plazo de recuento final. Sin embargo, el proyecto es flexible para incorporar un sello de tiempo avanzado de una Autoridad de Certificación de Sellado de Tiempo (TSA), según la RFC 3161 [69]. La decisión es una cuestión puramente de diseño del proyecto.

El estándar europeo XAdES añade al estándar internacional XMLDSig algunos elementos XML útiles para la mayoría de escenarios de firma. Es el caso principalmente del elemento 'xades: QualifyingProperties', cuya existencia está justificada para garantizar el no-repudio de la firma [70]. Este elemento recoge información sobre el proceso de firma, como por ejemplo, la fecha y hora de la firma, el certificado firmante, el identificador de la política de firma utilizada y el formato utilizado.

Por otro lado, los modos de firma establecidos en ETSI TS 101 903 se distinguen en función de si el documento firmado y su firma constituyen entidades separadas o

no. Así se explicitan el modo implícito en el que la firma se encuentra asociada al documento firmado y el modo explícito en el que los datos de la firma están en un fichero separado del documento original (generalmente firma 'detached').

Como el propósito fundamental de este trabajo es ofrecer un servicio a los ciudadanos integrando sistemas con garantías, la propuesta para el sistema de verificación de firmas consiste en integrar la plataforma Valide. De esta manera, el sistema de firma se realiza dentro de la aplicación OpenILP, mientras que el sistema de verificación se integra mediante un servicio externo, público y gratuito de un organismo oficial, permitiendo dar mayor confianza al proceso global de adhesiones a la iniciativa legislativa y, por ende, mayor transparencia democrática

Se ofrece además un doble mecanismo de validación de las firmas, al estar disponible para los organismos públicos los servicios de la Plataforma común @firma, uno de los cuales se encarga de la verificación de firmas, desde su propia Intranet, que permite acceder a la información de los Prestadores de Servicios de Certificación. Esta plataforma proporciona servicios a nivel servidor dentro de la propia Intranet gubernativa, por ejemplo, de validación de certificados y de firma electrónica de los principales Prestadores de Servicios de Certificación reconocidos en España. La plataforma actual se define como una arquitectura Web Service con soporte para los formatos de firma: PKCS7, CMS, XMLDSig, XAdES-BES y XAdES-T. Posteriormente se ha añadido CAdES. Las aplicaciones cliente se pueden configurar si se desea realizar un sellado de tiempo de sus Firmas Electrónicas, ya que la plataforma ofrece un servicio seguro de sellado de tiempo. Utiliza la infraestructura software sobre un servidor de aplicaciones JBOSS, sobre Java EE en alta disponibilidad, con soporte para webservices Apache AXIS y manejo de logs con Log4j. También utiliza motor de

persistencia Hibernate y base de datos Oracle. A su vez las operaciones criptográficas se basan en la librería estándar Java Cryptographic Extensions (JCE), la librería BouncyCastle y otras mejoras de la librería IAIK.

Las librerías criptográficas utilizadas en este proyecto para la firma en cliente son también de software libre, reutilizando el código cliente @firma, cuyo objetivo primordial es facilitar de una forma eficaz y sencilla la integración de aplicaciones que hacen uso de firma electrónica conforme a la Directiva Europea de firma, la Ley de Firma Electrónica (Ley 59/2003), así como es una solución de referencia para la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

3.5.7. ESTRATEGIA DE DESARROLLO

El entorno de desarrollo se ha centrado sobre web en lenguaje Java para aplicaciones web profesionales: Java EE 6, conservando la compatibilidad con Java EE 5. La plataforma Java consiste en un conjunto de tecnologías y librerías, presentando como ventajas su capacidad para reutilizar código de fuentes abiertas y la independencia del hardware ya que se basa en la ejecución sobre máquinas virtuales (JVM, Java Virtual Machine).

Para este proyecto de software libre se han utilizado también herramientas libres de desarrollo, principalmente el IDE Netbeans de Oracle-Sun, y en menor medida IDE Eclipse, aunque hubiera sido indiferente cualquier otro entorno de desarrollo para Java Web.

Como servidores para el desarrollo se ha utilizado, como servidor de aplicaciones web de referencia Glassfish, de Oracle-Sun, así como se ha comprobado la compatibilidad con Apache Tomcat sobre máquinas virtuales. La Figura 17 muestra la infraestructura de entornos representativa de la estrategia de desarrollo.

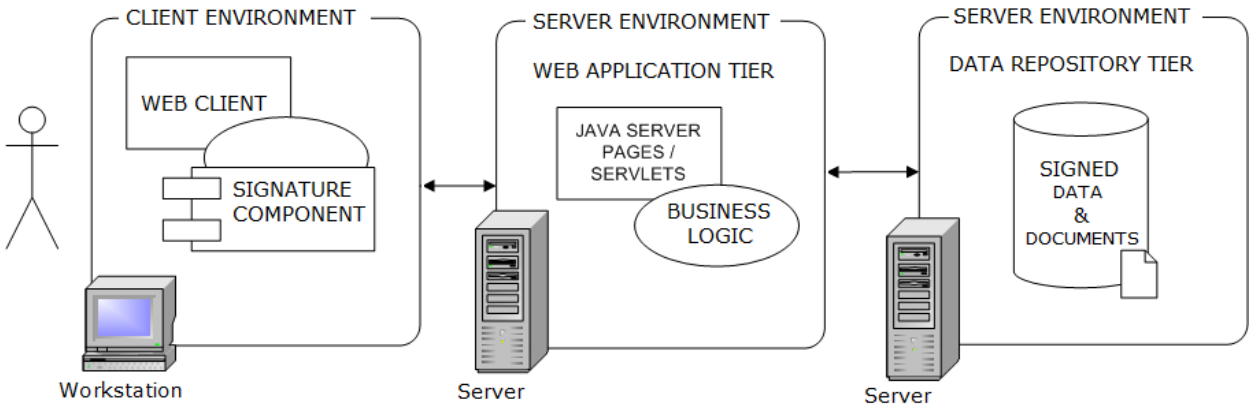
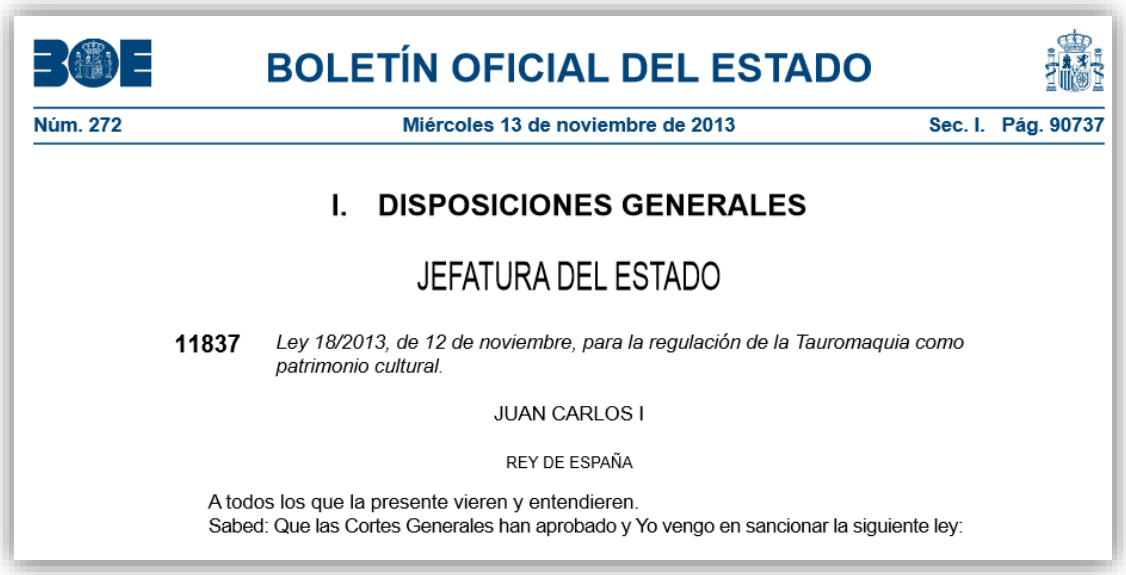


Figura 17. Entornos representativos de la estrategia de desarrollo

3.5.8. LA EXPERIENCIA DE LA OPENILP

OpenILP ha sido la primera plataforma que la Junta Electoral Central, organismo dependiente del Congreso de los Diputados, ha autorizado y ha sido utilizada con éxito para la recogida de firmas electrónicas en una iniciativa legislativa popular, según resolución de la Junta Electoral Central, de fecha 23 de noviembre de 2011, resolución que tuvo lugar previa valoración técnica del proyecto. Es el primer sistema electrónico donde se ha emitido la primera Ley en España con firma electrónica. En la Figura 18 puede verse la publicación en BOE.



BOLETÍN OFICIAL DEL ESTADO

Núm. 272 Miércoles 13 de noviembre de 2013 Sec. I. Pág. 90737

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

11837 *Ley 18/2013, de 12 de noviembre, para la regulación de la Tauromaquia como patrimonio cultural.*

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

Figura 18. Publicación de la ley de iniciativa ciudadana

En dicha fecha se emiten las resoluciones independientes que permiten aplicar OpenILP sobre dos Iniciativas Legislativas Populares concretas en vigor. La primera, para una propuesta de Ley para proteger la fiesta típica española de los toros y declararlo Bien de interés cultural (taurinos.openilp.org, www.ilptaurina.com). La segunda, para establecer un nuevo régimen de personal para los funcionarios policiales de la institución militar de la Guardia Civil (gc.openilp.org). Anexo a esta tesis puede verse la autorización informada del proyecto por parte de la presidencia de la Junta Electoral Central (Apéndice 1).

En el contenido del informe técnico se aprecia especialmente el esfuerzo de integración del proyecto, así como la validez jurídica de la firma resultante, por seguir los estándares de las administraciones públicas. El proyecto de software libre OpenILP

genera, de esta manera, confianza tanto a ciudadanos como a las entidades gubernamentales, prueba de ello es haber sido aceptada a la primera solicitud.

Durante las cuatro primeras semanas, la ILP electrónica de los Toros ha tenido repercusión social en los medios de comunicación, recibiendo una media aproximada de 1.000 visitas diarias, aproximadamente 25.000/primer mes.

El proyecto tiene una visión práctica sobre la Administración Electrónica y el acercamiento de los ciudadanos a las instituciones públicas, complementando la democracia tradicional con una nueva forma de democracia electrónica directa. La Iniciativa Legislativa popular electrónica integra de una forma eficiente las tecnologías web y la criptografía para realizar la firma electrónica de un texto propuesto.

La visión de futuro es facilitar la participación directa de los ciudadanos en las iniciativas legislativas, con arquitectura tecnológica a disposición de todos aquellos promotores, colectivos y personas interesadas en general. OpenILP, como proyecto universitario de software libre, pretende contribuir a acercar el Parlamento a los ciudadanos de forma directa, utilizando las nuevas tecnologías de una forma asequible y segura. La Figura 19 muestra el portal de inicio del proyecto desplegado (www.openilp.org).

Figura 19. Portal web de despliegue de OpenILP

3.6. MODELO CONCEPTUAL CIBEV BASADO EN VOTO ELECTRÓNICO

En esta sección se trata el trabajo realizado con respecto al diseño de sistemas relacionados con la participación ciudadana y los procesos de voto electrónico. El e-voting ha sido tratado y debatido durante la última década. Se han realizado experiencias y se han apuntado riesgos. Hoy en día, hay una alta demanda social para habilitar la posibilidad de expresar las preocupaciones ciudadanas y que sus opiniones sean oídas con respecto a la situación política. En ausencia de medios que satisfagan esta necesidad aceptados por las legislaciones vigentes, las redes sociales han sido utilizadas con este fin y el uso de Internet ha llegado a ser un canal para el cultivo de plataformas y aplicaciones de este tipo. Sin embargo, los grupos sociales exigen algo

más allá, de tal manera que los poderes públicos, como el parlamentario, lo tengan en cuenta para garantizar la fiabilidad y la representación de las encuestas de opinión.

Esta necesidad no es nueva, dependiendo de cada caso, una ley o regulación de menor rango, permiten alguna forma de participación ciudadana de carácter directo o semi-directo. Esto supone la necesidad de recoger una determinada cantidad de firmas para poder llevar adelante propuestas y que sean aceptables para los responsables políticos.

3.6.1. ASPECTOS BÁSICOS DE E-VOTING

Al tratar el tema de e-voting, hay que tener en cuenta específicamente también los aspectos relacionados con la privacidad y el voto secreto, el mecanismo de escrutinio y configuración del grupo de autoridades electorales. En este sentido hay muchas líneas en la fundamentación básica con la participación respecto de una iniciativa electrónica de participación como la presentada, si bien las aproximaciones a e-voting se acercan tradicionalmente al procesamiento algorítmico.

Como paso previo al e-vote y teniendo como objetivo fundamental que el proceso tenga la aceptación de las autoridades que velan por el correcto funcionamiento de la participación democrática, en este trabajo se introduce este vínculo entre voto electrónico y el framework para facilitar plataformas de e-participation de los ciudadanos de una forma más directa, sus componentes principales y qué pueden desarrollar los grupos sociales promotores y qué no pueden, pero debe proporcionarlo los poderes públicos necesariamente.

En sentido amplio, algunos autores, como en [71] advierten de los riesgos del voto electrónico a través de otros parámetros como son la fiabilidad, la seguridad y la transparencia. Por otro lado, en [72] se nos acerca la idea de la simplicidad en los procedimientos, el código de fuentes abiertas y la redundancia incorporada en el proceso de diseño. Otras consideraciones relevantes que sobre e-voting corresponden con grupos de trabajo y esfuerzos relativos a organizaciones de estándares y asociaciones profesionales de ingenieros, como puede verse en [73] y en [74].

3.6.2. MODELO CIBEV BASADO EN VOTO

En el desarrollo de los aspectos de voto electrónico en este framework sobre iniciativa ciudadana electrónica se tienen en cuenta como principios esenciales la confianza del flujo, la robustez criptográfica y la transparencia algorítmica. Esto nos permite describirlo mediante un modelo conceptual resultante que permite integrar modularmente e-voting dentro de nuestro framework global de e-democracia, denominándose CIBEV ("Citizen initiative based on electronic Voting"). Los principios de este modelo se identifican a continuación y se ilustran en la Figura 20.

1. **Confianza del flujo del proceso**.- Consiste en la fiabilidad en el esquema de pasos que forman el flujo de trabajo del proceso a nivel de usuario, de tal manera que la funcionalidad de votar sea vista de forma sólida desde la perspectiva del ciudadano.

2. **Transparencia algorítmica**.- La necesidad de establecer algoritmos que permitan las verificaciones del proceso de votación y garanticen el secreto del ejercicio del voto.

3. **Robustez criptográfica**.- El núcleo de los mecanismos de protección basado en diseños e implementaciones robustas desde el punto de vista de la seguridad criptográfica.

En este sentido, a partir de estos principios se persiguen dos objetivos fundamentales:

A. Facilitar la participación ciudadana a través de iniciativas electrónicas basadas en e-voting.

B. Que dicha participación sea aceptada por las instituciones gubernamentales que velan por el correcto funcionamiento del proceso.

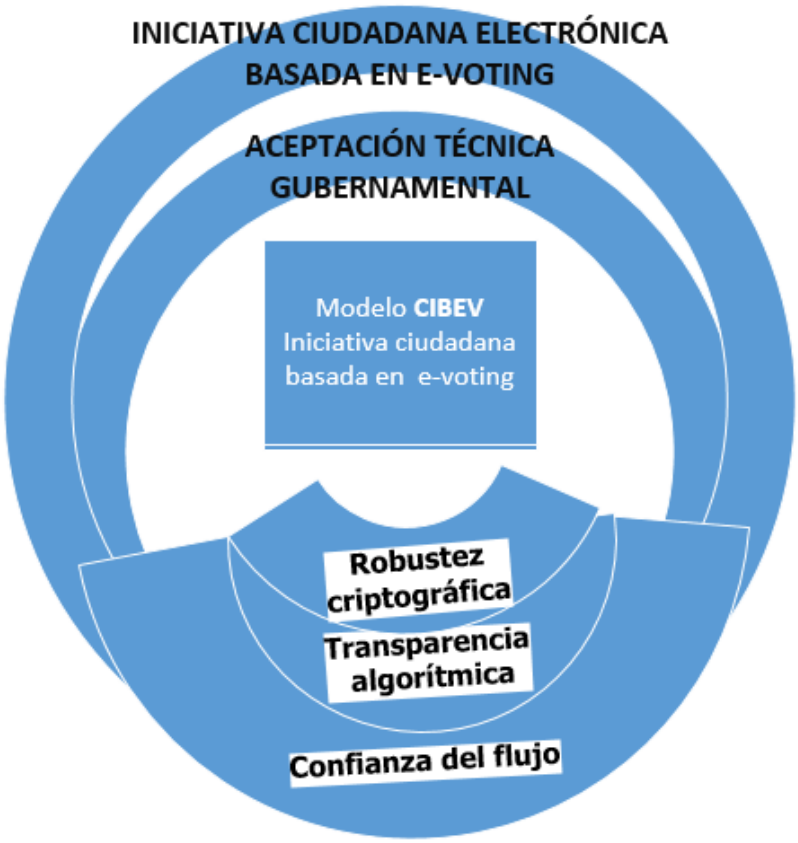


Figura 20. Diagrama conceptual CIBEV de iniciativa ciudadana basada en e-voting

En consideración a esto en la actualidad las legislaciones, dentro de sus limitaciones, y la tecnología han evolucionado en los últimos años aportando mayores mecanismos que mitiguen en gran parte los riesgos señalados para el proceso de votación electrónica, como se ha podido contrastar con los trabajos de investigación y experiencias relacionadas con la participación electrónica de este proyecto.

3.6.3. DISCUSIÓN Y EXPERIENCIA

Del despliegue del proyecto OpenILP es un hito significativo la aceptación técnica por parte del parlamento. Esto supone un apoyo diáfano al sistema de firma electrónica y sus procedimientos criptográficos, base para garantizar la identidad de la firma. Los sistemas de voto electrónico tienen una especialización respecto de los sistemas de participación en e-democracia, consideraciones que lo hacen diferente. Este es el caso de la transparencia algorítmica, el tercer principio que hemos expuesto, donde el secreto del ejercicio del voto y el sentido del voto son clave. Sin embargo, los dos primeros principios de nuestro enunciado son compartidos con el sistema de iniciativa electrónica planteado en las secciones anteriores.

En el marco de este modelo sería posible diseñar una firma electrónica para votar, en la que el voto estuviera incluido de una forma robusta. De hecho el modelo permite describir líneas de investigación abriendo paso a otros esquemas robustos como los sistemas biométricos para su uso en sistemas de e-voting. Sin embargo, superar los experiencias del voto electrónico experimentadas a lo largo de los últimos años, como se puede ver en [75], supone un esfuerzo que parte de la concepción, de las dificultades en interoperabilidad, y la eficacia de estándares y diseños universales tanto para e-voting como en el marco general de e-democracia. A estos retos pretende contribuir este trabajo.

3.7. EVALUACIÓN DEL PROYECTO SOBRE LA INICIATIVA CIUDADANA TAURINA

La experiencia del uso de la firma electrónica para el apoyo de la proposición de Ley en favor de los toros, conocida como "Proposición de Ley para la regulación de la fiesta de los toros como Bien de Interés Cultural" [76], ha sido utilizada por la plataforma de la ILP como un recurso que no sólo ha sumado nuevas firmas (digitales), sino que ha permitido dar mayor visibilidad y repercusión a la ILP, redundando en la ILP en formato papel gracias al impacto social y mediático que el proyecto ha tenido como se indica en los datos más adelante.

Una vez que la Junta Electoral Central autorizaba al proyecto de software libre OpenILP como plataforma de firma digital válida en España, la iniciativa estuvo en 2012 durante cuatro meses en producción. El número de usuarios participantes en el portal www.ilptaurina.com (equivalente a openilp.org/taurina, taurinos.openilp.org) ha sido de 33.821, la mayoría durante el primer mes, como puede observarse en la gráfica siguiente:

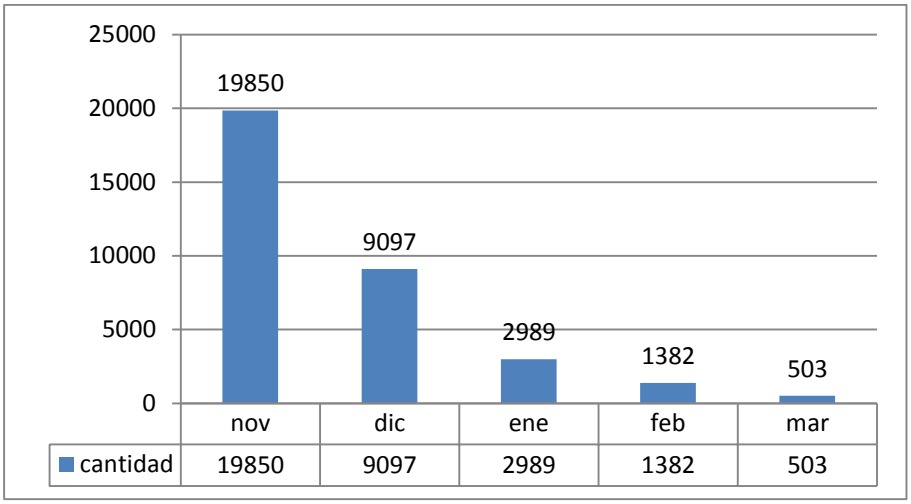


Figura 21. Participantes durante la fase de producción

Por otro lado, la difusión de la iniciativa electrónica ha permitido darle un nuevo impulso mediático a la ILP, por lo la iniciativa ciudadana resultó un éxito. Sin pretender ser exhaustivo, algunos medios donde el proyecto ha tenido repercusión son:

- Telediarios mediodía y noche. TELECINCO
- Diario La Razón, (edición digital), así como banner permanente del proyecto para invitar a la firmar
- Radio COPE, en varias ocasiones, y en la web banner para firmar
- Televisión Española, programa "Tendido Cero"
- Revista Burladero, edición digital, seguimiento continuo, con banner
- Revista Mundo Toro, edición digital, así como banner
- Radio, programa taurino L'H, entrevista sobre OpenILP
- Multitud de programas radiofónicos, televisivos y webs taurinas especializadas: barcelonataurina.com, vadebraus.com, etc.
- Uso de redes sociales: Facebook y Twitter.

La figura 22 y 23 muestran una imagen de la repercusión en algunas de las publicaciones en prensa nacional e internacional (Francia) que ha tenido el proyecto.

La ganadería de « Valdellán » pour la novillada lidiée à Parentis-en-Born le 7 août dernier par Daniel Martín, Juan Manuel Jiménez et Sergio Blanco.

Le prix « TIO PEPE » est décerné au picador français Gabin Rehabi pour ses suertes magistrales avec la pique durant toute la temporada et en particulier à l'occasion de la corrida de Victorino Martín à St-Vincent-De-Tyrosse, tout comme à l'occasion de la corrida concours des élevages français du 5 août à Vic-Fezensac.

Le prix « Monosabio » à Mr le Maire de Mimizan pour avoir maintenu la corrida du 27 août dans leurs arènes (première corrida formelle de l'histoire taurine de cette commune du Nord des Landes) en dépit des nombreuses pressions exercées par les anti-taurins.
(Pierre Vidal)

ILP

Vous êtes de nationalité espagnole, vous êtes de surcroît aficionado, alors ne tardez pas à participer à l'ILP engagée par la « Federación de Entitades Taurinas de Catalunya » car il manque encore à ce jour 95.000 signatures et vous pouvez apporter directement votre contribution en cliquant sur http://www.openilp.org/taurinos/proyecto.do?opcion=firma

Si vous connaissez des Espagnols susceptibles de participer à cette campagne, faites-leur connaître cette possibilité car maintenant le temps presse...

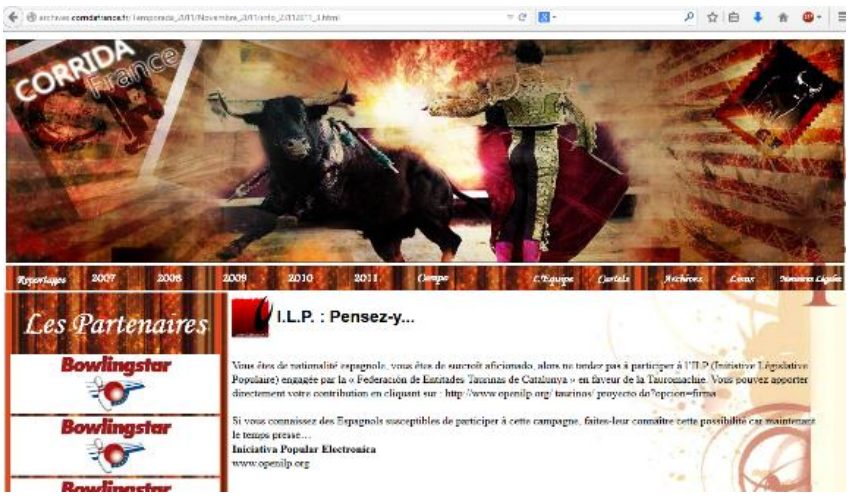


Figura 22. Repercusión en prensa francesa

Jueves, 10 Julio 2014. Actualizado a las 15:08h

LA RAZÓN.es

OPINIÓN ESPAÑA INTERNACIONAL ECONOMÍA SOCIEDAD SALUD RELIGIÓN DEPORTES MOTO

SE HABLA DE El desafío independentista Inversiones Consejo de Ministros Crecimiento eco Medidas económicas Congreso Autónomos Grupos

TOROS

Ya se puede apoyar la ILP taurina con la firma digital

Ya se puede usar la firma digital para apoyar la Iniciativa Legislativa Popular que pretende recoger 500.000 firmas para que la Fiesta de los Toros sea declarada Bien de Interés Cultural en España. www.ilptaurina.com

Me gusta 0 Twittear 3 Share

Ya se puede apoyar la ILP taurina con la firma digital

19 de noviembre de 2011, 17:22h

La Razón. Madrid.

La Iniciativa Legislativa Popular (ILP) que pretende que la Fiesta de los Toros sea declarada Bien de Interés Cultural en España está recogiendo firmas con el objetivo de alcanzar las 500.000, cantidad necesaria para que la iniciativa sea admitida a trámite en el Congreso de los Diputados.

La Comisión Promotora de la ILP taurina en colaboración con la Escuela Superior de Ingenieros e Informáticos de la UNED, ha creado un sistema por el cual los ciudadanos puedan utilizar su firma electrónica para dar apoyo a una ILP.

Hasta la fecha, llevan recogidas algo más de 400.000 y, para alcanzar su objetivo del medio millón, han puesto en habilitado la firma digital. Así, por primera vez en la historia de nuestra Democracia ya se puede apoyar una iniciativa Legislativa Popular con la firma electrónica. El mundo taurino ha sido el primero en poner en práctica una acción que facilitará de un modo fundamental, que la sociedad pueda hacer oír su voz.

Para ello, tan sólo será necesario acceder a la web http://www.ilptaurina.com donde existe un banner. Tan sólo hacen falta 30 segundos para introducir los datos y firmar digitalmente. Se debe recordar que aquellas personas que ya hayan firmado la ILP, no pueden volver a hacerlo. Es imprescindible respetar esta norma, ya que lo único que se conseguiría es dificultar el trabajo dela Comisión Promotora, que contará con unas firmas que posteriormente no iban a ser validadas por el Congreso de los Diputados.

La firma electrónica de la ILP Taurina está basada en un proyecto de software libre, llamado OpenILP, realizado por la Escuela Superior de Ingeniería Informática dela UNED. La herramienta servirá para futuros procesos de este tipo.

Figura 23. Artículo en prensa nacional sobre el proyecto OpenILP

Por otro lado, el proyecto ha sido conocido en los ámbitos académicos de ciencias políticos y derecho, como se ha constatado en la UOC y en la Universidad de Valladolid [77]. Y en otro orden de cosas, el interes de varios indexadores software donde el proyecto ha sido catalogado y clasificado como TIC de participación y democracia.

Se ha constatado el interés de aquellas personas que, no habiendo firmado ya, querían hacer el esfuerzo de realizar la firma por vía digital. De los participantes, 6.298 les fue imposible firmar por problemas técnicos y otros 4.916 estaban interesados en tener un certificado digital válido para realizar la firma.

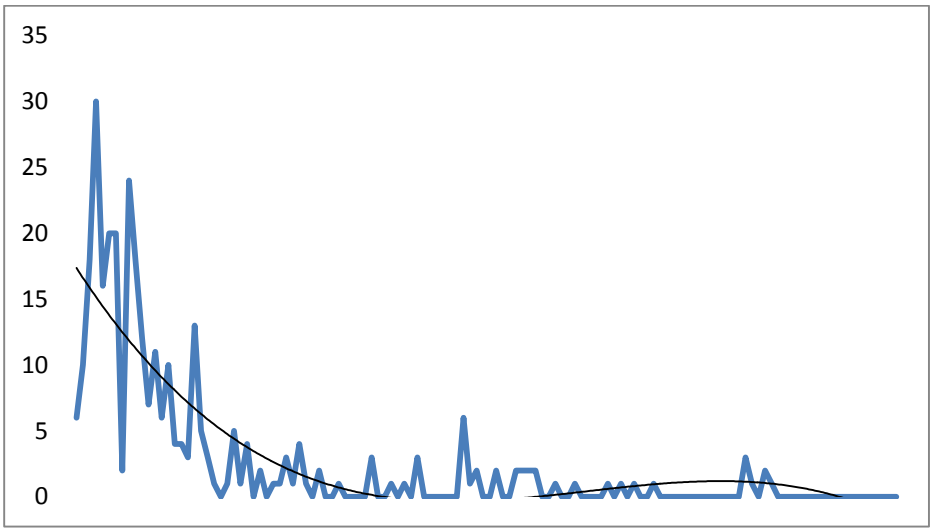


Figura 24. Curva de participación en operación y tendencia

El mérito de la ILP taurina ha sido haber movilizado a un colectivo tan tradicional como el aficionado taurino y poner en marcha el reto tecnológico de utilizar firma digital para proponer una ley en el Parlamento.

Figura 25. El proyecto en televisión, ediciones Telediarios Telecinco

Figura 26. Repercusión en radio, emisión COPE

Figura 27. Instantánea de la invitación al Congreso de los Diputados, junto a la comisión organizadora

En 2012 al sobrepasar la cantidad de firmas requeridas, se presentaron en el Congreso de los Diputados[3], donde una comitiva representativa fue invitada por el Presidente del Congreso, a la que asistimos en reconocimiento del impulso que la iniciativa electrónica tuvo en la consecución del objetivo. La Figura 26 muestra una instantánea del momento, en el hemiciclo del Congreso junto a varios de los representantes de toreros. A principios de 2013 se inicia la tramitación parlamentaria de la nueva ley que finalmente se aprobaría[4] en noviembre de 2013.

[3] http://politica.elpais.com/politica/2012/03/22/actualidad/1332420896_634433.html
[4] http://www.elmundo.es/cultura/2013/11/06/527ab20e684341e70a8b4576.html

3.8. CONCLUSIONES

Un modelo de arquitectura distribuida para e-democracy y que puede aplicarse a las Smart Cities ha sido presentado. Este framework reparte las cargas organizativas y económicas entre los agentes sociales y los gobiernos.

Se ha desarrollado un proyecto software que implementa un nodo de plataforma ciudadana. Se ha certificado técnicamente por el Parlamento de España, obteniendo el visto bueno gubernamental. Con ello, tiene todas las bendiciones para poderse extender a los gobiernos regionales y locales.

Finalmente se ha puesto en práctica mediante una experiencia que ha servido para perfeccionar el modelo propuesto. Como trabajo de investigación para el futuro se considera importante avanzar en la línea de la normalización y la estandarización de la Smart Governance y de un protocolo estándar de intercambio de información para e-democracy que garantice la interoperabilidad, abarate costes de producción y mejore el avance de la democracia electrónica directa.

Capítulo 4.

DOMINIOS CRÍTICOS SOBRE SEGURIDAD, CRIMINALIDAD Y TERRORISMO

4.1. INTRODUCCIÓN

La gestión de los sistemas de información en entornos arquitectónicos de seguridad crítica precisa en todos los sectores de un contexto estable y bien definido para la consecución de sus objetivos. Sin embargo, como es bien sabido y sufrido por la gran mayoría de sus gestores esta estabilidad es en el mejor caso muy relativa. La necesidad de los responsables informáticos (CIO) para adaptarse a los cambios de visión de los responsables del negocio (CEO) provocados por nuevos modelos de negocio asociados normalmente a la propia irrupción de nuevas tecnologías es el día a día en las empresas.

Entre los retos emergentes de la seguridad nacional de muchos países están la protección de personas e infraestructuras críticas, especialmente en dominios de ciberseguridad industrial que afectan masivamente a la población. Los Gobiernos se están concienciando alrededor de estas amenazas, elaborando legislaciones nacionales

o mejorando las que ya tienen para potenciar la colaboración entre agencias gubernamentales, empresas y ciudadanos. Aunque existen esfuerzos por desmitificar la complejidad de la ciberseguridad, como en [93], sin embargo, no existe un criterio claro en cuanto la forma de construir sistemas de información para evitar los riesgos de seguridad global cuando intervienen múltiples países, muchos sectores industriales y además ciudadanos de diferentes nacionalidades. De acuerdo con Landau y otros [94], alrededor de la ciberseguridad hay una crisis de priorización por parte de los gobiernos.

Este capítulo revisa la literatura de sistemas y arquitecturas de seguridad pública internacionales, de protección de personas e infraestructuras. Proponemos un modelo colaborativo de seguridad global donde pueden congeniar los sectores industriales y organismos públicos. Exponemos un caso práctico, la experiencia y las lecciones aprendidas en el desarrollo de una red eGovernment para el comercio de productos industriales peligrosos. Como discusión se evalúa el modelo desde el punto de vista de eGovernment, mejorar la colaboración ciudadana, implicar a las empresas e industrias afectadas, como puede ser el caso del control, prevención y protección de sustancias químicas peligrosas, suministros eléctricos o abastecimiento básico para la población, así como mejorar el control que evite su potencial objetivo dentro del uso delictivo o antisocial. Describiremos las consideraciones técnicas a tener en cuenta, las dificultades derivadas de su alcance supranacional y las particularidades derivadas de fusionar eGovernment y empresas privadas en un sistema de información distribuido para la seguridad colectiva.

En este capítulo se describe la gestión y consideraciones tecnológicas en la arquitectura de software y el enfoque ejecutivo para un proyecto que necesita requisitos de seguridad críticos y multifacéticos. Como consecuencia uno de los planteamientos necesarios es la promoción de medidas en relación con el intercambio de información por parte del sector privado a través de las redes públicas. Los arquitectos en tecnología ponen caminos para abordar estos problemas y sus dificultades desde el punto de vista de las modelos técnico-organizativas de e-Gobierno que se pueden aplicar. Las restricciones y condicionantes de los países en desarrollo y la necesidad de fomentar una alianza mundial para el desarrollo lo convierten en un reto más complicado [95].

En este sentido la gestión de la tecnología de la información y las comunicaciones (TIC) juega un papel multidisciplinar. Además los GCIO deberían abordar con gran precisión y grado de concreción los beneficios de una política pragmática de proyectos específicos, compartidos por todos los estados/partes participantes y relevantes para todos ellos.

4.2. ESTADO DEL ARTE, REVISIÓN DE LA LITERATURA Y TRABAJOS CONEXOS

El efecto de la globalización ha sido estudiado profusamente desde distintos planos, especialmente el económico, incluyendo los efectos que produce sobre la brecha digital entre países desarrollados y países en desarrollo. Sin embargo en la actualidad se considera que las tecnologías de la información y las comunicaciones (TIC) son recursos de los que disponen los gobiernos para incentivar la economía, más

si cabe en los países no desarrollados o en vías de desarrollo, siguiendo estudios de expertos de Naciones Unidas [96]. Zoughbi y otros consideran que invertir en la sociedad de la información y aprovechar las herramientas técnicas constituye una forma dinamizadora que reduciría la distancia entre países ricos y pobres.

4.2.1. EL ROL DEL GCIO

Las responsabilidades del CIO en el sector público o GCIO, de cualquier Gobierno resultan crucial para la economía, pero también para el progreso social y político de un país.

En la literatura respecto de las funciones del GCIO nos debemos remontar a la que se encuentra recogida en la regulación federal de la Administración americana, conocida como Clinger-Cohen Act (CCA) de 1996. Configuró un cuerpo de competencias que servía de base para perfilar el trabajo de los encargados de los sistemas de información gubernamental[5]. En esta norma se delega en las distintas regiones el desarrollo y mantenimiento de las arquitecturas de IT con la idea de maximizar los beneficios del uso de los sistemas de información y establecer estructuras de contabilidad y auditoría para el gasto. Esto es una aproximación hacia

[5] http://govinfo.library.unt.edu/npr/library/misc/itref.html, "Information Technology Management Reform Act" (1996)

la descentralización económica para hacer más ágiles políticas de IT, en la dirección de la reducción de papel y facilitar los procesos de rediseño.

Del mismo modo, en el ámbito de los Estados, los responsables gubernamentales de los sistemas de información deben tener en cuenta los posibles cambios, tanto de prioridades o como de intereses de sus CEOs, los gobiernos, con las particularidades que cada país presenta especialmente en países en desarrollo. Relacionado con esto, algunos autores, como Isaak [97] sostienen que los gobiernos deben actuar como "consumidores sabios".

Un GCIO que trabaja en una región en desarrollo y a menudo con limitaciones de recursos (aunque podríamos permitirnos decirlo para todo tipo de responsables y espacios) debe tener en cuenta los principios que inspiran una adecuada sostenibilidad social. La organización de las Naciones Unidas en su informe [98] sobre la agenda post-2015 mencionó en primer lugar que los grandes objetivos del milenio deben adaptarse a los desafíos actuales como consecuencia de la expiración del plazo para su cumplimiento [99]. Esto incluye contrarrestar el efecto de las desigualdades dentro de los países con motivo de la globalización, y en un segundo orden, la degradación ambiental, el desempleo y la violencia.

4.2.2. EL EQUIPO HUMANO

Es obvio que una de las capacidades de primera magnitud en el éxito de cualquier reto de TI son los recursos humanos, tanto en el plano de gerencia como de cualificación. En el sector tecnológico se ha estudiado especialmente el fenómeno del outsourcing como mecanismo para ampliar o sustituir el esfuerzo necesario para la

ejecución de un proyecto. Para situarnos resulta interesante la revisión histórica en [100], donde los autores parten de los antecedentes previos a los últimos 30 años y los trabajos de investigación en este tema. Siguiendo la literatura sobre este tema, como en [101], queda consolidada la idea de que la dirección de recursos en la industria de la tecnología es una actividad compleja en la hay que considerar la participación múltiple y externa. Un ejemplo de la realidad actual podemos encontrarla en multitud de compañías que se dedican a la fabricación de dispositivos electrónicos o a la prestación de servicios, donde la marca empresarial representa en la práctica un trabajo de integración donde las piezas y los recursos los facilitan otras empresas subcontratadas.

4.2.3. FACTORES CRÍTICOS Y TENDENCIAS

En cuanto al desarrollo software de sistemas de información es interesante la valoración del riesgo que supone tanto la gestión como la externalización. Como mencionan algunos estudios, como en [102], pueden llegar a un alto porcentaje de fracaso (incluso 50%) si no se tienen en cuenta los factores críticos de éxito desde el punto de vista del ciclo de desarrollo. Siguiendo este trabajo, podemos centrar nuestro interés en la identificación de las 12 áreas para agrupar los factores clave de un proyecto:

- Definición de requisitos
- Diseño
- Programación y realización de pruebas de código

- Integración y pruebas del sistema
- Migración de datos
- Paso a producción y transferencia tecnológica
- Integración del entorno de negocio
- Control y gestión de la planificación
- Gerencia y liderazgo
- Gestión comercial
- Seguridad, auditoría y gestión de riesgos
- Relaciones personales

En cuanto a los factores críticos, en otros trabajos como en [103] se enumeran siete elementos que teóricamente deben tenerse en cuenta grandes proyectos de tipo ERP, aunque puede servir como orientación a otros proyectos complejos o de grandes dimensiones:

- la comprensión clara de los objetivos estratégicos
- el apoyo decidido de la alta dirección
- una gestión excelente del proyecto
- la existencia de una gestión del cambio a nivel de negocio
- un buen equipo de implementación
- la calidad y precisión en los datos
- amplia educación y formación de usuario

Sin embargo, siguiendo los informes de Gartner [104] sobre los proyectos de carácter gubernamental, los GCIOs y responsables TI en general necesitan tener en

cuenta la propia cultura de la organización, que en el caso del Gobierno es esencial, los procesos y la tramitación burocrática, los sistemas de información heredados (legacy) que deben de mantenerse, el presupuesto y las dificultades para encontrar perfiles especializados adecuados en función de los proyectos y de la tecnología a utilizar. Las tendencias principales subrayadas en el sector público incluyen las arquitecturas escalables basadas en Web, del que tratamos en gran medida en este trabajo, y otras como Clouds híbridos, Internet of Thing, plataformas de smart cities, análisis de Big Data y la identificación electrónica e-ID. A esto hay que sumar la apertura de datos, el acceso multicanal, la recurrente oficina digital y la interoperabilidad que cubre una vasta área de investigación como en [105] y en [106]. Es interesante resaltar en la prospección a que nos referimos la influencia que la apertura de datos supone en la sociedad: se estima que en 2018 alcance el 30 por ciento de toda la información gestionada por sistemas de administración electrónica.

4.2.4. PROYECTO INTERNACIONAL: SCEPYLT

Como referencia nos apoyamos en un proyecto de intercambio de información sobre explosivos cuya concepción, arquitectura, diseño, desarrollo y primera implantación ha sido dirigida técnicamente por ese disertante. Bautizado con la denominación SCEPYLT (siglas en español de Sistema de Control de Explosivos para la prevención y lucha contra el terrorismo) la Unión Europea decidió desarrollar el sistema a medida [107]. Para este fin el Proyecto fue apoyado como parte del programa específico de la

Comisión Europea, en concreto de la Dirección General de Justicia, Libertad y Seguridad bajo la denominación del epígrafe para la prevención y gestión de las consecuencias del terrorismo y otros riesgos de seguridad (literalmente conocido como "Prevention, Preparedness and Consequence Management of Terrorism and other security related risks" - CIPS).

Hasta la fecha el sistema ha sido adoptado como plataforma de intercambio de información por todos los países de la Unión Europea, complementando otras iniciativas tecnológicas como el proyecto "European Bomb Data System" y otros, como el "Early Warning System" para temas de seguridad y propósitos policiales bajo los auspicios de Europol [108].

Como puede deducirse las características propias de SCEPYLT lo convierten en un ejemplo bien conocido para el análisis de dificultades y oportunidades. Es necesario determinar una tecnología común, deben compartirse datos muy sensibles, afecta a los estados y a la industria, requiere de altos niveles de seguridad etc. Y los beneficios son compartidos por todos los participantes.

Aplicaciones análogas con dificultades y soluciones similares son el control del transporte de ayuda humanitaria. A nivel de política internacional, incluso de la ONU, existe esta preocupación sobre promocionar la armonización del Derecho en áreas de negocio que afectan a la seguridad global y que permitan asimismo una rendición de cuentas entre las partes interesadas y con la sociedad. A través de estrategias tecnológicas para compartir información con criterios organizativos confiables y benevolentes en cierto sentido, el resultado puede ser económicamente viable. Esto supone una revisión de los esquemas de cooperación entre el sector privado y el sector

público, así como entre estos últimos. Este paradigma supone un hervidero de ideas de eGovernment conocido como P3 o PPP (Public-Private Parnertship) particularmente en áreas económicas y de gestión de empresas. De cualquier forma, los niveles nacionales, regionales y locales están preocupados por remover las barreras y promocionar buenas prácticas para alcanzar a cubrir las necesidades que demandan sus ciudadanos dentro de la sociedad digital. A estos efectos vamos a exponer en las secciones siguientes algunos de los puntos clave sobre la gestión de dominios de seguridad crítica y las lecciones aprendidas sobre el desarrollo de grandes proyectos de información. No obstante, se entiende que ante situaciones concretas es necesario un razonamiento y ajuste propio de las particularidades del ecosistema del proyecto en concreto.

4.3. GESTIÓN DE DOMINIOS DE SEGURIDAD CRÍTICA

En cuanto a la tecnología, las soluciones socio-políticas y la emergente aparición del Open Government, la situación del panorama técnico presenta una elevada tendencia a la innovación que ya se está empezando a concretar. Los esquemas de tramitación en eGovernment se enfrentan a una realidad donde los ciudadanos son digitalmente más exigentes y el paradigma burocrático debe revolucionarse por completo como consecuencia de la apertura del sector público, incluida la adaptación de los puestos de trabajo.

El acceso a la información y a los procedimientos administrativos multicanal va en esta línea y deben asumirse con la naturalidad con la que la sociedad toma del día a día. Una transformación que necesita liderazgo y la participación activa del GCIO como elemento articulador del ecosistema de gobierno electrónico. Pero también una nueva forma de hacer las cosas. Como muestra cabe mencionar una de las metodologías que, si bien aplicada a cualquier tipo de proyecto con experiencias muy interesantes en proyectos de tecnología, apuesta por la creatividad y la agilidad. Estamos hablando de la corriente de pensamiento del diseño (Design Thinking) donde las ideas innovadoras son pragmáticas y centradas en los usuarios. De hecho hay autores [109] que gráficamente lo describen con la alegoría de salir del palacio para en cambio poner la tienda de campaña.

El fenómeno de la apertura de datos por los Gobiernos está provocando la distribución y publicación masiva de conjuntos de datos (datasets) y de construcción de APIs (interfaces de acceso a aplicaciones) por todo el mundo. Sin embargo la madurez de las estructuras y tecnologías relacionadas con Open Data sigue en desarrollo, con lo que la necesidad de investigación científica en esta área es emergente como se muestra en [110] y en otros trabajos concretos como [111].

Al margen de tener en cuenta las cuestiones relacionadas con la política y la diplomacia, podemos entender que la cooperación internacional se presenta como una ventana hacia la solución. Para construir entornos colaborativos de información es necesario aislar en algún grado las situaciones inestables que no favorezcan las relaciones bilaterales entre los distintos gobiernos que intervienen en el dominio del problema. En este sentido también podemos tomar nota de la industria de

manufacturación sobre el campo de Redes Colaborativas (CN) para conseguir una mayor agilidad en las cadenas de suministros debido a la cambiante regulación y la necesidad de agilidad empresarial [112].

Realmente respecto a este tipo de proyectos interestatales es deseable que estén amparados o coordinados por un organismo internacional, que pueda ayudar a facilitar la estructura del proyecto. Evidentemente, la ONU, la UE y similares juegan a ese rol habitualmente. Sin embargo, asociaciones internacionales técnico-profesionales como IEEE, con amplio despliegue, o incluso organizaciones no gubernamentales pueden realizar esa coordinación básica y facilitar así un elemento de partida para la estabilidad del proyecto que permita generar confianza. La confianza es uno de los primeros parámetros que debe ganar un proyecto interestatal, ya que de eso va a depender la fidelidad de los participantes y la adhesión de los indecisos, en lugar de ser motivo o excusa para desencuentros. En la búsqueda de un equilibrio político en la construcción de grandes sistemas de información eGov entre varios gobiernos a veces este tipo de organizaciones neutrales pueden jugar un papel fundamental para el buen entendimiento de los estados participantes sobre la base de la profesionalidad y la tecnología.

No obstante hay que reconocer que generalmente este tipo de proyectos son técnicamente complejos y no están exentos de dificultades. Incluso en Estados con cierta estabilidad económica, política y social pueden producirse desencuentros irrenunciables. Esto ocurre en ocasiones al enfrentarse diferentes intereses legítimos en un asunto del que se informa el proyecto, al igual que existen conflictos internos

entre diferentes Administraciones de un mismo estado. Cuestiones tales como las decisiones sobre la tecnología a utilizar, la forma de gestionar y compartir los datos cuando estos son especialmente sensibles para todos los participantes y el control del proyecto puede constituirse en obstáculos insalvables.

La seguridad en el ciberespacio después de los atentados terroristas de New York del 11-S tiene cada vez más importancia en la agenda de los gobiernos, lo que afecta también en el plano tecnológico [113].

La amenaza terrorista ha sido una preocupación constante en las sociedades modernas, por ello se han establecido recomendaciones, disposiciones normativas y encomiendas de mayor o menor calado. Pero desde los ataques del 11 de septiembre las medidas políticas y sociales no se hicieron esperar, especialmente decisiones marco e incentivos para mejorar la cooperación policial y judicial.

La importancia de compartir información entre administraciones públicas, entre sectores industriales estratégicos, entre grupos sociales con intereses comunes pone a los ingenieros de la información ante un reto tecnológico, debido a la envergadura, las distintas sensibilidades políticas, la protección de la privacidad y la autonomía nacional de cada estado. Las empresas se ven condicionadas por las normativas legales nacionales y la propia competencia del sector económico en su ámbito privado. Ejemplos de estos sectores son las líneas aéreas, el control de viajeros, los fenómenos migratorios, el control del fluido eléctrico, el transporte de energía, entre otros.

Este capítulo describe la gestión y las consideraciones tecnológicas sobre arquitectura y modelos que necesitan una aproximación pragmática a dominios de seguridad crítica y multi-facetada.

4.4. FRAMEWORK DE E-GOV SOBRE TERRORISMO

En este apartado se presenta un modelo desarrollado como solución técnica contra la problemática terrorista en el marco de seguridad de la Unión Europea. Se define técnicamente la arquitectura software, los criterios de gestión y dirección técnica, las lecciones aprendidas y los beneficios obtenidos con este framework. Se expone la experiencia con mayor nivel de detalle y se evalúa el impacto. De este modo se presentó una propuesta técnica que estaba recogida en la propia inquietud de la directiva europea para intercambio de información sobre explosivos. Pero siendo lo suficientemente ambiciosos como no solo compartir información de transacciones comerciales, sino del propio inventario individualizado de las partidas transportadas, lo que permitiría un control detallado, exhaustivo y en tiempo real.

4.6.1. MOTIVACIÓN Y CONTEXTO DE TRABAJO

La tragedia del 11 de septiembre de 2001 en los Estados Unidos, los atentados terroristas del 11 de Marzo de 2004 en Madrid y, posteriormente, del 7 de julio de 2005 en Londres, conmocionaron a los ciudadanos del mundo, por el número de víctimas mortales y por la sensación de fragilidad de los países ante estos hechos, ocurridas en vías y transportes públicos a horas puntas.

Por otro lado, los procesos judiciales abiertos en Europa mostraron de forma alarmante que gran cantidad de los explosivos utilizados habían sido desviados de su curso comercial, robados o hurtados, resultando difícil de controlar policialmente [116]. Los explosivos son utilizados en el sector civil para industrias mineras, extracciones de materiales, demoliciones y voladuras controladas, perforaciones, explotaciones agrarias, etc. Estas sustancias viajan a diario por nuestras carreteras, ferrocarriles, vías marítimas y aéreas: es un producto comercial, que va desde dinamitas, cápsulas detonadoras, cartuchería, pólvora de caza y productos pirotécnicos. La normativa europea sobre estas materias previene sobre el riesgo que suponen en su diseño, fabricación y manipulación, unas directrices básicas para la armonización del mercado y control de los explosivos con fines civiles [117], pero a la luz de los atentados se observaron insuficientes en la práctica.

La preocupación de los Gobiernos por aquellos atentados trasladó a primer plano la necesidad de la prevención y el control de los explosivos [118]. Los ministros del Interior de los países integrantes del G5 (España, Francia, Reino Unido, Italia y Alemania) reunidos en la ciudad inglesa de Sheffield, 5 y 6 de julio de 2004, trataron, entre otros asuntos, la lucha contra el terrorismo. Esta será una de varias reuniones a alto nivel para potenciar las relaciones de cooperación entre estos cinco países con el fin intensificar sus relaciones para hacer un frente común contra al terrorismo y el crimen organizado. Entre los acuerdos políticos tomados, en este caso, se encontraba promover trabajos relativos al control de explosivos en la Unión Europea, siendo designada España la encargada de impulsar este proyecto [119].

En 2005 se creó un grupo de trabajo con este propósito, formado por expertos en explosivos de los cinco países y representantes de la Comisión Europea, grupo al que posteriormente se une Polonia, formando el denominado G6. El trabajo fue dirigido por la Guardia Civil de España, cometido que le encomendó la Secretaría de Estado de Interior dentro del mismo Ministerio. Tras una primera reunión se establecen un conjunto de líneas a seguir para promover el estudio sobre la seguridad de los explosivos en Europa. Una de estas líneas se centró en analizar qué podían aportar las nuevas tecnologías, para lo que se requirió el asesoramiento del Servicio de Informática la Guardia Civil. De esta reunión surge el encargo de proponer una solución informática, partiendo de que no existía ningún sistema electrónico actual en uso, que aportara mejoras y fuera viable económicamente. Tras un análisis tecnológico se elaboró un diseño arquitectónico para realizar el sistema informático distribuido que ya hemos introducido con el nombre de SCEPYLT. Su objetivo es mejorar el control de explosivos intercambiando información entre los países del G6 de una forma ágil, estándar y segura. Se trata recapitulando en un proyecto de ingeniería de sistemas distribuidos cooperativos sobre múltiples bases de datos sincronizadas mediante SOA para el control de información sobre explosivos.

En la segunda reunión del grupo de trabajo, en febrero de 2006, se presentó esta solución técnica, siendo ampliamente aceptada y apoyada por el grupo. La propuesta en esencia consistió en crear una base global de información entre los seis países, donde, entre todos, se tuviera toda la información sobre explosivos que transiten entre ellos, mediante nodos geográficamente distantes formados por bases

de datos locales, múltiples pero sincronizados adecuadamente. Además cada país alojaría la información que le afectara directamente o bien participaran dentro del itinerario en algún transporte, esto es, constituyéndose en un fragmento de esa base global. Esto supondría una redundancia de información, con criterio funcional, establecida a propósito, que permitiría determinada autonomía de un país para gestionar consultas básicas sin necesidad de que el resto de nodos estuviesen activos.

De este modo se presentó una propuesta técnica que estaba recogida en la propia inquietud de la directiva europea [120], en cuya redacción ya instaba a crear redes de datos para intercambio de información sobre explosivos. Se previó no sólo intercambiar información sobre autorizaciones de transportes, sino que además del contenido pormenorizado de las partidas transportadas, permitiendo su trazabilidad, lo que permitiría un control detallado, exhaustivo y en tiempo real de los explosivos. La trazabilidad supuso la necesidad de armonizar la normativa de los países europeos, lo que años después concluyó en la Directiva 2008/43/CE, modificada en la Directiva 2012/4/UE, 22 de febrero, de la Comisión Europea, y en la Directiva 2014/28/UE del Parlamento Europeo y del Consejo relativa a la armonización de las legislaciones nacionales en materia de comercialización y control de explosivos[6].

En esta solución técnica, que se presenta en el marco del grupo de trabajo de explosivos, definía técnicamente la arquitectura software, bajo las premisas de una arquitectura Java Enterprise orientada a servicios web, con intercambio de información en XML mediante protocolos semánticos, el uso intensivo de patrones de diseño y

[6] Diario oficial de la Unión Europea, http://www.boe.es/doue/2014/096/L00001-00044.pdf

buenas prácticas de desarrollo. A esto hay que añadir la definición de exigentes niveles de seguridad informática, de una rápida y fácil escalabilidad para añadir nodos/países, la creación de un protocolo de comunicación semántico XML, el enfoque de Administración Electrónica, posibilitando la participación de empresas del sector para agilizar los trámites burocráticos y cooperar con la seguridad en la trazabilidad, el soporte a tecnologías criptográficas de clave pública, y el uso de una metodología expresamente definida para este proyecto. En resumen, se tomaron criterios que garantizaran la conformidad con estándares, fomentando el uso de software libre y fuentes abiertas, para asegurar la portabilidad del proyecto sobre la mayoría de plataformas tecnológicas Java EE disponibles en el mercado.

Hubo un plazo de varios meses, donde se recibe el *feedback* de los países representantes del grupo de trabajo, tanto técnicas como funcionales, que conllevaría el visto bueno para el análisis y diseño arquitectónico propuesto. Seguidamente, la construcción informática se encargó a una empresa especializada en Software Factory, lo que supuso la contratación mediante procedimiento de concurso tipo informático propia de la Administración española. Este procedimiento resultó en la colaboración mediante outsourcing en la que participó la Empresa Soluziona, que posteriormente fue adquirida por la multinacional Indra. Posteriormente, se sufragaron los gastos de la red de trabajo sobre explosivos mediante una subvención de la Unión Europea del Programa de Cooperación Policial y Judicial en Materia Penal (AGIS), proyecto llamado "Procedimiento sobre Sistema de Control de Explosivos para la Prevención y Lucha contra el Terrorismo".

Durante el desarrollo, que duró unos seis meses, se utilizó una metodología de desarrollo orientada a procesos, iterativa e incremental, definida dentro del proyecto, donde en esencia se combinaron: técnicas metodológicas ágiles con aspectos de otras más formalizadas, como la metodología Metrica 3 de la Administración Pública española y la metodología de desarrollo software de la *European Space Agency* [121]. De esta forma, se planificaron y diseñaron tres iteraciones software o pilotos, que bajo un estrecho seguimiento, directo y cercano, debía facilitar poder ajustarse en el tiempo esperado, máxime cuando las reuniones del grupo europeo de trabajo eran pocas y muy rígidas en el tiempo (generalmente dos al año).

Durante cuatro años se han realizado una docena de reuniones de los seis países participantes en Madrid, así como miembros de la Comisión Europea. Dada la envergadura que está teniendo el proyecto, se requirió la presencia adicional de un responsable informático por cada país, formando un subgrupo de trabajo que se reuniría en paralelo y así descargar de los detalles técnicos al grupo de expertos sobre explosivos. Una vez finalizada la construcción del sistema se comenzaron a realizar las pruebas en un entorno de pre-producción resultando satisfactorias, poniéndose en marcha el sistema en paralelo al procedimiento tradicional.

A propuesta de la Unión Europea se plantea este proyecto como sistema de intercambio de información sobre explosivos para los países de la Unión. Para ello, se subvencionó el proyecto de expansión en la convocatoria de ayudas de 2007 en la partida presupuestaria del Programa específico «Prevención, Preparación y Gestión de las consecuencias del terrorismo y de otros riesgos en materia de seguridad» de la Dirección General de Justicia, Libertad y Seguridad de la Comisión Europea. A día de

hoy el proyecto SCEPYLT ha sido adoptado como plataforma para el intercambio de información europea universal para veintiocho países [122].

En este trabajo se presentan las ideas fundamentales de ingeniería para un sistema distribuido de base de datos, que ha servido de soporte para la construcción de la aplicación SCEPYLT. En concreto se trata de un diseño de ingeniería donde la información global se encuentra distribuida entre entidades distantes geográficamente, formando así un sistema de base de datos completamente descentralizado, mejorando la eficiencia de las consultas mediante el particionado horizontal y la redundancia de fragmentos sobre un subconjunto parcial de nodos. Este diseño se ha aplicado en la práctica satisfactoriamente en el ámbito del control de explosivos de uso comercial a nivel europeo y prevenir así su desvío fraudulento hacia actividades terroristas.

4.6.2. PRINCIPIOS BÁSICOS DE UN SISTEMA DISTRIBUIDO INTERNACIONAL

Los organismos públicos estatales suelen tener grandes sistemas computacionales, sumados a grandes redes. La complejidad de interconexión de estos sistemas radica en muchas ocasiones en la variedad de los responsables funcionariales y en la propia organización de red interna, lo que puede dificultar a veces el despliegue de aplicaciones, la detección de errores del sistema y cambios en la configuración. De

la experiencia se pueden extraer los siguientes principios básicos que pueden resultar muy útiles para el desarrollo de aplicaciones distribuidas internacionales.

Uno de los primeros principios que debemos plantear es que la tecnología es alegóricamente muy soberana. Aquí podríamos añadir a países, grandes corporaciones y empresas. La tecnología si bien tiene un carácter universal, pero cada parte interesada elige la parte de tecnología de forma reivindicativa en muchas ocasiones. De hecho, al margen de las directrices comunitarias, la ejecución de los sistemas informáticos corresponden a los organismos de cada país. Como consecuencia de esta naturaleza soberana del uso de la tecnología y elección de la misma, un proyecto de desarrollo transnacional debe desarrollarse pensando en que cada miembro podrá aceptar con agrado, o con reticencias, las soluciones desarrolladas, porque está condicionado por múltiples factores internos: económicos, socioculturales, organizativos, políticos… propios de una pluralidad de intereses. Admitir este enfoque supone respetar las opciones tecnológicas de cada uno y, en consecuencia, aceptar la flexibilidad y el esfuerzo extra que supone.

Se debe poner de relieve un principio básico en el trabajo colectivo que es la cooperación benevolente, donde se debe presumir que los participantes cooperan para llegar a una solución común, de forma leal y constructiva. Además la transparencia en el ciclo de desarrollo implica que la información técnica debe estar accesible a los participantes y se debe elegir una metodología entendible por todos, con entregables bien definidos, y código fuente bien organizada. En este sentido plataformas de desarrollo colaborativo de software con control de versiones es muy recomendable y existen soluciones de software libre que facilitan esta tarea.

Por otro lado, las comunicaciones deben securizarse de forma concienzuda. Para ello, se deben utilizar cifrados y autenticación que den confianza a los países. Por ejemplo, protocolos como SSL/TLS, ampliamente conocidos y la posibilidad de usar certificados digitales. En función de las infraestructuras disponibles, usar preferentemente redes aisladas de Internet, red intranet comunes y redes privadas virtuales (VPN) para tunelizar las redes nacionales es una buena idea. Una

Abundando en esto, el desacoplamiento de los nodos rema en la misma dirección. La dependencia del sistema respecto de una parte de ella, como un nodo o varios nodos, no debe afectar al sistema completo. Para ello, se debe considerar sistemas de comunicaciones asíncronas y orientación a servicios, entre otras opciones tecnológicas, que favorezcan la disponibilidad.

Finalmente, las ontologías y la internacionalización tanto de la interfaz de usuario como del diseño configuran un conjunto de buenas prácticas que redundarán en el éxito de la gestión del proyecto y en la calidad final del producto. Desde un punto de vista práctico, al tratar de intercambiar mensajes entre nodos debe existir un protocolo de intercambio de mensajes, mediante una ontología común y el uso de un vocabulario común que ayude al desarrollo y al mantenimiento posterior del sistema.

4.6.3. MODELO ARQUITECTÓNICO DISTRIBUIDO PROPUESTO

Las bases de datos distribuidas consisten en la conjunción de varios nodos de red de computadores, distribuida físicamente, pero componiendo un sistema lógico

unificado de datos: base de datos global. El diseño de bases de datos distribuidas incluye la decisión trascendente de elegir el tipo de control usado para procesar las transacciones al resto de nodos que forman el sistema. Si existe un componente concreto en el sistema distribuido que realiza esta función la arquitectura se denomina lógicamente centralizada; mientras que si el control se reparte entre todos los nodos la arquitectura es descentralizada o federada [123]. Esta decisión no es sólo técnica, en muchas ocasiones hay que sopesar el dominio de aplicación real, como la sensación de pérdida de propiedad de datos específicos o la confianza en la seguridad [124].

El procesamiento de la distribución física de los datos en una red distribuida tiene como uno de sus puntos claves de diseño el particionado eficiente y el diseño óptimo de la estructura de la red. El particionado influye de manera considerable en el rendimiento y la administración de la base de datos. El particionado vertical divide una entidad relacional en varios subconjuntos de columnas o atributos; mientras que el particionado horizontal consiste en obtener un conjunto de fragmentos relacionales, cada uno de los cuales con un subconjunto de filas o tuplas [125]. Seguidamente se presentan los tres aspectos más relevantes de la arquitectura, atendiendo a los principios básicos anteriormente mencionados.

Una solución distribuida completamente descentralizada implica que no existe un nodo coordinador, sino que el control de la distribución está repartido equitativamente entre todos los nodos de base de datos local. En el caso de un diseño con control centralizado tendríamos la ventaja de facilitar el desarrollo y la administración. Sin embargo, esto supondría que toda la información pasase

privilegiadamente en un nodo, volviéndose un recurso crítico de la infraestructura, lo que supondría además tomar medidas respecto del rendimiento y la seguridad [126].

La alternativa de diseño completamente distribuido descentralizado supone que en cada nodo se gestiona la comunicación con el resto de componentes del sistema y un conocimiento suficiente del emplazamiento de la información cuando se desea consultar. Además debe tenerse en cuenta que los nodos participan conforme a los principios básicos enunciados para un sistema distribuido internacional, especialmente, nodos suficientemente soberanos y benevolentes, o una medida de compromiso entre ellas. Con esto en la práctica un sistema completamente distribuido aporta a cada miembro los beneficios relacionados con que se comparte sólo lo necesario para el interés colectivo, la base de datos completa en un único sitio no existe ya que es un conjunto de bases de datos distribuidas donde nadie acapara toda la información en exclusiva y todos los nodos son igualmente importantes.

La implementación en red física de esta visión descentralizada se implementa mediante una topología de red en malla, conformando de esta manera una base distribuida P2P. De hecho, la red en malla supone un mayor esfuerzo en configuración, ya que cada nodo debe tener un inventario del resto de nodos locales en forma de fichero de configuración.

Si bien existen estudios como en el trabajo presentado en [127] para medir las características de las redes en malla P2P, tradicionalmente se considera que la administración de la red decae bastante cuando el número de nodos tiende a ser

elevado. A cambio un fallo en un nodo no afecta a toda la red, lo que permite diseñar un sistema en teniendo en cuenta los principios básicos que hemos venido enunciando: todos los nodos son igualmente importantes y ninguno prevalece sobre el resto.

En un entorno geográficamente distante, donde intervienen redes gubernamentales, además de Internet, la representación de la red en malla P2P es una representación lógica, que se consigue mediante control software, cuyo seguimiento se basa en el fichero de configuración de conexiones del nodo. Esto no supone, pues, un coste adicional a la infraestructura de red ni cableado adicional, como puede verse en la representación de más detalle conceptual en la figura.

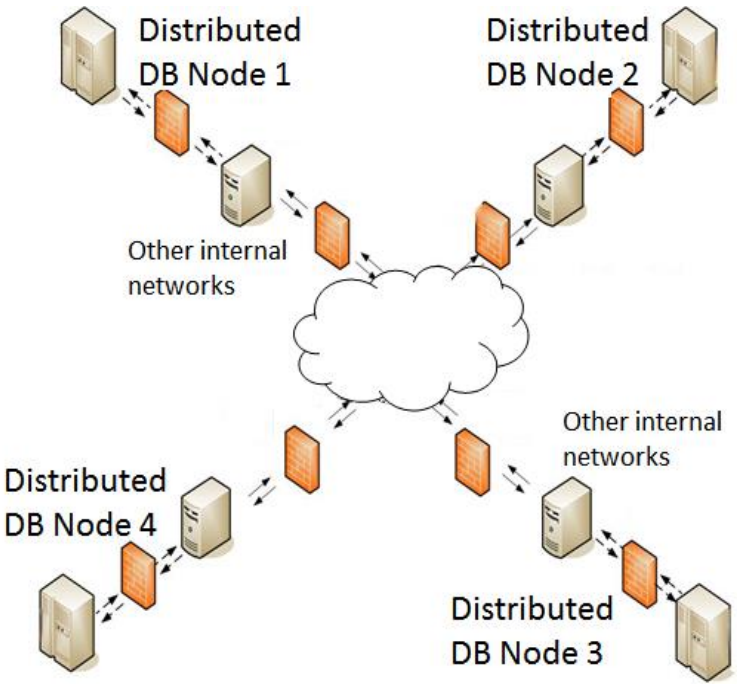


Figura 28. Representación de mayor nivel conceptual

Pero la red en malla aporta un nivel de seguridad adicional frente a la caída de uno de sus nodos: el resto siguen funcionando, además de que no presenta generalmente cuellos de botella ya que todos los nodos tienen el mismo papel frente a los otros [128].

4.6.4. NODOS DISTRIBUIDOS DE LA BASE GLOBAL

Para el diseño de la base de datos desde el enfoque complemente descentralizada es necesario establecer un nivel de abstracción de control sobre los nodos locales que conforman la base de datos distribuida global. Este control se articula en una estructura multicapa: una capa de servicio web de mensajería, interfaz común para todos en el sistema, una capa de lógica de negocio que procesa las transacciones globales, una capa de motor de persistencia de datos, así como repositorio de base de datos local. Este diseño arquitectónico se observa suficientemente independiente de la tecnología por lo que permite múltiples opciones de implementación.

La parte de control consiste, como se puede observar en la Figura, en una primera capa de interfaz con el resto de nodos mediante mensajería XML basado en SOAP denominada "Web Services Layer", donde se exponen los servicios web que implementan las transacciones para la base de datos global concretas necesarias funcionalmente. Su parámetro esencial es el tipo de transacción (TYPE), el nodo con el que se establece la comunicación (NODE) y el contenido de la transacción (MESSAGE). Completan este nivel de abstracción del control: la capa de Lógica del

nodo, donde se realiza las operaciones funcionales sobre la base, y la capa de motor de persistencia para independizar de la opción tecnológica de implementación del sistema gestor de la base de datos que forma el repositorio local.

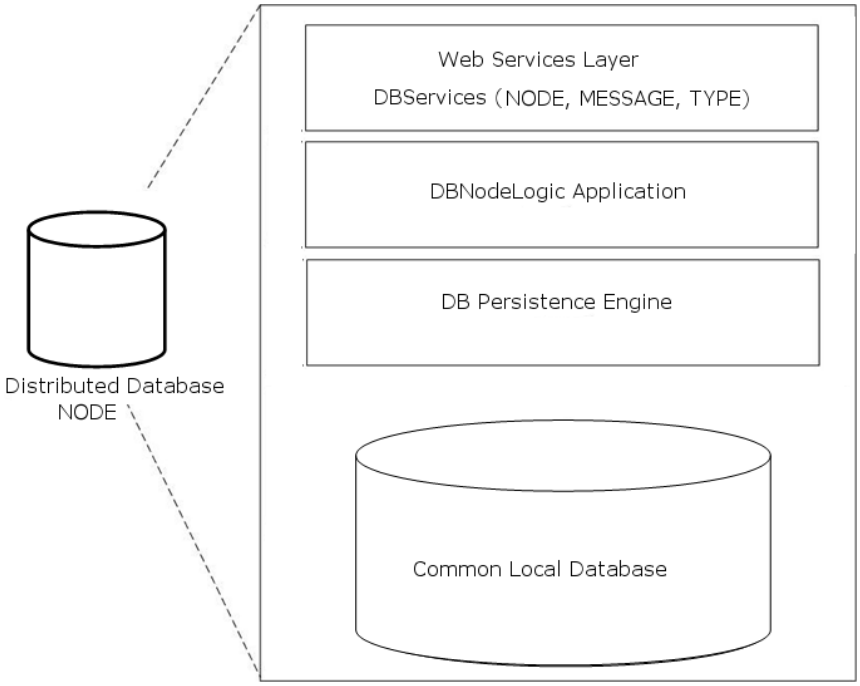


Figura 29. Arquitectura software de un nodo distribuido

El enfoque orientado a servicios web permite obtener una serie de ventajas como son la mejor organización de las funcionalidades que un nodo colaborador ofrece a los demás, el menor coste en el desarrollo y mayor flexibilidad, ya que la capa de servicio es igual a todos los nodos y permite que aquel usuario que lo desee pueda utilizar sistemas propios (legacy) realizando las adaptaciones necesarias para cumplir con los servicios ofrecidos. Además facilita el reaprovechamiento de los servicios y la reutilización del código y permite añadir capas de seguridad de más alto nivel, como por ejemplo cortafuegos de aplicación basados en XML.

Tanto la capa de servicio web, más externa, como la capa de persistencia, más interna, permiten obtener una arquitectura suficientemente desacoplada del resto de nodos y respecto de las distintas opciones tecnológicas.

4.6.5. TRANSACCIONES Y CONSULTAS

El particionado horizontal de la base de datos global tiene como objetivo mejorar el rendimiento de las transacciones y consultas. De hecho, una optimización del particionamiento parte del estudio de las consultas en un conjunto adecuado de pruebas.

El criterio de diseño principal elegido para nuestro sistema ha sido la localización geográfica, de tal manera que la información relacionada semánticamente con un nodo se aloje en su propio repositorio. Así un usuario encontrará las tuplas en las que participa directamente. En el caso de relaciones cuya semántica incluye información de dos nodos miembros distintos, las consultas sobre esta relación supondrían realizar la petición vía red de datos. Lo mismo ocurre en relaciones de bases de datos cuyas tuplas incluyan semántica de identificación de más de un nodo miembro. Este trasiego de transporte por red puede suponer una gran penalización del rendimiento.

Como medida se toma el criterio de insertar la misma fila en todos aquellos nodos miembro que estén identificados en una relación, añadiendo una redundancia horizontal que mejorará las consultas, a cambio de incrementar ligeramente las transacciones de inserción, actualización y borrado. Un ejemplo de este caso consiste

en la relación de "itinerario" donde la semántica indica tramos geográficos entre un par de puntos de partida y llegada. Sin embargo, para optimizar las consultas de "itinerarios" cada relación local contendrá no sólo las tuplas de los tramos en lo estén incluidos, sino del resto, ya que están semánticamente relacionados.

4.6.6. COMUNICACIONES BASADAS EN REDES CIFRADAS

Como un mantra la tendencia actual es acercar el eGoverment a toda la sociedad y de forma ideal para proyectos de TI el bien perseguido se vierte sobre los propios ciudadanos haciéndoles partícipes de la cuenta de resultados de la inversión pública en gobierno electrónico. Es un planteamiento de ganar-ganar, con doble beneficio, las Administraciones Públicas cumplen sus propios objetivos de gestión y de servicio.

Por otro lado, en la definición del proyecto se tuvo siempre muy en cuenta la apuesta por la tecnología y la innovación. Las instituciones europeas han desarrollado distintos planes de acción tendentes a mejorar la implantación de la sociedad de la información y la creación de puestos de trabajo. Es el caso del Plan de Acción eEurope2005, ya finalizado, seguido por la estrategia i2010, y la "Digital Agenda for Europe" [129] cuya pretensión trata de crear un marco favorable en el mercado europeo para la inversión privada en tecnologías de la información, la seguridad de los servicios, las aplicaciones y los contenidos basados en una infraestructura de banda ancha universal. Los marcos

europeos estratégicos han sido un impulso para conseguir una serie de objetivos básicos en las administraciones de los países europeos. Según dicho plan, Europa deberá contar con:

- Unos servicios públicos online modernos
- Una administración electrónica
- Unos servicios electrónicos de aprendizaje
- Unos servicios electrónicos de salud
- Un entorno electrónico para empresas que sea dinámico
- Banda ancha ampliamente disponible y a precios competitivos
- Una infraestructura segura para la información

Desde un punto de vista técnico, de servicio al sector comercial de los explosivos con fines civiles, los ciudadanos y las empresas pueden participar con las administraciones públicas de la siguiente manera:

1.- Las empresas alertando de forma temprana sobre robos, pérdidas, averías de transportes, incidencias.

2.- Identificando e inventariando las materias explosivas transportadas

3.- Colaborando en la cumplimentación electrónica de la tramitación burocrática.

Para ello, se diseña un subsistema "Portal de Administración electrónica", con despliegue independiente del resto del sistema y, organizativamente, de implantación

opcional. Específicamente, se desarrolla un módulo para que las empresas del sector comercial de explosivos puedan colaborar con la Administración Pública:

1º) alertando sobre incidencias en sus propios transportes;

2º) Cargando las partidas que se transportan mediante un inventario exhaustivo, informatizándolo, evitando el inventario genérico y en papel que dificulta el control; y

3º) Cumplimentando las autorizaciones administrativas, simplificando la tramitación burocrática.

Todo ello aporta una información estructurada imprescindible para las actuaciones de control, investigación y prevención de los poderes públicos; además redunda en una mayor agilización del servicio hacia las empresas, mejorando así los tiempos de respuesta de las administraciones; y en definitiva mejora la seguridad de los ciudadanos en general.

Dentro de estas medidas horizontales de los programas europeos de fomento de la sociedad de la información (IDABC), se debe destacar la creación y mantenimiento de una red intra-europea TESTA, que interconecta las Intranets de los distintos países de la Unión Europea, para servicios de interés común. TESTA cuenta con un nodo Gateway en cada país europeo y ha tenido desde el año 2000 una evolución positiva, pasando a denominarse como sTESTA, prefijo que denota el concepto de (s)eguridad.

Evidentemente uno de los puntos más delicados en el proyecto era las telecomunicaciones. Frente a la alternativa de crear redes privadas virtuales ad-hoc,

la opción de utilizar la red TESTA se planteó como la más atractiva, donde el coste de las infraestructuras no reporta directamente sobre los proyectos. Si bien supone una carga organizativa adicional para el proyecto, el equipo técnico de TESTA se compone de una persona de contacto "TESTA Contact Point" que agiliza enormemente la integración y la interoperabilidad general del sistema a través de esta red.

4.6.7. IMPLEMENTACIÓN DE REFERENCIA

El marco de referencia puede basarse, por ejemplo:

- Plataforma J2EE
- Servidor de aplicaciones Tomcat / JBoss
- Servidor Web Apache
- Servidor de Base de Datos MySQL
- Web Services basados en SOAP/XML

Ampliando el marco de referencia hemos de añadir compromisos de compatibilidad, por ejemplo:

- Servidor de aplicaciones compatibles: OAS / BEA WebLogic
- Servidor Web compatible: IIS
- Servidor de Base de Datos compatible: Oracle, MS SQL Server

En el caso de compatibilidades con varias bases de datos es recomendable utilizar módulos que facilitan el acceso a datos, como motores de persistencia (como Hibernate).

Mencionar dentro de esta sección, el uso de patrones de diseño que suponen la elección de buenas prácticas ampliamente reconocidas en el desarrollo de aplicaciones, especialmente el uso del patrón MVC (Modelo/Vista/Controlador), con implementación de Apache Struts, y otros extensamente utilizados: DO (DomainObject), BO (BussinessObject), DTO (Transfer Object), patrón Facade, por poner algunos ejemplos.

Siguiendo las tendencias actuales de desarrollo web, es fundamental acercarse a estrategias de desarrollo de tipo evolutivo, iterativo e incremental. Esto ha sido muy útil especialmente a la hora de elaborar *releases* para su entrega, donde parte de la funcionalidad puede ser utilizada por los usuarios. Esto además en un entorno de colaboración técnica internacional permite la distribución de los productos del desarrollo sin terminar para su revisión y auditabilidad. Es recomendable poder proporcionar al resto de colaboradores internacionales los códigos fuentes, software de base y manuales de instalación, de tal manera que las fuentes puedan ser auditadas, puedan desplegarse de forma completamente controlada y con la seguridad de que corresponden con lo verificado.

4.5. NUEVO ESQUEMA DISTRIBUIDO DE LAS RELACIONES DE GOBIERNO ELECTRÓNICO

Como consecuencia de la experiencia desarrollada durante años con el proyecto SCEPYLT y el framework de e-Government sobre terrorismo, en esta sección se

propone un nuevo esquema distribuido de gobierno electrónico que ponga énfasis en la interoprabilidad de la información.

Partimos de la idea de que tradicionalmente se han definido las relaciones de e-Government en tres tipos principales según la participación de los subjetos: Administración y Ciudadanos (G2C), Administración y empresas (G2B) y entre las administraciones entre sí (G2G). Un tipo especial que podemos considerar es la relación entre Administración y sus propios empleados, por su naturaleza especial de los funcionarios públicos (G2E). No hemos considerado en nuestro estudio otro tipo de relaciones propias del comercio electrónico como son B2C, donde el concepto de ciudadano se acerca al de "cliente" o el de B2B, relación entre empresas.

Estas relaciones vienen además establecidas por la dimensión de la gobernanza: local, regional, nacional, supra-nacional e internacional.

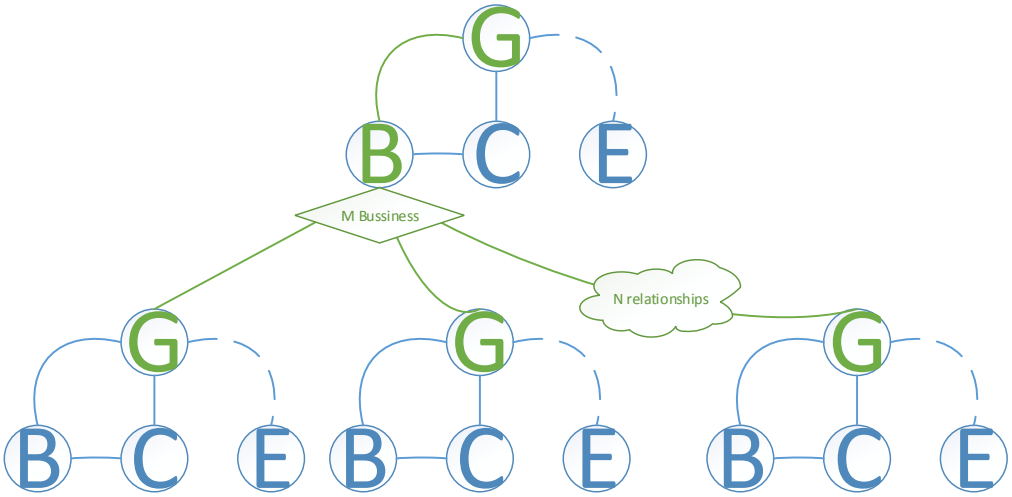


Figura 30. Escenario MxN de relaciones A2B

Un escenario teórico de relaciones en la industria en sectores comerciales que incluyen en la seguridad colectiva presenta la necesidad de interaccionar con la Administración Pública, que pueden ser una o varias en función del ámbito de negocio y la organización de las agencias gubernamentales. En la Figura 33 mostramos este escenario, donde *m* compañías de un mismo sector de negocio se relacionan con *n* Administraciones adicionales. Podemos intentar medir la gestión de la tramitación burocrática, haciendo un cálculo el número de relaciones que las empresas de un sector industrial tienen que establecer en un entorno con múltiples agencias gubernamentales, es: $R_b = m + m \cdot n$ y las relaciones establecidas por el sector público $R_g=0$, ya que no hay necesidad de colaborar.

De esta manera se expresa la interoperabilidad entre gobiernos para mejorar los servicios presentados desde el punto de vista de industria para optimizar las tareas administrativas de las empresas, ahorrando costes y molestias para éstas. Las relaciones con el segundo modelo propuesto sería: R_b = m y R_g = n. Adicionalmente, podríamos de la misma manera cuantificar matemáticamente los escenarios de tramitación burocrática de los ciudadanos, aunque nos centramos aquí en las relaciones sector industrial y gobiernos.

Como vemos el trabajo de gestión administrativa en el modelo propuesto supone una reorganización y del esfuerzo entre sector privado y sector público, donde este último asume parte de responsabilidad. Una adaptación del trabajo en la aspiración que supone el rediseño de los servicios públicos. Desde el punto de vista de la empresa, en la complejidad de la tramitación R_b es lineal respecto del volumen de agencias gubernamentales (ecuación I), mientras que en el esquema colaborativo es constante (ecuación II).

$$R = m\,(1\ + n) \qquad \text{(I)}$$

$$R = m \qquad \text{(II)}$$

Como consecuencia, una arquitectura interoperable entre administraciones públicas tiene un efecto directo en la competitividad del sector industrial. Pero no es el único valor que se pone de relieve aquí, sino también la posibilidad de implementar seguridad común entre los propios gobiernos. Ahora bien la siguiente pregunta es cómo conseguir diseños ingenieriles en las administraciones públicas que consigan este

efecto optimizador en el sector privado y, por ende, en la seguridad colectiva (pública y privada).

La visión planteada es establecer un framework con dos elementos: Un núcleo arquitectónico y un conjunto de portales basados en Web. El núcleo consiste en un esqueleto de comunicaciones seguras que implementen las relaciones G2G, que consiste en diseños mediante intercambio de información con una arquitectura orientada a servicios y redes de comunicaciones intra-administrativas. Las relaciones directas entre gobiernos suponen un diseño de comunicaciones en malla punto a punto (p2p).

En segundo lugar, un portal de servicio a la empresa que implemente la relación G2B, que respete la interacción entre la empresa y su principal agencia gubernamental. El resto de relaciones G2B se encaminarían, mediante protocolos de interoperabilidad, mediante las relaciones del núcleo arquitectónico G2G. La figura 2 muestra un esquema que representa el modelo conceptual propuesto en el framework de este rediseño.

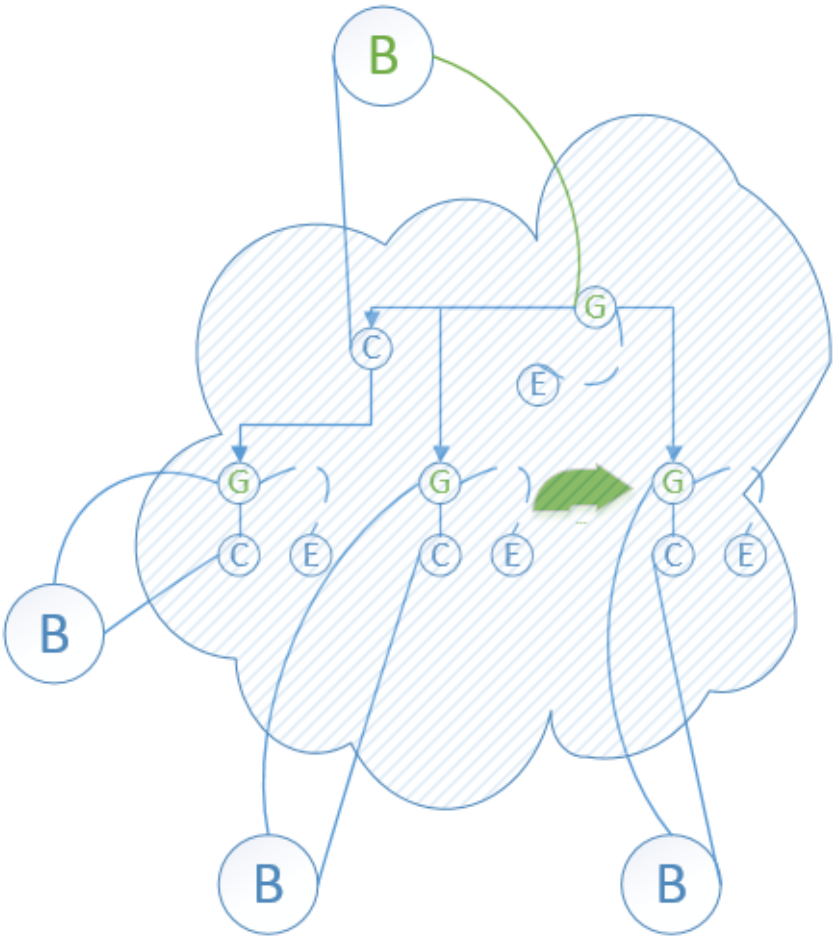


Figura 31. Esquema de rediseño conceptual de múltiples relaciones

4.6. CONCLUSIÓN

En este trabajo se propone cómo abordar las cuestiones, dificultades y lecciones aprendidas, bajo la perspectiva de gestión. Se pretende mostrar que hay modelos técnico-administrativos alternativos de e-Government que pueden ser de aplicación a países en desarrollo, con una conciencia ágil, y fomentar las alianzas para construir sistemas de información y comunicaciones, que ayude a alcanzar los objetivos del milenio y extender esa idea de impulso aprovechando la tecnología como punto de

apoyo. Asimismo definitivamente se propone un esquema distribuido que representa las relaciones clásicas de servicios electrónicos en un entorno de red sobre la base del paradigma de colaboración público-privada y la centralidad del ciudadano.

En este sentido se sigue las claves de un desarrollo internacional que se ha realizado bajo el prisma de la colaboración, la interoperabilidad, diseño creativo con arquitecturas, completamente distribuidas con bases de datos descentralizadas, sobre el sector comercial de productos regulados potencialmente peligrosos para la seguridad de la población.

Capítulo 5.

EL DOMINIO CRÍTICO DE E-JUSTICIA: ARQUITECTURAS DE SISTEMAS JUDICIALES ABIERTOS

Este capítulo presenta el dominio de e-Justicia bajo el prisma de los conceptos emergentes de eGovernment y las motivaciones de investigación científica en tecnologías inteligentes, abiertas y cercanas al ciudadano que además guarden la sensibilidad por la seguridad de la información. Esto supone nuevas aproximaciones arquitectónicas que afectan tanto al front-end como al back-end de las organizaciones públicas, de los tribunales de justicia ordinaria y de las cortes supremas.

Se propone una proyección de los conceptos de open Justice sobre un proyecto real desarrollado, desplegado y puesto en producción en un Tribunal de nivel constitucional. El principio básico es tomar como punto de partida un proceso de ingeniería más cercano y centrado en el ciudadano. Esta experiencia ha servido para promover la investigación en el campo de la e-justice para audiencias diversas, experta y amateur, multidisciplinar, en la línea entre las ciencias sociales y tecnológicas. Esta tesis contribuye a la visión innovadora de la Justicia abierta basada en estos conceptos sobre el dominio crítico de los sistemas de información de ámbito legal.

5.1. INTRODUCCIÓN

Con este trabajo se pretende ofrecer una visión de la justicia electrónica aplicada a la especificidad de los tribunales superiores y constitucionales en los sistemas de información legal sobre derecho, tanto desde un punto de vista jurídico como tecnológico. Los avances en IT se proyectan en la realidad como dinamizadores de cambios sociales y de nuevas relaciones entre ciudadanos y administraciones públicas. Las tecnologías de la información han habilitado una forma diferente de acceso de los ciudadanos a los servicios públicos bajo el paraguas del Gobierno electrónico dentro de sus distintos sectores de actividad. En el área de e-Justicia parece que los avances se perciben de manera diferente y particularmente en la justicia de instancias superiores, prueba de ello es la regulación diferenciada que se toma por parte de los poderes legislativos de algunos países. Este es el caso de España, donde aparece la Ley 18/2011 para el uso de las tecnologías de la información y la comunicación en la Administración de Justicia, a pesar de que se encontraba previamente legislado para el resto de la administración pública en la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

En este capítulo expondremos la integración de la justicia constitucional en el mundo de la justica electrónica, en el contexto del derecho europeo, como representación de un auténtico reto lleno de paradojas, que suponen desafíos para el diseño de arquitecturas tecnológicas eficaces y eficientes, distribuidas convenientemente y alineadas con la naturaleza del dominio especial jurisdiccional.

5.2. ANÁLISIS DE LA JUSTICIA ABIERTA

En esta sección vamos a describir brevemente un panorama general sobre el estado del arte y las necesidades en el contexto de lo que se podría denominar Justicia Abierta. En la actualidad se debaten tres aspectos fundamentales: los jurados y la transparencia en red.

Sin entrar en detalle describiremos seguidamente la situación relacionada con los jurados, aunque no es objeto de estudio en esta tesis.

El campo léxico de la justicia abierta comparte los descriptores que se aplican al gobierno electrónico pero con la especificidad del ámbito judicial. Su carácter principal se define por el uso de tecnologías de la información. Las aplicaciones emergentes van en la línea de aplicar estrategias de transparencia como Open Data, la participación del ciudadano, la colaboración y la responsabilidad de rendir cuentas. Todas ellas se apoyan sobre los principios clásicos de la administración pública: eficacia y eficiencia.

La Justicia Abierta, conocida ampliamente en su término anglosajón Open Justice, es un paradigma de principios legales que tratan de caracterizar el funcionamiento jurisdiccional en parámetros de transparencia y apertura. Estos conceptos van en la línea de los movimientos ciudadanos de defensa de la regeneración democrática, ya que permiten ver la aplicación de las leyes sobre casos y personas concretas, así como facilita la evaluación de la aplicación de las normas que los gobernantes deciden decretar. En cierto modo se trata de asegurar la confianza del ciudadano en el proceso de toma de decisiones legislativas, aspectos que tratamos en detalle en el capítulo anterior de esta tesis.

En este apartado se presenta un esfuerzo por analizar los dilemas contradictorios del dominio crítico que estudiamos en este capítulo, con la intención de introducir las dificultades que este tema de investigación suponen para el avance del gobierno electrónico en este sector especialmente por la realidad funcional que aparentemente puede chocar con el sentido tecnológico de resolver problemas y que en cierta medida supone un tratamiento especial de la gestión del cambio.

5.2.1. DILEMAS DE LA JUSTICIA ABIERTA

En un primer extremo de pensamiento que puede afectar a la Justicia Abierta, podemos enfocar la apertura sobre los actores que intervienen en este sistema. De ahí surge una primera antonimia, intrínseca a la propia naturaleza de la institución judicial, como una primera paradoja para la reflexión que podríamos expresar como: *Un grupo de personas no elegidas democráticamente toman decisiones sobre las decisiones de las personas elegidas democráticamente*.

Conocido como jurado, este grupo de personas juzga a un acusado, una disposición o una causa y dictan una sentencia. La apertura de la justicia electrónica y su desarrollo tecnológico suponen una ingente labor en el ciclo de vida del desarrollo software y la gestión del cambio de los sistemas de información. Se enfrenta a barreras internas difíciles de transformar que son consecuencia de la resistencia humana, de la tradición de los procedimientos de trabajo y de las leyes procesales.

5.2.2. LA ELECCIÓN DE LOS JUECES

En consecuencia en el caso de la justicia de los tribunales constitucionales ha venido apareciendo un enfrentado debate de la ausencia de legitimidad democrática de los miembros de un tribunal para controlar las decisiones de los representantes de la soberanía nacional. Esta crítica ha sido especialmente recurrente en la literatura jurídica estadounidense y en quienes se adscriben a la corriente del constitucionalismo popular. Siguiendo a algunos autores como en [78], una de las características principales del sistema legal norteamericano es la elección de los jueces que resuelven cuestiones constitucionales. Las diferencias entre las tareas relacionadas con las funciones de control judicial de las leyes y por otro lado las de interpretación suprema de la Constitución son puestas de relieve en este pensamiento jurídico, de tal manera que se pretende transmitir la idea de que el gobierno pertenece al pueblo y no a los jueces.

Como dice Aragón Reyes en [79] al respecto de la función de los tribunales constitucionales en la actualidad, "la función de los jueces (y sobre todo del juez constitucional como supremo intérprete de la Constitución) posee una dimensión 'recreadora' de la Constitución que no se puede negar, pero con el límite de que, al interpretarla, no pueden, en modo alguno, disponer libremente de ella".

Si bien se ha alimentado con argumentos que van más allá de lo estrictamente jurídico, se constata que se hacen valoraciones de oportunidad o eficacia de las normas enjuiciadas. Sin embargo, este fenómeno aparece en ocasiones en otros tribunales nacionales y supranacionales europeos. A pesar de que la publicitación de mucha información es uno de los grandes efectos beneficiosos de la apertura informática de

los tribunales constitucionales, esto conlleva el riesgo de que esos mismos tribunales se deslicen por la pendiente de la valoración de las normas legales controvertidas. En estos términos, la Justicia Abierta podría entrañar un riesgo para la existencia misma de la justicia.

5.2.3. LA PARTICIPACIÓN CIUDADANA EN EL JURADO

La participación y apertura a los ciudadanos como uno de los objetivos emergentes del gobierno electrónico en el ejercicio nuclear de las funciones del poder judicial chocan con obstáculos difíciles de salvar. Llevándolo a este extremo, se entiende que únicamente quienes están legitimados y son titulares de un derecho o interés, pueden, y deben, participar en el proceso. La discusión sobre la apertura a terceros podría incluso poner en tela de juicio la esencia misma del proceso judicial en un litigio donde las partes principales juegan un papel enfrentado.

Resulta interesante el plantearnos si la participación directa de los ciudadanos en las decisiones judiciales sea un objetivo al que debamos aspirar en la conceptualización de la Justicia Abierta. Ahora bien, en parte la aproximación ya establecida de la institución específica del jurado popular nos invita a la innovación a través de las tecnologías de la información y las comunicaciones, de la misma manera que la orientación planteada en las contribuciones sobre democracia electrónica más recientes y expuestas en el caso de esta tesis en relación a las ciudades inteligentes. De esta manera podríamos presentar un modelo extendido sobre los juzgados, en una especie de "smart justice".

Los jurados profesionales formados por juristas deciden la mayoría de las disputas judiciales frente a la opción de jurado popular instituida en algunos países. En la tipología de jurado anglosajón, existe un grupo de personas no versadas en leyes que resuelve sobre el asunto, normalmente por unanimidad, bajo el asesoramiento de un magistrado profesional que sobre la resolución dada decide la pena. Este es el caso de Estados Unidos, Canadá, Inglaterra, Australia o España, entre otros. Por otro lado, otro tipo de jurado consiste en un grupo colegiado de personas legas en la materia y profesionales, que es como se aplica en Francia, Italia, Suiza o Portugal.

Es normal que las cartas magnas recojan alguna forma de participación ciudadana, como en la Constitución Española de 1978 el tribunal del jurado que se regula en el artículo 125 bajo el literal "Los ciudadanos podrán ejercer la acción popular y participar en la Administración de Justicia mediante la institución del Jurado, en la forma y con respecto a aquellos procesos penales que la Ley determine, así como en los Tribunales consuetudinarios y tradicionales".

Si bien la participación como mecanismo está recogida en las democracias actuales, se puede considerar que los tribunales de justicia realizan no tanto el valor "democracia" como el relativo al imperio de la ley (rule of law), contrapunto del anterior. Además, dicho de otro modo, en la justicia en general, y en la constitucional en particular, se debe resaltar la concepción de que el imperio de la ley protege a las minorías. Esta protección podría quebrarse si se introducen criterios estrictamente democráticos, paradójicamente, que pongan en cuestión la supervivencia de las propias minorías. Esto es así de una manera sobresaliente cuando los asuntos judiciales tratan sobre derechos fundamentales, donde estos no son sino ámbitos en

los que no cabe la discusión amplia pues son elementos axiomáticos por sí, lo que le infiere un sentido contra-mayoritario.

5.2.4. LA JUSTICIA EN RED

En este apartado se plantea otro de los aspectos esenciales en la Justicia frente a los retos de las redes de comunicaciones e Internet. La interconexión extraprocesal entre órganos judiciales y el intercambio de información, fomentando así la colaboración no formal.

Pongamos por ejemplo nuestro foco en el planteamiento de una justicia constitucional en red en Europa [80]. Se enuncia como un sistema de justicia constitucional multinivel donde entran en escena diversos órganos judiciales, a saber, un conjunto de tribunales constitucionales nacionales, un Tribunal europeo de Derechos Humanos y un Tribunal de Justicia de la Unión; todos ellos en el ejercicio de funciones constitucionales. Además se debe resaltar que aplican instrumentos normativos diferentes, que se reclaman exclusivos y que se arrogan su supremacía, respectivamente, en el ámbito de un conjunto de Constituciones nacionales, el Convenio europeo de derechos humanos y la Carta de derechos fundamentales de la Unión Europea.

La justicia electrónica puede transformar esa tutela multinivel en un tutela en red, en la medida en que permite a los distintos órganos de la justicia constitucional conocer la forma como han resuelto sus pares los asuntos. Se abre así una auténtica vía para el "diálogo entre tribunales", diálogo que no puede articularse exclusiva —ni

aun preferentemente— por cauces procesales, pues no se dialoga desde la imposición de una única solución. Un diálogo entre operadores jurídicos que forma parte del BackOffice que redundará en el mejor funcionamiento de la gestión y por ende del servicio a la ciudadanía que hacen uso de la vía procesal de recursos que es la que la legislación les abre.

5.2.5. TRANSPARENCIA Y ASPECTOS TECNOLÓGICOS

Además de examinar estas paradojas, es importante tener en cuenta las infraestructuras y las arquitecturas software en la organización constitucional como un conjunto de herramientas y sistemas de información, implementados bajo criterios técnicos y organizativos. Una orientación a lo que se conoce como "Open Data" requiere de configuraciones y características específicas en el back office y en las arquitecturas de los sistemas de información. Desglosaremos una taxonomía de este tipo de sistemas, en una parte comunes a otras administraciones públicas, en otra similares al resto de la administración judicial ordinaria y en una tercera parte exclusiva de la informática constitucional propia de las cortes y tribunales supremos. Además de las peculiaridades de las TIC de tramitación procesal en este ámbito, es importante destacar los sistemas de gestión de la doctrina, en el doble plano de servicio interno y de acceso público a los ciudadanos. Las tecnologías emergentes como las redes sociales, el uso de la nube como almacenamiento persistente, la computación pervasiva o ubicua donde el ciudadano está permanentemente conectado, el auge los dispositivos de mano BYOD, e incluso la irrupción del Internet de las Cosas (IoT), empujan a la e-Justicia.

La actualización tecnológica y social que suponen estos avances debe de ser gestionada adecuadamente para no caer en situaciones conflictivas: la típica sensación de huida hacia adelante o la congelación-renuncia a la modernización.

Por otro lado, las TIC de justicia se presentan como pulsadores de la transparencia para los e-ciudadanos. Esto parte de la idea de la necesidad de inmediatez y accesibilidad de los conjuntos de datos que guarda la administración de justicia sobre su propia gestión y el escrutinio directo. Pero ¿hasta qué punto la transparencia?, se enfrentan dentro de la normativa procesal, penal o civil, una serie de principios o garantías que la e-Justicia no puede salvar.

Resulta interesante conocer la visión de las experiencias de iniciativas judiciales electrónicas en el ámbito constitucional a nivel internacional. En este sentido se presenta técnicamente el sistema de información para el acceso de los ciudadanos a la jurisprudencia en el caso del Tribunal Constitucional de España. La idea central del desarrollo es poner al ciudadano como actor principal, proporcionándole no sólo las sentencias y autos judiciales, sino también el conocimiento experto generado: síntesis, resúmenes, extractos, índices de leyes enjuiciadas y análisis semántico de descriptores jurídicos etiquetados basados en una ontología constitucional.

Las ontologías semánticas permite la formulación rigurosa del esquema conceptual de un dominio desde el punto de vista de la significación. Es una pieza transcendental en las arquitecturas que necesitan intercambiar información, haciendo posible la interoperabilidad entre sistemas. Pero por otro lado es un instrumento tecnológico que habilita la ingeniería del conocimiento y la utilización de técnicas de

inteligencia artificial, razonamiento, clasificación, generación y búsqueda avanzada de conocimiento.

Otros aspectos a tener en cuenta son aquellos que permiten a los ciudadanos participar tener espacios de co-creación del conocimiento. La experiencia presenta la actitud positiva de los ciudadanos frente a estas iniciativas, como por ejemplo en la propia calidad de los textos gubernamentales/jurisdiccionales puestos a su disposición y resto de información a su disposición estableciendo una retroalimentación significativa en el sistema. Esta idea centrada en el ciudadano se observa también en las decisiones tecnológicas para el diseño e implementación: capas de presentación de diseño natural-responsive, interfaces sencillas de interacción HCI, opción a medida para búsquedas más avanzadas, API de servicio REST, formatos OWL, JSON, XML, Office OpenXML, y PDF, entre otros, lo que puede comprenderse como un modelo que puede inspirar a otras cortes supremas constitucionales.

5.2.6. AMICUS CURIAE DIGITAL

Amicus Curiae es un instrumento traído del Derecho Romano que hace posible la personación en un proceso judicial sin ser parte en la causa, con la intención de favorecer la Justicia. Etimológicamente se refiere a una especie de amigo o colaborador de los magistrados. Pero la aplicación en la realidad actual apenas si está contemplada salvo en raras ocasiones y para casos especialmente complejos donde el interés general tiene una posición relevante. En los Estados Unidos su utilización ha sido más prolífica, pero en otros países la figura del Amicus es relativamente limitada. En el caso de España cabe mencionar que el legislador incorpora esta figura de participación en 2007 en la legislación de enjuiciamiento civil relacionado con los litigios relacionados

con la competencia. Ahora bien, la participación se circunscribe sólo a órganos públicos como la Comisión Europea, la Comisión del Mercado de Valores y aquellos órganos competentes en las Comunidades Autónomas.

La evolución de las tecnologías de la información no ha sido aprovechada sufrientemente para desarrollar el reconocimiento de derechos cívicos relacionados con la participación en la administración de justicia. Sin embargo, existen espacios para de una forma ágil para implementar alguna idea de Amicus Curiae como mecanismo Open Justice.

No obstante lo anterior, al margen de las decisiones generales legislativas o políticas, no se sostienen actitudes indiferentes de la administración judicial para mejorar los mecanismos de acceso de los ciudadanos a la justicia y especialmente a la constitucional. Pero la reivindicación de esta necesidad debe hacerse desde la toma de conciencia de que no se trata aquí tanto de participar en el ejercicio de la actividad jurisdiccional, sino de asegurar unos mecanismos de control informal sobre la acción de los jueces. Esta sensibilidad va en la línea de la Justicia transparente y atenta con los ciudadanos mediante el uso de tecnologías modernas que permitan ser eficientes en la consecución de estos objetivos.

En un primer lugar, la justicia electrónica permitirá a los ciudadanos aportar sus razones a debates jurídicos de interés público. Ninguno reviste mayor interés público que el debate sobre la ley: los ciudadanos podrán así aportar —aunque sea como "amicus curiae"— la opinión que les merece el trabajo de sus representantes.

En segundo lugar, no se trata de que los ciudadanos refrenden o no las decisiones adoptadas por los órganos judiciales, sino de que conozcan estas decisiones y puedan valorarlas a la luz de las circunstancias concurrentes. Incluso aquí puede jugar un papel singular el llamado "derecho al olvido", ya que de esta manera en ocasiones se podría articular la ocultación de datos capitales para poner llevar a cabo el control informal, como opuesto al procesal, de las decisiones judiciales. En nuestro ánimo por la conceptualización práctica de la apertura de la justicia hay que incluir la protección de los más débiles, como las víctimas de determinados delitos, los menores, los discapacitados y personas en riesgos de exclusión social.

En definitiva, si bien la participación directa de los ciudadanos en el proceso de decisión presenta un dilema transgresor, la apertura de instrumentos digitales de amicus curiae basados en soluciones tecnológicas centradas en los ciudadanos abre caminos interesantes e innovadores a su vez.

5.3. CONCEPCIÓN DE NUEVAS ARQUITECTURAS

En los años más recientes la transformación de la sociedad debido al impacto de las tecnologías de la información se están haciendo cada vez más patentes. Se observan en los movimientos sociales que además hemos estudiado en profundidad a lo largo de esta tesis. En el plano judicial el uso de herramientas TIC no ha venido suponiendo un cambio radical en el funcionamiento procesal ni decisorio. Pero esta tendencia viene agotándose hasta tal punto de que la formación en tecnologías de la información es necesaria para los operadores jurídicos y, especialmente, los jueces. Particularmente dramática es la necesidad cuando el objeto de fondo de la actividad

judicial versa alrededor de la propia temática tecnológica, asuntos cada día más habituales como consecuencia de la tecnificación de la sociedad.

5.3.1. ASPECTOS GENERALES

La transformación del uso de herramientas TIC de apoyo hacia la insalvable dependencia tecnológica de los Tribunales de justicia es tan inevitable como lo es para la humanidad en su conjunto. El reconocimiento de los sistemas de información tanto para la gestión judicial como para el acercamiento de los temas judiciales a los ciudadanos supone un nuevo paradigma en la implementación del Open Justice.

En un concierto de sistemas informáticos y de comunicaciones están surgiendo nuevas herramientas dentro de este campo apoyados por las novedades en el propio avance de la tecnología de la información. En contraste con los desafíos de la Sociedad global del Conocimiento en que vivimos, la judicatura se sigue viendo a menudo como un sector conservador, tradicional, formalizado y preestablecido donde los actores legales tienen roles rígidos de interacción.

En un sentido técnico la calidad se ha venido entendiendo como la conformidad con unas especificaciones o estándares, o con una totalidad de características que debe cumplir un servicio o software para cubrir unas necesidades dadas. Así que en la calidad de los servicios desarrollados en el ámbito de TI, es necesario controlar el proceso software y la gestión de la calidad. Para una visión más detallada en [81] se puede encontrar una revisión muy interesante sobre modelos de calidad.

En los últimos años, está cogiendo fuerza la idea de enfocar la calidad hacia el producto en sí, sobre el que se apoyaría la métrica de la calidad, particularmente en la especificación y en la evaluación del software. Esta es la base que se sostiene el estándar ISO/IEC 25000 denominado SQuaRE (Software Product Quality Requierement and Evaluation) [82].

En los apartados siguientes se estudian los factores importantes para esta concepción, se pone en contexto la investigación y cómo la justicia abierta puede ponerse como el primero de los requisitos para los sistemas judiciales. Finalmente se presenta la implementación desarrollada y se evalúan los resultados.

5.3.2. FACTORES IMPORTANTES

Aunque es un campo suficientemente especializado, la e-Justicia comparte gran parte de los planteamientos del Gobierno electrónico. Tal es el caso de las máximas y criterios de eficiencia y eficacia, así como del uso de tecnología avanzada y agilidad. En cuanto a su posición respecto de la ciudadanía, la justica necesita recorrer una distancia en solitario sobre un camino diferente al de otros sectores públicos, por la propia configuración de la naturaleza judicial, como se ha querido plantear en la sección primera de este capítulo.

En consecuencia la justicia debe intrincarse con la tecnología para implicarse en servicios más cercanos y comprensibles donde el elemento clave de diseño es la centralidad del ciudadano. Este paradigma en el desarrollo de TIC en el sector es completamente novedoso ya que la visión tradicional pone al final del catálogo de requisitos los asuntos de los ciudadanos, si existen, priorizando la de los actores judiciales. Curiosamente en el proceso de desarrollo de soluciones el ingeniero tiene

cara a cara a los actores judiciales, mientras que no así a la ciudadanía. Este fenómeno hace que a menudo las soluciones caigan en centrarse en el funcionario y que el servicio al ciudadano quede, en cuanto al diseño del proceso software, como valor marginal. Poner como primer requisito un ciclo de desarrollo centrado en el ciudadano supone llevar siempre encima unos prismáticos que permitan salvar esa distancia y ver a simple vista lo que nos parece de lejos, interactuando con los operadores jurídicos y planteando su aplicación/compatibilidad de forma recurrente en un esquema de justicia abierta.

- La accesibilidad es uno de los factores importantes en este esquema, que permite ese mayor objetivo de cercanía al ciudadano. Algunos autores como en [83] expresan la accesibilidad en términos de eficiencia y eficacia, aunque otros resaltan aspectos de la comprensión del lenguaje usado como paso previo para ofrecer mejores servicios a los ciudadanos [84]. Siguiendo esta idea los tribunales y los ciudadanos tienen algo más fácil la comunicación.

- La interrelación directa como factor que pueda plantear un escenario sin intermediarios para el acceso a la justicia a través de las TIC. Esto conduce a que al mismo tiempo los tribunales podrían tener una interacción con los ciudadanos no profesionales jurídicos.

- La cooperación entre actores jurídicos y entre tribunales, como forma estándar de trabajo, en aras de la transparencia que se canaliza hacia el ciudadano, y favoreciendo los mecanismos de eficacia del sistema judicial como un conjunto

global inspirado tanto en la lealtad institucional como en la visión de centralidad del ciudadano.

En conclusión se ponen de relieve los factores pro-activos de transparencia, participación y colaboración que deben cumplir las iniciativas en el campo de la Jusiticia Abierta.

Es obvio que nuestra sociedad no se entiende sin la referencia de Internet, cuya evolución ha impactado de forma definitoria en los usos y costumbres de la humanidad. Sociólogos como Castells [85] incluso hablan de la Sociedad de la Información y el conocimiento como un fenómeno bipolar entre el Ser y la Red que define el comportamiento de los individuos.

El uso de tecnologías de la información en el ámbito de la justicia tiene especial relevancia cuando las relaciones telemáticas entre ciudadanos y jueces, lo que supone un cambio trascendental en la realidad social sobre cómo se hacen las cosas en los tribunales. De hecho hay en la literatura opiniones advirtiendo de las consecuencias negativas que para los juzgados supone la infrautilización tecnológica [86], su potencial como sistema de gestión dentro de los juzgados [87] e incluso la formación de letrados y magistrados. En este sentido Jiménez [88] ha ejemplificado esta situación como parte de los mecanismos que deben instituirse dentro de la efectividad de la propia tutela judicial.

La comunidad científica viene en consecuencia abordando la necesidad de innovación en la concepción de la Administración de Justicia acorde a los retos de este siglo y que participan de los avances en general. Tomar ventaja de las capacidades de las tecnologías como parte de la misma Justicia no solo ayuda a lograr los objetivos

de la judicatura en sí sino que evita la brecha digital que a veces se siente por parte de los operadores judiciales y la sensación de persecución de las TIC.

Esto se consigue con la incorporación de nuevas habilidades y capacidades a nivel individual y a nivel organizativo para dirigir los recursos de TI hacia los desafíos de la Justicia Abierta. Para ello la concienciación y la instrucción son extremadamente necesarias para poder visualizar las posibilidades de las TIC en el proceso de cambio en el sector.

5.3.3. EVOLUCIÓN TECNOLÓGICA

En este apartado tratamos de dar una orientación evolutiva objeto de la investigación legal que permite enmarcar un caso práctico desarrollado. La aproximación centrada en el ciudadano, el uso de ontologías y la orientación open data desde el back-office hasta el front-office se presentan como ejes de los sistemas de apertura judicial.

Durante años, siglos, el uso de compendios sobre estos temas han sido acumulados en libros en soporte papel y han dominado las oficinas profesionales. La introducción del soporte multimedia en los últimos 30-40 años se sumó a la vasta cantidad de documentación legal, lo que implicaría distribuciones físicas incómodas y mantenimiento de mayor complejidad en cuanto al formato lógico.

Con la expansión de las redes de computadores aparece el uso de bases de datos jurídicas en despachos jurídicos y organizaciones públicas sobre los años 90. Una evidencia del estado de la situación en estos años la han dado investigadores

como Páez Mañá [89] donde hace una recopilación de sistemas de bases de datos legales y la incorporación de los tesauros jurídicos en la eficacia aplicada a la recuperación de la información.

Con la explosión de Internet de forma generalizada en los años 2000 el acceso online se superpone a la distribución empaquetada de multimedia y papel, extendiéndose el uso de las bases de datos en Web.

En la revolución tecnológica de la década siguiente, hay que mencionar los sistemas de información legal bajo el fenómeno transcendente de la conectividad permanente de la computación ubicua. Los avances en tecnología móvil han sido el detonante de una revolución que se completa con los dispositivos BYOD (*Bring Your Own Devices*), la generalización de la computación en Cloud y el advenimiento de la híper sensorización de las ciudades (*Smart Cities*) provocada por las tecnologías Internet of Thing (*IoT*). Así como en consecuencia, el tratamiento de ingentes cantidades de datos que requieren innovadores procesos de Big Data.

Por otro lado las autoridades gubernamentales no son inmunes a estos progresos. Las capacidades tecnológicas habilitan cambios en la sociedad, gran parte de ellos en cuanto a concienciación y psicología social hacia organizar el espacio colectivo de manera diferente. Esto deriva en impulsos frescos de Gobierno electrónico, aplicaciones novedosas, que incluyen la demanda generalizada por la transparencia, la política de apertura de información y la comprensibilidad de la gobernanza pública por parte de los ciudadanos. Todos estos fenómenos vienen a converger hoy día con el concepto de Administración electrónica para ir perfilando lo que viene denominándose Governanza Inteligente.

Uno de los principales puntos de investigación en este campo objeto de esta tesis, ha sido alcanzar una arquitectura tecnológica que sirva de palanca para avanzar en la investigación y el estudio de las ciencias jurídicas aplicadas. De esta manera, facilitar el estudio en profundidad de grandes volúmenes de datos jurídicos, encontrar estrategias de integración, análisis de la información y técnicas de visualización. La necesidad de comparar ordenamientos jurisdiccionales de alguna manera, la recolección de esta información, el impacto semántico de descriptores jurídicos y su valoración global resultan extremadamente complejos y tediosos sin abordarlo desde una perspectiva arquitectónica. Más si cabe cuando se considera el hecho de que mantener una visión completa del espacio jurídico en su conjunto es difícil de seguir debido a que es un dominio dinámico donde los cambios normativos tienen un impacto cuya prospección resulta humanamente complicada de concebir en detalle.

La investigación en el área de derechos fundamentales, basadas en las reglas de las constituciones y los estatutos de determinadas regiones o estados, requiere herramientas de este tipo, cuya traslación en la visión de la vida de los ciudadanos de a pie es directa en tanto que se trata de sus libertades y sus derechos. Pero para llegar a este punto, primero los sistemas de justicia necesitan estar diseñados técnicamente para que activen este salto cualitativo.

Se quiere subrayar la idea de la Justicia electrónica en el sentido de tratar a los ciudadanos como expertos de la vida cotidiana. Por tanto se acerca la oportunidad de abrir la ventana de la investigación legal mediante el acceso libre a los sistemas jurisdiccionales tradicionalmente dirigidos a profesionales y empresas. Usar tecnología

de la información para este propósito facilita, además ofrecer herramientas de ingeniería del conocimiento y poder analizar por sí mismos los resultados es una extensión funcional que debemos encuadrar también dentro de la Justicia abierta. De esta manera, las TIC se transforman en el puente sobre el que la ciudadanía alcanza las ciencias jurídicas.

5.4. UN FRAMEWORK PARA OPEN JUSTICE

Se debe tener en cuenta que la Justicia todavía retiene un aura de formalidad que no proporciona demasiadas facilidades para incorporar la perspectiva de los ciudadanos. Es normalmente un campo congeniado para expertos en asuntos legales, abogados, procuradores y académicos de las ciencias del Derecho. La tendencia de la mayoría de bases de datos jurídicas son comerciales, a través de algún tipo de licencia o subscripción, donde la información legal está particularmente organizada y se ofrecen otro tipo de servicios, como dar asistencia legal y consultoría. El foco está en el beneficio empresarial, legítimo por otra parte, y ese es el eje sobre el que circulan los servicios electrónicos prestados, especialmente de profesionales y bufetes de abogados.

Desde el punto de vista del interés general, con la madurez de Internet y la e-Sociedad, los organismos públicos relacionados con el poder judicial empiezan a dar publicidad a sus juicios y resoluciones, especialmente por canales web. De esta manera, como alternativa a otros proveedores privados, se permite el acceso a las sentencias y declaraciones jurisdiccionales desde la propia fuente de información. Si bien hay cierta intención de proporcionar información estructurada, no es así sobre el conocimiento generado a partir de esa información, ni resulta fácilmente accesible por

el público general. Para ello es necesario aplicar estrategias de gestión del conocimiento y arquitecturas que habiliten esta realidad social de apertura judicial.

Para contextualizar nuestro framework es necesario determinar parámetros constructivos de Open Justice. Para establecer un marco de trabajo para el análisis y evaluación de los aspectos definitorios de los sistemas de información ante la Justicia abierta se ha diseñado un instrumento que refleje una valoración de madurez puesto que no hay en la literatura un posicionamiento técnico universal en relación a la revolución tecnológica y social reciente. Los componentes que la integran pueden enlazarse con otros aspectos con significación similar en otros sectores del Gobierno electrónico inspirados en la filosofía Open Government. Ahora bien esto es así siempre y cuando se considere en todos los sectores el protagonismo del ciudadano como actor principal. Se ha enumerado un modelo de parámetros con 7 dimensiones que expresan los sistemas de información de Justicia Abierta:

- Acceso
- Centralidad
- Apertura
- Transparencia
- Semántica
- Gestión
- Unificación

Con esto se pretende comprender las dimensiones de la Open Justice en un entorno tecnológico y de herramientas TIC que nos permita describir

paramétricamente cualquier sistema. La experiencia empírica mostrada corrobora este modelo desarrollando y poniendo en marcha un sistema de información sobre jurisprudencia constitucional. Con el diseño orientado al ciudadano, se establece una arquitectura que da respuesta a la gestión de la doctrina jurídica y al acceso de los ciudadanos bajo criterios de gobierno electrónico con necesidades de ciberseguridad crítica. Se enfatiza la estructura arquitectónica para alcanzar un alto nivel de apertura de la información y transparencia, así como el diseño y construcción de una ontología jurisdiccional que modela el dominio de los derechos fundamentales y libertades constitucionales, de tal manera que permite ofrecer una alta consistencia de las fuentes de información y del conocimiento experto incorporado al sistema.

En la Figura 28 siguiente se muestra un esquema del diseño conceptual del sistema desarrollado y puesto en operación en el Tribunal Constitucional de España.

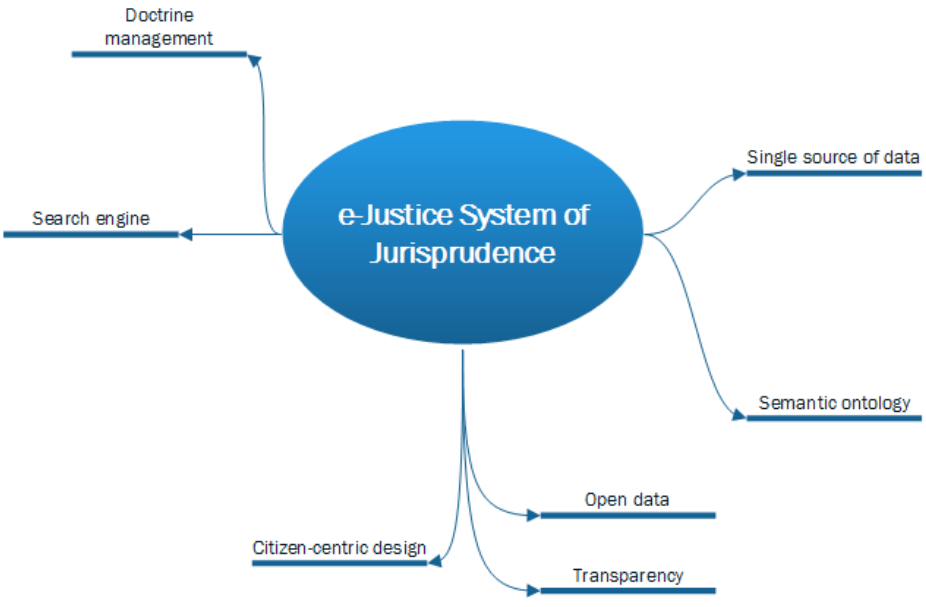


Figura 32. Esquema conceptual de la arquitectura desarrollada

Estas ideas fundamentales responden a algunas de las preguntas clave cuya respuesta se pretende facilitar desde la concepción son:

- ¿puede cualquier ciudadano tener acceso a la misma información de la misma manera que un juez?
- ¿Es posible no sólo tener información sino conocimiento experto propio del Know-how de los tribunales?
- ¿Es posible hacer Gobierno electrónico en el sector judicial donde en primera línea de la trinchera estén ciudadanos directamente, abogados y jueces?
- ¿Existen canales que permitan a los ciudadanos participar directamente en los sistemas judiciales?
- ¿Y pueden por sí ayudar a mejorar la calidad de la Justicia?

5.4.2. DESARROLLO DE UN SISTEMA TIC DE E-JUSTICIA

Las funcionalidades van en el sentido de optimizar el acceso y las búsquedas del conocimiento jurisdiccional, aplicado a las resoluciones del Tribunal, autos y sentencias, y su descripción semántica.

Para ilustrarlo se expone a continuación la herramienta de jurisprudencia en Internet (iHJ) disponible en la web principal del tribunal (www.tribunalconstitucional.es) o bien en el subdominio hj.tribunalconstitucional.es.

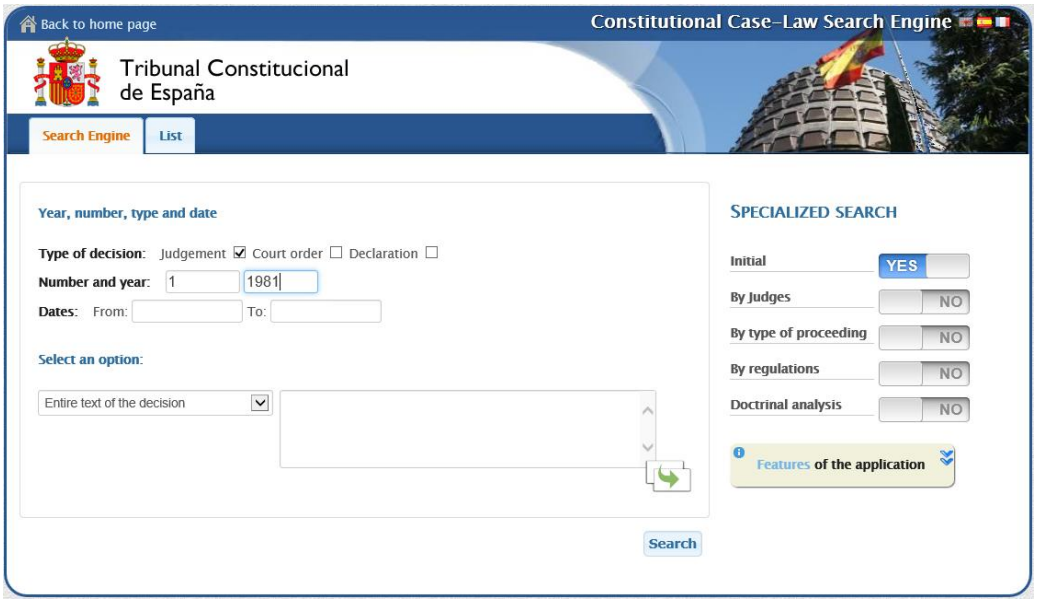


Figura 33. Interfaz público de la TIC iHJ

Este sistema proporciona una base de sentencias y autos, así como información y conocimientos asociados. Se implementa sobre una base de datos cuyos contenidos son exactamente la misma que es usada por letrados y magistrados, conformando la jurisprudencia para la toma de decisiones y concepción de las sentencias nuevas del Tribunal. Estas nuevas sentencias se incorporan al sistema, realimentando la información y evolucionando el conocimiento general.

Existe un juego rico de combinaciones para realizar las búsquedas que permiten explotar todas las posibilidades de acceso a la base de jurisprudencia. Por dar algunos casos, el contenido de una sentencia en sí misma mediante criterios como el tipo de la demanda (recurso de amparo, cuestión de constitucionalidad, recurso de inconstitucionalidad, o conflicto de competencias entre Administraciones, etc). Otros criterios, por tener una somera idea, están conforme a la Sala del Tribunal (Pleno, Sala primera o Sala segunda, e incluso salas especiales o temporales), por el número de

registro procesal, o bien por los votos particulares de los magistrados, entre otras muchas casuísticas que pueden consultarse directamente en la Web.

Sin embargo es especialmente relevante el acceso al conocimiento experto derivado de cada sentencia anterior que durante años ha sido de consumo interno y que con la herramienta iHJ es de acceso libre y público. Esto incluye los análisis doctrinales, las síntesis, los sumarios, los extractos, los resúmenes, los descriptores semánticos, la indexación, la colección de sentencias relacionadas, legislación relacionada y normas de rango inferior, todo ello accesible a cualquier ciudadano desde Internet.

Además de numerosas opciones en el sistema de cara al usuario ciudadano, se deben señalar dos. Como se muestra en la Figura 30, la primera de ellas es la pluralidad de estándares utilizados para la generación de documentos en un formato editable. Así ocurre por ejemplo, en relación a la documentación de [90], con las descargas ofrecidas en ISO/IEC 29500 o Standard ECMA-376, típicamente utilizado en formatos OpenXML tanto en entornos Mac, Windows y Linux, y amigable con las principales plataformas de ofimática del mercado tanto comercial como libre. Por otro lado, se permite el acceso en formatos tradicionalmente interoperables en XML y también en JSON.

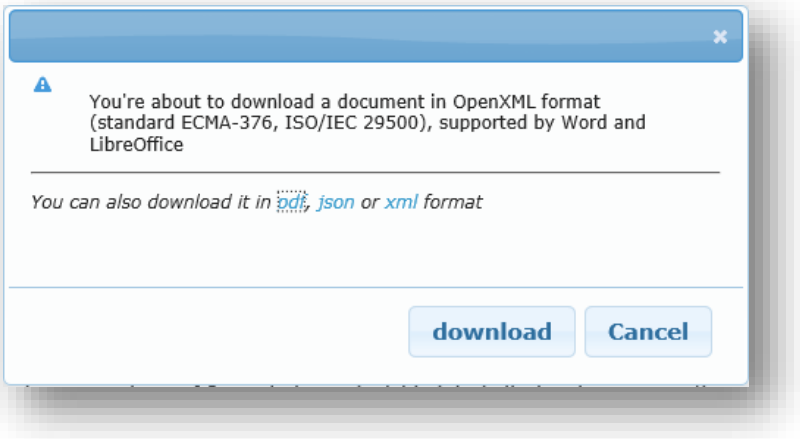


Figura 34. Una de las interfaces para descargas en varios estándares

Y en segundo lugar, se debe subrayar el escenario de uso de un mecanismo de retroalimentación del sistema para que el usuario ciudadano pueda aportar información que mejore o evalúe el propio sistema. Consecuentemente cualquier persona podría sugerir al Tribunal algún elemento erróneo o mal referenciado como se muestra en la figura.

Figura 35. Retroalimentación del ciudadano

En esta misma dinámica, otra interfaz permite poder sugerir descriptores semánticos relacionados con una sentencia, colaborando de esta manera a mejorar y optimizar la ontología semántica judicial del Tribunal. En la Figura 36 se muestra una representación visual de un subconjunto de descriptores de la ontología jurisdiccional disponible en la herramienta TIC desplegado en el portal web.

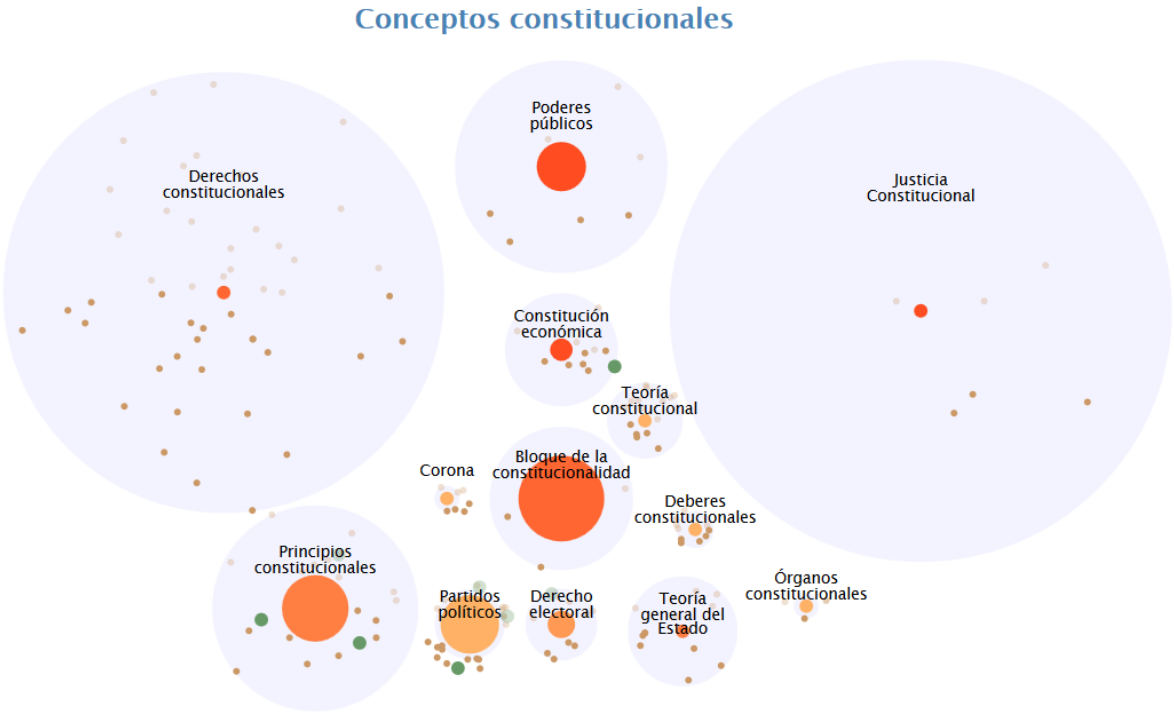


Figura 36. Visualización de descriptores ontológicos

(Web: hj.tribunalconstitucional.es)

5.4.3. ARQUITECTURA DE DISEÑO

Desde un punto de vista del ecosistema TIC y su diseño, el proyecto desarrollado consiste en tres sub-sistemas principales: el Sistema Software Web, el Sistema de Información Central y el Sistema de Cache de Contenidos.

- El Sistema Software Web (WSS), que es una aplicación multicapa distribuida cuyos usuarios son los ciudadanos y sus módulos básicos están compuestos por las vistas de ciudadanos, el esqueleto controlador y el modelo jurisdiccional.
  - Vistas de ciudadano.

    Consiste en el diseño de la capa de presentación sobre HTML5 y jQuery, con un estilo natural-responsive de diseño e implementación en sintaxis de marcado de servidor ASP.NET Razor version 4.
  - Esqueleto controlador.

    Consiste en controladores que dan forma a la arquitectura base MVC (model-view-controller) y a las funciones disponibles para ofrecer una capa de implementación Rest API que de servicios basados en json e xml. Esto habilita la comunicación máquina-maquina (M2M), más concretamente máquina del Tribunal con máquina del ciudadano (o grupo o movimiento ciudadano).
  - Modelo Jurisdiccional.

    Consiste en la lógica de negocio, la estructura de las entidades y las relaciones. Cabe destacar el uso de mecanismos de persistencia de datos como es Entity Framework así como las posibilidades de implementación con xml y json usado extensivamente.
- Sistema Software de Información Central (CISS)

Consiste en una infraestructura de bases de datos de servidor, indexadores, y estructuras de información experta y una ontología jurídica basada en descriptores, conceptos y relaciones que etiquetan semánticamente los items jurisdiccionales. Este sistema tiene a su vez dos partes claramente distintivas:

- Base de datos de conocimiento de jurisprudencia (KDJ).

  Está basado en una base de datos relacional, sobre la cual la información de las decisiones judiciales está intrincada con el conocimiento experto, quedando disponible hacia el exterior a través del sistema WSS para el acceso ciudadano.

- Sistema de Ontología Semántica.

  Consiste en una colección de descriptores conceptuales sobre justicia constitucional, especialmente sobre derechos fundamentales y libertades civiles. Se organiza mediante la jerarquización de conceptos (vertical), las relaciones puramente semánticas (horizontal) conformando un grafo semántico enlazado a sentencias y a otros nodos de la ontología y del KDJ.

- Sistema de Cache de Contenidos (CCS)

Es un sistema de contenido documental electrónico que hace posible las peticiones de documentos desde las rutinas de búsqueda y recuperación de la información del sistema WSS. Hay que considerar que la arquitectura está basada en un sistema de base de conocimientos, por ende no existen documentos que representen la jurisprudencia inicialmente y se va generando conforme lo solicita el ciudadano con un ciclo de vida dinámico según la vigencia del conocimiento utilizado. Adicionalmente se utiliza para el acceso, optimizaciones con el propósito de acelerar el rendimiento del servicio que libera ficheros editables Open XML. Tiene asimismo

otro módulo, que ofrece los documentos oficiales de la gaceta gubernamental BOE así como se integra las correcciones publicadas.

En la Figura 37 puede verse una representación de esta arquitectura que permite ver el esquema desplegado por el sistema en su conjunto.

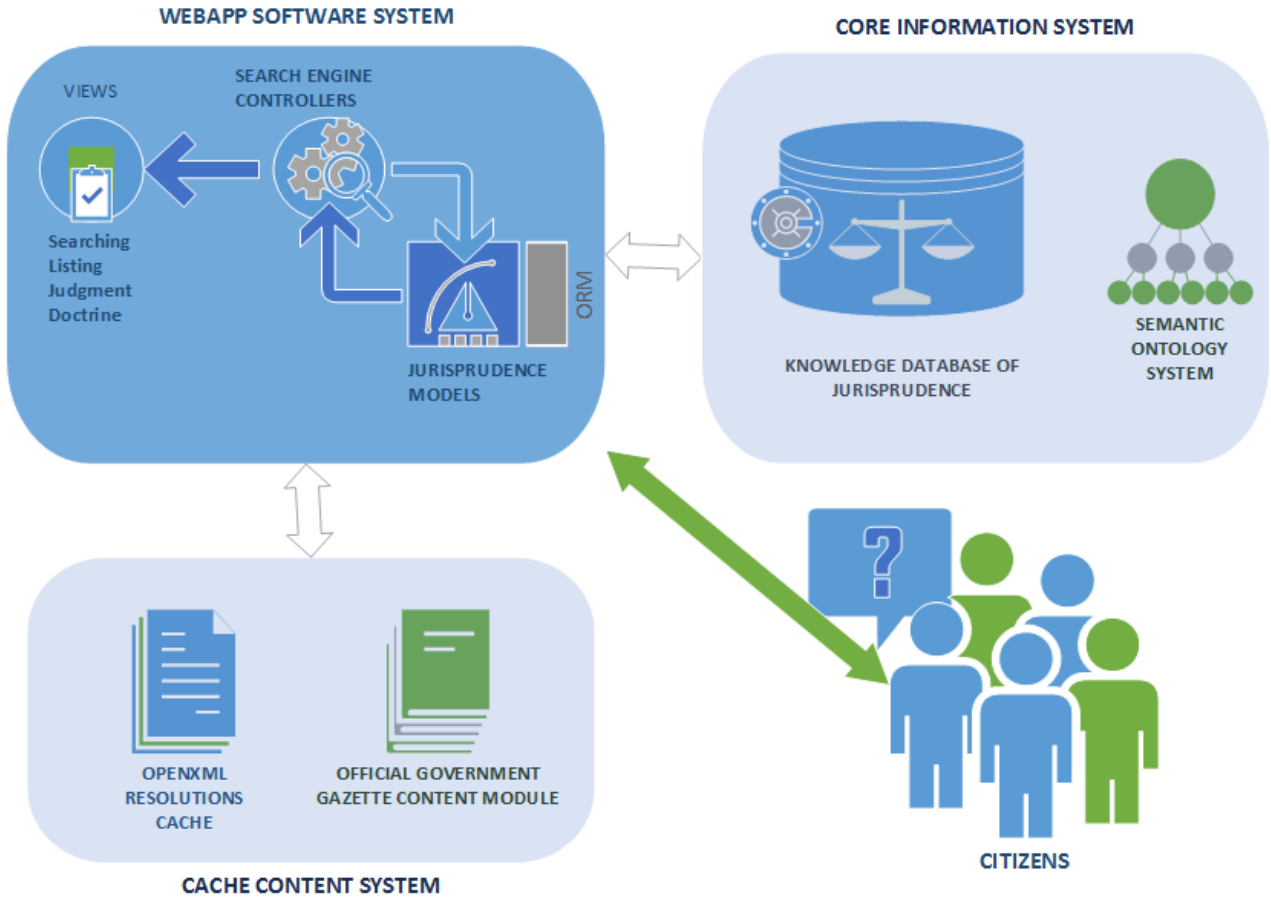


Figura 37. Visión arquitectónica de sistema de e-Justicia

5.5. CONCLUSIONES

En este capítulo se ha trabajado el dominio crítico de Justicia, introduciendo el área de investigación en este campo, bajo una visión tecnológica y estrechamente ligada a la ciberseguridad como elemento habilitante que permite dar el servicio continuo al ciudadano. Se han estudiado los distintos aspectos de la Justicia Abierta, así como de las herramientas TIC y la visión centrada en el usuario ciudadano. Aunque esté bajo el paraguas del Open Government, el sector judicial tiene una especificidad diferenciadora que hace que las propuestas tecnológicas en gobierno electrónico deban ser aplicadas de forma distinta.

Para ello se presenta un modelo de análisis de Open Justice basado en siete dimensiones que permitan parametrizar el diseño y construcción de un sistema judicial en apertura [91] [92].

Como iniciativa de investigación de futuro resultaría interesante considerar otras aristas de la justicia electrónica, como es el proceso electrónico o el acceso digitalizado de los expedientes judiciales por parte del ciudadano, aplicando las dimensiones expuestas en este trabajo.

Capítulo 6.

DOMINIOS CRÍTICOS DE E-EDUCACIÓN EN LA E-SOCIEDAD

En este capítulo introduciremos la Educación dentro de la Sociedad de la Información y el Conocimiento como dominios críticos del desarrollo del gobierno electrónico. Los sistemas de gestión de los sistemas de e-Educación y las estrategias de aprendizaje a través de herramientas TIC en relación con la ciberseguridad se presentan con contribuciones relevantes derivadas de esta tesis. En la sección 2 se expone el trabajo relacionado con la gestión educativa, con un framework de evaluación de sistemas de acreditación, la experiencia de construcción de un sistema de diplomas electrónicos y su puesta en marcha. En la sección 3 se presentará la investigación sobre el plano científico-educativo donde se diseña una metodología a través de tecnologías de la información para la construcción de un laboratorio de aprendizaje de la ciberseguridad y se estudia el resultado. En la sección 4 se incorporan varias extensiones de adaptación curricular e innovación educativa.

6.1. INTRODUCCIÓN

El concepto de e-Sociedad está estrechamente vinculado al de e-Educación en el sentido de extender los servicios que se prestan a las personas a través de las tecnologías digitales, particularmente Internet, para alcanzar una mejor gestión en el sistema educativo y unos contenidos curriculares para avanzar en los objetivos del desarrollo personal y desarrollar una serie de capacidades para aprender activamente y ser capaces de resolver problemas de la vida cotidiana a través de las adversidades que nos plantea la vida y la sociedad de la información y el conocimiento.

Considérese como muestra la Declaración de Incheon de 2015 promocionada por la UNESCO, como agencia de las Naciones Unidas especializada en educación, y firmada por los ministros del sector de más de 100 países. En la convicción de una educación de calidad esta declaración es un compromiso por el cambio en un marco de acciones para los próximos años, hasta 2030, entre las que se incluye el compromiso expreso por que la tecnología de la información sea el puntal para fortalecer los sistemas educativos, así como para la difusión del conocimiento, el acceso a la información, la prestación de servicios y el aprendizaje eficaz [130].

En el ámbito de la investigación realizada en esta tesis se ha abordado las arquitecturas en educación desde una doble aproximación. Por un lado, se trata de la gobernanza de la educación en el sentido de que a través de sistemas de información se habilite mecanismos de mejora de los procesos internos de negocio dentro de la propia organización educativa, a la que podemos aplicar estrategias de

gobierno electrónico. No obstante, esto quedaría incompleto a la luz de la visión moderna de gobierno electrónico si no añadiésemos un componente de apertura, acercamiento a los estudiantes y transparencia. Por otro lado, se trata también aplicar estos principios de gobierno abierto al sistema educativo, incluso al mismo proceso de enseñanza-aprendizaje como contenido y razón fundamental de la educación en la sociedad digital.

Para conseguir esta visión global de este dominio en la e-Sociedad, se ha profundizado en este trabajo en estos dos planos paralelos:

- Plano de gestión educativa: Aspectos formales de dominios críticos de e-Educación, donde se ha desarrollado un modelo de seguridad para la emisión de diplomas electrónicos con validez legal. Se ha desarrollado un sistema de información para darle solución y se ha puesto en marcha en organismos educativos reales con resultados satisfactorios. Los resultados han sido condensados en artículos de investigación, algunos de ellos todavía en proceso de publicación.

- Plano científico-educativo: Aspectos de contenido con creación de nuevos instrumentos didácticos a través de técnicas de aprendizaje y metodologías innovadoras, mediante el uso de recursos tecnológicos, diseño instruccional de estrategias basadas en la gamificación (GBL, Game-Based Learning), entre otras, en el área de la ciberseguridad. Se introduce una idea de acercar la ingeniería para el aprendizaje a la vida cotidiana, contribuciones que han sido valoradas por la comunidad técnica

con publicaciones en revistas de primer nivel de impacto y premiada en cuanto a su visión innovadora a nivel universitario.

Este capítulo se discute también sobre la problemática de la gestión y emisión de acreditaciones educativas, luego se plantea un modelo de seguridad de diplomas electrónicos y el desarrollo de una arquitectura software distribuida que utiliza técnicas criptográficas como elemento central para establecer este modelo, y en un último bloque se presenta la metodología, el diseño y construcción de un laboratorio de ingeniería sobre ciberseguridad.

6.2. PLANO DE GESTION EDUCATIVA

El objetivo de esta sección es mostrar un análisis de la situación y una solución tecnológica para la protección y detección del fraude académico de títulos universitarios y diplomas en general con validez legal, basada en las posibilidades de la criptografía, de las arquitecturas software interoperables y las buenas prácticas de gobierno electrónico. Esto supone en definitiva encajar el sistema tradicional, hacer reingeniería de procesos e incorporar nuevas formas digitales integradoras.

6.2.1. CONTEXTO DE LA INVESTIGACIÓN

Los retos involucrados en la apertura, transparencia y gobernanza inteligente actualmente están llegando de la mano de la evolución del eGovernment [131], en relación con la necesidad imperiosa de la e-Sociedad de trasladar beneficios tangibles a la comunidad educativa [132]. En pocos años ha dejado de ser una

posibilidad interesante y deseable en convertirse en una exigencia social. Esto plantea en una gran amplitud de factores, incluidos los correspondientes a las políticas públicas y el sector privado, que están muy intrincadas, como puede verse en el trabajo realizado por las Naciones Unidas, como se muestra en [133].

La comodidad y rapidez con que los criterios de gobierno electrónico se han extendido en los últimos años en los países desarrollados y también en los países en desarrollo en cierta medida, permite a los a los sistemas de información del sector educativo a permitir que el personal de administración y servicios, los profesores y el alumnado pueda enfocar sus necesidades de forma más eficiente.

Sin embargo, hay mucho que hacer en la sociedad digital para mejorar la e-Educación y por ende dar valor a la democracia y a la participación ciudadana en los asuntos sociales y políticos, algunos trabajos en este sentido pueden verse en [134] y este mismo autor [135].

En este dominio hay muchos avances en dos áreas clásicas. Primero, desde el punto de vista administrativo se han realizado progresos en profundidad en cuanto a registro y matrícula online, información a los pre-estudiantes, la comunicación electrónica de notas, son actualmente herramientas comunes. De acuerdo a la Ley 59/2003, de 19 de diciembre, sobre la firma electrónica en España (art. 4), la firma electrónica reconocida tendrá el mismo valor que la firma manuscrita consignada en papel. Y además la Ley 11/2007, artículo 13.1, viene a decir que los gobiernos tienen que admitir en sus relaciones electrónicas los sistemas de firma digital que cumplan los requisitos de la ley anterior y garantice la

identificación de los participantes, de su autenticidad y la integridad de los documentos.

De otro lado, el punto de vista educacional se ha avanzado en plataformas y tecnologías para la formación de estudiantes de una forma decidida. En este contexto, la UNED (www.uned.es), con unos 200.000 estudiantes es la Universidad más grande de España. Debido a que es una universidad a distancia las relaciones con sus estudiantes es plena: matricula online, portal del estudiante, plataforma de eLearning, sistema de video y web conferencia, y distribución segura de exámenes basado en Web.

En la literatura es fácil encontrar algunos trabajos buenos sobre el uso del papel, particularmente en educación, como en [136], pero un pertinente tercer área aún no ha sido investigado lo suficiente: la certificación oficial de diplomas. Todos los estados y sus gobiernos son responsables de certificar el conocimiento adquirido por sus ciudadanos y su nivel de competencia. El tema de los certificados es la fase final del proceso académico y supone uno de los más importantes por su relevancia social bien conocida.

Se debate en esta sección del problema de los diplomas digitales de certificación, pero también se introduce un marco de seguridad, se describe una TIC implementada en el entorno universitario llamado Opendiploma y se evalúan los resultados sobre la aceptación del modelo por parte de los estudiantes y se presentan datos sobre uso y rendimiento.

6.2.2. ANÁLISIS COMPARATIVO DE LA EDUCACIÓN Y EL GOBIERNO ELECTRÓNICO

Para contextualizar el trabajo se ha realizado un estudio multivariable de los datos que se publica por la ONU referente por un lado al Programa sobre Administraciones Públicas [137] y, por otro lado, la información sobre educación de los informes [138] del Programa para el Desarrollo (PNUD). Ambas fuentes de datos son elaboradas por distintas agencias por lo que toman criterios y notaciones ligeramente diferentes, motivo por el cual ha sido necesario para su tratamiento ha sido necesario un estudio y una revisión previa. Las variables analizadas se muestran en la lista siguiente, donde el nombre es una denotación tomada a efectos de formulación seguida de la descripción de la variable.

- X_0 Orden de clasificación en el ranking de eGovernment
- X_1 Es el índice general de eGovernment basado en la media de la valoración dada a los servicios online prestados, el capital humano y las infraestructuras de telecomunicaciones. Abreviado: EGDI. Se obtiene mediante la tipificación de las variables en una distribución normal estándar.
- X_2 Consiste en el índice general de participación electrónica aplicado a un país. Esta variable se presenta aparte del índice general de eGov.
- X_3 Es un índice normalizado que representa la capacidad de ofrecer servicios online gubernamentales. Se abrevia como $OSI_{normalized}$
- X_4 Es un índice normalizado sobre la capacidad de las administraciones públicas en cuanto a capital humano. Se denota: $HCI_{normalized}$

- X_5 Se trata del valor de infraestructuras de telecomunicaciones de un país. En el informe oficial se abrevia como $TII_{normalized}$

- Y_0 Se trata de una variable del rango a que corresponde en función de la valoración global de Desarrollo Humano de un país. El índice de desarrollo humano (IDH) está basado en un indicador social estadístico compuesto por tres parámetros: longevidad y salud, educación y nivel digno de vida.

- Y_1 Consiste en el índice de desarrollo humano obtenido para la Educación en un determinado país. Es calculado a partir de información objetiva sobre el número significativo de años escolarizados por la población en relación la expectativa de años de escolarización.

- X'_0 Corresponde con el orden de clasificación descartados algunos países por falta de disponibilidad de datos a los efectos de este capítulo

- X'_2 Se trata de un orden de clasificación considerando sólo los valores del índice de participación electrónica.
- Y'_0 Corresponde con la ordenación obtenida teniendo en cuenta sólo el índice en Educación. Se diferencia con Y0 en su carácter específico.

La serie de variables X_i es el resultado de la metodología de la ONU donde se evalúan los 193 estados miembros. Se tienen en cuenta sus portales Web, las políticas y estrategias de gobierno electrónico, así como los servicios que se prestan. Sin embargo, sobre Educación no se dispone información de 16 de esos países (Corea del Norte, Islas Marshall, Mónaco, Nauru, San Marino, Somalia, Sudán Del

Sur, Uruguay, Uzbekistán, Vanuatu, Venezuela, Vietnam, Yemen, Zambia, Zimbabue y Tuvalu).

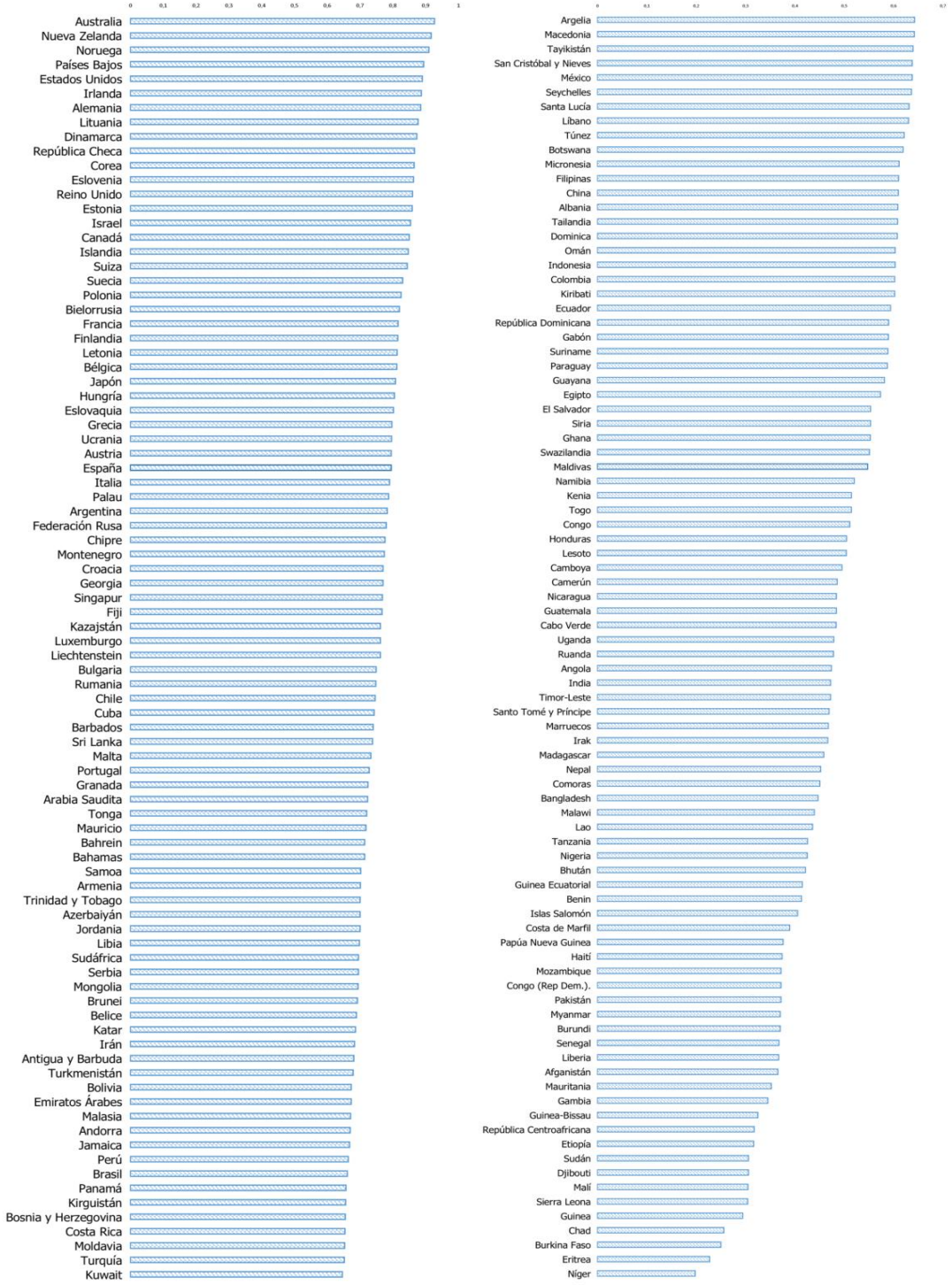


Figura 38. Representación del índice de desarrollo en Educación

La Figura 38 muestra una panorámica de los 177 países del que se disponen datos suficientes en cuanto a Educación. En la representación se muestran los nombres de un subconjunto de ellos si bien las líneas corresponden a todos.

En el Apéndice 2 se puede ver los valores obtenidos de las fuentes mencionadas, así como los clasificadores Y'_0, X'_0 y X'_2 elaborados. Como resultado interesante se muestra en la tabla siguiente el Top 10 de países con mayor índice de desarrollo humano en Educación y su correspondiente posición en cuanto a capacidad de eGovernment como de eParticipación.

País	Y'_0	X'_0	X'_2
Australia	1	2	6
Nueva Zelanda	2	9	18
Noruega	3	13	29
Países Bajos	4	5	1
Estados Unidos	5	7	8
Irlanda	6	22	32
Alemania	7	21	23
Lituania	8	28	32
Dinamarca	9	16	52
…			
España	32	12	18

Tabla 2. Top 10 (+ España) en Educación, eGov y eParticipación

Otra forma de resaltar estas variables es mostrando los mejores países en resultados de gobierno electrónico y observar su índice de desarrollo educativo:

País	X'_0	Y'_0	X'_2
Corea	1	11	1
Australia	2	1	6
Singapur	3	41	9
Francia	4	22	3
Países Bajos	5	4	1
Japón	6	26	3
Estados Unidos	7	5	8
Reino Unido	8	13	3
Nueva Zelanda	9	2	18
Finlandia	10	23	23
…			
España	12	32	18

Tabla 3. Vista del Top 10 por eGov - Educación

En la Figura 39 se muestra la distribución de las tres variables generales con la tendencia lineal de cada una gráficamente.

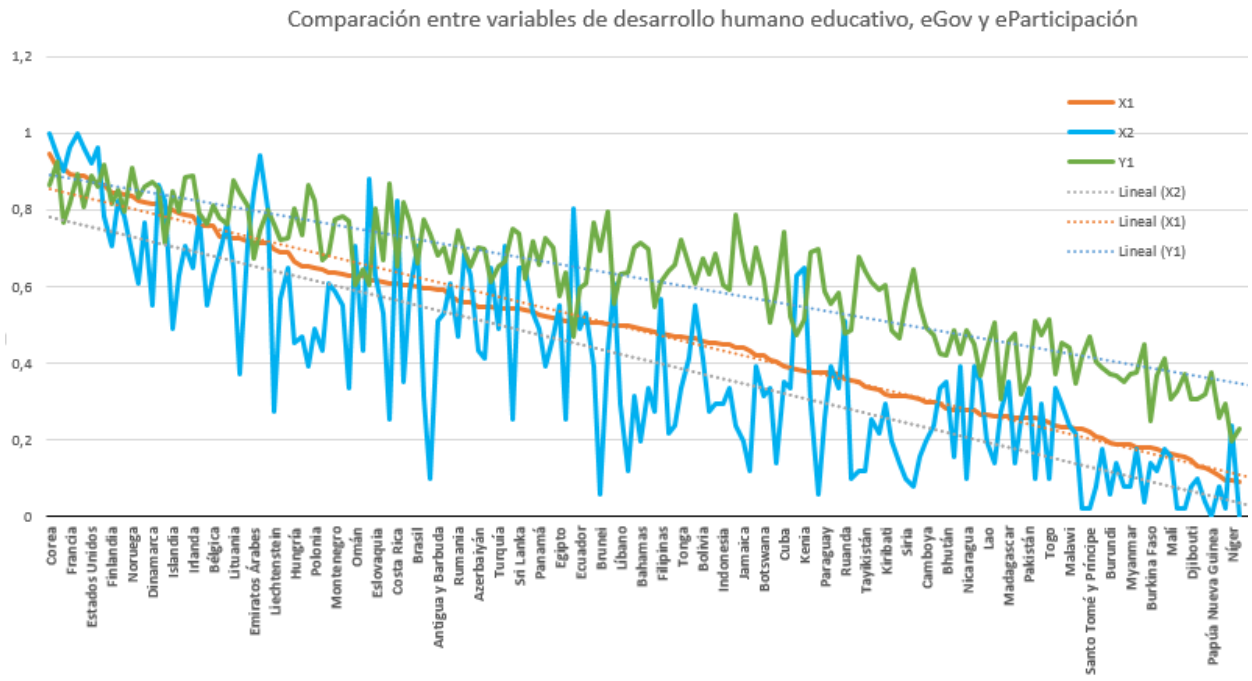


Figura 39. Resultado comparativo de las variables estudiadas

Si bien analizando las tablas anteriores se demuestra cierta disparidad entre niveles de Educación y de Gobierno electrónico curiosamente en algunos países puntuales, hay que resaltar que la correlación de las series estadísticas indica una interrelación positiva entre algunas de estas variables, como se puede ver en los siguientes cálculos:

$$P_{X1,Y1} = \text{corr}(X_1, Y_1) = 0{,}91 \qquad \text{(I)}$$

$$P_{X2,Y1} = \text{corr}(X_2, Y_1) = 0{,}66 \qquad \text{(II)}$$

$$P_{X1,X2} = \text{corr}(X_1, X_2) = 0{,}84 \qquad \text{(III)}$$

$$P_{Y1,X3} = \text{corr}(Y_1, X_3) = 0{,}09 \qquad \text{(IV)}$$

$$P_{Y1,X4} = \text{corr}(Y_1, X_4) = 0{,}13 \qquad \text{(V)}$$

$$P_{Y1,X5} = \text{corr}(Y_1, X_5) = 0{,}85 \qquad \text{(VI)}$$

Sin embargo, la correlación es más fuerte está en la ecuación (I), seguida de la (VI). Con esto podemos concluir que de este estudio se observa que hay una correlación entre el nivel de gobierno electrónico de un país y su nivel de desarrollo en Educación. Pero es más, el despliegue gubernamental en infraestructuras de telecomunicaciones está especialmente co-relacionado con el nivel de desarrollo educativo.

6.2.3. APROXIMACIÓN CONCEPTUAL DE LA ARQUITECTURA

Una primera aproximación consiste en mejorar las medidas de protección del propio soporte papel, añadiendo algún mecanismo criptográfico de protección adicional, como puede ser una marca de agua o código de validación expresa. Esta marca debería normalizarse y ser fácilmente verificable por vía telemática. Podríamos pensar en algún código hash, código de barras o firma digital impresa. El alcance de esta solución supone modificar el aspecto de los títulos, con el problema organizativo que supone especialmente la gestión del cambio para universalizar la propuesta.

En una segunda aproximación, es interesante proyectar la viabilidad de que la sociedad se adapte a cambiar el soporte tradicional de los títulos en papel. Esto permitiría aplicar al soporte electrónico los sistemas de protección actuales basados en firma digital y en infraestructuras de seguridad. Esto nos sitúa en un escenario de tecnificación donde organismos públicos, empresas privadas y particulares dispongan de posibilidades tecnológicas para usar los soportes intangibles. Las desigualdades tecnológicas, así como la conciencia social del papel, dificultan actualmente esta propuesta. No en balde la brecha digital en educación (digital divide en su término en inglés) es uno de los aspectos de la e-Sociedad más discutidos e investigados por tecnólogos, sociólogos, pedagogos y gobiernos.

En la definitiva tercera aproximación, presentamos una solución para incorporar una infraestructura criptográfica que permita detectar títulos falsos, localizar el detalle falsificado dentro del título, ofreciendo una arquitectura

interoperable basada en servicios web. Es importante que el sistema propuesto sea no intrusivo, es decir, que no afecte al procedimiento actual de elaboración de títulos con protecciones materiales y se sume de forma transparente al sistema de seguridad actual. Para ello existen tres posibilidades: establecer una marca de seguridad, no utilizar ninguna (o marca nula) o bien la impresión de un código de seguridad en el propio título. En cualquier caso consiste en un tratamiento criptográfico de alguna representación aplicada al diploma completo. Esto conformaría un sistema de información para emisión y gestión de diplomas.

Adicionalmente, uno de los servicios interoperables que podría ser ofrecido como un servicio público (o cualificadamente público) es la comprobación de diplomas, accesible por cualquier parte, ciudadano o empresa privada, de tal manera que pudiera comprobar la validez de un título. En este sentido, existen iniciativas gubernamentales que facilitan cierta información de comprobación por vía telemática, como en la sede española del Ministerio de Educación [139]. Esta comprobación requiere dotar de la mínima información necesaria para validar el documento, protegiendo cualquier posible dato de carácter personal. Otros servicios, accesibles por entidades públicas o educativas, podrían permitir identificar los datos personales de los interesados, hasta un nivel que se considere oportuno.

Este criptosistema intenta evitar el fraude académico de títulos universitarios, añade buenas prácticas de eGoverment, posibilitando el acceso de los ciudadanos a los servicios de información y mejorando el nivel de confianza en el sistema educativo en general.

6.2.4. UN FRAMEWORK DE E-EDUCACIÓN PARA CERTIFICADOS ELECTRÓNICOS RECONOCIDOS

La idea es presentar un marco seguro de e-Educación para hacer posible los diplomas electrónicos de forma segura y confiable en la Sociedad de la información y el conocimiento. Para ello se han estudiado el contexto actual de e-Educacion y se expone la resistencia a la supresión del papel en cuanto a las acreditaciones y diplomas en el ámbito universitario. Se plantea la necesidad de alcanzar cierta seguridad con respecto a los diplomas en la e-Sociedad, se investiga los puntos clave que serían necesarios para conseguir tal confianza y se propone un modelo de seguridad alrededor de los diplomas electrónicos. Por último, se presenta una ICT práctica que implementa este modelo y ha sido aplicado en el ámbito universitario.

6.2.4.1. Arquitectura de seguridad

La arquitectura de seguridad para diplomas electrónicos se basa en varios componentes que se exponen a continuación, identificados como el aspecto de firma electrónica competente (CS), el módulo de verificación abierta de autenticidad (VAA), la plataforma de trazabilidad electrónica independiente del formato (TEIF) y el sistema de token de uso limitativo o un solo uso (T1UL).

Típicamente en la firma de documentos a través de esquemas digitales de seguridad se requieren dos características técnicas: robustez y reconocimiento.

Estas cualidades son suficientes para la mayoría de los casos donde la firma digital se necesita para garantizar un nivel suficiente de seguridad.

En el mundo académico, los diplomas son generalmente usados para acreditar y certificar el conocimiento adquirido por un apersona y se considera comúnmente como un mérito en la búsqueda de trabajo tanto público como en la empresa privada. En consecuencia lejos de ser un mero documento de apoyo, los diplomas en sí requieren una atención particular.

Por lo tanto, las capacidades de robustez y reconocimiento que son propias del ámbito de la firma electrónica común de documentos, incluso con denominaciones avanzadas como la que se implementa con estándares como ETSI XAdES o PAdES [140], debe replantearse. Esto es así de la misma manera que un documento firmado en papel no tiene las mismas previsiones que un título universitario en papel. Convenimos que derivado de este cuestionamiento, debe evaluarse si es suficiente garantía por si solo un algoritmo de firma digital para cubrir los requisitos de seguridad en el campo de los diplomas electrónicos y en cualquier caso determinar las especificaciones añadidas o complementarias necesarias.

Para este propósito se presenta este framework al objeto de establecer la protección de los diplomas de certificación educativa con cuatro capacidades que se deben incorporar a la arquitectura como se ha mencionado al principio de este apartado.

6.2.4.2. Firma competente (CS)

Como hemos venido diciendo, los términos de firma robusta y reconocida son bien conocidos en los ámbitos de firma electrónica avanzada. Pero no es suficiente para entender la firma en el entorno de los diplomas electrónicos, que sustituyen a diplomas en papel como los títulos universitarios. Es necesario incluir un concepto novedoso en este dominio: la firma competente. Hemos de definirlo como el mecanismo que garantiza la responsabilidad y la identificación del firmante con competencia para firmar y que da validez al diploma como entidad en cualquier formato. Por ejemplo, como ocurre en muchos países, si el Rector debe firmar un diploma en papel físico, éste debe ser el firmante competente en el formato electrónico y no un artefacto electrónico ajeno a la persona competente. En este sentido la firma en servidor tiene contextos de uso mucho más limitados que los escenarios de firma en cliente y que se proyectan directamente ante las personas firmantes. A esta nueva característica es a lo que llamamos firma competente.

6.2.4.3. Verificación abierta de la autenticidad de la firma (VAA)

Una vez que el diploma certificado ha sido firmado con una firma competente, la autenticidad de la firma debe poder ser validable por entidades públicas ajenas al software que generó la firma. Es decir, la verificación del resultado criptográfico de firma debe poder ser contrastado por una tercera parte ajena al emisor con confianza pública, como por ejemplo, una plataforma gubernamental de verificación de firmas digitales. Pero aún más, debe ser verificable por cualquier ciudadano de forma asequible, lo que le confiere una forma de ofrecer los servicios electrónicos relacionados con la verificación y validación de documentos y certificaciones.

6.2.4.4. Trazabilidad electrónica independiente del formato (TEIF)

Consiste en mantener una traza en el diploma electrónico de tal manera que mediante un código de trazabilidad pueda consultar los metadatos o el documento que representa al diploma electrónico. Esto puede ser un código en sí y podría incluir el sitio de consulta o URL. Este mecanismo de trazabilidad no debe confundirse con el de autenticidad, ya que en sí lo que garantiza es que existe en la plataforma de emisión de certificados. En algunos sistemas esta característica se suele confundir con un sellado de tiempo que de alguna manera genera una falsa expectativa de autenticidad cuando en el contexto hay un marco de seguridad de nivel bajo.

6.2.4.5. Token de un solo uso o uso limitativo (T1UL)

Finalmente es necesario un mecanismo por el cual un usuario con derecho a recibir un diploma electrónico puede tener acceso a él y descargarlo. Se debe establecer un procedimiento por el cual de una forma segura se envía al usuario la llave que permite custodiar el diploma, al efecto de facilitar por ejemplo mediante correo electrónico un token de un sólo uso o definible en cuanto al número de usos.

6.2.4.6. Esquema de clasificación de la seguridad

Usando estas cuatro características para la seguridad de diplomas electrónicos ahora es posible clasificar los sistemas de emisión de diplomas electrónicos en función de este modelo. La Tabla 4 muestra esta clasificación.

	CS	TEIF	T1UL	VAA
Seguridad alta	X	X	X	X
Seguridad media	X	X	X	
Seguridad baja	X	X		

Tabla 4. Clasificación de sistemas de firma de diplomas electrónicos

6.2.5. EL PROYECTO DE OPENDIPLOMA

Siguiendo estos criterios, se ha desarrollado un sistema de información que siga este modelo y nos permita tener una visión práctica de la realidad de la viabilidad del sistema de acreditaciones educativas. En la figura se muestra una interfaz de la aplicación correspondiente a la gestión y firma de certificados.

Esta herramienta ha estado funcionando durante dos años y más de 20.000 diplomas electrónicos certificados han sido emitidos, firmados y enviados a usuarios finales de la fundación de la Universidad Nacional a Distancia. El contenido de los cursos va relacionados con programas de aprendizaje para la vida cotidiana (Life Long Learning, LLL) con un volumen de más de 50.000 estudiantes.

El Proyecto de Diploma Abierto (OpenDiploma) se ha desarrollado como paradigma MVC, multicapa a nivel software y dos partes físicamente distribuidas en bloques de servidor y de cliente. Un esquema de la arquitectura del proyecto se puede ver en la Figura 40.

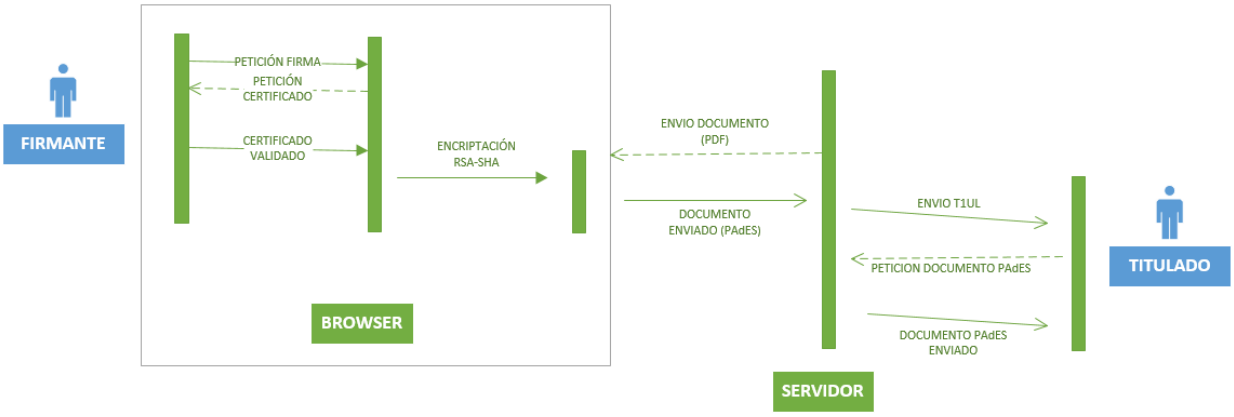


Figura 40. Esquema del proyecto de diploma electrónico

En primer lugar, la persona firmante ha tenido que autenticarse en el sistema usando un navegador ordinario, como se muestra en la Figura 41. Disponiendo de un certificado de firma robusta y reconocida, esta operación se hace sobre el lado cliente para garantizar además una firma competente.

Figura 41. Acceso a la plataforma de diplomas

Una vez en el sistema, existen diversas funcionalidades de gestión, como son la generación, preparación de lotes de firma o envío masivo de diplomas mediante

un mecanismo de T1UL definido en el framework. La Figura 42 consiste en una de las interfaces que centraliza en un único cuadro algunas de estas posibilidades.

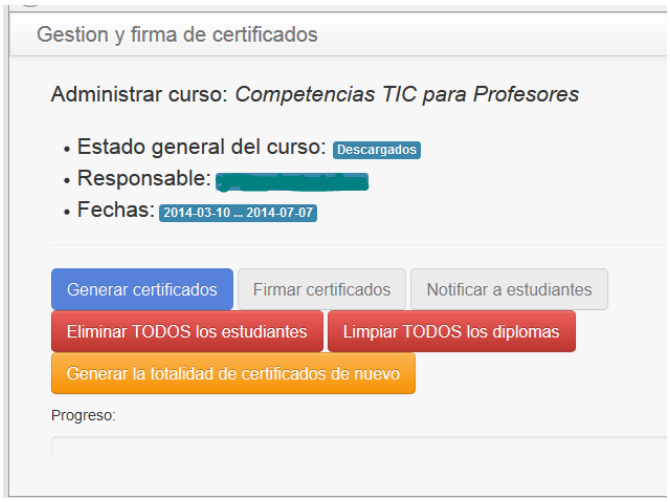


Figura 42. Una vista de administración

Si se selecciona la opción de "Generar certificados", los diplomas electrónicos y un código de validación segura (CVS) se genera y almacena para cada uno de ellos. Una vez que están emitidos, la persona firmante puede proceder a realizar la firma digital. Para ello, se habilita una opción de "Firma de diplomas". Después de la firma los diplomas electrónicos se impulsan al servidor. A continuación se envía por correo electrónico mediante el uso de un token T1UL que se genera para cada estudiante, como puede seguirse en la Figura 40 mostrada anteriormente. En la Figura 43 se muestra la notificación a los estudiantes cuando acceden al sistema para recoger su diploma electrónico, una vez agotado el token, advirtiendo que se la descarga no es válida o bien se ha descargado anteriormente el número de veces establecida.

Figura 43. Notificiación de descarga con token agotado

En otro orden de cosas, los gestores de recursos humanos encargados de los diplomas disponen de un cuadro de control y chequeos. Así es posible comprobar la firma de una plataforma de validación universal con el fichero de diploma. Adicionalmente puede comprobar mediante la gestión de códigos de validación en un sistema de comprobación como se muestra en la Figura 44.

Figura 44. Vista del módulo de verificación y validación

En cuanto a los detalles de implementación además de seguir un esqueleto determinado por el patrón Web Modelo-Vista-Controlador, ha sido desarrollada en lenguaje PHP, con orientación a objetos, sobre servidor web Apache y motor de datos MySQL. Se utiliza además tecnologías como HTML5, Twitter Bootstrap, PDO, FPDF, JSON, jQuery y Ajax. Como muestra en la figura 45, el fragmento de código del módulo T1UL está invocado desde uno de los controladores de la aplicación para la invocación y envío del token a los estudiantes.

```
    }

    private function send($id)
    {

        $curso_estudiante = CursoEstudiante::find($id);
        $estudiante = $curso_estudiante->estudiante();
        $course = $curso_estudiante->curso();
        $http_protocol = strtolower(substr($_SERVER["SERVER_PROTOCOL"], 0, 5)) == 'https' ? "https" : "http";
        $download_base_url = $http_protocol . "://" . $_SERVER['SERVER_NAME'] . ":" . $_SERVER['SERVER_PORT'] . '/certificate
/download/';

        //generate ott
        $ott = new CourseValidation($curso_estudiante);

        if (!$ott->generateOTT()) {
            return false;
        }


        $subject = "Diploma del curso " . $course->nombre;
        $body = 'Estudiante: ' . $estudiante->apellidos . ', ' . $estudiante->nombre . '<br/>';
        $body .= 'Curso: ' . $course->nombre . '(' . $course->horas . ') <br/><br/>';
        $body .= 'Se encuentra disponible su diploma con firma electrónica en formato PDF en la plataforma de emisión de
certificados <br/>';
        $body .= 'Enlace de descarga: ' . $download_base_url . $curso_estudiante->ott;
```

Figura 45. Fragmento de código usado por el módulo T1UL

6.2.5. EVALUACIÓN Y SATISFACCIÓN DE LA EXPERIENCIA

Una de las experiencias se ha desarrollado sobre el sistema de formación de la Fundación de la Universidad Nacional de Educación a Distancia. Los datos correspondiente al funcionamiento del proyecto durante el año 2014, se dio servicio a un total de 7.920 estudiantes a los que se les emitió un diploma electrónico en sustitución del de papel. No se ha recopilado información sobre aspectos demográficos ya que el objetivo principal era conocer si los estudiantes percibían este uso electrónico como un primer paso hacia el escenario definitivo de esta tecnología en estudios reglados y no reglados. De los 7920 estudiantes, 2019 contestaron un cuestionario simple sobre la pregunta de "¿Piensas que el uso de un diploma electrónico es útil para ti?". Las respuestas estaban en una escala de tres ítems: (0) No me resulta útil, (1) No sé, y (2) Es realmente útil.

Una vez recibido el token de acceso de uso limitativo que garantiza la autenticidad del acceso al diploma electrónico, los estudiantes que voluntariamente querían contestaron. Como resultado se obtuvieron 1.671 posturas positivas al cambio en formato electrónico, 218 contestaron negativamente y sin decidir/indecisos en cantidad de 130. Esto supone un porcentaje del 83% de estudiantes a los que el sistema implementado les pareció una buena solución, frente a un 11% que rechaza el diploma electrónico como mecanismo alternativo al formato papel.

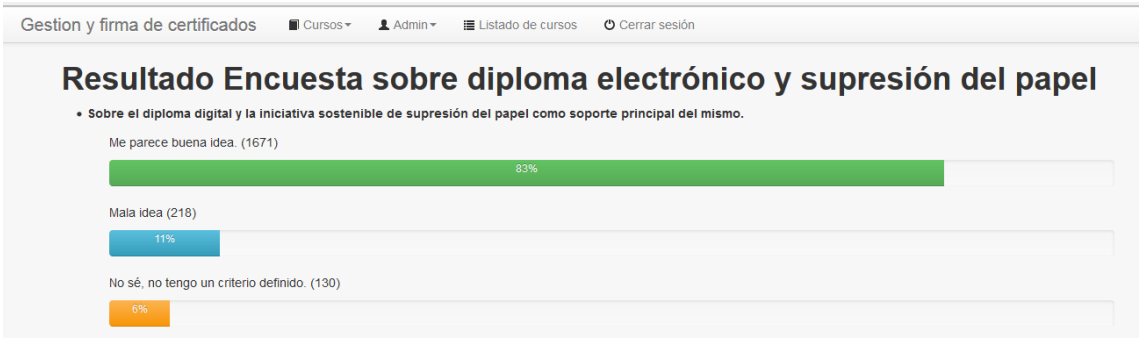


Figura 46. Resultado encuesta sobre diploma electrónico

6.2.6. DISCUSIÓN Y CONCLUSIONES DEL PROYECTO

En esta sección se ha presentado una experiencia de gobernanza electrónica relacionada con la gestión y emisión de los diplomas que se ha desplegado en el ámbito de una fundación universitaria (FUNED) alcanzando más de 20.000 diplomas electrónicos generados, firmados y enviados a los estudiantes.

Se ha diseñado un framework para diplomas electrónicos y se ha introducido una nueva característica a tener en cuenta, el aspecto de firma competente, entre otras que se establecen para caracterizar un sistema de emisión de diplomas y permita su clasificación en grados de seguridad. Esta clasificación permitirá determinar qué clase de sistema se propone a una institución o empresa y qué nivel de seguridad debe ser el esperado.

En relación a la herramienta TIC se ha realizado un somero estudio económico que nos permita discernir sobre la viabilidad de este tipo de sistemas. Se ha tomado para esta valoración 10.000 diplomas electrónicos. Como se muestra en la tabla, el coste de enviar 10.000 diplomas manualmente supone un coste

estimado de 17.300 euros, lo que supone 1,73€ por diploma. El desglose se puede ver asimismo en la tabla.

Partida ***10.000 diplomas***	**Coste estimativo** **(€)**
Impresión (papel, tinta) *(Papel calidad media)*	8.000
Ensobrado	2.000
Sellado postal	6.500
Coste en personal (ofimática, base de datos, organización) 8 horas.	800
Total	17.300

Figura 47. Coste de hacer 10.000 diplomas a mano

El número estimado de diplomas que la organización como la FUNED por año puede esperarse cercano a los 20.000. Con estas premisas parece claro que el uso de diplomas electrónicos podría ser una buena opción para una institución educativa de tamaño medio, incluso si existiesen costes de infraestructuras para la arquitectura tecnológica.

Aparte se ha evaluado el rendimiento del sistema diseñado mediante un análisis en profundidad de los tiempos de respuesta. Considerando el tiempo que implica el aspecto CS para firmar en el lado del cliente, la duración media de este proceso criptográfico emplea 2,5 segundos por diploma. Esto significa que el

proceso de firma es lento comparado con un proceso de firma en servidor y extremadamente más rápido que el proceso tradicional manual.

En este sentido los niveles tecnológico y legal se han explorado a fin de mejorar la aplicabilidad del sistema a nuevos escenarios de seguridad en el ámbito del Derecho. Consecuentemente mientras que el concepto de la oficina sin papel ha sido recurrente durante años, la evolución del eGovernment y la eSociedad requieren aire fresco to fomentar los escenarios emergentes de e-Educación. Esto en cambio implica retos, en gran medida dentro de un panorama multidisciplinar.

6.2.7. TRABAJO FUTURO DE INVESTIGACIÓN

Se estima que a nivel mundial que la emisión de gases de efecto invernadero (GHG) ha aumentado un 70 por ciento desde 1970. Hoy día el criterio de los expertos en la materia trata de subrayar el papel de las TIC para contribuir de manera esencial a la mitigación de los efectos del cambio climático [141].

Como continuación de esta investigación en el plano de gestión, es interesante hacer hincapié en las acciones que permitan promocionar soluciones innovadoras para la conciencia medioambiental y la supresión efectiva del uso del papel en e-Educación y por extensión a eGovernment. Una línea entre muchas podría ser un evaluar el soporte a un diploma electrónico sostenible (e-green diploma), una vez consolidado un modelo de emisión y de seguridad expuesto en este capítulo.

No obstante se puede afirmar que la sustitución del papel en documentación con valor legal depende del nivel de seguridad implementado, por lo que la pareja

conceptual visión ecológica y seguridad están íntimamente ligados, y tienen relación directa con la satisfacción de los usuarios.

Los retos emergentes de gobernanza inteligente y sostenible implican una nueva visión de trabajo en los negocios, en la industria, en el sector privado y en el sector público. Por el camino esto implica apertura y transparencia en la gestión, provocan nuevos retos y nuevas estrategias de la información y de las comunicaciones, especialmente si aplicamos el concepto sostenible medioambiental.

6.3. PLANO CIENTÍFICO-EDUCATIVO

Esta segunda parte del capítulo se presenta una investigación sobre los aspectos de fondo de la Educación mediante el uso de herramientas TIC, gamificación y estrategias educativas innovadoras. Se ha desarrollado un modelo de laboratorio de ciberseguridad educativa enfocada como plataforma curricular basada en actividades de aprendizaje activo, que permita incorporar actividades prácticas y experiencias de perfil tecnológico para estudiantes con un enfoque multidisciplinar y una aproximación hacia el aprendizaje para la vida. El resultado de este trabajo de la tesis permite extrapolar este modelo a otras disciplinas sociales, a profesionales del sector público y privado, así como a los ámbitos educativos universitarios. Nuestra argumentación parte de la idea de que

actualmente las personas en edad escolar han crecido como nativos digitales, lo que facilita la transversalidad de este proyecto.

6.3.1. ASPECTOS GENERALES

En la actualidad diversas áreas de la ingeniería y en especial de la ingeniería informática pueden considerarse ampliamente transversales. Su implicación en la vida cotidiana hace necesario que algunos de los conocimientos técnicos sean entendidos y comprendidos por profesionales no técnicos. Nuestra argumentación es que en nuestras universidades aterrizan cada año más estudiantes nativos digitales, que se han relacionado desde temprana edad con dispositivos electrónicos.

En este trabajo exploramos el reto y la experiencia de desarrollar habilidades típicamente ingenieriles relacionada con la ciberseguridad en un inusual contexto académico dentro de la rama de las ciencias sociales, en concreto en alumnos de Derecho y Criminología.

Se hace un estudio mixto en varias partes: primero, cualitativamente de la intercepción de lo ingenieril y lo social en cuanto a corpus de conocimiento; segundo basado en técnicas de encuesta se investigan las concepciones previas sobre un grupo experimental de estudiantes; y tercero se diseña un laboratorio de aprendizaje basado en juegos (GBL) aplicando modelos teóricos instruccionales y motivacionales; finalmente se muestra la experiencia del laboratorio y se discuten los resultados.

Observamos las concepciones previas sobre los ítems técnicos evaluados, el resultado de la puesta en práctica del laboratorio diseñado y la satisfacción de los estudiantes con la experiencia.

Las experiencias basadas en habilidades ingenieriles deben ser incorporados de forma transversal al resto de ramas de las ciencias no tecnológicas, nuestra investigación aporta una experiencia en esta línea y aporta confianza en este sentido para a las nuevas hornadas de estudiantes cada vez más nativos digitales.

6.3.2. MOTIVACIÓN CIENTÍFICA

En la actualidad diversas áreas de la ingeniería, especialmente la ingeniería informática y electrónica, aunque no solo, pueden considerarse ampliamente transversales. En este contexto puede considerarse el caso de la ciberseguridad como un ejemplo paradigmático. Su transversalidad no sólo afecta al ámbito de la ingeniería. Afecta a la vida cotidiana de manera que debemos ocuparnos de ella desde múltiples puntos de vista: derechos y libertades individuales, colectivos, factores económicos, intereses corporativos y nacionales, consumidores, etc.

De este modo, los profesionales relacionados con el Derecho, abogados, jueces, criminólogos, entre otros, requieren cada vez más de una formación técnica suficiente. Aunque no es necesario que lleguen al conocimiento técnico altamente especializado, estos profesionales si deben ser capaces de comprender claramente el dominio de la realidad en la que se mueven. Y en el caso de los criminólogos

además deben ser capaces de dirigir una investigación con solvencia, aunque posteriormente tengan que apoyarse en otros especialistas.

La preocupación por la formación en ciberseguridad en todos los niveles es de interés para el mundo académico. La interacción entre ingenieros y profesionales no-técnicos está en el punto relevante de la educación a día de hoy en esta esta materia como exponen McGettrick [142] o se puede ver en [143] donde Burley y Bishop concluyen que la educación en software seguro debe aplicarse tanto a programadores como no programadores. A todos los niveles, pero especialmente en el entorno universitario, se ve necesario actualizarse y aprovechar la experiencia y el conocimiento de la empresa privada y de las instituciones gubernamentales, como se sintetiza en [144] y en los trabajos de la profesora Atman [145]. Asociaciones profesionales como ACM o IEEE trabajan en este sentido en el "The Joint Task Force on Computing Curricula" con el fin de facilitar un currículum de referencia en seguridad de la información para el currículum de las ciencias de la computación [146].

Nuestra investigación presenta el análisis, diseño y experiencia de un curso de ciberseguridad para Criminología. Hoy en día en general todas las titulaciones en criminología incorporan materias relacionadas con los delitos "digitales". Sin embargo, la formación básica de estos profesionales no es técnica. Sus fundamentos se centran en Derecho y en las técnicas criminalísticas tradicionales bien establecidas. Por ello, enseñar ciberseguridad a no ingenieros se presenta como un desafío, pero a la vez como una necesidad en una sociedad del conocimiento cada vez más tecnificada. Para abordar esta tarea, una aproximación

educacional interesante puede ser utilizar el aprendizaje basado en juegos (GBL), una tendencia emergente que nos puede prometer cruzar confortablemente ese puente entre la ingeniería y las ciencias sociales. Además de pretender habilidades ingenieriles que extiendan su aprendizaje en la vida, se pretende introducir habilidades para aprender-a-aprender y el aprendizaje continuo necesario posteriormente en la vida laboral.

En la actualidad GBL y concretamente los serious games son una tendencia claramente emergente en diversos ámbitos, tanto educativos como tecnológicos y profesionales. De hecho, en IEEE estiman que jugar en 2020 va a ser una actividad integrada en más del 85% de las tareas diarias, de tal manera que tanto en la empresa como en la educación será habitual encontrar elementos de juegos [147].

El interés general de la ciberseguridad en diversas disciplinas científicas así como los diferentes perfiles profesionales relacionados con esta área hacen que los serious games y el aprendizaje orientado a juegos puedan ofrecer recursos educativos que faciliten su comprensión y aprendizaje. De hecho a lo largo de los últimos años se han realizado numerosos estudios relacionados con los juegos digitales desde distintos puntos de vista y para distintos sectores.

Desde otro punto de vista también es interesante la tendencia a diseñar juegos con intención educativa. Las teorías modernas de aprendizaje efectivo sugieren que el aprendizaje es más efectivo cuando es activo, experiencial, funcional y contextualizado, basado en problemas (Problem-Based Learning, PBL) y de feedback inmediato.

Sobre la base de la evolución tecnológica, hoy día los investigadores han revitalizado, abundado y ordenado estas ideas. Al éxito de los videojuegos, se suma el dinamismo de los juegos en Internet, en las redes sociales y tecnología ubicua. Y en general se distingue entre los juegos para el divertimento y los juegos útiles para conseguir otros objetivos [148]. Así, el objetivo de los serious games es aportar valor a áreas del conocimiento como salud, educación, gobierno, etc.

Sin embargo, fue el profesor Clark C. Abt, en 1970, quien aplicó este concepto sobre juegos aplicados en su libro "Serious Games" de una forma generalista, aunque para juegos de mesa con tablero y cartas [149].

Como antecedente de interés, la idea del juego como un elemento característico necesario y anterior a la cultura social, fue estudiado por el historiador holandés J. Huizinga, quien acuñó el término "Homo Ludens" a mediados del siglo XX en referencia a que el juego es una característica propia del ser humano [150].

En cuanto a la educación con juegos, más recientemente algunos trabajos vienen explorando el estado del arte de juegos relacionados con la seguridad para que puedan ser útiles para estudios de ingeniería, como en [151], donde en concreto estudian algunos juegos orientados a la enseñanza de la ingeniería y la administración de redes. Otros autores han aportado juegos y en relación con juegos específicos para ciberseguridad destaca CyberCIEGE, un simulador con formato de videojuego para simular entornos y mecanismos de seguridad en red [152]. Aunque su jugabilidad ha devenido en obsoleto con la evolución de las técnicas de animación, su utilidad sigue siendo notable sobre escenarios en red en

general e incluso en aspectos más especializados de las mismas como puede verse en el artículo de Irvine y Tompson en [153].

Por otro lado, entendemos que los juegos deben incorporarse a la formación aportando valores docentes. No basta con que sean ilustrativos, entretenidos o diviertan a los estudiantes. Deben tener algún valor pedagógico y debe precisarse a partir de sus características qué papel pedagógico desempeñan.

Se han desarrollado varios modelos educativos que explican los distintos resultados que se producen del aprendizaje basado en juegos. Así, O'Neill, Wainess y Baker [154] han identificado las habilidades cognitivas con respecto a los juegos, agrupándolas en cinco familias que tratan de la comprensión del contenido, la resolución de problemas, la colaboración del trabajo en equipo, la comunicación y la auto-regulación. El modelo propuesto por Wouters, Spek y Oostendorp posteriormente, por otro lado, contempla cuatro tipos de resultados de aprendizaje, clasificados en conocimientos y habilidades cognitivas, habilidades motoras, resultados de aprendizajes afectivos y resultados de aprendizajes comunicativos [155].

Nuestra investigación se ha aplicado a la asignatura "Sistemas y planes de seguridad y emergencia" del Grado en "Criminología y ciencias de la seguridad", dentro del área de Seguridad de la Información impartido en la Facultad de Derecho de la Universidad San Pablo, premiado en 2015 como proyecto de innovación docente [156].

Este trabajo de investigación está organizado de la siguiente forma. En primer lugar se detalla la metodología utilizada para construir un laboratorio de juegos. Para ello se analiza el área de conocimiento y el perfil de los estudiantes. Con estas consideraciones previas, se describe una encuesta realizada a los estudiantes con anterioridad a la construcción del laboratorio con el fin de determinar carencias, temores y prejuicios. Estos datos serán útiles en el momento de decidir qué juego incorporar para solventar estos aspectos. Seguidamente se detallan qué criterios generales se utilizarán para la incorporación de serious games al laboratorio y qué decisiones deberá tomar el equipo docente. A continuación se presenta la construcción del laboratorio de juegos para la asignatura concreta teniendo en cuenta las anteriores consideraciones y la evaluación de los resultados. Por último, se presenta las conclusiones del proyecto y el trabajo futuro que se abre a partir de esta investigación.

6.3.3. METODOLOGÍA DE LA INVESTIGACIÓN

Dado que el objetivo del trabajo es sencillo de enunciar: diseñar un curso de ciberseguridad basado en juegos bajo los criterios expuestos. Los métodos para llevarlo a cabo deben servir para detallar suficientemente el proceso de construcción para que sea reproducible. En esta sección se analiza este proceso, los criterios utilizados y las decisiones que ha realizado desde el punto de vista docente en cada parte del proceso.

En primer lugar se analiza el contexto de la asignatura a impartir, desde su área de conocimiento hasta el marco de la titulación en que se encuadra atendiendo

especialmente tanto al perfil de los estudiantes como a los resultados del aprendizaje y las capacidades objetivo de la asignatura en la titulación.

Seguidamente se analiza el grupo de estudiantes con el fin de detectar conocimientos ya alcanzados o carencias, prejuicios y temores relacionados con la materia. Con ello, se estudia la idoneidad de incorporar serious games en el proceso docente.

6.3.3.1. Análisis de aplicación

El análisis del curso de ciberseguridad en un entorno de educación universitaria como este debe considerar necesariamente los objetivos generales de la titulación. Entre las salidas profesionales de los titulados en criminología está la especialización pública, como es el caso de letrados, miembros de la judicatura o policías, y la especialización privada, en la línea de directores de seguridad y detectives.

En la Tabla 5 se muestra el plan de formación a nivel general que ha sido desarrollado. La asignatura que consta de 12 créditos ECTS (European Credit Transfer System), se distribuyen en áreas de seguridad física, seguridad electrónica y seguridad de la información. En este trabajo nos centramos en esta última área. La relación entre teoría mediante clases y práctica de laboratorio ha sido de 2:1, es decir, dos horas de contenidos teórico prácticos en el aula por cada hora de trabajo en el laboratorio. Debe tenerse en cuenta que el software utilizado en el laboratorio es de libre distribución y los estudiantes pueden trabajar con él en cualquier parte,

no sólo en el laboratorio. Si bien esas horas que el estudiante ha dedicado libremente no se han incluido en la relación anterior.

ESQUEMA GENERAL DE FORMACIÓN

1	Principios de la seguridad.
2	Política, planes y procedimientos.
3	El factor humano.
4	Vulnerabilidades, amanezas y malware.
5	Ciberterrorismo, ciberespionaje y organizaciones criminales.
6	La respuesta ante incidentes e informática forense.
7	Acceso a la información y criptografía aplicada
8	Escenarios de seguridad en red
9	Wifi y delincuencia ubicua
10	Falsedades, estafas y phising
11	Fenomenología del pago electrónico y crimen económico
12	Delincuencia informática
13	Protección de datos personales

Tabla 5. Esquema del plan de formación

6.3.3.2. Estudio del contexto educativo

En la actualidad la relación de la criminología y la ciberseguridad resulta evidente. Con el avance de la tecnología, su uso generalizado en la sociedad actual y la globalización [157], los comportamientos desviados son instrumentalizados también de forma digital. La Criminología es una ciencia de la seguridad que estudia la fenomenología criminal y el comportamiento antisocial del hombre. Áreas de conocimiento que estudian los mecanismos de prevención, técnicas de

investigación, el tratamiento de la víctima, y el por qué, cómo y cuándo se desarrolla el acto criminal. Esto supone una fuerte carga de derecho penal, psicología y sociología, pero también científico-médico y tecnológico.

Por otro lado, el cuerpo común de la ciberseguridad incluye disciplinas fundamentales como las ciencias e ingenierías informáticas, derecho, ética y psicología, gestión de negocios y didáctica, sociología y sus aspectos criminológicos [158].

Las oportunidades para la formación de ciberseguridad en los grados universitarios de Criminología son escasas y en gran medida se concentran en alguna asignatura, o parte de ella. En otras ocasiones y de forma adicional, se puede presentar el uso de la informática como un recurso para abordar otras materias y técnicas tradicionales criminológicas, como representación del escenario del crimen, trazabilidad instrumental y balística, ayuda al análisis de pruebas y evidencias, etc., cuya temática no es objeto de la ciberseguridad.

La aparición de nuevas formas delictivas y conductas antisociales viene potenciada por la aparición de nuevas tecnologías. Las redes sociales, comunicación permanente, computación en la nube, el fenómeno de la Internet de las Cosas…, en todos ellos pueden encontrarse oportunidades para la delincuencia. Es necesario comprenderlas y enseñarlas desde el prisma criminológico y tecnológico.

Por tanto, ambas disciplinas son multidisciplinares y es necesario acomodar enfoques científico-tecnológicos con los jurídicos, psicológicos etc.

La naturaleza de la Criminología, con gran *background* en derecho, y de la ciberseguridad, con un fuerte componente tecnológico, es diferente. En la Figura 48 se ha intentado confeccionar en este trabajo una representación conceptual de la relación entre criminología y ciberseguridad a que nos estamos refiriendo.

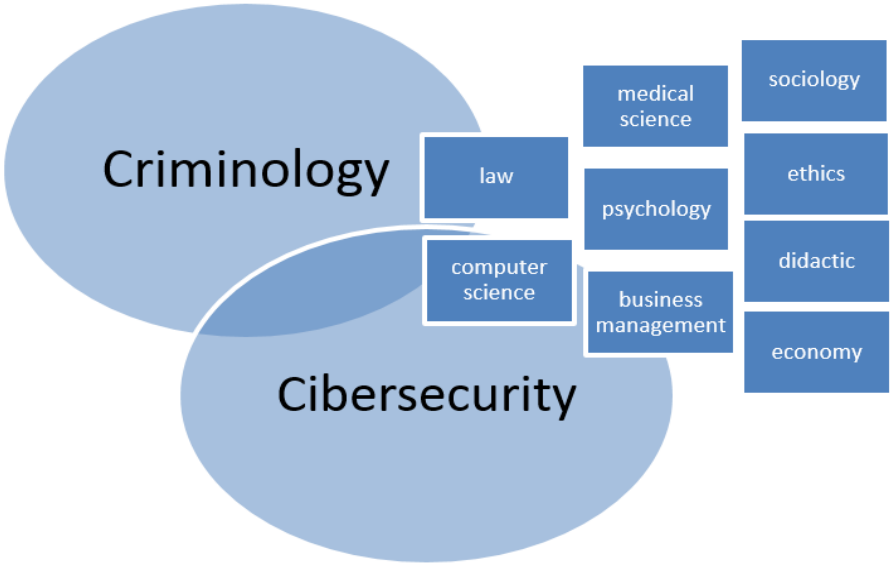


Figura 48. Relación conceptual entre criminología y ciberseguridad

Con todo ello, el perfil de los estudiantes se caracteriza por tener una sólida formación jurídica y en técnicas tales como inspección ocular, balística y médico-forense, así como psicología, pero con poca formación en ciencia de la computación o ingeniería en general. En la práctica, la criminología digital todavía tiene grandes retos por delante.

6.3.4. FASE DE LAS IDEAS PREVIAS

Sobre la base del contexto universitario planteado, la siguiente fase de la investigación ha sido realizar un estudio sobre las ideas previas de los estudiantes, sus prejuicios sobre la materia y sus temores. El carácter multidisciplinar de la asignatura y de la titulación debe entenderse como un reto y las dificultades originadas por ello deben ser superadas.

6.3.4.1. Métodos aplicados a las ideas

Para ello se ha utilizado la técnica de la encuesta, con respuestas breves y/o identificación de conceptos. Se ha diseñado un modelo de evaluación de ideas previas basado en 20 ítems principales y 26 descriptores sobre ciberseguridad.

El objetivo de la encuesta es establecer una visión inicial en el proceso de enseñanza-aprendizaje. De esta manera, se evalúan contenidos conceptuales, actitudinales y predisposición procedimental, dirigido por el plan de formación establecido. En la Tabla 6 se muestra estos ítems y en la Tabla 7 los descriptores.

#	ÍTEM DE EVALUACIÓN	PREGUNTA PLANTEADA
I1	Prospección y expectativas generales.	¿Qué crees que vas a aprender en esta materia?
I2	Concepto de información.	¿Podrías decir qué es la información y los sistemas de información?

I3	Descriptores clave sobre ciberseguridad	¿Cuáles de estas palabras te suena y sabrías identificar de qué tratan?
I4	Actitud inicial sobre la materia	¿Crees que es un arte o una ciencia?
I5	Inquietudes y preferencias	¿Qué enfoque te atrae más para estudiar esta área? (Ejemplos: matemáticas, prácticas, procedimientos, técnicas)
I6	Motivación por la ciberseguridad	¿Has visto alguna película o leído alguna novela que te haya llamado la atención sobre seguridad de la información?
I7	Aspectos sociológicos o morales	¿Crees que atacar sistemas es bueno o malo / es necesario o innecesario?
I8	Organización de la seguridad	¿Sabes lo que es un Sistema de Gestión de la Seguridad de la Información (ISMS)?
I9	Experiencia personal sobre incidentes	¿Qué experiencia tienes con problemas de seguridad informática?
I10	Colaboración general en Internet	¿Compartes información por Internet? ¿Qué medios usas principalmente?
I11	Idea sobre abusos por correo	¿Te aparecen mensajes de remitentes desconocidos a menudo? ¿Sabes sobre spam?
I12	Prospección sobre redes sociales	¿Cómo utilizas las redes sociales? (Facebook, tuenti, twitter, linkedIn, myspace…) ¿Conoces cómo configurar la privacidad en esas redes?
I13	Posicionamiento moral frente a tecnologías emergentes	¿Sabes lo que es el Cloud Computing? ¿Crees que es bueno o malo?
I14	Disyuntiva ante la computación ubicua - pervasiva	La computación ubicua (dispositivos móviles siempre conectados, teléfonos, tabletas...) ¿Crees que dan más beneficios que problemas?

I15	Sensación de riesgo	¿Te suena lo de los ataques de inyección de SQL, o el XSS, o el web side defacement?
I16	Psicología y prejuicios	¿Qué tipo de personas crees que son los hackers?
I17	Idea sobre la firma electrónica	¿Sabes cómo funciona la firma electrónica o mencionar algún ejemplo?
I18	Concepto de certificado digital	¿Sabes lo que es un certificado digital?
I19	Prospección abierta	¿Alguna otra cuestión de tu interés para reflejar tus ideas previas?
I20	Meta evaluación y predisposición	¿Qué te parece esta encuesta?

Tabla 6. Modelo de ideas previas para la encuesta sobre ciberseguridad

El ítem de evaluación i3 se desglosa en una colección de descriptores que exploran sobre aspectos conceptuales relacionados con la ciberseguridad. Se han establecido 26 descriptores etiquetados como se muestra en la Tabla 7. El propósito de este modelo es marcar por identificación los conceptos que les suenan a los estudiantes.

a. Ciberseguridad	**b. Ciberamenazas**	**c. Riesgo informático**	**d. Vulnerabilidad**
e. Exploits	f. Script kiddie	g. Gusano	h. Troyano
i. ISO 27001	j. Virus	k. Pentest	l. Criptología
m. Spyware	n. Criptosistema	o. Scamming	p. Skimming
q. Esteganografía	r. Plan de continuidad	s. Plan de contingencia	t. Phising
u. DoS	v. Cookie	w. Firewall	x. IDS
y. DMZ	z. Datos personales		

Tabla 7. Modelo de descriptores evaluados sobre ciberseguridad

6.3.4.2. Resultados y discusión

El resultado empírico de la encuesta de ítems de ideas previas se ha representado en un cuadro de doble entrada, que se puede ver en la Tabla 8. Este es el resultado del análisis de las respuestas y clasificación. Los valores tomados son:

- 1 equivale a una visión positiva del ítem evaluado
- 0 equivale a no desea responder, valor consecuente con el carácter voluntario de la participación
- -1 equivale a una visión negativa sobre el ítem evaluado

En la tabla, cada fila representa la evaluación de un estudiante de criminología y las columnas los ítems evaluados sobre ciberseguridad.

Estudiante/item	**i1**	**i2**	**i3**	**i4**	**i5**	**i6**	**i7**	**i8**	**i9**	**i10**	**i11**	**i12**	**i13**	**i14**	**i15**	**i16**	**i17**	**i18**	**i19**	**i20**
e1	1	1	1	1	0	-1	1	0	0	0	0	1	1	0	0	0	0	1	0	0
e2	0	0	1	1	0	-1	-1	-1	-1	1	1	0	-1	-1	-1	1	-1	-1	0	0
e3	1	0	1	1	1	1	1	-1	1	1	1	1	1	1	-1	-1	1	-1	0	1
e4	1	0	1	1	1	0	-1	1	1	1	0	-1	-1	-1	-1	1	0	0	0	1
e5	1	0	1	1	1	0	1	0	-1	1	1	1	1	1	-1	-1	1	0	0	1
e6	1	1	1	0	1	0	1	0	0	0	-1	1	0	0	0	0	0	0	0	0
e7	1	1	1	1	1	1	1	1	-1	1	1	-1	1	-1	-1	1	1	1	1	1
e8	1	1	1	1	1	0	1	-1	-1	-1	-1	-1	-1	1	-1	1	-1	1	0	1

e9	1	1	1	1	1	1	0	1	-1	1	1	1	1	1	0	-1	0	0	0	1
e10	1	0	1	1	1	1	1	-1	-1	1	1	1	0	1	-1	-1	1	0	0	1
e11	1	0	1	1	1	0	0	-1	-1	1	-1	1	-1	1	-1	1	1	-1	0	1
e12	1	1	1	1	1	1	1	1	-1	1	1	1	1	1	-1	-1	-1	-1	-1	1
e13	1	1	1	1	1	1	-1	0	-1	1	0	1	0	1	0	0	0	0	0	1
e14	1	-1	1	1	0	-1	-1	-1	-1	1	1	-1	1	-1	-1	1	1	-1	-1	1
e15	1	1	1	1	1	0	1	-1	1	1	-1	-1	-1	1	-1	1	-1	-1	1	1
e16	1	1	1	1	1	1	1	1	-1	1	1	1	-1	0	0	1	0	0	0	0
e17	1	1	1	1	-1	-1	-1	-1	-1	-1	1	1	1	-1	-1	0	-1	-1	-1	1
e18	1	1	1	1	1	1	1	-1	1	1	1	1	1	1	-1	-1	-1	-1	-1	1
e19	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e20	1	1	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
e21	1	0	1	1	1	-1	1	-1	-1	1	1	1	1	-1	-1	1	-1	-1	-1	1
e22	1	1	1	1	1	0	0	1	-1	1	1	1	1	-1	0	-1	0	0	0	1
e23	1	-1	1	1	1	-1	1	-1	-1	1	1	1	-1	1	-1	1	-1	1	0	1
e24	1	1	1	1	1	1	1	-1	0	1	1	1	1	1	-1	1	1	-1	-1	1
e25	1	0	1	1	1	0	-1	0	-1	1	1	1	1	-1	0	1	1	0	1	1
e26	1	1	1	1	1	1	1	-1	-1	1	1	1	-1	1	-1	1	1	-1	-1	1

e27	1	1	1	1	1	1	1	-1	1	1	1	1	-1	1	-1	-1	1	1	0	1
e28	1	1	1	1	0	0	0	0	-1	0	-1	1	0	0	0	1	0	0	0	1
e29	1	0	1	1	1	0	-1	-1	-1	1	1	1	1	0	-1	1	1	-1	-1	-1
e30	1	0	1	1	1	1	-1	-1	-1	-1	-1	1	-1	1	-1	-1	-1	-1	-1	1
e31	1	1	1	1	1	1	1	-1	-1	1	1	1	-1	1	-1	1	1	1	-1	1
e32	1	0	1	0	1	1	-1	0	0	1	0	1	0	-1	0	-1	0	0	0	1

Tabla 8. Representación empírica de sentimiento de los resultados de ideas previas

El estudio de las ideas previas de los estudiantes de grado en Criminología da como resultado una visión global muy útil para poder investigar el tipo de laboratorio y tener una base de partida para diseñar el curso y explorar las posibilidades y tipología de juegos que deben aplicarse a este dominio de la educación sobre ciberseguridad. Podemos apreciar en la Figura 49 una visión de las ideas previas con una significación negativa, por su dificultad, desconocimiento o aversión hacia el ítem evaluado. De ellas, destacan el ítem i8, i9 y el i15. Las ideas negativas están relacionadas con la organización de la seguridad, la experiencia de personal sobre incidentes y la sensación de riesgo.

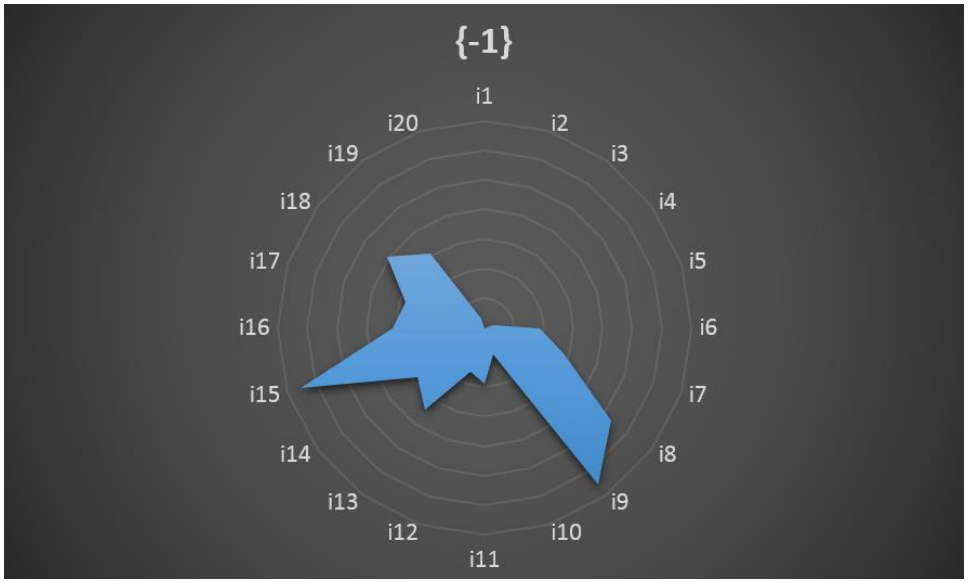


Figura 49.Representación de negatividad en la fase previa

En cuanto a las ideas positivas evaluadas, los ítems i1, i3, i4, i5, i10, i12 e i20 presentan resultados positivos. Los parámetros i1, i4 e i5 evalúan aspectos globales que indican una predisposición positiva para acercarse al aprendizaje de la ciberseguridad. Interesante la positividad manifestada frente a colaboración en Internet y sobre el uso de las redes sociales (ítems i10 e i12). El ítem i20 es una meta-visión sobre el propio estudio de ideas previas que como vemos ha sido acogida como una iniciativa positiva.

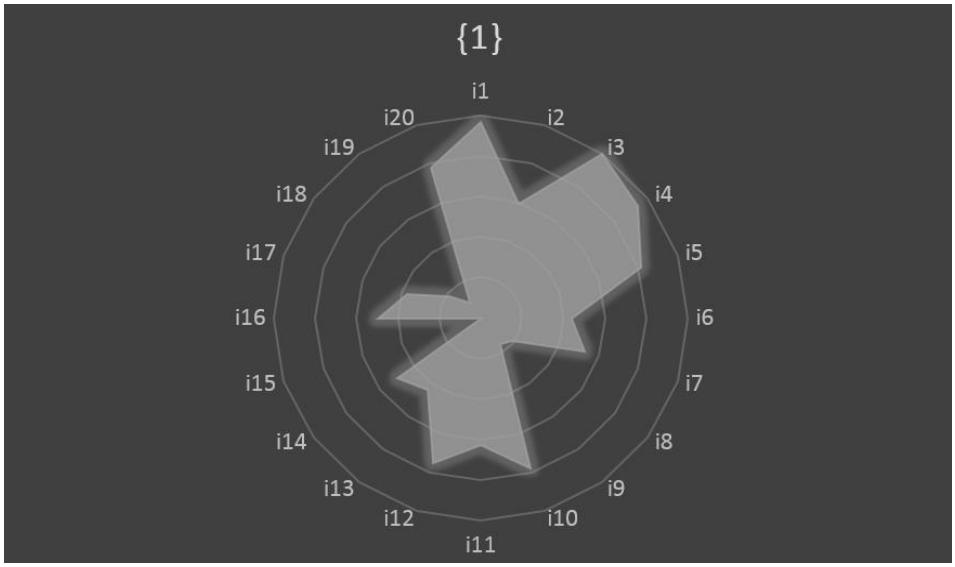


Figura 50. Representación de positividad en la fase previa

El ítem i3 evalúa contenidos conceptuales sobre un conjunto de descriptores mediante un proceso de identificación y marcado, cuyos resultados se tratan a continuación. La Figura 50 muestra gráficamente estos resultados.

La evaluación de los descriptores es una prueba objetiva de reconocimiento de términos identificativos de la seguridad de la información, que pretenden sondear el nivel de conocimiento de la materia desde el prisma de los criminólogos en formación. En la Tabla 9 se muestran los resultados, donde las columnas muestran los descriptores.

ESTUDIANTE/ DESCRIPTOR	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E1													•		•							•	•			•
E2	•			•			•	•		•												•	•			•
E3							•	•				•	•	•								•	•			
E4		•					•	•		•												•				•

E5	•	•	•	•			•	•		•			•													
E6	•	•	•					•		•			•													•
E7	•	•	•	•			•	•					•						•			•	•			•
E8	•	•	•	•			•	•		•																•
E9	•	•	•	•			•	•		•												•				•
E10	•	•		•			•	•		•										•		•				•
E11	•	•	•	•			•	•		•												•				•
E12	•	•	•	•				•					•						•	•		•	•			•
E13		•	•					•																		
E14		•		•				•		•												•				•
E15	•	•	•	•			•	•		•		•	•									•	•			•
E16	•	•	•	•				•	•	•		•	•	•					•			•	•			•
E17	•	•	•	•			•	•		•		•	•							•		•	•			•
E18	•	•		•			•	•		•			•						•	•		•	•			•
E19	•	•		•				•		•			•	•						•		•	•			•
E20	•			•			•	•														•				•
E21	•	•								•										•						
E22	•	•	•	•			•	•		•		•										•	•			•
E23	•	•	•					•		•			•									•	•			•
E24	•	•		•			•	•		•			•							•		•	•			•
E25	•	•	•	•	•		•	•	•	•		•	•		•				•	•	•	•	•			•
E26							•	•		•												•	•			•
E27	•	•	•	•	•		•	•		•		•	•	•	•							•	•			
E28	•	•	•					•		•			•							•		•	•			•
E29	•	•	•	•			•	•				•										•	•			•
E30	•	•					•	•		•										•			•			
E31	•	•								•												•	•			•
E32	•	•								•																•

Tabla 9. Resultados de la encuesta de descriptores

Los resultados sobre términos de seguridad permiten definir un perfil de partida para organizar el proceso de enseñanza-aprendizaje. Sobresalen los

descriptores *a, b, h, j, v*, *z*, sobre los cuales debe partir el marco de trabajo teórico del laboratorio. Hay una identificación conceptual inicial sobre términos de ciberseguridad, ciberamenazas, troyanos, virus, cookies y datos personales. Estos pueden ser estos cimientos cognitivos para nuestro laboratorio.

La colección de descriptores *f, k, p, q, r, u, x*, y con un bajo resultado indagan los términos de scripts kiddies, pentest, skimming, esteganografía, plan de continuidad, IDS y DMZ. Por este lado, descubrimos carencias variadas tanto en técnicas, estructuras de protección y organización de la seguridad, que deberán ser reforzados mediante el diseño de proceso de laboratorio. La Figura 51 muestra estos resultados.

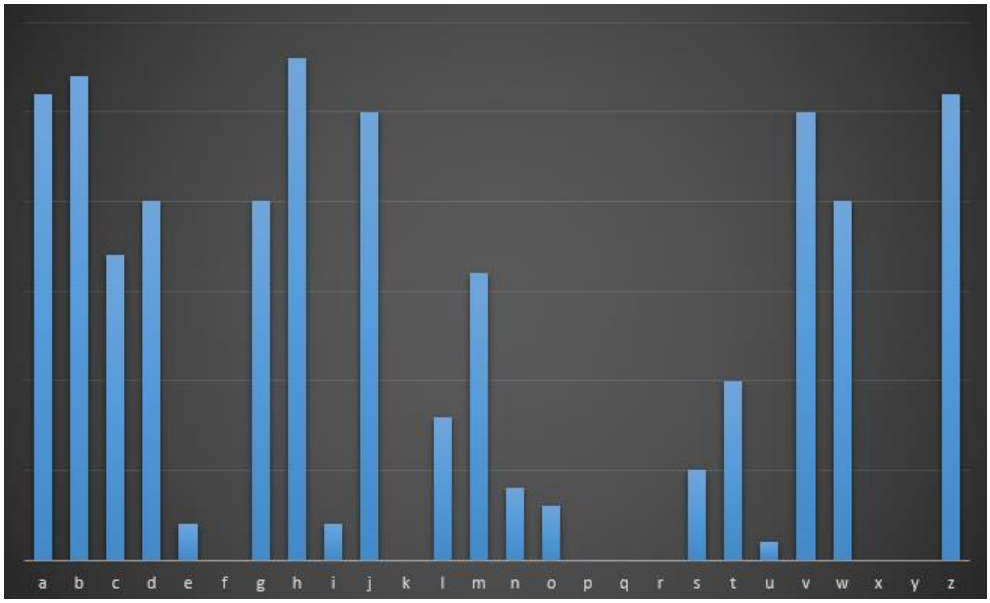


Figura 51. Evaluación de descriptores de ciberseguridad

6.3.4.3. Conclusiones parciales de la fase previa

Hasta aquí se puede concluir que la actitud y predisposición inicial de los estudiantes es buena, como se deduce que la percepción general mostrada hacia la materia es más positiva que negativa. En consecuencia, se ha estudiado los aspectos sentimentales positivos y por otro los negativos. Obsérvese que superponiendo las áreas evaluadas de sentimiento positivo y negativo el cálculo resultante es positivo, como se representa en la Figura 52 a continuación.

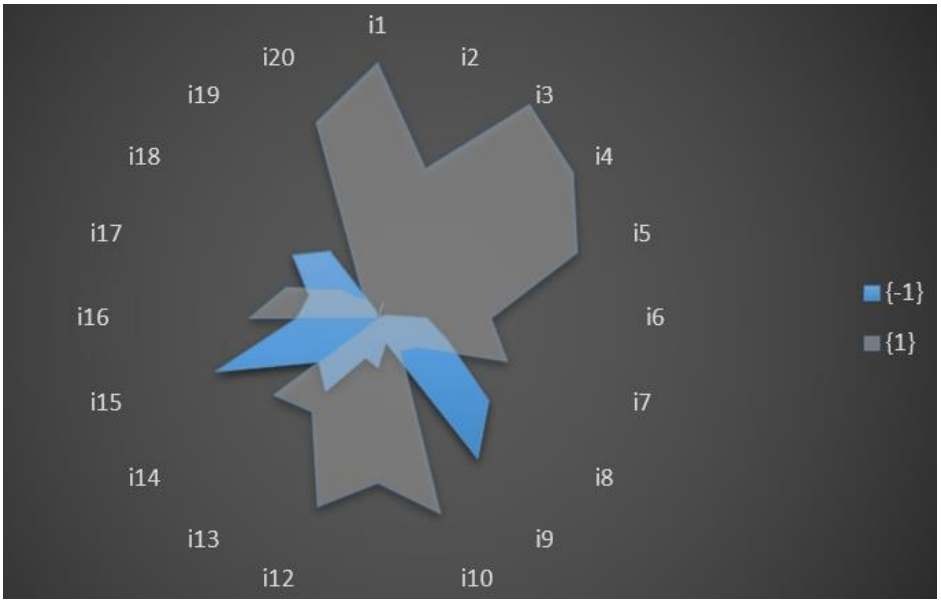


Figura 52. Superposición del análisis previo

El punto de partida sobre los contenidos conceptuales ha quedado establecido, en la evaluación de los descriptores que hemos definido, como una concreción de la evaluación general. Estadísticamente el valor modal del estudio de esta distribución cualitativa es cero, lo que supone un porcentaje del 27% de concepto nada conocidos. Visualmente puede verse en la Figura 53, donde se puede apreciar la línea de tendencia desde descriptores mejor conocidos hasta los menos conocidos. Esto nos permite tener una valoración para elaborar una estrategia aprendizaje de contenidos basado en conceptos significativos para los estudiantes.

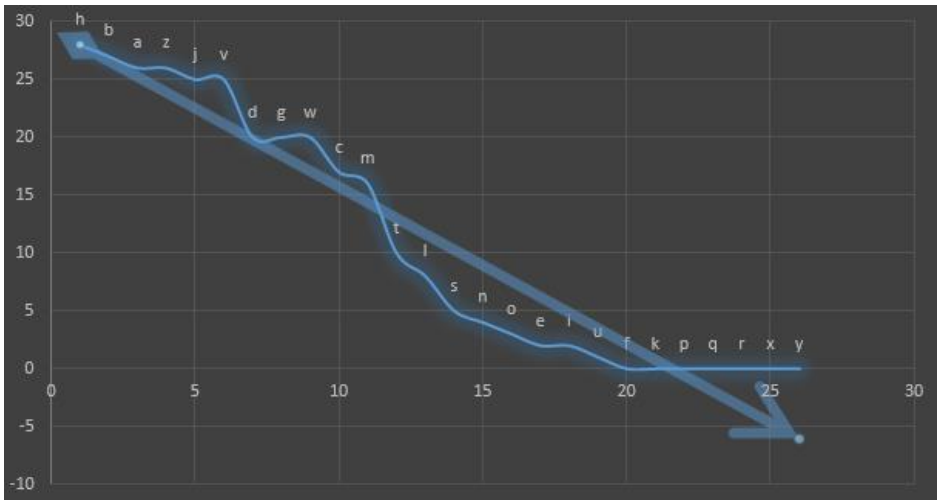


Figura 53. Tendencia de conceptos significativos basado en los descriptores

6.3.5. FASE DE DISEÑO DE LA INSTRUCCIÓN

Teniendo en cuenta la naturaleza del curso a impartir y el análisis realizado sobre las ideas previas de los estudiantes que lo recibirán, los serious games

aparecen como una herramienta útil como elemento facilitador de la adquisición de conocimiento.

El objetivo de los juegos en el curso es facilitar el estudio, no evitarlo. Son un complemento útil para ayudar a comprender los *procesos*. Incluso, en la medida de lo posible, deben permitir aumentar la productividad del aprendizaje permitiendo abordar contenidos que técnicamente son más complejos y quedarían fuera del alcance de los objetivos del curso, pero que conceptualmente pueden ser estudiados para comprender qué e incluso cómo suceden. La experiencia de "vivir" el proceso ayuda a entender los hechos y facilita la comunicación entre los profesionales de perfil tecnológico y socio-jurídico.

6.3.5.1. Métodos aplicados a la instrucción

Esta sección describe los métodos considerados en la investigación para diseñar un laboratorio de juegos como recurso didáctico que apoye la formación en ciberseguridad expuesta anteriormente.

El planteamiento de diseño del curso se realiza teniendo como base las teorías de aprendizaje y el diseño instruccional orientado para que el alumno pueda construir su propia experiencia a través de pequeños juegos que a su vez son comentados en una guía elaborada por el profesor.

La metodología del laboratorio de juegos consta de tres partes. En primer lugar se presenta cada juego, con una introducción sobre su relación con los

objetivos del curso y una reseña motivadora sobre la relación del tema tratado con sus inquietudes tanto personales como profesionales. En segundo lugar los estudiantes se distribuyen en parejas, facilitando el trabajo en grupo, el intercambio de opinión, la apertura de debates para el grupo, la búsqueda de información y la exploración a través de Internet facilitando con todo ello una participación activa. Finalmente, cada estudiante debe realizar individualmente una autoevaluación basada en los resultados de cada juego e indicar impresiones de satisfacción sobre cada unidad de juego de aprendizaje.

El laboratorio se ha puesto en marcha en un aula de informática con ordenadores en red y conectividad a Internet para estudiantes de tercer curso del grado universitario de Criminología. El número de estudiantes fue de 32 en total, 17 hombres y 15 mujeres. Así pues, el perfil del alumnado presenta una tasa relativa de género masculino-femenino equitativa, aproximada al 50% para el curso estudiado. El grupo cubre una edad objetivo de 20-24 años. Cabe destacar que no se pudo establecer un grupo de control ya que todos quisieron en principio participar de los laboratorios y consideraron "injusto" no hacerlo.

Para la selección de los serious games se ha considerado el modelo de Gagné de los nueve eventos de la instrucción con el fin de determinar la capacidad del juego para dirigir el aprendizaje hacia los resultados deseados desde un punto de vista funcional [159] y el modelo ARCS de Keller para considerar los componentes motivacionales [160].

Por último, entendemos que los juegos deben ser una herramienta facilitadora del autoaprendizaje a lo largo del curso, pero también del

autoaprendizaje futuro. Por tanto, deberá decidirse qué tipos de juegos utilizar antes de determinar los juegos concretos.

Con todo ello, se pueden establecer los siguientes criterios de selección:

- Qué tipos de juegos utilizar
- Qué contenido del temario cubre el juego
- Qué valor pedagógico instruccional cubre el juego
- Qué valor motivacional cubre el juego
- Qué valor añadido aporta

La primera decisión a tomar es qué juegos incorporar. Una primera alternativa de aproximación es utilizar un producto conocido. En el ámbito de la asignatura podría utilizarse CyberCIEGE, herramienta bien conocida que ya hemos presentado en secciones anteriores.

Sin embargo, entendemos que la actitud del equipo docente ante la incorporación del juego debe ser activa, no pasiva. Es decir, debemos construir el curso utilizando juegos como piezas de puzle que encajen hasta conseguir los objetivos deseados. Un único juego puede llevar al equipo docente a adoptar una actitud pasiva de manera que el juego determine el curso y no que el curso determine el juego. Por ello, entendemos que los juegos deben desempeñar el mismo papel que los bien conocidos objetos de aprendizaje en el entorno de eLearning.

Por otro lado, la reutilización de recursos es hoy en día una norma establecida en el área de ciencias de la computación (reutilización de código, librerías de programación, etc.). Y además este concepto ha sido ampliamente aceptado y utilizado de muy diversas formas en la red.

Por ello, entendemos de mayor interés construir el curso basado en juegos reutilizables de aprendizaje. Entendemos que las características de los recursos-juegos deben ser suficientemente simple, flexible, modular y reutilizable como para actuar como piezas de puzle.

Por otro lado, el no utilizar una única fuente y buscar los recursos disponibles en la red tiene como valor añadido un aspecto de especial interés. En primer lugar, los recursos deberán estar en sitios de confianza. Gran número de instituciones, universidades, organismos públicos y empresas de solvencia incorporan en sus páginas web recursos que pueden ser muy útiles en este contexto. Así, al utilizar estos recursos, el estudiante comprende de forma activa dónde puede y debe encontrar información fiable lo que será especialmente útil para su formación a lo largo de la vida. Pero además, este método tiene la ventaja de que el equipo docente tiene que "tomarse la molestia" de buscar, analizar y decidir si ese recurso es el más adecuado pero no sólo en contenidos. Especialmente se centrará en si es o no adecuado para el perfil concreto de sus estudiantes, sus aspectos motivacionales, etc.

Con todo ello, la propuesta se basa en construir un curso basado en un conjunto de juegos reutilizables que atienden tanto a las necesidades educativas como a los perfiles de ideas previas de los estudiantes concretos.

Aunque en la selección de los juegos durante la búsqueda se consideraron todas las necesidades simultáneamente, la elección puede concretarse en tres etapas. La primera etapa de la investigación consiste en explorar, identificar y evaluar los juegos disponibles de libre distribución atendiendo especialmente a la completitud de sus contenidos. Seguidamente se realizó una selección entre ellos atendiendo a los valores instruccionales y motivacionales y finalmente se analizó de qué manera podían proporcionar valor añadido en relación con las ideas previas de los estudiantes. La Figura 54 ilustra este proceso.

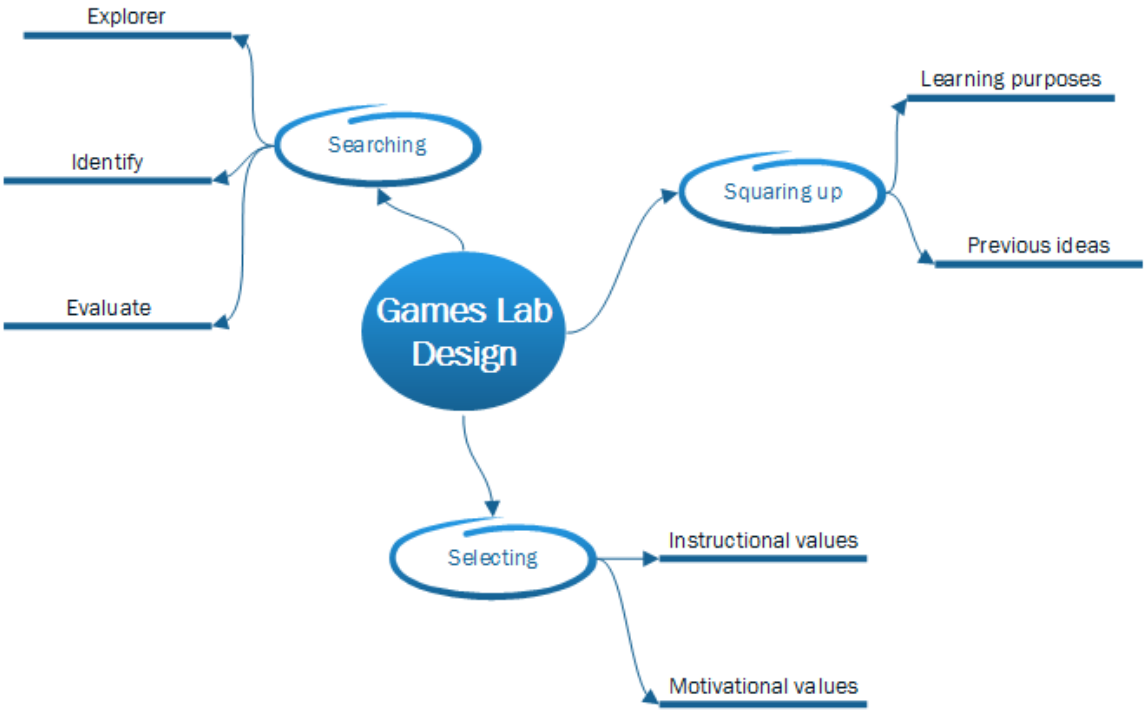


Figura 54. Esquematización del proceso de decisión

6.3.5.2. Discusión

Esta sección describe el resultado de la investigación para diseñar el laboratorio de juegos dentro de los estudios de grado de Criminología. Para ello, se realizó una búsqueda exhaustiva en la red.

La siguiente etapa de nuestra investigación consiste en explorar las posibilidades de juegos para plantear el laboratorio, clasificar y seleccionar los adecuados para el perfil previo en Criminología. Para ello, se investiga sobre bibliografía científica, webs de ciberseguridad de instituciones públicas y privadas, descargas de juegos instalables, y juegos más ligeros.

6.3.5.3. Elección de los juegos

La elección de los elementos del laboratorio de juegos se ha basado en la información obtenida de la etapa de investigación de ideas previas de los simuladores y serious games relacionados con seguridad de la información disponibles y de la idoneidad sobre los objetivos educativos definidos. Los juegos seleccionados deben estar accesibles, bien en descarga o bien en formato online, así como facilitar el aprendizaje activo, la exploración autónoma al ritmo del estudiante y deben fomentar la búsqueda de soluciones.

Con estas premisas, el marco de trabajo del laboratorio ha sido modelado en 15 actividades basadas en juegos. Cada actividad de juego se trabaja con tres recursos didácticos: el conocimiento teórico-conceptual ya trabajado, el aprendizaje

durante el juego y la reflexión posterior de consolidación de conocimientos. Esta colección de juegos, contextualizados en el laboratorio, permite abordar de forma global el plan de formación.

De la exploración sobre proveedores se han seleccionado a cuatro, de especial interés en el ámbito de la Ciberseguridad. En primer lugar, denotado *P1, Center for Information Systems Security Studies and Research* (CISR) perteneciente a la *Naval Postgraduate School* (NPS), proporciona información detallada en su web (cisr.nps.edu), donde facilita además descargas. Participa en la primera actividad formativa.

En segundo lugar, P2, Federal Trade Commission del gobierno de Estados Unidos, en colaboración con otras agencias federales. Proporciona en su sitio (onguardonline.gov) una profusa información y buenas prácticas de seguridad, en varios formatos digitales como video, texto y pequeños juegos descargables. Los juegos consisten en la exposición de un contexto o situación y una dinámica de toma de decisiones en la que participa el usuario contestando preguntas durante el juego. Por su facilidad de uso, hemos seleccionado este recurso como apoyo, para gran parte de las actividades (2-13).

Tercero, denotaremos *P3, Office of the National Coordinator for Health Information Technology's* (ONC), que presenta un juego interactivo online basado en el escenario de un centro sanitario organizado en varias rondas (healthit.gov). Ha sido la base para desarrollar la actividad formativa 14.

Y por último, *P4: National Center for Missing & Exploited Children,* que presenta varios juegos centrados en la concienciación y protección de niños (missingkids.com, nsteens.org). Nos ha servido para las desarrollar la actividad formativa 15.

6.3.5.4. Catálogo de juegos

Específicamente, las actividades de juego y su relación con los contenidos de la asignatura son los siguientes apartados.

- ***Juego 1***

Denominado "CyberCIEGE" (P1). Este juego es descargable desde la web del CIRS. Ellos mismos se definen como un simulador para la enseñanza de la seguridad en red. Su diseño modular mediante distintos escenarios permite su utilización parcial, como elementos de aprendizaje.

El módulo de "Information Assurance & Security Policies" permite trabajar los conceptos de principios de seguridad, organización de la seguridad y gestión de incidentes para los estudiantes de criminología, con la suficiente abstracción tecnológica. El escenario de la actividad se desarrolla en la oficina de una empresa y la problemática asociada a la incorporación de dos nuevos empleados.

El propósito de este juego es reforzar y enfatizar los contenidos relativos a los temas 1, 2, 3 y 6 del plan de formación del curso (ver Tabla 5 anterior).

1.1.1.1.1. Juego 2

"The case of the Cyber Criminal" (P2). Trabaja los conceptos de vulnerabilidades, amenazas, riesgos y delincuencia individual. El propósito de aprendizaje de este segundo juego es subrayar la relación entre crimen y ciberespacio, aprovechando la predisposición propia de los estudiantes de ciencias criminológicas.

Nuestro énfasis se centra en cubrir las necesidades de refuerzo del aprendizaje del tema 4 del plan de formación.

1.1.1.1.2. Juego 3

"Auction Action" (P2). Introducir el comercio electrónico y su problemática asociada. El propósito de la actividad trata de poner la atención sobre los tipos de fraudes relacionados con las transacciones por Internet, asimilando los contenidos del tema 11 y 12 del plan de formación.

1.1.1.1.3. Juego 4

"Follywood Squares" (P2). Permite trabajar los contenidos relacionados con el acceso a la información, los datos sensibles y la confianza de la información volcada en Internet. Nos interesa con esta actividad reforzar los contenidos en relación con el tema 7 y 8 del plan de estudios (Tabla 5).

1.1.1.1.4. Juego 5

"Invest Quest" (P2). Introduce la temática criminológica relacionada con conceptos financieros online. El propósito de este juego es ilustrar un escenario de seguridad en red con una temática profesional relacionada y la delincuencia

asociada, asentando los contenidos del tema 8, 11 y 12 del plan de formación especificado.

1.1.1.1.5. Juego 6

"Mission, laptop security" (P2). Refuerza los contenidos de seguridad física y gestionada. Nos interesa enfatizar los conceptos relacionados con las normas de organización de la seguridad, protección de datos desde un punto de vista físico y acceso a la información relacionado con el tema 2, 7 y 13.

1.1.1.1.6. Juego 7

"Phising, avoid the bait" (P2). Permite estudiar los conceptos de ingeniería social, fraudes, engaños, delincuencia y su relación con la protección de datos en red. El propósito de esta actividad es centrarnos en los aspectos de seguridad del tema 10, 12 y 13.

1.1.1.1.7. Juego 8

"P2P threeplay" (P2). Permite trabajar las áreas de seguridad en redes, colaboración y compartición de información, junto con amenazas y sus riesgos. Refuerza los contenidos de los temas 3, 4 y 8, relativos al factor humano en la seguridad, el malware y las amenazas relacionadas con escenarios de intercambio de ficheros en red.

1.1.1.1.8. Juego 9

"Friend finder" (P2). Presenta un escenario sobre el uso de redes sociales, sus amenazas y prevenciones necesarias. Nos permite enfatizar los contenidos del tema 3, 8 y 13.

1.1.1.1.9. Juego 10

"Spam scam slam" (P2). Trabajar la seguridad en el uso del correo, los engaños, estafas y las situaciones delictivas latentes. Es apropiado para tratar el tema 10 y 12.

1.1.1.1.10. Juego 11

"Beware of spyware" (P2). Trabaja los conceptos de malware, sus amenazas y la gestión de incidencias de una forma cercana al usuario. Nos permite reforzar los objetivos de aprendizaje del tema 4 y poder enfatizar parcialmente los del tema 5 con el propósito de resaltar su relación con el espionaje.

1.1.1.1.11. Juego 12

"Invasion of the wireless hackers". Es útil para reforzar los conceptos de redes inalámbricas, incluso introducir la movilidad con la computación pervasiva en la ciberseguridad. Nos resulta útil para trabajar el objetivo principal del tema 9, así como los conceptos relacionados con criptografía del tema 7.

1.1.1.1.12. Juego 13

"Id theft faceoff" (P2). Permite introducir el acceso a la información y la delincuencia relacionada con la suplantación de la identidad en la red y los conceptos de protección de datos personales. Los objetivos perseguidos con este juego cubren los temas 10, 12 y 13, relacionados con la cibercriminalidad y la protección de datos.

1.1.1.1.13. Juego 14

"CyberSecure:Your Medical Practice" (P3). Es un juego que presenta una dinámica más compleja sobre un escenario que simula un centro sanitario con múltiples estancias. Está dirigido por rondas y presenta casos de uso con preguntas que debe responder el usuario. Para nuestro laboratorio, es interesante para trabajar los conceptos de principios y organización de la seguridad, el factor humano y la protección de información sensible, correspondientes a los objetivos de los temas 1, 2, 3 y 13.

1.1.1.1.14. Juego 15

"Cyberbully Zombies Attack" (P4). Es un juego simple de tipo plataforma cuyo escenario simula un centro educativo atacado por intimidadores, simbólicamente representados como zombies. Es interesante para presentar las problemáticas de ciberbully y en general las conductas antisociales en el ciberespacio. El propósito del aprendizaje se centra en los temas 7 y 12 sobre fenomenología de la delincuencia y acceso a la información.

6.3.6. APLICACIÓN DEL MODELO INSTRUCCIONAL

Una vez establecidos los contenidos del curso y cómo las actividades en forma de juegos aportan conocimiento a estos contenidos, se consideraron el modelo de eventos de Gagné y el esquema motivacional ARCS de Keller con el fin de valorar su características y adecuación para el proceso de aprendizaje. La Tabla 10 presenta los elementos del modelo instruccional y el ARCS que se encuentra implícita o explícitamente en cada juego.

JUEGO	**GAGNÉ - EVENTOS DE INSTRUCCION**	**KELLER - ELEMENTOS MOTIVACIONALES**
JUEGO 1: CYBERCIEGE INFORMATION ASSURANCE & SECURITY POLICIES	Eventos: 1, 4, 5, 6,7, 8	Attention, Relevance, Confidence, Satisfaction
JUEGO 2: THE CASE OF THE CYBERCRIMINAL	Eventos 1, 4, 6, 7, 8, 9	Attention, Relevance, Satisfaction
JUEGO 3: AUCTION ACTION	Eventos: 1, 4, 6, 7, 8, 9	Attention, Relevance, Confidence, Satisfaction
JUEGO 4: FOLLYWOOD SQUARES	Eventos: 1, 6, 7, 8,9	Attention, Confidence, Satisfaction
JUEGO 5: INVESTQUEST	Eventos: 1, 4, 7, 8, 9	Attention, Relevance, Satisfaction
JUEGO 6: MISSION LAPTOP SECURITY	Eventos: 1, 4, 6, 7, 8, 9	Attention, Relevance, Confidence, Satisfaction
JUEGO 7: PHISHING AVOID THE BAIT	Eventos: 1, 3, 4, 6, 7, 8, 9	Attention, Relevance, Confidence, Satisfaction
JUEGO 8: P2P THREEPLAY	Eventos: 1, 3, 4, 6, 7, 9	Attention, Relevance, Confidence, Satisfaction
JUEGO 9: FRIENDFINDER	Eventos: 1, 3, 4, 6, 7, 9	Attention, Relevance, Confidence, Satisfaction
JUEGO 10: SPAM SCAMSLAM	Events: 1, 4, 6, 7, 9	Attention, Relevance, Confidence, Satisfaction
GAME 11: BEWARE OF SPYWARE	Eventos: 1, 4, 6, 7, 9	Attention, Relevance, Satisfaction

JUEGO 12: INVASION OF THE WIRELESS HACKERS	Eventos: 1, 4, 7, 9	Attention, Relevance, Satisfaction
JUEGO 13: ID THEFTFACEOFF	Eventos: 1, 4, 6, 7, 9	Attention, Relevance, Confidence, Satisfaction
JUEGO 14: CYBER SECURE YOUR MEDICAL PRACTICE	Eventos: 1, 4, 5, 6, 7, 9	Attention, Relevance, Confidence, Satisfaction
JUEGO 15: CYBERBULLY ZOMBIES ATTACK	Eventos: 1, 3, 4, 5, 6, 7, 9	Attention, Relevance, Confidence, Satisfaction

Tabla 10. Valores de aplicabilidad del modelo instruccional propuesto

La identificación de los eventos de Gagné en los juegos nos ha permitido establecer las condiciones de aprendizaje sobre las que apoyar nuestro diseño instruccional y fundamentar la selección de los juegos. Adicionalmente, nos permite observar las necesidades que debemos ofrecer por parte del equipo docente complementarias a los juegos para seguir para alcanzar los objetivos planteados.

Del estudio debemos destacar el primer evento en cuanto a que nos asegura un estímulo introductorio para "atraer la atención" del estudiante. De hecho, el propio ambiente fuera de la clase ordinaria refuerza el evento: aula de ordenadores, trabajo colaborativo, participación menos formal y directa que una clase presencial magistral. La evaluación realizada, sin embargo, valora específicamente al elemento-juego, mostrando en su ejecución un interés por el tópico utilizado por el juego para contestar y comprender interrogantes que van a ser aclaradas con el hecho de jugar.

El evento segundo que trata sobre "informar los objetivos" no son propios de los juegos, ya que por naturaleza son piezas reutilizables: serious games como

objeto de enseñanza. Por ello, la proyección sobre los objetivos educativos, propios de nuestro plan de estudios, no son informados por el juego y deben suplirse, consecuentemente, por parte del equipo docente presentando los objetivos de aprendizaje aparte y haciendo ver el plan de formación de la asignatura. En este mismo sentido, se presenta el evento número 3 de Gagné y, en determinados juegos, el evento 5. Todos ellos se completan por el equipo docente reforzando el evento necesario para el aprendizaje, como la "estimulación de recuerdos" o la "guía del proceso".

La tabla 8 expresada arriba representa la selección final de los juegos y sus características cuyo proceso de búsqueda se ha realizado valorando para cada uno de los contenidos a cubrir. Por otro lado, la información obtenida en esta tabla permite acompañar cada juego con una guía didáctica específica de manera que se completen las posibles carencias. Por ejemplo, en caso de que el juego no ofrezca autoevaluación la guía la podrá incorporar.

6.3.7. SECUENCIACIÓN DE ACTIVIDADES DE APRENDIZAJE

Una vez establecido el conjunto de juegos que forma nuestro laboratorio, es necesario tener en cuenta las dependencias educativas entre juegos y objetivos de aprendizaje. Parece coherente que los contenidos magistrales se entremezclen con las actividades de juegos en cierto orden. Esta relación sobre los propósitos educativos de los juegos se muestra en la Tabla 11. Como puede observarse un

juego tiene relación con uno o varios temas, lo que permite varias combinaciones posibles de secuenciación de los juegos.

CONTENIDOS DE APRENDIZAJE RELACIONADOS		**J1**	**J2**	**J3**	**J4**	**J5**	**J6**	**J7**	**J8**	**J9**	**J10**	**J11**	**J12**	**J13**	**J14**	**J15**
1	Principios de la seguridad	X													X	
2	Política, planes y procedimientos	X					X								X	
3	El factor humano	X							X	X					X	
4	Vulnerabilidades, amenazas y malware.		X						X			X				
5	Ciberterrorismo, espionaje y organizaciones criminales											X				
6	La respuesta ante incidentes e informática forense.	X														
7	Acceso a la información y criptografía aplicada				X		X						X			X
8	Escenarios de seguridad en red				X	X			X	X						
9	Wifi y delincuencia ubicua												X			
10	Falsedades, estafas y phising							X			X			X		

11	Fenomenología del pago electrónico y crimen económico			X		X										
12	Delincuencia informática.			X		X		X			X			X		X
13	Protección de datos personales						X	X		X				X	X	

Tabla 11. Propósito de los juegos respecto al plan de estudio

Estos resultados nos permiten planificar mejor el diseño del laboratorio de juegos permitiendo determinar el momento más adecuado para la actividad de aprendizaje. Conforme a esto, un juego será adecuado realizarlo al menos cuando comience el tema de contenidos con el que esté relacionado. También sería adecuado después, entre el primer y último tema relacionado (como se deduce de la Tabla 11), e incluso al final de todos los contenidos del plan de formación (Tabla 5).

Consecuentemente, en la Figura 55 se muestra un grafo de dependencias entre juegos, donde se ha tenido en cuenta la cuestión expresada sobre el tema de contenidos inicial (notado en color oscuro). Esto se ha representado básicamente siguiendo la técnica de evaluación y revisión PERT. Para mejorar su expresividad se han ordenado las tareas-juegos en niveles horizontales en función del tema de contenidos inicial del que se trate.

Como puede comprobarse, para una implementación concreta debe elegirse un juego de cada nivel horizontal y ubicar el resto de tareas-juego en el resto de

niveles de forma descendente. Así un ejemplo de secuenciación podría ser la lista ordenada: J1, J6, J9, J11, J4, J5, J7, J3, J14, J8, J2, J12, J15, J10 y J13, donde la temporalización concreta viene determinada por el tema final (notado en color claro). En esta implementación a partir del juego J14 en la secuencia se planificaría después o a la vez que se enseña los contenidos del tema 12.

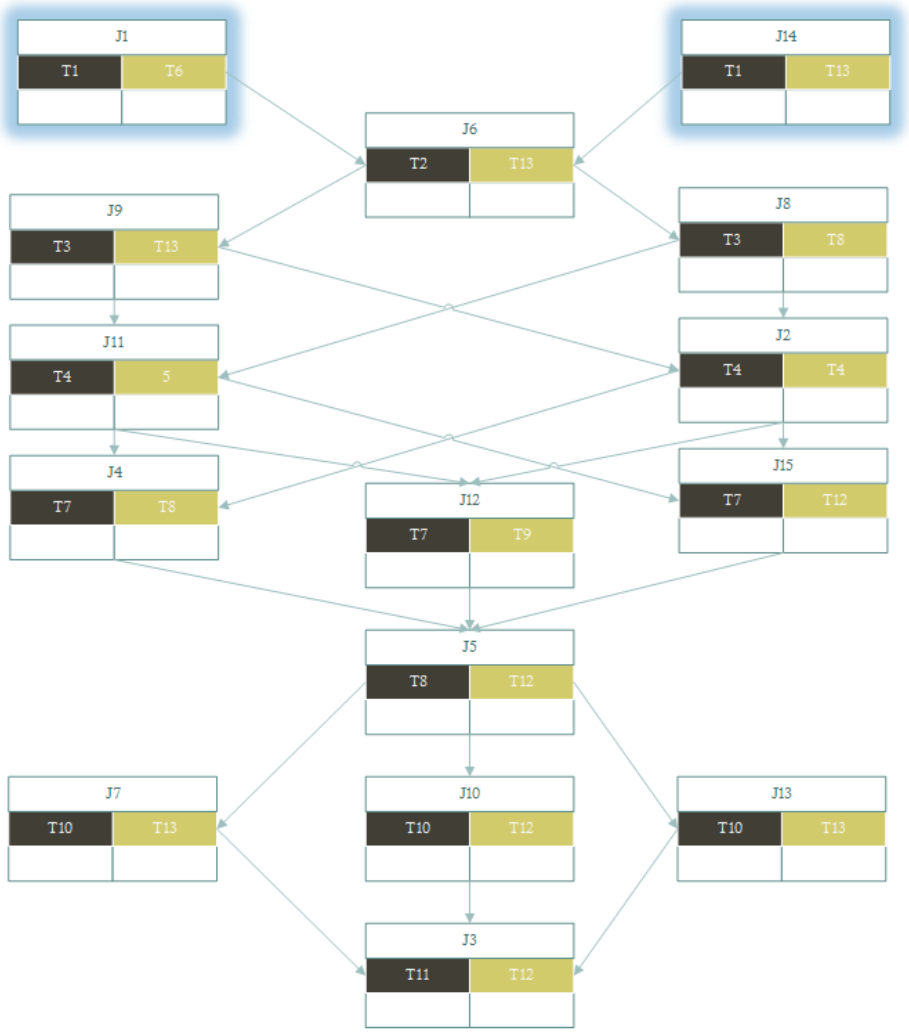


Figura 55. Grafo ordenado de aprendizaje basado en dependencias entre juegos

Esta técnica proporciona un razonamiento coherente con los objetivos de aprendizaje y la suficiente flexibilidad, dentro de un orden didáctico, para planificar el curso.

6.3.8. EVALUACIÓN DEL LABORATORIO

La evaluación de la experiencia de laboratorio en conjunto se ha medido mediante una encuesta voluntaria. El índice de participación ha sido del 87.5%, de los que el 46.9% corresponde a alumnos frente al 40.6% de género femenino.

Los resultados sobre la elección de los temas tratados en el laboratorio muestran una percepción calificada como buena o excelente en un 72%. La profundidad ha sido calificada como buena o adecuada en un 92%; y un 80% de los estudiantes considera que las actividades de juego son buenas o excelentes en cuanto a la aplicabilidad a su área profesional. La Figura 56 muestra gráficamente estos resultados.

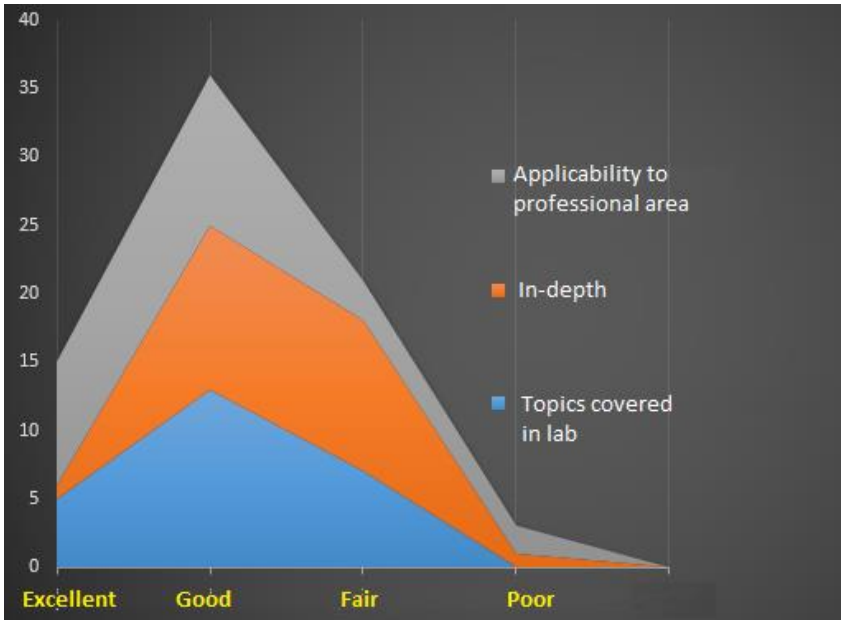


Figura 56. Resultados de la evaluación sobre el laboratorio

Asimismo se ha evaluado la percepción de los estudiantes respecto a la utilidad personal de los laboratorios. Una gran mayoría considera muy útil (88%), mientras que un 4% considera que no va a tener ninguna utilidad. Se muestra en la Figura 57 estos resultados.

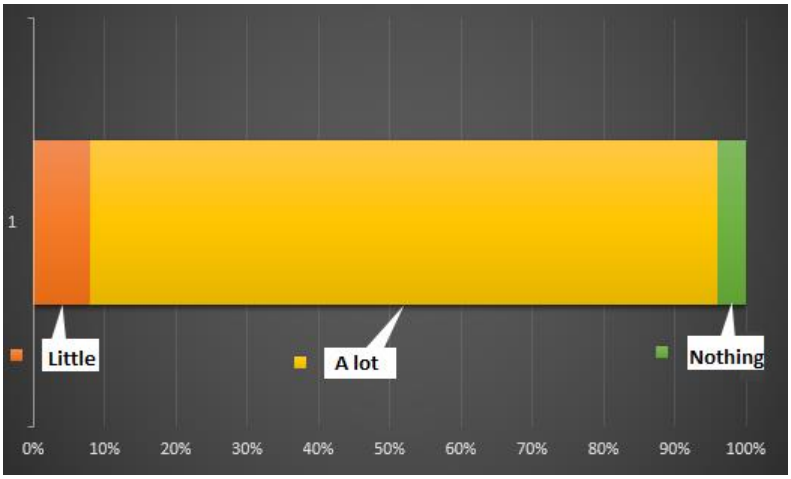


Figura 57. Evaluación sobre utilidad personal

Por otro lado, se solicitaron a los estudiantes propuestas de nuevos temas para el laboratorio. Entre ellas destacan las sugerencias sobre aspectos de interés como ingeniería social, hackers, defensa y detección de ataques, empleados problemáticos (insiders), criptografía en wifi, virus y ciberespionaje. Algunos de ellos estaban presentes en algunas de las actividades de laboratorio, pero estas sugerencias muestran interés en profundizar en estos aspectos tras haber cursado la asignatura.

Por último, se considera si el laboratorio de juegos mejora el proceso de aprendizaje de la materia de ciberseguridad en el entorno de los estudios de criminología. La respuesta delos alumnos fue sorprendentemente contundente: el 96% contesta que sí.

6.3.9. DISCUSIÓN SOBRE EL LABORATORIO

Llegados a este punto del trabajo es importante considerar la percepción del equipo docente y reflexionar sobre algunas de las lecciones aprendidas.

En general, el proceso más laborioso es evidentemente el de búsqueda. La laboriosidad de este proceso sería menor y la construcción de los laboratorios sería más eficaz si se considerasen y tratasen como objetos de aprendizaje, en el sentido habitual del e-learning. Sería muy útil una taxonomía y etiquetado de los elementos no sólo en función de sus contenidos sino considerando especialmente sus valores formativos, tanto desde el punto de vista instruccional como del motivacional.

En segundo lugar es importante destacar la necesidad de feedback en los juegos. Es decir, sería recomendable tener como norma al diseñarlo incorporar algún medio de autoevaluación que permita al usuario determinar su dominio sobre el juego concreto. Encontramos dificultades en la normalización de los datos de feedback, requiriendo la intervención y el procesamiento ad-hoc sobre cada juego.

Por último, destaca como muy positivo el hecho de que el laboratorio de juegos ha permitido que los estudiantes tengan la sensación de que pueden seguir formándose-informándose en los sitios de garantías a lo largo de la vida. Estos estudiantes que por su perfil no son tecnólogos, se encuentran capaces de buscar por sí mismos y ampliar conocimientos y destrezas que permitan seguir actualizarse, preocupación muy importante para ellos debido a la rapidez de los cambios en la tecnología y emergente uso antisocial relacionado.

6.3.10. CONCLUSIONES EN EL PLANO CIENTÍFICO-EDUCATIVO

Este trabajo muestra la metodología utilizada para construir un curso de ciberseguridad basado en juegos. Teniendo en cuenta todos los factores implicados, como el perfil no técnico de los estudiantes a los que va dirigido el curso, los prejuicios iniciales de los mismos y el reto que supone para los docentes preparar un curso de estas características, la experiencia podemos considerarla muy positiva tanto para los estudiantes como para los docentes.

En el caso específico de la tecnología relacionada con la ingeniería informática cada día más es necesario impartir conocimientos a profesionales no especializados técnicamente en este ámbito. En este contexto, los serious games pueden resultar una herramienta muy útil y eficaz.

Sin embargo, creemos que para utilizar los juegos con fines académicos sería muy valioso estandarizar y catalogar sus características tanto desde el punto de vista instruccional como desde el motivacional. Entendiendo los juegos como objetos de aprendizaje etiquetados podrían ser una herramienta habitual en el diseño de los cursos.

En conclusión, las experiencias basadas en habilidades ingenieriles para ciencias no-tecnológicas pueden dar resultados satisfactorios. Ha quedado demostrado en este trabajo de investigación considerando dos realidades: la capacitación previa de los estudiantes como nativos digitales y la necesidad de un

enfoque educativo transversal del currículo que facilite construir puentes entre las ingenierías y el resto de ramas del conocimiento científico.

6.4. EXTENSIONES EDUCATIVAS DE LA INVESTIGACIÓN

Como extensión de la investigación expuesta en la sección 3, una adaptación/aplicación se puede plantear para extenderlo a otras disciplinas especialmente las ingenieriles con fuerte enfoque en seguridad de la información. De hecho la idea de la globalización y la educación en ingeniería ha sido ampliamente recogida en revistas especializadas e ilustrada en artículos como en [161]. En la idea de extensión aquí podrían consistir en una revisión pedagógica del laboratorio y en añadir prácticas de laboratorio no basadas en juegos para incluir contenidos más cercanos a hacking ético.

Así esa otra línea de trabajo que se plantea en el plano educativo, priorizando la innovación y la inclusión de estrategias cercanas al constructivismo como idea pedagógica y el andamiaje educativo de autores clásicos en educación como Ausubel [162] y Bloom [163]. Un trabajo realizado al hilo de este capítulo cuyo resultado todavía está en proceso es la co-creación de instrumentos educativos con los alumnos, incluyendo proyectos en pequeños grupos y construcción de los exámenes de evaluación.

6.4.1. INNOVACIÓN CONTINUA

La innovación continua en el Espacio Europeo de Educación Superior (EEES) supone desarrollar nuevos mecanismos de enseñar y aprender, donde nuestros estudiantes tengan un papel más protagonista de su proceso educativo, una participación más activa y colaborativa. En consecuencia, *aprender haciendo (learning by doing)* parece en este sentido una estrategia más efectiva [164], que completa y perfecciona la misión educativa de las clases magistrales, de los seminarios y de los grupos de trabajo. De esta manera se prima la construcción del conocimiento desde un enfoque didáctico orientado a la acción.

6.4.2. PRINCIPIOS PEDAGÓGICOS EMERGENTES

La consideración desde el principio de habilitar a los estudiantes para el aprendizaje en la vida, en base a las habilidades y destrezas que pueden adquirir, es fundamental para el desarrollo pedagógico de nuestro laboratorio. Se trata que los estudiantes potencien sus capacidades más allá de las aulas, de tal manera que sean capaces de aplicarlos en su vida cotidiana y ser co-directores de su propio aprendizaje.

En este sentido, el laboratorio de ciberseguridad trabajado en esta tesis con un alto grado práctico prepara a los alumnos para ampliar su proyección laboral.

Cada vez en nuestra sociedad se demanda profesionales con competencias digitales solventes y tener unos andamiajes bien estructurados en seguridad de la información soporta los retos actuales y futuros.

En la misma línea que venimos exponiendo, con un laboratorio especializado sobre un entorno guiado, el estudiante puede sentir que se enfrenta a problemas reales de seguridad a los que debe dar respuesta, en la línea de las estrategias del aprendizaje basado en problemas.

Un laboratorio como aula especial propone una dinámica motivadora, rompe la rutina de clases presenciales tradicionales. Asimismo resulta en cierta medida menos formalista en cuanto al formato de comunicación entre alumno y profesor, y viceversa lo que permite una retroalimentación (feedback) más individualizada y un clima socio-emocional cálido para el aprendizaje.

Las actividades a realizar deben ser atentamente preparadas, para ello los elementos instruccionales son importantes y tomar referencias pedagógicas nos permite acercarnos de forma sistemática a la construcción de los contenidos, procedimientos y actitudes que nuestro laboratorio debe desplegar. El modelo instruccional de Gagné para un aprendizaje efectivo es una estrategia orientada a la capacitación que ya hemos presentado detenidamente en la sección anterior. Pero además y relacionado con esto es necesario en las actividades se correspondan con esos niveles de instrucción: informar de los objetivos claramente a los alumnos, estimular sus conocimientos previos, presentar el material nuevo a trabajar en el laboratorio, guiar el aprendizaje para que sea "acompañado" el alumno en su

proceso, suscitar el rendimiento individual, proporcionar retroalimentación, evaluar la eficiencia del rendimiento y favorecer la retención que permite construir el conocimiento. Pero, recordando de nuevo a Gagné, hay que cuidar asimismo las condiciones externas al aprendizaje, como las condiciones externas del aprendizaje, las actitudes de los estudiantes, la comunicación verbal, las destrezas intelectuales, las habilidades motoras y las estrategias cognitivas.

La motivación debe un pilar que sustente a largo plazo todo el trabajo en el aula o el laboratorio. Las estrategias sobre la relevancia de las actividades en los estudiantes deben hacerle comprender para qué le sirve el nuevo conocimiento sobre la base de lo ya conocido y para qué puede ser útil en el futuro. Otro aspecto de la motivación es la confianza, especialmente la confianza en el éxito, la enseñanza de estas materias en ciberseguridad cercanas a la ingeniería deben ser organizadas e instruccionadas. La satisfacción como la oportunidad de aplicar los conocimientos adquiridos redondea el esquema motivacional del alumno.

Por otro lado, como se aprecia en el ideario de las estrategias recientes sobre aprendizaje visible, se podría considerar a priori que todos los estudiantes pueden alcanzar el éxito [165]. Eso sí, si conseguimos el contexto de aprendizaje adecuado. Llevarlo a la práctica es un principio que entronca asimismo con algunas teorías como la del *mastering learning [166]*, donde otros componentes entran en escena, como el tiempo. Nuestra pretensión como consecuencia es diseñar un modelo de laboratorio que permita en nuestro entorno educativo preparar estudiantes

altamente competentes, especialmente en habilidades experienciales que les poder continuar su formación en ciberseguridad fuera del aula.

6.4.3. TÉCNICAS DIDÁCTICAS, INSTRUMENTOS Y RECURSOS

Las técnicas educativas que planteamos se enmarcan en sesiones donde se puedan resolver actividades de laboratorio. Estas actividades tienen una clara visión didáctica en técnicas de aprendizaje basado en problemas (ABP) o casos de estudio (ABC). La estrategia pretende el aprendizaje autónomo con la guía docente necesaria proponiendo un ejercicio similar al que pueden encontrar en el mundo real. Con estas técnicas basadas en problemas se fomenta no solo el estudio de conceptos, sino también de habilidades cognitivas como el razonamiento creativo y el aprendizaje significativo. Consecuentemente con la aplicación de las técnicas en pequeños grupos, se fomentan otras habilidades como son el trabajo colaborativo, la valoración del compañero, la responsabilidad, la toma de decisiones y el compromiso.

Los instrumentos entendidos como herramientas educativas para aplicar el proceso de enseñanza-aprendizaje que consideramos son:

- La encuesta. Dos tipos: una realizada en una fase inicial para descubrir las asunciones previas del estudiante respecto de la ciberseguridad. En segundo lugar, una encuesta final para evaluar los resultados, el proceso y la satisfacción.

- Instrumentos vivenciales del tipo programas de ordenador basado en simuladores y juegos.
- Talleres, donde a través de una actividad lúdica se desarrolla una habilidad de forma práctica.
- Tareas autónomas, que tratan de acercar la realidad mediante la observación empírica del comportamiento los sistemas de información y comunicación que rodean al alumno
- Experimentos, que ponen en práctica un concepto concreto basado en una hipótesis previa para trabajar y evaluar los resultados.

Los recursos necesarios consisten en un aula con material informático, de comunicaciones y de ingeniería forense. En consecuencia para la implantación del laboratorio de ciberseguridad en el contexto educativo, se puede estimar una primera visión que debe adaptarse las características del centro, alumnos y profesores, consistente en:

- 20 ordenadores personales, que son los medios principales de trabajo para los alumnos
- 2 servidores, con varios discos en RAID (Redundant Array) y suficiente memoria RAM para definir entornos virtualizados
- 20 discos USB, para trabajo de los alumnos en el laboratorio
- Estación hardware de clonación de discos duros
- Herramientas de ingeniería digital:
    - Herramientas forenses, del tipo EnCase Forensic o equivalente.

    - Herramientas de recuperación de datos, del tipo PC3000 o equivalente.
    - Herramientas de e-discovery, para el tratamiento de evidencias con valor judicial
    - Herramientas de análisis de vulnerabilidades
    - Herramientas de auditoría y test de penetración
    - Herramientas de detección de intrusiones
- Red de datos de comunicaciones en el aula
- Conexión a Internet

Hay que tener en cuenta que gran parte del software usado en los laboratorios de criminalística forense y peritaje digital actualmente emplean licencias comerciales de alto coste. Sin embargo, existen alternativas, en la mayoría de los casos parciales, de software de fuentes abiertas que podrían dar un buen rendimiento. Por otro lado, la dotación material de ordenadores puede aprovechar el parque informático existente si bien requiere de un análisis de viabilidad que permita su puesta en marcha e instalación. En lo que respecta a recursos humanos, el laboratorio requiere de un apoyo a la docencia orientada a la preparación de las actividades y la configuración de los entornos informáticos y de comunicaciones.

Con el propósito de facilitar que el proyecto sea reproducible se muestra una estimación de coste en la Tabla 12, teniendo en cuenta si no se dispone del material necesario y considerando un despegue desde cero. Si bien esta estimación debe adaptarse a la evolución propia de la tecnología, la obsolescencia de software concretos y las posibilidades de reutilización disponibles.

ITEM/VALOR ESTIMADO	VALOR APROX.
20 ORDENADORES PERSONALES	20000
2 SERVIDORES	3000
20 DISCOS USB	400
ESTACIÓN CLONADORA HARDWARE	200
HERRAMIENTAS FORENSES, DEL TIPO ENCASE FORENSIC	2750
HERRAMIENTAS DE RECUPERACIÓN DE DATOS, DEL TIPO PC3000	3000
RED DE DATOS	incluido
CONEXIÓN A INTERNET	incluido
BIBLIOGRAFÍA ESPECÍFICA	1000
APOYO DOCENTE DE PRÁCTICAS	4000
TOTAL ESTIMATIVO	**34350**

Tabla 12. Estimación de coste de laboratorio desde cero

6.4.4. DISCUSIÓN

La novedad del proyecto de laboratorio de ciberseguridad pone de relieve la dinámica activa en el aprendizaje, que resulta complicado realizar mediante clases

magistrales y seminarios entendidos como una presentación verbal de un tema por parte del profesor. Supone una mejora en cuanto a las competencias que un laboratorio de estas características permite desarrollar al alumnado. El enfoque mediante simuladores, casos de estudio o problemas prácticos, así como talleres y experimentos de informática forense permiten mejorar la docencia de la asignatura y dar una experiencia significativa a los estudiantes, que además podrá ser útil para su vida cotidiana.

El proyecto planteado consideramos que supone una mejora en la medida en que la seguridad de la información es un área de las ciencias cuyo aprendizaje es más efectivo con la experiencia de campo. Las clases de contenidos se plantean insuficientes para adquirir competencias y habilidades sobre conceptos relacionados con la tecnología, los comportamientos antisociales relacionados con las intrusiones, los virus, los hackers y las pruebas periciales que permiten la evidencia ante los tribunales de justicia.

La utilidad del proyecto de laboratorio de ciberseguridad se incardina en el valor añadido de dotar a la Facultad de Derecho de un laboratorio integrado curricularmente y un aula experiencial en materias relacionadas con la ciberseguridad, de actualidad tanto tecnológica y jurídica. Con ello, los servicios que se ofrecen al alumnado mejoran cuantitativa y cualitativamente, tanto a nivel pedagógico como especializado.

6.4.5. PROPUESTA DE ADAPTACIÓN CURRICULAR

Práctica de laboratorio 16

El caso de investigación de un disco borrado. Se trata de realizar una investigación sobre un disco USB borrado, pero que se sospecha que ha sido usado por parte de una organización criminal. El escenario es garantizar la preservación de la prueba y detallar las evidencias encontradas en un informe. El propósito de aprendizaje va relacionado con los temas 5 y 6 de los contenidos del plan (recordando la Tabla 5).

Práctica de laboratorio 17

La problemática de esnifar la red. Esta actividad supone un escenario donde cualquiera con conexión a tu misma red local puede rastrear todas tus comunicaciones. Se pretende analizar su uso, comprender la información y manejar las herramientas técnicas necesarias.

Se relaciona con los contenidos de los temas 7 y 8.

Práctica de laboratorio 18

El caso de la organización de la seguridad. Se trata de un escenario de un centro donde trabajan varias personas con sistemas de información, tanto con ordenadores personales como servidores. El propósito es hacer un informe simple de seguridad basado en la organización mediante la norma ISO/IEC 27001, indicando controles.

Esta actividad enfatiza los contenidos de los temas 1, 2 y 13 del plan de formación.

Práctica de laboratorio 19

El caso del hacking ético. Esta actividad se plantea en un escenario donde se toma el rol de hacker para realizar test controlados de intrusión sobre tu propio sistema de información con el objetivo de detectar los fallos antes de que lo encuentre una persona malintensionada. La relación de esta práctica con el plan de formación se concreta sobre los temas 3, 7 y 8.

Práctica de laboratorio 20

El caso del análisis forense en red. Se trata de realizar una identificación de la red criminal de datos, a fin de determinar evidencias digitales de su estructura, personas conectadas, dispositivos y funcionamiento. Los temas relacionados son 6, 8 y 12.

6.5. CONCLUSIÓN

En este capítulo hemos podido mostrar un vasto trabajo de investigación para comprender cómo funciona y que naturaleza existe en el dominio de la e-Educación al servicio de la e-Sociedad. Se han ordenado en dos planos convergentes. Por un lado la gobernanza propia de la administración y servicios educativos, donde se han realizado varias contribuciones relacionadas con la seguridad de los documentos oficiales acreditativos, como son los diplomas o títulos oficiales.

Por otro lado, se ha abordado la educación de fondo a través de herramientas TIC y se ha diseñado un marco didáctico basado en juegos aplicándolo a un laboratorio de ciberseguridad partiendo de las ideas previas de los estudiantes.

Complementariamente, se ha expuesto una extensión del plano científico-educativo aplicada a cualquier rama del conocimiento incorporando métodos basados en problemas sin juegos y, ampliatoriamente, se ha planteado una revisión pedagógica con más presencia de componentes constructivistas y de orientación al aprendizaje visible y efectivo.

Capítulo 7.

CONCLUSIONES Y TRABAJO FUTURO

En este capítulo se describen las conclusiones aportadas por la investigación acumulada en el trabajo de esta tesis y cuestiones planteadas en el futuro para profundizar en algunas de las líneas de investigación abiertas.

A lo largo de los capítulos de esta tesis se ha realizado un esfuerzo por proyectar el trabajo sobre modelos reproducibles y experiencias reales, sobre el entorno natural de los dominios estudiados, más que en meros diseños de laboratorio. Combinar el conocimiento interno con el externo, expresar estas ideas a través de frameworks, diseñar artefactos y en su caso liberar el código fuente desarrollado ha sido reconfortante en el sentido de devolver a la comunidad científica al menos una pequeñísima parte de lo que comparte.

La investigación sobre ingeniería de la seguridad y arquitecturas distribuidas de gobierno electrónico ha sido un reto multidisciplinar en cierta medida amplio y profundo. La tesis que aquí concluye recoge los resultados de esta actividad a lo largo de los últimos años.

- Se ha analizado las necesidades para la recogida de firmas con valor para las iniciativas populares. Se ha desarrollado una plataforma OpenILP, que fue el primer sistema electrónico de participación ciudadana con firma digital que ha tramitado una ley en España y ha sido autorizado por la Junta Electoral Central para iniciativas legislativas populares.

- Se ha comprobado el interés que tienen este tipo de plataformas debido a éxito mediático y social con la ley 18/2013 de regulación de la tauromaquia.

- Se ha observado que proyectos surgidos del ámbito académico, liberado como software libre, estimula la actividad y movimientos sociales, realimentando la idea de utilidad pública de la Universidad.

- El diseño arquitectónico distribuido presentado para democracia electrónica ha despertado cierto interés en la comunidad científica, particularmente en cuanto al modelo que permite el ejercicio de la co-creación de servicios públicos y la interoperabilidad.

- Se han analizado sistemas distribuidos de dominios críticos de seguridad, criminalidad y terrorismo, planteando un framework de intercambio de información para mejorar la seguridad global y un modelo de arquitectura basada en un ecosistema distribuido de relaciones de e-Government que estimule el sector privado. Para ello

nos apoyamos en el desarrollo de la plataforma SCEPYLT de intercambio de información crítica para varios países europeos, desplegada por la Unión Europea.

- Se constata el interés por sistemas de intercambio de información, distribuidos por red a través de protocolos web para interconectar nodos gubernamentales heterogéneos y mejorar la seguridad y la tramitación tradicional. Las regulaciones legales constatan este interés como la Directiva 2014/28/UE.

- Se ha analizado el dominio de Justicia electrónica y el fenómeno de la apertura sobre las arquitecturas tecnológicas, especialmente en cuanto a reingeniería de procesos (BPR) y la concepción, desarrollo e implementación de nuevos sistemas de e-Justicia.

- Se introducen los escenarios de participación en este sector, en la línea de lo que denominamos Amicus curiae digital. Se introduce para ello la experiencia desarrollada en el Tribunal Constitucional, que ha permitido un mayor conocimiento de este domino de eGov.

- Se ha expuesto las posibilidades de las tecnologías centradas en el ciudadano y el uso del análisis del conocimiento, ontologías semánticas y motores de búsqueda que faciliten el acceso a la Justicia.

- Se ha analizado la gobernanza de los procesos de e-Educación y el uso de herramientas tecnológicas para la gestión educativa. Se

presenta un modelo de acreditación electrónica de diplomas y de evaluación de sistemas de este tipo.

- El interés de este tipo de sistemas se ha constatado mediante el desarrollo de una solución distribuida para la emisión de títulos certificados en el ámbito universitario.

- Se ha estudiado la participación y la realimentación recogida de las valoraciones de los usuarios de este tipo de sistemas de e-Educación, que da una visión relativamente positiva de la gestión del cambio.

- Se ha analizado la e-Educación entendida como el uso de tecnologías de la información al servicio de la docencia. En este plano se ha congeniado aspectos puramente tecnológicos con otros de tipo pedagógico.

- Se ha presentado el diseño y la construcción de un laboratorio en red de ciberseguridad para no-ingenieros, que ha mostrado el interés científico y académica por este tipo de sistemas.

- Se introduce en este tema de e-Educación una serie de extensiones al modelo de laboratorio planteado. Primero, para su aplicación a cualquier rama de conocimiento; segundo, su ampliación didáctica; tercero, introducir estrategias marcadamente constructivista.

Fruto de estas investigaciones, basadas en varios sistemas desarrollados, puestos en marcha y desplegados en su contexto, se ha podido concluir en la obtención una arquitectura distribuida que dé respuesta al panorama de eGoverment y se fundamenta en los trabajos realizados en esta tesis.

Las soluciones tecnológicas de gobierno electrónico de cualquier dominio se vienen desarrollando en general bajo criterios propios de cada organismo. Se ponen en marcha a menudo sistemas monolíticos, poco o nada interoperables, cuya obsolescencia deriva en prematuro para un uso eficiente de los recursos públicos.

La arquitectura que se concluye en esta tesis plantea la necesidad de un estándar de eGovernment que sirva de capa de servicios, que permita arbitrar el intercambio de información, extendiendo un protocolo necesario para la escalabilidad y operatividad real de las arquitecturas públicas. De tal manera las agencias gubernamentales pueden desarrollar sólo parte de la solución de forma estándar y dejar otra parte de la plataforma para la iniciativa privada (empresas y ciudadanos), habilitando la co-creación y la participación ciudadana. En otro caso, puede desarrollar las dos plataformas cumpliendo con este requisito, facilitando la posterior escalabilidad con posibles plataformas privadas.

En definitiva, se trata de un esquema que se induce y congenia a partir de varias de las ya presentadas parcialmente a lo largo de esta tesis, como la Figura 11, 31 y 37, entre otros esquemas representados, junto a las lecciones aprendidas y resultados obtenidos de los dominios críticos de democracia, seguridad, justicia y educación.

Esta conclusión definitiva a la tesis ha sido planteada ante el comité ejecutivo de IEEE eGovernment que ha mostrado su interés en la iniciativa como trabajo futuro para la estandarización de sistemas distribuidos de gobierno electrónico.

Jesús Salvador Cano Carrillo -

REFERENCIAS

Del Capítulo 1

[1] Anderson, T., & Shattuck, J. (2012). Design-based research a decade of progress in education research?. Educational researcher, 41(1), 16-25.

[2] Collins, A., Joseph, D., & Bielaczyc, K. (2004). Design research: Theoretical and methodological issues. The Journal of the learning sciences, 13(1), 15-42.

[3] Hevner, A.R., March, S.T., and Park, J. "Design Research in Information Systems Research", Mis Quarterly (28:1) 2004, pp 75-105

[4] Van Aken, J. E., & Romme, A. G. L. (2012). A design science approach to evidence-based management. *The Oxford handbook of evidence-based management*, 43-61.

Del Capítulo 2

[5] George Coulouris, Jean Dollimore, Tim Kindberg y Gordon Blair, "Distributed Systems, concepts and design". ISBN 0-13-214301-1. 5ª Edición. Pearson. 2011.

[6] Jack Dongarra, Ian Forter, Geoffredy Fox, William Gropp, Ken Kennedy, Linda Torczon y Andy White, "Sourcebook of parallel computing". ISBN: 1-55860-871-0. Elsevier Science. 2003.

[7] Mack, C., "The Multiple Lives of Moore's Law," *Spectrum, IEEE* , vol.52, no.4, pp.31,31, April 2015

[8] Wikipedia, "Transistor count". [Disponible online] http://en.wikipedia.org/wiki/Transistor_count [Accedido: 2015]

[9] Kai Hwang, Jack Dongarra, Geoffrey C. Fox, "Distributed and Cloud Computing: From Parallel Processing to the Internet of Things" ISBN: 01-23858-80-1. Elsevier Editorial. 2011.

[10] Mohammadfazel Anjomshoa, Mazleena Salleh and Maryam Pouryazdanpanah Kermani, "A Taxonomy and Survey of Distributed Computing Systems" [Online disponible] http://scialert.net/fulltext/?doi=jas.2015.46.57&org=11 [Accedido 2015]

[11] W3C. "Web Architecture". [Disponible online] http://www.w3.org/TR/2004/REC-webarch-20041215/[Accedido: 2015]

[12] Chandra Misra, D. (2006) "Defining e-government: a citizen-centric criteria-based approach". 10th National Conference on e-Governance, 2006, Bhopal, Madhya Pradesh, India [Disponible online] unpan1.un.org/intradoc/groups/public/documents /UNPAN/UNPAN025373.pdf [Accedido: 2015]

[13] Comisión Europea (2003) "eGovernment". Communication of 26 September 2003 from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "The Role of

eGovernment for Europe's future" [Disponible online] europa.eu/legislation_summaries/information_society/strategies/l24226b_en.htm [Accedido: 2015]

[14] Almarabeh T., AbuAli A. (2010) "A General Framework for E-Government: Definition, Maturity Challenges, Opportunities, and Success " European Journal of Scientific Research. ISSN 1450-216X Vol.39 No.1, pp.29-42

[15] Abdoullah Fath-Allah, Laila Cheikhi, Rafa E. Al-Qutaish, Ali Idri (2014) "A Comparative Analysis of E-Government Quality Models". World Academy of Science, Engineering and Technology. International Journal of Social, Education, Economics and Management Engineering Vol:8, No:11, 2014

[16] Jimenez, Carlos E.; Solanas, Agusti; Falcone, Francisco, "E-Government Interoperability: Linking Open and Smart Government," *Computer*, vol.47, no.10, pp.22, 24, Oct. 2014 doi: 10.1109/MC.2014.281

[17] Iván Arce, Kathleen Clark-Fisher, Neil Daswani, Jim DelGrosso, Danny Dhillon, Christoph Kern, Tadayoshi Kohno, Carl Landwehr, Gary McGraw, Brook Schoenfield,

Margo Seltzer, Diomidis Spinellis, Izar Tarandach, and Jacob West (2014) "Avoid the top 10 software security design flaws" [Disponible online] cybersecurity.ieee.org/images/files/images/pdf/CybersecurityInitiative-online.pdf [Accedido: 2015]

[18] The White House (2015) "SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity

Efforts". Office of the Press Secretary. Comunicado de prensa del Presidente de US. [Disponible online] www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat [Accedido:2015]

[19] U.S. Department of State. "Assessment / Examination Process" [Sitio online] http://www.state.gov/m/ds/career/c54778.htm [Accedido: 2015]

[20] Carpio Camara, M.; León, A.; Cano Carrillo, J.; Jiménez, C.E. (2015) "Regulación y ciberseguridad: contribuciones al modelo de gobernanza". Capítulo del libro "La Gobernanza de Internet en España" editado por el IGF Spain. [Disponible online] igfspain.com/doc/archivos/Gobernanza_Internet_Spain_2015.pdf [Accedido: 2015]

[21] Comisión Europea (2015) "Stronger data protection rules for Europe". [Disponible online] europa.eu/rapid/press-release_MEMO-15-5170_en.htm [Accedido: 2015]

[22] Comisión Europea (2002) "Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001". [Disponible online] www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf [Accedido: 2015].

[23] Ministerio del Interior. Secretaría de Estado. (2014) "Informe de cibercriminalidad". [Disponible online]

www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf [Accedido: 2015]

[24] Iguer, H.; Medromi, H.; Sayouti, A.; Elhasnaoui, S.; Faris, S., "The Impact of Cyber Security Issues on Businesses and Governments: A Framework for Implementing a Cyber Security Plan," *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on* , vol., no., pp.316,321, 27-29 Aug. 2014

Del Capítulo 3

[25] ITU-T, 2014. "The World in 2014: ICT facts and figures". [Disponible online] www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf [Accedido: 2015]

[26] ITU-T, 2014. Portal estadístico del ITU & The key 2005-2014 ICT data & Time Series by Countries [Disponible online] www.itu.int/en/ITU-D/Statistics/ Pages/stat/default.aspx & 2014/ITU_Key_2005-2014_ICT_data.xls & 2014/Individuals_Internet_2000-2013.xls [Accedido: 2015]

[27] Internet live stats. Portal estadístico. [Disponible online] www.internetlivestats.com/internet-users/spain [Accedido: 2015]

[28] Documentación Foro de la Gobernanza de Internet de España. [Disponible online] igfspain.com/doc/archivos/Documentaci%C3%B3n_Jornadas_Madrid_2015_05_28_29.pdf [Accedido: 2015]

[29] Statista Portal. "Number of social network users worldwide from 2010 to 2018 (in billions)". [Disponible online] www.statista.com/statistics/278414/number-of-worldwide-social-network-users [Accedido: 2015]

[30] Centro de Investigaciones Sociológicas (CIS). "Barómetros" [Disponible online] www.cis.es/cis/opencm/ES/1_encuestas/TiposEncuestas/barometros.jsp [Accedido: 2015]

[31] Mostashari, A.; Arnold, F.; Maurer, M.; Wade, J., "Citizens as sensors: The cognitive city paradigm," *Emerging Technologies for a Smarter World (CEWIT), 2011 8th International Conference & Expo on* , vol., no., pp.1,5, 2-3 Nov. 2011

[32] McPhee, C.; Westerlund, M.; Leminen, S., "Editorial: Living Labs" Technology Innovation Management Review. Sep. 2012 [Disponible online] timreview.ca/sites/default/files/article_PDF/Editorial_TIMReview_September2012.pdf [Accedido: 2015]

[33] UNPAN, United Nations Public Administration Network. (2014). "UN E-Government Survey 2014". [Disponible online] unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf [Accedido: 2014]

[34] Sun Dizhong, "Political Functions of E-Democracy," *Management and Service Science (MASS), 2010 International Conference on*, vol., no., pp.1, 4, 24-26 Aug. 2010

[35] Peristeras, V.;Mentzas, G.; Tarabanis,K. A.; Abecker, A. "Transforming E-Government and E-Participation through IT", IEEE Intelligent Systems, vol. 24, no. 5, 2009, pp. 14-19

[36] Barber, B.J. WStrong Democracy: Participatory Politics for a New Age". Berkeley, CA: University of California Press, 1984.

[37] A. V. Anttiroiko. 2003. "Building strong E-democracy - The role of technology in developing democracy for the information age," Communications of the ACM, vol. 46, pp. 121-128

[38] Gross, T. 2000. "Technological support for e-democracy: history and perspectives," Database and Expert Systems Applications, 2000. Proceedings. 11th International Workshop, pp.391-395

[39] Kalampokis, E.; Tambouris, E.; Tarabanis, K. 2008. "A Domain Model for eParticipation," Internet and Web Applications and Services, 2008. ICIW '08. Third International Conference, pp.25-30, 8-13

[40] Carter, L.; Belanger, F. 2004. "Citizen Adoption of electronic government initiatives" System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference, pp. 10 pp., 5-8

[41] Macintosh, A. 2004. "Characterizing e-participation in policy-making" *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference*, pp.10 pp.5-8

[42] Macintosh A.; Whyte, A. 2006. "Evaluating how eParticipation changes local democracy" in Proc. eGovernment Workshop 2006: eGov06, Edinburg.

[43] Kubicek, H. 2007. "Electronic Democracy and Deliberative Consultation on Urban Projects. Putting E-Democracy into Context". Report for the Congress of

Local and Regional Authorities. [Disponible online] www.ifib.de/publikationsdateien/Creative_final.pdf [Accedido: 2015]

[44] Freeman, J. & Quirke, S. (2013). "Understanding E-Democracy: Government-Led Initiatives for Democratic Reform". Journal of eDemocracy and Open Government. JeDEM 5(2): 141-154.

[45] Rudan, S. M.; Rudan, S. (2014). "Democracy framework politics & leadership in online communities," eDemocracy & eGovernment (ICEDEG), 2014 First International Conference on, vol., no., pp.67,72, 24-25

[46] Sousa, A.J.A.; Gouveia, L.M.B. 2012. "A proposal for digital mediation for direct public participation during electoral periods," Information Systems and Technologies (CISTI), 2012 7th Iberian Conference, pp.1-5, 20-23

[47] Kindberg, T.; Chalmers, M.; Paulos, E. 2007. "Guest Editors' Introduction: Urban Computing" Pervasive Computing, IEEE, vol.6, no.3, pp.18-20

[48] Carenini M.; Whyte, A.; Bertorello, L.; Vanocchi M. 2007. "Improving Communication in E-democracy Using Natural Language Processing" Intelligent Systems, IEEE, vol.22, no.1, pp.20-27

[49] Sheth, A. (2009) "Citizen Sensing, Social Signals, and Enriching Human Experience," Internet Computing, IEEE, vol.13, no.4, pp.87-92

[50] Gascó, M. 2012. "Approaching E-Government Interoperability". *Soc. Sci. Comput. Rev.* 30, 1 (February 2012), 3-6. DOI=10.1177/0894439310392181

[51] Jimenez, C.E.; Criado, J. I.; Gasco, M. 2011. "Technological e-Government Interoperability. An Analysis of Ibero American Countries," Latin America Transactions, IEEE, vol.9, no.7, pp.1112-1117

[52] Smart Cities Council. "Smart Cities Readiness Guide", 2013 [Disponible online] smartcitiescouncil.com/system/files/premium_resources/SmartCitiesCouncil-READINESSGUIDEV1.5-7.17.14.pdf [Accedido: 2015]

[53] Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanović, N., & Meijers, E., (2007) "Smart Cities: Ranking of European Medium-Sized Cities", Vienna, Austria: Centre of Regional Science (SRF), Vienna University of Technology. [Disponible online] http://www.smartcities.eu/download/smart_cities_final_report.pdf [Accedido: 2015]

[54] EU Parliament, Directorate-general for Internal Polices. (2014). "Mapping Smart Cities in EU". [Disponible online] http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf [Accedido: 2015]

[55] Jiménez, Carlos E. (2011) "Gobierno abierto: hacia un gobierno como plataforma". Jornada sobre gobierno abierto de la Comunidad Foral de Navarra. [Disponible Online] http://sites.ieee.org/spain-tmc/files/2011/11/Es_OpenGovernment_Jimenez.pdf [Accedido: 2015]

[56] European Commission. "Strengthening the EU's telecommunications backbone"

[Sitio online] ec.europa.eu/isa/actions/02-interoperability-architecture/2-4action_en.htm [Accedido: 2015]

[57] "La iniciativa legislativa popular". Editado por: Centro de Estudios Políticos y Constitucionales (Ministerio de la Presidencia). Miguel A. Fernández Ferrero. 2001. ISBN: 84-259-1157-5.

[58] European Parliament (2011) "Regulation (EU) No 211/2011 of the European Parliament and of the council of 16 February 2011 on the citizens' initiative". [Disponible online] eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= OJ:L:2011:065:0001:0022:EN:PDF [Accedido: 2015]

[59] Parlamento de España (1984) "Ley Orgánica 3/1984 de 26 Marzo sobre Iniciativa Legislativa Popular, modificada por la Ley Orgánica 4/2006 de 26 Mayo". [Sitio online] http://www.ine.es/en/oficina_censo/iniciativas_en.htm [Accedido: 2015]

[60] European Commission (2006) "Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures". Marzo 2006. [Disponible online]

eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0120:FIN:EN:PDF [Accedido: 2015]

[61] European Parliament (1999) "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures". [Disponible online] europa.eu/legislation_summaries /information_society/other_policies/l24118_en.htm [Accedido: 2015]

[62] "Royal Decree 3/2010, of January 8th, which regulates the National Security Framework within the scope of eGovernment". Oficial State Gazette. Spanish Government. [Disponible online] http://www.csi.map.es/csi/pdf /ENS_SECURITY_ENGLISH_final.pdf [Accedido: 2015]

[63] "Royal Decree 4/2010, of January 8th, which regulates the National Interoperability Framework within the e-government scope". [Disponible online]

www.csi.map.es/csi/pdf/ENI_INTEROPERABILITY_ENGLISH_final.pdf

[Accedido: 2015]

[64] "Royal Decree 1553/2005 of 23 December which regulates the issuing of National Identification Cards and electronic signature certificates". Ministerio del Interior. Gobierno de España. Boletín Oficial del Estado nº 307 de 2005.

http://www.boe.es/boe/dias/2005/12/24/pdfs/A42090-42093.pdf

[65] European Communities (2007) "Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications: NATIONAL PROFILE GERMANY". April 2007. [Disponible online]

http://ec.europa.eu/idabc/servlets/Doc4a9a.pdf?id=29077 [Accedido: 2015]

[66] European Commission (2010) "The European eGovernment Action Plan 2011-2015. Harnessing ICT to promote smart, sustainable & innovative Government". December 2010. [Disponible online]

http://ec.europa.eu/information_society/activities/egovernment/action_plan_2011_2015/docs/action_plan_en_act_part1_v2.pdf

[Accedido: 2015]

[67] Junta Electoral Central. [Sitio online] http://www.juntaelectoralcentral.es [Consulta web] http://goo.gl/7T3RJy [Accedido: 2015]

[68] Estándar RFC 3280 sobre certificados X.509. http://www.ietf.org/rfc/rfc3280.txt

[69] Estándar RFC 3161 sobre sellado de tiempo. http://www.ietf.org/rfc/rfc3161.txt

[70] "European Standard XML Advanced Electronic Signatures (XAdES):ETSI TS 101 903". ETSI. http://uri.etsi.org/01903/v1.4.1

[71] Matt Bishop and David Wagner. 2007. Risks of e-voting. *Commun. ACM* 50, 11 (November 2007), 120-120.

[72] Paul, N.; Tanenbaum, A.S., "The Design of a Trustworthy Voting System," *Computer Security Applications Conference, 2009. ACSAC '09. Annual* , vol., no., pp.507,517, 7-11 Dec. 2009

[73] IEEE Tecnology Navigator. Topics about electronic voting. http://technav.ieee.org/tag/5787/electronic-voting

[74] "IEEE Standards Working Group P1622 on Voting Systems Electronic Data Interchange Current Project Status". http://www.nist.gov/itl/vote/ieee-swg-p1622.cfm

[75] Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, Richard A. Kemmerer, William Robertson, Fredrik Valeur, Giovanni Vigna, "An Experience in Testing the Security of Real-World Electronic Voting Systems", *IEEE Transactions*

on Software Engineering, vol.36, no. 4, pp. 453-473, July/August 2010, doi:10.1109/TSE.2009.53

[76] Publico Noticias (2012). "590.000 firmas para declarar los toros Bien Cultural en Catalunya" [Disponible online] www.publico.es/espana/590-000-firmas-declarar-toros.html [Accedido: 2015]

[77] Cotino Hueso, L. (2012). "Democracia electrónica y libertades en la red". Universidad de Valladolid. [Disponible online] www.documentostics.com/component/option,com_docman/task,doc_view/gid,1531 [Accedido: 2015]

Del Capítulo 4

[93] Talbot, E.B.; Frincke, D.; Bishop, M., (2010) "Demythifying Cybersecurity," Security & Privacy, IEEE , vol.8, no.3, pp.56,59, May-June 2010

[94] Landau, S.; Stytz, M.R., "Overview of cyber security: a crisis of prioritization," *Security & Privacy, IEEE* , vol.3, no.3, pp.9,11, May-June 2005 doi: 10.1109/MSP.2005.76

[95] United Nations. (2010) "E-Government Survey 2010: Leveraging e-government at a time of financial and economic crisis". [Disponible online] http://www2.unpan.org/egovkb/documents/2010/E_Gov_2010_Complete.pdf] [Accedido: 2015]

[96] Sukaina Al-Nasrawi, Saleem Zoughbi (2014) "Information Society, Digital Divide, and E-Governance in Developing Countries". In M. Khosrow-Pour (Ed.),

Encyclopedia of Information Science and Technology, Third Edition (pp. 6525-6533). IGI Globa. September 1, 2014

[97] Isaak, J., "The role of government in IT standards," Computer , vol.31, no.12, pp.129, 132,, Dec 1998. doi: 10.1109/2.735853

[98] UN Report. (2012) "The Post-2015 Agenda". [Disponible online] http://www.undp.org/content/dam/undp/library/Poverty Reduction/Realizing the future we want.pdf [Accedido: 2015]

[99] UN (2013) "Report of the UN System Task Team on the Post-2015 Development Agenda". [Disponible online] http://www.un.org/en/development/desa/policy/untaskteam_undf/report.shtml [Accedido 2015]

[100] Hatonen, J.; Eriksson, T. (2009). "30+ years of research and practice of outsourcing–Exploring the past and anticipating the future". Journal of International Management, 15(2), 142-155.

[101] Jens Dibbern, Tim Goles, Rudy Hirschheim, and Bandula Jayatilaka. 2004. Information systems outsourcing: a survey and analysis of the literature. SIGMIS Database 35, 4 (November 2004), 6-102.

[102] Hanlie Smuts, Alta van der Merwe, Paula Kotzé, and Marianne Loock. 2010. Critical success factors for information systems outsourcing management: a software development lifecycle view. In Proceedings of the 2010 Annual Research

Conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT '10). ACM, New York, NY, USA, 304-313.

[103] Elisabeth J. Umble, Ronald R Haft, M.Michael Umble (2003) "Enterprise resource planning: Implementation procedures and critical success factors", European Journal of Operational Research, Volume 146, Issue 2, 16 April 2003, Pages 241-257, ISSN 0377-2217, http://dx.doi.org/10.1016/S0377-2217(02)00547-7.

[104] Gartner (2015) "Highlights Top 10 Strategic Technology Trends for Government" [Disponible online] http://www.gartner.com/newsroom/id/3069117 [Accedido 2015]

[105] Tambouris, E.; Loutas, N.; Peristeras, V.; Tarabanis, K.; , "The role of interoperability in eGovernment applications: An investigation of obstacles and implementation decisions," Digital Information Management, 2008. ICDIM 2008. Third International Conference on , vol., no., pp.381-386, 13-16 Nov. 2008

[106] Carlos E. Jiménez, Francisco Falcone, Agusti Solanas, Héctor Puyosa, Saleem Zoughbi, Federico González (2014) "Smart Government: Opportunities and Challenges in Smart Cities Development", Handbook of Research on Democratic Strategies and Citizen-Centered E-Government Services, Chapter 1, pages 1-19

[107] Cano, J.; Hernandez, R., "SCEPYLT: An Information System for Fighting Terrorism," Software, IEEE , vol.30, no.3, pp.73,79, May-June 2013

[108] European Police Office. "Europol Review. General Report on Europol Activities". 2011. [Online:

https://www.europol.europa.eu/sites/default/files/publications/europolreview-en.pdf]. [Accesed: 2015]

[109] Vetterli, Christophe; Brenner, Walter; Uebernickel, Falk; Petrie, Charles, "From Palaces to Yurts: Why Requirements Engineering Needs Design Thinking," Internet Computing, IEEE , vol.17, no.2, pp.91,94, March-April 2013

[110] Wimmer, M.A.; Traunmuller, R.; , "Perspectives e-Government 2020: Results and Conclusions from the EC Roadmap 2020 Project," Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on , vol., no., pp.1-4, 7-11 April 2008

[111] Ding, Li; Peristeras, Vassilios; Hausenblas, M., "Linked Open Government Data [Guest editors' introduction]," Intelligent Systems, IEEE , vol.27, no.3, pp.11,15, May-June 2012

[112] Camarinha-Matos, L.M.; Afsarmanesh, H.; "Collaborative networks: a new scientific discipline," Journal of Intelligent Manufacturing. Springer. October 2005, Volume 16, Issue 4-5, pp 439-452

[113] King, R.S., "How 5 technologies fared after 9/11," Spectrum, IEEE , vol.48, no.9, pp.13,13, September 2011

[114] Garside, A. "The political genesis and legal impact of proposals for the SIS II: what cost for data protection and security in the EU?". Sussex Migration Working Paper no. 30. University of Sussex. March 2006. www.sussex.ac.uk/migration/documents/mwp30.pdf

[115] Secretariat of Eurodac Supervision Coordination Group. "Coordinated Supervision of Eurodac Activity Report 2008-2009". March 2010. [Disponible online] http://www.edps.europa.eu/EDPSWEB/edps/Supervision/Eurodac [Accedido: 2015]

[116] New York Times, 2004. [Disponible online] http://www.nytimes.com/2004/03/12/world/bombings-in-madrid-the-attack-10-bombs-shatter-trains-in-madrid-killing-192.html. [Accedido: 2015].

[117] European Union Council. "Directive 93/15/EEC about Approval of explosives intended for civilian use" 1993. [Online] http://europa.eu/legislation_summaries/consumers/consumer_safety/l11024_en.htm. [Accedido: 2015].

[118] Casale, D. "EU Institutional and Legal Counter-terrorism Framework". Defence Against Terrorism Review. Vol. 1, No. 1, 49-78. ISSN: 1307-9190. Spring 2008.

[119] "After Madrid: the EU's response to terrorism". HOUSE OF LORDS.European Union Committee.5th Report of session 2004-05.Mar 2005. http://www.statewatch.org/news/2005/mar/after-Madrid-HoL.pdf

[120] European Federation of Explosives Engineers. "The EU directives committee: enhancing the Security of explosives". EFEE Newsletter March 2009. [Online] http://efee.eu/Newsletter/EFEE Newsletter 2009 March.pdf [Accedido: 2015].

[121] ESA. "Metodología de Agencia Espacial Europea". [Disponible online] http://www.esa.int/TEC/Software_engineering_and_standardisation [Accedido 2015]

[122] "Council conclusions on systems and mechanisms for the enhancement of security of explosives". Council of the European Union. 2010. [Disponible online] www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114017.pdf [Accedido: 2015]

[123] Papazoglou, M.P. "Distributed database architectures". IEEE International Conference on Databases, Parallel Architectures and Their Applications, PARBASE-90, pp.549, ISBN**:** 0-8186-2035-8. Mar 1990

[124] Xizhong Song; Renzhi Zhang. "Research on constructing distributed large database based on J2EE". IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp.704-707.May 2011

[125] Rodriguez, L.; Xiaoou Li. "A dynamic vertical partitioning approach for distributed database system". IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp.1853-1858. Oct 2011

[126] Thuraisingham, B.; Rubinovitz, H.; Foti, D.; Abreu, A. "Design and implementation of a distributed database" IEEE COMPSAC 93 Proceedings, Seventeenth Annual International Computer Software and Applications Conference, 1993, pp.152-158, Nov 1993.

[127] Karimi, O.B.; Yousefi, S.; Fathy, M.; Mazoochi, M. "Availability measurement in peer to peer network management systems". IEEE *Third International Conference onDigital Information Management, 2008.ICDIM 2008*, pp.745-750. Nov 2008.

[128] Liu Tian-shi; Li Jiao; GaoRong-fang; Ma Gang. "Overview of P2P Distributed Database System". IEEE International Conference on Web Information Systems and Mining (WISM), 2010, vol.2, pp.192-197. Oct 2010

[129] Unión Europea. Agenda de acción digital. [Disponible online] http://ec.europa.eu/information_society/digital-agenda/index_en.htm [Accedido 2015]

Del Capítulo 5

[78] POZEN, David. Judicial Elections as Popular Constitutionalism. *Columbia Law Review*, 2010, vol. 110, p. 2047-2134.

[79] Aragón Reyes, Manuel. "Dos problemas falsos y uno verdadero: neoconstitucionalismo, garantismo y aplicación judicial de la constitución". Cuestiones Constitucionales. Volume 2013, Issue 29, July–December 2013, Pages 3–25

[80] CEPEJ. "European judicial systems – Edition 2014 (2012 data): efficiency and quality of justice". [Disponible online] http://www.coe.int/t/dghl/cooperation/cepej/evaluation/2014/Rapport_2014_en.pdf [Accedido: 2015]

[81] Singh, B.; Kannojia, S.P., "A Review on Software Quality Models," *Communication Systems and Network Technologies (CSNT), 2013 International Conference on* , vol., no., pp.801,806, 6-8 April 2013
doi: 10.1109/CSNT.2013.171

[82] UC3 (2013) *I Jornada sobre calidad del producto software*. 21 y 22 de noviembre 2013. Universidad Carlos III. [Sitio web] http://calidaddelproductosoftware.com/2013 [Accedido: 2015]

[83] Commission of EU (2008). "Towards a European e-Justice Strategy". Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee. Brussels.

[84] Reiling, D. (2011). "E-justice: experiences with court IT in Europe"*.* En*: Buenas prácticas para la implementación de soluciones tecnológicas en la Administración de Justicia*. Compiladors Caballero, J.A., De Grácia, C.G. y Hammergren, L. México.

[85] Castells, M. (1996). *The Rise of the Network Society*. Cambridge: Blackwell Publishers, Inc.

[86] Yáñez, R. (2008). *L'Oficina Judicial a Catalunya. Mitjà real d'una Justícia eficaç pel ciutadà del segle XXI.* Barcelona: Centro de Estudios Jurídicos y Formación Especializada.

[87] Cerrillo, A. & Fabra, P. (2009). *E-Justice: Using Information Communication Technologies in the Court System*. Hershey, PA: IGI Global.

[88] Jiménez, C. E. (2013). Impact of the Law Regulating the Use of ICT in the Administration of Justice. *Centre of Legal Studies and Specialised Formation (CEJFE). Barcelona*.

[89] Páez Mañá, Jorge. "Bases de datos jurídicas". Editado por CINDOC, CSIC, Centro de Información y Documentación Científica (Madrid). 1994.

[90] ECMA International. *ECMA-376, Office Open XML File Formats — Fundamentals and Markup Language Reference*, 4th edition. Dec 2012.

[91] Cano, J.; Jimenez, C.E.; Hernandez, R.; Ros, S., "New tools for e-justice: legal research available to any citizen," *eDemocracy & eGovernment (ICEDEG), 2015 Second International Conference on* , vol., no., pp.108,111, 8-10 April 2015 doi: 10.1109/ICEDEG.2015.7114455

[92] IGI Global [Disponible online] http://www.igi-global.com/publish/call-for-papers/call-details/1641 [Accedido: 2015]

Del Capitulo 6

[130] UNESCO, «Incheon Declaration. Education 2030 towards inclusive and equitable quality education and lifelong learning for all,» [Disponible online] www.uis.unesco.org/Education/Documents/education_2030_incheon_declaration_en.pdf. [Accedido: 2015].

[131] Jimenez, C., Falcone, F., Solanas, A., Puyosa, H., Zoughbi, S., & Gonzalez, F. (2014). Smart Government: Opportunities and Chanllenges in the Development of Smart Cities. En Handbook of Research on Democratic Strategies and Citizen-Centered E-Government Services (pág. 389). IGI GLobal.

[132] Jimenez, C., Solanas, A., & Falcone, F. (2014). E-Government Interoperability: Linking Open and Smart Government. Computer , 47 (10), 22-24.

[133] Kerby, R. (2014) *Trends on the 2014 UN e-Government Survey United Nations*. Department of Economic and Social Affairs. Muscat, Oman April 21 2014. [Disponible online]

www.ita.gov.om/hmaward/Trends-in-2014-e-Gov-Survey-by-Richard-Kerby.pdf [Accedido: 2015]

[134] Terán, L. (2014). SmartParticipation. A fuzzy-based recommender system for political community-building ISBN-13: 978-3319065502 . Ed. Springer

[135] Cano, J., Hernández, R., & Ros, S. (2014). Distributed Framework for Electronic Democracy in Smart Cities. Computer , 47 (10), 65-71.

[136] Nichols, D., & Cunningham, S. (2009). The use of paper in everyday student life. ACM (Ed.), In Proceedings of the 10th International Conference NZ Chapter of the ACM's Special Interest Group on Human-Computer Interaction , July, págs. 65-68. Auckland, New Zeland.

[137] UN (2014); "United Nations Public Administration Estudies" [Disponible online] http://unpan3.un.org/egovkb/Data-Center [Accedido: 2015]

[138] UN (2013); "Human Development Reports". [Disponible online] http://hdr.undp.org/en/content/education-index [Accedido: 2015]

[139] Ministerio de Educación, «Sede electrónica del Ministerio de Educación del Gobierno de España.,» 2015. [Sitio web].

[140] ETSI TS 102 778-4 (2009). Electronic signatures and infraestructures (ESI)-PDF advanced electronic signature profiles. [Online available] www.etsi.org [Accedido: 2015].

[141] ITU-T (2012). "Information and communication technologies, environment and climate change". [Disponible online] www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.73-2012-PDF-E.pdf [Accedido: 2015]

[142] McGettrick A.; Cassel, L.N.; Dark, M.; Hawthorne, E.K. and Impagliazzo, J. (2014). Toward curricular guidelines for cybersecurity. In Proceedings of the 45th ACM technical symposium on Computer science education (SIGCSE '14). ACM, New York

[143] Burley, D. & Bishop, M. (2011) Summit on Education in Secure Software Final Report.(GW-CSPRI-2011-7) (CSE-2011-15) June 30, 2011. [Disponible online] http://nob.cs.ucdavis.edu/bishop/notes/2011-sess/2011-sess.pdf [Accedido: 2015]

[144] Schneider, F. B. (2013) *Cybersecurity Education in Universities*. Security & Privacy, IEEE. Volume: 11, Issue: 4. Page(s): 3 – 4

[145] Atman, C. J., Adams, R. S., Cardella, M. E., Turns, J., Mosborg, S., & Saleem, J. J.(2007). Engineering Design Processes: A Comparison of Students and Expert Practitioners. Journal of Engineering Education, 96(4), 359-379.

[146] ACM/IEEE CS, 2013. *The Joint Task Force on Computing Curricula, Computer Science Curricula 2013, Ironman Draft (version 1.0)*. [Online available] http://ai.stanford.edu/users/sahami/CS2013/ironman-draft/cs2013-ironman-v1.0.pdf [Accedido: 2015]

[147] IEEE News (2014). *Everyone's a Gamer – IEEE Experts Predict Gaming Will Be Integrated Into More than 85 Percent of Daily Tasks by 2020*. [Online available] www.ieee.org/about/news/2014/25_feb_2014.html [Accedido: 2015]

[148] Zyda, M. (2005). *From visual simulation to virtual reality to games*. *Computer*, vol.38, no.9, pp.25, 32

[149] Abt, C. (1970)*Serious Games*. New York: Viking Press. [Disponible Online] books.google.es/books?isbn=0819161489 [Accedido: 2015]

[150] Huizinga, J., (1955). *Homo Ludens: A Study of the Play-Element in Culture*. The Beacon Press, Boston, MA.

[151] Pastor, V.,Díaz, G., Castro, M. (2010) State-of-the-art simulation systems for information security education, training and awareness. Education Engineering (EDUCON), IEEE. Page(s): 1907 - 1916

[152] Irvine, C.E., Thompson, M.F. & Allen, K.(2005). *CyberCIEGE: gaming for information assurance*. Security & Privacy, IEEE. Volume: 3 , Issue: 3 Digital Object Identifier: 10.1109/MSP.2005.64. Page(s): 61 - 64

[153] Irvine, C.E. & Thompson, M.F. (2010) *Simulation of PKI-Enabled Communication for Identity Management Using CyberCIEGE*. Military Communications Conference, November 1-3 2010, pp.1758-1763.

[154] O'Neil, H.F., Wainess, R. and Baker, E.L. (2005). *Classification of learning outcomes: evidence from the computer games literature*. The Curriculum Journal, Vol. 16, No. 4, pp. 455 – 474

[155] Wouters, P., Spek, E. van der, & Oostendorp, H. van (2009). Current practices in serious game research: A review from a learning outcomes perspective. In T. Connolly, M. Stansfield & L. Boyle (Eds.), Games-Based Learning Advancements for Multi-Sensory Human Computer Interfaces: Techniques and Effective Practices: Information Science Reference.

[156] CEU (2015), "El proyecto laboratorio de ciberseguridad premiado por su innovación docente". Noticias. [Disponible online] http://www.uspceu.com/prensa/noticiacompleta.aspx?q1=2044&q2=not [Accedido: 2015]

[157] Karl D. S.; Michael,K.; Michael, M.G.; Jacob,L. y Anesta, E. (2012) "Social Implications of Technology: Past, Present, and Future" Proceedings of the IEEE 100.13: 1752-1781. [Disponible online] http://works.bepress.com/kmichael/255 [Accedido: 2015]

[158] Theoharidou, M. & Gritzalis, D. (2007). *Common Body of Knowledge for Information Security.Security & Privacy, IEEE*, vol.5, no.2, pp.64-67

[159] Gagné, R. M., Wager, W. W., Golas, K. C., Keller, J. M., & Russell, J. D. (2005). *Principles of instructional design* (5th ed.). Belmont, CA: Wadsworth

[160] Keller, J. M. (2010). *Motivational design for learning and performance: The ARCS model approach*. New York, NY: Springer.

[161] Stukalina, Y. (2009) "Globalization and engineering education preparing students for the 21t century professions" [disponible online] http://www.tsi.lv/sites/default/files/editor/science/Publikacii/Education/2009/10_stukalina.pdf [Accedido: 2015]

[162] Ausubel, D.P. (2010). Psicología educativa: un punto de vista cognoscitivo. Editorial Trillas (reedición)

[163] Bloom, B. S. (1984) Taxonomy of Educational Objectives. Pearson Education (reedición)

[164] Llorente Barroso, C; Muñoz de Luna, A.B.; Viñarás Abad, M. (2013) Implementación del aprendizaje basado en problemas (ABP) y el learning by doing en el Grado en Publicidad y Relaciones Públicas para la adquisición de competencias Historia y Comunicación Social. Vol. 18. Nº Esp. Nov. (2013) 639-650

[165] Hattie, J. (2012). Visible learning for teachers: Maximizing impact on learning. Routledge. ISBN: 9780415690157.

[166] Guskey, T. R. (2007). Closing achievement gaps: revisiting Benjamin S. Bloom's "Learning for Mastery". Journal of Advanced Academics, 19(1), 8-31.

APÉNDICE 1. AUTORIZACIÓN JUNTA ELECTORAL CENTRAL

Junta Electoral Central

JUNTA ELECTORAL CENTRAL
Nº 004519 23.11.2011
SALIDA

TRANSMISIÓN OFICIAL POR FAX

DE EXCMO. SR. PRESIDENTE DE LA JUNTA ELECTORAL CENTRAL
A
COMISIÓN PROMOTORA

Fax – 93 200 82 46

Esta Presidencia, en virtud de lo dispuesto en el último párrafo del artículo 20 de la Ley Orgánica del Régimen Electoral General, ha adoptado la resolución que se transcribe sobre el asunto de referencia:

Expte.400/86 09/03/2011 Nº registro: 849
Autor: Excmo. Sr. Presidente del Congreso de los Diputados.

Objeto: Proposición de Ley de Iniciativa Legislativa Popular para la regulación de la fiesta de los toros como Bien de interés cultural.

Informe de la Oficina del Censo Electoral sobre el sistema de firma electrónico comunicado por la ILP

RESOLUCION.- Remitir los informes de referencia a la Comisión Promotora de la ILP.

Palacio del Congreso de los Diputados, 23 de noviembre de 2011.

JUNTA ELECTORAL CENTRAL * PRESIDENCIA *

P1

23/11 2011 18:00 FAX 914298707 CONGRESO-GAB TELEGRAFICO 002/005

18. NOV. 2011 14:51 OF. CENSO ELECTORAL 915834695 Nº 081 P. 1

OFICINA DEL CENSO ELECTORAL

Iñic

400
86

JUNTA ELECTORAL CENTRAL
Nº 009034 18 11 2011
ENTRADA

Excmo. Sr. Presidente de la
Junta Electoral Central

Madrid, 18 de noviembre de 2011

Adjunto se remite informe sobre el sistema de firma electrónica comunicado por la comisión gestora de la ILP de Declaración de la fiesta de los Toros como bien de interés cultural.

El Director de la Oficina
del Censo Electoral,
P.A. El Subdirector

Fdo.: José Luis Viedma Lozano

REGISTRO GRAL.DEL INE
S.G DEL CENSO ELECTORAL
Salida 072 Nº. 2011072000351 18/11/11
12:35:37

C/ Capitán Haya, 51
28020 Madrid ESPAÑA
TELÉF.:915834807 – FAX: 915834695

P2

23/11 2011 18:00 FAX 914298707 CONGRESO-GAB TELEGRAFICO 003/005
18. NOV. 2011 14:51 OF. CENSO ELECTORAL 915834695 Nº 081 P. 2

Informe sobre el sistema de firma electrónica comunicado por la comisión gestora de la ILP de Declaración de la fiesta de los Toros como bien de Interés cultural.

Madrid, 18 de noviembre de 2011

El Acuerdo de la JEC de 17 de septiembre de 2009 sobre firma digital a efectos de pliegos de recogida de firmas para presentación de iniciativa legislativa popular establece:

Esta Junta considera que el uso de la firma electrónica para la recogida de firmas a efectos de la presentación de una iniciativa legislativa popular debe entenderse válida siempre que se ajuste a lo dispuesto en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, modificada por Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, y, en consecuencia, se acompañe de certificado válidamente proporcionado por la Fábrica Nacional de Moneda y Timbre o por otra entidad autorizada al efecto, todo ello sin perjuicio de que además se guarden las garantías de autenticación de firmas previstas en los artículos 9 y 10 de la Ley Orgánica 3/1984, de 26 de marzo, reguladora de la Iniciativa Legislativa Popular. A tal efecto, la Comisión Promotora deberá comunicar a la Junta Electoral Central el sistema de firma electrónica que pretende utilizar y facilitar a ésta, en el caso de que fuera necesario, el sistema utilizado para la verificación de las firmas electrónicas.

La Comisión Gestora de la ILP de Declaración de la fiesta de los Toros como bien de interés cultural, en cumplimiento del citado Acuerdo comunica que va a utilizar la aplicación OpenILP de la Escuela Técnica Superior de Ingeniería Informática de la UNED, con un sistema de firma electrónica basado en el cliente @Firma del Ministerio de Política Territorial y Administraciones Publicas y que la firma es verificable por la plataforma publica VALIDE del Ministerio de Industria, Turismo y Comercio.

En consecuencia se informa de la validez del sistema de firma propuesto. No obstante lo anterior, la Comisión Gestora deberá facilitar a la Junta Electoral Central el sistema utilizado para la verificación de las firmas electrónicas, si le fuera requerido.

Además, se hacen las siguientes aclaraciones:

- Los datos personales del firmante imprescindibles para la posterior comprobación de su inscripción en el Censo Electoral como mayor de edad son: Nombre, Primer apellido, Segundo apellido, Documento Nacional de Identidad o Pasaporte y fecha de nacimiento.

- El fichero de datos a firmar deberá tener formato XML y deberá incluir los datos personales del firmante y el texto de la proposición de ley.

- Para homogeneizar el tratamiento de certificación de la condición de elector mayor por parte de la oficina del Censo Electoral se recomienda el siguiente formato XML del fichero sin firmar

```
<?xml version="1.0" encoding="UTF-8" ?>
  <oce>
    <ilp>
      <firmante>
          <nomb />
          <ape1 />
          <ape2 />
          <fnac />
          <tipoid />
          <id />
        </firmante>
        <textoilp />
      </ilp>
    </oce>
```

- La estructura y restricciones de contenido del fichero anterior queda definido por el siguiente fichero xsd (XML Schema Definition).

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">
 <xs:element name="oce">
   <xs:complexType>
     <xs:sequence>
       <xs:element name="ilp" type="ilpType" />
     </xs:sequence>
   </xs:complexType>
 </xs:element>
 <xs:complexType name="ilpType">
    <xs:sequence>
      <xs:element name="firmante" type="firmanteType"
        />
      <xs:element name="textoilp" type="xs:string" />
    </xs:sequence>
```

```
 </xs:complexType>
<xs:complexType name="firmanteType">
 <xs:sequence>
    <xs:element name="nomb" type="nombrefirmante"
      />
    <xs:element name="ape1" type="apellidofirmante" />
    <xs:element name="ape2" type="apellidofirmante" />
    <xs:element name="fnac" type="fechan" />
    <xs:element name="tipoid" type="tipoidentificador"
      />
    <xs:element name="id" type="identificador" />
  </xs:sequence>
</xs:complexType>
<xs:simpleType name="tipoidentificador">
  <xs:annotation>
    <xs:documentation>Tipo de documento identificador,
      1.-NIF, 2.-NIE</xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:string">
    <xs:enumeration value="1" />
    <xs:enumeration value="2" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="nombrefirmante">
  <xs:restriction base="xs:string">
    <xs:maxLength value="20" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="apellidofirmante">
   <xs:restriction base="xs:string">
    <xs:maxLength value="25" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="identificador">
  <xs:restriction base="xs:string">
    <xs:maxLength value="9" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="fechan">
  <xs:annotation>
    <xs:documentation>Formato de la fecha de
      nacimiento "AAAAMMDD",
      "20110908"</xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:string">
    <xs:maxLength value="8" />
  </xs:restriction>
 </xs:simpleType>
</xs:schema>
```

APÉNDICE 2. VALORES NORMALIZADOS EGOV/EDUCACIÓN ORDENADOS

**Fuentes basadas en datos de la ONU: Programa sobre Administraciones Públicas [137] & Programa para el Desarrollo (PNUD) sobre educación [138]*

País	Y'_0	X'_0	X'_2	Y_0	Y_1	X_0	X_1	X_2	X_3	X_4	X_5
Australia	1	2	6	2	0,92653552	2	0,91034	0,94117	0,92913	0,9978	0,80405
Nueva Zelanda	2	9	18	7	0,916766667	9	0,86436	0,78431	0,84251	100.000	0,75057
Noruega	3	13	29	1	0,909922222	13	0,83572	0,68627	0,7559	0,938	0,81328
Países Bajos	4	5	1	4	0,893532297	5	0,88966	1,00000	0,92913	0,9224	0,81751
Estados Unidos	5	7	8	5	0,889759207	7	0,87483	0,92156	0,94488	0,939	0,74059
Irlanda	6	22	32	11	0,887066667	22	0,781	0,64705	0,67716	0,9619	0,70391
Alemania	7	21	23	6	0,884371952	21	0,7864	0,70588	0,66929	0,8862	0,80377
Lituania	8	28	32	35	0,876659891	29	0,72709	0,64705	0,7559	0,8557	0,56968
Dinamarca	9	16	52	10	0,872826055	16	0,8162	0,54901	0,66141	0,9132	0,87403
República Checa	10	51	116	28	0,866222222	53	0,60695	0,2549	0,37007	0,8755	0,57532
Corea	11	1	1	15	0,864509636	1	0,94623	1,00000	0,97637	0,9273	0,93503
Eslovenia	12	39	79	25	0,863083331	41	0,65054	0,39215	0,42519	0,9072	0,61925
Reino Unido	13	8	3	14	0,860260145	8	0,86948	0,96078	0,89763	0,8574	0,8534
Estonia	14	15	21	33	0,858533333	15	0,81796	0,7647	0,77165	0,8889	0,79337
Israel	15	17	11	19	0,85426783	17	0,81615	0,86274	0,87401	0,8545	0,71998
Canadá	16	11	13	8	0,8503	11	0,84177	0,82352	0,91338	0,8952	0,71676
Islandia	17	19	63	13	0,846866667	19	0,797	0,49019	0,61417	0,9178	0,85906
Suiza	18	29	86	3	0,844089209	30	0,7267	0,37254	0,50393	0,8562	0,81992
Suecia	19	14	44	12	0,830134011	14	0,8225	0,60784	0,70078	0,8802	0,88656
Polonia	20	40	63	35	0,824699932	42	0,64822	0,49019	0,5433	0,8396	0,56182
Bielorrusia	21	53	87	53	0,819984164	55	0,60529	0,35294	0,32283	0,8861	0,60691
Francia	22	4	3	20	0,815549416	4	0,89384	0,96078	100.000	0,8812	0,80029
Finlandia	23	10	23	24	0,815088889	10	0,84491	0,70588	0,77165	0,9037	0,8594
Letonia	24	30	23	48	0,813187844	31	0,71775	0,70588	0,70078	0,8288	0,62367
Bélgica	25	25	39	21	0,812291688	25	0,75638	0,62745	0,67716	0,8932	0,6988
Japón	26	6	3	17	0,808	6	0,88744	0,96078	0,94488	0,8621	0,85533
Hungría	27	37	71	43	0,804893768	39	0,66374	0,45098	0,55905	0,8668	0,56536
Eslovaquia	28	49	39	37	0,8021	51	0,61478	0,62745	0,48818	0,8265	0,52963
Grecia	29	33	16	29	0,796988551	34	0,71176	0,80392	0,60629	0,8741	0,65487
Ucrania	30	83	72	83	0,795511111	87	0,50316	0,43137	0,26771	0,8616	0,38016

Austria	31	20	39	21	0,794481027	20	0,79124	0,62745	0,74803	0,866	0,75972
España	32	12	18	27	0,794396973	12	0,84098	0,78431	0,94488	0,9152	0,66288
Italia	33	23	18	26	0,789505799	23	0,7593	0,78431	0,74803	0,8552	0,67473
Palau	34	102	122	60	0,786759955	108	0,4415	0,23529	0,16535	0,7999	0,35922
Argentina	35	44	52	49	0,783355597	46	0,63059	0,54901	0,55118	0,8571	0,48347
Federación Rusa	36	26	29	57	0,779955556	27	0,72959	0,68627	0,70866	0,8388	0,6413
Chipre	37	56	102	32	0,776198377	58	0,59576	0,31372	0,47244	0,7828	0,53203
Montenegro	38	43	48	51	0,773555556	45	0,63455	0,58823	0,52755	0,8279	0,54814
Croacia	39	45	92	47	0,770334477	47	0,62817	0,33333	0,46456	0,7928	0,62711
Georgia	40	54	48	79	0,770333333	56	0,60468	0,58823	0,59842	0,7895	0,42613
Singapur	41	3	9	9	0,767777778	3	0,90762	0,90196	0,99212	0,8515	0,87927
Fiji	42	81	79	88	0,766517427	85	0,50437	0,39215	0,3937	0,8322	0,28719
Kazajstán	43	27	21	70	0,762266667	28	0,72827	0,7647	0,74803	0,8619	0,57488
Luxemburgo	44	24	52	21	0,762111044	24	0,75911	0,54901	0,62204	0,783	0,87225
Liechtenstein	45	34	112	18	0,761544444	35	0,69823	0,2745	0,51181	0,8361	0,74682
Bulgaria	46	69	116	58	0,749407205	73	0,54209	0,2549	0,23622	0,796	0,59406
Rumania	47	61	68	54	0,747894287	64	0,56315	0,47058	0,44094	0,81	0,43854
Chile	48	32	6	41	0,745675257	33	0,71216	0,94117	0,81889	0,8236	0,49396
Cuba	49	109	87	44	0,742877778	116	0,39165	0,35294	0,22834	0,8497	0,09687
Barbados	50	57	152	59	0,739777778	59	0,5933	0,09803	0,22047	0,8865	0,67295
Sri Lanka	51	70	32	73	0,737777778	74	0,54176	0,64705	0,65354	0,7376	0,23412
Malta	52	38	68	39	0,732538011	40	0,6518	0,47058	0,40157	0,7855	0,76834
Portugal	53	36	32	41	0,727614636	37	0,68996	0,64705	0,63779	0,8227	0,60943
Granada	54	74	79	79	0,723975689	78	0,52197	0,39215	0,34645	0,8166	0,40289
Arabia Saudita	55	35	50	34	0,723174097	36	0,69001	0,56862	0,77165	0,7461	0,55227
Tonga	56	94	92	100	0,720333333	98	0,47057	0,33333	0,34645	0,8304	0,23482
Mauricio	57	72	57	63	0,718096828	76	0,53375	0,52941	0,47244	0,6882	0,44061
Bahrein	58	18	13	44	0,713966667	18	0,80885	0,82352	0,937	0,784	0,7055
Bahamas	59	88	130	51	0,713954676	92	0,49	0,19607	0,33858	0,7138	0,41758
Samoa	60	105	79	106	0,701508208	111	0,42039	0,39215	0,24409	0,7499	0,26723
Armenia	61	59	57	87	0,701366667	61	0,58969	0,52941	0,61417	0,766	0,3889
Trinidad y Tobago	62	87	102	64	0,700320689	91	0,49317	0,31372	0,3307	0,6945	0,45429
Azerbaiyán	63	64	72	76	0,699777778	68	0,5472	0,43137	0,43307	0,748	0,46049
Jordania	64	75	68	77	0,699725098	79	0,51674	0,47058	0,51968	0,7202	0,31035
Libia	65	114	165	55	0,697888889	121	0,3753	0,05882	0,01574	0,7821	0,32809
Sudáfrica	66	89	92	118	0,695447164	93	0,48688	0,33333	0,38582	0,7282	0,34662
Serbia	67	65	76	77	0,695444444	69	0,54715	0,41176	0,3937	0,7796	0,46814
Mongolia	68	62	29	103	0,693666667	65	0,55808	0,68627	0,61417	0,7887	0,27138
Brunei	69	82	165	30	0,692111111	86	0,50424	0,05882	0,3622	0,7815	0,36898
Belice	70	113	105	54	0,688888889	120	0,37738	0,29411	0,37795	0,6012	0,15295
Katar	71	42	44	31	0,685686747	44	0,63615	0,60784	0,65354	0,6671	0,58786
Irán	72	99	105	75	0,683455556	105	0,45075	0,29411	0,37007	0,6882	0,29401

Antigua y Barbuda	73	58	61	61	0,681141333	60	0,59266	0,5098	0,41732	0,7669	0,59378
Turkmenistán	74	120	147	103	0,678712889	128	0,35109	0,11764	0,08661	0,7478	0,21885
Bolivia	75	97	76	113	0,6735	103	0,45617	0,41176	0,3937	0,7424	0,23242
Emiratos Árabes	76	31	12	40	0,673214954	32	0,71358	0,84313	0,88188	0,6657	0,59319
Malasia	77	50	57	62	0,670544444	52	0,61152	0,52941	0,67716	0,7119	0,44546
Andorra	78	41	72	37	0,670286667	43	0,6426	0,43137	0,43307	0,7277	0,76706
Jamaica	79	103	130	96	0,668355556	109	0,43882	0,19607	0,31496	0,7262	0,27533
Perú	80	68	23	82	0,664337879	72	0,54354	0,70588	0,62992	0,7289	0,2718
Brasil	81	55	23	79	0,661305629	57	0,60082	0,70588	0,59842	0,7372	0,46681
Panamá	82	73	63	65	0,657411111	77	0,52422	0,49019	0,37007	0,7455	0,45713
Kirguistán	83	95	76	125	0,656288889	101	0,46568	0,41176	0,27559	0,7413	0,38013
Bosnia y Herzegovina	84	93	122	86	0,655318208	97	0,47069	0,23529	0,28346	0,7288	0,3998
Costa Rica	85	52	13	68	0,653921604	54	0,60614	0,82352	0,61417	0,7582	0,44607
Moldavia	86	63	39	114	0,653444444	66	0,55708	0,62745	0,52755	0,7201	0,42355
Turquía	87	67	63	69	0,652023697	71	0,54428	0,49019	0,55905	0,7133	0,36048
Kuwait	88	47	72	46	0,645787499	49	0,6268	0,43137	0,5748	0,7194	0,5862
Argelia	89	128	159	93	0,642588889	136	0,31064	0,07843	0,07874	0,6543	0,19885
Macedonia	90	92	127	84	0,641897778	96	0,47198	0,21568	0,24409	0,7198	0,45207
Tayikistán	91	121	147	133	0,639444444	129	0,33951	0,11764	0,06299	0,7249	0,23062
San Cristóbal y Nieves	92	86	147	73	0,637912633	90	0,49795	0,11764	0,13385	0,7279	0,63209
México	93	60	44	71	0,637833108	63	0,5733	0,60784	0,66141	0,7445	0,31393
Seychelles	94	77	116	71	0,635928889	81	0,51126	0,2549	0,3307	0,731	0,47206
Santa Lucía	95	98	112	97	0,631431389	104	0,45248	0,2745	0,24409	0,7133	0,40004
Líbano	96	85	105	65	0,630576124	89	0,49823	0,29411	0,35433	0,7374	0,40298
Túnez	97	71	32	90	0,621455556	75	0,53895	0,64705	0,63779	0,6717	0,30741
Botswana	98	106	102	109	0,619	112	0,41984	0,31372	0,30708	0,6555	0,29694
Micronesia	99	122	116	124	0,611084533	130	0,33371	0,2549	0,18897	0,7023	0,10985
Filipinas	100	91	50	117	0,609984056	95	0,47681	0,56862	0,48031	0,7051	0,24508
China	101	66	32	91	0,609666667	70	0,54501	0,64705	0,60629	0,6734	0,3554
Albania	102	80	57	95	0,608519363	84	0,50455	0,52941	0,44881	0,71	0,3548
Tailandia	103	96	52	89	0,607965284	102	0,46308	0,54901	0,44094	0,664	0,28428
Dominica	104	104	147	93	0,607498001	110	0,4338	0,11764	0,18897	0,6701	0,44237
Omán	105	46	23	56	0,603279117	48	0,62732	0,70588	0,73228	0,6624	0,48725
Indonesia	106	100	105	108	0,603136041	106	0,44874	0,29411	0,3622	0,6786	0,30544
Colombia	107	48	10	98	0,602222411	50	0,6173	0,88235	0,7874	0,7348	0,32971
Kiribati	108	124	105	133	0,602070533	132	0,3201	0,29411	0,21259	0,6812	0,06654
Ecuador	109	79	63	98	0,5938375	83	0,50529	0,49019	0,48031	0,7037	0,33184
República Dominicana	110	101	92	102	0,590170542	107	0,44808	0,33333	0,38582	0,6639	0,2945
Gabón	111	123	127	112	0,589333333	131	0,3294	0,21568	0,09448	0,6677	0,22601
Suriname	112	108	141	100	0,588380289	115	0,40446	0,13725	0,14173	0,6749	0,39678
Paraguay	113	115	116	111	0,587322222	122	0,374	0,2549	0,22834	0,67	0,22361
Guayana	114	117	92	121	0,581655556	124	0,36952	0,33333	0,24409	0,6301	0,23437
Egipto	115	76	52	110	0,573444444	80	0,51293	0,54901	0,59055	0,5912	0,35705
El Salvador	116	84	44	115	0,553261879	88	0,49885	0,60784	0,53543	0,6414	0,31975
Siria	117	127	152	118	0,553191582	135	0,31341	0,09803	0,15748	0,5835	0,19924

Ghana	118	116	79	138	0,552744444	123	0,37354	0,39215	0,31496	0,5613	0,24438
Swazilandia	119	129	138	148	0,551288889	138	0,30558	0,15686	0,13385	0,62	0,16288
Maldivas	120	90	112	103	0,547543357	94	0,48129	0,2745	0,3622	0,6865	0,39516
Namibia	121	110	92	127	0,520188889	117	0,38799	0,33333	0,32283	0,5693	0,27187
Kenia	122	112	32	147	0,514555556	119	0,38054	0,64705	0,42519	0,5552	0,1612
Togo	123	148	152	166	0,514422222	162	0,24463	0,09803	0,11023	0,5401	0,08359
Congo	124	146	152	140	0,511333333	160	0,25696	0,09803	0,10236	0,5233	0,14526
Honduras	125	107	92	129	0,504963149	114	0,40826	0,33333	0,40157	0,6281	0,19514
Lesoto	126	140	141	162	0,504158407	153	0,26294	0,13725	0,15748	0,5135	0,11785
Camboya	127	130	130	136	0,495177778	139	0,29986	0,19607	0,17322	0,5189	0,20745
Camerún	128	134	138	152	0,485788889	144	0,27823	0,15686	0,19685	0,5421	0,09579
Nicaragua	129	136	152	132	0,4839	147	0,27585	0,09803	0,09448	0,5639	0,16924
Guatemala	130	125	130	125	0,483879889	133	0,31603	0,19607	0,1496	0,5272	0,27125
Cabo Verde	131	119	152	123	0,483466667	127	0,35505	0,09803	0,16535	0,6032	0,29658
Uganda	132	143	141	164	0,478643671	156	0,25926	0,13725	0,1496	0,5271	0,10108
Ruanda	133	118	61	151	0,478166667	125	0,35888	0,5098	0,51181	0,482	0,08284
Angola	134	131	122	149	0,474212067	140	0,29703	0,23529	0,29921	0,4941	0,09778
India	135	111	39	135	0,472666667	118	0,38343	0,62745	0,5433	0,4698	0,13723
Timor-Leste	136	147	105	128	0,472406667	161	0,25276	0,29411	0,20472	0,4831	0,07042
Santo Tomé y Príncipe	137	154	170	142	0,469165789	169	0,22179	0,0196	0,00787	0,5177	0,13976
Marruecos	138	78	16	129	0,467855556	82	0,50598	0,80392	0,69291	0,4901	0,33499
Irak	139	126	141	120	0,466555556	134	0,31414	0,13725	0,19685	0,5283	0,21727
Madagascar	140	142	87	155	0,458425611	155	0,2606	0,35294	0,24409	0,4889	0,04879
Nepal	141	150	105	145	0,452311111	165	0,23442	0,29411	0,15748	0,3774	0,16843
Comoras	142	162	168	159	0,450419756	177	0,18077	0,03921	0,01574	0,4662	0,06037
Bangladesh	143	137	79	142	0,446880445	148	0,27572	0,39215	0,34645	0,3866	0,09414
Malawi	144	151	122	174	0,439666667	166	0,23208	0,23529	0,17322	0,4746	0,04837
Lao	145	139	130	139	0,435866667	152	0,26588	0,19607	0,14173	0,4941	0,16177
Tanzania	146	135	79	159	0,425888889	146	0,27642	0,39215	0,29921	0,4492	0,08082
Nigeria	147	132	92	152	0,42486	141	0,29287	0,33333	0,30708	0,3811	0,19045
Bhután	148	133	87	136	0,421244444	143	0,28285	0,35294	0,24409	0,429	0,17546
Guinea Ecuatorial	149	153	170	144	0,414911111	168	0,22675	0,0196	0,03149	0,5288	0,11996
Benin	150	165	135	165	0,413555556	180	0,1685	0,17647	0,11023	0,2756	0,11964
Islas Salomón	151	155	159	157	0,405498789	170	0,20871	0,07843	0,05511	0,4702	0,10084
Costa de Marfil	152	156	135	171	0,389222222	171	0,20385	0,17647	0,17322	0,2992	0,13917
Papúa Nueva Guinea	153	172	175	157	0,376311111	188	0,12028	0	0,00787	0,3	0,05296
Haití	154	161	135	168	0,374277778	176	0,18086	0,17647	0,11023	0,3372	0,09521
Mozambique	155	149	92	178	0,372055556	164	0,23837	0,33333	0,31496	0,3457	0,05449
Congo (Rep Dem.).	156	168	170	186	0,371777778	183	0,15514	0,0196	0,04724	0,3845	0,03369
Pakistán	157	145	92	146	0,371667343	158	0,25799	0,33333	0,32283	0,3337	0,11743
Myanmar	158	160	159	150	0,370555556	175	0,18694	0,07843	0,02362	0,5288	0,00836
Burundi	159	157	165	180	0,370088889	172	0,19278	0,05882	0,01574	0,5393	0,02332

Senegal	160	138	87	163	0,367811111	151	0,26657	0,35294	0,30708	0,3283	0,16437
Liberia	161	164	147	175	0,367244444	179	0,17682	0,11764	0,07874	0,3754	0,0763
Afganistán	162	158	141	169	0,365333333	173	0,19003	0,13725	0,1811	0,2418	0,14722
Mauritania	163	159	159	161	0,352277778	174	0,1893	0,07843	0,04724	0,3581	0,16256
Gambia	164	152	127	172	0,345611111	167	0,22851	0,21568	0,20472	0,3326	0,14816
Guinea-Bissau	165	167	170	177	0,325333333	182	0,16085	0,0196	0,00787	0,3869	0,08776
República Centroafricana	166	171	168	185	0,317866667	187	0,12574	0,03921	0,03937	0,3099	0,02799
Etiopía	167	144	116	173	0,316521973	157	0,25888	0,2549	0,45669	0,2934	0,02659
Sudán	168	141	112	166	0,305955556	154	0,26062	0,2745	0,29133	0,3059	0,18466
Djibouti	169	169	159	170	0,305877778	184	0,1456	0,07843	0,06299	0,3182	0,05557
Malí	170	166	138	176	0,305180943	181	0,16335	0,15686	0,13385	0,2212	0,13501
Sierra Leona	171	170	152	183	0,3045	186	0,13286	0,09803	0,04724	0,2692	0,08211
Guinea	172	174	170	179	0,294444733	190	0,09543	0,0196	0	0,2359	0,05044
Chad	173	173	159	184	0,255851922	189	0,10761	0,07843	0,04724	0,2341	0,04146
Burkina Faso	174	163	141	181	0,250033333	178	0,18043	0,13725	0,29921	0,1578	0,08423
Eritrea	175	176	175	182	0,227513722	192	0,09075	0	0	0,2723	0
Níger	176	175	122	187	0,197933333	191	0,09456	0,23529	0,12598	0,1192	0,03851

**No evaluados: Corea del Norte, Islas Marshall, Mónaco, Nauru, San Marino, Somalia, Sudán Del Sur, Uruguay, Uzbekistán, Vanuatu, Venezuela, Vietnam, Yemen, Zambia, Zimbabue, Tuvalu*

APÉNDICE 3. CURRÍCULUM VITAE

Jesús Salvador Cano Carrillo

Nací en Écija – Sevilla - en 1974. Ingeniero, oficial facultativo de la Guardia Civil en servicios especiales y actualmente adscrito al Tribunal Constitucional de España. He estado trabajando en el sector público desde 1997. Me gusta la buena lectura, el futbol, correr, la bici, las motos, pasear e ir a la piscina con mis niñas.

jesus.cano@computer.org
jcano@scc.uned.es

Puestos

2009-Act.	Jefe de Área de Sistemas Informáticos, Tribunal Constitucional, Madrid.
2004-2009	Jefe de Área en el Servicio de Informática y Estadística, Guardia Civil, Madrid.
2000-2004	Administrador de Sistemas en el Dpto. de Sistemas centrales, Guardia Civil, Madrid.
1997-2000	Agente de la Guardia Civil (varios destinos: Jaen, Sevilla, Madrid).
1996-1997	Empleado de Disney, Sevilla.

Puestos universitarios

2013-Act.	Profesor colaborador en Criminología, Facultad de Derecho de la Universidad San Pablo CEU, Madrid.
2008-Act.	Profesor asociado (2011, 2012) y colaborador en el Departamento de Sistemas de Comunicación y Control, ETS de Ingeniería Informática, UNED, Madrid.

Educación

2015	Doctorando en Ingeniería eléctrica, electrónica y control industrial, ETS de Ingenieros Industriales, UNED (Pendiente defensa).
2011	Ingeniero superior en Informática, ETS de Ingeniería Informática, UNED.
2009	Especialista militar en Criptografía, Centro Superior de Estudios de la Defensa Nacional, Ministerio de Defensa, Madrid.
2008	Master en Comunicación, redes y gestión de contenidos, ETS de Ingeniería Informática, UNED.
2008	Diploma de Aptitud Pedagógica, Instituto de Ciencias de la Educación, Universidad de Alcalá, Madrid. Además, reconocida la acreditación militar de aptitud pedagógica.
2004	Oficial de la Guardia Civil. Academia militar de Aranjuez, Madrid.

2000 Ingeniero Técnico en Informática de Sistemas Físicos, ETS de Ingeniería Informática, Universidad de Sevilla.

1997 Guardia Civil, Academia militar de Baeza, Jaén.

Experiencia en proyectos tecnológicos de interés (selección)

1997-1998 Industria. Sistema de punto de venta para heladerías. Dirección y desarrollo. Heladerías Torres y Europa. Sevilla.

1999 Industria. Proyecto de gestión de reparaciones de coches, chapa y pintura. Dirección y desarrollo. Sevilla.

2000 e-Government. Proyecto de mantenimiento y desarrollo de una librería software de comunicación para el intercambio de información relacionada con la identificación decadactilar entre cuerpos de policía. Departamento de Sistemas, Servicio de Informática, Dirección General de la Guardia Cviil, Madrid.

2001-2003 e-Government. Proyecto de solución de alta disponibilidad y gestión robotizada de backups del sistema de servidores centrales del centro de proceso de datos. Administrador de sistemas y desarrollador UNIX. Guardia Civil, Madrid.

2004-2005 e-Government. Proyecto para la unificación de sistemas de bases de datos (proyecto marco SUBA). Miembro del comité técnico para la unificación de bases de datos policiales y gestión técnica relacionada con la base de armas y explosivos. Secretaría de Estado de Seguridad, Madrid.

2005-2009 e-Government. Proyecto internacional para el sistema pan-europeo de información sobre control de explosivos, prevención y lucha contra el terrorismo. Dirección técnica, diseño y arquitectura. Unión Europea.

2006-2007 e-Government. Proyecto de gestión de las intervenciones de armas y explosivos. Jefe de proyecto. Jefe de area de desarrollo, Servicio de Informática, Guardia Civil. Madrid.

2007-2009 e-Government. Gestión de certificados y tarjetas criptográficas de identificación personal de la Guardia Civil. Jefe de area de desarrollo. Servicio de Informática, Guardia Civil. Madrid.

2006-2009 e-Government. Sistema de gestión administrativa de la interceptación de las comunicaciones (Proyecto GAITA). Jefe de proyecto, diseño, arquitectura. Servicio de Informática, Guardia Civil. Madrid.

2010-2011 e-Government. Proyecto de e-Justice para la gestión de la doctrina constitucional. Jefe de proyecto, diseño y arquitectura. Servicio de informática, Tribunal Constitucional. Madrid.

2011-2015 e-Government. Proyecto de e-Justice para el desarrollo de un motor de búsqueda para el acceso de los ciudadanos a la jurisprudencia constitucional sobre Internet. Dirección, diseño, arquitectura. Servicio de informática, Tribunal Constitucional. Madrid.

2011-2013 e-Democracia. Proyecto universitario para el diseño y desarrollo de un sistema de participación ciudadana para iniciativas legislativas populares OpenILP. Diseño, arquitectura, desarrollo. ETS Ingeniería Informática, UNED. Madrid.

2012-2013 e-justicia. Proyecto para la gestión del flujo y agenda de decisiones jurisdiccionales. Jefe de proyecto, diseño, arquitectura. Área de desarrollo, Servicio de Informática, Tribunal Constitucional, Madrid.

2013-2015 e-Educación. Proyecto de gestión de diplomas electrónicos mediante técnicas criptográficas de protección Opendiploma. ETS Ingeniería Informática, UNED. Madrid.

2015- e-Government. Proyecto de registro telemático y tramitación electrónica de demandas. Jefe de proyecto, diseño, arquitectura. Área de desarrollo, Servicio de Informática, Tribunal Constitucional, Madrid.

Publicaciones, conferencias y premios relacionados

- Cano, J.; Hernandez, R.; Ros, S., "Distributed Framework for Electronic Democracy in Smart Cities," Computer , vol.47, no.10, pp.65,71, Oct. 2014 doi: 10.1109/MC.2014.280
- Cano, J.; Hernandez, R., "SCEPYLT: An Information System for Fighting Terrorism," Software, IEEE , vol.30, no.3, pp.73,79, May-June 2013 doi: 10.1109/MS.2013.23
- Cano, J.; I Jornada sobre calidad del producto software. Noviembre 21-22, 2013 (http://calidaddelproductosoftware.com/2013/programa) – Participación ponencia
- Cano, J.; Hernández, R.; Ros, S., "Bringing an engineering lab into social sciences: didactic approach and an experiential evaluation," Communications Magazine, IEEE , vol.52, no.12, pp.101,107, December 2014 doi: 10.1109/MCOM.2014.6979960
- Premio académico a la Innovación Docente 2014 (accesit) por el diseño de un laboratorio de ciberseguridad mediante aprendizaje basado en problemas.. Jesus Cano & Alfredo Vazquez. Universidad San Pablo CEU. Enero 2015.
- Cano, J.; Jimenez, C.E.; Hernandez, R.; Ros, S., "New tools for e-justice: legal research available to any citizen," eDemocracy & eGovernment (ICEDEG), 2015 Second International Conference on , vol., no., pp.108,111, 8-10 April 2015 doi: 10.1109/ICEDEG.2015.7114455 https://edem-egov.org/ICEDEG-2015
- Carpio Cámara, M.; León, A.; Cano Carrillo, J.; Jiménez, C.E. "Regulación y ciberseguridad. Contribuciones al modelo de Gobernanza" Capítulo del libro "Gobernanza de Internet en España" Edita: IGF Forum Spain. 2015. Licencia Common Creative.[Disponible online] http://igfspain.com/doc/archivos/Gobernanza_Internet_Spain_2015.pdf [Accedido: 2015]
- Cano, J.; First IEEE International Smart Cities Conference. Octubre 25-28, 2015. – Participación como PC, Program Committee. (http://sites.ieee.org/isc2) Guadalajara, Mexico.
- Jimenez, C.E.; Cano, J.; Hernandez, "Emerging trends in engineering applied to e-Government and e-Justice". Hawai, Estados Unidos. 49th Hawaii International Conference on System Sciences. HICSS. Enero 5-8, 2016. (http://www.hicss.org)
- Cano, J., Hernandez, R. "Managing Software Architecture in Domains of Security-Critical Systems: Multifaceted Collaborative eGovernment Projects". Capitulo del libro "Securing Government Information and Data in Developing Countries". Editado por Dr. Saleem Zoughbi. IGI-Global. Serie: Advances in Information Security, Privacy, & Ethics (AISPE) Book Series. ISSN: 1948-9730
- Cano, J.; Hernandez, R.; Jimenez, C.E.; Pomed, L.; "Open justice in constitutional courts: securing Networked Constitution, challenges of electronic justice, transparency and citizen participation". Capítulo del libro "Achieving Open Justice through Citizen Participation and Transparency". Editado por: Jiménez, C.E. & Gascó, M. IGI-Global. Serie: Advances in Public Policy and Administration (APPA) Book Series

Dirección de proyectos académicos finales

- "Plataforma de explotación de datos abiertos de seguridad pública: Open Data Security". Proyecto final del Master de Comunicación, redes y gestión de contenidos, de Parra, E. ETS Ingeniería Informática, UNED. – En curso –
- "Arquitectura de voto electrónico para iniciativas en el ámbito europeo basado en OpenILP". Proyecto final del Master de Comunicación, redes y gestión de contenidos, de De Diego, R. ETS Ingeniería Informática, UNED. – En curso –
- "Ciberespionaje entre países". Proyecto final del Grado en Criminología y Seguridad, de Martínez, P.J. Facultad de Derecho, Universidad San Pablo CEU. Mayo 2015.
- "Investigación aplicada al malware con mecanismos criptográficos". Proyecto final del Master de Comunicación, redes y gestión de contenidos, de Parra, E. ETS Ingeniería Informática, UNED. Septiembre 2014.
- "Dispositivos de redes y comunicaciones móviles en la investigación criminológica, interceptación y seguridad a nivel nacional y europeo". Proyecto final del Grado en Criminología y Seguridad, de Bringas, M.E. Facultad de Derecho, Universidad San Pablo CEU. Mayo 2014
- "Sistema logístico de vestuario securizado mediante técnicas criptográficas aplicadas al motor de bases de datos". Proyecto final del Master de Comunicación, redes y gestión de contenidos, de González, M. ETS Ingeniería Informática, UNED. Marzo 2013.
- "Organizador digital de fotos mediante DNI electrónico". Proyecto final del Master de Comunicación, redes y gestión de contenidos, de Barbudo, A. ETS Ingeniería Informática, UNED. Febrero 2012.
- "Aplicación para el cifrado de imágenes basado en criptografía visual". Proyecto final del Master de Comunicación, redes y gestión de contenidos, de Méndez, E. ETS Ingeniería Informática, UNED. Febrero 2012.

Colaboraciones y voluntariado, IEEE

- IEEE Computer Society eGovernment, Secretario, desde agosto 2014
- IEEE Cyber-ethics and Cyber-peace Initiative, co-fundador, desde mayo 2015
- IEEE 1as Jornadas Smart City, Program Committee Guadalajara – México, ISC2-2015