

nov@t@ca

Revista de la Asociación de Técnicos de Informática

Nº 215, enero-febrero 2012, año XXXVIII



Computación en la nube

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software). **Novática** co-edita asimismo **UPGRADE**, revista digital de **CEPIS** (Council of European Professional Informatics Societies), en lengua inglesa, y es miembro fundador de **UPENET** (**UPGRADE** European Network).

<<http://www.ati.es/novatica/>>
<<http://www.ati.es/reicis/>>
<<http://www.cepis.org/upgrade/>>

ATI es miembro fundador de **CEPIS** (Council of European Professional Informatics Societies) y es representante de España en **IFIP** (International Federation for Information Processing); tiene un acuerdo de colaboración con **ACM** (Association for Computing Machinery), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AIZ**, **ASTIC**, **RITSI** e **HispaniLinux**, junto a la que participa en **ProInnova**.

Consejo Editorial

Ignacio Aguillo Sousa, Guillem Aínsa González, María José Escalona Cuaresma, Rafael Fernández Calvo (presidente del Consejo), Jaime Fernández Martínez, Luis Fernández Sanz, Didac Lopez Viñas, Celestino Martín Alonso, José Onofre Montesa Andrés, Francesc Noguera Puig, Ignacio Pérez Martínez, Andrés Pérez Payeras, Viktu Pons i Colomer, Juan Carlos Vigo López

Coordinación Editorial

Llorenç Pagés Casas <pages@ati.es>

Composición y autoedición

Jorge Llécer Gil de Ramales

Traducciones

Grupo de Lengua e Informática de ATI <<http://www.ati.es/gt/lengua-informatica/>>

Administración

Tomas Brunete, María José Fernández, Enric Camarero, Felicidad López

Secciones Técnicas - Coordinadores

Acceso y recuperación de la información

José María Gómez Hidalgo (Optene), <jmgomez@yahoo.es>

Manuel J. María López (Universidad de Huelva), <manuel.mana@diehsia.uhu.es>

Administración Pública electrónica

Francisco López Crespo (MAE), <flc@ati.es>

Arquitecturas

Enrique F. Torres Moreno (Universidad de Zaragoza), <enrique.torres@unizar.es>

Jordi Tubella Moragas (DAC-UPC), <jordi@ac.upc.es>

Auditoría SITIC

Marina Touriño Troitiño, <marinatourino@marinatourino.com>

Manuel Palao García-Suelto (ATI), <manuel@palao.com>

Derecho y tecnologías

Isabel Hernando Collazos (Fac. Derecho de Donostia, UPV), <isabel.hernando@ehu.es>

Elena Davara Fernández de Marcos (Davara & Davara), <edavara@davara.com>

Enseñanza Universitaria de la Informática

Cristóbal Pareja Flores (DSIP-UCM), <cpajef@sis.ucm.es>

J. Angel Velázquez Hurtado (ULSI, URJC), <angel.velazquez@urjc.es>

Entorno digital personal

Andrés Marín López (Univ. Carlos III), <amarin@it.uc3m.es>

Diego Gachet Páez (Universidad Europea de Madrid), <gachet@uem.es>

Estándares Web

Encarna Quesada Ruiz (Virati), <encarna.quesada@virati.com>

José Carlos del Arco Prieto (TCP Sistemas e Ingeniería), <jcarco@gmail.com>

Gestión del Conocimiento

Juan Baiget Solé (Cap Gemini Ernst & Young), <juan.baiget@ati.es>

Informática y Filosofía

José Ángel Olivas Varela (Escuela Superior de Informática, UCLM), <joseangel.olivas@uclm.es>

Roberto Feltrero Oreja (UNED), <rfeltrero@gmail.com>

Informática Gráfica

Miguel Chover Selles (Universitat Jaume I de Castellón), <mchover@lsi.uji.es>

Roberto Vivó Hernando (Eurographics, sección española), <rvivo@dsic.upv.es>

Ingeniería del Software

Javier Dolado Cosin (ULSI-UPV), <dolado@si.ehu.es>

Daniel Rodríguez García (Universidad de Alcalá), <daniel.rodriguez@uah.es>

Inteligencia Artificial

Vicente Boti Navarro, Vicente Julián Inglada (DSIC-UPV), <[vboti,vinglada@dsic.upv.es](mailto:(vboti,vinglada)@dsic.upv.es)>

Interacción Persona-Computador

Pedro M. Latorre Andrés (Universidad de Zaragoza, AIPO), <platorre@unizar.es>

Francisco L. Gutiérrez Vela (Universidad de Granada, AIPO), <fgutien@ugr.es>

Lengua e Informática

M. del Carmen Ugarte García (ATI), <cugarte@ati.es>

Lenguajes Informáticos

Oscar Belmonte Fernández (Univ. Jaime I de Castellón), <obellem@lsi.uji.es>

Inmaculada Coma Taty (Univ. de Valencia), <inmaculada.coma@uv.es>

Lingüística computacional

Xavier Gómez Guinovart (Univ. de Vigo), <xgg@uvigo.es>

Manuel Palomar (Univ. de Alicante), <mpalomar@dsi.ua.es>

Mundo estudiantil y jóvenes profesionales

Federico C. Mon Trotti (RITSI), <fcmon@redes@gmail.com>

Mikel Salazar Peña (Área de Jóvenes Profesionales, Junta de ATI Madrid), <mikelbo_xi@yahoo.es>

Profesión Informática

Rafael Fernández Calvo (ATI), <rfcalvo@ati.es>

Miguel Sarrías Gil (ATI), <msarrias@ati.es>

Redes y servicios telemáticos

José Luis Marzo Lázaro (Univ. de Girona), <joseluis.marzo@udg.es>

Juan Carlos López López (UCLM), <juancarloslo@uclm.es>

Robótica

José Cortés Arenas (Sopra Group), <jccort@redes.com>

Juan González Gómez (Universidad Carlos III), <juan@learobotics.com>

Seguridad

Javier Arellano Bertolin (Univ. de Deusto), <jarellito@deusto.es>

Javier López Muñoz (ETS Informática-UMA), <jlm@lcc.uma.es>

Sistemas de Tiempo Real

Alejandro Alonso Muñoz, Juan Antonio de la Puente Alfaro (DIT-UPM), <faalonso_ipuente@dit.upm.es>

Software Libre

Jesus M. González Barahona (Universidad Politécnica de Madrid), <ismael.herraz@upm.es>

Israel Herráz Tabernerro (UAX), <isra@herraz.org>

Tecnología de Objetos

Jesus García Molina (DIS-UM), <jmolina@um.es>

Gustavo Rossi (LPIA-UNLP Argentina), <gustavo@sol.info.unlp.edu.ar>

Tecnologías para la Educación

Juan Manuel Doderó Beardo (UC3M), <doderom@inf.uc3m.es>

César Pablo Córcoles Briogio (UOC), <ccorcoles@uoc.edu>

Tecnologías y Empresa

Didac López Vilas (Universitat de Girona), <didac.lopez@ati.es>

Francisco Javier Cantis Sánchez (Infra Sistemas), <fcantis@gmail.com>

Tendencias tecnológicas

Alonso Álvarez García (TID), <aad@tid.es>

Gabriel Martí Fuentes (Interbitis), <gabi@atinet.es>

TIC y Turismo

Andrés Aguayo Maldonado, Antonio Guevara Plaza (Univ. de Málaga), <[aguayo, guevara@lcc.uma.es](mailto:(aguayo, guevara)@lcc.uma.es)>

Las opiniones expresadas por los autores son responsabilidad exclusiva de los mismos. **Novática** permite la reproducción, sin ánimo de lucro, de todos los artículos, a menos que lo impida la modalidad de © o copyright, elegida por el autor, debiendo en todo caso citar su procedencia y enviar a **Novática** un ejemplar de la publicación.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid

Padilla 66, 3º dcha., 28006 Madrid
Tfno. 91 4029391 - fax 91 5939686 - novatica@ati.es

Composición, Edición y Redacción ATI Valencia

Av. del Reino de Valencia 23, 46005 Valencia
Tfno. 963740173 - novatica_prod@ati.es

Administración y Redacción ATI Cataluña

Via Laietana 46, ppal. 1º, 08003 Barcelona
Tfno. 934125236 - fax 934127713 - secre@ati.es

Redacción ATI Aragón

Lagaasca 9, 3-B, 50006 Zaragoza.
Tfno. fax 976235181 - secreara@ati.es

Redacción ATI Andalucía

Redacción ATI Galicia <secregal@ati.es>

Suscripción y Ventas <<http://www.ati.es/novatica/interes.html>>, ATI Cataluña, ATI Madrid

Publicidad Padilla 66, 3º dcha., 28006 Madrid.

Tfno. 91 4029391 - fax 91 5939686 - novatica@ati.es

Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.

Depósito legal: B 15.154-1975 - ISSN: 0211-2124; CODEN NOVAEC

Portada: Malvasisco - Concha Arias Pérez / © ATI

Diseño: Fernando Agresta / © ATI 2003

Nº 215, enero-febrero 2012, año XXXVIII

editorial

Asamblea General Extraordinaria de ATI: un impulso hacia el futuro de la Asociación y de Novática

> 02

noticias de IFIP

Firma del memorando de entendimiento entre IFIP y el Gobierno del Paraguay para la organización de WITFOR 2013

> 03

Ramon Puigjaner Trepal

en resumen

Cerrando el círculo: La computación en la nube en la práctica habitual

> 08

Llorenç Pagés Casas

monografía

Computación en la nube

Editor invitado: Fernando Piera Gómez

Presentación. ¿Cloud computing? o ¿Computación en la nube?

> 06

Fernando Piera Gómez

Tecnologías de infraestructura en la nube

> 09

Enrique Birlanga Terrón

ISO 20000-7: Guía para la implantación de la ISO/IEC 20000-1 en la nube

> 11

Guillermo López Moratinos

Cuestiones legales sobre Cloud Computing

> 14

Karen Elizabeth Sánchez Quiñones, Ignacio Delgado Gonzalez, Idoia Uriarte Lauzirika

Desarrollo de aplicaciones cloud con Windows Azure:

Cuatro experiencias prácticas

> 19

Ramon Costa Pujol

Seguridad en el cómputo en la nube

> 24

Guillermo Morales-Luna

Seguridad en la nube, algo nuevo bajo el sol

> 29

Olof Sandstrom

Análisis forense en un ecosistema tecnológico: redes sociales, tecnologías móviles y computación en la nube

> 33

Jeimy J. Cano

secciones técnicas

Interacción Persona-Computador

Enriqueciendo la evaluación en videojuegos

> 37

José Luis González Sánchez, Rosa María Gil Iranzo, Francisco Luis Gutiérrez Vela

Seguridad

Análisis de la seguridad del sistema reCAPTCHA

> 43

Noemí Carranza, Ricardo Palma Durán, Gonzalo Álvarez Maraño, José María Gómez Hidalgo

Referencias autorizadas

> 49

Sociedad de la Información

Resultados de investigación

La Investigación en Informática en España: Análisis bibliométrico

> 54

Francisco Ruiz González

Programar es crear

El Problema del Laberinto Cuadrado

> 59

(Competencia UTN-FRC 2011, problema B, solución)

Julio Javier Castillo, Diego Javier Serrano, Marina Elizabeth Cárdenas

El Problema del Superbowling

> 60

(Competencia UTN-FRC 2011, problema F, enunciado)

Julio Javier Castillo, Diego Javier Serrano, Marina Elizabeth Cárdenas

asuntos interiores

Coordinación editorial / Programación de Novática / Socios Institucionales

> 61

Asamblea General Extraordinaria de ATI: un impulso hacia el futuro de la Asociación y de Novática

El pasado 16 de febrero se celebró una importante Asamblea General Extraordinaria de nuestra asociación¹. En el curso de la misma la Junta Directiva General informó del Plan de Acción de medidas de sostenibilidad que se han puesto en marcha para afrontar la comprometida coyuntura económica, que de no ser abordadas con decisión podrían poner a ATI en una posición financiera delicada. Asimismo, la Junta Directiva sometió a debate y votación el futuro de nuestro producto estrella, la revista **Novática**, presentándose a los compromisarios diversas opciones para su publicación en función tanto de su impacto presupuestario como de otros parámetros cualitativos.

Desde el punto de vista formal hay que subrayar que la Junta Directiva General no estaba obligada estatutariamente a convocar esta Asamblea General Extraordinaria. A pesar de ello consideró altamente conveniente que el máximo órgano de nuestra asociación conociese lo antes posible las medidas tomadas dentro del Plan de Acción para la sostenibilidad de ATI y decidiese sobre nuestra revista, pues el impacto presupuestario de ambos asuntos no permitía aplazar la decisión a la Asamblea General Ordinaria, que suele celebrarse en junio. También es importante señalar que es la primera vez que, en sus cuarenta y cinco años de vida, ATI realiza una Asamblea General Extraordinaria para un tema que no sea una modificación estatutaria.

La reunión fue altamente constructiva y productiva, con un intercambio de ideas y

opiniones muy válidas para el presente y el futuro de nuestra asociación. Hubo unanimidad en señalar que esta difícil coyuntura debe ser aprovechada como una oportunidad para repensar de forma global el modelo estructural y funcional de ATI. Se aspira a construir un modelo que, sin perder lo esencial de nuestras características distintivas, refuerce nuestra presencia en las diversas comunidades que conforman la profesión informática y en la sociedad en su conjunto, con la vista puesta no sólo en nuestro país sino en el conjunto de los países de habla española.

En lo concreto, los compromisarios fueron informados de las medidas de reestructuración funcional, administrativa y laboral emprendidas para equilibrar el presupuesto de ATI cara al año en curso y a ejercicios sucesivos, incluyendo una adecuación de la plantilla a nuestras necesidades reales, algo que lamentamos profundamente pero que era imprescindible para alcanzar dicho equilibrio. La medida ha afectado a dos de nuestros colaboradores, en condiciones que se ha intentado que fuesen lo menos desfavorables posible para sus legítimos intereses y aplicando las normas legales anteriores a la reciente reforma laboral.

En lo que se refiere a **Novática**, partiendo de que la revista pasará a ser exclusivamente digital a partir de 2013, los compromisarios aprobaron que en el año en curso se inicie el proceso de digitalización de forma gradual. A tal fin se publicarán tres números impresos de 64 páginas cada uno y tres digitales de 80 páginas, en vez de los actuales seis números impresos de 80 páginas.

Se señaló que la distribución de **Novática** en formato exclusivamente digital debe suponer mucho más que la edición de la revista en PDF, aprovechando este cambio de modelo para conseguir nuevas oportunidades de comunicación, control de la difusión, alternativas en publicidad y patrocinio, etc. Se trata asimismo de reinventar el contenido y el contenido con el fin de elaborar un nuevo producto de gran calidad que al mismo tiempo ratifique nuestra puesta al día con las tecnologías más efectivas y actuales y con el uso de redes sociales, en las que tanto ATI como **Novática** deben estar cada vez más presentes.

En resumen, el positivo resultado de la Asamblea General Extraordinaria es un potente estímulo para conseguir, de acuerdo con la misión de “*ser útil a sus socios y a la sociedad*”, una ATI cada vez más activa, presente e influyente en la comunidad informática y en nuestra actual Sociedad de la Información.

La Junta Directiva General de ATI

¹ Como de costumbre, la Asamblea se celebró mediante el sistema ISABEL de videoconferencia, con sedes principales en Madrid y Barcelona, a la que se unieron varios socios de forma individual. Agradecemos de nuevo su magnífica y desinteresada colaboración al Depto. de Ingeniería de Sistemas Telemáticos (DIT) de la ETSI Telecomunicación de la Universidad Politécnica de Madrid (UPM) y a la ETSETB de la Universitat Politècnica de Catalunya (UPC).



Estudiante de Informática
(Ingeniería Superior o Técnica,
o Formación Profesional)



Preocupado por tu
integración profesional



La asociación de profesionales informáticos más numerosa, dinámica, abierta y veterana de nuestro país ha puesto en marcha **servicios específicos para socios estudiantes** que te ayudarán a verlo más claro



Conócenos en www.ati.es/estudiantes
y/o escribenos a info@ati.es

Firma del memorando de entendimiento entre IFIP y el Gobierno del Paraguay para la organización de WITFOR 2013

Ramon Puigjaner Trepas

Vicepresidente de IFIP; Catedrático Emérito de la Universitat de les Illes Balears; ex-presidente de ATI

<putxi@uib.es>

En la visita de Ramon Puigjaner a Asunción el 15 de diciembre de 2011, se firmó un memorándum de entendimiento entre la Secretaría Técnica de Planificación (STP) del gobierno paraguayo (con categoría de ministerio) y la IFIP.

La STP fue representada por el Ministro Hugo Royg y la IFIP por Ramon Puigjaner, debidamente autorizado por el presidente, Leon Strous. Además asistieron a esta reunión Benjamín Barán, ex-Presidente de CLEI y el líder en la impulsión de la candidatura de Paraguay para la celebración de WITFOR (World Information Technology Forum) 2013, Nicolás Pereyra, asesor en políticas de TIC de la casa civil del presidente de la república, y Rubén Cubilla, asistente del Ministro Hugo Royg en la STP.

A finales de enero de 2012, el ministro Hugo Royg nombró a las personas clave de su país para la organización de WITFOR 2013 que se incorporaron al equipo ya nombrado por el Presidente de IFIP, Leon Strous. Con ello el organigrama de WITFOR 2013 queda como sigue:

- **Margarita Rojas**, Co-presidente del Comité Directivo; responsable del Plan Director de las TIC.
- **Ramon Puigjaner**, Co-presidente del Comité de Dirección, Vice-Presidente de la IFIP y Catedrático Emérito de la Universitat de les Illes Balears.
- **Benjamín Barán**, Co-presidente del IPC, el primer doctor en Informática en Paraguay, profesor de la Universidad Nacional de Asunción y de la Universidad Católica de Asunción, y director de su propia empresa de consultoría.

- **Ana Pont**, Co-presidente del IPC, Ex-presidenta del WG6.9 sobre Redes de comunicación para los países en desarrollo y catedrática de la Universitat Politècnica de València.
- **Nicolás Pereyra**, presidente del Comité Organizador; Asesor en Políticas de TIC de la Casa Civil del Presidente de la República.
- **Rubén Cubilla**, vicepresidente del Comité Organizador, asistente del Ministro Hugo Royg en la STP.
- **María Elena García**, miembro del Comité Organizador, Directora del departamento de Informática de la Universidad Nacional de Asunción, que ha demostrado su capacidad en la organización de grandes eventos como CLEI 2010.

NOVEDAD IMPORTANTE

NOVÁTICA n° 216
Revista de la Asociación de Técnicos de Informática

**se publicará solamente
en digital**



Después de 37 años en formato papel, nos proponemos una transición hacia un formato digital que nos facilite dar un mejor servicio a nuestros lectores:

- Nuevos espacios y contenidos más adecuados al interés del lector.
- Mayor interactividad y obtención de información de retorno.
- Crear comunidad alrededor de Novática.

¿Te gusta la idea de que hagamos evolucionar nuestra revista?

¿Quieres conocer más y aportar tus ideas para enfocar esta transición?

¡Participa desde ahora en el blog del Director de Novática! <<http://www.ati.es/blog/>>

(Para más información, ver el editorial de este mismo número)

Fernando Piera Gómez

Especialista en Business Intelligence, computación en la nube y temas legales relacionados; Ex-Vicepresidente Primero de ATI

<fpiera@ati.es>

En el momento presente, nos encontramos en una transición de la gestión de los negocios por individuos a la gestión por equipos. La naturaleza de cómo la gente trabaja, está cambiando. Ya no es suficiente apoyar a quienes contribuyen individualmente a una función u objetivo de la organización. Los usuarios finales requieren apoyo sobre el modo en que logran hacer las cosas. La colaboración en equipos y la comunicación a través de los departamentos y las fronteras geográficas, todos en un contexto específico de negocio o actividad es una necesidad.

Típicamente, la gente que colabora toma mejores decisiones que aquellos que lo hacen de manera aislada, y lo hacen de manera incremental por su exposición a lo fácil de hacer, por ej. en aplicaciones flexibles de Internet. Los usuarios de negocios de hoy día esperan ser autosuficientes y crear y definir su propio entorno de soluciones, en lugar de siempre depender de las soluciones informáticas predeterminadas. Además, se observa un movimiento del negocio hacia las redes de negocio. La naturaleza de cómo los negocios se conectan unos con otros está cambiando. Las empresas y demás tipos de organizaciones no pueden ya mantener relaciones dentro del alcance de la mano con sus clientes y suministradores. La organización necesita optimizar el rendimiento del negocio a través de una red dinámica de socios con los que está subcontratando y recibiendo sus contratos, con los que mantiene relaciones comerciales. Estas redes de negocios posibilitan a la organización facilitar innovaciones más rápidamente a los clientes, a menores costes, compartiendo las inversiones, los bienes de capital y las ideas, pero además, para tener éxito, se requiere ser capaz de reunir y de compartir información de manera efectiva.

A pesar del tiempo empleado en mejorar las operaciones de los negocios, hoy en día los usuarios se encuentran esencialmente con los mismos problemas de siempre: la dificultad de obtener los datos y las informaciones que necesitan cuando las necesitan y de una forma útil para su trabajo.

Nos encontramos 50 años después de que la Informática tomara consciencia de su existencia, no porque naciera entonces, allá por el inicio de la década de los años 60 del siglo pasado, sino porque fue cuando se comenzó a manejar con las denominadas calculadoras,

Editor invitado

Fernando Piera Gómez es Licenciado en Derecho y en Informática y lleva en la profesión informática desde 1967. Funcionario TAC de la Administración del Estado, creó el CPD del Ministerio de Educación y Ciencia de España y diseñó la creación del Instituto de Informática, ambos en 1969. Fue director General Adjunto de la Oficina Intergubernamental para la Informática (IBI) y trabajó dirigiendo y gestionando proyectos de I+D financiados por la Unión Europea en Indra Sistemas S.A. Fue Vicepresidente Primero de ATI y representante de la asociación ante CEPIS durante más de una década. Actualmente trabaja en temas relacionados con *Business Intelligence*, computación en la nube y temas legales relacionados. Dirigió desde su creación hasta fines de 2011 la Revista Cloud Computing <<http://www.revistacloudcomputing.com/>>. Da cursos y escribe sobre estos temas.

luego llamadas ordenadores o computadores/as, los datos e informaciones de las organizaciones, de las empresas y de las administraciones públicas.

En aquellos años iniciales, aquellas máquinas todavía no hacían más que lo que desde los años 20 del siglo pasado, se venía realizando con las máquinas de tarjetas perforadas, tabuladoras, clasificadoras, etc., que en el fondo no era otra cosa que ordenar datos para poder realizar contabilidades y nóminas más deprisa y con mayor exactitud que cuando se hacían de manera manual.

Luego, con la aparición de ordenadores más potentes, a fines de los años 60, ya se pasó no solo a manejar los datos, sino también a ajustar a los nuevos medios electromecánicos los procedimientos de gestión de aquellos datos. En aquellos tiempos, al reajuste de los procedimientos de gestión se denominaba "Organización y Métodos", porque se organizaban los datos y las informaciones y se "racionalizaban" los procedimientos de gestión. Pero a eso mismo, en los años 80 y 90 se le denominaba "reingeniería de sistemas", y en la actualidad hablamos de "inteligencia de los negocios", la "*Business Intelligence*". Lo que indudablemente se ha modificado y ha cambiado es la tecnología utilizada, las herramientas, pero el fondo sigue siendo lo mismo, estamos reinventando la rueda modificando la terminología empleada porque así se vende mejor. Son instrumentos de marketing los que nos pueden despistar y creer que estamos ante cosas nuevas, ante nuevos inventos, cuando en realidad en el mejor de los casos lo que se ha realizado es mejorar los procedimientos de análisis y organización y optimizar los métodos de gestión de esos datos e informaciones para lograr un mejor conocimiento.

Presentación. ¿Cloud computing? o ¿Computación en la nube?

Ya no se habla prácticamente de procesos batch ni de batch remoto, pero lo que se está desarrollando en la actualidad con el fenómeno denominado "*Cloud computing*" (este término inglés se está usando muy a menudo en los países de habla castellana a pesar de que "computación en la nube" es una muy buena traducción) tiene mucho de proceso en batch y de proceso en batch remoto. De hecho el procesamiento en la nube no es más que la vuelta a las "Oficinas de servicios informáticos" (en inglés "*Data Processing Service Bureaus*") de hace 40 años. Basadas ahora en las facilidades de comunicación vía Internet y otras tecnologías similares, así como en la necesidad de centralización de los datos que hace que los PC individuales, en organizaciones, empresas y administraciones públicas, se vean desfasados.

Dentro de este contexto nos encontramos también con el tema de la virtualización que tiene una gran semejanza con el procesamiento en la nube y con la simulación, pues en el fondo la virtualización no es más que una simulación, una apariencia de lo que en realidad no es, y también la simulación lleva años de existencia en nuestro mundo informático. Pero hablar de "virtualización" queda mucho mejor a efectos de marketing.

Hay que reconocer que lo que ha progresado es la tecnología de la programación, pero si lo miramos fríamente los programas actuales solo son eficientes gracias a que se dispone de procesadores mucho más potentes. Cuando en los tiempos primitivos se programaba en ensamblador, equivalente a lo que ahora se denomina microprogramación, y en cierto modo el *firmware* también es semejante, los programas eran relativamente breves y muy eficientes porque las disponibilidades de memoria principal eran realmente reducidas y el

proceso de programación era relativamente lento. En la actualidad, con los lenguajes de programación disponibles, no se tarda mucho menos en el proceso de programación, pero en cambio los programas resultantes son bastante más complicados y requieren procesadores mucho más potentes, lo cual nos lleva a plantear la duda de si en realidad son más eficientes.

No se puede evitar recordar que en sectores de la economía básicos, las grandes aplicaciones informáticas todavía funcionan con programas desarrollados en el viejo lenguaje Cobol y nadie se atreve a "modernizar" esos programas en lenguajes más actuales ¿Por qué? Una razón básica en informática es que lo mejor es enemigo de lo bueno, y lo que funciona bien es mejor dejarlo y no tocarlo. Queda mucho por innovar en la rueda informática, pero poco por inventar. Habrá que esperar a la consolidación de los servicios que ofrece la computación en la nube, que no son más que una fórmula novedosa de "outsourcing", de "externalización de servicios", para analizar si se progresa de alguna manera.

La presente monografía tiene sus limitaciones y no pretende ser exhaustiva, pero sí hemos logrado reunir una serie de temas y de autores que nos proporcionan una visión global de la problemática que plantea la computación en la nube, y que tan de moda se ha puesto hoy en día.

En primer lugar, **Enrique Birlanga Terrón**, con más de 17 años de experiencia internacional en el mundo de las tecnologías de la información (TI), y que ha sido consultor de negocio para importantes multinacionales del sector informático, nos expone las tecnologías de infraestructura en la nube intentando analizar y comprender como el desarrollo del *cloud computing* afecta a las tecnologías y más concretamente a las infraestructuras que lo sustentan, proporcionando así una visión general de la computación en la nube.

En segundo lugar, **Guillermo López Moratino**, director de calidad en Prisa Digital y miembro del grupo de trabajo 25 del SC7 del CTN 71 de Aenor que se ocupa precisamente de los temas relativos a la gestión de los servicios de computación en la nube, nos describe como la norma ISO 20000-7 ("Guía para la implantación de la ISO/IEC 20000-1 en la nube"), que en estos momentos se está desarrollando, deberá recoger tanto la óptica del proveedor de servicios en la nube que ha de adaptar su Sistema de Gestión de Servicios (SGS) como la del proveedor de servicios de TI que tiene o está implantando un SGS y que migra a la nube, consumiendo por lo tanto servicios de un proveedor de servicios de nube. La computación en la nube no solo es una

cuestión puramente tecnológica sino que también hace necesario examinar como se regulan las relaciones entre los agentes que participan en sus operaciones, es decir, los proveedores de servicios y los clientes/consumidores/usuarios de esos servicios. Para ello, **Karen Sánchez Quiñones, Ignacio Delgado González e Idoia Uriarte Lauzirika**, abogados con gran experiencia en el tema de los aspectos legales de la Informática y sus tecnologías, exponen cuestiones legales sobre *cloud computing*, tratando sobre la novedad de esta forma de contratar el software como servicio y sobre los conocidos, pero no fáciles de entender por el común de los mortales, SLAs (*Service License Agreements*).

Una de las áreas de la Informática que ha dado lugar a la aparición de la computación en la nube es la utilización del software como servicio, el conocido SaaS. **Ramon Costa Pujol**, responsable del área de Acuerdos y *Partners* del Centro de Innovación en Productividad de Microsoft, responsabilidad que combina con la docencia, nos ofrece, en el cuarto artículo de esta monografía, su apreciación del desarrollo de aplicaciones *cloud* con Windows Azure, explicando cuatro experiencias prácticas y entrando también en las cuestiones de IaaS (*Infrastructure as a Service*), PaaS (*Platform as a Service*) y SaaS (*Software as a service*). Se constata que la mayoría de las compañías son usuarias de aplicaciones en modalidad *cloud* (SaaS) y las grandes organizaciones están migrando su infraestructura a la nube.

Pero la computación en la nube, la *cloud computing*, también presenta su cara peligrosa. Se trata del problema, muy extendido, de la seguridad tanto en cuanto a buen funcionamiento como en la prevención de los peligros planteados por acciones provocadas por agentes externos a la nube.

Para ello presentamos dos planteamientos complementarios, siendo el primero de ellos el que ofrece el profesor **Guillermo Morales-Luna**, Investigador Titular en el Departamento de Computación del Centro de Investigación y Estudios Avanzados del Instituto Politécnico Nacional de México (Cinestav-IPN), quien en su artículo sobre la "Seguridad en el cómputo en la nube" nos reseña los servicios de seguridad y privacidad en el cómputo en la nube debatiendo también sobre la interrelación entre seguridad y eficiencia en el cómputo en la nube, resultando de gran interés las conclusiones que propone.

A continuación, el sexto artículo nos presenta la "Seguridad en la Nube como algo nuevo bajo el sol", en el que **Olof Sandström**, director de Arsys, empresa española que proporciona infraestructura para la nube, argumenta que al *Cloud Computing* se le suelen

atribuir aspectos relacionados con la seguridad que no tienen que ver con el hecho de que los servicios se presten desde la nube, y también que el nivel de seguridad que proporciona un ISP suele ser bastante más elevado que el proporcionado por una empresa en sus propias instalaciones, debido a la alta disponibilidad, cortafuegos, sistemas de detección y prevención, monitorización 24 horas x 7 días a la semana, etc.

Esta monografía no podía evitar, tendríamos incluso que decir que estaba obligada, para completar una visión global de la computación en la nube, a tratar los fallos *post mortem* que acaecen en el entorno de la nube y de la tecnología móvil que la acompaña en numerosas ocasiones. Para ello, el profesor **Jeimy J. Cano**, miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes (Colombia), presenta un análisis forense en un ecosistema tecnológico: redes sociales, tecnologías móviles y computación en la nube. El Dr. Cano plantea una reflexión básica para analizar conductas punibles en un escenario asistido por las redes sociales, las tecnologías móviles y la computación en la nube, un nuevo ecosistema tecnológico que revela la complejidad de las posibilidades y la realidad de la inseguridad en un medio lleno de interrelaciones, intereses y necesidades que invita a repensar nuestra vista tradicional de las investigaciones forenses informáticas.

Para acabar, las referencias útiles citadas más abajo son simplemente ejemplificativas. Existen pocos libros en cualquier idioma que estén al día debido a la constante evolución de las tecnologías utilizadas en la nube y de los conceptos y servicios que se van incluyendo en este concepto. La literatura en español es muy limitada y casi todo lo útil hay que encontrarlo en inglés.

Este editor invitado se pone a disposición de los lectores interesados en temas concretos de la nube para intentar facilitarles en el momento oportuno bibliografía de artículos sobre aquellos aspectos que sean de su interés.

Referencias útiles sobre "Computación en la nube"

Las referencias que se citan a continuación, junto con las proporcionadas en cada uno de los artículos, tienen como objetivo ayudar a los lectores a profundizar en los temas tratados en esta monografía permitiendo contrastar ideas y obtener información actualizada.

Libros

■ **Jordi Torres Viñals.** *Empresas en la nube: Ventajas y retos del Cloud Computing.* Editorial Libros de Cabecera, Barcelona 2011. Primer capítulo descargable desde: <<http://www.librosdecabecera.com/empresas-en-la-nube>>.

■ **Fernando Piera Gómez.** *Todo sobre Cloud Computing.* Editado por la Revista Cloud Computing, junio 2011, <<http://www.revistacloudcomputing.com/2011/07/todo-sobre-el-cloud-computing-2/>>.

Artículos

■ **Pablo de la Cueva.** 3 motivos por los que en España el modelo cloud para las Administraciones Públicas tardará más que en otros países... y al final nos saldrá más caro. *RevistaCloudComputing.com*, septiembre 2011. <<http://www.revistacloudcomputing.com/2011/09/3-motivos-por-los-que-en-espana-el-modelo-cloud-para-las-administraciones-publicas-tardara-mas-que-en-otros-paises-y-al-final-nos-saldrá-más-caro/>>.

■ **Morgan Timothy Prickett.** Atom smasher claims Hadoop migration victory. *The Register*, junio 2011. <http://www.theregister.co.uk/2011/06/30/seamicro_hadoop_benchmark_test/>.

■ **Stacy Collett.** 5 legal gotchas in the cloud, don't sign that contract until you consider five red flags in cloud service deals. *Computerworld*, abril 2011. <http://www.computerworld.com/s/article/355454/Legal_Risks_in_the_Cloud>.

■ **Lucy Sherriff.** Be happy in the cloud with the right SLA, fine print reveals providers' true intentions. *The Register*, junio 2011. <http://www.theregister.co.uk/2011/06/16/cloud_service_level_agreement/>.

Otras publicaciones

■ **Google.** *La guía del cloud computing para la pequeña empresa.* IDG Connect, sección "Whitepapers", julio 2011. <<http://www.idg.es/idgconnect/whitepaper/DescargaWhitepaper.aspx?white=612&or=web>>.

■ **Vmware.** *Cloud Strategy for the Enterprise.* Whitepaper 2011.

■ **IBM.** *The benefits of Cloud Computing.* Whitepaper, julio 2009.

■ **Steven John.** *10 Critical Requirements for Cloud Applications.* Workday blogs, abril 2011, <http://blogs.workday.com/Blog/10_critical_requirements_for_cloud_applications.html>.

■ **Frost & Sullivan.** *Critical Communications for Business Continuity: How to Ensure Employees, Partners & Customers.* Whitepaper, agosto 2011

■ **Frank M. Grillo.** *Unified Communications as a Service for Law Firms: New solutions to address client service, profitability and business continuity objectives.* Whitepaper de Cypress Communications, a Broadvox, company, septiembre 2011. <<http://cypresscom.net/docs/news/WhitePaper-UCaaS-for-Law-Firms.pdf>>.

■ **Liz Herbert, Jon Erickson.** *The ROI Of Cloud Apps.* Forrester, junio 2011. <http://resources.idgenterprise.com/original/AST-0042573_Forrester_Report_The_ROI_of_Cloud_Apps.pdf>.

en resumen Cerrando el círculo: La computación en la nube en la práctica habitual

Llorenç Pagés Casas

Coordinación Editorial de *Novática*

A primeros del año 2010 programamos y editamos dos monografías de *Novática* con la intención principal de proporcionar a nuestros lectores visiones futuristas de hacia donde iba a evolucionar la Informática, dando en ellas especial énfasis al ámbito empresarial.

Se trata de las monografías sobre "*Tendencias en Tecnologías de la Información*" (Novática 204) y "*Ciencia y tecnología de los servicios informáticos*" (Novática 205) donde destacaron en el conjunto de sus contenidos diversos artículos sobre un paradigma, por entonces todavía emergente, como es el de la computación en la nube o *Cloud Computing*, que prometía en aquellos momentos modificar de manera relevante el espectro de posibilidades y oportunidades de empresas y organizaciones a la hora de gestionar sus procesos de datos automatizados.

En aquel entonces y para los meses siguientes, podríamos ya habernos planteado una monografía específica para este tema puesto que las posibilidades que abre la "nube" siguieron resonando a todos los niveles, pero el hecho de haber tratado los aspectos teóricos y los análisis de impacto principales en aquellas

dos monografías nos permitió esperar hasta una mayor consolidación de esta tendencia.

Y esto es en realidad lo que ha sucedido. Así, la monografía del presente número sobre "*Computación en la nube*" cuyo editor invitado es **Fernando Piera Gómez** (especialista en tecnologías avanzadas y ex-Vicepresidente de ATI) representa sobre todo una crónica "viva" de lo que está ya sucediendo ahora mismo en el ámbito empresarial con respecto a la adopción, la oferta y la contratación en la práctica de servicios informáticos que se ejecutan desde la "nube".

De este modo, podemos ofrecer al lector distintas visiones y puntos de vista, tanto sobre tecnología como sobre motivaciones, aspectos legales, estandarización, experiencias, etc. acerca del tema tratado, cosa que siempre suele ser nuestro principal objetivo. Además, en este caso diríamos que cerramos ese círculo que abrimos en 2010 cuando empezamos a hablar de "*Cloud Computing*" como un tema de futuro que ahora nos ha llegado plenamente.

Y hablando de futuro, me queda por comentaros que Novática 216, conteniendo

una amplia monografía sobre "Informática y cultura", va a representar un hito en la evolución de nuestra revista puesto que va a ser el primer número de *Novática* publicado exclusivamente en formato digital (aunque habrá aún números impresos de *Novática* en 2012, ver programación en página 61).

Con motivo de esta oportunidad nos estamos planteando una evolución en contenidos, formatos y propuestas de interacción con nuestros lectores que vamos a ir perfilando en los próximos meses. Por lo tanto, ahora más que nunca vamos (y yo en particular, "voy") a tener abiertos los canales de participación (correo electrónico, blog, foros de socios de ATI, etc.) para que nos enviéis vuestras opiniones y propuestas.

Muchas gracias por vuestra colaboración e interés.



Enrique Birlanga Terrón
 Director de Desarrollo de Negocio en APC
 by Schneider Electric

<enrique.birlanga@gmail.com>

Tecnologías de infraestructura en la nube

Cloud Computing se refiere al uso y acceso de múltiples recursos computacionales basados en servidores a través de una red digital (WAN, conexión de Internet utilizando World Wide Web, etc.). Los usuarios de *cloud* pueden acceder a los recursos de los servidores utilizando un ordenador, tableta, "smartphone", u otro dispositivo.

En *Cloud Computing*, las aplicaciones son proporcionadas y gestionadas por servidores *cloud* y los datos también son almacenados remotamente en la configuración *cloud*. Los usuarios no descargan ni instalan aplicaciones sobre sus ordenadores o dispositivos; todo el proceso y almacenamiento se mantiene en el servidor "cloud" (a partir de ahora "nube"). Los servicios en línea pueden ser ofrecidos desde un proveedor en la nube o por una organización privada. El término "software como servicio" (SaaS) es a veces utilizado para describir aplicaciones de programas ofrecidos a través de computación en la nube.

Los usuarios pueden almacenar remotamente y acceder a ficheros personales tales como música, fotos, videos y juegos; o procesadores de texto en servidores remotos. Los datos son almacenados centralmente, de tal forma que el usuario no necesita llevar un sistema de almacenamiento como un DVD o *pen drive*.

Las aplicaciones de sobremesa que conectan a proveedores de correo electrónico de Internet pueden ser consideradas aplicaciones en la nube, incluyendo las basadas en servicios de correo electrónico *web* como Gmail, Hotmail, o Yahoo. Las compañías privadas pueden hacer uso de sus propios servidores personalizados de correo electrónico en la nube para sus empleados.

El NIST (*National of Standards and Technology*), define cinco características esenciales para la definición correcta de computación en la nube. Las características requeridas para que cualquier solución pueda llegar a ser considerada como "cloud" incluyen:

- Servicios bajo demanda
- Acceso de red abierto
- Recursos de *pooling*
- Rápida elasticidad
- Servicios medidos

Y los tres modelos de servicios o capas de arquitectura se definen según NIST como:

- IaaS – Infraestructura como Servicio

Resumen: Este artículo intenta analizar y ayudar a comprender como el desarrollo del cloud computing afecta a las tecnologías y más concretamente a las infraestructuras que lo sustentan, aportando una visión de la computación en la nube y de como los sistemas DCIM (Gestión de infraestructuras de centros de datos) pueden ayudar a gestionar la capacidad de los sistemas, realizar análisis del impacto que los fallos pueden tener sobre la evolución de los servicios, realizar análisis de costes y dar información sobre la influencia que podrían llegar a tener las infraestructuras en los servicios en la nube.

Palabras clave: Cloud Computing, DCIM, infraestructura en el cloud.

Autor

Enrique Birlanga Terrón tiene más de 17 años de experiencia internacional en el mundo de las tecnologías de la información. Ha sido consultor de negocio para importantes multinacionales del sector de las tecnologías en el ámbito de aplicaciones y sistemas de bases de datos, herramientas de desarrollo de aplicaciones en Internet, plataformas de tecnologías de Televisión Interactiva y en los últimos 8 años, como experto en el mundo de los centros de datos, es responsable del Desarrollo de Negocio de las soluciones para las infraestructuras de los centros de datos. En el último año y medio es el Director de Desarrollo de Negocio para Schneider Electric IT en la plataforma de software de soluciones de gestión y monitorización de los centros de datos, trabajando activamente en la adopción y comprensión por parte de la comunidad informática de los nuevos términos y buenas prácticas que ha de adoptar como es el caso del DCIM (Gestión de infraestructuras de centros de datos).

- SaaS – Software como Servicio
- PaaS – Plataforma como Servicio

Una de las ventajas que tiene la computación en la nube es precisamente su elasticidad para la utilización de los servicios. No es una tecnología nueva, sino un nuevo modelo de entrega de servicios. Esta nueva forma de entregar servicios, no solamente debe ser capaz de disponer de escalabilidad tanto hacia arriba como hacia abajo, en todos los recursos que se utilizan, sino que está estrechamente relacionada con la escalabilidad de los pagos por los servicios.

La gente quiere implementar aplicaciones en la nube privada o acceder a los servicios a través de la nube pública, lo que significa que a los operadores de los centros de datos se les solicita la implementación de la virtualización (un concepto muy desarrollado en la línea de la nube) y las nuevas herramientas de gestión de los nuevos recursos dinámicos que están detrás la computación en la nube.

Hoy en día, la nube presenta una gran dificultad a las personas encargadas de las infraestructuras porque adoptar la "nube" implica la implementación de redundancia en todas las capas de los servicios a proveer.

La creciente adopción de servicios en la nube aporta más a las necesidades de los clientes

para dar flexibilidad, disponibilidad y capacidad que a la reducción de costes. La adopción de los servicios *cloud* es hoy una de las tendencias más fuertes y claras en los centros de datos. Para aquellos centros de datos que soportan servicios en la nube, tanto privados como públicos, esta tendencia ha introducido una multiplicidad de asuntos técnicos y de gestión.

El impacto completo del modelo de la nube sobre el diseño de la infraestructura no ha sido todavía comprendido, aunque se ha argumentado que los centros de datos necesitan ser cada vez más modulares, para que se abandonen los diseños tradicionales con falso suelo y ser sensibles a la volatilidad de Tecnologías de la Información (TI) y las cargas caloríficas. De forma incremental, será requerida una integración de una forma muy ajustada entre las capas físicas y lógicas, así como más monitorización y control de software.

Otro de los elementos importantes para la adopción de los servicios en la nube son los intereses particulares de los clientes. Es el propio cliente/usuario el que está dictando los comportamientos del mercado, demandando unas expectativas a un nivel muy superior. Dentro de las propias organizaciones, el departamento de TI va a tener que facilitar la conectividad y flexibilidad al usuario. Es una

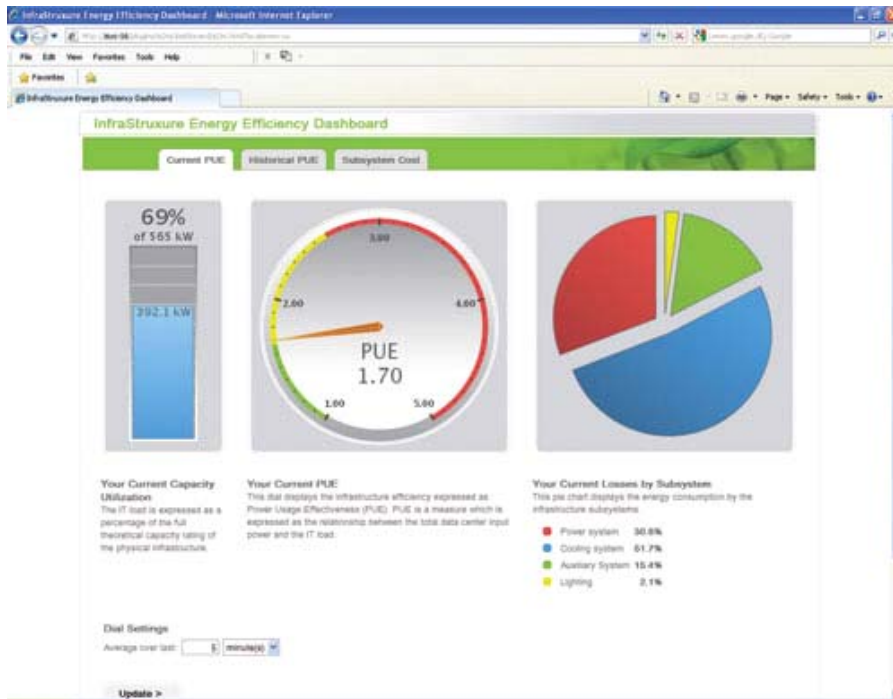


Figura 1. Ejemplo de herramientas DCIM: Panel de gestión de la eficiencia energética.

sensación de necesidad que transforma la negativa a no poder disponer de algo en la actitud de poderlo conseguir de todas formas uno mismo ahí afuera.

Una cosa que se observa con las nuevas aplicaciones es que se maneja un volumen de datos increíblemente superior a los habituales. Incrementar los datos no solo es un reto para la gestión de la infraestructura sino también para los análisis de los modelos de negocio y la gestión del almacenamiento.

Las organizaciones, y particularmente los departamentos de TI, van a pasar por una transformación ya vivida anteriormente como fue el paso de una arquitectura centralizada en grandes computadores y terminales tonos, a disponer de servidores centrales pero con terminales con mucha capacidad de procesamiento, descentralizando rutinas diarias y dando entrada a la era de Internet.

La evolución de las TI volvió de nuevo a los sistemas centralizados reduciendo la necesidad de espacio, gestionando y concentrando la capacidad de procesamiento en equipos más potentes y mucho más utilizados, maximizando los recursos disponibles y dando entrada a nuevos sistemas como la virtualización que ha permitido la adopción de la implementación de la nube; inicialmente a nivel privado para luego explotar y seguir evolucionando estos sistemas hacia el modelo de nube que hoy conocemos. Quiero hacer notar que todavía esto no ha terminado de evolucionar y que en los próximos años esta evolución seguirá su progreso, y donde hoy todavía se hacen muchas labores manuales

pasaremos a la automatización completa sin apenas intervención del ser humano.

Como citó Paul Maritz, Director Ejecutivo (CEO) de VMWare: "Nos estamos moviendo hacia un mundo donde la infraestructura se está convirtiendo en el nuevo hardware. Necesitamos tomarnos esto muy seriamente. Creemos que la infraestructura estará cada vez más automatizada, estandarizada y se utilizará cada vez más como un servicio."

La importancia creciente de esa monitorización y control de software hace necesario sistemas DCIM (*Data Center Infrastructure Management*, es decir "Gestión de infraestructuras de centros de datos") de una forma fácil y sencilla con plataformas abiertas que puedan ser monitorizadas y gestionadas, y que no impliquen grandes esfuerzos de integración con los sistemas existentes o los que en un futuro pudieran ser integrados. De ahí la adopción de usos de protocolos estándar del mercado, como SNMP (*Simple Network Management Protocol*) u otros.

Otro elemento importante para los servicios en la nube son las plataformas donde esta tecnología residirá para su procesamiento y ejecución (infraestructura TI de servidores, sistemas de almacenamiento, etc.). Estos sistemas, para funcionar correctamente, requieren de recursos de infraestructura física "dinámica" (esto es, alimentación eléctrica, refrigeración, etc.), y éstos tienen la necesidad de poder adaptarse a las demandas variables en concepto de alta densidad, disipación térmica, consumo eléctrico variable, etc.

Serán soluciones modulares tanto en sistemas de alimentación modulares como sistemas de refrigeración entre filas que permitan copar con las necesidades generadas por las nuevas tecnologías.

Para la óptima utilización de estos sistemas, se produce un uso más amplio de sistemas que puedan automatizar el inventario, la configuración y gestión de las cargas de trabajo, al mismo tiempo que se usan sistemas de monitorización y análisis.

Una definición del concepto de DCIM mencionado anteriormente sería: "Sistema de Gestión de Infraestructura de Centros de Datos que recoge y gestiona información sobre el inventario del centro de datos, utilización de los recursos y estado operacional. Esta información es distribuida, integrada, analizada y aplicada para optimizar el rendimiento del centro de datos".

Los sistemas DCIM han sido diseñados para interoperar con otros o complementarse entre ellos. El uso de estas plataformas vendrá liderado por la proximidad de trabajar de los sistemas de TI con los mecánicos/eléctricos, que harán la ampliación/unión de las infraestructuras de mantenimiento de los centros de datos, inventario físico de los dispositivos y la virtualización de dichos dispositivos TI.

Los sistemas DCIM ayudan a adaptarse más rápidamente a los cambios técnicos y de negocio, reducir desperdicio y sobre-dimensionamiento innecesario, planificar inversiones y nueva capacidad, reducir los riesgos de fallo, y optimizar el consumo de energía (ver figura 1).

"Cloud" representa así un modelo de negocio que se situará por encima de una infraestructura de centros de datos de gran escalabilidad.

Los retos con la nube son:

- La rapidez en la escalabilidad es crítica
 - Los dispositivos deben ser modulares para escalar rápido.
 - Los subsistemas de mantenimiento deben ser modulares para escalar rápido.
 - La cadena de suministro debe ser mundial para entregas rápidas y predecibles.
- La virtualización crea retos de energía, refrigeración, disponibilidad y eficiencia
 - Alimentación y refrigeración tienen que seguir las cargas virtuales dinámicas para maximizar la eficiencia.
 - La densidad por rack puede ser mucho mayor.
 - Software (VMM) de gestión de máquinas virtuales sofisticado que confíe en sistemas DCIM.

Guillermo López Moratinos
 Director de calidad en PrisaDigital; Miembro del grupo de trabajo 25 sobre "Gestión y buen gobierno de TI" del CTN71/SC7 de AENOR

<glopez@prisadigital.com>

ISO 20000-7: Guía para la implantación de la ISO/IEC 20000-1 en la nube

1. Introducción

La familia ISO/IEC 20000 estandariza en estos momentos los requisitos y guías para la implantación de un Sistema de Gestión de Servicios (SGS) que permita a una organización (independientemente de su naturaleza y tamaño) el alineamiento de su catálogo de servicios de Tecnologías de la Información (TI) con el negocio, así como el aseguramiento de la calidad en la provisión de los servicios, el control y entrega de los mismos, la resolución de incidencias o problemas y la correcta relación del prestador de servicio con sus clientes.

La futura ISO/IEC 20000-7, actualmente en elaboración por los comités de normalización, será la guía de ayuda para la aplicación de la ISO/IEC 20000-1 en la nube. Conviene recordar que la parte certificable es exclusivamente la ISO/IEC20000-1, que estandariza los requisitos para la implantación de un Sistema de Gestión de Servicios (en adelante SGS) y que el resto de partes de la familia exponen guías de implantación del SGS o detallan partes específicas como la definición del alcance, una terminología común, etc.

2. Aspectos de la nueva norma ISO/IEC 20000-7

A continuación expondré lo que, en mi opinión personal, serán aspectos importantes en la futura norma.

En primer lugar, considero fundamental que la norma **defina correctamente su apar-**

Resumen: En estos momentos se está procediendo dentro de los comités técnicos de ISO/IEC a la votación para la aprobación de un nuevo trabajo dentro de la serie de documentos de ISO 20000, que aportará las guías para la adopción de la norma ISO/IEC 20000-1 en entornos cloud. El presente artículo expondrá una opinión personal acerca del contenido que la futura parte 7 de la norma debería contener, ya que conformará la guía de ayuda que analizará las consideraciones específicas de un Sistema de Gestión de Servicios en un entorno cloud y que, en opinión del autor, deberá recoger tanto la óptica del proveedor de servicios en la nube que ha de adaptar su SGS (Sistema de Gestión de Servicios) como la del proveedor de servicios de Tecnologías de la Información (TI) que tiene o está implantando un SGS y que migra a la nube y por tanto consume servicios de un proveedor de servicios de nube.

Palabras clave: Cloud, gestión, ISO20000, nube, SGS.

Autor

Guillermo López Moratinos es director de calidad en PrisaDigital y miembro del grupo de trabajo GT25 sobre "Gestión y buen gobierno de TI" del CTN71/SC7 de AENOR coordinando el grupo ISO/IEC DIS 27013. Es además miembro del grupo de trabajo Difusión ISO 20000 itSMF. Es Ingeniero Superior en Informática por la Universidad Autónoma de Madrid (UAM) y posee certificados de AENOR de Auditor de Sistemas de Gestión de Servicios y de Especialista implantador de sistemas de gestión de seguridad de la información (CISA/CRISC).

tado de alcance, de manera que suponga una guía tanto para el **proveedor de servicio de nube** (quien ofrece nube, cualquiera que sea el tipo) como para el **proveedor de servicio de TI que está considerando su migración a nube** (que va a consumir servicios de proveedor de nube y para el que surgirán necesidades adicionales de gestión de procesos operados por terceras partes de la manera en que se describe en la ISO/IEC 20000-1: cláusula 4.2), y de alineamiento de determinados procesos cuya operación saldrá de su ámbito en parte y entrará en la nube.

Esto no exime de sus responsabilidades al proveedor de servicios de TI ya que la responsabilidad del SGS es suya como prestador de servicio y no del prestador de servicio de nube, y por tanto, aunque la nube le de ventajas en determinados procesos tendrá que cuidar de gestionarlos adecuadamente (ver **figura 1**).

Por poner un ejemplo, el proveedor de servicio de nube será responsable de operar la capacidad de la infraestructura que el proveedor de servicio de TI consume, pero el responsable de capacidad del proveedor de servicio de TI

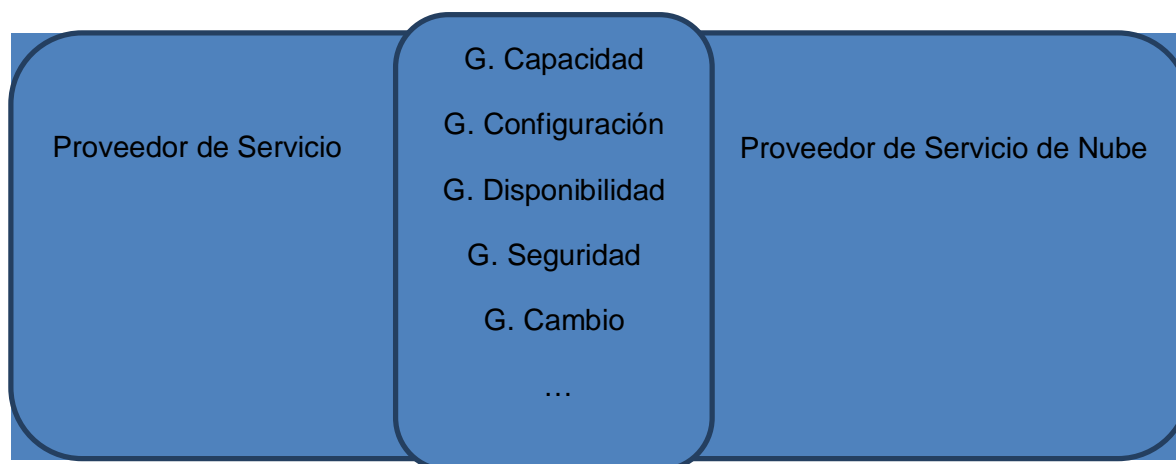


Figura 1. Responsabilidades de gestión de los proveedores de servicios que se basan en servicios de nube.

deberá monitorizar, controlar y gestionar la forma en que el proveedor de servicio de nube le está gestionando la capacidad. Por lo tanto, todo se basará en la correcta **operación del proveedor de servicio de nube y en la gestión del proveedor de servicio de TI** (que es cliente del proveedor de servicio de nube).

Es decir, el proveedor de servicio de nube de cara a su propio SGS es responsable de gestionar sus procesos, pero de cara al SGS del proveedor deberá asegurar la operación de dichos procesos, ya que la responsabilidad de gestión es de su cliente, el proveedor de servicio que ha llevado sus servicios a la nube y que deberá encargarse de que los procesos de ambos estén alineados, las métricas y formas de medición acordadas y las responsabilidades claramente definidas.

La norma habrá de considerar las diferentes **modalidades de nube**, tanto bajo el prisma del **qué se lleva a la nube** (IAAS, SAAS, PAAS) como de **cómo se lleva a la nube** (privadas, públicas, híbridas) y quizá **exponer alguna recomendación al respecto de qué aspectos debería valorar una organización a la hora de elegir el tipo de nube** al que migrar servicios dentro del alcance del SGS. Por ejemplo, un proveedor de servicio cuyo alcance del SGS incluya el servicio de correo electrónico a sus clientes, podría migrar el correo a nube pública, al tratarse el correo electrónico de un servicio estandarizado, muy consolidado, cuya migración a nube pública permite beneficiarse de un ahorro significativo del coste, de una mayor escalabilidad y autoservicio, pero sin comprometer la gestión de dicho servicio al tratarse de un servicio ampliamente estandarizado en el sector.

O bien, un proveedor de servicio que esté implantando o haya implantado un SGS podrá decidir migrar a nube privada un servicio específico de su negocio que si bien requiera autoservicio y escalabilidad no disponga de una estandarización *out-of-the-box* que le permita ir a una nube pública compartida con otros clientes, y tenga así mayores requisitos de gestión personalizada (privada), pudiendo requerir escalar a nube pública (modelo híbrido) ante situaciones puntuales de demanda (picos).

Será aconsejable que la norma enumere de forma breve, y sin con ello pretender que la enumeración sea completa, algunos de los **principios vertebradores del paradigma cloud**, como son el **pago por uso**, la **escalabilidad** con un tiempo mínimo de provisión, el **autoservicio** por parte del cliente de servicios de nube, la necesaria **estandarización de las TI** que permita la **automatización** en la provisión, monitorización y control de los activos de

información, así como la **transparencia** como elemento necesario para generar confianza no solo en el servicio consumido sino en la **seguridad** del mismo.

Exponer en la norma los principios fundamentales del cloud permitirá desarrollar a continuación la guía en que el SGS ha de implantarse. Por ejemplo, por poner uno solo de los muchos casos que una implantación de un SGS en nube deberá considerar, el proveedor de servicio de nube deberá definir y estandarizar el catálogo de servicios que ofrece en nube, de manera que la estandarización de cada servicio posibilitará la automatización en la provisión, monitorización y control, y esto permitirá el autoservicio. Es lo que denominaría **la cadena de valor de la nube:**

Definición – Estandarización – Automatización – Control – Autoservicio/Escalado – Transparencia

(aquí cada guión debe leerse como "posibilita").

Es decir, en este ejemplo la nube estará siendo eficaz si un cliente puede autoservirse o escalar en caso de necesidad (evitando flujos adicionales de contratación) de manera que en un tiempo prácticamente inmediato disponga de los recursos que requiere. Para eso el catálogo de servicios deberá ser estándar, la provisión automática y el elemento que se provisiona a cliente de forma casi inmediata deberá estar monitorizado y controlado (CMDB, *Configuration Management DataBase*), de manera que todos los elementos deberán estar automatizados y controlados, para que esté gestionada su seguridad, configuración, capacidad, disponibilidad, etc.

Es decir, **la nube es enemiga de la indefinición**, requiere de un esfuerzo de estandarización, automatización, medición y seguridad que genere la confianza necesaria en la calidad del servicio.

Expuestos ya los distintos alcances de aplicación de la ISO/IEC 20000-7, los distintos tipos de nube con algunas recomendaciones al respecto de qué aspectos debería valorar una organización a la hora de elegir el tipo de nube, y los principios generales del *cloud*, la norma podrá abordar entonces uno por uno los apartados de la ISO/IEC 20000-1 deteniéndose exclusivamente en aquellos elementos que son objeto de comentario o guía adicional.

No pretendo, al menos en este artículo introductorio, entrar a desgranar los aspectos relevantes que un SGS en nube deberá considerar por cada uno de los 13 procesos de la ISO/IEC 20000-1, pero sí quería destacar la importancia de desarrollar suficientemente

el proceso de **gestión de la seguridad**, haciendo especial hincapié en los aspectos relacionados con la LOPD.

Quiero mencionar este punto porque, rompiendo una falsa creencia del sector, **la nube no es sinónimo de inseguridad, es decir, la nube no constituye más que un paradigma tecnológico y será la forma de implementarla y gestionarla lo que provocará una mayor o menor seguridad** de los activos de información, lo cual es aplicable a cualquier implantación hoy en día.

Un *firewall* por sí solo no nos dará mayor seguridad si no lo configuramos y gestionamos adecuadamente y el modelo *cloud* no supondrá un riesgo de seguridad si elegimos adecuadamente el tipo de nube que se ajusta al tipo de servicio que vamos a migrar y seleccionamos un proveedor de nube confiable, bajo el marco de un acuerdo de nivel de servicio que preste, por ejemplo, especial atención a las subcontrataciones que el proveedor de nube pudiera requerir hacer para prestarnos el servicio o al ámbito geográfico (UE o fuera de la UE) desde el que vaya a prestarlo, ya que el control y la gestión adecuados por parte del proveedor de servicio de TI (cliente de la nube) de estos aspectos serán clave en el cumplimiento de la LOPD (Ley Orgánica de Protección de Datos) y en la correcta gestión de la seguridad.

3. Conclusión

Quisiera cerrar este artículo indicando mi firme creencia de que la futura ISO/IEC 20000-7 constituirá una guía fundamental para asesorar a los proveedores de servicio de TI (clientes de nube) y proveedores de servicio de nube en la implantación del SGS y reiterar a modo de conclusión que la nube requiere un esfuerzo adicional de estandarización tanto de las Tecnologías de la Información como de la gestión de dichas TI, como elemento posibilitador del automatismo, que a su vez posibilite el autoservicio...

Esta realidad hace hoy más que nunca que la ISO 20000-1 sea absolutamente necesaria para cualquier prestador de servicio que quiera prestar un servicio de calidad a sus clientes.

Karen Elizabeth Sánchez Quiñones¹, Ignacio Delgado Gonzalez¹, Idoia Uriarte Lauzirika²

¹Socios de BDS Abogados, ²Directora Gerente de tuCloud S.L.

<ksq@bdsabogados.com>,
<idg@bdsabogados.com>,
<uriarte.idoia@gmail.com>

1. Introducción

La computación en nube (*Cloud Computing*) es la entrega de la computación como un servicio más que cómo un producto, mediante el cual los recursos compartidos, software, e información se proporcionan a los ordenadores y otros dispositivos como un servicio de acceso al público en general (como lo es la red eléctrica) en una red (generalmente Internet).

El término "nube" se utiliza como una metáfora de la Internet, basada en el dibujo de nubes utilizado en el pasado para representar a la red telefónica, y más tarde para representar el Internet en los diagramas de red de computadoras, como una abstracción de la infraestructura subyacente que representa.

Como es de esperar con cualquier cambio revolucionario en el panorama de la computación a nivel internacional, surgen ciertos problemas legales; desde problemas de seguridad, como infracción de la propiedad industrial e intelectual, marcas, intercambio de datos personales y propiedad de recursos.

La utilización del *Cloud Computing* puede ayudar a las organizaciones a reducir los costos ya que no tienen que invertir tanto dinero en equipos hardware y la infraestructura física, dado que sus datos se almacenan en un lugar seguro y sólo se paga por el uso y derechos de licencia relacionados con la computación en nube.

2. Aspectos legales relacionados con el Cloud Computing

Hay algunas importantes cuestiones jurídicas que deben tenerse en cuenta antes de firmar un contrato con cualquiera de los proveedores de la nube para su organización, empresa o institución.

2.1. La ubicación física de sus datos

2.1.1. ¿Dónde se almacenan los datos físicamente?

Sus datos pueden ser almacenados en cualquier país y puede que ni siquiera se sepa dónde se encuentra el centro de datos. La "ubicación física" plantea la cuestión de la jurisdicción aplicable sobre los datos allí almacenados.

El cliente debe tener claro qué disposiciones de la legislación vigente son aplicables en ese Estado (jurisdicción) en particular.

Cuestiones legales sobre Cloud Computing

Resumen: Dada la novedad de esta forma de contratar el software como servicio, en este artículo tratamos aspectos a tener en cuenta a la hora de contratar con proveedores de software, en concreto los niveles de exigencia de dicho servicio con los SLAs (Service License Agreements), así como la titularidad de los derechos de propiedad industrial e intelectual, y aspectos de protección de datos personales e información confidencial. También proporcionamos una visión técnica de cómo adaptar las organizaciones a los servicios que se pueden obtener a través de la nube, como es por ejemplo el escritorio virtual.

Palabras clave: Cloud computing, copyright, escritorio virtual, propiedad industrial, propiedad intelectual, protección de datos, Service License Agreement, SLA.

Autores

Karen Elizabeth Sánchez Quiñones obtuvo el título de Licenciada en Derecho en 1999 por la Universidad Complutense de Madrid, siendo experta universitaria en gestión de la Innovación Tecnológica y en Ayudas y Subvenciones de la Unión Europea. Es socia de BDS Abogados desde 2009, cuya especialidad es el área de Nuevas Tecnologías de desarrollo y asesoramiento jurídico con empresas españolas y extranjeras, tanto en contratos de investigación como de colaboración entre universidades, *Joint Ventures*, biotecnología y nanotecnología, propiedad intelectual e industrial, implantación de la normativa de protección de datos y Ley de Servicios de la Sociedad de la Información española e internacional.

Ignacio Delgado González es licenciado en Derecho por la Universidad de Deusto, MBA por la ESTE de San Sebastián, y Master en Comercio Exterior por la UPV. Ha colaborado con el ESI (*European Software Institute*) en el programa ECUA, ponente de un "paper" en Redondo Beach California en el ICCBSS (*International Conference on Composition-Based Software Systems* – III Conferencia Internacional sobre COTS, *comercial off-the-self*) en febrero de 2004, y ponente en un tutorial de la IV Conferencia Internacional sobre COTS (ICCBSS), celebrada en Bilbao en febrero de 2005. Además, ha impartido ponencias sobre aspectos jurídicos del software, sitios web y protección de datos personales en Bizkaia Empresa Digitala, Araba Empresa Digitala, CEBEK y ASLE. Trabaja en temas de asesoramiento jurídico sobre derecho de las nuevas tecnologías para empresas de distintos sectores. Es socio de BDS abogados desde 2009.

Idoia Uriarte Lauzirika es una profesional con un fuerte carácter emprendedor. Tras finalizar su carrera como Ingeniera en Telecomunicaciones en la Universidad de Deusto, cursó un Master en Gestión de Redes y Sistemas, y actualmente está cursando un MBA (*Master in Business Administration*) en la Escuela Europea de Negocios. A lo largo de 6 años ha participado activamente en el lanzamiento de varios proyectos empresariales centrados en el sector de la Virtualización de Escritorios y ha publicado un libro junto con Michael Fox (experto en Virtualización de Escritorios) titulado "Desmitificando el Escritorio Virtual". Actualmente está inmersa en el lanzamiento de una plataforma online creada para impulsar el comercio local y participa activamente tanto organizando como fomentando eventos de *Networking* con un amplio grupo de empresarios.

2.1.2. Si surge una controversia

Por ejemplo en el caso de un conflicto entre el proveedor de la nube (EEUU) y el cliente (España), ¿Cuál será el lugar de la competencia jurisdiccional (fuero aplicable)? ¿Qué sistema judicial y qué legislación resolverá el conflicto?

Siguiendo con el ejemplo, el proveedor definitivamente prefiere zanjar el asunto en un tribunal estadounidense, y como el cliente, no tiene los medios financieros y recursos para solucionar la controversia en la jurisdicción de otro país, queda desamparado.

2.2. Responsabilidad de los datos

¿Qué pasa si el centro de datos se ve afectado por un desastre?

Puede ocurrir que las instalaciones del proveedor se vean seriamente afectadas debido a un desastre. Incluso las presentaciones de Google Inc. en la *Securities and Exchange Commission* de los EE.UU. mencionan ese riesgo:

"Nuestros sistemas son vulnerables a los daños o la interrupción de los terremotos, ataques terroristas, inundaciones, incendios, pérdida de energía, fallos en las telecomunica-

ciones, los virus informáticos, la negación del equipo de los ataques del servicio, o de otros intentos para dañar nuestros sistemas".

Es algo que puede ocurrir por lo que se tendrá en cuenta por el responsable de las Tecnologías de la Información y la Comunicación (TIC) de la organización, empresa o institución.

2.2.1. ¿Hay alguna cobertura de responsabilidad civil por violación de la privacidad?

Si una violación de la privacidad se produce debido a un fallo del proveedor de la nube, ¿hay alguna política de cobertura de responsabilidad asumida por el proveedor? El alcance de la violación de la privacidad se ha ampliado considerablemente en los últimos años en el ámbito de los seguros de riesgos cibernéticos.

2.2.2. ¿Qué se puede hacer si el centro de datos es pirateado?

A pesar de que todos los proveedores de la nube hacen todo lo posible para defenderse de los piratas informáticos, la configuración de seguridad no se supone que sea infalible.

2.3. Derechos de Propiedad Intelectual

2.3.1. ¿Están sus datos protegidos por derechos de propiedad intelectual?

Si sucede que los datos son de su propia creación (como las fotografías, contenidos, etc.), entonces hay que comprobar que estén protegidos bajo los derechos de propiedad intelectual de ese país y en caso de infracción cómo se defienden.

2.3.2. ¿Son seguros los secretos comerciales?

Los datos almacenados en la "nube" pueden contener secretos comerciales o información privilegiada que debe ser protegida como en la relación abogado-cliente.

Podemos pensar en una situación inversa; si al proveedor de servicios en la nube se le escapa un secreto comercial de otra entidad comercial.

2.3.3. El acceso de terceros

El proveedor puede otorgar a algunos terceros un acceso privilegiado a los datos almacenados. La identidad de las partes, si las hubiere, debe ser revelada al cliente. Aquí, el tercero puede ser una autoridad judicial o un empleado interno. El cliente siempre debe ser informado antes de que el proveedor permita que terceros tengan acceso a los datos almacenados.

Así, para proteger los intereses de su negocio es extremadamente importante leer los términos y condiciones cuidadosamente antes de suscribirse a un servicio basado en la nube.

Si el vendedor ofrece un formulario estándar de contrato (que es una práctica general),

entonces como cliente debe ser plenamente consciente de que todos los términos y condiciones se aplicarán, esto es el contrato entre las partes. Le ahorrará sorpresas desagradables y debe estar preparado tanto financiera como legalmente para salvar su negocio de las posibles consecuencias desfavorables de la computación en la nube.

2.4. Responsabilidad por los datos ilegales

Se estima la responsabilidad del proveedor de servicios en la nube de los contenidos ilegales en muchas jurisdicciones: los proveedores de la nube pueden ser considerados responsables de los datos ilegales que pueden ser objeto de alojamiento en comercio electrónico. La Directiva (2000/31/CE) introdujo la protección especial de responsabilidad para los proveedores de alojamiento: *"no se hace responsable por los servicios que consisten en el almacenamiento de la información electrónica bajo la condición de que el proveedor no tiene conocimiento o conciencia de la ilegalidad... y elimina o bloquea los datos de ilegal cuando se adquiere conocimiento y toma de conciencia de la ilegalidad (notificación y retirada)".*

La responsabilidad de proveedor de servicios en la nube de problemas de contenido ilegal: la protección especial se centra en el almacenamiento, y no tiene en cuenta las actividades de procesamiento. Existe gran cantidad de jurisprudencia de ello (en particular en Francia) que no ofrece protección cuando los servicios no se compongan exclusivamente de cobertura de responsabilidad civil de almacenamiento de las actividades y no evita las medidas cautelares, que puede ser tan costosas y consumen mucho tiempo dado que no existe una norma de notificación.

2.5. Las cuestiones de cumplimiento

Las cuestiones acerca del cumplimiento de las obligaciones de retención de datos son requisitos relacionados con el almacenamiento impuestos por la legislación de facturación electrónica de comercio electrónico, así como la legislación de firma electrónica.

2.6. Los problemas de contratación

Por un contrato que parece de poca importancia, la responsabilidad es tan grande que los servicios de *Cloud Computing* ofrecen escasas barreras a la entrada y son fáciles de aplicar las prácticas de "acuerdos *click-wrap*" (como en las licencias de software con abrir el paquete se entiende aceptado el contrato) que en todo caso tienen fuerza legal.

Muchos contratos de computación en la nube limitan la responsabilidad del proveedor de alojamiento a un nivel que no está de acuerdo con los contratos de riesgo potencial de *Cloud Computing*. Al final parecen típicas licencias de software, aunque el riesgo potencial es mucho mayor.

Un ejemplo de estas cláusulas son:

"Nosotros y nuestros licenciantes no serán responsables de cualquier interrupción del servicio, incluyendo, sin limitación, los apagones, fallos del sistema o interrupciones, incluyendo las que afectan a la recepción, procesamiento, aceptación, finalización o liquidación de los servicios de pago. (...)

Ni nosotros ni ninguno de nuestros licenciatarios serán responsables ante usted por daños directos, indirectos, incidentales, especiales, consecuenciales o punitivos, incluyendo pero no limitado a, daños por pérdida de ganancias, buena voluntad, uso, datos u otras pérdidas (...)"

Otra cuestión contractual referente a los proveedores de tecnología es que no hay ningún requisito legal para que un proveedor ofrezca los servicios de exportación de datos, todo depende de su acuerdo contractual, ya que existe libertad de negociación entre partes, y si se produce una resolución unilateral por parte del proveedor de *Cloud Computing* a menudo se reserva el derecho de suspender unilateralmente su participación en la prestación de múltiples servicios sin un solo punto de contacto.

En referencia a otros requisitos contractuales de auditoría, muchos contratos imponen la posibilidad de auditoría que incluye la inspección física, pero ¿cómo se pueden cumplir estos requisitos de auditoría cuando se utilizan servicios de *cloud* geográficamente descentralizados?

Si la Ley aplicable y jurisdicción competente son de otro Estado, cualquier litigio puede llegar a ser prohibitivo. Y por otro lado, ¿Qué sucede en caso de quiebra del proveedor?

3. Los acuerdos de nivel de servicio (SLA)

Las organizaciones, empresas e instituciones suelen delegar en la nube aplicaciones críticas que al final vendrán definidas en un contrato. Si el contrato es de arrendamiento de servicios se deben definir los parámetros de exigencia de servicio en el acuerdo de nivel de servicio (*Service License Agreement, SLA*).

Este Acuerdo de Nivel de Servicio es importante en cualquier contrato de servicios de computación, desarrollo de software, bases de datos, etc. pero es crucial en un contexto de computación en nube.

Hay varios puntos de atención: ¿Cómo se calcula la disponibilidad dispensada por el proveedor? *Por ejemplo, 10 cortes de 6 minutos frente a un apagón de una hora de medición independiente de la actuación.*

Como se verá a continuación, la mayor parte de las cuestiones planteadas anteriormente

deben ser explícitamente contestadas y acordadas con el proveedor del servicio de *Cloud Computing* a través del documento esencial que es el Acuerdo de Nivel de Servicio (SLA).

Cuando una organización ha elegido los sistemas de los proveedores para ofrecer sus servicios, ha de acordar previamente con esos proveedores un cierto nivel de calidad en el servicio que ofrezcan, lo cual puede suponer un riesgo si no se llega a un acuerdo conveniente para las dos partes.

El modelo de Acuerdo de Nivel de Servicio (SLA) consiste en un contrato en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes.

Se refleja contractualmente el nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad por fallos en el servicio, etc.

Fases de implantación de un SLA:

- 1) Definición de objetivos: mejora de la eficacia, reducción de costes, formalización de la relación, etc.
- 2) Identificación de expectativas: qué es lo que espera la organización del acuerdo.
- 3) Optimización o rediseño de procesos: cómo se gestionarán los servicios y los procesos de comunicación entre el proveedor y el cliente (gestión de incidencias, auditoría de la información en la nube, etc.) para que sean lo más eficientes posibles.

Los principales errores a la hora de elaborar un SLA suelen ser: definir niveles de servicio inalcanzables, regulación excesiva, mala asignación de las prioridades, excesiva complejidad técnica, etc.

Así, los principales puntos que debe cubrir el acuerdo son:

- Tipo de servicio (adaptabilidad).
- Garantías del sistema y tiempos de respuesta.
- Disponibilidad (sanciones por caída del sistema).
- Conectividad.
- Provisiones para seguridad y datos (*backup*, pérdidas).
- Cumplimiento de la ley vigente (por ejemplo, la Ley de Protección de Datos).
- Migración de datos, estandarización.
- Soporte a clientes y asistencia.
- Seguridad en la gestión de la información.

Dado que la información de la organización se transmitirá a través de Internet, es necesario establecer un sistema seguro de comunicaciones contra posibles amenazas o corrupción de los datos. Para garantizar la seguridad, en ciertos casos la información deberá estar encriptada o protegida.

Por otra parte, no se puede pensar que controlar los datos es tan sólo una cuestión técnica, también es algo procedimental: no se deben firmar contratos de exención de responsabilidades o delegar absolutamente todo en los proveedores como la mejor forma de gestionar la seguridad.

Siempre se debe garantizar el acceso autorizado a la información gestionada en la nube, los usuarios deben disponer de un inventario de la información aportada al proveedor de *Cloud Computing*, garantizando que esa información está correctamente clasificada.

4. El cumplimiento con la legislación vigente de protección de datos personales en Cloud Computing

En la Unión Europea (UE), la privacidad y la protección de datos se desarrollan en la Directiva 95/46/CE y transposiciones de cada uno de los Estados Miembros como es, por ejemplo, la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD). Las normas y reglas de la UE son mucho más restrictivas que las normas de otros países (especialmente EE.UU.).

La privacidad y la protección de datos de computación en la nube se exponen a la aplicación de la formalidad y complejidad de las leyes vigentes, ya que muchas cuestiones legales no se han resuelto por completo. Tres ejemplos de estos problemas son: ¿Quién es el controlador? ¿Qué ley se aplica? ¿Qué ocurre si hay transferencia de datos fuera de la UE?

Entre "los responsables del tratamiento" y "los datos de los procesadores", la legislación hace una distinción fundamental entre tratamiento de los datos (en el cual se define y realiza el objetivo) y los medios de procesamiento de datos: "el artista mudo". La distinción es crucial para saber quién es el responsable del tratamiento de datos y quién es responsable ante el controlador de datos, que debe elegir procesadores de datos apropiados, y debe buscar la protección contractual adecuada de los mismos.

La ley de protección de datos de la legislación nacional en un Estado miembro de la UE se aplicará cuando el establecimiento en que se base el controlador en la Unión Europea se encuentre en su territorio.

Cuando los procesos de tratamiento de datos personales están fuera de la UE se utiliza el concepto de "equipo" dentro del territorio, que aplica a la computación en nube del centro de datos con sede en la UE. La mayoría de las autoridades interpretan el concepto de "equipo" de una manera muy amplia (incluso las *cookies* del navegador).

En cuanto a la transferencia de datos fuera de la UE, en principio no hay transferencia de

datos de países fuera de la UE que no ofrezca un "nivel adecuado de protección", salvo las excepciones de Suiza, Argentina y Canadá, pero se podrá pedir permiso a todos los "interesados" involucrados si la transferencia fuera necesaria para ejecutar contratos con dichos interesados.

Para los EE.UU., la suscripción a la "lista de puerto seguro", "normas empresariales vinculantes" de acuerdo con la Comisión Europea, define el modelo de transferencia de datos fuera de la UE en la práctica. Así sólo se utiliza el proveedor de la nube con los centros de datos dentro de la UE. Por ejemplo, Amazon EC2 con elección del lugar (este de EE.UU., oeste de EE.UU. o Irlanda), o asegurándose de que el modelo de acuerdo se haya concluido con el proveedor de la nube.

Es necesario asegurarse de que la información en la "nube", cumple con la normativa legal de gestión de la información y plantear estos aspectos debidamente revisados a la empresa proveedora del servicio de *Cloud Computing* antes de firmar el acuerdo de nivel de servicio que se explicó en el punto anterior.

En España, destaca la obligatoriedad de cumplir con la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), una de las cuestiones que más preocupación causa entre las empresas que tratan datos personales a la hora de adoptar servicios de *Cloud Computing*, en los cuales este tipo de datos se vean involucrados. Antes de abordar esta cuestión, cabe señalar que las condiciones a cumplir por los servicios de *Cloud Computing* son idénticas a las aplicadas a los tradicionales servicios de *hosting*, por lo que muchas empresas estarán familiarizadas con estos requisitos.

Según la LOPD, en este caso la empresa responsable del tratamiento de los datos personales de los usuarios gestionados en una aplicación será aquella que contrata el servicio de *Cloud Computing*, definiendo a su vez un segundo rol denominado "Encargado del Tratamiento" que corresponderá a la empresa tercera que ofrece el servicio de *cloudy* que será la que almacene físicamente la información en sus instalaciones.

Para formalizar esta asignación de responsabilidades y garantizar que la comunicación de los datos personales y su posterior tratamiento son legales, deberá existir un contrato formal de prestación de servicio entre el Responsable de la Información y el Encargado del Tratamiento (según la LOPD, "la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido").

Por otra parte, en este caso corresponde al encargado del tratamiento (la empresa que ofrece el servicio en *cloud*) elaborar el documento de seguridad e implementar las medidas adecuadas de seguridad sobre la información, entre ellas la gestión de incidencias, la realización de copias de respaldo, criterios de archivo, almacenamiento y traslado de la información, realización de auditorías, etc. Dichas medidas dependerán, entre otros aspectos, del nivel de privacidad definido en la LOPD que corresponda con los datos personales almacenados en la aplicación.

Asimismo, al tratarse de una prestación de servicios no es necesario obtener el consentimiento de los titulares de los datos para que la tercera empresa pueda tratarlos (art. 12 de la LOPD).

Finalmente, deben tenerse presentes los aspectos recogidos en la Ley relativos al movimiento internacional de datos. Dado que cabe la posibilidad de que los servidores que almacenan físicamente la información no se encuentren en el territorio nacional, deberá obtener "autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas".

5. Adaptabilidad de la organización a la "nube"

Puede ocurrir que la empresa pretenda externalizar ciertas aplicaciones ya implantadas en su organización hacia el modelo de *Cloud Computing*. Si bien las ventajas pueden ser muy numerosas, también es cierto que las aplicaciones deberán estar adaptadas a la infraestructura que ofrece la "nube", que comúnmente está formada por arquitecturas o sistemas muy paralelizables, es decir, que realizan trabajos conjuntamente entre varios sistemas. Esto implica que las ventajas competitivas que pueda ofrecer *Cloud Computing* sólo podrán maximizarse si las aplicaciones que se migran desde una empresa a la nube están adaptadas a ellas.

Además, los formatos de los datos que se manejan han de ser lo suficientemente estándar como para poder encontrar algún software en la nube con el que se pueda evolucionar, es decir que permita su adaptación a nuevas versiones sin necesidad de realizar grandes cambios.

Por todas estas razones, puede ser necesario rediseñar las aplicaciones de una empresa para su adaptación eficiente a la "nube". Los posibles tipos de adaptación son:

- 1) Adaptación total: El nuevo sistema se adapta de forma radical. Es recomendable para organizaciones que aún no tienen un sistema de información adaptado a su proceso de negocio.
- 2) Adaptación con mantenimiento: El nuevo

sistema y el sistema antiguo conviven durante un tiempo, evitando en la medida de lo posible la información compartida entre éstos para no dar lugar a errores. Es recomendable para organizaciones que puedan adaptar los nuevos negocios al sistema nuevo y la información almacenada sobre procesos más antiguos no sea necesaria para ellos.

3) Adaptación parcial y gradual de los servicios evitando cambios bruscos. Esta opción es similar a la anterior pero en este caso el proceso se desarrollará de forma más lenta, siendo posible mantener en funcionamiento tanto el sistema antiguo como la aplicación en *Cloud Computing* tras su implementación.

5.1. Estandarización de los sistemas de la "nube"

Los sistemas que utilicen los proveedores del *Cloud Computing* han de cumplir ciertos estándares que faciliten el uso de sus servicios asociados. Para ello, esos sistemas deberán estar diseñados de acuerdo al cumplimiento de ciertas normativas proporcionadas por diversos organismos internacionales de estandarización, o por asociaciones que agrupen a la mayoría de los proveedores con el objetivo de que sus sistemas sean interoperables entre sí, y su comunicación y funcionamiento conjunto sea lo más eficiente posible.

La mayor ventaja de la estandarización radica en la posibilidad de migrar las aplicaciones a otro proveedor o entorno con mayor facilidad, ya que si no se utilizan formatos estandarizados, en la mayoría de los casos la adaptación será más costosa.

5.2. Control sobre los servicios ofrecidos en la "nube"

Las organizaciones que hagan uso de los servicios ofrecidos por el *Cloud Computing* han de acordar o crear ciertos sistemas de control sobre los mismos para poder optimizarlos en conjunción con el proveedor de servicios de acuerdo con las necesidades de la organización.

5.3. Disponibilidad de los servicios

En cuanto a la disponibilidad, se ha de negociar con el proveedor un acuerdo de nivel de servicio que especifique una garantía de acceso continuo a los servicios con una calidad mínima. Asimismo, una empresa debe plantearse seriamente la cuestión ¿Qué ocurriría si no se dispusiera de acceso a Internet?

En este punto la empresa debe valorar el impacto que su negocio o gestión sufriría en caso de indisponibilidad de alguna de las aplicaciones desplegadas en *cloud* y las probabilidades de que esto ocurra.

Por otra parte, es necesario analizar las posibles soluciones existentes en situaciones de indisponibilidad tanto desde el punto de vista del proveedor como de la empresa.

Algunas de ellas son:

- 1) Escoger aplicaciones que ofrezcan la posibilidad de trabajar en modo *offline*, para lo que pueden incorporar herramientas como Google Gears, por ejemplo Zoho Writer y Zoho Mail.
- 2) Contratación de una línea alternativa RTB (Red Telefónica Básica) o RDSI (Red Digital de Servicios Integrados), de forma que en caso de indisponibilidad de la línea ADSL se permita conexión a Internet para la aplicación. Asimismo, se puede contratar una nueva línea ADSL a un proveedor diferente para situaciones de emergencia, esto es, de menor capacidad y por lo tanto de menor coste.
- 3) Adquirir un acceso 3G con conexión al PC a través de USB en el que se efectúa pago por consumo.

Por supuesto, en cualquiera de estas situaciones será necesario evaluar los costes y la adecuación de contratar servicios de *Cloud Computing* en función de la criticidad del proceso en el seno de la organización.

5.4. Personal de soporte para los servicios ofrecidos en la "nube"

En muchos entornos se tiende a pensar que con la irrupción de los servicios ofrecidos en la nube se reducirá la necesidad de personal técnico en las empresas, y esto en la situación económica actual genera un cierto rechazo desde los departamentos técnicos. Si bien esa reducción se puede llegar a dar, no será tan dramática como se describe desde varios sectores.

La tendencia cambia de dirección y ahora las empresas, en lugar de requerir de un gran número de técnicos de un nivel medio-bajo para dar servicio de soporte al personal de la compañía, requerirán de más profesionales técnicos más cualificados.

Pongamos el siguiente ejemplo:

Una empresa con su propio departamento técnico implementa una solución de escritorios virtuales para varios departamentos y ofrece aplicaciones virtualizadas para el resto de empleados. Hasta ahora, cuando un empleado requiere de soporte llama al departamento técnico, éste abre una incidencia y a continuación solucionan el problema. Para solucionar dicha incidencia, en primer lugar se clasifica según su importancia en nivel 1 (mínima importancia), nivel 2 y nivel 3 (máxima importancia), y en base a dicha categorización se establece un protocolo de actuación u otro.

Las incidencias de nivel 1 son mucho más asiduas que las de nivel 3, por ello la empresa contratará a más personal técnico con una cualificación media que a profesionales con un alto conocimiento técnico. Esta tendencia cambia radicalmente cuando se administran sistemas o servicios en la nube. Debido a su

propia naturaleza y a las beneficios que ofrecen, el departamento técnico verá como se reducen las incidencias de nivel 1, tales como errores a la hora de acceder a las aplicaciones, errores de sistema, etc. Aunque no verán reducidos errores como el restablecimiento de contraseñas, cambio de idioma, etc., por poner un ejemplo. En esta nueva dinámica sí que se ve una menor necesidad de personal de soporte de nivel 1.

En cambio en los niveles 2 y 3 de soporte pasa exactamente lo contrario. Imaginémos que un usuario quiere acceder a su escritorio virtual para comenzar con su jornada laboral, pero por un motivo u otro no puede y le da un error. En ese momento llama al servicio de soporte y pide que le solucionen la incidencia con la mayor brevedad posible. En una primera instancia la incidencia la atiende el nivel 1, pero dado que no pueden solucionarla, la pasan al nivel 2 o nivel 3. Dada la naturaleza centralizada de los servicios ofrecidos en la nube, es muy probable que dicho error se repita en varios usuarios, por lo cual, en pocos minutos el departamento de soporte se puede estar enfrentando a una situación en la cual varios empleados, incluso departamen-

tos enteros, no puedan acceder a su escritorio corporativo, originándose una pérdida de productividad a la empresa.

En este caso, lo más probable es que se activaría la copia de seguridad y se restaurarían las sesiones para mitigar en primera instancia el problema del acceso y restablecer el entorno de trabajo a los empleados de la empresa. Pero en cuanto se recupere la normalidad, el departamento técnico iniciará la reparación de los problemas que se han dado. Para ello se necesita personal cualificado que conozca los sistemas y sea capaz de solucionar estos problemas con la mayor brevedad y efectividad posible.

Es por ello que, a diferencia de la actualidad donde los departamentos técnicos se componen de un gran número de técnicos de nivel medio y unos pocos profesionales altamente cualificados, con la entrada del *Cloud Computing* se reforzarán estos departamentos con más personal de nivel 2 y nivel 3. Con esto se puede decir que el sector profesional técnico sufrirá un cambio hacia una mayor cualificación de sus profesionales en los sistemas que forman la computación en la nube.

Nota

¹ *Desmitificando el Escritorio Virtual: Comenzando con la Virtualización de Escritorios*, CreateSpace, octubre 2011. ISBN-10: 146628479X.



ACTUALIZACIÓN DATOS SOCIO ATI

¿Has cambiado de domicilio, de empresa, y lo has comunicado a la Secretaría General?

¿Recibes el correo postal de la asociación?

¿Te llegan los correos electrónicos enviados por las Secretarías de ATI?

Si has contestado que **NO** a todas estas preguntas, te agradeceríamos que enviaras un mensaje a secregen@ati.es con tus nuevos datos con el fin de tener actualizada tu ficha de socio y, de este modo, nos ayudes a mejorar la comunicación entre la asociación y sus miembros.

* Del mismo modo, si sabes de algún compañero tuyo, miembro de ATI, que no recibirá esta información, te agradeceríamos que se la hagas llegar para que se pueda poner en contacto con nosotros.

ATI Secretaría General | Via Laietana 46, ppal. 1a. | 08003 Barcelona | 93 412 52 35 | secregen@ati.es | www.ati.es

Ramon Costa Pujol
 Director de Proyectos de MIC Productivity

<ramonc@micproductivity.com>

Desarrollo de aplicaciones *cloud* con Windows Azure: Cuatro experiencias prácticas

1. Introducción

Si revisamos las previsiones y estudios de los principales analistas y medios especializados sobre las tendencias en Tecnologías de la Información (TI) para el 2012¹, en todas las apuestas aparece (y ya aparecía en anteriores años) el "cloud computing" y la virtualización de infraestructuras, base de las tecnologías en dicho modelo.

El modelo de *cloud computing* permite a las organizaciones acceder a capacidades tecnológicas de forma flexible y bajo una fórmula de pago por uso. Es un nuevo modelo de prestación de servicios de negocio y tecnología que facilita al usuario (entiéndase también empresa u organización) acceder a un catálogo de servicios estandarizados y responder a las necesidades de su negocio, de forma flexible y adaptativa, en caso de demandas no previsible o de picos de trabajo, pagando únicamente por el consumo efectuado.

Después de varios años en los que las empresas han estado explorando y evaluando el modelo de gestión y trabajo con las Tecnologías de la Información (T.I.) en "la nube" (*Cloud computing*), su adopción se está abriendo camino en la mayoría de los países, entre ellos España.

Las empresas tenderán, cada vez más, a construir entornos de servicios en la nube.

Las previsiones que se manejan, por parte de diferentes consultoras y analistas, es que para el 2020, el peso del *cloud* en el mundo se cuadruplicará, lo que supondrá un 8% del presupuesto tecnológico de las empresas.

2. Cloud Computing: IaaS, PaaS y SaaS

Ahora bien, cuando hablamos de *cloud computing* tenemos que diferenciar entre las modalidades de IaaS (Infraestructura como Servicio), PaaS (Plataforma como Servicio) y SaaS (Software como Servicio).

El primer caso o nivel, IaaS, se encuentra en la capa inferior y es un medio de entregar almacenamiento básico y capacidades de cómputo como servicios estandarizados en la red: servidores, sistemas de almacenamiento, conexiones, enrutadores y otros servicios. Un ejemplo de este ámbito sería Amazon Web Services².

Resumen: Cloud computing es un término cada vez más asumido por las organizaciones que ven en esta nueva manera de consumir tecnologías de la información una importante serie de ventajas y beneficios. Cuando hablamos de Cloud Computing tenemos que referirnos a las modalidades de las S (Infraestructura como Servicio), PaaS (Plataforma como Servicio) y SaaS (Software como Servicio). Si bien la mayoría de las compañías son usuarias de aplicaciones en modalidad cloud (SaaS) y las grandes organizaciones están migrando su infraestructura (total o parcial) a una modalidad IaaS, hay un segmento importante de compañías, tanto de servicios de Tecnologías de la Información (TI) como empresas con departamentos de desarrollo de software, que están optando también por la modalidad PaaS. De la mano de cuatro ingenierías de software como son Itequia, Raona, Softeng y Pasiona, analizamos su experiencia de trabajo con la plataforma Windows Azure de Microsoft.

Palabras clave: Cloud Computing, Itequia, MIC Productivity, PaaS, Pasiona, Raona, Softeng, Windows Azure.

Autor

Ramon Costa Pujol es Ingeniero en Informática y Máster en Cualificación Pedagógica por la UPC, y Diplomado en Dirección General por la Escuela de Negocios EADA. Es Director de Proyectos y Responsable del área de acuerdos y *Partners* del Centro de Innovación en Productividad de Microsoft, MIC Productivity <www.micproductivity.com>, responsabilidad que combina con la docencia universitaria en la UAB en el área de la Gestión de Proyectos y Consultoría, y la docencia en la Escuela de Negocios EADA como Profesor Adjunto del Departamento de Operaciones y Sistemas de Información. Ha sido cofundador de la iniciativa emprendedora inPreneur <www.actioningorganizations.com>.

En el caso de PaaS, lo que se ofrece es la encapsulación de un entorno de desarrollo y el empaquetamiento de servicios, como los ejemplos de Google App Engine³ y Windows Azure⁴, de Microsoft, que permite el desarrollo y ejecución de aplicaciones codificadas en varios lenguajes y tecnologías como .NET, Java y PHP.

Finalmente, las soluciones SaaS se caracterizan por ser una aplicación completa ofrecida como un servicio, "on-demand" vía multitenencia, una sola instancia del software que corre en la infraestructura del proveedor sirviendo a múltiples organizaciones. Ejemplos de este tipo de soluciones serían Salesforce.com⁵, Google Apps⁶ o Microsoft Office 365⁷, que incluye versiones *online* de la mayoría de las aplicaciones de la *suite* ofimática de Microsoft, el servidor de correo corporativo Exchange, el servidor de comunicaciones online Lync o la plataforma de colaboración SharePoint.

3. Beneficios, temores e inhibidores en las organizaciones

A la hora de plantearse la migración o trabajo con soluciones en la nube, aparecen un conjunto de importantes beneficios, pero también algunos temores que actúan de barrera

o inhibitorio para que las compañías hagan el salto final.

La reducción de los costes tecnológicos es una de las ventajas de uso de esta modalidad, ya que el gasto se adapta al consumo de recursos que haga la organización, pagando sólo por lo que se necesita y convirtiendo unos gastos fijos e inversiones, actualmente, en gastos variables.

Otra ventaja es la flexibilidad y agilidad de este modelo, ya que permite a las empresas aumentar o disminuir los recursos tecnológicos de forma instantánea. Por ejemplo, una compañía puede hacer frente a un pico de ventas en Internet contratando en la nube más capacidad de cálculo, memoria y almacenamiento durante el tiempo que dure la campaña.

Las empresas pagan su estructura informática de la misma forma que la luz, el agua o el gas, convirtiendo esta infraestructura en una "commodity".

El temor acerca de aspectos relativos a la seguridad y privacidad de los datos son algunos de los factores que inhiben a las organizaciones a adoptar este modelo tecnológico. Es por ello que muchas empresas optan por

trabajar con "nubes privadas" en vez de "nubes públicas", aquellas en las que la infraestructura es compartida. U optan, también, por redes híbridas en las que una parte de la red es pública y otra parte de servicios residen en la red privada.

Otro reto a superar por parte de las empresas es el temor a la disponibilidad y accesibilidad de la información y aplicaciones. Muchos proveedores aseguran por contrato una alta disponibilidad del servicio como el caso de Microsoft, que garantiza un 99,9% del mismo.

Otro aspecto importante a considerar, bajo el prisma de los departamentos de TI y Sistemas de Información es todo aquello relacionado con la integración de sistemas, datos y seguridad, entre las soluciones en *cloud* y las "on premise".

4. Experiencias reales en España

La mayoría de los agentes del sector de las TIC (operadores de telecomunicaciones, proveedores de tecnología, empresas de *hosting*, desarrolladores de software y compañías de Internet) están adoptando este modelo de trabajo en sus servicios y productos.

IBM prevé dar soporte a cerca de 200 millones de usuarios en la nube para 2012 y facturar 3.000 millones de dólares en 2015.

Microsoft, por ejemplo, cuenta con más de 1,6 millones de usuarios en organizaciones privadas y públicas en España haciendo uso de sus soluciones en la nube.

Nos encontramos con ejemplos de organizaciones de todos los tamaños y sectores que ya han decidido adoptar esta nueva manera de consumir tecnología:

- Correos implantará el software de gestión empresarial SAP con una infraestructura de nube privada.

- La Generalitat de Catalunya ha transferido a la nube el correo de sus 105.000 funcionarios como parte de una estrategia de *cloud* privada⁸.

- La Corporación Extremeña de Medios Audiovisuales utiliza una solución de infraestructura en la nube para ofrecer contenidos en *streaming* y *podcast*, alojando los contenidos y servicios de su web y dominios en una nube pública, pagando por consumo real.

- BBVA ha firmado un acuerdo con Google para utilizar su paquete de soluciones para sus más de 110.000 empleados, previendo su migración durante 2012.

- El Gobierno Vasco aprobó una proposición de ley para estudiar y diseñar una estrategia de racionalización de su estructura informática en base al *cloud computing*⁹.

- El Gobierno Regional de Castilla-La Mancha dio el primer paso hacia la unificación de los sistemas de información de sus

distintas Consejerías en un único Centro de Proceso de Datos, valiéndose para ello de una infraestructura de computación en la nube privada puesta en marcha de la mano de Telefónica y la alianza VCE (Cisco, VMWare y EMC)¹⁰.

- La campaña viral Gente Sin Miedo lanzada por el Grupo Catalana Occidente para captar clientes entre los usuarios de las redes sociales precisaba una plataforma flexible y ágil que soportara el acceso simultáneo de gran número de usuarios a la web que fue implementada con Microsoft Windows Azure¹¹.

- Egencia, agencia de gestión de viajes, implantó Salesforce.com para automatizar sus procesos comerciales¹².

5. Microsoft Windows Azure: Plataforma cloud como servicio

Si bien en las grandes empresas, el *cloud computing* se implanta a través de la infraestructura como servicio (IaaS), en las pequeñas y medianas el foco se centra en trabajar con soluciones en modo *cloud computing* (SaaS). Es decir, disponer de sus sistemas de gestión empresarial, como por ejemplo, las herramientas CRM (Gestión de la Relación con los Clientes) o las plataformas de productividad (Correo Electrónico, Audio y Vídeo Conferencias, Entornos de Colaboración...). Las grandes empresas también son usuarios, pero en menor porcentaje relativo de este tipo de soluciones, centrándose sobre todo en servicios como el correo corporativo en la nube, por ejemplo.

Sin embargo, las empresas de servicios de software, integradores de soluciones o compañías con departamentos de desarrollo de software son las principales usuarias de las plataformas *cloud* en modalidad PaaS. Una de las opciones de plataforma en esta modalidad, como comentamos anteriormente, es la ofrecida por Microsoft: Windows Azure.

Windows Azure es un sistema operativo de servicios en la nube que funciona como entorno de desarrollo, hospedaje y gestión de servicios para la plataforma del mismo nombre. Windows Azure ofrece a los desarrolladores funcionalidades de almacenamiento y procesamiento bajo demanda para hospedar, escalar y gestionar aplicaciones web en Internet a través de los centros de datos de Microsoft.

Esta plataforma de nube abierta permite compilar (en cualquier lenguaje, herramienta o marco), implementar y administrar aplicaciones rápidamente, en una red global de centros de datos administrados por Microsoft, e integrar las aplicaciones de nube públicas con el entorno de TI existente en la organización.

Windows Azure permite escalar aplicaciones a cualquier tamaño con facilidad, prestando

un autoservicio totalmente automatizado para el aprovisionamiento de recursos en cuestión de minutos, pagando los recursos que utiliza la aplicación. Permite almacenar los datos en cualquier tipo de sistema de datos: bases de datos relacionales, bases de datos NoSQL o datos distribuidos, no estructurados. Es posible manipular con facilidad estos datos, o usar la funcionalidad de Hadoop y *Business Intelligence* para proceder a la minería de datos e identificar las ideas fundamentales.

Windows Azure incluye sólidas funciones de mensajería para aplicaciones distribuidas e híbridas, puede exponer aplicaciones a través de *firewalls*, puertas de enlace NAT y otros límites de red y está disponible en varios centros de datos del mundo, lo que permite implementar las aplicaciones cerca de los clientes.

A continuación exponemos la experiencia de 4 empresas de servicio de ingeniería de software, Itequia, Pasiona, Raona, Softeng, Pasiona, que nos comparten sus vivencias y aprendizajes con el desarrollo de aplicaciones sobre Windows Azure.

Anexo 1: Itequia - "La experiencia del Tercer Lugar"

(Escrito por **Oriol Fernández Moreno**, Team Leader en Itèquia. <oriol.fernandez@itequia.com>)

"¿Quién no ha tenido la necesidad, alguna vez, de trabajar fuera de la oficina o fuera de casa y de encontrar un lugar adecuado para hacerlo?"

La aplicación

Ideado por Microsoft Productivity Center y desarrollado por Itèquia, Tercer lugar es una aplicación web desarrollada con ASP.net y, en su versión móvil, con Windows Phone 7 SDK que nace con el objetivo de cubrir algunas de las necesidades de los trabajadores móviles como:

- Informar las ubicaciones y las características de éstas dentro de la ciudad donde poder trabajar.

- Dar de alta nuevos espacios, cualificar y opinar sobre los mismos de forma participativa.

- Ofrecer enlaces de interés, artículos y casos de éxito sobre el trabajo móvil.

- Ofrecer consejos y buenas prácticas que se incorporen a este modo de trabajar.

- Descargar aplicaciones para dar de alta y consultar ubicaciones desde dispositivos móviles.

La implementación

A la hora de implementar la aplicación barajamos diferentes opciones sobre qué tecnologías utilizar y qué arquitectura implementar: desde hospedar la aplicación en servidores on-

premise del MIC Productivity, hasta, en aquellos momentos, hospedarla en la aún incipiente nube. Para este caso concreto, la decisión estaba tomada, la aplicación se iba a desarrollar sobre la nube. Concretamente sobre Windows Azure (*de aquí en adelante Azure*), dada la escalabilidad, la replicación y consistencia frente a cambios de la aplicación que ofrece; sin olvidar la alta disponibilidad del sistema sin costes de operación. En otras palabras, gracias a Azure, TercerLugar está disponible el 99,9% sin necesidad de designar una persona que tenga que monitorizar su estado.

Suponiendo que el lector ya está, en mayor o menor grado, familiarizado con los conceptos PaaS (*Platform as a Service*) y con la arquitectura de Azure os explicaré cómo estructuramos la aplicación dentro del servicio.

Como podréis observar, se trata de una implementación básica de servicios de Azure. La aplicación cuenta con dos *web roles* dentro de *Azure compute*. Por un lado el *web role* encargado de gestionar y hospedar toda la parte web de la aplicación y por el otro el *web role* encargado de gestionar y hospedar los servicios web encargados de proporcionar la información necesaria a la aplicación móvil. La autenticación y autorización se gestionan mediante *Azure App Fabric Access control* utilizando el Live ID del usuario (solo es necesaria autenticación si el usuario quiere añadir nuevos lugares o bien si quiere añadir comentarios). Y los datos tales como la localización de los lugares, las características de los mismos y las opiniones de los usuarios se almacenan en SQL Azure.

Es evidente que el modo correcto de implementar los servicios web y la aplicación, así como la autenticación y la autorización sobre Azure es el descrito, pero ¿porqué utilizar SQL Azure para almacenar los datos? ¿Porqué no utilizar Azure Storage Tables? La clave en la decisión es la estructura de los datos. Se trata de un modelo relacional, donde todos los registros deben cumplir un esquema; este modelo es imposible de representar dentro de Azure Storage Tables dado que aunque soportan el almacenamiento de información en formato tabular, no te aseguran la integridad y el cumplimiento del esquema de los datos.

De este modo, podemos representar la estructura de la aplicación como se puede observar en la **figura 1**.

Conclusiones

El hecho de desarrollar la aplicación sobre Azure no supone muchas diferencias en cuanto a desarrollar una aplicación web para ser hospedada *on-premise*. Este hecho es gracias a que Azure ofrece a los desarrolladores las

mismas características que usarían para implementar una aplicación web destinada a un entorno "no Azure".

Podréis pensar en el modelo de facturación de Azure a la hora de implementar una aplicación sobre la plataforma; tened en cuenta (tal y como se detalla en Windows Azure Platform¹³) que Azure factura por el uso de los siguientes Servicios, entre otros: instancias de *Azure Compute*, de *Azure Storage*, de transacciones de *access control* o bien de uso de *SQL Azure*. Bien, pues, está en nuestras manos el hecho de hacer que esta facturación sea mínima: deberemos de programar en lo que a veces se denomina como programación en función de costes; esto pasa por optimizar las instancias de *compute* que vamos a usar, optimizar las peticiones a las bases de datos de SQL Azure o bien intentar optimizar las funciones que usan características de Azure *App Fabric* como *Access Control*, *Caché* o *Service Bus*.

Anexo 2: Pasiona - ClickPost.com, en un único buzón toda tu correspondencia

(Escrito por **Txema Moreno**, Project Manager de Pasiona. <jmmoreno@pasiona.com>)

Click post, un único buzón para toda tu correspondencia. Así podríamos definir en una frase el servicio gratuito que ofrece esta *startup* nacida en Barcelona y con objetivos internacionales.

El Proyecto ClickPost nace de un concepto muy sencillo a la vez que extremadamente interesante: convertir el buzón de cartas de toda la vida en un buzón *online*, con las ventajas que supone disponer de nuestra correspondencia (facturas, recibos, etc...) de forma conjunta y categorizada. ClickPost proporciona muchas ventajas para el usuario: eliminar los recibos físicos que inundan los cajones de nuestra casa, buscar fácilmente un recibo o factura, etiquetar y agrupar los recibos, son solo algunas de ellas.

Una correspondencia informatizada además, permite explotar la información de nuestros consumos, pudiendo visualizar gráficos de tendencia, comparativas con el resto de usuarios y llevar una contabilidad doméstica.

La apuesta de ClickPost fue desarrollar la herramienta con tecnología Microsoft acompañada de la mano de Pasiona, empresa especialista en el desarrollo de software del fabricante americano y con un área dedicada en exclusiva a prestar soluciones a medida para *startups* en Internet.

Pasiona, alineada a la estrategia de Microsoft en entorno web, apostó por desarrollar el

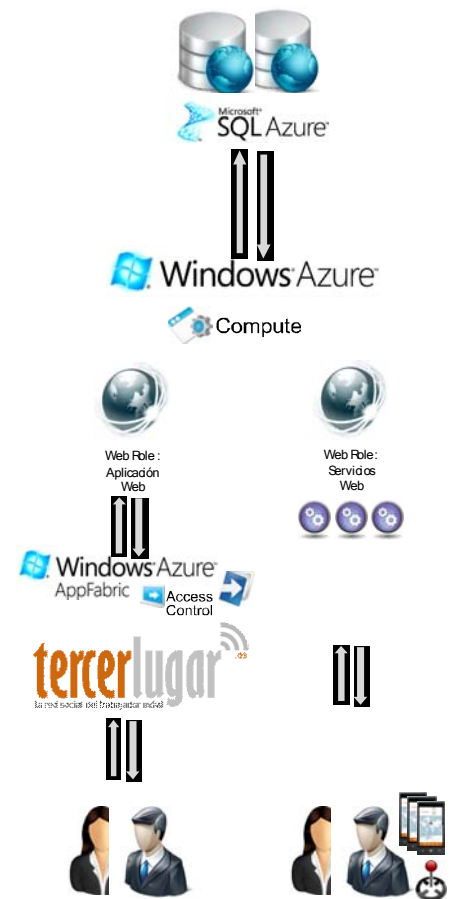


Figura 1. Estructura de la aplicación TercerLugar.

front-end del aplicativo en MVC ASP.NET y decidió alojar el software sobre el sistema operativo en la nube Windows Azure.

El primero, permite crear páginas "ligeras", particularmente indicadas para un consumo masivo mientras el segundo conlleva todas las ventajas de un alojamiento en la nube y permite al cliente disponer de una solución cuyos costes son proporcionales al volumen de visitas.

Particularmente, la plataforma Windows Azure ofrece a este modelo de negocio ventajas incomparables, tanto en los tiempos de desarrollo como en los costes de mantenimiento posteriores.

La solución requería dos líneas de desarrollo:

- Por un lado, la Integración con Emisores, que se compone de una capa de *middleware* dedicada a la realización de procesos de integración entre el *backOffice* de ClickPost y los diferentes emisores de documentos (bancos, *utilities*, etc.). Estos procesos, requieren una carga importante de CPU en días determinados del mes así que las tareas de conexión, normalización de documentos, extracción de metadatos y entrega al usuario se sustentan sobre *Worker Roles* y *Colas de Azure* de una

forma totalmente asíncrona. Azure permite además levantar tantas instancias como sean necesarias durante el proceso y reducirlas una vez finalizado optimizando al máximo los recursos y en consecuencia los costes.

■ Por otro lado, el desarrollo del Portal Web se sustenta sobre el *Web Role* de Azure en su versión MVC, que ofrece la posibilidad de crear un portal claramente orientado al usuario. Al igual que los *Worker Roles*, es posible dimensionarlo en función de las necesidades de carga, pudiendo variar en función de la franja horaria incluso en un mismo día. El dimensionamiento es dinámico y se puede parametrizar para que, cuando se sobrepasen una serie de indicadores, el sistema sea capaz automáticamente de levantar instancias para garantizar el acceso fluido a la web.

Azure además ofrece otras ventajas que se han aprovechado para el proyecto ClickPost y que son aplicables en mayor o menor medida a cualquier otra solución:

■ El *Blob Storage*, que permite el almacenamiento masivo de documentos con un volumen prácticamente ilimitado, aportando una velocidad de acceso óptima gracias a su motor de búsqueda e indexación.

■ La Escalabilidad. Como hemos comentado anteriormente, Azure permite escalar tanto en número de máquinas virtuales como en la configuración de las mismas, adaptándose a las necesidades del servicio que queremos prestar.

■ La Disponibilidad. Microsoft garantiza un 99.99% de disponibilidad en la firma del SLA de servicio. Aparte, el sistema de gestión de versiones de Azure permite pasar fácilmente de un entorno de *Staging* a Producción, gracias a la funcionalidad de "SWAP VIP", sin que la web deje de funcionar en ningún momento.

■ El Cache Distribuido. Debido a que un portal puede tener "n" instancias levantadas para garantizar un tiempo de respuesta óptimo, Azure dispone de un proveedor de Cache Distribuido, configurable y escalable en función de las necesidades.

■ La Seguridad. El *Access Control* resuelve las problemáticas de seguridad. La autenticación de usuarios, la gestión de *cookies* y los *tokens* están integrados en el entorno del propio Azure, facilitando tanto el desarrollo como su posterior gestión.

■ Y por último las pruebas de stress que, una vez diseñadas, no requieren realizar estimaciones de "cuántos usuarios aguantarían 'n' máquinas". Azure permite realizar un test real levantando instancias y analizando el comportamiento de las mismas con el objetivo de encontrar el equilibrio entre tiempos de respuestas del sistema y coste de infraestructura.

Anexo 3: Raona - ItsHappy, ocio y solidaridad en Windows Azure

(Escrito por **David Solsona**, Business Development & Integration Manager en Raona, <david.solsona@itshappy.com>)

ItsHappy es un portal donde el usuario puede gestionarse los regalos, organizar fiestas y su agenda del ocio además de ayudar a las ONG's con recursos y tecnología.

Nuestra experiencia con Windows Azure empieza en diciembre de 2010, cuando se realizó la migración de la plataforma desde un servicio de *hosting* estándar a Windows Azure.

¿Tiempo de migración? Una noche.

¿Motivo de la migración? Escalabilidad, teníamos previsión de un aumento indeterminado de visitas al portal, durante un espacio corto de tiempo al principio y necesitábamos flexibilidad y facilidad para aumentar o reducir la capacidad disponible.

¿Por qué Windows Azure? Aquí tuvimos en cuenta las siguientes consideraciones:

■ Conocimiento del equipo de desarrollo de las tecnologías Microsoft. Ya cuando se decidió apostar en desarrollar en .NET, fue por el conocimiento de la tecnología y por la productividad que ofrecen las herramientas de desarrollo de Microsoft frente a otras existentes.

■ SQL Azure es el servicio de base de datos independiente a los servicios de cómputo y presentación, el cual puede utilizarse tanto para las aplicaciones desplegadas en Azure como para las que podamos tener localmente. Excepto algunas funcionalidades que todavía no tienen implementadas, la mayor parte de las necesidades de nuestra plataforma quedan cubiertas por el gestor, e insistimos, podíamos aprovechar el conocimiento de nuestro equipo técnico. Además existe la forma de poderlo gestionar *online* y con las herramientas habituales.

■ Facilidad de despliegue algo que en mi experiencia a veces es difícil de conseguir. Pues bien bajo este punto quisiera comentar lo siguiente:

- Entorno de pruebas similar: al crear una imagen exacta de lo que vas a poner en producción, una vez comprobado, y solo con un click, rápidamente pasas a tener la nueva versión operativa. Y algo muy valorable, si por cualquier motivo tienes que hacer *rollback*, con el mismo click tienes el sistema en la versión anterior.

- Despliegue gestionado desde el propio Visual Studio, lo que nos supone gran productividad y eficiencia.

- Despliegues parciales: En caso de querer realizar despliegues parciales útiles para resolver rápidamente alguna incidencia, es tan sencillo como si tuvieras los servidores localmente, realizando una conexión mediante los servicios de terminal o con alguna utilidad que despliegue los binarios o páginas afectadas.

■ El servicio de *storage*, una solución perfecta para poner todos aquellos recursos generados o utilizados por el portal, como imágenes, ficheros de estilos, *javascripts*, etc.

Todo aquello que podrías modificar sin necesidad de realizar un despliegue.

■ Coste, es algo que en el momento de decidir no fue el punto principal, nos basamos en una referencia de precios que nos presentaron, y aparte de pagar cara la inexperiencia, se ajustó bastante a lo esperado.

¿Nivel de satisfacción? Llevo muchos años trabajando con diferentes tecnologías incluidas las de Microsoft y sinceramente he de decir que en esta ocasión han superado mis expectativas, hasta el momento satisfacción máxima. Enumeraré los indicadores para mí, más representativos:

■ Productividad: El equipo solamente se dedica al desarrollo de los servicios, nuestra responsabilidad de que funcione y la de Azure de tenerlo disponible.

■ Rendimiento: Muchos me preguntan, ¿es barato? ¿no sale caro?, y no tengo argumentos para dar una respuesta definitiva; de momento nuestra experiencia es: 0 problemas, 0 tiempo dedicado a resolver tareas de sistemas, tiempo de adaptación al nuevo entorno bajo. Aunque no sabemos qué hubiese pasado si la decisión hubiese sido otra.

■ Soporte: Lógicamente tenemos el apoyo de los ingenieros especialistas de Raona para solucionar cualquier contingencia o estar al día de las novedades que nos ayuden a mejorar la plataforma.

Espero que os haya sido útil nuestra experiencia y por favor contactad conmigo en el caso de requerir más información.

Anexo 4: Softeng

(Escrito por **Carlos Colell**, Director General de Softeng, <ccolell@softeng.es>)

Fundada en 1997, Softeng es una consultoría e ingeniería de software experta en tecnologías Microsoft y especializada en *cloud*. La compañía cuenta con la certificación como *Gold Certified Partner* de Microsoft y con 22 competencias tecnológicas, es la empresa española con más certificaciones Microsoft.

Las tres áreas de negocio de Softeng son el Desarrollo de proyectos Web mediante *Softeng Portal Builder*, Intranets colaborativas mediante *SharePoint*, e Ingeniería de sistemas críticos (que abarca el diseño, despliegue y administración de infraestructuras robustas con tecnología Microsoft, tanto *on-premise* como en "la nube").

A la primera área pertenece su solución *Softeng Portal Builder*, una plataforma concebida para el desarrollo y gestión de proyectos Web empresariales, evolucionada hacia "la nube" aprovechando los beneficios que ofrece Windows Azure de Microsoft y desarrollada usando una arquitectura orientada a dominio (DDD).

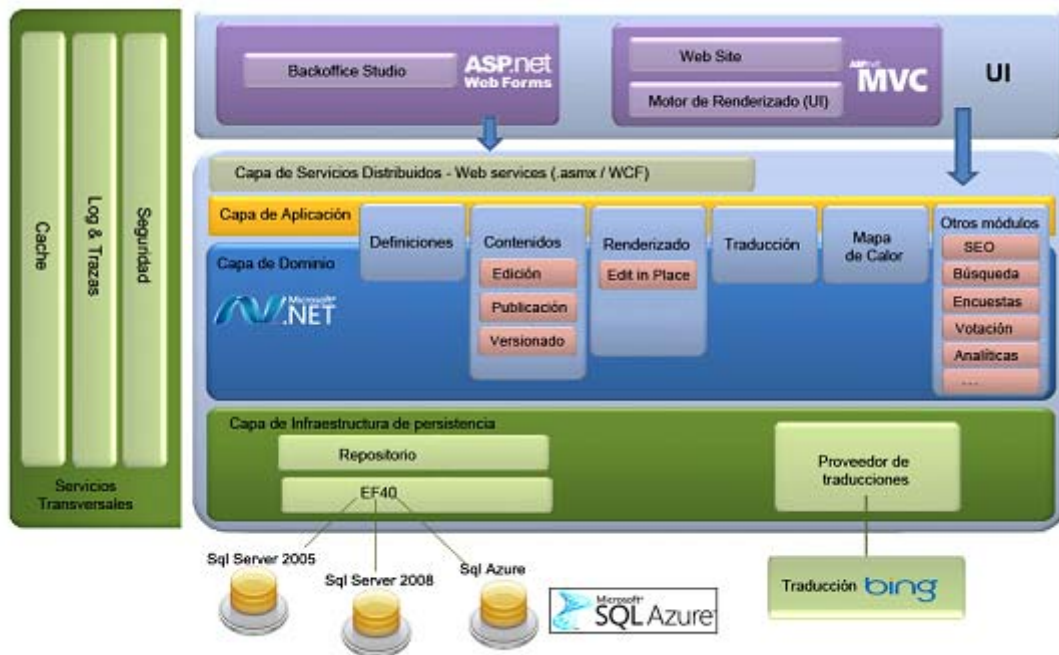


Figura 2. Arquitectura de Softeng Portal Builder.

Softeng Portal Builder es una plataforma empresarial para llevar a cabo proyectos web en la nube de forma rentable, ayudando a impulsar a las empresas a través de la Web y ofreciendo autonomía y productividad en la gestión del sitio con bajos costes de propiedad (ver figura 2).

La plataforma está pensada para los sitios públicos estratégicos de la mediana y gran empresa con necesidades constantes de actualización y rotación de contenidos. De entre todas sus ventajas destacan la productividad que brinda la edición visual desde la propia web, la mejora del posicionamiento en buscadores, el sistema de traducción simultánea de contenidos y las analíticas web de última generación que permiten conocer el comportamiento de los visitantes incrementando su conversión y mejorando así los resultados del sitio.

El punto de partida antes de evolucionar a Windows Azure era una aplicación de arquitectura compleja que podía estar instalada en los servidores del centro de datos de Softeng, en los del propio cliente o en un ISP.

Tal y como había previsto Softeng, este movimiento inicial hacia la nube se realizó de forma no demasiado traumática, gracias a las similitudes entre Azure y el entorno de desarrollo anterior, pero inicialmente resultó que Portal Builder no podía funcionar de forma óptima en Azure pues requería un consumo excesivo de recursos para que su rendimiento fuera el deseado. Por lo tanto, se decidió llevar a cabo una reingeniería total de la aplicación.

Durante la fase de inecpción de la nueva arquitectura, Softeng tomó contacto con la versión beta de la Guía de "Arquitectura N-Capas orientada al Dominio con .NET 4¹⁴", creada por Microsoft Ibérica. Si bien aún estaba madurando, esta guía mostró un claro mapa de arquitectura DDD relacionado con las tecnologías de Microsoft disponibles para realizar el trabajo. Además, la Guía de Arquitectura y la aplicación de ejemplo de Microsoft también ayudó a los ingenieros de Softeng a cubrir aspectos importantes de arquitectura que no se cubren en el libro original de Eric Evans, tales como la inyección de dependencias (DI) e inversión de control (Ioc) utilizando Microsoft Unity. Bien utilizado sirve para seguir el principio de diseño Open Closed Principle o Protected Variations, importante principio de diseño que permite flexibilidad y extensibilidad.

Gracias a la nueva arquitectura, actualmente Softeng Portal Builder ofrece una escalabilidad lineal en Azure con un muy bajo consumo de recursos así como un rendimiento extraordinario. En resumen, es capaz de atender a 2.500 usuarios simultáneos por instancia mediana de Azure, sirviendo las peticiones a una media de 30 ms.

Entre las razones para cambiar a Azure no solo estuvo el fuerte compromiso de Softeng con la innovación: Queremos que el mercado perciba nuestra plataforma como puntera, encuadrada en el estado del arte de la tecnología, y Azure contribuye en gran medida a lograr esta percepción. Con Azure ya no tenemos que invertir fuerte y constantemente en hardware, software y personal de soporte

para mantener un datacenter clásico, reduciendo notablemente nuestros costes.

Notas

- ¹ Ver por ejemplo, <<http://trends.ticbeat.com/trends-2012-tendencias-innovacion-2012/>> y <<http://www.computereconomics.com/page.cfm?name=technology%20trends>>.
- ² <<http://aws.amazon.com/es/>>.
- ³ <<http://code.google.com/intl/es-ES/appengine/>>.
- ⁴ <<http://www.windowsazure.com/es-es/>>.
- ⁵ <<http://www.salesforce.com>>.
- ⁶ <<http://www.google.com/apps>>.
- ⁷ <<http://www.microsoft.com/es-es/office365>>.
- ⁸ <<http://www.microsoft.com/spain/prensa/noticia.aspx?infoid=/2011/04/n001-Microsoft-proporciona-servicios-cloud-a-Generalitat-Catalana>>.
- ⁹ <<http://www.euskadinnova.net/es/enpresadigitala/noticias/gobierno-vasco-pondra-marcha-experiencias-cloud-computing/7603.aspx>>.
- ¹⁰ <http://www.clubdeinnovacion.es/index.php?option=com_mtree&task=viewlink&link_id=466&Itemid=64>.
- ¹¹ <<http://www.microsoft.com/spain/enterprise/casos-exito/detalle-casos-de-exito.aspx?ContentoID=20110315001>>.
- ¹² <http://www.salesforce.com/es/customers/travel-transportation/expedia_corp_travel.jsp>.
- ¹³ <<http://msdn.microsoft.com/en-us/library/windowsazure/dd163896.aspx>>.
- ¹⁴ <<http://microsoftnlayerapp.codeplex.com/>>.

Guillermo Morales-Luna

Departamento de Computación, Centro de Investigación y Estudios Avanzados del Instituto Politécnico Nacional, Cinvestav-IPN (México)

<gmorales@cs.cinvestav.mx>

1. Introducción

El, digamos, *cómputo en la nube* (*cloud computing*) significa la relegación de servicios informáticos a proveedores terceros, y, en consecuencia, plantea problemas de seguridad de diversa índole, tales como de confidencialidad, de privacidad, de integridad y de acceso seguro, entre muchos más. Naturalmente, la resolución efectiva y eficiente de estos problemas hará mucho más asequible esta tecnología a públicos generales. Los problemas mencionados son áreas de interés de la Criptografía, y en consecuencia, las técnicas criptográficas son cruciales en el desarrollo del cómputo en la nube. Las ventajas principales de éste radican en la ubicuidad de sus servicios y en su efectividad de costos. En la práctica, es un servicio de subcontratación (*outsourcing*) de servicios informáticos lo que libera a los usuarios, sean individuos, empresas (privadas o públicas), o incluso agencias gubernamentales, de la gestión de recursos de hardware y software para el manejo de la información propia. El servicio se presta de manera global y está por encima de divisiones territoriales o nacionales.

La seguridad es acaso el aspecto más importante del cómputo en la nube y puede superar en importancia al propio rendimiento o a la disponibilidad. La seguridad del cómputo en la nube se basa en un paradigma identificado en inglés como CIA: *Confidentiality, Integrity, Availability*, o acaso en español como CID: *Confidencialidad, Integridad, Disponibilidad*, y su tratamiento ha dado lugar al surgimiento del *cómputo confiable* (*trusted computing*). En su vertiente de *infraestructura como servicio* (IaaS: *Infrastructure as a Service*), el cómputo en la nube proporciona una máquina virtual para procesar la información que le fue encomendada. Para realizar esto de manera eficiente, procura tener la información en claro, con lo que el cliente ha de confiar en la discreción del proveedor, y éste ha de reforzar el aspecto físico de sus recursos para evitar intromisiones de terceros, sean éstos externos o incluso internos.

Entre los ataques al cómputo en la nube están los convencionales: aquellos dirigidos contra las máquinas virtuales empleadas en la nube, los hechos mediante la inyección de código malicioso a través de servicios de *web*, los dirigidos contra los usuarios a través de la propia nube, la suplantación de entidades de acceso a la nube (*phishing*), etc.

Un aspecto fundamental en el uso de la nube es su *disponibilidad* (*availability*). Por supuesto que los tiempos de respuesta de la nube deben ser comparables a los de la infraestructura local de los usuarios. En consecuencia, ciertos procesos han de limitarse para que la satisfacción de ellos no afecte a los demás usuarios. También ha de haber confianza y certeza en los usuarios de que los resultados provistos por la nube son, en efecto, correctos. Finalmente, la diversidad de puntos de acceso a la nube la puede hacer más vulnerable.

Por otra parte, los usuarios deben tener la certeza de que el manejo que ellos hacen de su propia información se ejecuta fielmente en la nube. Por ejemplo, si se borra un registro en una base de datos, ese registro efectivamente es borrado y no queda una copia espuria a disposición del propietario de la nube, o si se actualiza una información, ésta queda reflejada inmediatamente de manera independiente al punto de acceso que se use hacia la nube. Bien puede suceder que los gestores de la nube subroguen a terceros la gestión de ciertos servicios, por lo que la relación a simple vista *nube-usuarios* puede ser una relación entre

Seguridad en el cómputo en la nube

Resumen: En este artículo hacemos una reseña de los servicios de seguridad y privacidad en el cómputo en la nube. Inicialmente, revisamos las nociones relevantes de seguridad y de los estándares asumidos por la comunidad internacional, luego bosquejamos protocolos criptográficos para procesar de manera remota la información colocada en una nube y para comprobar la subsistencia de la información y la buena devolución de ésta a sus propietarios. Finalmente, discutimos la relación entre seguridad y eficiencia en el cómputo en la nube.

Palabras clave: Cifradores basados en homomorfismos, cómputo en la nube, estándares de seguridad, pruebas de recuperabilidad de la información.

Autor

Guillermo Morales-Luna es Investigador Titular en el Departamento de Computación del Centro de Investigación y Estudios Avanzados del Instituto Politécnico Nacional (Cinvestav-IPN, México), es Licenciado en Física y Matemáticas por la ESFM-IPN, Maestro en Ciencias con especialidad en Matemáticas por el Cinvestav-IPN, y Doctor en Ciencias Matemáticas por el Instituto de Matemáticas de la Academia Polaca de Ciencias, en Varsovia (Polonia). Sus áreas de interés son los Fundamentos Matemáticos de Computación, Lógica y Deducción Automática, Criptografía y Teoría de la Complejidad. Ha sido profesor en el Instituto Politécnico Nacional de México y en la Benemérita Universidad Autónoma de Puebla. Ha realizado dos estancias sabáticas en el Instituto Mexicano del Petróleo. Es mexicano por nacimiento y le fue concedida la ciudadanía polaca.

muchas partes. Servicios como el auditado de los usuarios de su propia información, las obligaciones contractuales y el espionaje en la nube se complican debido a esa relación multilateral.

Otros riesgos potenciales a la seguridad en una nube son la recolección de datos respecto a hábitos y consultas de los usuarios, lo que afecta a su privacidad, la defensa de la disponibilidad (amenazada por ataques de denegación de servicio, por ejemplo), la autenticación de servidores, y la explotación de la información recolectada (*mashup*), durante las tareas de gestión de la nube, relativa a los usuarios.

Finalmente, recordamos que un sistema es *responsable* cuando se pueden detectar fallas en su funcionamiento y además se puede reconocer (se le puede atribuir responsabilidad) al nodo donde surgió la falla. Obviamente, los sistemas responsables en el cómputo en la nube son esenciales en las relaciones clientes-proveedores.

Ha habido diversos estándares adoptados y acatados por la comunidad internacional relativos a la seguridad del cómputo en la nube [1], y entre éstos mencionamos tan solo los siguientes:

- **NIST 800-14:** (NIST: *National Institute of Standards & Technology*, EEUU). Es un conjunto de normas para procedimientos y codificación de servicios de seguridad.
- **ISO/IEC 20000:** (ISO/IEC: *International Organization for Standardization/International Electrotechnical Commission*) Es propiamente la parte operacional, establece los objetivos y condiciones

que deben cumplir y alcanzar los proveedores de servicio: disponibilidad, integridad, confidencialidad, eficiencia, efectividad, etc.

- *ISO/IEC 2700X*: Es una serie de normas relativas propiamente a la parte de seguridad de la información. Establecen los procedimientos de autenticación, de cifrado, de auditado, de no-repudio, etc.
- *ISO/IEC JTC1 SC38 (Distributed Application Platforms and Services)*: Es un comité técnico de ISO/IEC que define la taxonomía, la terminología y la proposición de valores para el cómputo de nube, y concilia los estándares de otras agencias en este tema, pues aunque el propósito de estandarización es el de uniformizar los servicios, éstos aún se implementan de manera variada [2].

A nivel internacional, diversas agencias han sido reconocidas como estandarizadoras de los servicios de cómputo en la nube. Entre las más importantes están las siguientes:

- National Institute of Standards and Technology, <<http://csrc.nist.gov>>.
- IEEE Standards Association, <<http://standards.ieee.org>>.
- Internet Engineering Task Force, <<http://www.ietf.org/>>.
- International Standards Organisation, <<http://www.iso.org>>.
- ITU-T (Telecommunications Standardisation Sector of the ITU), <<http://www.itu.int>>.
- European Telecommunications Standards Institute, <<http://www.etsi.org>>.
- British Standards Institute, <<http://www.bsigroup.com>>.
- ITIL: IT Infrastructure Library, British, <<http://www.itil.org>>.
- CEN Information Society Standardisation System, <<http://www.cenorm.be/iss>>.
- Standards Australia, <<http://www.standards.org.au/>>.

En enero de 2011, el NIST (*National Institute of Standards and Technology*) publicó una guía para la instrumentación de servicios de cómputo en la nube [3]. Ahí se recomienda planear cuidadosamente, con antelación a la puesta en marcha de una nube, sus aspectos de seguridad y de privacidad, demarcar los alcances de seguridad de la nube y verificar que efectivamente se cumple con esas demarcaciones, asegurarse que del lado de los clientes éstos cumplen con los requisitos de seguridad y privacidad en la nube y mantener la responsabilidad de la seguridad y la privacidad de los datos y de las aplicaciones montados en la nube. Esta guía recomienda considerar la especialización del personal que atenderá la nube, la fortaleza de su infraestructura, la disponibilidad de los recursos físicos, las políticas de respaldo y de recuperación, los puntos de acceso móviles y la concentración de datos.

En esta guía se hace pues énfasis en el aspecto físico de la seguridad y no se formula recomendación alguna sobre sus aspectos lógicos y los métodos criptográficos para asegurar confidencialidad y eficiencia.

2. Protocolos elementales

Todo cliente, al depositar información en un servidor propiedad de un proveedor de cómputo en nube, querría mantener la privacidad de su información y ponerla al abrigo de intromisiones indeseables, tanto de cualquier otro cliente en la nube, como incluso del propio proveedor del cómputo en la nube. Para esto, el cliente querría cifrar la información depositada. Sin embargo, para hacer una consulta a la información, en un primer enfoque *naif*, tendría que descargarla, descifrarla, realizar localmente la consulta, volver a cifrar y luego volverla a depositar con el proveedor. Esto, por supuesto, es muy costoso y hace perder el valor de acudir a un cómputo en la nube. Surge entonces la pregunta de si acaso es posible hacer consultas de la información en la propia nube, aunque esté cifrada, recuperar la respuesta y descargarla para entonces descifrarla y obtener la respuesta en claro de la consulta formulada. Algunos esquemas de cifrado que permiten realizar estos procedimientos de manera eficiente, son los llamados *homomorfismos de cifrado*.

Otro aspecto de la seguridad en el cómputo en la nube es el siguiente: En una relación entre un proveedor de cómputo en nube y un cliente puede haber varios puntos de suspicacia. Desde el punto de vista del cliente, él querría verificar en cualquier momento que el proveedor conserva la información que le ha sido encomendada y que ni la ha suprimido ni la ha modificado. Desde el punto de vista del proveedor, él querría evitar que el cliente pretenda desconocer que la información que le haya sido devuelta se le entregó tal como él la proveyó originalmente.

Por ejemplo, para detectar modificaciones, el cliente podría firmar con una propia clave secreta la información que entrega. Si la información que se le devolviera no satisficiera a la firma digital, tendría evidencia de que la información fue alterada, pero no sabría en dónde y no podría recuperarla. Las firmas digitales elaboradas con este propósito se llaman *códigos de autenticación de mensajes* (MAC: *Message Authentication Codes*), y pueden muy bien ser incorporados como sufijos a sus propios mensajes. Incluso es posible asociarle a un fichero todo un *árbol de síntesis*: las hojas son propiamente MAC's de bloques del fichero y los nodos internos son MAC's de bloques de MAC's [4].

Para verificar que el proveedor posee la información encomendada, el cliente podría elegir una familia de funciones de síntesis \mathcal{H} , y antes de entregar una información F podría calcular la familia de sus síntesis $(h(F))_{h \in \mathcal{H}}$ y conservarla para sí. Así en cualquier momento posterior, el cliente podría desafiar al proveedor planteándole una función $h \in \mathcal{H}$, y a este desafío, el proveedor debería responder con el valor

$h(F)$. Si en un momento dado el proveedor no puede responder satisfactoriamente al desafío, el cliente tendría evidencia de que el proveedor ha perdido F .

Veamos a continuación algunos protocolos específicos.

2.1. Homomorfismos de cifrado

Una *función de cifrado* $e : M \rightarrow C$ asocia a cada mensaje en claro $m \in M$ un *texto cifrado* $c = e(m) \in C$, y depende, naturalmente, de una *clave* $k \in K$, que puede ser pública o privada. La función de cifrado debe ser inyectiva y debe poseer una propia *función de descifrado* $d : C \rightarrow M$. De hecho, se ha de tener (1)

$$\forall m \in M : d(e(m)) = m \text{ y también } \forall c \in C : e(d(c)) = c.$$

Si al conjunto de mensajes se le ve como una base de datos, una *consulta* es propiamente un operador $\gamma : M^n \rightarrow M$: ante n operandos (m_0, \dots, m_{n-1}) , ha de producir una *respuesta* $m = \gamma(m_0, \dots, m_{n-1})$. La consulta, en el espacio de los textos cifrados, se convierte en la composición de funciones (2)

$$\gamma^* : (c_0, \dots, c_{n-1}) \mapsto e \circ \gamma(d(c_0), \dots, d(c_{n-1})).$$

La parte derecha de (2) ejecuta el procedimiento descrito al inicio de la presente sección: dados los cifrados c_i , los descifra para pasar al espacio de mensajes en claro, resuelve ahí la consulta, y luego cifra para regresar al espacio de textos cifrados.

El cliente busca entonces una expresión equivalente a γ^* pero que sea menos onerosa.

En el mejor de los casos, si los espacios de mensajes en claro y de textos

cifrados coincidieran, podría aspirarse incluso a que $\gamma^* = \gamma$, en cuyo caso, el costo de la consulta en el espacio de textos cifrados coincidiría obviamente con su costo en el de mensajes en claro. Para esto último, se ve de las relaciones (1) y (2), que necesariamente ha de valer la relación.

$$\forall m_0, \dots, m_{n-1} \in M : e \circ \gamma(m_0, \dots, m_{n-1}) = \gamma(e(m_0), \dots, e(m_{n-1})).$$

Cuando se cumple esta última relación, se dice que e es un *homomorfismo de cifrado*, respecto al operador γ , es equivalente a decir que las operaciones de cifrado y de consulta "conmutan", es irrelevante el orden en que se ejecutan. Con un tal homomorfismo, el cliente podría realizar las consultas en la propia nube sin tener que desvelar el contenido de su información en ningún momento.

Como el ejemplo más elemental, recordemos que en el esquema de cifrado RSA, la clave pública de un cliente está conformada por una pareja de enteros (n, e) donde $n = pq$ el producto de dos primos suficientemente grandes. Su clave privada es la tripleta (p, q, d) donde $d = e^{-1} \pmod{(p-1)(q-1)}$. El espacio de mensajes en claro y de textos cifrados es el anillo de enteros módulo n , \mathbb{Z}_n . La función de cifrado es $e : m \mapsto m^e \pmod n$ y la de descifrado es $d : c \mapsto c^d \pmod n$ (nos disculpamos por denotar de la misma manera a los exponentes y a las exponenciaciones). Ya que

$$(m_0 \cdot m_1)^e \pmod n = (m_0^e \pmod n) \cdot (m_1^e \pmod n)$$

tenemos que el cifrado es un homomorfismo de cifrado respecto al producto.

Un *homomorfismo completo de cifrado* (FHE: *Fully Homomorphic Encryption*), para una clase de operadores Γ es una función e tal que se cumple la relación (3) para todo operador $\gamma \in \Gamma$. Desde la década de los 70 se planteó el problema de construir FHE's para ciertas clases de funciones. A finales de la década pasada, Craig Gentry propuso un primer FHE para funciones booleanas [5][6][7]. Una FHE puede también construirse codificando programas para calcular eficientemente, sin necesidad de descifrar, los operadores γ^* , dados por la relación (2), para cada uno de los operadores $\gamma \in \Gamma$.

2.2. Prueba de posesión de la información

El protocolo de Filho-Barreto se presentó en 2006 [8]. Se supone que un proveedor posee una información digital solicitada por un cliente.

Se quiere, por un lado, que el proveedor entregue la información sin ninguna alteración, y por otro que el cliente no pretenda desconocer que haya recibido la información legítima cuando ya se la hubiera entregado el proveedor. En un escenario, el proveedor podría ser un agente que renta filmes en DVD y el cliente un solicitante de un filme en renta, o en otro, el proveedor sería uno de cómputo en nube y el cliente un solicitante de un fichero que hubiera depositado ahí previamente en custodia, y del cual no conservó copia alguna.

Además del proveedor y del cliente, participa un *servidor*, como una tercera parte que certifica que las transacciones se realicen de manera legal.

Sean $m, n \in \mathbb{Z}^+$ dos enteros positivos, con $m \gg n$. Para $b \in \mathbb{Z}_n - \{0, 1\}$ fijo, la función $H_{bmn} : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$, $d \mapsto H_{bmn}(d) = b^d \pmod n$, es un homomorfismo del grupo aditivo $(\mathbb{Z}^m, +)$ al semigrupo multiplicativo (\mathbb{Z}^n, \cdot) , es pues una función de síntesis que es a la vez un homomorfismo. Claramente, dos elementos $d, e \in \mathbb{Z}^m$ colisionarán siempre que $d = e \pmod{\phi(n)}$, donde ϕ es la función *indicatriz* de Euler (en cada entero tiene como valor el número de elementos entre 1 y él que son primos relativos con ese entero). Así que si se conociera $\phi(n)$ sería muy fácil encontrar parejas de colisiones. Pero si n fuese un entero de RSA, $n = pq$, con p y q primos, conocer $\phi(n)$ puede ser equivalente a factorizar n .

Supongamos que \mathbb{Z}_m es el espacio de mensajes. Inicialmente, la tercera parte, el servidor, elige un entero de RSA, $n = pq$, con p y q primos, publica n y guarda para sí p y q . El servidor conoce $\phi(n) = (p-1)(q-1)$ y puede calcular la proyección $\pi_{m, \phi(n)} : \mathbb{Z}_m \rightarrow \mathbb{Z}_{\phi(n)}$, $d \mapsto \pi_{m, \phi(n)}(d) = d \pmod{\phi(n)}$. También el servidor considera como espacio de claves \mathbb{Z}_k y una función de "enmascaramiento" $f : \mathbb{Z}_k \rightarrow \mathbb{Z}_m$.

Envío de ficheros. El proveedor ha de entregar el mensaje $d \in \mathbb{Z}_m$ al cliente (ver **figura 1**).

Para verificar que la transmisión haya sido correcta, cualquiera de P o de C , somete al servidor S la pareja (κ, ρ) , donde $\rho = \rho_P = \rho_C$, así como el mensaje $d \in \mathbb{Z}_m$. El servidor calcula $\rho_S = H_{bmn}(f(\kappa)) \cdot b^{\pi_{m, \phi(n)}(d)}$ en \mathbb{Z}_n . Si acaso $\rho == \rho_S$, el servidor dictamina que la transmisión fue correcta.

Como un segundo protocolo, supongamos que el cliente ha deposti-

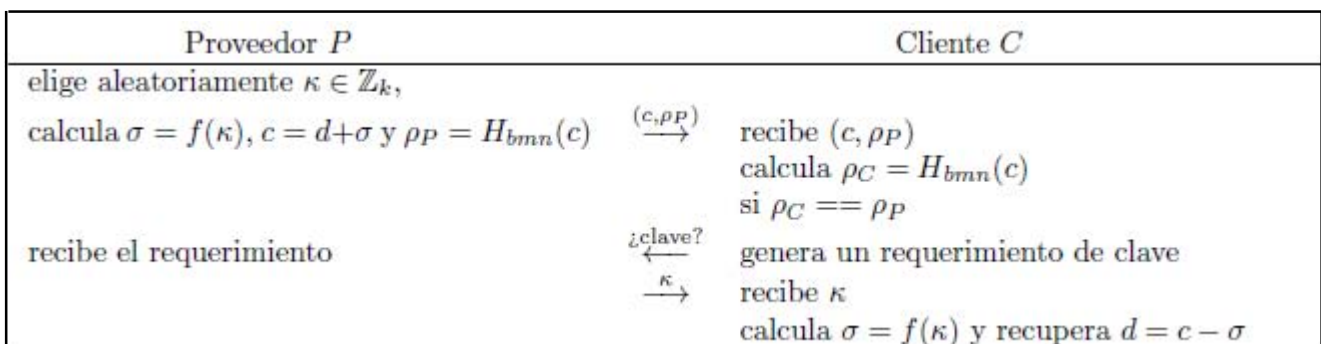


Figura 1. Entrega del mensaje del proveedor al cliente.

Cliente C	Proveedor P
elige un $b \in \mathbb{Z}_n - \{-1, 0, 1\}$	\xrightarrow{b} recibe b
recibe r	\xleftarrow{r} calcula $r = H_{bmn}(d)$
calcula $r' = H_{bmn}(d')$	
si $r == r'$ comprueba que P posee d	

Figura 2. Comprobación de que el proveedor posee el mensaje.

tado un mensaje $d \in \mathbb{Z}_m$ con el proveedor y quiere estar seguro de que el proveedor lo mantiene y no lo ha eliminado (acaso con el propósito de utilizar el espacio que quede libre).

Con los parámetros y los participantes arriba expuestos, supongamos que el servidor le entrega al cliente el valor de síntesis $d' = \pi_{m,\phi(n)}(d)$.

Prueba de posesión de datos. El cliente quiere comprobar que el proveedor está en posesión del mensaje $d \in \mathbb{Z}_m$ (ver figura 2).

2.3. Recuperabilidad

Desde el punto de vista de un proveedor de servicios de cómputo en la nube, luego de haber recibido diversos ficheros y de haberlos guardado a lo largo de varios períodos de tiempo, que pueden ser desde unos cuantos nanosegundos hasta varios años, de acuerdo con normatividades usuales de conservación de datos digitales, el proveedor debe mostrar que los ficheros que le han sido encomendados no han sufrido alteración alguna. Los protocolos criptográficos que permiten esta constatación forman la denominada *prueba de recuperabilidad* (POR: *proof of retrievability*) [9].

Un proveedor P hará las veces de *probador* de que el fichero bajo su custodia no ha sido modificado, en tanto que un cliente V , acaso propietario del fichero, hace las veces de un *verificador* de la prueba provista por P .

Sea $\mathbb{B}_\ell = \{0, 1\}^\ell$ el conjunto de palabras consistentes de ℓ bits cada una. Se puede confundir naturalmente al conjunto de palabras \mathbb{B}_ℓ con el cuerpo finito F_2^ℓ de característica 2. Supongamos que un fichero $F = (F_i)_{i=0}^{m-1}$ se ha factorizado como la concatenación de m palabras $F_i \in \mathbb{B}_\ell$. Se puede entonces elegir un (n, ℓ) -código lineal H y almacenar, en vez de F , a su código $F^* = (H(F_i))_{i=0}^{m-1}$, junto con una lista de MAC's $(\mu_i)_{i=0}^{m-1}$ donde cada μ_i es una firma digital de $H(F_i)$ elaborada con la clave secreta del cliente. Los MAC's hacen las veces de *verificadores de integridad de grano grueso*, en tanto que los códigos $H(F_i)$ son *verificadores de integridad de grano fino* que permitirían, inclusive, corregir errores.

La ventaja principal en esta factorización de la información está en que el cliente podría solicitar en cualquier momento una subsucesión $G_I = ((H(F_i), \mu_i))_{i \in I}$, para un subconjunto de índices $I \subset \llbracket 0, m-1 \rrbracket$, que elija aleatoriamente, y a partir de la respuesta que obtenga del proveedor podría verificar que éste mantiene

una copia incólume del fichero depositado, y esto sin necesidad de descargar completamente una copia del fichero F . Por supuesto que el tamaño de I fijará el nivel de confianza en esta prueba.

En este mismo sentido, se han desarrollado protocolos para que un cliente verifique que el proveedor mantiene el número de réplicas que asegura tener del fichero provisto o bien para verificar que el fichero puede subsistir a pesar de que se haya tenido un cierto número de fallas en sus copias.

2.4. Uso de curvas elípticas

Un esquema de recuperabilidad utiliza curvas elípticas y es similar al esquema de cifrado KMOV [10]. Para dos parámetros a, b se considera la ecuación de Weierstrass $E_{ab} : Y^2 = X^2 + aX + b$.

Si $p \in \mathbb{Z}^+$ es un entero primo entonces la curva elíptica $E_{ab}(\mathbb{F}_p)$ es un grupo abeliano, y su operación suma

$$((x_0, y_0), (x_1, y_1)) \mapsto (x_0, y_0) +_p (x_1, y_1) = (x_2, y_2)$$

se calcula haciendo (4)

$$\begin{aligned} x_2 &= (\lambda^2 - x_0 - x_1) \bmod p \\ y_2 &= (\lambda(x_0 - x_2) - y_0) \bmod p \end{aligned}$$

donde

$$\lambda = \begin{cases} (3x_0^2 + a)(2y_0)^{-1} & \text{si } x_0 = x_1 \bmod p \\ (y_0 - y_1)(x_0 - x_1)^{-1} & \text{si } x_0 \neq x_1 \bmod p \end{cases}$$

Si p, q son dos primos, de aproximadamente el mismo número de bits en sus representaciones binarias, se considera su producto $n = pq$. La curva $E_{ab}(n)$ se define como la suma directa $E_{ab}(n) = E_{ab}(\mathbb{F}_p) \oplus E_{ab}(\mathbb{F}_q)$. Pues bien, puede verse que una manera de representar a esta curva es como $E_{ab}(\mathbb{Z}_n)$, es decir, como el conjunto de parejas en \mathbb{Z}_n^2 que satisfacen la ecuación de Weierstrass E_{ab} , donde las operaciones se realizan de manera similar a las relaciones (4), pero en el anillo \mathbb{Z}_n . El módulo n puede hacerse público y cualquiera puede calcular en consecuencia la aritmética de la curva $E_{ab}(n)$.

En particular, para $a = 0$, resulta que la curva $E_{0b}(\mathbb{F}_p)$ contiene exactamente $p + 1$ puntos, por lo que la curva $E_{0b}(n)$ tiene orden $(p + 1)(q + 1)$. Por tanto, conocer el orden de $E_{0b}(n)$ puede ser tan complejo como factorizar n .

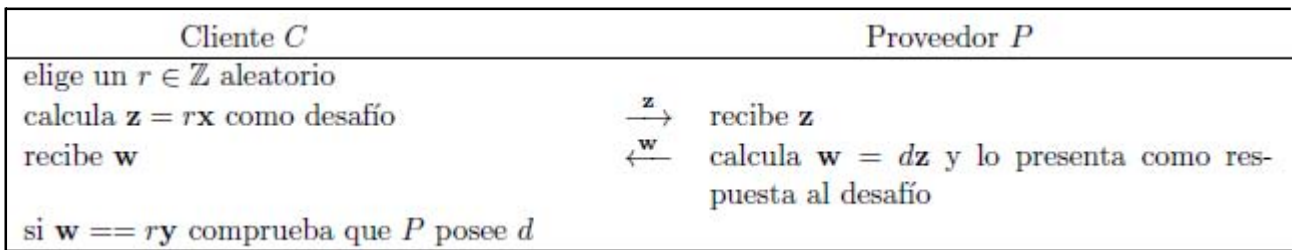


Figura 3. Prueba de posesión de datos del proveedor P.

El cliente entonces genera una curva elíptica $E_{ob}(n)$ cuyo orden o_n sólo él conozca y elige un generador $\mathbf{x} \in E_{ob}(n)$ de un subgrupo de la curva de orden suficientemente grande de manera que el Problema del Logaritmo Discreto sea difícil en el subgrupo $\langle \mathbf{x} \rangle$ generado por \mathbf{x} . Cuando va a depositar una información $d \in \mathbb{Z}$, calcula el elemento (5) $\mathbf{y} = (d \bmod o_n)\mathbf{x}$ y lo conserva para sí.

Prueba de posesión de datos. El cliente quiere comprobar que el proveedor está en posesión del mensaje $d \in \mathbb{Z}$ (ver figura 3).

En efecto, si todo ha sido ejecutado de manera correcta, se ha de tener:

$$\mathbf{w} = d\mathbf{z} = d(r\mathbf{x}) = r(d\mathbf{x}) = r\mathbf{y}.$$

Si hubiera perdido d , el proveedor no podría superar la prueba. Primero, el proveedor debería resolver el Problema del Logaritmo Discreto para calcular r a partir de que sabe que $\mathbf{z} = r\mathbf{x}$, luego, si acaso hubiera calculado \mathbf{y} al recibir d , para recuperar d , debería resolver una nueva instancia del Problema del Logaritmo Discreto, lo que hace extremadamente implausible que pueda responder con el valor correcto de \mathbf{w} .

Vale la pena observar que el mensaje d depositado por el cliente en los recursos del proveedor puede ser un mero mensaje en claro, o bien la codificación, con el propósito de poder corregir errores, o el cifrado, con el propósito de mantener la confidencialidad, de uno en claro.

3. Conclusiones

La seguridad en el cómputo en la nube es fundamental, y a primera vista pareciera que fuera inversamente proporcional a su desempeño: para realizar procesamientos remotos de manera tanto más eficiente, más abierta (o menos segura) se debe confiar la información de los clientes a los proveedores. Obviamente, una nube insegura es absolutamente inútil. Una nube sobreprotegida conlleva altos costos económicos y de recursos temporales y espaciales. Se debe pues mantener un equilibrio entre seguridad y eficiencia. Diversos protocolos criptográficos han sido desarrollados para garantizar confidencialidad, integridad y disponibilidad, y en la actualidad los proveedores de cómputo en la nube los han implementado con varios grados de calidad.

Referencias

- [1] ITU Telecommunication Standardization Bureau Policy & Technology Watch Division. *Activities in Cloud Computing Standardization Repository* (Version 1.0, May 2010). <http://www.itu.int/dms_pub/itu-t/oth/49/01/T49010000020002PDFE.pdf>.
- [2] Sixto Ortiz. The Problem with Cloud-Computing Standardization. *Computer*, 44(7):13-16, julio 2011.
- [3] Wayne Jansen, Timothy Grance. Guidelines on security and privacy in public cloud computing. *NIST Special Publication*, 800-144, diciembre 2011.
- [4] Christian Cachin, Idit Keidar, Alexander Shraer. Trusting the cloud. *SIGACT News*, 40:81-86, junio 2009.
- [5] Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford, CA, USA, 2009. AAI3382729.
- [6] Craig Gentry. Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st annual ACM symposium on Theory of computing, STOC '09*, pp. 169-178, New York, NY, USA, 2009. ACM.
- [7] Marten van Dijk, Craig Gentry, Shai Halevi, Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. En Henri Gilbert, editor, *EUROCRYPT, volume 6110 of Lecture Notes in Computer Science*, pp. 24-43. Springer, 2010.
- [8] Décio Luiz Gazzoni Filho, Paulo Sérgio Licciardi Messeder Barreto. Demonstrating data possession and uncheatable data transfer. *IACR Cryptology ePrint Archive*, 2006:150, 2006.
- [9] Ari Juels, Burton S. Kaliski Jr. Pors: proofs of retrievability for large files. En Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors, *ACM Conference on Computer and Communications Security*, pages 584-597. ACM, 2007.
- [10] Kenji Koyama, Ueli M. Maurer, Tatsuaki Okamoto, Scott A. Vanstone. New public-key schemes based on elliptic curves over the ring \mathbb{Z}_n . En Joan Feigenbaum, editor, *CRYPTO, volume 576 of Lecture Notes in Computer Science*, pp. 252-266. Springer, 1991.

Seguridad en la nube, algo nuevo bajo el sol

Olof Sandstrom
Director de Operaciones de Arsys

<osandstrom@arsys.es>

1. Introducción

Desde que se empezó a popularizar la prestación de servicios de Internet en la nube se ha estado hablando de los aspectos relacionados con la seguridad. Desde distintos foros se le han atribuido al *Cloud Computing* una serie de deficiencias en materia de seguridad que supuestamente no existían en los entornos tradicionales. Entre los aspectos que normalmente se mencionan podemos destacar:

- Los datos ya no están en los servidores de la empresa sino en los servidores de un proveedor externo.

- No es sencillo garantizar que los datos no van a salir del país, lo cual desde el punto de vista de la protección de datos de carácter personal supone un serio problema.

- Como cliente, no tengo derecho a auditar la seguridad del proveedor donde están alojados los servidores desde los que se accede a mis datos.

- Si el Centro de Proceso de Datos de mi proveedor se cae, me quedo sin servicio.

- Mi organización tiene que fiarse de las medidas de seguridad que el proveedor haya puesto en producción.

- Los sistemas de detección y prevención de intrusiones de mi proveedor no paran todos los ataques informáticos que recibe.

- Por otro lado, se habla de que para tener unos servicios seguros en la nube se debe escoger un proveedor que tenga alta disponibilidad en su centro de proceso de datos, cortafuegos, herramientas para el control de código malicioso, sistemas de detección y prevención de intrusiones, etc.

Sinceramente, mencionar que han aparecido estos problemas de seguridad en el *Cloud Computing* como algo nuevo no es serio. Realmente estos aspectos no tienen absolutamente nada que ver con el hecho de que se presten desde la nube o desde entornos tradicionales basados en servidor, por lo que se hace necesaria una reflexión sobre cada una de estas supuestas amenazas, que nos ayude a acabar con algunos falsos mitos y a comprender mejor el funcionamiento y las ventajas del *Cloud Computing*.

Desde hace años las empresas externalizan sus servidores y sus servicios de Internet en proveedores de servicios de Internet (*Internet Service Providers* o ISP). Por lo tanto, la prestación de los servicios en la nube no introduce ninguna consideración nueva a este respecto en materia de seguridad.

Resumen: Al *Cloud Computing* se le suelen atribuir aspectos relacionados con la seguridad que no tienen que ver con el hecho de que los servicios se presten desde la nube. Es necesaria una reflexión. El nivel de seguridad que proporciona un ISP suele ser bastante más elevado que el proporcionado por una empresa en sus propias instalaciones, por su alta disponibilidad, cortafuegos, sistemas de detección y prevención, monitorización 24 x 7, etc. El *Cloud* permite aprovisionar rápidamente una nueva plataforma completa, dimensionar los sistemas según necesidades, concentrar servicios en un mismo entorno y pagar por ellos cuando los usemos. En la nube, las soluciones de seguridad tradicionales son parte integral del servicio.

Palabras clave: Almacenamiento externo, Centro de Proceso de Datos, *Cloud Computing*, *Cloud Hosting*, CPD, entorno *Cloud*, ISP, seguridad, servidores, sistemas de certificación, virtualización.

Autor

Olof Sandstrom es Director de Operaciones de Arsys. Es Ingeniero Técnico de Telecomunicación por la Universidad de Las Palmas de Gran Canaria, y *Certified Information Systems Auditor* y *Certified Information Security Manager* por la Asociación para la Auditoría y Control de los Sistemas de Información (ISACA). Se incorporó a Arsys en 2006 como Director de Seguridad, procedente de la entidad de certificación Applus+. En 2009 fue nombrado Director de Operaciones, con el objetivo de definir las líneas estratégicas de los Procesos de Desarrollo Tecnológico (I+D+i) y de Seguridad Integral de Arsys. Además, Sandstrom es Presidente de la Comisión de Seguridad Integral de la patronal de empresas tecnológicas AMETIC.

Estos ISP disponen de Centros de Proceso de Datos (CPD) con unas medidas de seguridad mucho más elevadas, por lo general, que las medidas de seguridad que tiene implantadas la empresa dentro de sus instalaciones. La cuestión es que hasta ahora esta externalización se hacía sobre servidores físicos en lugar de hacerlo sobre servidores en *Cloud*, pero la realidad es que hace más de 10 años que los clientes están externalizando servicios, servidores, bases de datos, correo electrónico, etc. en ISP, depositando la confianza de la prestación de estos servicios y de la seguridad asociada a los mismos en las infraestructuras del proveedor.

Por su parte, que los datos salgan o no de un país depende exclusivamente del ISP que escogamos. Si para nuestra organización el hecho de que los datos no salgan del país, o de la Comunidad Económica Europea, es un requerimiento de negocio, deberemos hacérselo saber al proveedor durante el proceso de contratación, de forma que pueda diseñar nuestro servicio cumpliendo con este requerimiento.

Efectivamente, en la mayoría de los servicios que contratamos, como clientes, no tenemos derecho de auditoría sobre el servicio que nos están prestando. No podemos auditar a nuestro banco para verificar si está siguiendo los procesos bancarios de forma adecuada o no,

ni podemos auditar a la línea aérea con la que volamos para verificar si los mantenimientos de los aviones están haciendo regularmente y por personal cualificado. Simplemente tenemos que escoger a un proveedor que nos dé la confianza suficiente.

Cuando lo que se contratan son servicios de Internet la situación es similar. El ISP puede aportar las certificaciones de la empresa para prestar los servicios o los argumentos comerciales que estime oportuno, pero no es viable contemplar dentro de un contrato estándar el hecho de que cualquier cliente pueda auditar sus operaciones. En cualquier caso si esto fuera un requerimiento para la prestación de los servicios, ocurre algo similar a lo que planteaba en el caso de la salida o no del país de los datos, el cliente se lo debe de transmitir al proveedor durante el proceso de contratación, y éste determinará si está en condiciones de ofrecer ese servicio, y cuánto cuesta.

Pero en cualquier caso no se trata de un problema que haya aparecido con el *Cloud*, es la misma situación que teníamos cuando lo que se contrataban eran servidores físicos.

Si el CPD del proveedor se cae, el servicio se cae, pero una vez más esto no tiene absolutamente nada que ver con el *Cloud*. Los CPD ya se caían antes de la aparición del *Cloud*. De hecho, se caían antes de que aparecieran

Microsoft, Linux y la mayoría de los sistemas que utilizamos hoy en día.

Mi organización tiene que fiarse de las medidas de seguridad que el proveedor haya puesto en producción. Normalmente, estas medidas se acuerdan previamente a la puesta en producción del servicio. Si el cliente contrata alta disponibilidad, cortafuegos, sistemas de detección y prevención de intrusiones, monitorización 24 x 7, gestión de capacidad, etc., el proveedor le proporcionará estos servicios.

Algo que sí es importante tener presente es que las medidas de seguridad de la mayoría de servicios hospedados en las instalaciones del cliente no son tan rigurosas como las que implantan los ISP. No es frecuente que una empresa disponga de un CPD con dos centros de transformación eléctrica, dos grupos electrógenos, dos sistemas de alimentación ininterrumpida, dos circuitos de datos, un equipo técnico con presencia 24 x 7, y cortafuegos en alta disponibilidad, sistemas de detección y prevención de intrusiones en producción y cortando ataques y, en definitiva, un equipo técnico altamente cualificado monitorizando y supervisando la situación de los distintos servicios.

Por todo ello, normalmente el nivel de seguridad que proporciona un ISP suele ser bastante más elevado que el que proporciona una empresa en sus propias instalaciones.

Por último, en relación a los sistemas de detección y prevención de intrusiones, hoy en día cualquier servidor que esté conectado a Internet recibe ataques. No es necesario que se trate de un objetivo estratégico para los atacantes, simplemente existen organizaciones que lanzan ataques indiscriminadamente y los mismos perfiles de los ataques varían constantemente. Por eso, es necesario contar con un equipo humano de profesionales de seguridad que modelicen estos ataques y programen firmas específicas que sean capaces de detectarlos y bloquearlos.

Los ISP suelen contar con estos profesionales en plantilla, de forma que sus sistemas de detección y prevención de intrusiones están mejor ajustados que los que están en producción en aquellos entornos en los que no se cuenta con este equipo técnico.

Pero, una vez más, esta situación no tiene nada que ver con el hecho de que los servicios se presten desde la Nube o desde un entorno tradicional, ya que no hay diferencias entre atacar a una plataforma hospedada en *Cloud* o a una plataforma hospedada en un entorno físico.

2. ¿Por qué todo el mundo habla de la nube?

Cuando se habla de la prestación de servicios desde la nube siempre se hace referencia al significativo ahorro de costos que supone el hecho de contar con una plataforma en la cual sólo se paga por lo que se usa. Realmente, la nube ofrece muchísimas más cosas y algunas de ellas son absolutamente diferenciales a la hora de prestar servicios en Internet.

En cierta forma pasa algo parecido a lo que ocurre con los coches automáticos. La mayoría de nosotros estamos acostumbrados a utilizar coches con cambio manual y, cuando alguien nos plantea la posibilidad de comprar un coche con cambio automático, decimos que no. Argumentamos que se averían más, que tiene menos control sobre la marcha del vehículo, que aumenta el consumo de gasolina, etcétera.

Sin embargo, no conozco a nadie que después de haber estado utilizando un coche automático durante un tiempo, vuelva a comprarse un coche con cambio manual. En *Cloud* pasa algo parecido, conozco mucha gente que ha puesto todas las pegadas del mundo antes de empezar a utilizar servicios en *Cloud*, pero no conozco a nadie que después de haberlo probado vuelva a trabajar con entornos físicos. *Cloud* supone un cambio radical en la forma de pensar y en la manera de trabajar de las personas responsables de diseñar y poner en producción los servicios, dotándoles de unas herramientas que hasta el momento sólo eran un sueño, una utopía.

2.1. Aprovisionamiento

Tal vez uno de los aspectos más significativos sea la posibilidad de aprovisionar muy rápidamente una nueva plataforma completa, un mini CPD, a golpe de ratón y en un tiempo muy reducido. En un entorno físico tradicional poner en producción una plataforma que cuente con varios frontales web, servidores *backend* de base de datos, balanceo de carga, cortafuegos, políticas de copia de seguridad, redes privadas virtuales y todo lo necesario para poner en producción un nuevo servicio Internet puede llevarnos varias semanas.

Dependerá, fundamentalmente, del plazo que tengamos para que nos aprueben el presupuesto, aprovisionar el equipamiento, de lo que tardemos en instalarlo y, por último, de lo que tardemos en configurar todo el entorno de red.

En la nube este tipo de acciones se hace a golpe de ratón y se puede tener todo el entorno en producción en un par de horas. Esta facilidad a la hora de aprovisionar entornos y plataformas era impensable cuando trabajábamos con entornos físicos tradicionales. Normalmente las organizaciones dedican muchísimo tiempo a planificar los entornos y preparar solicitudes de ofertas, pedidos, asignación de recursos, etc. antes de ni siquiera poder empezar a plantear la puesta en marcha del servicio.

Ahora simplemente los técnicos tienen que sentarse delante del panel de control para diseñar su plataforma, darle a un botón del ratón y ponerla en producción. Así de fácil.

2.2. Gestión de recursos

La gestión de capacidad de recursos de procesador, memoria o disco, es otro de los grandes dolores de cabeza de los equipos técnicos cuando trabajan con entornos físicos. Los entornos tienen que dimensionarse para la capacidad máxima de recursos que van a consumir, aunque esta demanda de recursos sólo se dé durante una o dos semanas al año. Para aumentar o disminuir los recursos en un entorno físico es necesario hacer intervenciones bastante costosas, que siempre implican corte del servicio.

En los entornos *Cloud* el cliente puede dimensionar sus sistemas para las necesidades habituales y aumentar o disminuir sus recursos en caliente cuando lo requiera pagando, en cada caso, únicamente por los recursos que está utilizando.

2.3. Entornos de desarrollo, pruebas y producción

Aunque las buenas prácticas dicen que las plataformas críticas deberían contar con entornos separados de desarrollo, pruebas, y producción, la realidad es que el disponer de estos tres entornos en una plataforma física supone un sobrecoste que, para la mayoría de las organizaciones, no es asumible.

Cuando estas plataformas se ponen en producción desde la nube resulta rápido, sencillo y barato poder desplegar los entornos de desarrollo y pruebas asociados al entorno de producción. Para empezar, únicamente pagaremos por estos entornos durante el tiempo en el que estén funcionando.

Por otra parte, la espada de Damocles que siempre han supuesto las averías del equipamiento (en tanto en que, si una máquina se avería, el servicio se ve afectado) desaparece en los entornos *Cloud*. Si una máquina física se estropea, las máquinas virtuales (que son las que realmente están ejecutando los servicios) "vuelan" de un servidor físico a otro, sin que prácticamente resulte perceptible en el servicio.

En este sentido, nos olvidamos completamente de qué equipamiento hardware tenemos por debajo de nuestros servicios, para centrarnos únicamente en los recursos que nuestro servicio necesita.

2.4. Concentración de servicios

Lo que sí es cierto es que la aparición de servicios en la nube ha supuesto una concentración de servicios en un mismo entorno muy superior a lo que conocíamos hasta el momento.

En un entorno *Cloud* podemos encontrarnos con 1.500 servidores virtuales corriendo dentro de un único *rack*. Con el antiguo modelo físico, si se caía un *rack* afectaba a 40 servidores, mientras que ahora si se cae un *rack*, en realidad, se están cayendo 1.500 servidores. Esto hace que lo que antes podía ser una incidencia más o menos asumible, ahora sea realmente una crisis, ya que entre que se caigan 40 servidores ó 1.500 puede mediar un abismo en lo que a impacto se refiere.

En este sentido, no es que *Cloud* se caiga más. De hecho, se cae mucho menos, pero lo que es indiscutible es que cuando se cae afecta a muchísimos más servicios.

3. Entonces, ¿qué hay de nuevo?

Dentro de este nuevo escenario, el ISP tiene que aportar confianza a sus clientes de una forma mucho más clara que en el pasado. Las certificaciones de sistemas de gestión (de calidad, de seguridad, de gestión medioambiental o de servicios) suelen tener detractores que alegan que una empresa esté certificada no quiere decir que haga bien las cosas.

Lo cierto es que una organización que dispone de todos los procedimientos, normativas, manuales y políticas que exigen estos sistemas de certificación, los ha puesto en producción y ha pasado satisfactoriamente una auditoría de certificación de una tercera parte de confianza (entidad de certificación acreditada), sin ningún género de dudas tiene que ser más fiable que otra que no lo ha hecho.

De forma similar, las certificaciones personales del equipo técnico que va a dar soporte a la plataforma de los clientes dan al mercado un mensaje claro de que esa organización cuenta con profesionales capacitados para la prestación del servicio. No porque lo diga la empresa, sino porque lo dice el fabricante de las tecnologías en las que se basa el servicio.

3.1. Soporte técnico

Con respecto al soporte técnico, debemos tener muy presente el nivel de soporte que nos va a prestar el proveedor.

Empleando el símil de los coches, nos compramos un coche porque nos gusta, es potente, tiene buenas medidas de seguridad, consume poco, etc. Y, sin embargo, lo que realmente nos enamora de un coche es que no nos deje tirados en la carretera, que cuando lo llevemos al taller siempre haya alguien ahí para atendernos, que nos lo reparen bien y rápido, en resumen, que haya un buen servicio detrás de lo que hemos comprado.

Con los servicios de *hosting* pasa lo mismo: tan importante es el servicio que hemos contratado como el soporte que nos va a prestar el proveedor.

Por eso es tan importante tener presente a la hora de contratar un proveedor de servicios *Cloud* todos los aspectos relacionados con el soporte: si el soporte va a ser 24 x 7, si voy a tener atención telefónica o sólo correo electrónico y si voy a poder tener acceso a un grupo de especialistas en caso de que lo necesite, etc. Por tanto, para los proveedores es fundamental poder acreditar que el servicio que ofrecen cuenta con un soporte excelente.

3.2. Seguridad

Con respecto a la seguridad, el entorno *Cloud* también supone un cambio de perspectiva. En el entorno tradicional, a la hora de contratar un servicio de *hosting*, las soluciones de seguridad tradicionales (cortafuegos, antivirus, IDS, etc.) no se han tenido en cuenta como una parte integral del servicio, sino como elementos opcionales que se podían contratar o no.

Volviendo al mundo del automóvil podemos equipararlo a que durante años los coches no venían con cinturones de seguridad en las plazas traseras, *airbags*, frenos con ABS o control de tracción ESP. Estas medidas de seguridad eran opcionales. Sin embargo, hoy en día vienen de serie en la mayoría de los vehículos.

Con los servicios de *Cloud* pasa lo mismo, todas estas soluciones tradicionales de seguridad deben dejar de ser opcionales y entrar a formar parte del servicio como una característica más.

En términos generales la seguridad de los servicios en la nube no difiere demasiado de la seguridad en entornos tradicionales. Digamos que una vez que el tráfico ha salido del *host* físico donde están corriendo las máquinas virtuales, las medidas de seguridad en un entorno tradicional y en un entorno *Cloud* son bastante similares.

Donde sí se introducen diferencias significativas en lo que se refiere a la seguridad es en el aislamiento que hay que establecer entre las máquinas virtuales que están dentro de una misma máquina física, para que no puedan "verse" entre sí.

Estas características de aislamiento deben estar incorporadas en la arquitectura base del proveedor de servicios *Cloud*, de manera que una máquina virtual no pueda atacar fácilmente a otras máquinas que estén ejecutando dentro de la misma máquina física.

Tal vez uno de los retos más interesantes que tiene la industria de seguridad será el desarrollo de herramientas que se integren directamente a nivel de hipervisor, de forma que las soluciones estén totalmente integradas a bajo nivel en la arquitectura del *Cloud*.

3.3. Red

Con respecto a la red, hay que tener en cuenta que hasta el momento el hecho de que un servidor contase con uno o varios enlaces de Gb solía ser más que suficiente.

Con el esquema actual, nos encontramos con un servidor sobre el que realmente están corriendo hasta 100 máquinas virtuales, donde cada una de ellas está generando tráfico. Esto hace que el tráfico total de entrada y salida que tiene que gestionar el servidor físico a través de sus tarjetas de red sea muy superior a los niveles de tráfico a los que estábamos acostumbrados.

Por eso suele ser frecuente que se saturen más los enlaces de comunicaciones de los servidores cuando estamos trabajando en *Cloud*. Para solventar este problema lo que normalmente se hace es instalar o bien varios enlaces de Gb y agregarlos, o directamente instalar tarjetas con puertos de 10 Gb. En cualquier caso lo que ya no podemos hacer es utilizar los enlaces de *gigabyte* que utilizábamos hasta el momento ya que éstos lo saturaremos muy rápidamente.

3.4. Almacenamiento

También cambian considerablemente los requerimientos del sistema de almacenamiento externo con respecto a los requerimientos que teníamos hasta la fecha.

De forma similar a lo que nos ocurre con los enlaces de red, hasta ahora lo normal era que a una misma cabina de almacenamiento conectáramos hasta un total de 100 servidores físicos. Ahora, cuando se trabaja con entornos *Cloud* no es extraño encontrarnos con cabinas de almacenamiento que están prestando servicio a 1.200 o 1.500 servidores virtuales. Evidentemente, los parámetros de rendimiento que requieren las cabinas en este último caso son muy superiores a los que normalmente demandábamos cuando las instalaciones se hacían basadas en entornos físicos. Así, los niveles de rendimiento que le vamos a exigir a las controladoras y los niveles de IOPS (operaciones por segundo) son muy superiores a lo que usábamos normalmente. Como no puede ser de otra forma debemos tener presentes estos nuevos requerimientos a la hora de diseñar la plataforma y escoger el equipamiento.

Y en lo que se refiere a los niveles de redundancia y la capacidad de replicación de las cabinas también debemos incorporar funcionalidades que nos permitan trasladar el almacenamiento entre cabinas, o incluso entre CPD, de una forma rápida y sencilla y, por supuesto, sin que afecte al servicio.

3.5. Gestión de capacidad

Por último, no podemos olvidar que los entornos de la nube simplifican de manera

importante la gestión de capacidad para el cliente final. Éste únicamente tendrá que determinar qué capacidad necesita, tanto en número de servidores, como los recursos de cada uno de ellos y, después, apretar un botón.

Desde el punto de vista del proveedor de servicios *Cloud*, ésto (que para el cliente es como una bendición del cielo) se puede convertir en un verdadero infierno.

En un entorno tradicional, cualquier ISP al que le llegara una solicitud de un cliente para levantar, digamos 100 servidores, tenía un plazo de varias semanas para poder poner en producción los equipos.


En un entorno *Cloud* esto no es así. Si un cliente decide aprovisionar digamos por ejemplo 100 servidores con dos procesadores, 4 Gb de memoria y medio Tb de almacenamiento, simplemente tiene que entrar en el panel de control, preparar la solicitud de la plataforma y darle el botón de "siguiente".



A partir de ese momento, el proveedor de servicios en la nube tiene que aprovisionar el equivalente a la capacidad de 200 procesadores, 400 Gb de memoria, y 50 Tb de disco y tenerlo en producción en un par de horas.

Los proveedores de servicios *Cloud* salvamos la dificultad que supone la gestión de capacidad, contando con un stock importante de equipos para poder absorber este tipo de demandas y con unos procesos de gestión de capacidad muy bien ajustados que nos permitan detectar rápidamente las necesidades de crecimiento de la plataforma.

iThings 2012

The 2012 IEEE International Conference on
Internet of Things
<http://ieee-iot.org/>
Besançon, France, September 11-14, 2012



Honorary chairs
Stephen Yau, Arizona State University, US
Ramon Puigjaner, Universitat de les Illes Balears, Spain

General Chairs
Julien Bourgeois, University of Franche-Comté, France
Josep Solé Pareta, Univ. Politecnica de Catalunya, Spain

INTRODUCTION
The Internet of Things (iThings) is a network of Internet-enabled objects and internet-based services, which aims at increasing the ubiquity of the Internet by integrating every object/service for interaction and leads to the highly distributed network of devices /services communicating with human beings as well as things. Combining with the infrastructures of the every heterogeneous networks including Internet and mobile networks, these objects can communicate with humans, and enable peoples to enjoy their intelligent services anytime, anywhere.

The 2012 IEEE International Conference on Internet of Things (iThings'12) will provide a high-profile, leading-edge forum for researchers, engineers, and practitioners to present state-of-art advances and innovations in theoretical foundations, systems, infrastructure, tools, testbeds, and applications for the Internet of Things, as well as to identify emerging research topics and define the future. iThings'12 is the next edition of the successful series, previously held as iThings'11 (Dalian, China), IOTS 2010 (Hangzhou, China), MINES 2009 (Hangzhou, China), and MINES 2008 (Chengdu, China).

Important Dates

Paper Submission Deadline:	May 15, 2012
Notification of Acceptance:	Jun 30, 2012
Camera-Ready Paper Due:	Jul 15, 2012

SCOPE AND INTERESTS
The scope of interest includes, but not limited to:

- Track 1. Architecture and Infrastructure
- Track 2. System Design, Modeling and Evaluation
- Track 3. Intelligent Data Processing and Ubiquitous Computing
- Track 4. Networks and Communications
- Track 5. Scalable distributed sensing and control
- Track 6. Reliability, Security, Privacy and Trust
- Track 7. Internet of nanothings and nanonetworks
- Track 8. Applications, Educations, Business and Social Issues

PAPER PUBLICATIONS
Each submission should be regarded as an undertaking that, if the paper is accepted, at least one of the authors must attend the conference to present the work in order for the paper to be included in the IEEE Digital Library. Accepted papers will be published in the proceedings of iThings'12 by IEEE Computer Society (EI indexed). Extended versions of selected papers will be considered for publication in several SCI-index international journals (check the website for details).

Jeimy J. Cano

Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática, Facultad de Derecho, Universidad de los Andes (Colombia)

<jjcano@yahoo.com>

Análisis forense en un ecosistema tecnológico: redes sociales, tecnologías móviles y computación en la nube

1. Introducción

Estamos en una época de cambios, transiciones y revoluciones que implican una valoración permanente del entorno por parte de los profesionales de todas las disciplinas. No hace algunos años estábamos preguntándonos por las implicaciones de las aplicaciones cliente/servidor y hoy estamos en la era de las aplicaciones y arquitecturas basadas en servicios. ¿Qué vendrá después? No sabemos, pero será algo que con toda seguridad nos hará nuevamente pensar e investigar para desafiar los límites del conocimiento.

Luego de estos primeros diez años del nuevo milenio, se advierten una serie de tendencias y estrategias tecnológicas que establecen nuevos retos para la seguridad de la información y por lo tanto, para la computación forense. De acuerdo con varias reflexiones revisadas alrededor de predicciones en seguridad de la información para los próximos 10 años se revelan en el horizonte aspectos críticos como [1]:

- Perímetros porosos y móviles
- Computación en la nube
- Desobediencia del factor humano
- Ciberseguridad e infraestructura crítica
- *Hacktivismo*

Cada uno de estos temas implica grandes interrogantes para la computación forense que son semejantes a los que la inseguridad plantea y materializa. Desarrollar una investigación forense en informática en algunos de los temas planteados exige el análisis detallado de cada uno de ellos, y descubrir la fuente del conocimiento y entendimiento que permite a la computación forense aportar en el develamiento de la verdad, esa que está tras las huellas informáticas de los intrusos.

En este contexto, este documento busca desarrollar una aproximación conceptual y práctica para descifrar algunos aspectos del análisis forense más allá de la nube (en un ecosistema tecnológico), como un primer esfuerzo académico para advertir aspectos clave y cuidados básicos que un investigador debe conocer y revisar cuando se enfrente al reto de un mundo administrado en torno a servicios, distribuido en muchas partes, balanceado en capacidad de almacenamiento, con aplicaciones en línea y operado por múltiples actores que exigen servicios de información instantánea.

Resumen: *Estamos en un mundo altamente influenciado por las tecnologías y servicios de información, una realidad donde todos creamos contenidos y somos parte del desarrollo de una nación sin fronteras como lo es Internet. En este sentido, este documento plantea una reflexión base para analizar conductas punibles en un escenario asistido por las redes sociales, las tecnologías móviles y la computación en la nube, un nuevo ecosistema tecnológico que revela la complejidad de las posibilidades y la realidad de la inseguridad en un medio lleno de relaciones, intereses y necesidades, que invita a repensar nuestra vista tradicional de las investigaciones forenses informáticas.*

Palabras clave: *análisis forense, computación en la nube, ecosistema tecnológico, redes sociales, tecnologías móviles.*

Autor

Jeimy J. Cano es Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes (Colombia) y Profesor Distinguido de dicha Facultad. Es Ingeniero y Magister en Ingeniería de Sistemas y Computación de la citada Universidad. Es doctor en *Business Administration* por la *Newport University* (CA, USA), *Executive Certificate in Management and Leadership* por la *MIT Sloan School of Management* (MA, USA) y egresado del programa de formación ejecutiva *Global Change Agent* de la *Harvard Kennedy School of Government* (MA, USA). Es profesional certificado como *Certified Fraud Examiner* (CFE) por la *Association of Certified Fraud Examiners*, y *Cobit Foundation Certificate* por ISACA.

Este intento por comprender las implicaciones del análisis forense en un ecosistema tecnológico implica comprender en primer lugar las consideraciones técnicas del modelo de servicios que se implementa en la nube, la seguridad de la información en este contexto, las redes sociales, los medios inalámbricos y cómo estas variables impactan el desarrollo de una investigación en dicho ecosistema.

2. Entendiendo la computación en la nube

Hablar sobre la computación en la nube no es solamente comentar sobre una moda o término deslumbrante para impresionar a otros, es hablar sobre toda una estrategia corporativa para afianzar un modelo de manejo de demanda de recursos tecnológicos que se inicia en infraestructura técnica: servidores, enrutadores, cajas de seguridad, hasta aplicaciones y productos de software que pueden ser utilizados por múltiples personas sin tener que instalar ningún programa adicional en los computadores de escritorio.

Para el *National Institute of Standard and Technology* (NIST norteamericano) la computación en la nube es "un modelo para manejo conveniente de la demanda de un conjunto de recursos computacionales compartidos (p.e redes, servidores, almacenamiento, aplicaciones y servicios) a través de redes, que pueden ser provisionados rápidamente

y entregados con un mínimo esfuerzo de administración o interacción con el proveedor del servicio" [2].

Esta definición nos advierte que este nuevo paradigma computacional busca el desarrollo de una computación de bajo costo, altamente eficiente y flexible según se requiera. En este sentido, los servicios, las aplicaciones y las infraestructuras forman parte del "lego tecnológico" que las empresas requieren para operar sin preocuparse por aspectos como cuánto procesamiento requieren, la compatibilidad entre plataformas, la continuidad ante fallas y la actualización del software base, entre otros.

Considerando la definición propuesta por el NIST y las investigaciones actuales sobre el tema [3][4] sí se tienen actualmente algunos acuerdos respecto a los servicios que se entregan en la nube como son software como servicio, plataforma como servicio e infraestructura como servicio (ver **figura 1**).

Software como servicio (SaaS) se traduce como la capacidad provista al consumidor o cliente de utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura tecnológica en la nube, la cual es accesible desde varios dispositivos tecnológicos a través de un cliente de interfase liviana como lo puede ser un navegador web. Esto es, *el cliente*

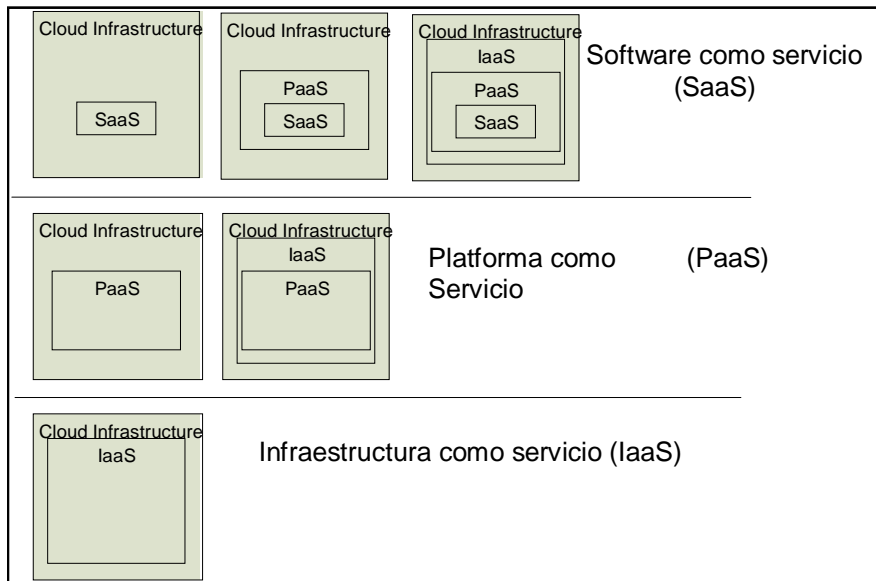


Figura 1. Esquema de servicios disponibles desde la nube (adaptado de [2]).

no tiene que preocuparse del software, tipo de sistema operativo o lenguaje en que está construida la aplicación. Adicionalmente no se requiere ninguna instalación de software adicional [4].

Plataforma como servicio (PaaS) es la capacidad provista al consumidor o cliente para desplegar en una infraestructura tecnológica en la nube las aplicaciones creadas por éste utilizando para ello lenguajes y herramientas de programación que son soportadas por el proveedor. Esto es, *el cliente final no controla o administra las redes, servidores, sistemas operativos o almacenamiento de las aplicaciones*, pero sí el despliegue de sus aplicaciones y posibles consideraciones del entorno de alojamiento de éstas [4].

Infraestructura como servicio (IaaS) nos habla de la capacidad provista al consumidor o cliente para alquilar recursos computacionales (capacidad de procesamiento, almacenamiento, redes, entre otros) donde éste tiene la posibilidad de desplegar y ejecutar software de manera libre, lo cual incluye tanto sistemas operativos como aplicaciones. Esto es, *el cliente no administra o controla la infraestructura en la nube*, pero sí lo hace sobre los sistemas operativos, el almacenamiento, el despliegue de las aplicaciones y posiblemente la selección de algunos componentes de red (por ej., *firewalls*, balanceadores de carga) [4].

En consecuencia con lo anterior, para darle vida a un esquema como el anteriormente presentado se requieren una serie de tecnologías y servicios que deben ser instalados y configurados de tal forma que la magia de la administración de la demanda de recursos de tecnologías de información sea una realidad.

A continuación detallamos algunas de esos elementos tecnológicos requeridos para que la nube pueda operar.

A **nivel de infraestructura**, se hace necesario establecer las redes de banda ancha que permitan un acceso prácticamente en línea a los recursos. Dichos recursos, como son servidores, almacenamiento y la red misma, deberán configurarse bajo una capa de virtualización que es la que permite reorganizar y armar los diferentes escenarios que demanden los clientes. Esto es posible gracias al software de virtualización que es el que le ofrece la flexibilidad al proveedor de servicios en la nube (PSN o CSP, *Cloud Service Provider*) para mover o asignar más o menos recursos dependiendo de la demanda de sus clientes.

A **nivel de plataforma**, una vez se encuentra configurada la infraestructura se inicia la instalación de los servicios requeridos para operar sus aplicaciones. Esto es los servicios de bases de datos, marcos de desarrollo (J2EE, .NET, WebServices, entre otros), consolas de administración de los servicios ofrecidos, tarificación de uso de los servicios, servicios de control de acceso, entre otros, que les permiten a los desarrolladores escribir y desplegar aplicaciones de manera ágil sobre la nube.

A **nivel de software**, se delega en un tercero el modelo de adquisición, licenciamiento y actualización de las aplicaciones. Esto es, que la organización centraliza el uso del software, haciendo liviana la ejecución de las mismas, pues no se requiere que se materialicen de manera local, utilizando recursos locales, sino con la distribución y uso más apropiado de la infraestructura propia del CSP. Esta estrategia de software en la nube generalmente requiere el

uso de algunos API (*Application Program Interface*) para acceso a través del navegador a los recursos disponibles en la nube.

3. Seguridad y control en la nube

La seguridad en una estrategia de computación en la nube, de acuerdo con Vinton Cerf, se basa en la confianza y en quién controla qué en el estilo de nube configurada (privada, pública o híbrida). Esto es, en una seguridad diseñada a nivel de la plataforma, PaaS y las aplicaciones SaaS, las cuales se basan en los servicios disponibles en estos dos niveles, y en un aseguramiento de la infraestructura (IaaS a cargo del CSP), basada en buenas prácticas de seguridad y control de las tecnologías de información reales propiedad del proveedor [5]. Éstas últimas deberán proveer parte de la seguridad contratada por el cliente, para lo cual deberá asegurarse con la definición de acuerdos de nivel de servicio que complementen los diseños de seguridad propios de sus aplicaciones [6][7][8].

A nivel de infraestructura en la nube, la consigna es pagar por la cantidad de procesamiento, espacio en disco y consumo de ancho de banda, entre otros. En este sentido, el CSP tiene el completo control de las máquinas y dispositivos tecnológicos, haciendo que el cliente solamente use lo que solicita, sin preocuparse por la forma como están organizados estos recursos. En consecuencia, existirá un concepto base de seguridad en la IaaS basado en el aseguramiento de los recursos virtualizados, el software utilizado para ello y las fallas asociadas con la arquitectura de software requerida para el manejo de la demanda de estos recursos.

De otra parte, a nivel de plataforma, la idea es contar con los modelos de operación de las aplicaciones, esto es los motores y modelos de despliegue de aplicaciones, las librerías y servicios requeridos por los marcos de desarrollo en los cuales se crean y funcionan los programas. En este contexto, el proveedor de servicios en la nube deberá establecer los servicios básicos de seguridad de la información de las aplicaciones, basado en un aseguramiento de los flujos de información diseñados alrededor del software y las especificaciones del cliente, como parte inherente del marco de desarrollo seleccionado, para que al desplugarlo se haga parte inherente de las soluciones que sobre ella se ejecuten.

Finalmente y no menos importante, a nivel del software que se desarrolla en la nube, el concepto de orientación a servicios se convierte en el paradigma de programación más apropiado para un despliegue ágil de dichos servicios, los cuales son publicados en directorios específicos en la nube para ser invocados por las aplicaciones generalmente orientadas al web, a través de API. En línea con lo anterior, las medidas de seguridad y control

propias del desarrollo de software deben estar asociadas con las funcionalidades y servicios expuestos a través de las aplicaciones, de tal forma que cualquier uso no autorizado se pueda advertir y atender siguiendo los protocolos de atención de incidentes previstos [9].

"En este contexto, el reto de los modelos, buenas prácticas y estrategias de seguridad y control no es ubicar las restricciones necesarias para mitigar o limitar las fallas propias de la operación de la nube, sino reconocer las relaciones y puntos de integración entre sus componentes que permitan simultáneamente compartir y aprender de la dinámica de la nube, y así aceptar el cambio continuo y natural de un concepto tecnológico que entiende el control y la seguridad como esa propiedad emergente propia del diseño de la interacción de cada uno de sus componentes tecnológicos, procedimentales y humanos, en el tejido estratégico de las iniciativas empresariales para generar valor con el cliente, que ahora vive en la nube." [10].

4. Análisis forense en un ecosistema tecnológico: Consideraciones básicas

Estamos asistiendo a una nueva década dominada por las redes sociales, la computación móvil y la computación en la nube. Esta nueva condición de la sociedad digital, ubica a la información como uno de los elementos más sensibles y más apetecidos por todos los participantes de esta realidad interconectada. Nada más cierto que el empoderamiento evidente de jóvenes y niños, que exigen de las redes mayor velocidad, mayor conectividad y renovados contenidos. Así las cosas, la información en movimiento, como la vida misma, es un reto que demanda de los mejores analistas de seguridad de la información, propuestas innovadoras para comprender ahora qué significa "estar seguros" en un ambiente de cambio permanente, altamente impredecible, inalámbrico y de operación 7x24x365.

Entender la realidad actual de servicios y conexiones "sin cables" es actualizar la reflexión de los retos asociados con los elementos materiales probatorios informáticos, medianamente conocidos y asegurados en un contexto cableado. Si encontrar o identificar a posibles atacantes en infraestructuras de configuraciones y flujos de información conocidos ha sido un reto evidente durante los últimos 10 años, sumergirse en el desafío forense a través de las redes sociales, en medios inalámbricos y administrados por un tercero en la nube, describe una nueva disciplina y nuevos campos de investigación que exigen repensar la informática forense o computación forense en un nuevo nivel, con una vista más sistémica, para establecer elementos sistemáticos que permitan avanzar en nuevos procedimientos estandarizados [11][12].

En un primer momento, conociendo esta realidad actual, se tiene la tentación de aplicar los procedimientos conocidos y generalmente utilizados para abordar el reto forense a través del trinomio red social, móviles y la nube, pues al estar cada uno de ellos articulados y fundados en plataformas tecnológicas suena coherente desarrollar los aseguramientos de evidencia, siguiendo los protocolos establecidos asociados con datos volátiles y no volátiles. Adicionalmente, poder seguir los rastros en cada uno de estos mundos, no debería ser diferente de lo que actualmente se efectúa cuando de investigaciones informáticas se trata.

Pero la realidad del análisis y reto de las investigaciones forenses en este renovado contexto abierto, de flujo de información permanente y ubicua genera más incertidumbres que certezas, más preguntas que respuestas y más imprecisiones que claridades. Mientras la esencia misma de la computación forense es establecer hechos y datos propios de la realidad que se investiga, una revisión de los diferentes actores de este nuevo escenario nos propone diferentes perspectivas que confrontan los fundamentos de los procedimientos generalmente aceptados para avanzar en el aseguramiento de evidencias en un proceso forense digital [13][14].

En esta primera revisión del tema forense en el contexto actual, trataremos de analizar cada uno de los participantes y aquellos elementos críticos que hacen exigente una validación forense digital en un ecosistema tecnológico movilizad por los medios sociales, apalancado en tecnologías móviles y convenientemente ubicado en la nube.

Para efectos de este documento entenderemos un ecosistema tecnológico como una extensión del concepto de un ecosistema natural, donde la interacción de cada uno de sus participantes establece y define el comportamiento y estabilidad del sistema mismo. En este contexto, en un ecosistema tecnológico participan activamente los usuarios, las tecnologías móviles y la computación en la nube, los cuales desarrollan una serie de interacciones claves para su supervivencia, basado en demandas permanentes de servicios y posibilidades cada vez más novedosas e instantáneas [15].

4.1. Una vista desde el usuario

Iniciemos con el usuario, con las personas de las que se advierte una cada vez más alta dependencia de las redes sociales, y consumo de contenidos y servicios en la web. Con el paso del tiempo los hábitos de las personas, particularmente de los niños y los jóvenes han venido migrando de una necesidad natural de interacción cara a cara, a una mediada por la tecnología, con información instantánea y de acceso técnicamente ágil y prácticamente ilimitado. Esto si bien es una gran ventaja para

mantenerse actualizado y en movimiento, supone debilitar la natural exigencia de explorar y revelar nuevas preguntas que forjen los nuevos investigadores del futuro, con hambre de logro, más allá de un click que hable de lo que "hay disponible". Pero esta es una reflexión que está fuera del alcance de este análisis.

Desde el punto de vista forense, el caminar por las redes sociales es descubrir un perfil de la persona, sus hábitos para compartir información, sus patrones de conexión, las aplicaciones extra que utiliza y los amigos con los cuales más comparte. De igual forma, es detallar sus habilidades para configurar su interacción, los cuidados para aceptar a nuevos amigos y las particularidades de su personalidad que se describen en cada una de sus publicaciones.

Analizar a un individuo en una red social es ir más allá de cuál de ellas utiliza, es entender la interacción que existe entre el navegador y el sitio mismo, sabiendo que éste último está en un ecosistema tecnológico, con dependencias identificadas, tanto para los servicios ofrecidos a sus usuarios como para la infraestructura que los soporta. Así las cosas, una vista de la problemática estará en la forma como los terceros que intervienen han sabido estructurar la interacción de sus aplicaciones para ofrecer lo prometido y otra, la forma como la tercera parte mantiene y asegura los servidores y equipos de cómputo sobre los cuales se ejecutan los programas (ver **sección 3**).

4.2. Integrando el concepto de movilidad

Como quiera que entender estas interacciones demanda una comprensión de un ecosistema que se articula en una malla de relaciones técnicas y de información, la incorporación a este escenario de los conceptos de movilidad define una realidad ampliada que no es posible comprender sólo desde los elementos naturales de las redes inalámbricas y sus servicios, pues éstas representan sólo un medio adicional que se suma a las interacciones del ecosistema tecnológico que tenemos en la actualidad.

Así las cosas, las investigaciones forenses que conjugan las redes sociales y dispositivos móviles superan las consideraciones actuales que los investigadores puedan tener, para recabar la información requerida con la profundidad necesaria, y así entender el cúmulo de relaciones y puntos de contacto que son necesarios para encontrar patrones y respuestas a preguntas que se pueden hacer en una operación sin cables y altamente social y digital. Basta con revisar los nuevos servicios de información diseñados para tabletas, teléfonos inteligentes y demás dispositivos móviles, para comprender cómo avanzamos hacia una realidad de contar con un *unified digital locker* (casillero digital unificado) [16] en la

nube donde la llave de acceso está asociada con el dispositivo móvil utilizado.

Conjugar estas dos tendencias exige de parte del investigador forense reconocer que su entrenamiento actual se queda corto para asistir a la justicia en la persecución de las nuevas y silenciosas tácticas que la delincuencia viene utilizando a través de las redes sociales y los medios inalámbricos. Mientras los "chicos malos" avanzan diariamente en la búsqueda de nuevas opciones y oportunidades para continuar con su imperio del engaño y defraudación, apoyados bien en nuestras malas prácticas, fallas tecnológicas o de las aplicaciones, poco hacemos en nuestro propio ejercicio de manera sistemática y formal para asegurar lo requerido por las personas, procesos y tecnología.

4.3. La nube, el eslabón estratégico

No contentos con lo anterior, ahora sumamos a la ecuación, por cierto desde el punto de vista económico y estratégico claramente positiva y rentable, la realidad de una relación más dependiente y más flexible de articulación de servicios de infraestructura, plataforma y aplicaciones, lo que se denomina en el mundo tecnológico "computación en la nube".

La computación en la nube es el eslabón "que hacía falta" para contar con una facilidad de almacenamiento prácticamente infinito, disponibilidad permanente y movilidad sin restricciones. La nube se convierte en el nuevo paradigma que "hace transparente" la relación entre usuarios y proveedores, la promesa de valor de pagar por lo que se usa, de agilidad para contar con lo que se quiere y desplegar los servicios de acuerdo con el cambio de las tendencias del mercado.

Así las cosas, se completa el cuadro de la complejidad que debe atender el nuevo observador forense digital, que consiste en entender primero las relaciones entre el usuario y su red social, luego la red social y los medios inalámbricos, y finalmente los servicios tercerizados y sus accesos desde los medios móviles así como las consideraciones de interacción de los usuarios.

Como podemos ver, adelantar una investigación forense en una realidad como la que hemos analizado no es una extensión de lo que conocemos hoy en forensia digital. Es elevar nuestra reflexión general del análisis de datos que soportan los informes técnicos por un ejercicio de desdoblamiento de la complejidad entendiendo a los actores comprometidos y sus relaciones en una escena virtual que tiene sentido en un escenario real.

5. Reflexiones finales

Concentrarnos en el análisis forense en un ecosistema tecnológico es reconocer que existe una complejidad inherente a las nuevas

interacciones de los individuos, las tecnologías y sus procesos. Es asomarnos a la exigencia permanente de nuevos servicios y retos empresariales y sociales, que buscan en las tecnologías una forma de hacer más eficiente y eficaz sus procesos de negocio, balanceando sus márgenes de costos e integrando la nueva cultura de información instantánea y la vida en línea.

Por tanto, dejamos planteados tres elementos básicos del análisis forense en un ecosistema tecnológico, los cuales definen la ruta del reconocimiento no sólo de los componentes que integran este nuevo panorama, sino de sus interacciones, las cuales materializan y manifiestan los rastros informáticos, ahora en una realidad aumentada y tan particular como cada uno de los individuos que en ella participan. Las redes sociales, como motor fundamental que hace fluir la información y el reconocimiento particular de sus participantes como creadores de contenido, muestra el primer momento de este análisis.

Los dispositivos móviles, podríamos decir, catalizador complementario de las redes sociales, que materializa la idea de una vida perfectamente informada, interconectada y de comunicación asincrónica, son el segundo elemento que establece un reto a superar para un análisis forense; un componente que por sí solo demanda un conocimiento técnico particular y especializado para descubrir sus entrañas, pero que, en combinación con las redes sociales, exige una vista más socio-técnica y estratégica para entender las motivaciones de los posibles intrusos, un ejercicio exigente que busca acertar en un blanco en movimiento.

Complementando la ecuación, hace su aparición la computación en la nube, un escenario abierto y flexible que aumenta las posibilidades de expansión de la capacidad de cómputo y almacenamiento, en cualquier parte y en cualquier momento. Un mundo de posibilidades que, integrado al ambiente móvil presentado previamente, define una interacción local de alcance global, donde la evidencia de los hechos puede estar en muchas partes al mismo tiempo, con diferencias horarias, diversidad de tecnologías y aplicaciones.

Como quiera que esta realidad supera claramente las capacidades de un solo analista forense en informática, se hace necesario establecer modelos y métodos que respondan a esta realidad, más allá de los aportes tradicionales de las metodologías forenses informáticas actuales, que permitan entender la complejidad del entorno de análisis, para lo cual actualmente se revisan enfoques desde la cibernética organizacional que prometen una vista más positiva y estructural para comprender y avanzar frente a la criminalidad que se potencia en la movilidad, la nube y las redes sociales.

Referencias

- [1] J. Cano. *Pronósticos de seguridad de la información 2012*. Blog "IT-Insecurity", 2012. <<http://insecurityit.blogspot.com/2012/01/pronosticos-de-seguridad-de-la.html>> (Consultado: enero de 2012).
- [2] P. Mell, T. Grance. *Draft NIST Working Definition of Cloud Computing*, 2009. <<http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>> (Consultado: enero de 2012).
- [3] K. Birman, G. Chockler, R. Van Renesse. *Toward a cloud computing research agenda. Proceedings of Large-Scale Distributed System and Middleware, LADIS 2008*. <http://www.cs.cornell.edu/projects/quicksilver/public_pdfs/sigact2.pdf> (Consultado: enero de 2012).
- [4] Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, 2009. <<http://www.cloudsecurityalliance.org/guidance/csaguide.pdf>>.
- [5] T. Mather, S. Kumaraswamy, S. Latif. *Cloud Security and Privacy*. O'Reilly, 2009.
- [6] J. Brodtkin. (2008) *Gartner: Seven cloud-computing security risk*. Infoworld, 2008. <<http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853>> (Consultado: diciembre de 2009).
- [7] European Network and Information Security Agency (ENISA). *Cloud computing. Benefits, risk and recommendations for information security*, 2009. Disponible en: <<http://www.enisa.europa.eu/>> (Consultado: enero de 2012).
- [8] V. Raval. *Risk landscape of Cloud computing. ISACA Journal*, 2010, Vol. 1.
- [9] M. Savage. *Carefully evaluate provider's SaaS security model. Information Security Magazine*, diciembre 2009. (Consultado: diciembre de 2009).
- [10] J. Cano. *Cumplimiento, seguridad y control en la nube. Conceptos y riesgos. Revista SISTEMAS*, No.112, octubre 2009-enero 2010. <http://www.acis.org.co/fileadmin/Revista_112/uno.pdf> (Consultado: enero de 2012).
- [11] J. Barbara. *Cloud computing: Another digital forensic challenge. Forensic Magazine*, October/November 2009. <<http://www.forensicmag.com/article/cloud-computing-another-digital-forensic-challenge>> (Consultado en: enero de 2012).
- [12] F. Cohen. *Culture clash: Cloud computing and digital forensics*. 2009. <<http://all.net/Analyst/2009-05b.pdf>> (Consultado en: enero de 2012).
- [13] K. Ruan. *Cloud forensics: Challenges and opportunities. Centre for cybercrime investigation*, 2010. University College Dublin. <<http://confluence.jetbrains.net/download/attachments/36015346/Cloud+Forensics+-+Challenges+and+Opportunities.pdf>> (Consultado: 17-07-2011).
- [14] B. Wright. *Digital forensics and social media*, 2010. <<http://computer-forensics.sans.org/blog/2010/04/20/digital-social-media/>> (Consultado: 17-07-2011).
- [15] P. Trimintzios, C. Hall, R. Clayton, R. Anderson, E. Ouzounis. *Resilience of the Internet Interconnection Ecosystem*, 2011. <<http://www.enisa.europa.eu/act/res/other-areas/inter-x/report/interx-report>> (Consultado: 17-07-2011).
- [16] Morgan Stanley. *Internet Trends*, 2010 (Presentación). <http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf> (Consultado: Enero de 2012).

José Luis González Sánchez¹,
Rosa María Gil Iranzo², Fran-
cisco Luis Gutiérrez Vela³
^{1,3}GEDES – Universidad de Granada,
²GRIHO – Universitat de Lleida

<joseluisgs@ugr.es>,
<rgil@griho.net>,
<fgutierr@ugr.es>

1. Introducción

La Experiencia de Usuario (UX) se define formalmente como "la percepción de una persona y las respuestas subjetivas de ésta como resultado de la utilización y/o uso de un producto, sistema o servicio" [1], ligada al conjunto de sentimientos y respuestas emocionales al interactuar con un producto software [2], e incluye aspectos subjetivos que afectan al proceso interactivo. Los videojuegos tienen como principal objetivo que el usuario experimente sentimientos de diversión y entretenimiento durante el proceso de juego. Comprobar estos objetivos es un proceso complejo y en el que es habitual aplicar criterios muy subjetivos e imprecisos. Podemos observar cómo se hacen necesarios mecanismos que caractericen la calidad de la experiencia de juego como la jugabilidad [3][4]. A la hora de realizar una evaluación de la UX debemos "enriquecer" los mecanismos de evaluación con técnicas que nos muestren los aspectos subjetivos que caracterizan la experiencia sentida por los usuarios, especialmente en procesos de juego.

En este trabajo, se propone como principal objetivo evaluar la UX en videojuegos (campo "extremo" en explotar los parámetros subjetivos de la UX) completando la información obtenida usando el análisis de la jugabilidad, con información sobre la respuesta emocional del jugador y cómo se manifiesta según el contexto sociocultural del jugador.

Comenzamos con una visión sobre la evaluación de la UX y comentando aspectos sobre la jugabilidad y la caracterización de la UX en videojuegos. A continuación mostramos nuestra propuesta de evaluación de la UX en videojuegos aplicada bajo objetivos pragmáticos y hedónicos. Posteriormente presentamos la puesta en práctica de los métodos de evaluación propuestos sobre un caso de estudio con un producto comercial concreto. Finalmente mostramos las conclusiones y trabajos futuros que se extraen de los resultados presentados a lo largo de este trabajo.

2. Evaluación y factores de la UX en sistemas interactivos

La Experiencia de Usuario (UX) tiene como objetivo ofrecer información sobre el conjunto de emociones y sensaciones que un usuario obtiene como respuesta al interactuar con un sistema interactivo, es decir, completar la *información objetiva* de la realización de una

Enriqueciendo la evaluación en videojuegos

Este artículo ha sido seleccionado de entre las mejores ponencias presentadas en el XII Congreso Internacional de Interacción Persona-Ordenador (Interacción 2011) celebrado en Lisboa del 2 al 5 de septiembre de 2011, en el que ATI fue entidad colaboradora.

Resumen: Los videojuegos son un campo de importante avance en el sector interactivo en la actualidad. Ante esta realidad, es necesario analizar en profundidad la Experiencia del Usuario (UX) en busca de factores que repercutan en la aceptación del producto por parte de los usuarios. Este trabajo muestra cómo completar la información existente sobre la UX respecto a la "jugabilidad" con técnicas de análisis hedónico tales como el impacto emocional y cultural, las cuales provocan que la UX sea distinta entre los distintos perfiles de jugadores. De esta manera, se consigue maximizar el rendimiento así como los resultados de la inversión si se utiliza la metodología mostrada en el artículo para ser usada desde los primeros prototipos hasta el producto final.

Palabras clave: Emociones, experiencia del usuario, jugabilidad, métodos de evaluación, multiculturalidad, sistemas de ocio y entretenimiento.

tarea, con *información subjetiva* sentida a la hora de realizarla. Siendo la UX *dinámica* y dependiente del *contexto del usuario*, ayudando a mejorar la aceptación de los usuarios, ganar la fidelidad de estos y mejorar el retorno económico del desarrollo del producto [2].

La evaluación de la UX difiere de las técnicas de evaluación tradicionales en el ámbito de la Interacción Persona-Ordenador (IPO), las cuales se centran más en la *evaluación pragmática* de la realización de una tarea (¿qué y para qué realizamos una tarea?) al completarla con una *evaluación hedónica* asociada al proceso interactivo (¿qué sentimos al realizar la tarea?). Surge como evolución del análisis de la *satisfacción del usuario*.

Los enfoques tradicionales de evaluación de la satisfacción (por ej. la usabilidad) evalúan generalmente la percepción de "satisfacción" según la eficacia y eficiencia, de modo que si los usuarios perciben como eficaz y eficiente el uso del producto se da por hecho que están satisfechos [5]. Pero hay aspectos de la UX [6], como la diversión, placer, emotividad, influencia sociocultural o el entretenimiento, que contribuyen de manera significativa a la satisfacción del usuario respecto con el producto. Factores que han llegado a formar parte del nuevo estándar de la Calidad en Uso ISO/IEC 25010 [7].

En [8] se discuten los métodos y necesidades actuales a tener en cuenta en la evaluación de la UX en sistemas interactivos destacando la importancia de la *respuesta emocional* y las restricciones debidas a la *influencia sociocultural*. Es por ello que los *métodos de evaluación deben enriquecerse* con dichos factores para conseguir información más completa de la UX en el proceso de interacción usuario(s)-sistema(s).

Uno de los aspectos que caracterizan la UX es la *respuesta emocional* del usuario ante el proceso interactivo factor que puede provocar deseo u odio por el mismo [6][9]. Existen numerosos estudios sobre las "emociones" en la literatura especializada, incluso se han propuesto definiciones consensuadas del término y de sus propiedades.

Una respuesta emocional o *sentimiento* es una reacción psicológica relacionada con las necesidades, objetivos o preocupaciones de un individuo y que está compuesta por factores conductuales, fisiológicos, afectivos y cognitivos, en *respuesta a unos estímulos que se producen a la hora de interactuar* con un producto y son propias de cada individuo [9][10].

Entre los métodos más usuales encontramos las herramientas de medida verbales que se presentan como auto-informes donde los encuestados utilizan una escala para registrar sus emociones [10][12]. La principal crítica de este tipo de técnicas es que solo registran estados emocionales conscientes del usuario, pero son muy populares por ser relativamente fáciles de implementar. Debido a que las emociones son automáticas y dinámicas, es importante captarlas en el instante en que se producen; para ello podemos hacer uso de heurísticas de emociones [11] o representar emociones con cartas de emoticonos (*Emocards*) para que el usuario identifique visualmente cómo se siente durante el proceso interactivo y posteriormente comparar ambos métodos [12].

La *influencia sociocultural* en el usuario puede provocar grandes diferencias en la UX. Hofstede [14] considera la *cultura* como un término utilizado para referirse a la programación mental. Cada persona tiene en su interior modelos de pensamiento, sentimien-

to y actuación que actúa como "software mental". Las personas se diferencian por un conjunto de aspectos culturales diferenciadores entre sociedades y por características internas. Estos metamodelos culturales, que representan la influencia sociocultural del individuo [13][14], provocan que *el diseño de los sistemas interactivos sigan unas ciertas reglas o patrones* dependiendo del grupo de usuarios al que va dirigido con el fin de mejorar la experiencia interactiva. Se utilizarán en este estudio los puntos relacionados con procedencia y género.

3. Jugabilidad y la UX en videojuegos

La *jugabilidad* es un término empleado en el diseño y análisis de juegos que suele ser usado para medir la calidad de la experiencia de juego en términos de las mecánicas de juego, elementos software y del proceso interactivo usuario-videojuego. Existen importantes trabajos centrados en recopilar artículos o investigaciones sobre factores que hacen más "jugable" y profundizan en la UX en videojuegos [15][16][17].

A lo largo de este trabajo nos basaremos en ellos complementándolos con las propuestas de González Sánchez et al. [3][4][18]. Dicha propuesta, ofrece un modelo adecuado para la *jugabilidad* como *caracterización de la experiencia del usuario* en videojuegos, ofreciendo mecanismos tanto para su identificación como para su evaluación durante las distintas fases de desarrollo de videojuegos.

La jugabilidad se define "*como el conjunto de propiedades que describen la experiencia del jugador ante un sistema de juego determinado, cuyo principal objetivo es divertir y entretener de forma satisfactoria y creíble ya sea solo o en compañía*". Dicho de otro modo, la jugabilidad representa "*el grado en el cual jugadores específicos alcanzan metas específicas del juego con efectividad, eficiencia, flexibilidad, seguridad y especialmente satisfacción en un contexto jugable de uso*" [3][4][18].

La jugabilidad viene descrita por una serie de atributos y propiedades que ayudan a caracterizarla. Estos atributos son: *Satisfac-*

ción, agrado o complacencia del jugador ante el videojuego o parte de éste; *Aprendizaje*, facilidad para comprender el sistema y mecánica del videojuego; *Efectividad*, tiempo y recursos necesarios para lograr los objetivos propuestos en el videojuego. *Inmersión*, capacidad para creerse lo que se juega e integrarse en el mundo virtual mostrado en el juego; *Motivación*, característica del videojuego que mueve a la persona a realizar determinadas acciones y persistir en ellas para su culminación, *Emoción*, impulso involuntario, originado como respuesta a los estímulos del videojuego, que induce sentimientos y que desencadena conductas de reacción automática. *Socialización*, atributos que hacen apreciar el videojuego de distinta manera al jugarlo en compañía (multijugador) ya sea de manera competitiva, colaborativa o cooperativa.

Además, este modelo nos ofrece un mecanismo para guiar el proceso de evaluación de la UX en base de las distintas propiedades de la jugabilidad denominadas *facetas de la jugabilidad*, aportándonos información tanto pragmática como hedónica de la experiencia de juego. Estas facetas son las siguientes: *Jugabilidad Intrínseca*, es la proyección de los elementos característicos de un videojuego al jugador (elementos del *Game Core*); *Jugabilidad Mecánica*, está asociada a la calidad del videojuego como sistema software (*Game Engine*); *Jugabilidad Interactiva*, se asocia a todo lo relacionado con la interacción del usuario con el videojuego (*Game Interface*); *Jugabilidad Artística*: observa la adecuación artística y estética de todos los elementos del videojuego; *Jugabilidad Intrapersonal*, tiene como objetivo conocer la percepción y respuesta emocional del usuario ante el videojuego; *Jugabilidad Interpersonal*, analiza las sensaciones mientras se juega en compañía.

4. Propuesta de test y ejemplo de Evaluación Rica en videojuegos

Nuestra propuesta de Evaluación Rica de la UX tiene como principal objetivo *analizar la UX en base a la jugabilidad, pero complementando dicha información con el impacto emocional que le producen al jugador los distintos elementos del videojuego y cómo es capaz de reaccionar según sus características*

socioculturales (siguiendo las ideas sugeridas en [18]).

Hemos partido también de la necesidad de maximizar los resultados respecto al costo de la evaluación para ser usada desde los primeros prototipos asegurando la correcta experiencia a lo largo del desarrollo ágil del videojuego. Evitando errores finales que sean imposibles o muy costosos de solucionar, y siendo complementada posteriormente con otras más específicas.

De forma general, los test de usuarios se dividen en tres partes: Pre-Test, Test y Post-Test.

La fase de *Pre-Test* tiene como objetivo escoger el *perfil del jugador*. Completamos la información, como usuario de videojuegos, con su estado anímico y qué siente y cómo de familiar (culturalmente hablando) le son determinados elementos del juego. Indicando cómo identifican dichas cualidades en ellos (por ej. qué sentimiento les provoca una melodía musical, o la identificación del contexto por el ropaje o la arquitectura de distintos elementos del escenario).

Durante el *Test*, tendrán la total libertad para jugar una determinada sección del videojuego. Serán grabados por dos cámaras con el objetivo de identificar los cambios en la expresión facial y corporal y en los comentarios, obteniendo información del impacto emocional usando las heurísticas propuestas en [11]. La información de la fugacidad de las emociones se complementa con la medida de la frecuencia cardiaca para detectar a nivel biométrico cómo se representan las emociones percibidas [16].

La fase de *Post-Test* está caracterizada por la realización de un conjunto de cuestionarios sobre los distintos aspectos del juego donde la valoración será realizada usando *Emocards* [12] y métodos de varios niveles de respuesta [19]. El principal objetivo de estos cuestionarios es obtener información de los aspectos positivos y negativos de las cuestiones que se interrogan tras las tareas encomendadas. Este tipo de preguntas ayudan a responder ante cuestiones hedónicas donde el usuario no se siente seguro para otorgar un valor numérico

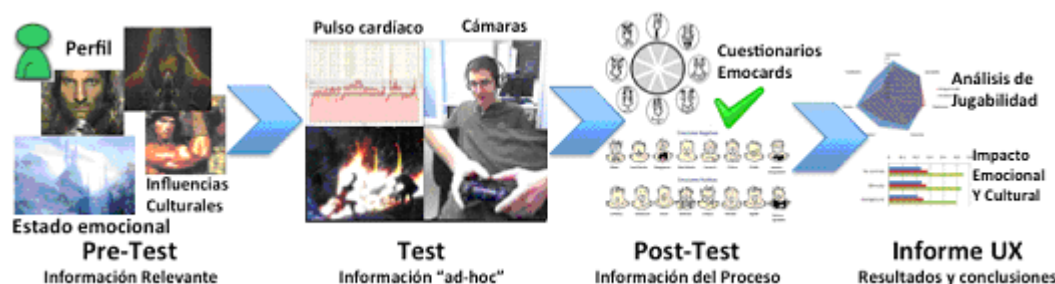


Figura 1. Proceso de Evaluación Rica de la experiencia del jugador en videojuegos.

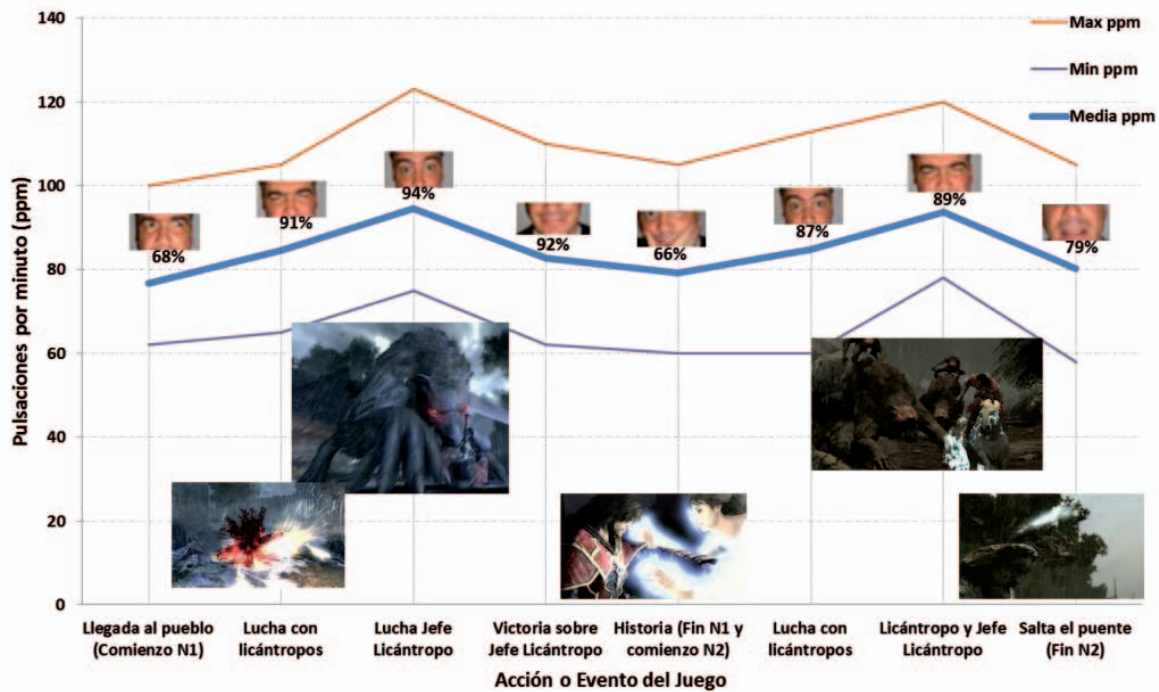


Figura 2. Emociones detectadas (%) y evolución de las pulsaciones en el proceso de juego.

pero sí para identificar como se ha sentido en relación al aspecto por el que está siendo interrogado. Además, usaremos *Emocards* específicas para que el usuario identifique cómo se ha sentido en determinados momentos del test/videojuego, completando la información mediante entrevistas informales.

La información será procesada y analizada junto a los informes de *Pre-Test* y *Test* para obtener información que complemente el análisis realizado sobre la jugabilidad debida al videojuego [4][19] con el impacto emocional sentido por el jugador ante los distintos elementos del videojuego. Un ejemplo de las herramientas y del proceso de evaluación rica puede verse resumido en la figura 1.

El videojuego para poner en práctica nuestra propuesta es *"Castlevania: Lords of Shadow"* desarrollado por los españoles *MercurySteam Entertainment* y producido por *Konami Corp.* Este es un juego que disfrutó de numerosos premios y reconocimiento desde la crítica especializada desde su salida a finales del 2010.

Nos centraremos en su beta, como prototipo del juego, para el estudio de la jugabilidad, impacto emocional y cómo se transmite a lo largo del juego, y si estos factores son indicativos para el producto final. Además, se hará uso de material de arte del juego y materiales de la franquicia o saga "Castlevania".

Para el desarrollo del test contaremos con un conjunto de 35 usuarios pertenecientes a la Universitat de Lleida comprendidos entre los 18 y 34 años, ($\approx 75\%$ entre los 19 y 22 años y

$\approx 15\%$ son del sexo femenino). Se destaca que más del 90% de los usuarios tienen más de dos plataformas de juego, donde casi el 80% juega una media de entre 4 a 8 horas semanales. Las preferencias en los géneros de juego destacadas son aventura ($\approx 60\%$) y lucha ($\approx 30\%$) prefiriendo el 87% jugar en compañía de amigos. Se destaca que *culturalmente* pertenecen a una *sociedad de consumo de ocio electrónico* y están familiarizados con ello. El número de usuarios para el test es correcto según [20] con el objetivo de disminuir el costo de la evaluación y maximizar el rendimiento en la evaluación de prototipos.

Los objetivos del *Pre-Test* son conocer a priori la influencia sociocultural que el cine, novelas u otros juegos de la saga pueden provocar en la asimilación de los contenidos del juego, analizar el impacto emocional producido por éstos y corroborar también que nos hallamos frente al perfil establecido en líneas anteriores.

Para analizar la empatía con el héroe del juego se le presentan distintos protagonistas de temáticas parecidas al del juego. La opción preferida de protagonista para una aventura fantástica es la de Aragorn ("El Señor de los Anillos", 57%) considerado más *honesto* ($\approx 77\%$) destacando de éste su mirada (43%), y la cara y pelo ($\approx 15\%$).

Respecto a las *emociones* producidas por la música del juego, se analizó el impacto de un fragmento de 30s. del mismo. Al $\approx 83\%$ les inspiraba "batalla" y "acción", mientras el 17% indicaron "venganza"; el 81% remarcaba que el fragmento les hacía *sentirse* "enérgicos",

mientras el 5% indicaba que sentía "miedo". Sobre una imagen de uno de los entornos del juego, el $\approx 74\%$ indicó que se trataba de un paraje europeo por la arquitectura típica (*influencia cultural*), generando unos *sentimientos* de "miedo" ($\approx 47\%$) y "curiosidad" (32%).

Ante la adecuación del héroe a la ambientación del juego, se realizó una comparación respecto a otros protagonistas de la saga "Castlevania". Más del 85% eligieron al protagonista actual como el más idóneo, destacando sobre todo que las facciones del rostro (87%) y la ropa (7%) *representan mejor a un guerrero del S. XI* (también pensamos que este resultado es fruto de que ha sido analizado en una determinada cultura).

Durante la fase de *Test* los usuarios jugaron abiertamente a la demo. Mientras tanto fue grabada su expresión facial/corporal [11][21] y monitorizado su ritmo cardíaco [16]. El objetivo es detectar reacciones emocionales viscerales que aparecen durante el proceso de juego y correlacionarlas con los datos biométricos del usuario. Para ello haremos uso de las directrices de detección emocional analizando cómo han podido afectar dichas emociones a las estrategias de juego ante los retos propuestos.

En la figura 2 podemos apreciar el progreso en el nivel del juego, las emociones detectadas (en %) y cómo se correlaciona con las constantes biométricas (Máx., Min., y Media de las pulsaciones por minuto, ppm.).

Al comienzo de la aventura los usuarios están en situación de incertidumbre, desviando la

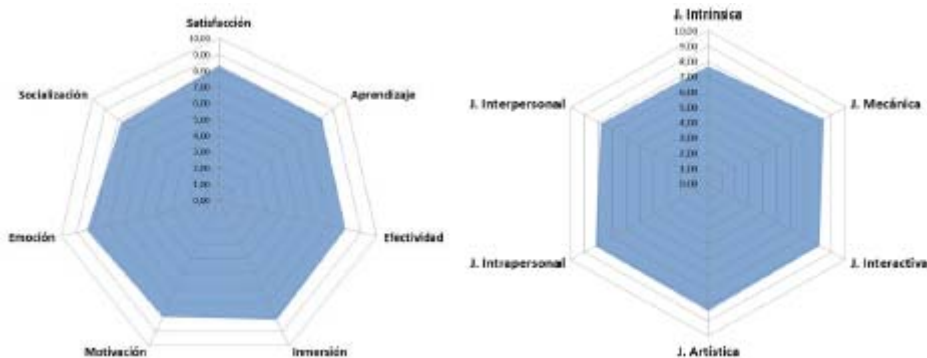


Figura 3. Análisis UX: Atributos de la jugabilidad (izqda.) y facetas de la jugabilidad (dcha.).

mirada para captar todos los elementos de la pantalla ($\approx 68\%$). Con la aparición de los primeros enemigos, el uso del mando se vuelve intensivo, frunciéndose el ceño ($\approx 91\%$).

Uno de los clímax de la demo viene dado por la aparición del jefe de nivel, el cual por su tamaño sorprende al jugador, observándose este hecho por el levantamiento de las cejas ($\approx 94\%$). Además, este reto provoca un aumento del nerviosismo reflejado en el incremento a nivel medio de 15 ppm. en los jugadores. El estrés puntual se vuelve satisfacción al conseguir la victoria, expresándose como un leve sonreír ($\approx 92\%$). Durante el intervalo entre un nivel y otro se muestra parte de la historia, provocando desconfianza, expresado mayoritariamente en tocarse la mano con la cara ($\approx 66\%$) para dar paso a una nueva oleada de enemigos que sorprenden al jugador ($\approx 87\%$), llegando al segundo clímax del nivel, otro jefe de nivel.

De nuevo el estrés por tener tantos enemigos provoca que el jugador se concentre y actúe con rapidez. Este momento de estrés se repre-

senta mayoritariamente frunciendo el ceño, apretando la mandíbula y ejecutando los movimientos con el control de juego de manera más violenta ($\approx 89\%$). Finalmente, el estrés se transforma en alivio, siendo expresado con un leve jadeo o suspiro ($\approx 79\%$).

Cabe destacar que las situaciones de estrés o agobio al jugador de manera controlada provocan que afloren dos tipos de estrategias, una defensiva adoptada por los 100% de los usuarios femeninos y un 25% de los masculinos, los cuales se sienten intimidados por los enemigos (tamaño y rugidos) y arriesgan menos, teniendo acciones más racionales y comedidas.

Por otro lado, el 75% de los usuarios masculinos prefieren un enfrentamiento directo y violento. En ambos casos el grado de inmersión es elevado, factor que se ve indicado por el aumento de pulsaciones por minuto (≈ 15 ppm. en el clímax), la rigidez y fuerza en la mandíbula (provocando el silencio) y por la continua pulsación del control de juego incluso entre escenas cinemáticas que existen,

donde el jugador no interactúa, solo visualiza. Se constata que la estrategia depende de un factor cultural como es el género que se establece en el parámetro de masculinidad/feminidad.

Durante el **Post-Test** se ha hecho uso de entrevistas informales y cuestionarios los cuales siguen los criterios de evaluación guiados por facetas para interrogar atributos de la jugabilidad que pueden encontrarse en [3][4] siguiendo las metodologías y herramientas propuestas en [18], así como *Emocards* [10] [12][17] para el análisis del impacto emocional de los distintos elementos del videojuego.

Los resultados de la jugabilidad son representados por las superficies de la jugabilidad, obteniéndose los resultados mostrados en la **figura 3** (escala de puntuación de 0 a 10).

El análisis de jugabilidad realizado no muestra que este videojuego provoque una experiencia muy equilibrada, pues no existe un atributo o faceta que se desmarque sobre las demás. Cabe destacar que los comentarios

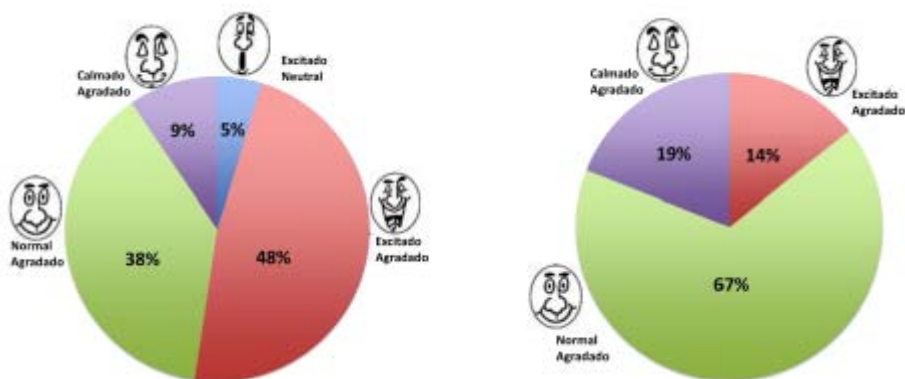


Figura 4. Impacto Emocional: ambientación (izqda.) y efectos sonoros/melodías musicales (dcha.).

centrales de los usuarios se centran en la gran calidad gráfica y los efectos cinemáticos (*Jugabilidad Mecánica*) que provocaban ganas de seguir jugando (*Motivación, Satisfacción*). Por otro lado, como se ha mostrado en la **figura 2**, la calidad técnica del juego, unida a un buen cuidado de los efectos artísticos, provoca que la *Inmersión y Motivación* sean elevadas.

Con las *Emocards* se han analizado factores donde los usuarios pueden tener dificultad para responder con distintos niveles de respuesta, pero que fácilmente pueden identificar su *impacto anímico*, por ejemplo con la música o arte del juego donde existe *dificultad para valorar objetivamente* su calidad artística, pero se puede *identificar como se han sentido* ante ellos y como encajan con el videojuego. Ejemplos de estas preguntas y respuestas pueden verse en la **figura 4**.

Los resultados del *Post-Test* reafirman la buena opinión de los usuarios ante la ambientación y contexto, así como los efectos sonoros y la música en general (alto grado de satisfacción, caracterizándose mayoritariamente por un estado de agrado, que varía entre la excitación y un estado neutral).

Estos factores favorecen una mejor ambientación y *emotividad*, destacando la *cercanía y familiaridad a nivel cultural* que suponen para los jugadores los distintos elementos del juego. El protagonista y paisajes del juego son bien valorados y la mayoría destacan que las características propias del medio hacen el juego más cercano (transmisión de emociones y contexto histórico) al jugador.

Sin embargo, usuarios de origen mexicano indicaron que este tipo de héroe no era confiable por su palidez de rostro (12%) y los parajes les resultaban extraños (12%). La calidad cinemática con los elementos artísticos (los mejores valorados) mejora la efectividad en la asimilación de todas las experiencias que propone el universo del videojuego, fomentando que el jugador se sienta más integrado en éste y fomentando la efectividad del mismo.

A nivel global se puede indicar que los resultados sobre la UX son muy positivos porque la mayoría de los jugadores son pseudo-expertos pertenecientes a la *sociedad del ocio y consumo electrónico*, y juegan bastante. Además de consumidores de *cultura multimedia*, lo que ayuda a la mejor asimilación de los distintos elementos artísticos y culturales usados en el juego, mostrándose la importancia de conocer a quién va dirigido un producto (nivel social y cultural) para desarrollarlo correctamente.

A la vista de los resultados, destacamos la importancia de este tipo de análisis en otros

sistemas interactivos (por ej. sistemas web o móviles) donde la *importancia cultural* o el *impacto emocional* marquen cómo debe ser el diseño (por ej. diseño, navegación, metáforas, etc.) para mejorar la experiencia [5][6][9] o que un mismo producto se "maquille" según las características de la población a la que va destinado [13][22].

6. Conclusiones y trabajos futuros

A lo largo de este trabajo hemos mostrado cómo la UX de usuario aborda todas las respuestas emocionales y sensaciones existentes en el proceso interactivo. Para ello los *métodos tradicionales de evaluación deben enriquecerse* con el análisis de las propiedades hedónicas que caracterizan la UX.

Especialmente, hemos destacado dos factores con peso en la experiencia: la *respuesta emocional* y la *influencia sociocultural*. En el campo de los videojuegos, la UX es un factor clave que explota las características hedónicas del proceso interactivo siendo caracterizado por la jugabilidad.

Para completar los análisis realizados en base a la jugabilidad usamos técnicas propias del diseño emocional (*Emocards*, constantes biométricas, heurísticas ricas y análisis sociocultural). De esta manera podemos comprobar si la experiencia es lo más óptima posible además de si los elementos de un videojuego son aptos para un perfil de usuario determinado dadas sus características socioculturales. Como ejemplo de aplicación de la metodología de evaluación se ha realizado un análisis de la UX para la demo del videojuego "*Castelvania: Lords of Shadow*".

De los resultados obtenidos hemos observado que la *evaluación rica* de la experiencia de usuario es válida no sólo para videojuegos, sino para cualquier sistema interactivo donde cada vez es más importante *conocer el impacto emocional y cultural de los productos desarrollados para mejorar la aceptación de nuestros productos por partes de los usuarios y mejorar el éxito de éstos en un mercado cada vez más saturado y competitivo*.

Además, este análisis debe hacerse desde la etapa más temprana del desarrollo, *intentando disminuir los costos de la evaluación*, para evitar errores difíciles de solventar a nivel de UX. Por otro lado, estas técnicas *facilitan la evaluación* por parte del usuario, donde la imprecisión/inseguridad para ofrecer una valoración numérica o verbal (*falta de seguridad o criterio objetivo*, por ejemplo a nivel de calidad musical, calidad estética) se ve *completada por la asimilación de un estado anímico* que representa el proceso interactivo a la hora de realizar una tarea (por ej. cómo hacen sentir los efectos sonoros del producto, o los colores de la interfaz gráfica).

Como resultado indirecto se ha observado que según *el género* se puede jugar siguiendo unos *patrones/estrategias distintas*, por lo que puede ser interesante iniciar un proceso de experimentación para comprobar si la experiencia en determinados juegos puede estar ligada al género del jugador además de otros *factores sociales y culturales*, como se ha comprobado en otros sistemas interactivos (como puede ser la navegación web), es decir, se constata que existe una dependencia de factores socio-culturales que influye en el proceso interactivo (en este caso jugar).

Dentro de los trabajos futuros abordamos la tarea de la aplicación de las evaluaciones ricas en sistemas web, para detectar patrones de diseño que fomenten determinadas emociones a partir de parámetros socio-culturales como son la posición social, la pertenencia a otras culturas y los modelos mentales de los usuarios. Además de completar el proceso con técnicas de captación automática de emociones a través de reconocimiento facial [21] y biométrico [16]. No sólo para el uso de prototipos dentro de un desarrollo ágil, sino para una evaluación más profunda en las fases finales del desarrollo del producto.

Parte de estos resultados se están aplicando en el desarrollo de videojuegos educativos con el objetivo de mejorar la experiencia y el desarrollo emocional de los alumnos de estos sistemas mejorando la efectividad del proceso de enseñanza/aprendizaje guiado por videojuegos.

Agradecimientos

Este trabajo está financiado por el Ministerio de Ciencia e Innovación de España a través de los proyectos de investigación DESACO (TIN2008-06596-C02) y OMediaDis (TIN2008-06228). Gracias a MercurySteam Entertainment por su apoyo y atención en la realización de este trabajo.

Referencias

[1] ISO. *ISO/IEC 9241-210*, 2010. Ergonomics of Human-System Interaction – Part 210: Human centred Design for Interactive Systems. Clause 2.15.

[2] E. Law et al. Understanding, Scoping and Defining User Experience: A Survey Approach. *Proc. Human Factors in Computing Systems (CHI'09)*, pp.719-728 (2009).

[3] J.L. González Sánchez, N. Padilla Zea, F.L. Gutiérrez. From Usability to Playability: Introduction to Player-Centred Video Game Development Process. *Proc. Human-Computer Interaction International (HCI'09)*, pp. 65-74 (2009).

[4] J.L. González Sánchez, N. Padilla Zea, F.L. Gutiérrez. Playability: How to Identify the Player Experience in a Video Game. *Proc. 12th IFIP TC13 Conference on Human-Computer Interaction (INTERACT'09)*, pp. 356-359 (2009).

[5] M. Hassenzahl. The thing and I: understanding the relationship between user and product. En M. Blythe, C. Overbeeke, A. F. Monk, & P. C. Wright (Eds.), *Funology: From Usability to Enjoyment*. Dordrecht: Kluwer Academic Publishers, pp. 31-42 (2003).

[6] G. Cockton. Putting Value into E-evaluation. En Law, Effie Lai-Chong (Eds.) *Maturing Usability: Quality in Software, Interaction and Value*. Springer Verlag, 2008.

[7] ISO. *ISO/IEC 25010*. Software product Quality Requirements and Evaluation (SQuaRE). Software product quality and system quality in use models (2011).

[8] A. Vermeeren et al. User Experience Evaluation Methods: Current State and Development Needs. *Proceedings of NordCHI 2010*, pp. 521-530 (2010).

[9] S. Brave, C. Nass. Emotion in human-computer interaction. En J. Jacko & A. Sears (Eds.), *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications*. Lawrence Erlbaum Associates, 2002.

[10] A. Mehrabian, J.A. Russell. *An approach to environmental psychology*. Cambridge, MA: M.I.T. Press, 1974.

[11] E. De Lera, M. Garreta-Domingo. Ten Emotion Heuristics: Guidelines for Assessing the User's Affective Dimension Easily and Cost-Effectively. *Proc. 21st BCS HCI Group Conference (HCI'07)*, pp. 163-166 (2007).

[12] P.M.A. Desmet et al. Designing products with added emotional value: development and application of an approach for research through design. *The Design Journal*, 4(1), pp. 32-47 (2001).

[13] G. Hofstede. *Cultures and organizations: software of the mind*. NY: McGraw-Hill, 2005.

[14] LCW. *The Cultural Iceberg*, <<http://www.languageandculture.com/cultural-iceberg>> (2009).

[15] R. Bernhaupt (Ed). *Evaluating User Experience in Games: Concepts and Methods*. Springer, 2010.

[16] L. Nacke et al. Playability and Player Experience Research. *DiGRA 2009: Breaking New Ground: Innovation in Games, Play, Practice and Theory*.

[17] K. Isbister, N. Schaffer (Eds). *Game Usability: Advancing the Player Experience*. Morgan Kaufmann, 2008.

[18] J.L. González Sánchez. *Jugabilidad y Videojuegos. Análisis y Diseño de la Experiencia del Jugador en Sistemas Interactivos de Ocio Electrónico*. Ed. Académica Española, Lambert Academic Publishing GmbH & Co KG., 2011.

[19] Rensis Likert. A Technique for the Measurement of Attitudes. *Archives of Psychology*, Vol. 140, No. 55. (1932).

[20] U. Sekaran. *Research methods for business*. New York: John Wiley & Sons, Inc., 2000.

[21] I. Hupont, E. Cerezo, S. Baldassarri. Sensing Facial Emotions in a Continuous 2D Affective Space". *(SMC'10) IEEE International Conference on Systems, Man, and Cybernetics*, pp. 2045-2051 (2010).

[22] M. Chen et al. Creating cross-cultural appeal in digital games: Issues in localization and user testing. Presentation in *52nd Conference Society for Technical Communication (STC'05)* (2005).

2012

JENUI

Ciudad Real, del 10 al 13 de Julio de 2012

<http://jenui2012.uclm.es/>

Jornadas de Enseñanza
XVIII Universitaria Informática
de la **JENUI 2012**
Ciudad Real del
10 al 13 de Julio

Estas Jornadas pretenden promover el contacto, el intercambio y la discusión de conocimientos y experiencias entre profesores universitarios de Informática y grupos de investigación, debatir sobre el contenido de los programas y los métodos pedagógicos empleados, así como materializar un foro de debate en el que presentar temas y enfoques innovadores orientados a mejorar la docencia de la Informática en las Universidades.

UCLM UNIVERSIDAD DE CASTILLA-LA MANCHA

esi Escuela Superior de Informática

AENUI Asociación de Enseñanza Universitaria de Informática

Análisis de la seguridad del sistema reCAPTCHA

Noemí Carranza¹, Ricardo Palma Durán¹, Gonzalo Álvarez Marañón¹, José María Gómez Hidalgo²

¹Departamento de Tratamiento de la Información y Codificación, Instituto de Seguridad de la Información, Consejo Superior de Investigaciones Científicas; ²Director de I+D de Optenet, Coordinador de la sección técnica "Acceso y recuperación de la información" de *Novática*

<{noemi.carranza,ricardo.palma,gonzalo}@iec.csic.es>, <jgomez@optenet.com>

1. Introducción

En 1997, Andrei Broder y sus colegas en el motor de búsqueda Altavista desarrollaron el primer CAPTCHA como sistema de control de acceso a una aplicación Web, el formulario de alta de URLs en el índice de dicho motor de búsqueda. Desde entonces, los CAPTCHAs (*Completely Automated Public Turing test to tell Computers and Humans Apart* – Test de Turing completamente automático para separar humanos y computadoras) se han convertido probablemente en el método más popular para la protección de servicios *online* frente a abusos por parte de robots, es decir, sistemas automáticos que rellenan formularios web de suscripción, realizan comentarios en blogs, o recolectan recursos para difundir correo basura, software malicioso, etc. [1]. Un CAPTCHA es una prueba automática orientada a confirmar que el usuario de una aplicación es un ser humano en lugar de un robot [2], y generalmente toma la forma de una palabra o una secuencia de caracteres distorsionados que el usuario debe acertar para acceder a un determinado recurso, como por ejemplo, a la posibilidad de realizar un comentario en una Red Social como Facebook. Se espera que la palabra distorsionada sea muy difícil de averiguar para un sistema automático, y al mismo tiempo sencilla para una persona. De este modo, la prueba habilita el acceso al servicio protegido sólo a los seres humanos, y evita el acceso y el abuso por parte de los robots o sistemas automáticos.

Dado que los *spammers* y los *hackers* están altamente motivados para abusar de los servicios *online* con el fin de realizar actividades dañinas, están continuamente diseñando métodos para resolver los CAPTCHAs de manera automática. Se ha demostrado tanto de manera teórica ([3][4]) como práctica¹ que sus métodos pueden tener éxito, por lo que los diseñadores de CAPTCHAs están obligados a evolucionar sus técnicas para aumentar su dificultad sin perder usabilidad por parte de las personas. En otras palabras, los CAPTCHAs deben evaluarse periódicamente usando sistemas de reconocimiento

Resumen: En los últimos tiempos se han popularizado extraordinariamente los sistemas CAPTCHA, que protegen servicios Web planteando al usuario una prueba destinada a verificar que se trata de un ser humano y no de un robot, o sistema automático para el envío de correo basura o difusión de malware. Estos sistemas están siempre expuestos a que *spammers* y *hackers* sean capaces de comprometer su seguridad, y abusar de los recursos subyacentes (cuentas de correo, blogs, etc.) para realizar sus actividades ilícitas. Por ello, es necesario comprobar periódicamente su seguridad usando herramientas como sistemas de reconocimiento óptico de caracteres (OCR), sistemas de análisis de imagen, y otras. En este artículo realizamos un análisis de la seguridad del sistema reCAPTCHA, que probablemente es el más usado en Internet actualmente. Para ello, utilizamos diversas técnicas de análisis de imagen orientadas a corregir las deformaciones y distorsiones realizadas por el sistema en las imágenes que muestra al usuario, así como el eficaz sistema de OCR Tesseract. Se han analizado dos versiones del sistema reCAPTCHA y se ha comprobado que la seguridad del sistema probablemente ha aumentado en la segunda versión, más reciente, aunque es posible comprometer la seguridad del sistema si se cuenta con recursos suficientes en forma de una botnet de tamaño medio (unos 10.000 ordenadores).

Palabras clave: CAPTCHA, correo basura, Heuristic Over Segmentation, reCAPTCHA, seguridad web, spam, Shape Context, Tesseract.

óptico de caracteres (OCR, *Optical Character Recognition*) estándar, y técnicas de procesamiento de imagen actuales, con el fin de mantener su seguridad.

El objetivo de este artículo es presentar los resultados de una evaluación de estas características aplicada al sistema CAPTCHA más popular y difundido de la actualidad, el sistema reCAPTCHA.

2. El sistema reCAPTCHA

Hoy en día existen múltiples tipos de CAPTCHAs (de texto, de imagen o video, auditivos, cognitivos, etc. - véase [1] para una revisión exhaustiva), aunque los más popu-

lares son con diferencia los de texto, es decir, los que muestran una secuencia de caracteres en una imagen distorsionada utilizando diversas técnicas: adición de ruido, deformaciones, etc. y solicitan al usuario que introduzca dicha secuencia en un campo de texto de un formulario.

Si hay un CAPTCHA de texto singularmente importante por su difusión y su utilidad, ése es desde luego el sistema reCAPTCHA² [2][5]. Este sistema fue desarrollado por un equipo de investigadores de la Carnegie Mellon University, y ya en 2008 estaba desplegado en más de 40.000 sitios web, y había sido resuelto por humanos más de 1.200 millones de veces



Figura 1. Un ejemplo reciente del sistema reCAPTCHA.

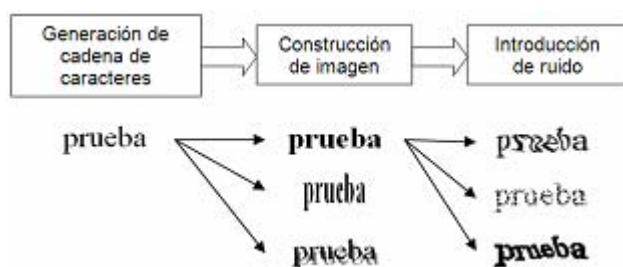


Figura 2. Proceso de generación de un CAPTCHA de texto.

en un año. Posteriormente ha sido adquirido por Google³, lo que ha contribuido aún más a su popularidad.

El sistema reCAPTCHA funciona como un servicio que se puede syndicar en cualquier sitio Web con unas pocas líneas de código, y que muestra al usuario dos palabras que debe introducir en el campo de texto para acceder al recurso protegido (ver figura 1). Mientras que muchos otros sistemas CAPTCHA exigen al usuario la introducción de una sola secuencia de caracteres, este sistema exige dos, una de las cuales ha sido generada automáticamente, y la otra ha sido obtenida como resultado de la aplicación de un OCR sobre un texto antiguo. La palabra generada automáticamente actúa como texto de control, mientras que la otra se usa para corregir los errores de reconocimiento del OCR.

De este modo, se aprovecha el tiempo invertido por los seres humanos en la resolución de reCAPTCHA para digitalizar manuscritos antiguos, en lugar de desperdiciar todo ese tiempo de "computación humana". De acuerdo con [5], en un solo año se han digitalizado el equivalente a 17.600 libros transcritos manualmente con un índice de éxito superior al 99%. Esta utilidad "solidaria" hace aún más popular e interesante al sistema reCAPTCHA. Las palabras transcritas manualmente por los usuarios de reCAPTCHA pertenecen al archivo del periódico New York Times, o a libros disponibles en Google Books.

3. Comprobando la seguridad de los CAPTCHAs

Los CAPTCHAs han sido objeto de continuos ataques, muchos de ellos con éxito, durante toda su existencia [1]. De ahí que sea esencial comprobar periódicamente que un CAPTCHA particular es resistente a los ataques y que sus creadores lo perfeccionen si los ataques tienen éxito.

Una pregunta esencial es qué porcentaje de éxito debe tener un ataque para que se considere un CAPTCHA inseguro. Supongamos que un sistema automático tiene la capacidad de resolver un CAPTCHA con un porcentaje de éxito de un 0,01%, o en otras palabras, es capaz de resolver automáticamente un

CAPTCHA una de cada 10.000 veces. Esto significa que si el atacante dispone de una botnet (red de ordenadores bajo su control infectados por medio de un virus) de 10.000 unidades⁴, con 10 hilos por unidad, es capaz de resolver unos 10 CAPTCHAs por segundo, lo que equivale a la creación de 864.000 cuentas de correo falsas al día si se está atacando el formulario de registro de un sistema de Webmail como Gmail o Hotmail [4]. En otras palabras, una tasa de resolución automática que intuitivamente se puede considerar muy moderada, puede en la práctica convertir a un sistema CAPTCHA en tremendamente inseguro.

Existen múltiples formas de intentar resolver automáticamente un CAPTCHA, que dependen obviamente del tipo de sistema utilizado (imágenes de texto, vídeo, audio, etc.), así como de otros factores como la propia seguridad de su implementación. Por ejemplo, para atacar el sistema reCAPTCHA no es necesario intentar reconocer las palabras de la imagen, ya que es posible atacar su funcionalidad de audio, que se presenta en la figura 1 a través del símbolo del altavoz, para resolver el reto planteado por el sistema. Esta funcionalidad, destinada a hacer el CAPTCHA accesible para sus usuarios con dificultades visuales, podría en consecuencia debilitar de manera crítica la seguridad del sistema si es comprometida.

Dado que los CAPTCHAs más populares son los de texto, y que el sistema particular en el que nos concentramos utiliza esta modalidad como vía principal de uso, trataremos el ataque a estos sistemas. El ataque a un sistema CAPTCHA de texto consiste, en la práctica, en una inversión de su proceso de generación. En la figura 2 se muestran los pasos habituales para la generación de un

CAPTCHA de texto, que serían los siguientes:

- 1) Generación de la cadena de caracteres que se utilizará como test para el usuario. Esta cadena puede ser aleatoria, constar de números, letras y otros caracteres, o puede ser obtenida a partir de un diccionario.
- 2) Obtención de una imagen inicial a partir de la cadena, que puede incluir ya perturbaciones a nivel de carácter, como el solapamiento de los caracteres que la forman, creación de sombras artificiales, o uso de distintos colores para cada carácter.
- 3) Introducción de ruido en la imagen generada, como ruido gaussiano (píxeles de distintos colores que disminuyen el contraste entre la cadena y el fondo), formas en negativo (como la que aparece en la cadena "gerYou" de la figura 1), deformaciones y rotaciones, etc.

Por analogía inversa, el proceso de ataque consta de los siguientes pasos:

- 1) Reducción del ruido de la imagen, como la aplicación de un algoritmo de binarización (paso a dos colores) para la identificación de áreas de interés (posibles caracteres), eliminación de píxeles aislados, etc.
- 2) Segmentación de la imagen en potenciales caracteres aislados, proceso que se puede realizar de diversas formas en función de las perturbaciones. Por ejemplo, se puede segmentar usando líneas imaginarias verticales que mantienen el color de fondo, si los caracteres no están solapados y no hay líneas que los unan.
- 3) Identificación de los caracteres aislados en cada fragmento de imagen, y su combinación para formar una palabra con sentido si la imagen original se ha generado a partir de un diccionario lingüístico.

Obviamente, los pasos que se dan para atacar un CAPTCHA dependen de los pasos que se han dado para crearlo. Por ejemplo, si no se han utilizado colores en su creación (como es el caso de reCAPTCHA), tampoco es preciso el proceso de binarización o paso a dos colores.

Siguiendo procesos similares a los anteriores, la seguridad de muchos CAPTCHAs ha sido comprometida. Por ejemplo, Mori y Malik [3] utilizaron una secuencia de pasos similar a la anterior para comprometer el sistema EZ-Gimpy, utilizado por Yahoo!, con un éxito de un 83% (158 sobre 191 casos de prueba), lo cual acabó obligando a dicha empresa a descartar el sistema.

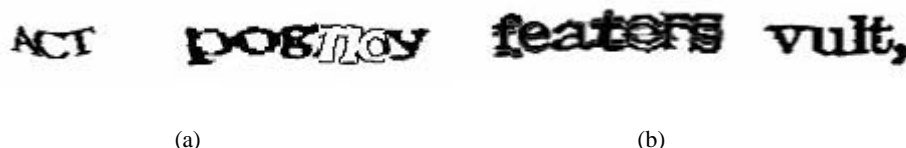


Figura 3. Versiones de reCAPTCHA analizadas en este trabajo.



Figura 4. Proceso de corrección de la deformación del texto: imagen original, proceso para estimar la ondulación, e imagen final.

4. Método de análisis de reCAPTCHA

4.1. Versiones de reCAPTCHA analizadas

Analizaremos aquí dos versiones recientes de reCAPTCHA, concentrándonos en el ataque a las imágenes proporcionadas por el sistema, que se muestran en la figura 3. En la primera versión (3.a), los caracteres utilizados en el texto están difuminados de manera que no se puedan separar, y en ocasiones, se muestra sólo el borde de las letras de las palabras. En la segunda versión (3.b), los caracteres usados también se unen con el fin de dificultar el proceso de aislamiento, y una de las palabras se "duplica" formando una sombra variable. En esta versión, la palabra no duplicada es usada para la corrección de OCR, mientras que la duplicada es el texto de control generado automáticamente.

4.2. Descripción general del proceso

Con el fin de analizar las versiones anteriores de reCAPTCHA, se ha procedido a implementar un proceso inverso al de generación de las imágenes, consistente en corregir las deformaciones y distorsiones introducidas y luego detectar los caracteres utilizados en las mismas. Cada palabra individual se ha tratado siguiendo los procesos siguientes:

- Aplicación del reconocedor óptico de caracteres Tesseract directamente sobre la imagen.
- Corrección de las deformaciones e inclinaciones de la imagen, y aplicación de Tesseract.
- Alternativamente, utilización de los algoritmos *Heuristic Over Segmentation* (HOS) y *Shape Contexts* (SC) sobre la imagen original, para la detección de los caracteres utilizados en ella.

Tesseract⁵ (v.3.01) es un sistema reconocedor óptico de caracteres de software libre considerado actualmente entre los más eficaces. Una de sus características más importantes es la utilización de múltiples diccionarios, siendo uno de los más extensos el del idioma inglés.

El proceso de corrección de deformaciones e inclinaciones de la imagen, desarrollado con el fin de aumentar la eficacia de Tesseract, y los algoritmos HOS y SC han sido implementados en MatLab, y se explican en las próximas secciones.

4.3. Pre-procesamiento de la imagen

El pre-procesamiento de la imagen, orientado a corregir las deformaciones más básicas, consta de los siguientes pasos:

- 1) Se intenta corregir la deformación global de las palabras de la imagen, calculando la línea horizontal central de la imagen, y transformando la imagen para que dicha línea sea recta. Este proceso se puede ver en la figura 4. Para ello, se obtiene la línea de máximos en la imagen, la línea de mínimos y la línea central, que será la que dé la pauta para corregir la ondulación de la figura. A la línea central se le aplican varios procesos de filtrado para suavizarla, debido a que letras como "p" o "l" que son más altas o bajas que el resto pueden dar lugar a deformaciones erróneas. De esta forma, se logra de forma suavizada la deformación de la palabra en global.
- 2) Se procede a corregir la inclinación de los caracteres, para lo que se construye una serie de imágenes rotadas en distintos ángulos. De estas imágenes obtenidas, se realiza una proyección horizontal de todas ellas, y se escoge aquella en que esta proyección tiene un menor

número de píxeles (en este caso, la primera de las cuatro que se muestra en la figura 5a). Tras elegir esta proyección, se obtiene el ángulo que se ha rotado y se puede corregir la imagen de la misma forma en que se modificó la ondulación de los caracteres, corrigiendo este ángulo de rotación, de forma que se bajan las letras en función del ángulo obtenido.

El resultado final de corregir ondulaciones e inclinaciones de las letras es el que se muestra en la figura 6.

4.4. Aislamiento de caracteres con el método HOS

Tanto en la primera versión de reCAPTCHA, pero sobre todo en la segunda, las correcciones anteriores son insuficientes ya que se ha introducido el duplicado de la palabra para dificultar en gran medida el aislamiento de los caracteres individuales, que es el paso fundamental en el ataque a un CAPTCHA. Este proceso en cuestión se suele denominar segmentación, y es habitualmente el proceso más complejo en los procesos de OCR.

Una técnica para realizar la segmentación, que con el tiempo se ha convertido prácticamente en un estándar, se denomina *Heuristic Over Segmentation* (HOS)[6]. Esta técnica consiste en la generación de un gran número de cortes potenciales entre los caracteres, usando métodos heurísticos de procesamiento de imagen, y la selección posterior de la mejor combinación de cortes de acuerdo con las probabilidades o resultados numéricos arrojados por un OCR. La eficacia de esta técnica depende, por tanto, de la calidad de los cortes generados, así como de la habilidad del OCR para distinguir correctamente los po-

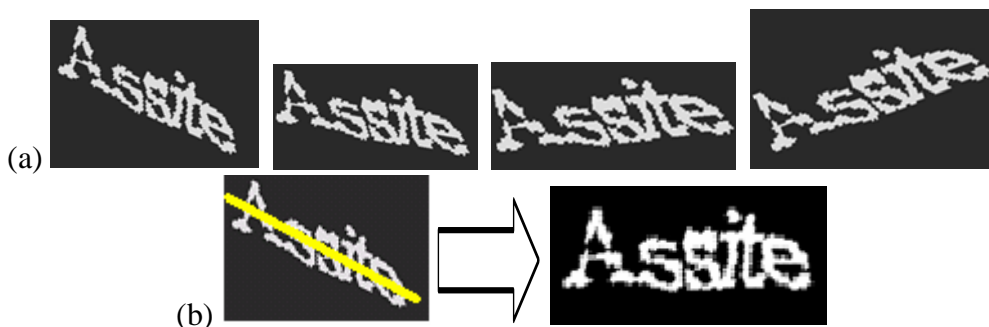


Figura 5. Proceso de corrección de la inclinación de los caracteres. Cuatro de las rotaciones obtenidas de la imagen (a), y corrección de la inclinación de la cadena a partir de la seleccionada (b).



Figura 6. Resultado global del proceso de corrección de la inclinación del texto.

tenciales caracteres segmentados a partir de sus partes.

Para determinar los posibles cortes, se analiza la palabra mostrada en la imagen y se establece un posible corte con un valor cuando se detecta un cambio abrupto en la parte superior o inferior del perfil horizontal (altura) de la misma. Cuando se encuentra al mismo tiempo un cambio abrupto en el perfil superior e inferior, el valor se duplica para ese posible carácter.

En la figura 7 se muestran los posibles cortes para una palabra de ejemplo. Se han representado dichos cortes correspondientes tanto a cambios abruptos en el perfil superior como en el inferior, usando líneas amarillas.

El proceso heurístico de generación de cortes se ha diseñado con el objetivo de obtener más cortes de los necesarios, en la esperanza de que el conjunto correcto de cortes esté incluido entre los generados. Una vez que se han obtenido los posibles cortes, las segmentaciones candidatas se representan a través de un grafo denominado grafo de segmentación. Se trata de un grafo acíclico dirigido con un nodo de inicio y un nodo final. A cada nodo interno se le asigna un corte candidato producido por el algoritmo de segmentación. Cada arco entre dos nodos se asocia con una imagen que contiene todos los píxeles entre el corte asociado al nodo origen, y el corte asociado al nodo destino de dicho arco [6].

Cada arco lleva asociado un valor que se determina utilizando la distancia entre histogramas, que se explicará en la sección siguiente sobre *Shape Contexts*, que es la forma en que se estima la distancia de cada "corte" con una letra del alfabeto. Por ejemplo, suponiendo que hay cuatro posibles cortes como se muestra en la figura 8, con los distintos pesos de ir de un nodo a otro se puede computar el camino mínimo y obtener



Figura 7. Cortes potenciales entre caracteres para una palabra de ejemplo.

el resultado final de la palabra. En este caso, el camino mínimo sería el formado por los nodos 1-3-4, con peso total 2.

4.5. Cálculo de similitud con el método Shape Contexts

La contribución principal en el trabajo de Belongie *et al.* [7] es un algoritmo robusto y simple para encontrar correspondencias entre formas. Las formas se representan con un conjunto de puntos muestreados de las formas, normalmente unos cien puntos. El descriptor de forma, llamado *Shape Context* (SC, Contexto de Forma), se utiliza para describir la distribución del resto de la forma con respecto a un punto determinado de la misma. Encontrar las correspondencias entre dos formas equivale a encontrar para cada punto muestreado en una forma el punto en la otra forma que tiene un SC más parecido.

En nuestro caso, hemos realizado 62 modelos de caracteres (26 letras del alfabeto, 26 letras en mayúscula y 9 dígitos), con 100 puntos elegidos para cada uno de los caracteres, que se comparan con el modelo que proviene de cada carácter de la imagen obtenida en reCAPTCHA.

Para cada punto p_i de la primera forma, se quiere encontrar el punto q_j más similar que se corresponda con la segunda forma. Consideramos un conjunto de vectores originados de un punto hacia todos los otros puntos de la forma. Estos vectores expresan la configuración de la forma entera relativa al punto de referencia.

Se calcula un histograma, desde el punto p_i a los $n-1$ puntos restantes, usando la siguiente fórmula:

$$h_i = \#\{q \neq p_i : (q - p_i) \in \text{bin}(k)\}$$

Este histograma se define como el SC de p_i . Se ha utilizado un sistema de coordenadas log-polar, para que el descriptor sea más sensible a diferencias en los píxeles más cercanos (ver ejemplo en figura 9). Además, se han normalizado los histogramas para que se puedan utilizar con un número diferente de puntos.

Para comparar distintos histogramas se ha usado la distancia X^2 , tal y como se muestra en la siguiente ecuación:

$$d(h_i, h_j) =$$

$$\sum_{\text{bins } k} \frac{\|h_i(k) - h_j(k)\|^2}{\|h_i(k)\| + \|h_j(k)\|}$$

Éste es el número que se utilizará en el ejemplo de la figura 8 para hallar las distancias de un nodo a otro.

5. Experimentos y resultados

5.1. Primera versión: bordes y deformaciones

Para la primera versión de reCAPTCHA, con bordes y deformaciones, se han obtenido 100 ejemplares que se corresponden con 200 palabras, y se han evaluado utilizando dos métodos. Por un lado, se ha aplicado el sistema OCR Tesseract de Google a las imágenes originales, y a las imágenes pre-procesadas para corregir las inclinaciones y deformaciones del texto. Por el otro, se han aplicado los métodos HOS y SC a las imágenes originales.

En la figura 10 se muestran los resultados de ambos métodos. En el gráfico de la izquierda se muestra el porcentaje de éxito del OCR Tesseract con las imágenes originales y pre-procesadas. Como se puede observar, dicho OCR es capaz de identificar correctamente un 4,5% de las palabras presentes en las imágenes originales, y más de un 10% cuando se han pre-procesado. Cabe reseñar que Tesseract hace

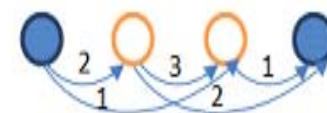


Figura 8. Ejemplo para determinar el proceso de selección de cortes y la palabra final.



Figura 9. Histograma en un punto de la letra A.

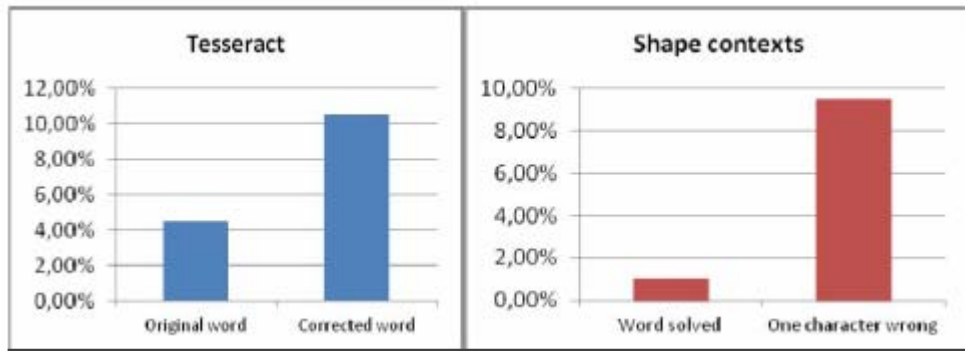


Figura 10. Resultados sobre el primer tipo de reCAPTCHA.

uso internamente de un diccionario del idioma inglés, lo que le permite identificar correctamente una palabra aunque no sea capaz de acertar todos los caracteres de la misma, y que la mayoría de las palabras usadas en reCAPTCHA están en idioma inglés.

Por otra parte, en el gráfico de la derecha se muestran los resultados de la aplicación de la técnica SC. Con esta técnica, se identifican correctamente un 1% de las palabras originales, y en casi un 9,5% de las palabras se falla un solo carácter. En consecuencia, con la ayuda de un diccionario de inglés, sería posible identificar correctamente hasta un 9,5% de las palabras.

Es importante reseñar que estos grados de éxito no se corresponden directamente con los de resolución de reCAPTCHA, dado que éste muestra dos palabras elegidas independientemente, y sólo una de ellas es la palabra de control. Si, por ejemplo, con el uso del pre-procesamiento y del OCR es posible acertar un 10% de las palabras, entonces podemos estimar un grado mínimo de acierto de las dos palabras de un 1% del CAPTCHA, pero el grado de resolución de reCAPTCHA puede alcanzar hasta un 10% si casualmente se acierta siempre la palabra de control, y en media puede alcanzar un 5% (es decir, la mitad de las veces que se acierta la palabra, ésta es la de control).

5.2. Segunda versión: palabras duplicadas

Para el análisis del segundo tipo de CAPTCHAs, también se han recolectado 100 ejemplares correspondientes a 200 palabras. En este tipo de reCAPTCHA, la palabra duplicada es siempre la palabra de control, por lo que es posible establecer una correspondencia más directa entre el número de palabras duplicadas resueltas y el de ejemplares de reCAPTCHA resueltos.

En la figura 11 se muestran los resultados de aplicar Tesseract sobre la palabra original, sobre la palabra pre-procesada, y sólo sobre las palabras duplicadas. A la derecha se muestran los resultados de aplicar Shape Context, y en particular, el porcentaje de veces que se resuelve la palabra completa, el porcentaje en que se falla sólo en un carácter, y el porcentaje de acierto sobre las palabras duplicadas. Como en el caso anterior, Tesseract hace uso de un diccionario de inglés, mientras que Shape Context no.

Como se puede observar, el OCR es capaz de identificar correctamente un 20% de las palabras originales. Sin embargo, el pre-procesamiento no permite mejorar los resultados, ya que las palabras que se muestran no sufren otra deformación que la propia duplicación de la palabra de control. Sin embargo, si nos concentramos en los resultados sobre las

palabras duplicadas, se puede observar que se obtiene un grado de acierto de un 1%, y dado que se trata de la palabra de control, se puede afirmar que el CAPTCHA se rompe en un 1% de las ocasiones.

Por lo que respecta a los resultados de Shape Contexts se puede observar que sólo es capaz de resolver un 0,5% de las palabras, alcanzando un 3% de aciertos cuando se falla sólo un carácter, y que su grado de acierto sobre las palabras duplicadas es del 0%. En conclusión, los resultados son sustancialmente peores que en el caso del primer tipo de reCAPTCHA, y no se puede concluir que esta técnica sea capaz de comprometer esta segunda versión.

6. Conclusiones

Para mantener la seguridad de los populares CAPTCHAs de texto, es necesario evaluar su resistencia a las técnicas más actuales de reconocimiento de imágenes. En este artículo se han evaluado dos versiones del sistema reCAPTCHA, uno de los más populares en la actualidad, usando dos técnicas diferentes. La primera versión, que incluye alteraciones en los caracteres para mostrar sólo su contorno, es vulnerable a la utilización del OCR Tesseract (capaz de resolver con éxito un 10% de las palabras), y a la técnica Shape Context (capaz de resolver con éxito un 1% de las palabras sin ayuda de un diccionario). Sin embargo, casi todas las palabras resueltas no

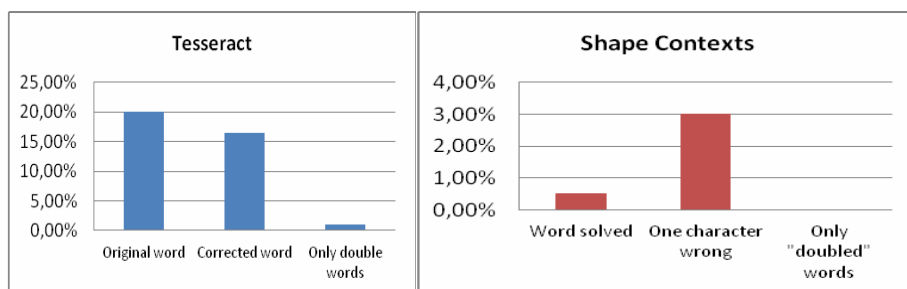


Figura 11. Resultados sobre el segundo tipo de reCAPTCHA.

habían sido alteradas con contornos, que suelen ser en torno a un 20% de las mostradas en reCAPTCHA. Además, no es posible conocer exactamente la tasa de éxito en la resolución de CAPTCHAs, porque no es posible conocer a priori cuál es la palabra de control.

En la segunda versión de reCAPTCHA, que utiliza sombras para duplicar las palabras de control, se ha conseguido resolver un 20% de las palabras usando Tesseract, y un 0,5% con Shape Contexts. Centrándonos sólo en la palabra de control, Tesseract es capaz de resolver un 1% de los reCAPTCHAs, mientras que Shape Contexts se queda en el 0% de éxito.

El proceso previo necesario para poder aplicar Shape Contexts consiste en la segmentación de la palabra en sus caracteres, que es una de las principales diferencias entre reCAPTCHA y otros CAPTCHAs, en los que se muestran los mismos completamente separados [3]. Por tanto, la técnica de segmentación HOS descrita en este artículo es esencial.

Por otra parte, Tesseract ha demostrado ser bastante robusto en las pruebas realizadas en este trabajo. Sin embargo, si las palabras utilizadas en el CAPTCHA no aparecen en el extenso diccionario de inglés usado por este programa, cabe esperar una reducción importante en la tasa de éxito de este sistema. En

cualquier caso, el pre-procesamiento usado en este trabajo puede marcar la diferencia entre romper o no romper un CAPTCHA.

Finalmente, sobre la evolución de las versiones de reCAPTCHA usadas en este artículo, se puede señalar que se resuelven más palabras en el segundo caso, pero el número de ejemplos de reCAPTCHA es inferior, por lo que se puede concluir que la seguridad del sistema ha aumentado. Sin embargo, los atacantes pueden deducir fácilmente que la palabra de control es la duplicada, y ahorrar bastante tiempo tratando de resolver sólo dicha palabra, aumentando por tanto las probabilidades de comprometer la seguridad del sistema.

Referencias

- [1] J.M. Gómez Hidalgo, G. Álvarez Marañón. CAPTCHAs: An Artificial Intelligence Application to Web Security. En Marvin V. Zelkowitz, ed. *Advances in Computers*, Vol. 83, Burlington: Academic Press, 2011, pp. 109-181.
- [2] L. von Ahn, M. Blum, J. Langford. Telling humans and computers apart automatically—how lazy cryptographers do AI. *Comm. of the ACM* 47 (2004), pp. 56-60.
- [3] G. Mori, J. Malik. Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA. *Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 1,

2003.

[4] Jonathan Wilkins. *Strong CAPTCHA Guidelines v1.2*, 2009. <<http://es.scribd.com/doc/24497942/Strong-CAPTCHA-Guidelines-v1-2>>.

[5] L. von Ahn, B. Mauer, C. McMillen, D. Abraham, M. Blum. reCAPTCHA: Human-Based Character Recognition via Web Security Measures, *SCIENCE*, Vol. 321, pp.1465-1468, septiembre 2008.

[6] Y. LeCun, L. Bottou, Y. Bengio, P. Haffner. Gradient-Based Learning Applied to Document Recognition, *Proceedings of the IEEE*, Vol. 86, No. 11, noviembre 1998.

[7] S. Belongie, J. Malik, J. Puzicha. Shape Matching and Object Recognition Using Shape Contexts. *IEEE transactions on Pattern Analysis and Machine Intelligence*, Vol. 24, No. 24, abril 2002.

Notas

¹ <<http://community.websense.com/blogs/securitylabs/archive/2012/01/30/trojan-caught-on-camera-shows-captcha-is-still-a-security-issue.aspx>>.

² <<http://www.google.com/recaptcha>>.

³ <<http://googleblog.blogspot.com/2009/09/teaching-computers-to-read-google.html>>.

⁴ De acuerdo con, por ejemplo, los resultados de un estudio de la empresa de seguridad Danballe, existen *botnets* integradas por millones de ordenadores, y una cantidad apreciable de botnets con más de 10,000 ordenadores: <<http://blog.danballe.com/?p=361>>.

⁵ <<http://code.google.com/p/tesseract-ocr/>>.

INVITA A UN AMIGO A QUE DISFRUTE, SIN COSTE ALGUNO Y DURANTE ESTE AÑO, DE LAS VENTAJAS DE SER SOCIO DE ATI
La esencia actual de ATI sigue siendo la misma que la originó:
Crear una red de profesionales que permita una mejora constante de la profesión informática, individual y colectivamente.

Solo necesitas introducir en el siguiente formulario tus datos (nombre, apellidos y número de socio y correo-e) y los datos de contacto de la persona a quien deseas invitar a ATI (nombre, apellidos y correo-e) y le remitiremos tu invitación.

No te llevará más de dos minutos y contribuirás a enriquecer vínculos asociativos, además de ayudar a fortalecer y hacer crecer esta red de profesionales.

>> Acceso al formulario: <http://bit.ly/atiinvita12>



* La persona beneficiada gozará durante el 2012 de: descuentos en formación, ofertas especiales, invitaciones a presentaciones y eventos, consulta de la revista Novática vía intranet, participación en foros, listas de distribución, grupos de interés, acceso preferente a la bolsa de trabajo, cuenta de correo electrónico...

** Esta promoción está limitada a un invitado por socio. No se podrá invitar a más de uno.

Las habituales referencias que desde 1999 nos ofrecen los coordinadores de las Secciones Técnicas de nuestra revista pueden consultarse en <<http://www.ati.es/novatica/lecturas.html>>.

Sección Técnica "Acceso y recuperación de información" (José María Gómez Hidalgo, Manuel J. Maña López)

Tema: Conferencia

El II Congreso Español de Recuperación de Información se celebrará en la Escuela Técnica Superior de Ingeniería Informática de la Universidad Politécnica de Valencia el 18 y 19 de junio de 2012. El congreso busca ser un foro de encuentro para investigadores, profesionales y docentes con interés en el área de la Recuperación de Información (RI), en el que se obtenga una visión de la actividad que se realiza en (pero no restringida a) España, así como servir de punto de encuentro para el debate y fomento de futuras iniciativas orientadas a la promoción del área en nuestro país.

Los organizadores de este congreso invitan a investigadores de instituciones y empresas nacionales y extranjeras a enviar trabajos originales, en español o inglés, que traten sobre cualquiera de las áreas relacionadas con RI, incluyendo, por ejemplo: Modelos de RI, RI en la Web, sistemas de filtrado y recomendación, RI en redes sociales, RI en imágenes y vídeos, minería de texto (clasificación y agrupamiento), RI multimedia y multilingüe, RI en biomedicina, RI geográfica, etc. <<http://users.dsic.upv.es/grupos/nle/ceri/index.html>>.

Tema: Libro

Estamos ante la segunda edición del libro *Modern Information Retrieval* de Ricardo Baeza-Yates y Berthier Ribeiro-Neto publicado el año 1999. La primera edición de este libro tuvo un éxito notable entre la comunidad internacional del ámbito de la Recuperación de Información, siendo libro de referencia de asignaturas en cientos de universidades de todo el mundo. Después de más de diez años, una parte significativa de la primera edición ha sido reescrita para incorporar nuevos resultados de investigación y, además, se han añadido nuevos capítulos para tratar temas de interés que no se recogían en la primera edición. En total, más de la mitad del material es nuevo.

El libro consta de 17 capítulos y un anexo (913 páginas), organizados en siete grandes temas: el problema de la recuperación de información y la interfaz de usuario, los aspectos clásicos de la recuperación de información, documentos y consultas, indexación y búsqueda, búsqueda en la Web, bibliotecas digitales y temas avanzados. Entre los temas avanzados encontramos: recuperación en texto estructurado, recuperación de información multimedia y sistemas de búsqueda de información en empresas.

El libro está fundamentalmente orientado a estudiantes e investigadores del área de la recuperación de información, incluyendo en cada capítulo una sección en la que se presentan los retos de mayor interés en investigación relacionados con los temas tratados en dicho capítulo y otra sección en la que se hace una discusión bibliográfica sobre los trabajos de mayor interés publicados hasta el momento. Sin embargo, también puede ser de utilidad para los profesionales interesados en el diseño de sistemas de búsqueda y recuperación de información.

Ricardo Baeza-Yates lidera en la actualidad el laboratorio de Yahoo! Research en Barcelona. Por su parte, Berthier Ribeiro-Neto dirige la Oficina de Ingeniería de Google para América Latina. El libro cuenta además con 13 colaboradores que han escrito capítulos enteros o han realizado contribuciones en algunos de ellos. La lista de estos autores es: Eric Brown, Carlos Castillo, Marcos André Gonçalves, David Hawking, Marti Hearst, Mounia Lalmas, Yoelle Maarek, Christian Middleton, Gonzalo Navarro, Dulce Poncela, Edie Rasmussen, Malcolm Slaney y Nivio Ziviani. La referencia completa del libro es: **Ricardo Baeza-Yates y Berthier Ribeiro-Neto. *Modern***

Information Retrieval. The Concepts and Technology behind Search. Second Edition, Pearson, 2011.

El libro cuenta con una página Web en la que puede encontrarse material adicional como, por ejemplo, diapositivas para cada capítulo y otros recursos educativos: <<http://www.mir2ed.org/>>.

Sección Técnica "Auditoría SITIC" (Marina Touriño Troitiño, Manuel Palao García-Suelto)

Tema: Errores y Fraudes. Auditoría Interna. Analíticas. CAAT y GAS. Auditoría Continua.

"*El diablo está en los detalles*"¹ publicado recientemente por ISACA nos ha llamado la atención, tanto por el caso de uso de 'herramientas de extracción y análisis de datos' (*audit analytics*)² que expone, cuanto por las diversas citas de estudios y encuestas que recoge. En estas líneas dedicaremos más atención a las citas que al caso. Pensamos que uno y otras pueden interesar a los lectores.

Según un estudio³, "el fraude impactó en 2010 al 87% de las organizaciones". Otro "estudio global de 1.843 casos de fraude ocupacional... encontró que la cuarta parte de ellos supuso pérdidas de al menos 1M USD, mientras que el descubrimiento de las actividades fraudulentas llevó (como mediana) 18 meses"⁴. Una tercera encuesta arrojó que "el 65% de los más de 1.400 que respondieron estaban de acuerdo en que la auditoría interna es para las empresas una importante línea de defensa contra el fraude"⁵.

Los autores del artículo afirman que "La mejor forma de descubrir fraudes, fugas de ingresos y abuso de los recursos corporativos es un enfoque sistemático [de la auditoría interna], con una metodología basada en riesgos". Lo que se puede hacer de forma "más eficaz y eficiente" con una 'herramienta de extracción y análisis de datos'. Añadiríamos que mejor con la incorporación, cuando proceda, de extracción, análisis y auditoría continuados⁶.

Esa forma "más eficaz y eficiente" debería proceder (según concluye PricewaterhouseCoopers, en una encuesta internacional a más de 2.000 auditores internos) de "emplear la tecnología enfocada a la resolución de un problema de negocio, más que adquirir la tecnología por la tecnología"; lo que "exige hallar formas de usar la tecnología para permitir una eficiencia medible"⁷. Los autores del artículo concluyen que "la auditoría basada en extracción y análisis de datos debería usarse para lograr objetivos bien definidos basados en un examen concienzudo de las áreas de riesgo clave".

El Instituto de Auditores Internos señaló en 2010 que "el uso por las funciones de auditoría interna de herramientas o técnicas automáticas se había convertido en una de las cinco prioridades estratégicas"⁸.

Por ello en RLI⁹, la empresa del caso -y en la que trabajan tres de los cuatro autores-, "cada auditoría comienza con seis semanas de planificación, durante cuyo lapso los auditores completan narrativas, flujogramas, evaluaciones de riesgos (que siempre incluyen un componente de fraude) y recorridos (*walk-throughs*) detallados de los procesos de auditoría. Esta es una fase crítica para todos los grupos de auditoría interna. Este enfoque disciplinado sirve para desarrollar un programa de auditoría basada en riesgo, con mucho hincapié en las técnicas de extracción y análisis de datos". Creo que en esto, muchos se podrían mirar y preguntar aquello de 'espejito, espejito...'

En RLI "los auditores se aseguran de que tanto los datos analizados cuanto los corporativos se comprendan, para cerciorarse de la validez de los resultados analíticos". "Es crucial validar los datos antes de su análisis y comprender el propósito de utilizar cada campo de entrada. Y aquí es donde resulta especialmente valiosa la experiencia con las herramientas analíticas y en técnicas de auditoría".

En la encuesta sobre auditoría interna del 2010 del Instituto de Auditores Internos "el 56% de las respuestas de empresas del 'Fortune 500' señalaron que creían que los auditores deben tener habilidades en minería y análisis de datos; requisito sólo precedido por el de conocimientos específicos del negocio y sector (61%) en el conjunto de habilidades de carrera más importantes para los auditores internos de hoy en día"¹⁰.

¹ 'El diablo está en los detalles. Lucha contra el fraude mediante auditoría analítica'. Traducción libre del título del artículo de Davis, Ferrel, Scranton and Millar: "The Devil's in the Details. Fighting Fraud With Audit Analytics" *ISACA Journal*, vol 1, 2012. <<http://www.isaca.org/Journal/Pages/default.aspx>>. ISACA tiene la política de limitar a sus socios el acceso a los artículos recién publicados (como éste) y abrirlos al público al poco tiempo, por lo que a la publicación de esta "referencia", probablemente sea ya público.

² o CAAT o GAS, de los cuales ACL, IDEA y SAS son ejemplos destacados.

³ Kroll, *Global Fraud Report*, 2010/11, <www.kroll.com/>.

⁴ Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud and Abuse, 2010, <www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/rtrtn-2010.pdf>.

⁵ Ernst & Young, *11th Global Fraud Survey, Driving ethical growth—new markets, new challenges*, 2010, <www.ey.com/GL/en/Services/Assurance/Fraud-Investigation—Dispute-Services/11th-Global-Fraud-Survey—Driving-ethical-growth—new-markets—new-challenges>.

⁶ Si se nos permite la broma, soltando unos 'demonios' para perseguir al 'diablo'.

⁷ PricewaterhouseCoopers, *A Future Rich in Opportunity: State of the Internal Audit Profession Study*, 2010, <www.pwc.com/us/en/press-releases/2010/pricewaterhousecoopers-2010-global-internal-audit-study.jhtml>.

⁸ The Institute of Internal Auditors, *Internal Auditing in 2010: Shifting Priorities for a Changing Environment*, 2010, <www.theiia.org/download.cfm?file=56143>.

⁹ RLI Insurance, <www.rlicorp.com>.

¹⁰ Nota 7.

Sección Técnica "Derecho y Tecnologías" (Elena Davara Fernández de Marcos)

Tema: ACTA: controvertido acuerdo en materia TIC

No cabe duda de que nos encontramos inmersos de lleno en la denominada "Sociedad de la Información" donde las Tecnologías de la Información y las Comunicaciones (TIC) desempeñan un papel fundamental y en el que cuestiones como la privacidad, el comercio electrónico o la propiedad intelectual han saltado a la palestra como protagonistas del debate político, social e incluso económico tanto a nivel nacional, como comunitario e internacional. En este sentido, a nivel internacional, una de las iniciativas que mayor controversia ha generado en los últimos meses ha sido el conocido como Tratado ACTA (*Anti-Counterfeiting Trade Agreement*) que tiene por objeto erradicar la lacra de la piratería de contenidos protegidos por derechos de autor. Conviene tener en cuenta que lo estipulado en el citado Tratado no tiene carácter vinculante para los Estados signatarios que, a día de hoy, son: Austria, Bélgica, Bulgaria, República Checa, Dinamarca, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Polonia, Portugal, Rumanía, Eslovenia, España, Suecia y Reino Unido.

Por lo que se refiere al contenido en sí y teniendo en cuenta que aborda un tema tan controvertido como el de la propiedad intelectual, baste decir que en el mismo se incluyen, entre otras medidas, la introducción de sanciones contra los proveedores de Internet por las infracciones realizadas por sus usuarios. Y es que, conviene tener en cuenta que, aunque ACTA hace hincapié en que los procedimientos que se pacten respeten la libertad de expresión y la privacidad, no han tardado en alzarse las voces en contra de su contenido, afirmando la necesidad

de ofrecer un marco que garantice los intereses de todos los agentes implicados. <<http://www.elmundo.es/elmundo/2012/01/27/navegan-te/1327685066.html>>.

Tema: Propuesta de nueva normativa comunitaria sobre privacidad y protección de datos

El derecho fundamental a la protección de datos va adquiriendo un mayor protagonismo con el paso de los años, tanto por la plena implantación de las TIC en todos los sectores de la vida política, social, económica y de ocio de los ciudadanos como por la mayor formación, información y, consecuentemente, concienciación que tienen éstos sobre el valor de sus datos de carácter personal y el riesgo al que, prácticamente a diario, se ven expuestos por prácticas de diversas entidades que les someten a tratamiento, en muchos casos, no autorizados. Hay que tener presente que el derecho a la protección de datos está amparado por varias normas que (tanto a nivel nacional como internacional) han tratado de ofrecer la mayor seguridad jurídica al titular de los datos, imponiendo deberes y obligaciones al responsable del fichero, responsable del tratamiento y encargado del mismo respecto a las medidas que han de adoptar a la hora de realizar un tratamiento de datos de carácter personal. Sin embargo, la rapidez en la aparición y desarrollo de Nuevas Tecnologías que suponen, además de grandes avances, un aumento en el riesgo al que se ven expuestos los datos de carácter personal, ha supuesto que la normativa comunitaria en la materia (que data de 1995) haya quedado obsoleta y no dé respuesta a algunas de las cuestiones de mayor relevancia en este sentido. Precisamente por ello, y tras un largo proceso de debate, reflexión y estudio, la Comisión Europea acaba de sacar a la luz sendas propuestas de modificación de la normativa vigente en protección de datos en forma de Directiva y Reglamento que vienen a aportar algo de luz en algunas cuestiones de vital importancia en materia de privacidad y protección de datos.

En todo caso, conviene tener en cuenta que la nueva normativa aún ha de ser aprobada por todos los Estados Miembros y publicada en el Diario Oficial de la Unión Europea para que comience a surtir efecto. Entre las principales novedades de las propuestas citadas, destacan: la aparición de nuevas definiciones de "dato de carácter personal", "dato biométrico" o "niño"; la inclusión de la obligación de notificar cualquier fallo en la seguridad que haya afectado a los datos de carácter personal en un plazo de 24 horas; la importancia tanto de la privacidad desde el diseño como de la privacidad por defecto; la incorporación del derecho al olvido o el derecho a ser borrado a los del titular, o la obligación para determinadas empresas de contar con un responsable en protección de datos, entre otros. <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf>.

Sección Técnica "Enseñanza Universitaria de Informática" Cristóbal Pareja Flores, J. Ángel Velázquez Iturbide

Tema: Python: referencias atípicas, ma non troppo

Cada vez se inicia más tempranamente el aprendizaje de la programación, y muy pronto la primera lengua materna no será el español o el polaco, sino el binario (que Dios no lo quiera), o el Python (que ya es otra cosa). Por ahora, los primerizos en programación son adolescentes o preuniversitarios, ya sea por su propia iniciativa o en el colegio, y en cualquiera de estos casos el lenguaje Python es una de las opciones más recomendables según opiniones autorizadas. Las referencias que podríamos apuntar desde aquí para iniciarse en este lenguaje en expansión son bien conocidas, pero nos fijamos en la siguiente: **Al Steward**, *Invent your Own Computer Games with Python*, 2nd. Edition, ISBN 978-0-9821060-1-3.

Este libro realiza una introducción al lenguaje mediante la programación de juegos. En realidad, este enfoque no es tan novedoso, y no son pocos los libros que prestan importancia a la programación de juegos. Pero es que, en esta referencia, los juegos son el pretexto principal, el

leitmotif que dirige el aprendizaje de la programación, y eso es lo atractivo para aprendices jóvenes y lo que hace esta referencia merecedora de nuestra atención. En la misma línea está el sitio *pygame*, un conjunto de librerías para programar en Python juegos o programas con gráficos y sonido: <<http://www.pygame.org/>>.

Hemos preferido esta vez dar pocas referencias, aunque el último sitio es en realidad un punto de partida bien surtido. No obstante, quien se quede insatisfecho siempre puede ir a *Youtube*, poner *Python programming* o *Game python programming*, y ver lecciones en vivo sobre este tema como si fueran los episodios de nuestra serie favorita de televisión.

Sección Técnica "Entorno Digital Personal" (Diego Gachet Páez, Andrés Marín López)

Tema: *Nuevos dispositivos y el Internet de las cosas*

Cada día nos abruma con la aparición de un nuevo dispositivo móvil, quizá un modelo de teléfono, quizá un *notebook*, una tableta o un lector de libros electrónico, siendo lo común en prácticamente todos ellos que tienen capacidad de conexión a Internet.

Algunos analistas pronostican que la próxima década tendremos en el planeta alrededor de 50 mil millones de dispositivos conectados a Internet, siendo ésta, definitivamente, la Internet de las cosas. Ni que decir tiene que las compañías telefónicas que proporcionan conectividad a estos dispositivos han hecho ya incursiones en varios sectores como la banca, salud, transporte, entretenimiento, etc. presentando ellas mismas soluciones de todo tipo a la conectividad M2M (*Machine to Machine*).

De todos estos sectores quizá el más prometedor es el de la salud. Hay que considerar que las actuales perspectivas de envejecimiento de la población y la infrautilización de las Tecnologías de la Información en este sector constituyen un campo propicio para la implantación masiva de soluciones M2M, soluciones que tienen que ver sobre todo con el cuidado en remoto de pacientes crónicos, así como dotar a los médicos y personal sanitario de herramientas y funcionalidades para el diagnóstico y tratamiento de este tipo de enfermedades.

Sección Técnica "Informática Gráfica" (Roberto Vivó Hernando, Miguel Chover Sellés)

Tema: *Videojuegos, la creación de contenidos es clave*

La industria del videojuego sigue creciendo de forma notable y aunque durante el año 2011 la consola continúa siendo el dispositivo más usado con una cuota de mercado del 21,5%, el consumo de juegos en móviles ha crecido hasta el 6,1% y se acerca al 7,8% de las videoconsolas portátiles. Este incremento de los juegos para móviles abre posibilidades al desarrollo de herramientas que faciliten la creación de juegos para este tipo de plataformas, donde hay que enfrentarse a diferentes arquitecturas y sistemas operativos:

GameSalad Creator. Herramienta de autor para la creación de juegos para no programadores que utiliza editores visuales y un sistema de lógica basada en la asignación de comportamientos a los actores del juego. Muy utilizado para el prototipado rápido. La aplicación está desarrollada para Mac OS X y puede generar juegos para iPhone y Web en formato HTML5. La versión profesional tiene un coste de 379€ por año <<http://www.gamesalad.com/>>.

StencylWorks. Herramienta para el desarrollo de juegos iOS y Flash, usando tanto ordenadores Mac como PCs, pudiendo programar o no dependiendo de las necesidades del usuario. Los juegos producidos pueden venderse en la tienda *online* de Apple. También puede usarse la plataforma de publicidad de Apple iAd, así como generar ingresos integrando anuncios de Mochi y las API de portales como Newgrounds y Kongregate. Su precio es de 113€ por año <<http://www.stencyl.com/>>.

Construct 2. Aplicación para la creación de juegos en formato HTML5 para quien quiera crear juegos sin necesidad de programar, incluyendo un

motor de físicas. Los juegos pueden integrarse en Facebook, distribuirse a través de la tienda *online* de Chrome, así como jugarse en dispositivos móviles y tabletas. La versión de uso comercial completa tiene un coste de 275€ <<http://www.scirra.com/>>.

GameMaker. Entorno de desarrollo de juegos que pueden ser publicados en iOS, Android, Symbian y HTML5. El sistema permite el diseño de juegos con fondos, gráficos animados, música y efectos sonoros. Además dispone de un lenguaje de *scripting* (GameMaker Language) para obtener máxima flexibilidad en la creación de videojuegos. Esta disponible para Windows y Mac y el precio de su versión más cara es de 75€ <<http://www.yoyogames.com/>>.

Sección Técnica: "Lengua e Informática" (M. del Carmen Ugarte García)

Tema: *Resumen de los principales cambios en la gramática y ortografía del español*

Si siempre te ha interesado la corrección en el empleo de la lengua, puede que estés un poco preocupado por los cambios que tanto en gramática, a raíz de la publicación de la "Nueva gramática de la lengua española" (2009), como en la ortografía, "Ortografía de la lengua española" (2010), se han producido en los últimos años, y de los que la prensa se ha hecho eco, pero las notas de prensa no son por sí mismas suficientes para estar al día de esos cambios.

Tanto la Gramática como la Ortografía son lo suficientemente voluminosas como para desanimar a los no especialistas. ¿Qué hacer para entonces? El especialista en gramática normativa, Leonardo Gómez Torrego, pone a nuestra disposición en línea un excelente resumen en 17 didácticas páginas de los cambios en la gramática y ortografía del español. <www.sm-ele.com/ArchivosColegios/NuevoELEAdmin/Archivos/Descargables/Colección_Gómez_Torrego/134002_normativa_FOLLETO>.

Sección Técnica: "Lenguajes de Programación" (Oscar Belmonte Fernández, Inmaculada Coma Tatay)

Tema: *Liberado bajo licencia Apache el lenguaje de programación Kotlin*

La empresa JetBrains <<http://www.jetbrains.com>> ha hecho Open Source su lenguaje de programación Kotlin. JetBrains es conocida por sus entornos integrados de desarrollo para lenguajes tales como Java, Python o C#. Kotlin es un lenguaje de programación basado en tipos estáticos, con una sintaxis más sencilla que la de Java, incluyendo *closures*, un tiempo de compilación similar al de Java y generando código para ser ejecutado en un máquina virtual Java.

Tema: *Libro*

Óscar Belmonte Fernández, Carlos Granell Canut y María del Carmen Erdozain Navarro han publicado un libro electrónico con licencia Creative Commons titulado "Desarrollo de proyectos informáticos con tecnología Java", que se puede descargar desde la página <<http://www3.uji.es/~belfern/docencia.html>>. El objetivo de este libro es doble, por una parte mostrar el lenguaje de programación Java, y por otra algunas de las herramientas que se han convertido en imprescindibles en los proyectos que utilizan este lenguaje de programación.

Sección Técnica "Lingüística computacional" (Xavier Gómez Guinovart, Manuel Palomar)

Tema: *Manual de PLN*

Nitin Indurkha, Fred J. Damerau (eds.). *Handbook of Natural Language Processing, Second Edition.* Machine Learning & Pattern Recognition Series. Boca Raton, Chapman and Hall/CRC, 2010, 704

páginas. ISBN 978-1-4200-8592-1. Versión completamente actualizada del clásico libro del mismo título cuya primera edición en el año 2000 estuvo a cargo de Robert Dale, Hermann Moisl y Harold Somers. En este caso, la elaboración del manual se ha llevado a cabo bajo la dirección de Nitin Indurkha, de la University of New South Wales y del ya fallecido Fred J. Damerou, investigador del IBM T. J. Watson Research Center pionero en el campo del procesamiento de textos.

El libro actual incluye 26 capítulos repartidos en tres partes. La primera reúne 6 capítulos sobre el procesamiento simbólico del lenguaje a nivel gráfico, léxico, sintáctico, semántico y textual. La segunda parte, que es la más extensa del volumen, incluye 11 capítulos que versan sobre los modelos estadísticos de procesamiento lingüístico, con apartados dedicados al tratamiento de corpus, a la desambiguación léxica, al reconocimiento del habla o a la traducción automática estadística. Finalmente, la tercera parte agrupa 9 capítulos que presentan el estado de la cuestión de diversas aplicaciones del PLN de gran relevancia actual, como la traducción automática, la recuperación de la información, la respuesta a preguntas, la extracción de información, la generación de informes, la construcción de ontologías, la minería de textos o el análisis de sentimientos.

Entre los más de 40 especialistas de todo el mundo que han participado en la elaboración del volumen, cabe destacar, por su proximidad geográfica, a Leo Wanner, de la Universitat Pompeu Fabra, autor del capítulo sobre la generación automática de informes, y a José Luis Vicedo, de la Universitat de Alacant, coautor junto a Diego Mollá Aliod del capítulo sobre sistemas de respuesta a preguntas.

En suma, se trata de un manual académico amplio y actualizado, muy adecuado para impartir esta disciplina en cursos de postgrado. El manual se acompaña de una wiki en línea con actualizaciones y material suplementario, de libre consulta en <<http://handbookofnlp.cse.unsw.edu.au/>>.

Sección técnica "Profesión Informática" (Rafael Fernández Calvo, Miquel Sarries Griño)

Tema: *La Junta de Andalucía rechaza los estatutos del Colegio Profesional de Ingenieros Técnicos en Informática de Andalucía*

Nuestro compañero Ignacio Agulló, Presidente de ATI Galicia y miembro de la Junta Directiva General, ha subido al portal barrapunto.com un comentario sobre el requerimiento hecho por la Junta de Andalucía al Colegio Profesional de Ingenieros Técnicos en Informática de Andalucía para que subsanen los numerosos errores e ilegalidades incluidos en sus Estatutos. Además, el portal Meneame indica en <<http://www.meneame.net/story/varapalo-junta-estatutos-cptia>> que la situación del Colegio Profesional de Ingenieros en Informática de Andalucía es similar.

Éste es el texto del jugoso y documentado comentario de Ignacio Agulló en <<http://espana.barrapunto.com/article.pl?sid=12/03/20/1135211>>: "Que la profesión informática no necesita de colegiación obligatoria es algo bastante obvio, es la dirección en la que se han estado moviendo siempre el estado español y la Unión Europea.

Aún así, siempre hay gente que se frota las manos pensando en recuperar el sistema de gremios de la Edad Media y hacer de la profesión un coto cerrado en el que solamente unos cuantos puedan trabajar; y en algunas autonomías como Andalucía, consiguieron llevarse al huerto a los políticos y que aprobaran leyes que exigían la colegiación obligatoria para poder ejercer la profesión (11/2005 y 12/2005).

Por eso esta noticia es tan importante, más allá de la anécdota de unos estatutos plagados de fallos:

- Porque la resolución de la Junta de Andalucía rechaza la colegiación obligatoria para el ejercicio de esta profesión.

- Porque este rechazo se fundamenta en la reciente ley 10/2011, que modifica la Ley 10/2003, reguladora de los colegios profesionales de Andalucía (lo cual a su vez enmienda el error cometido en las leyes 11/2005 y 12/2005); de manera que la colegiación no sólo deja de ser obligatoria en Andalucía para los ingenieros técnicos sino también para los ingenieros.

- Porque a su vez esta ley andaluza 10/2011 sigue el dictado de la ley española 25/2009, que modifica la ley 2/1974, sobre colegios profesionales, y establece que la obligatoriedad de colegiación solamente podrá ser establecida por ley estatal, que para el caso de la informática no hay ni se la espera. Queda anulada así la obligatoriedad que se había ido estableciendo una serie de autonomías además de Andalucía: Canarias, Castilla-La Mancha, Castilla-León, Comunidad Valenciana, Extremadura y Galicia.

Hoy es un gran día porque por fin ha quedado demostrado que la colegiación obligatoria no tiene lugar en la informática. No está de más un recuerdo a la labor de ATI, Asociación de Técnicos de Informática, que dio la cara contra la colegiación obligatoria, y también por AII, que también se mojó."

A este respecto hay que señalar que ATI se ha declarado contraria en numerosas ocasiones a la colegiación obligatoria y a los colegios excluyentes, incluidos los de Andalucía (ver el editorial "Andalucía: otra Ley de Colegios excluyente e inoperante" en el nº 175 de *Novática*, mayo-junio 2005).

Hay en particular una frase premonitoria en el documento "ATI ante los Colegios Profesionales de Informáticos", publicado en el nº 139 de *Novática*, mayo-junio 1999: "Pero aun siendo cierto que el reto de los Colegios Profesionales es importante para el futuro de ATI, no debemos olvidar que muy probablemente lo sean mucho más el efecto de la globalización de la economía sobre el ejercicio profesional, la rápida obsolescencia de los conocimientos tecnológicos, la creciente importancia del ámbito europeo de decisión en lo que se refiere a las condiciones para el ejercicio profesional y, sobre todo, el reto de un cambio social y económico inducido por las TIC sobre el que los informáticos y sus organizaciones profesionales tenemos mucho que decir y que hacer desde diversos puntos de vista (tecnológico, ético, social)."

Sección técnica "Seguridad" (Javier Areitio Bertolín, Javier López Muñoz)

Tema: *Libros*

C. Elisan. "Malware, Rootkits and Botnets. A Beginner's Guide". McGraw-Hill Osborne Media. ISBN 0071792066, 2012.

J. Zhan, S. Matwin. "Secure Data Mining". Springer. ISBN 038787965X, 2012.

N.K. McCarthy. "The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk". McGraw-Hill Osborne Media. ISBN 007179039X, 2012.

A. Karasaridis. "DNS Security". Springer. ISBN 038776545X, 2012.

W. Krag Brotby, G. Hinson. "Practical Information Security Metrics". Auerbach Publications. ISBN 1439881529, 2012.

M. Jakobsson. "The Death of the Internet". Wiley-IEEE Computer Society. ISBN 1118062418, 2012.

L. Andrews. "I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy". Free Press. ISBN 1451650515, 2012.

A.-R. Sadeghi, D. Naccache. "Towards Hardware Intrinsic Security. Foundations and Practice". Springer ISBN 3642144516, 2010.

Tema: *Congresos-Conferencias-Reunión-Simposium*

RECSI-2012. Reunión Española de Criptología y Seguridad de la Información. Del 4 al 7 de septiembre 2012. San Sebastián, España.

Usenix Security 2012. 21st Usenix Security Symposium. Del 8 al 10 de agosto 2012. Washington, USA.

SECURMATICA'2012. XXIII Congreso Español de Seguridad de la Información. Del 24 al 26 de abril 2012. Campo de las Naciones, Madrid, España.

Privacy Security Trust 2012. 10th Annual Conference on Privacy, Security and Trust. Del 16 al 18 de julio 2012. París, Francia.

NSS'2012. The 6th International Conference on Network and System Security. Del 21 al 23 de noviembre 2012. Wu Yi Shan-Fujan, China.

Sección Técnica: "Tecnología de Objetos" (Jesús García Molina, Gustavo Rossi)

Tema: OCL en el Desarrollo de Software Dirigido por Modelos

OCL (*Object Constraint Language*) fue definido por OMG como un lenguaje "compañero" de UML para dotar de mayor expresividad a los modelos creados con este lenguaje de modelado visual. Con OCL es posible añadir a un diagrama de clases UML construcciones como invariantes, pre y postcondiciones de métodos, reglas de derivación o *queries*, y en un diagrama de máquinas de estado UML podríamos expresar con OCL las condiciones de una transición o restricciones sobre los estados. Es bien sabido que la combinación de UML y OCL permite escribir modelos orientados a objetos precisos y exentos de ambigüedad. En esta sección ya se presentó una de las principales referencias para aprender OCL, el libro de Jos Warmer y Anneke Kleppe titulado "*The Object Constraint Language. Getting your modelos ready for MDA*" (segunda edición).

En el Desarrollo de Software Dirigido por Modelos (MDD), al cual hemos dedicado varias columnas en esta sección y una monografía (*Novática* n° 192, marzo-abril, 2008), OCL juega un papel importante ya que es utilizado en la creación de Lenguajes Específicos de Dominio (DSL). En la columna del pasado octubre (n° 213) abordamos el tema de la creación de DSLs y en esta ocasión analizaremos el papel que juega OCL en este proceso, para lo cual profundizaremos en la naturaleza que tiene un metamodelo.

Un DSL consta de tres elementos: la *sintaxis abstracta* que define los conceptos del lenguaje y las relaciones entre ellos, así como las reglas que establecen cuando un modelo está bien formado (*well-formedness rules*); la *sintaxis concreta* que establece la notación, y la *semántica* del lenguaje que normalmente es definida a través de la traducción de los conceptos del DSL a conceptos de otro lenguaje destino cuya semántica es conocida (por ej., un lenguaje de programación como Java).

En MDD, la sintaxis abstracta de un DSL se define mediante un metamodelo, esto es, un modelo conceptual del lenguaje que es expresado normalmente en un lenguaje de metamodelado que ofrece los conceptos básicos del modelado estructural orientado a objetos: clases, atributos, agregación, referencias entre clases y herencia. Ecore es el lenguaje de metamodelado más extendido y es el elemento central del *Eclipse Modeling Framework* (EMF) que proporciona la infraestructura básica del proyecto de Eclipse para crear herramientas y soluciones MDD <<http://www.eclipse.org/modeling/emf/>>. Además del modelo conceptual de la sintaxis abstracta del DSL, la creación del metamodelo también requiere de un lenguaje que permita expresar las reglas que establecen cuando un modelo está bien formado. OCL (o una variante) es el lenguaje más usado para escribir estas reglas, de ahí parte de su importancia en MDD.

Recientemente, se ha creado como parte del proyecto MDT de Eclipse/EMF un DSL textual denominado OCLinEcore <<http://wiki.eclipse.org/MDT/OCLinEcore>> que permite escribir código OCL que se asocia a un metamodelo. Dado que también existe el DSL Emfatic <<http://wiki.eclipse.org/Emfatic>> para expresar metamodelos (esto es, la parte estructural) ahora se dispone de la facilidad de expresar metamodelos completos en forma textual.

Una vez definida la sintaxis abstracta, el desarrollador de un DSL debe abordar la tarea de dotarlo de una sintaxis concreta o notación que puede ser textual, gráfica o híbrida para lo cual puede usar herramientas como Metaedit+ o DSL Tools en el caso de un DSL gráfico, o MPS, Xtext o EMFText en el caso de uno textual. Y para acabar debe escribir las transformaciones modelo-a-texto, que pueden ir acompañadas de transformaciones modelo-a-modelo si se crean modelos intermedios para facilitar la transformación. Tanto los lenguajes de transformación modelo-a-modelo (por ejemplo, ATL o Xtend) como los modelo-a-texto (por ej., MofScript, Mof2Text o Xpand) proporcionan algún lenguaje tipo-OCL para navegar por los modelos o para definir *queries* sobre ellos. Esta navegación es esencial cuando se escriben transformaciones de cualquier tipo para acceder a la información deseada de los modelos de entrada a una transformación. Esta es la segunda razón de la importancia de OCL en MDD. Conviene notar que las reglas del metamodelo simplifican la escritura de transformaciones dado que el proceso de validación de un modelo se puede realizar antes de ejecutar la transformación.

Por tanto, la enseñanza de OCL suele formar parte de los cursos de formación en MDD ya que cualquiera que desee crear soluciones y herramientas MDD (no simplemente ser usuario de soluciones) debe dominarlo bien. La importancia de OCL en MDD fue subrayada justo cuando escribíamos esta columna en el blog de Jordi Cabot <<http://modeling-languages.com/why-you-need-to-learn-ocl/>>, responsable de uno de los grupos de investigación en MDD más relevantes, y aprovechamos para sugerir que todos aquellos interesados en MDD visiten este estupendo blog.

Sección Técnica: "TIC y Turismo" (Andrés Aguayo Maldonado, Antonio Guevara Plaza)

Tema: Congreso TURITEC 2012

El congreso Turitec (Tecnologías de la Información y las Comunicaciones Aplicadas al Turismo) tiene carácter bianual y es el principal evento científico-técnico sobre TIC y turismo. En este año se cumple su novena edición y se celebrará en el Palacio de Ferias y Congresos de Málaga durante los días 25 y 26 de octubre de 2012.

Durante los últimos años, se ha convertido en un foro de referencia nacional donde los profesionales del sector y los investigadores universitarios se encuentran para intercambiar experiencias y comunicar sus resultados de investigación.

El congreso consistirá en una serie de sesiones en las que se presentarán contribuciones científico-técnicas y experiencias de gestión en el sector. Igualmente se desarrollarán varias conferencias de personalidades de relevancia del sector turístico en España y ponencias ofrecidas por expertos en los distintos campos del congreso.

Los trabajos pueden enviarse hasta mediados del mes de junio y siguen un sistema de revisión por pares. Las líneas de interés de este congreso incluyen cualquier área dentro de las tecnologías de la información y las comunicaciones en turismo, prestando especial atención a los temas que el lector podrá encontrar referenciados en la sección "Ámbito y temas" de la web del congreso: <<http://www.turitec.com/>>.

Francisco Ruiz González
 Instituto de Tecnologías y Sistemas de Información,
 Universidad de Castilla-La Mancha;
 socio sénior de ATI

<francisco.ruizg@uclm.es>

La Investigación en Informática en España: Análisis bibliométrico

1. Introducción

La cienciometría se dedica al estudio de la producción científica. Habitualmente está basada en el empleo de datos sobre publicaciones científicas, recibiendo entonces el nombre más específico de bibliometría. Entre las principales fuentes bibliométricas destaca "Web of Science" (WOS), de Thompson-Reuters [1], conocida hasta hace poco como ISI. Es probablemente la más reconocida a nivel mundial gracias a su índice JCR (*Journal Citation Report*) para clasificar y valorar revistas científicas.

En este artículo se presenta un resumen de los resultados de un estudio bibliométrico sobre la producción científica en Informática en España. La versión completa puede encontrarse en la web <http://alarcos.esi.uclm.es/per/fruiz/wos_cs/>, incluyendo todos los datos en forma de tablas y de mapas, así como archivos .kmz para visualizarlos y consultarlos con Google Earth.

Los principales criterios aplicados en el estudio fueron:

- Utilizar WOS, al ser la referencia más reconocida para estos fines.
- Emplear el quinquenio 2006-2010 para tener una visión actual (no histórica) a la vez que se evitan las fluctuaciones anuales. Las consultas WOS utilizadas pueden ser descargadas de la web para que el lector pueda replicarlas.
- Emplear el número de artículos en revistas y el número de veces que una publicación es referida por otras (citas) como indicadores cuantitativo y cualitativo, respectivamente.
- Analizar los datos a nivel global de Informática y también por especialidades (llamadas *categories* en WOS) [2].
- Evaluar la situación global de España y también por organizaciones individuales.

Aunque es sabido que los congresos desempeñan un papel clave en la investigación en Informática, se optó por contar sólo artículos en revistas buscando un alineamiento con la manera de proceder de las disciplinas más tradicionales en investigación. Además, la gran mayoría de las citas proceden de los artículos en revistas (3,9 de media por artículo de revista frente a 0,9 de un "paper" en congreso).

El resto del artículo se organiza de la siguiente manera: en la **sección 2** se presenta la posi-

Resumen: En los últimos 20 años la investigación en Informática en el estado Español ha logrado unos avances muy importantes. Así, Informática ha logrado posicionarse como una de las disciplinas en las que España tiene más peso a nivel internacional. Esto ha sido posible gracias a la constitución de una importante comunidad de profesores investigadores en un número significativo de universidades. En este artículo se resume un estudio estadístico, basado en datos bibliométricos obtenidos del 'Web of Science' (antiguo ISI), que permite hacerse una clara composición cuantitativa y cualitativa de la situación.

Palabras clave: Estudio bibliométrico, investigación en Informática.

ción que desempeña España a nivel mundial y en la **sección 3** se ofrece una panorámica general a nivel de país y un resumen de la evolución reciente. La **sección 4** se dedica a mostrar el mapa de la investigación Informática por organizaciones. Con más detalle, la **sección 5** precisa la situación para las 7 especialidades (categorías WOS). El artículo finaliza con un resumen y conclusiones en la **sección 6**.

2. Posición internacional

En la **tabla 1** se muestran las cifras de artículos para los diez países con mayor producción en el periodo 2006-2010. España ocupa una muy honrosa novena posición, de forma que el 4,7% de los artículos publicados en el mundo tienen algún autor español. Si se comparan los porcentajes con el quinquenio 1996-2000, cabe concluir que la evolución de España ha sido de las más favorables ya que se encuentra entre los cuatro países, junto con China, Corea del Sur y Taiwán, que han mejorado más de 2 puntos. Estos buenos datos no coinciden con la realidad industrial del país, pero debe recordarse que se trata de

producción de conocimiento y nada significan en términos de su transferencia (patentes, etc.). Este otro es el gran y difícil reto que tenemos pendiente y que corresponde, fundamentalmente, al tejido empresarial, ya que son las empresas las únicas que pueden aprovechar de forma práctica el conocimiento generado por las universidades y centros de investigación.

Si se analizan los datos desglosados para las siete categorías en que WOS divide la Informática, se comprueba que en todas ellas la producción española tiene un peso internacional significativo, oscilando entre un máximo del 5,6% para la Inteligencia Artificial y un mínimo del 3,6% para los Sistemas de Información. Respecto del promedio mundial, estas diferencias manifiestan un pequeño sesgo hacia las especialidades más teóricas. Si se mira la evolución relativa de los porcentajes sobre el total mundial, se observa que la muy positiva evolución de la producción científica Informática española es común a todas sus especialidades, aunque destacando ligeramente la Ingeniería y Tecnología del Software.

	PAIS	Artículos		%		
		2006-2010	1996-2000	2006-2010	1996-2000	cambio
1	Estados Unidos	47055	38240	26.41	34.45	-8.03
2	China	23014	2698	12.92	2.43	10.49
3	Inglaterra	11077	7916	6.22	7.13	-0.91
4	Alemania	10670	8851	5.99	7.97	-1.98
5	Francia	9914	6296	5.57	5.67	-0.11
6	Canadá	9322	4962	5.23	4.47	0.76
7	Taiwán	9255	3199	5.20	2.88	2.31
8	Japón	8488	6862	4.76	6.18	-1.42
9	ESPAÑA	8395	2750	4.71	2.48	2.24
10	Corea del Sur	7996	2300	4.49	2.07	2.42
TOTAL MUNDIAL		178139	111007			

Tabla 1. Producción de artículos en Informática por países.

Disciplina	Artículos	% Mundial	Citas	FI
Astronomía	5589	7.52%	70439	12.60
Ciencia y Tecnología de los Alimentos	7267	7.21%	49617	6.83
Ciencias Medioambientales y Ecología	11800	5.08%	85227	7.22
Economía y Negocios	5057	4.82%	14625	2.89
INFORMÁTICA	8395	4.71%	32837	3.91
Agricultura	9258	4.68%	48264	5.21
Ciencias de la Comunicación y la Información	1209	4.61%	2332	1.93
Matemáticas	11692	4.51%	40309	3.45
Biología	11404	4.48%	69933	6.13
Ingeniería Química	4295	4.44%	32193	7.50
Química	28949	4.14%	251585	8.69
TODAS las disciplinas	190800	3.54%		

Tabla 2. Producción científica española por disciplinas (2006-2010).

3. Situación dentro de España

A continuación se comentan los datos que permiten comparar, dentro de España, con el resto de disciplinas. Para ello se han estudiado las cifras para 37 disciplinas que clasifican todas las áreas del saber. La **tabla 2** muestra las cifras para las disciplinas en las que el porcentaje de artículos españoles supera el 4% del total mundial. Esta tabla permite hacerse una idea general de las disciplinas en que España tiene más peso internacional y, por tanto, de aquellas en que los esfuerzos de transferencia podrían impactar de manera más evidente en la competitividad internacional del país. Informática aparece en quinta posición, siendo la primera disciplina dentro del ámbito de la ingeniería y tecnología, seguida por Agricultura.

En términos absolutos las primeras disciplinas en producción son Medicina Clínica, Química, Física y Ciencias Básicas de la Vida, todas ellas con más de 20.000 artículos. Las diferencias en producción absoluta entre unas disciplinas y otras dependen de diversos factores, como el tamaño de la comunidad investigadora y su productividad media, pero también de la cultura o hábitos. En este sentido, Informática es una disciplina que ha avanzado mucho en los últimos años en el hábito de publicar en revistas. Además, si se computan los trabajos publicados en actas de congresos, tan importantes en nuestra disciplina, la producción media de artículos por investigador es parecida a la de las áreas de ciencias experimentales. La columna FI muestra el factor de impacto, es decir, la media de citas por artículo. En cifras de impacto estamos bastante más atrás que otras disciplinas, que cuentan con una comunidad de investigadores y de revistas, donde publicar, significativamente mayores.

Llama un poco la atención que las disciplinas en que España juega un papel más importante a nivel mundial no son las que habitualmente se ven reflejadas en los medios de comunica-

ción y que en los ámbitos académicos aparecen también muchas veces como los puntos fuertes del país en investigación. Así, se ha transmitido una cierta idea de que donde España es más potente a nivel científico es en Ciencias Básicas de la Vida y en Ciencias Biomédicas. De hecho, la mayoría de las noticias sobre ciencia y tecnología se refieren a ellas y los grandes centros de investigación públicos, con cientos de investigadores, están dedicados fundamentalmente a ellas. Obviamente, en tamaño, las comunidades de estas dos disciplinas son bastante mayores que la de Informática, y parecido pasa a nivel mundial. Sin embargo, la producción científica en Informática española supone el 4,7% del total mundial, mientras que en Ciencias Básicas de la Vida es el 3,9% y en Ciencias Biomédicas el 3,3%.

En cuanto al grado de internacionalización de los 8.395 artículos en Informática, cabe mencionar que el 33,8% se han realizado en colaboración con autores de otros países, destacando en primer lugar Estados Unidos (7,1%), seguido de Inglaterra, Italia, Francia y Alemania. Respecto de la multidisciplinariedad, los datos de WOS permiten establecer que el 56,8% de los artículos están publicados en revistas que también se incluyen en categorías no informáticas. Entre dichas categorías destacan Ingeniería Eléctrica y Electrónica (16,1%), Matemáticas y Estadística (15,6%), Automática (4,9%), y Telecomunicaciones (4,6%).

Llama la atención que, prácticamente, no existe intersección con las categorías de "Administración" (*Management*), Negocios (*Business*) y Economía (*Economics*). Quizás nuestros intereses en investigación no coinciden con los de los colegas de Economía y Negocios; o quizás nuestra manera de trabajar, sistémica y rigurosa por obligación, les queda demasiado lejana. La situación es más llamativa si cabe cuando se compara con otros países en los cuales la colaboración en

investigación entre ambas disciplinas es bastante común.

El positivo presente de la investigación española en Informática es, lógicamente, fruto de una muy favorable evolución histórica, como se refleja al analizar las cifras de artículos indexados en WOS en los últimos 30 años. Así, en 1981 sólo se publicaron 13 artículos con autor español. En 1989 se superaron, por primera vez, los 100 artículos. En 2001 se sobrepasaron los 500 y en 2006 se alcanzó el millar. La evolución ascendente ha seguido en los últimos años hasta llegar a 1.820 en el año 2010. Esta fuerte mejora en cifras absolutas también ha significado una importante mejora en el peso que la producción científica en Informática significa en el total español. Se comprueba que en los últimos 30 años la producción en Informática (14.696 artículos) ha supuesto, de media, el 2,7% del total español. Dicha media esconde una importante mejora. Así, en 1980 los artículos en Informática eran tan solo el 0,4% del total de artículos con autor español. En 1985 se alcanzó por primera vez el 1% y en 1998 el 2%. En la última decena se ha reafirmado la mejora, lográndose el 3% en 2003 y un 4,2% en el año 2010.

4. Organizaciones más significativas

En este apartado se presenta el mapa de las organizaciones donde trabajan los investigadores españoles en Informática. Contando las que tienen al menos 5 artículos en el quinquenio 2006-2010, resultan 82 organizaciones: 56 universidades (8 de ellas privadas), 19 centros públicos de investigación, 2 hospitales y 5 empresas o centros privados de investigación. Se puede afirmar que casi toda la investigación se realiza en instituciones públicas, ya que las 13 organizaciones privadas (universidades, empresas y centros) acumulan menos del 3% de los artículos y citas. Las Universidades realizan la inmensa mayoría de la investigación en Informática en España (más del 90% de los artículos y de las citas corresponden a las 56 seleccionadas), seguidas a gran distancia por los centros públicos de investigación (6,6% de los artículos y 7,9% de las citas).

La **tabla 3** muestra los datos para las 15 primeras organizaciones, 14 universidades públicas y el CSIC (Centro Superior de Investigaciones Científicas), que superan los 200 artículos. La columna "H" muestra el índice de Hirsch [3], que se suele emplear como indicador de la cantidad de artículos más citados (un valor H significa que existen H artículos con al menos H citas). La columna "Esp" indica la especialidad con más artículos: Aplicaciones Interdisciplinares (API), Cibernética (CIB), Hardware y Arquitectura (HAR), Ingeniería y Tecnología del Software (SOF), Inteligencia Artificial (INT), Siste-

Pos	Organización	Tipo	Artíc.	% Artíc.	Citas	% Citas	FI	H	Esp.
1	UNIV POLITECNICA DE CATALUNYA	U	862	10.27	2815	8.57	3.27	17	TEO
2	UNIV POLITECNICA DE VALENCIA	U	628	7.48	2308	7.03	3.68	19	API
3	UNIV GRANADA	U	552	6.58	3121	9.50	5.65	25	INT
4	UNIV POLITECNICA DE MADRID	U	458	5.46	1476	4.49	3.22	17	TEO
5	UNIV COMPLUTENSE DE MADRID	U	393	4.68	1525	4.64	3.88	15	TEO
6	UNIV CARLOS III DE MADRID	U	382	4.55	1049	3.19	2.75	13	TEO
7	CSIC	C	363	4.32	1880	5.73	5.18	19	INT
8	UNIV SEVILLA	U	308	3.67	1104	3.36	3.58	14	TEO
9	UNIV CASTILLA-LA MANCHA	U	302	3.60	1089	3.32	3.61	15	SOF
10	UNIV MALAGA	U	290	3.45	1076	3.28	3.71	14	INT
11	UNIV AUTONOMA DE MADRID	U	284	3.38	1208	3.68	4.25	16	INT
12	UNIV ZARAGOZA	U	244	2.91	1017	3.10	4.17	14	API
13	UNIV AUTONOMA DE BARCELONA	U	220	2.62	915	2.79	4.16	13	INT
14	UNIV PAIS VASCO	U	218	2.60	669	2.04	3.07	12	INT
15	UNIV POMPEU FABRA	U	212	2.53	1156	3.52	5.45	16	INT

Tabla 3. Lista de organizaciones con 200 o más artículos (2006-2010).

mas de Información (SIN), y Teoría y Métodos (TEO).

En la web ya mencionada y que complementa este artículo, se encuentra la lista completa de organizaciones con todos sus datos. Analizando estos datos se puede extraer que la investigación informática española está bastante repartida, con 37 instituciones con más del 1% de los artículos y 34 con un H igual o superior a 10, lo que puede interpretarse como que cuentan con una comunidad de investigación en Informática consolidada en producción e impacto. Entre las 10 primeras organizaciones en producción de artículos se encuentran 9 universidades públicas: una catalana (Politécnica de Catalunya), una valenciana (Politécnica de Valencia), tres andaluzas (Granada, Sevilla y Málaga), tres madrileñas (Politécnica de Madrid, Complutense y Carlos III) y una castellano-manchega (Castilla-La Mancha). Aunque las universidades privadas eran 23 en 2010 (con el 12,2% del total de estudiantes de grado), sólo 8 de ellas cumplen el filtro de los 5 artículos en el quinquenio analizado. La primera privada es la Universidad de Navarra (posición 46, 0,6% de artículos y 0,5% de citas). Le siguen la Oberta de Catalunya (posición 48), la Ramón Llull de Barcelona (posición 53) y la Europea de Madrid (posición 62). Entre los centros públicos de investigación, ocupando la séptima posición, destaca el CSIC con un 4,3% de artículos y 5,7% de citas, con más producción que todos los demás centros públicos juntos. Telefónica I+D es la primera entre las empresas privadas (posición 52) con el 0,4% de los artículos y citas.

Aún tratándose de artículos científicos, el número de empresas y centros privados (solo 5) es excepcionalmente bajo. Estas cifras son un reflejo de que las empresas españolas,

salvo honrosas excepciones, siguen aplicando el principio de "investiguen ellos" (referido a otros países y a las instituciones públicas de España).

Si clasificamos las organizaciones en base a la categoría WOS en que tienen mayor número de artículos (especialidad mayoritaria) se obtiene el siguiente reparto: 27 en Inteligencia Artificial, 24 en Aplicaciones Interdisciplinarias, 17 en Teoría y Métodos, 8 en Sistemas de Información, 4 en Ingeniería y Tecnología del Software, 1 en Hardware y Arquitectura, y 1

en Cibernética. En la figura 1 se muestra el mapa con la localización geográfica de las 82 organizaciones. El tamaño de los círculos es proporcional al número de artículos, mientras que el relleno indica la especialidad mayoritaria en la organización.

5. Análisis por especialidades

El campo de la Informática ha crecido tanto en amplitud que es necesario, cada vez más, realizar una cierta especialización. En el mundo de la investigación esta situación es, si cabe, todavía mayor. Por ello, en el informe

Organización	GLOBAL	INT	CIB	HAR	API	SIN	SOF	TEO
UNIV POLITECNICA DE CATALUNYA	1	2	4	1	2	1	1	1
UNIV POLITECNICA DE VALENCIA	2	4	7	4	1	4	2	2
UNIV GRANADA	3	1	2	10	3	2	7	5
UNIV POLITECNICA DE MADRID	4	5	9	8	5	5	4	4
UNIV COMPLUTENSE DE MADRID	5	10	3	2	6	14	5	3
UNIV CARLOS III DE MADRID	6	6	18	3	9	3	12	7
CSIC	7	3	13	7	4	13	18	12
UNIV SEVILLA	8	16		5	14	17	8	6
UNIV CASTILLA-LA MANCHA	9	15		13	12	8	3	9
UNIV MALAGA	10	9	6	9	21	7	6	8
UNIV AUTONOMA DE MADRID	11	7	5	12	18	6	10	10
UNIV ZARAGOZA	12	25	15	16	10	9	11	15
UNIV AUTONOMA DE BARCELONA	13	13		32	19	16	22	13
UNIV PAIS VASCO	14	11	8	17	20	18	32	14
UNIV POMPEU FABRA	15	8	12	26	16	20	21	16
UNIV VALENCIA	16	19	11	28	7	33	23	32
UNIV OVIEDO	17	17			11	31	14	25
UNIV BARCELONA	18	20	10	38	8	25	27	28
UNIV ROVIRA I VIRGILI	19	29		14	37	10	26	11
UNIV ALICANTE	20	22	1	42	25	12	13	18
UNIV VIGO	21	26		36	13	19	9	20
UNIV VALLADOLID	22	23	16	30	17	15	25	17
UNIV MURCIA	23	31		6	32	11	15	24

Tabla 4. Posiciones de las organizaciones por especialidades (2006-2010).

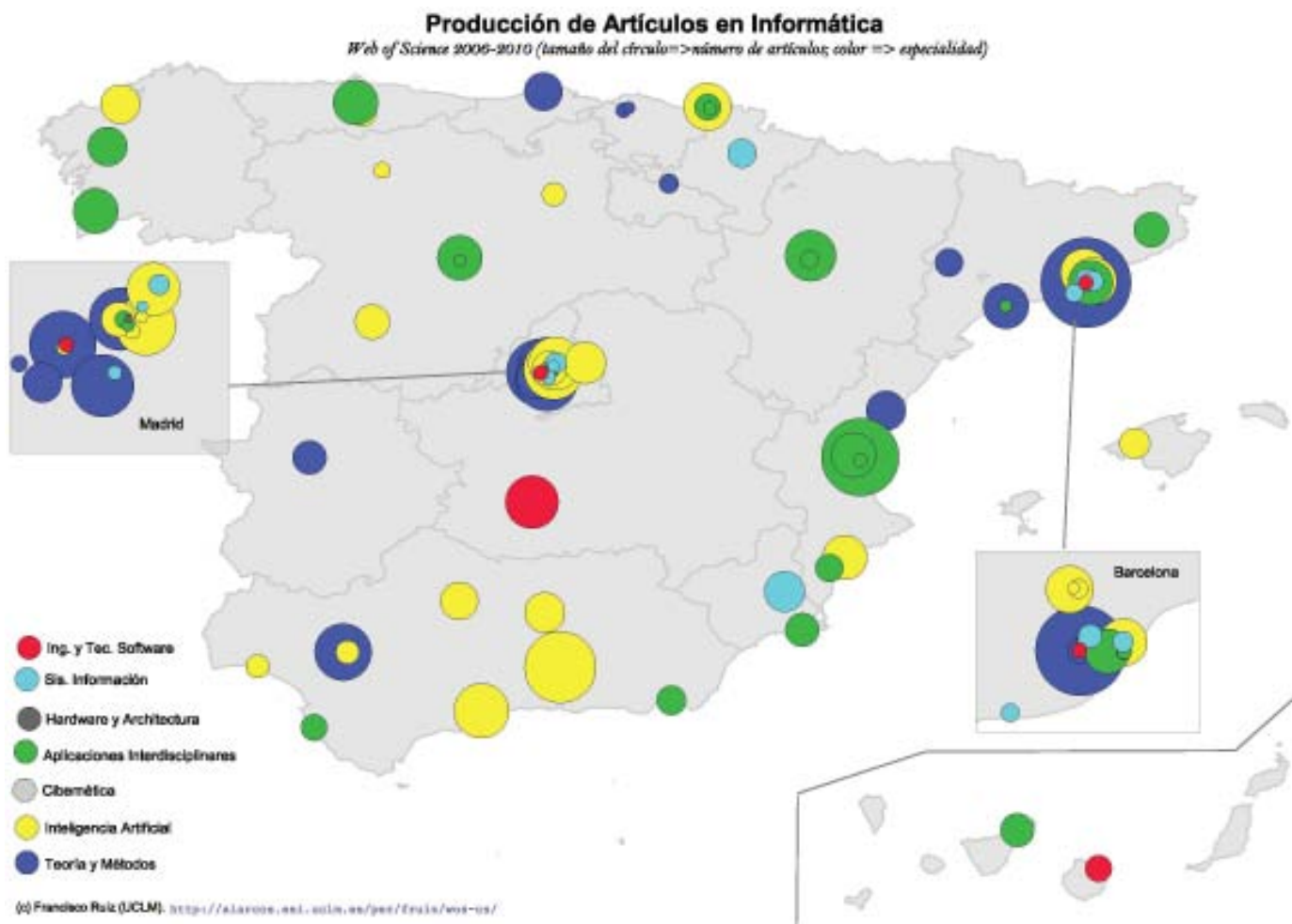


Figura 1. Número de artículos (tamaño del círculo) y especialidad mayoritaria (relleno).

completo disponible en la web se incluye información detallada de los principales actores, a nivel de organizaciones, en cada una de las siete especialidades. Por problemas de espacio en este artículo solo es factible mostrar algunos de los datos. En la **tabla 4** se muestra un resumen de las posiciones que ocupan, en el global de Informática y en cada especialidad, las principales organizaciones en cuanto a cifras de artículos. Se han marcado en **negrita y fondo resaltado** las tres primeras posiciones y solo en **negrita** los puestos del 4 al 10. En los subapartados se incluye un breve resumen de los resultados obtenidos para cada especialidad.

5.1. Aplicaciones Interdisciplinarias (API)

En esta especialidad, centrada en la aplicación de la Informática a otras disciplinas, las tres primeras posiciones en número de artículos están ocupadas por las universidades **Politécnica de Valencia (10,9%)**, **Politécnica de Catalunya (9,1%)** y **Granada (6,1%)**. Hasta 6 organizaciones cuentan

con más de un centenar de artículos. Los índices H más altos, todos con 14, corresponden a las universidades **Politécnica de Valencia**, **Granada** y **Santiago de Compostela**, junto con el CSIC.

5.2. Cibernetica (CIB)

Esta categoría es la de menor producción científica, seguramente por el menor número de investigadores dedicados a ella. Por número de artículos las primeras instituciones son las universidades de **Alicante (12,9%)**, **Granada (8,1%)** y **Complutense (8,1%)**. El índice H más alto corresponde a la **Universidad Politécnica de Catalunya (H=6)**.

5.3. Hardware y Arquitectura (HAR)

En esta categoría existe un importante liderazgo por parte de la **Universidad Politécnica de Catalunya (20,9%** de los artículos y **25,8%** de las citas), siendo la única que supera el centenar de artículos, siguiéndole de lejos las universidades **Complutense (8,5%)** y **Carlos III de Madrid (8,0%)**. Los índices H más altos los ostentan las universidades

Politécnica de Catalunya (11), **Complutense (9)** y **Politécnica de Valencia (8)**.

5.4. Ingeniería y Tecnología del Software (SOF)

Por número de artículos, las tres primeras instituciones y las únicas que superan el centenar, son las universidades **Politécnica de Catalunya (10,2%)**, **Politécnica de Valencia (9,5%)** y **Castilla-La Mancha (7,7%)**. Los índices H más elevados corresponden a las universidades **Politécnica de Catalunya (10)**, **Castilla-La Mancha (8)** y **Complutense (8)**.

En casos como esta categoría pueden resultar llamativas las importantes diferencias en el factor de impacto entre unas organizaciones y otras. Obviamente, en entidades con un bajo número de artículos es más fácil que se produzcan desviaciones grandes respecto de la media. En estos casos puede influir mucho la temática de unos pocos artículos publicados en revistas compartidas con otras disciplinas y que suelen tener cifras bastante más altas de citas y de impacto. Ejemplo de ello es

que los tres artículos más citados, entre los más de 8.300 del global de Informática correspondientes al quinquenio 2006-2010, están publicados en la revista "Bioinformatics", y el primero cuenta con 646 citas, un impacto "astronómico" para lo habitual en Informática (solo 242 artículos, el 2,9%, tienen 20 o más citas).

5.5. Inteligencia Artificial (INT)

Por cifras de artículos la lista la encabezan las universidades de Granada (10,5%) y Politécnica de Catalunya (6,5%), seguidas del CSIC (6,0%). Otras dos universidades, las politécnicas de Valencia y de Madrid, superan el centenar de artículos. Las organizaciones con valores más altos del índice H son la Universidad de Granada (22), el CSIC (15) y las universidades de Jaén y Politécnica de Valencia, ambas con H=14.

5.6. Sistemas de Información (SIN)

Esta categoría la lidera de manera holgada la Universidad Politécnica de Catalunya con el 12,3% de los artículos, seguida por las también universidades de Granada (6,1%) y Carlos III de Madrid (6,1%). Los índices H más elevados corresponden a las universidades de Granada (12), Politécnica de Catalunya (11) y Castilla-La Mancha (9).

5.7. Teoría y Métodos (TEO)

Las principales organizaciones en cifras de artículos son las universidades Politécnica de Catalunya (11,6%), Politécnica de Valencia (7,3%) y Complutense de Madrid (6,2%). Los valores más elevados del índice H corresponden a las universidades de Granada (13), Complutense de Madrid (11) y Politécnica de Catalunya (11).

6. Conclusiones

Se ha presentado un resumen de un informe elaborado para obtener una visión de la producción científica española en la disciplina de Informática. Para ello se han empleado los datos de artículos y citas en el periodo 2006-2010 proporcionados por el "Web of Science" (antiguo ISI). Otros indicadores utilizados han sido el factor de impacto (ratio entre número de citas y artículos) e índice H. El estudio se ha desglosado para las siete especialidades (categorías) en que WOS divide la Informática ("Computer Science"). Además de analizar la situación a nivel general del estado español, también se ha revisado la situación para cada una de las 82 organizaciones que tienen una producción media de un artículo al año.

Algunas conclusiones, extraídas del análisis de los resultados, son:

- España ocupa la novena posición en el ranking mundial con el 4,7% de la producción de artículos en Informática. Por especialidades, oscila entre el 5,6% de Inteligencia Artifi-

cial y el 3,6% de Sistemas de Información.

- La evolución en los últimos 10 años ha sido especialmente favorable ya que se encuentra entre los únicos cuatro países, y el único occidental, que han mejorado su peso mundial en más de 2 puntos porcentuales.

- A nivel interno de España y comparando con las demás disciplinas, se obtiene que Informática es la quinta (de 37 disciplinas) en la que España tiene más peso en el total mundial, estando nuestro 4,7% por encima de otras disciplinas de ingeniería relacionadas, como Automática y Robótica (4,0%), Telecomunicaciones (3,4%), o Ingeniería Eléctrica y Electrónica (3,2%).

- De los 8.395 artículos en Informática en el periodo 2006-2010 que cuentan con algún autor español, el 33,8% se escribieron en colaboración con autores de otros países destacando, en primer lugar, Estados Unidos, seguido de Inglaterra. El 43,2% de dichos artículos se publicaron en revistas "puras" de Informática, es decir, que no están indexadas en paralelo en otras disciplinas.

- La evolución del número de artículos en términos absolutos ha sido muy positiva, pasando de solo 13 en 1981 a 100 en 1990, 493 en 2000 y 1.820 en 2010. En términos relativos, dichos artículos han supuesto cada vez un porcentaje mayor del total de artículos españoles en todas las disciplinas: 0,4% en 1981, 1,1% en 1990, 2,2% en 2000 y 4,2% en 2010.

- La producción científica está bastante repartida, contando con 82 organizaciones españolas que tienen 5 o más artículos publicados en el quinquenio analizado. Destacan de manera considerable las 48 universidades públicas, que suponen el 89,5% de los artículos y el 90,7% de las citas.

- Las cuatro organizaciones que superan el 5% del total de artículos son las universidades Politécnica de Catalunya, Politécnica de Valencia, Granada y Politécnica de Madrid. Entre las 10 primeras organizaciones se encuentran 9 universidades públicas, una de Cataluña, una de la Comunidad Valenciana, tres de Andalucía, tres de Madrid, y una de Castilla-La Mancha.

- Usando el índice H, los impactos más significativos corresponde a la Universidad de Granada (H=25), seguida de la Politécnica de Valencia y el CSIC, ambos con H=19.

- Entre los centros públicos de investigación destaca el CSIC con el 4,3% del total de artículos. Solo 8 universidades privadas aparecen en la lista, siendo la primera la de Navarra (posición 46 y 0,5% de los artículos). Entre las instituciones privadas, solo superan los 10 artículos Telefónica I+D y el centro de I+D de Yahoo! en Barcelona, aunque ambos en posiciones posteriores a la 50 en el ranking.

- Existe una cierta diferenciación de las organizaciones según las especialidades mayoritarias en ellas. Las más frecuentes son Aplicaciones Interdisciplinarias (con 27 organizaciones), Inteligencia Artificial (24) y Teoría y Métodos (17). Sistemas de Información es

mayoritaria en 8 organizaciones, e Ingeniería y Tecnología del Software en 4. Las categorías de Hardware y Arquitectura y de Cibernética solo tienen mayoría en sendas organizaciones.

- Las organizaciones que aparecen en alguna de las tres primeras posiciones en una o varias de las siete especialidades son: Universidad Politécnica de Catalunya (en 6), Universidad de Granada (en 4), Universidad Politécnica de Valencia (en 3), Universidad Complutense de Madrid (en 3), Universidad Carlos III de Madrid (en 2), CSIC (en 1), Universidad de Castilla-La Mancha (en 1) y Universidad de Alicante (en 1). La Universidad Politécnica de Madrid, aunque ocupa la cuarta posición en el ranking global de Informática, no supera esa misma posición en los rankings de las siete especialidades.

Referencias

[1] Thompson-Reuters. "Web of Science". <<http://science.thomsonreuters.com/es/productos/wos/>>.

[2] Thompson-Reuters. "Scope Notes. 2011 Science Citation Index". <http://science.thomsonreuters.com/mjl/scope/scope_scie/>.

[3] J. E. Hirsch. "An index to quantify an individual's scientific research output". *Proc Natl Acad Sci USA*. 102(46), pp. 16569-16572 (2005).

Julio Javier Castillo, Diego Javier Serrano,
Marina Elizabeth Cárdenas

Laboratorio de Investigación de Software MsLabs, Dpto. Ing. en
Sistemas de Información, Facultad Regional Córdoba - Universidad
Tecnológica Nacional (Argentina)

<jotacastillo@gmail.com>,
<diegojserrano@gmail.com>,
<ing.marinacardenas@gmail.com>

En este problema se nos presenta un laberinto como una matriz de números unos y ceros, donde los caminos son representados con conjuntos de números 1 adyacentes en la matriz. El objetivo entonces es encontrar un camino de números 1 que inicie en la esquina superior izquierda (1,1) y llegue hasta la esquina inferior derecha (n,n). Adicionalmente, se conoce que en todos los casos de prueba existirá un único camino lo cual simplifica mucho el problema, ya que la existencia de múltiples caminos puede obligarnos a identificar todos o el más corto. Por otro lado, al indicar que en la solución no se pasa dos veces por el mismo casillero evita que un ciclo en el camino pueda provocar que nuestro programa ingrese en un ciclo infinito al recorrer el laberinto.

La solución aquí planteada muestra la implementación del algoritmo de búsqueda en profundidad (DFS, *Depth first search*) recorriendo la matriz como si se tratara de un grafo en el que los números 1 corresponden a nodos y los arcos existen entre aquellos números 1 adyacentes. Se prefirió la búsqueda en profundidad en lugar de la búsqueda en amplitud en virtud de que existe un único camino que soluciona el laberinto, por lo tanto al encontrar ese camino se puede interrumpir la búsqueda inmediatamente.

La búsqueda está implementada en el método *BuscarCamino*, que de manera recursiva recorre la matriz desde una posición inicial (parámetro actual) buscando el primer número 1 que encuentre entre todas sus posiciones adyacentes. Cuando se encuentra un vecino que se puede recorrer se continúa buscando desde ahí. Si ningún vecino puede ser recorrido el método retorna "false". De esta forma cuando se encuentra un camino candidato se lo recorre hasta que finalice, ya sea porque se interrumpe, porque llega a un borde de la matriz o porque llega al objetivo. Cuando finaliza sin llegar al objetivo se produce el *backtracking*, esto provoca que se recorra el camino hacia atrás a un casillero por vez (a través de la desapilación de llamadas recursivas) y se continúe buscando nuevos vecinos que se puedan recorrer.

Para registrar el camino completo en cada llamada recursiva al método *BuscarCamino* se almacena en una pila (parámetro recorrido) la posición que está procesando. Cuando el método finaliza sin encontrar un camino desde una posición dada, desapila la misma. Si el método finaliza encontrando la posición de la salida del laberinto retorna "trae" pero sin desapilar la posición actual. Al recibir un retorno "trae", todas las llamadas recursivas apiladas finalizan de la misma forma, retornando "trae" sin desapilar las posiciones. De esta manera al finalizar la primera llamada a *BuscarCamino* la pila queda conteniendo todas las posiciones recorridas desde el inicio del laberinto hasta la salida del mismo.

Ya que el problema enuncia que siempre existirá una solución el algoritmo no realiza ningún chequeo para determinar si esa solución existe, sino que simplemente se asume que existe. Sin embargo, si un laberinto no poseyera solución, el método finaliza recorriendo hacia atrás hasta volver al inicio del laberinto, dejando la pila con el recorrido vacío, indicando así la inexistencia del camino solución.

Cuando se recorren los vecinos desde cada posición se evalúan los mismos en un orden arbitrario, incluso visitando la posición anterior en el camino, lo cual podría generar un ciclo infinito. Por otro lado si existe un ciclo en un camino, debemos eliminarlo de la solución pues se requiere que un

El Problema del Laberinto Cuadrado

El enunciado de este problema apareció en el número 214 de *Novática* (noviembre-diciembre 2011, p.75)

camino no pase más de una vez por el mismo lugar. Para ello, mientras se recorre un camino "hacia adelante" haciendo nuevas llamadas recursivas, se modifica la matriz asignando un 2 en la posición actual. Por otra parte, al retornar sin encontrar la solución se vuelve al valor original de 1. Esto nos permite no tener que acceder más de una vez a la misma posición pues sólo se recorre al encontrar un número 1 (cualquier valor podría haber servido, incluso se podría haber asignado 0 eliminando los caminos que de todas formas no se vuelven a recorrer).

Una variante para no modificar el laberinto es verificar si cada vecino que se quiere recorrer no existe previamente en la pila que almacena el recorrido. Conceptualmente es lo más adecuado, pero una búsqueda en la pila nos agrega una operación lineal por cada vecino que se intenta visitar incrementando la complejidad temporal del algoritmo. Por otra parte, se optó por modificar la posición actual en la matriz ya que es una operación de tiempo constante y que no afecta la complejidad algorítmica.

```
import java.util.Scanner;
import java.util.Stack;

class Punto {
    public int x, y;

    public Punto(int x, int y)
    {
        this.x = x; this.y = y;
    }

    public Punto add(Punto offset)
    {
        return new Punto(x + offset.x, y + offset.y);
    }
}

public class Laberinto {
    static int n;
    static short [][]tablero = new short[9][9];
    static Punto []vecinos = { new Punto(-1, 0), new
    Punto(0, -1), new Punto(1, 0), new Punto(0, 1) };

    public static void main(String[] args) {
        Scanner sc = new Scanner(System.in);

        int c = sc.nextInt();
        while (c-- > 0)
        {
            // Carga de datos
            n = sc.nextInt();
            for (int i = 1; i <= n; i++)
                for (int j = 1; j <= n; j++)
                    tablero[i][j] = sc.nextShort();

            //Búsqueda del camino
            Stack<Punto> recorrido = new Stack<>();
            BuscarCamino(recorrido, new Punto(1,1));

            //Presentación de resultados
            boolean primero = true;
            for(Punto p:recorrido)
            {
```

```

        if (!primero)
System.out.print(«,»);
        primero = false;
        System.out.print(«(« + (p.y) + «,»
+ (p.x) + ')');
    }
    System.out.println();
}
}

private static boolean BuscarCamino(Stack<Punto>
recorrido, Punto actual) {
    if (actual.x >= 0 && actual.x <= n && actual.y
>= 0 && actual.y <= n && tablero[actual.y][actual.x]
== 1)
    {
        recorrido.push(actual);
        tablero[actual.y][actual.x] = 2;
        if (actual.x == n && actual.y == n)
return true;
        for(Punto v: vecinos){
            if (BuscarCamino(recorrido,
actual.add(v))
                return true;
        }
        recorrido.pop();
        tablero[actual.y][actual.x] = 1;
    }
    return false;
}
}

```

El problema del *Superbowling*

Julio Javier Castillo, Diego Javier Serrano, Marina Elizabeth Cárdenas
Laboratorio de Investigación de Software MsLabs, Dpto. Ing. en Sistemas de Información, Facultad Regional Córdoba - Universidad Tecnológica Nacional (Argentina)

<jotacastillo@gmail.com>, <diegojserrano@gmail.com>, <ing.marinacardenas@gmail.com>

Este es el enunciado del problema F de los planteados en la Tercera Competencia de Programación de la Facultad Regional de Córdoba (Universidad Tecnológica Nacional, Argentina) UTN-FRC celebrada el 29 de noviembre de 2011.

Nivel del problema: Sencillo

En el juego de *bowling* se debe derribar un conjunto de piezas de madera llamadas bolos o pinos. Los pinos se distribuyen en 4 hileras formando un triángulo equilátero según indica la **figura 1**.

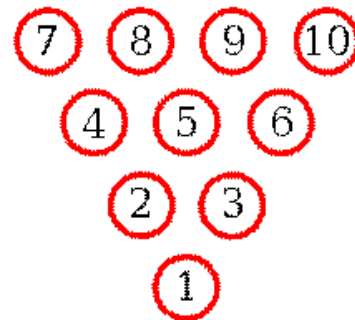


Figura 1. Distribución de los pinos en el juego de *bowling*.

En este problema debe suponerse la creación de una estructura similar que albergue una mayor cantidad de pinos.

Entrada

La entrada comienza con una línea conteniendo un número entero C indicando la cantidad de casos de pruebas. A continuación se reciben C líneas con un número entero N en cada una.

Condiciones:
 $0 < C < 100000$
 $0 < N \leq 10^9$

Salida

Por cada caso de prueba se debe imprimir un número que indique la cantidad de hileras necesarias para armar un triángulo de *bowling* que contenga al menos N pinos.

Ejemplo

Entrada	Salida
3	4
10	3
5	44721
1.000.000.000	

Formación acreditada para profesionales TIC

ATI acaba de anunciar un programa de Formación Acreditada para Profesionales TIC y Preparatoria para la Obtención de Certificados Emitidos por Organismos Oficiales y Reconocidos.

A través de este programa se imparten cursos sobre certificaciones profesionales promovidos por el Plan Avanza 2 Formación que tienen precios ajustados para asociados, y disfrutan de una bonificación en el precio de la matrícula para los alumnos que cumplan los requisitos del programa y se presenten a la obtención de la certificación correspondiente.

Estos cursos están dirigidos a trabajadores en activo pertenecientes a PYMES y trabajadores autónomos que realicen su labor profesional en el ámbito de las Tecnologías de la Información y la Comunicación (TIC), o a aquellos para quienes la formación recibida les permita desarrollar puestos de trabajo relacionados con el sector TIC. Tendrán acceso prioritario los trabajadores en activo de las siguientes regiones de convergencia de la U.E.: Castilla-La Mancha, Andalucía, Extremadura y Galicia. Más información en: <<http://www.ati.es/spip.php?article2011>>.

Soporte en línea de ATI

Con la intención de ofrecer una mejor atención al socio e interesados en la Asociación, se ha abierto en la web de ATI <<http://www.ati.es/>> un nuevo servicio de soporte en línea a través del cual se quieren canalizar todas las consultas (preguntas, sugerencias, incidencias...) de los interesados de una manera interactiva.

Los socios de ATI disponen de acceso al área de consultas a partir de su usuario y contraseña de acceso al correo electrónico de [ati.es](mailto:ati@ati.es) (atinet.es) mientras que quienes no son socios disponen de un formulario donde introducir su consulta así como el correo electrónico donde desean recibir su respuesta.

Programación de Novática

Por acuerdo del Consejo Editorial de **Novática**, los temas y editores invitados de las monografías restantes de 2012 serán, salvo causas de fuerza mayor o imprevistos, los siguientes:

Nº 216 (marzo-abril 2012): "Informática y cultura". Editores invitados: **Karim Gherab Martín** (Centro de Ciencias Humanas y Sociales, Consejo Superior de Investigaciones Científicas) y **Luisana Rodríguez Castellanos** (Ingeniera de Proyectos Tecnológicos y Culturales). Este número se publicará **exclusivamente en versión digital**.

Nº 217 (mayo-junio 2012): "Privacidad y nuevas tecnologías". Editores invitados: **Gemma Galdon Clavell** (Universitat Oberta de Catalunya) y **Gus Hosein** (London School of Economics; Privacy International). Este número se publicará tanto en versión impresa como en versión digital.

Nº 218 (julio-agosto 2012): "Sistemas multiagente". Editores invitados: **Jordi Sabater Mir** (Instituto de Investigación en Inteligencia Artificial, IIIA) y **Vicente Julián Inglada** (Universidad Politécnica de Valencia). Este número se publicará **exclusivamente en versión digital**.

Nº 219 (septiembre-octubre 2012): "Redes sociales y multicanalidad". Editora invitada: **Encarna Quesada Ruiz** (Responsable de Comunicación de Virati Comunicación Interactiva). Este número se publicará tanto en versión impresa como en versión digital.

Nº 220 (noviembre-diciembre 2012): "Experiencias y retos en IPv6". Editores invitados: **Jordi Domingo Pascual** (Universitat Politècnica de Catalunya), **Carlos Ralli Ucendo** (Telefónica I+D; Observatorio IPv6 en España) y **Eduardo Jacob Taquet** (Universidad del País Vasco / Euskal Herriko Unibertsitatea). Este número se publicará **exclusivamente en versión digital**.

Socios institucionales de ati

Según los Estatutos de ATI, pueden ser socios institucionales de nuestra asociación "las personas jurídicas, públicas y privadas, que lo soliciten a la Junta Directiva General y sean aceptados como tales por la misma".

Mediante esta figura asociativa, todos los profesionales y directivos informáticos de los socios institucionales pueden gozar de los beneficios de participar en las actividades de ATI, en especial congresos, jornadas, cursos, conferencias, charlas, etc. Asimismo los socios institucionales pueden acceder en condiciones especiales a servicios ofrecidos por la asociación tales como Bolsa de Trabajo, cursos a medida, *mailings*, publicidad en Novática, servicio ATInet, etc.

Para más información dirigirse a <info@ati.es> o a cualquiera de las sedes de ATI. En la actualidad son socios institucionales de ATI las siguientes empresas y entidades:

AGENCIA DE INFOR. Y COMUN. COMUNIDAD DE MADRID
 AGROSEGURO, S.A.
 AIGÜES TER LLOBREGAT
 ALC ORGANIZACIÓN Y SISTEMAS,S.L.
 ALMIRALL, S.A.
 AVANTTIC, CONSULTORÍA TECNOLÓGICA, S.L.
 CENTRO DE ESTUDIOS VELAZQUEZ S.A. (C.E. Adams)
 CETICSA, CONSULTORIA Y FORMACIÓN
 CONSULTORES SAYMA, S.A.
 COSTAISA, S.A
 DEPARTAMENT D'ENSENYAMENT DE LA GENERALITAT
 ELOGOS, S. L.
 EPISER, S.L.
 ESPECIALIDADES ELÉCTRICAS, S.A. (ESPELSA)
 ESTEVE QUÍMICA, S.A.
 FUNDACIÓ BARCELONA MEDIA - UNIVERSITAT POMPEU FABRA
 FUNDACIÓ CATALANA DE L'ESPLAI
 FUNDACIÓ PRIVADA ESCOLES UNIVERSITÀRIES GIMBERNAT
 IIR ESPAÑA
 IN2
 INFORMÁTICA Y COMUNICACIONES AVANZADAS, S.L.
 INSTITUT D'ESTUDIS CATALANS
 INSTITUT MUNICIPAL D'INFORMÀTICA
 INVERGAMING GRUP
 KRITER SOFTWARE, S.L.
 NETMIND, S.L.
 ONDATA INTERNATIONAL, S.L.
 PRACTIA CONSULTING, S.L.
 QRP MANAGEMENT METHODS INTERNATIONAL
 RCM SOFTWARE, S.L.
 SADIÉL, S.A.
 SCATI LABS, S.A.
 SISTEMAS TÉCNICOS LOTERIAS ESTADO (STL)
 SOCIEDAD DE REDES ELECTRÓNICAS Y SERVICIOS, S.A.
 SQS, S.A
 TRAINING & ENTERPRISE RESOURCES
 T-SYSTEMS ITC Services España S.A.
 UNIVERSIDAD ANTONIO DE NEBRJIA
 UNIVERSITAT DE GIRONA
 UNIVERSITAT OBERTA DE CATALUNYA

Apellidos Nombre
 Empresa/Organismo CIF/NIF
 Domicilio
 Ciudad Provincia
 Código Postal País
 Teléfono Fax Correo elec.

Nota: Rellenar los siguientes datos solamente si la dirección de envío es diferente de la anterior.

Domicilio para envíos
 Ciudad Provincia
 Código Postal País

Tarifas 2012. Deseo suscribirme a Novática (6 numeros al año) en las siguientes condiciones (marcar con X la opción deseada y, en su caso, la cantidad de suscripciones solicitadas):

*** España**

- 1 suscripción: 62,00 € (+4% IVA)
- _ suscripciones: 58,00 € cada una (+4% IVA)

*** Otros países de la Unión Europea y Marruecos**

- 1 suscripción: 75,00 €
- _ suscripciones: 70,00 € cada una

*** Resto del mundo**

- 1 suscripción: 82,00 €
- _ suscripciones: 76,00 €

Abonaré el importe:

- Con domiciliación de cobro por entidad bancaria (deberá rellenar los datos bancarios abajo solicitados)
- Talón adjunto
- Transferencia bancaria a la cta. 3025-0004-30-1500001500, Caja de Ingenieros, Calle Buen Pastor 5, 08018, Barcelona, (España)

Fecha Firma

De conformidad con la LO 15/99 de Protección de Datos de carácter personal le informamos que los datos que usted nos facilite serán incorporados a un fichero propiedad de Asociación de Técnicos de Informática para poder gestionar su suscripción a nuestra revista y hacerle llegar los ejemplares correspondientes. Si usted desea acceder, rectificar, cancelar u oponerse al tratamiento de sus datos puede dirigirse por escrito a secregen@ati.es.

DATOS BANCARIOS PARA DOMICILIACION

Banco/Caja.....

CÓDIGO CUENTA CLIENTE			
ENTIDAD	OFICINA	D.C.	NÚMERO DE CUENTA

NV 215



AUTORIZACIÓN DE COBRO

Le rogamos escriba otra vez los datos bancarios. ATI se encarga de su envío al Banco o Caja.

Banco/Caja.....

CÓDIGO CUENTA CLIENTE			
ENTIDAD	OFICINA	D.C.	NÚMERO DE CUENTA

Ruego a Uds. se sirvan tomar nota de que, hasta nueva orden mía en contra, deberán adeudar en mi cuenta arriba indicada los recibos que a nombre de D./Dª le sean presentados por la Asociación de Técnicos de Informática (ATI), en concepto de suscripción a la revista Novática.

Fecha..... Firma



Hoja de solicitud de inscripción en ATI (2012) (Asociación de Técnicos de Informática)

NV 215

Todos los datos son obligatorios a menos que se indique otra cosa

Una vez cumplimentada esta hoja, se ruega enviarla por correo electrónico a secregen@ati.es, o por fax al 93 4127713, o por correo postal a ATI, Vía Laietana 46, ppal. 1ª, 08003 Barcelona

www.ati.es

► Solicito inscribirme como: Socio de número (81€)* / Socio junior (23€)* / Socio jubilado (26€)* / Socio adherido (55€)*

(Para inscribirse como socio estudiante se ruega utilizar la hoja de inscripción específica disponible en <http://www.ati.es/estudiantes>

- ver en la siguiente página información detallada sobre ATI y los diferentes tipos de socios)

* **Nota importante:** la cuota cubre el año natural, de 1 de enero a 31 de diciembre. Las inscripciones a socios de número realizadas de 1 de julio a 31 de octubre tienen una reducción de cuota del 50% y todas las cuotas son gratuitas si se realizan del 1 de noviembre al 31 de diciembre. En este último caso, si se desea acceder a descuentos en servicios ofrecidos por terceros no se aplicarán reducciones a la cuota anual de asociado, que deberá abonarse en su totalidad.

- Datos personales del solicitante

Apellidos		
Nombre		
Domicilio	Nº	Piso
Localidad	Código Postal	
Provincia	Teléfono	
Dirección de correo electrónico ¹		
Fecha de nacimiento	DNI	

- Datos de la empresa o entidad donde trabaja (si es autónomo indíquelo en el campo "Empresa o entidad")

Empresa o entidad	Sector
Puesto actual	Depto.
Dirección	Nº
Localidad	Código Postal
Provincia	Teléfono

- Domiciliación de la cuota anual (ATI se encarga de su envío al banco o caja)

Nombre de la entidad bancaria: _____

Código de entidad	Oficina	D.C.	Cuenta

- Datos complementarios (si necesita más espacio para estos datos continúe en otra hoja)

Títulos superiores o medios que posee y centros otorgantes:

.....

Resumen de experiencias profesionales:

.....

Número de años de experiencia profesional informática:

- Presentado por los Socios de número (**)

(**) Esta información no es necesaria para solicitar inscribirse como socio junior, estudiante o adherido; para inscribirse como socio de número o jubilado, si el solicitante no conoce a ningún socio de número que pueda presentarle, la Secretaría General de ATI le contactará para determinar otra forma fehaciente de acreditar su profesionalidad.

1) Apellidos y Nombre Nº de socio Fecha .../.../..... Firma

2) Apellidos y Nombre Nº de socio Fecha .../.../..... Firma

Firma del solicitante

Fecha _____

Mediante su firma el solicitante declara que todos los datos incluidos en esta solicitud son ciertos.

Nota sobre protección de datos de carácter personal: De conformidad con la LO 15/99 de Protección de Datos de Carácter Personal, le informamos de que los datos que usted nos facilite serán incorporados a un fichero propiedad de Asociación de Técnicos de Informática (ATI) para poder disfrutar de los servicios que su condición de socio le confiere, así como para enviarle información acerca de nuevos servicios, ofertas y cursos que ATI ofrezca y puedan resultar de su interés. Sus datos podrán ser comunicados a aquellas instituciones, sociedades u organismos, con los que ATI mantenga acuerdos de colaboración, relacionados con el sector de los seguros, la banca y la formación para el envío de información comercial. Si usted desea acceder, rectificar, cancelar u oponerse al tratamiento de sus datos puede dirigirse por escrito a secregen@ati.es.

No deseo recibir información comercial de ATI ni de terceras entidades colaboradoras de ATI.

No deseo recibir información comercial de terceras entidades colaboradoras de ATI.

No autorizo la comunicación de mis datos a terceras entidades colaboradoras de ATI.

¹ Una vez validados por la Secretaría de ATI la hoja de inscripción y los documentos requeridos, y aceptada su solicitud, Vd. recibirá en esta dirección de correo la información sobre el procedimiento para poder utilizar todos los servicios de la red ATINET (ver reverso).



Una asociación abierta a todos los informáticos

Una asociación útil a sus socios, útil a la Sociedad

Creada en 1967, **ATI (Asociación de Técnicos de Informática)** es la asociación profesional más numerosa, activa y antigua de las existentes en el Sector Informático español, con sedes en Barcelona (sede general), Madrid, Valencia y Zaragoza. Cuenta con 4.000 socios, que ejercen sus funciones como profesionales informáticos en empresas o Administraciones Públicas, o como autónomos.

ATI, que está abierta a todos profesionales informáticos independientemente de su titulación, representa oficialmente a los informáticos de nuestro país en Europa (a través de CEPIS, entidad que coordina a asociaciones que representan a más de 400.000 profesionales informáticos de 32 países europeos) y en todo el mundo (a través de IFIP, entidad promovida por la UNESCO para coordinar trabajos de Universidades y Centros de Investigación), y pertenece a la CLEI (Centro Latinoamericano de Estudios en Informática). ATI tiene también un acuerdo de colaboración con ACM (*Association for Computing Machinery*).

En el plano interno tiene establecidos acuerdos de colaboración o vinculación con Ada Spain, ASTIC (Asociación Profesional del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado), Hispalinux, AI2 (Asociación de Ingenieros en Informática), Colegios de Ingenierías Informáticas de Cataluña y con RITSI (Reunión de Estudiantes de Ingenierías Técnicas y Superiores de Informática).

Tipos de socio

- √ Socios de número: deben acreditar un mínimo de tres años de experiencia profesional informática (o dos años si se posee un título de grado superior o medio), o *bien* poseer un título de grado superior o medio relacionado con las Tecnologías de Información, o *bien* haber desarrollado estudios, trabajos, o investigaciones relevantes sobre dichas tecnologías
- √ Socios estudiantes: deben acreditar estar matriculados en un centro docente cuya titulación dé acceso a la condición de Socio de Número (hoja específica de inscripción para socios estudiantes disponible en <http://www.ati.es/estudiantes>)
- √ Socios junior: la condición de socio junior de un profesional informático será válida hasta el día final del año en que cumpla los 30 años de edad
- √ Socios jubilados (Aula de Experiencia): socios de ATI que, al jubilarse y cesar su actividad laboral, deciden continuar perteneciendo a ATI colaborando con su experiencia con la asociación
- √ Socios adheridos: profesionales informáticos que no cumplan las condiciones para ser Socios de Número o también personas que, no siendo profesionales informáticos, quieran participar en las actividades de ATI
- √ Socios institucionales: personas jurídicas, de carácter público o privado, que quieran participar en las actividades de ATI (para más información sobre esta modalidad se ruega ponerse en contacto con la sede general de ATI)

¿Qué servicios ofrece ATI a sus socios?

Mediante el pago de una cuota anual, los socios de ATI pueden disfrutar de la siguiente gama de servicios:

- √ Formación Permanente
 - Cursos, Jornadas Técnicas, Mesas Redondas, Seminarios,
 - Conferencias, Congresos
 - Secciones Técnicas y Grupos de Trabajo sobre diversos temas
 - Intercambios con Asociaciones Profesionales de todo el mundo
- √ Servicios de información
 - Revistas bimestrales **Novática** (decana de la prensa informática española), **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software) y **UPGRADE**, publicación digital editada en lengua inglesa por **Novática** en nombre de CEPIS
 - Red asociativa **ATInet** (IntrATInet, acceso básico gratuito a Internet, correo electrónico con dirección permanente, listas de distribución generales y especializadas, foros, blogs, página personal, ...)
 - Servidor web <http://www.ati.es>, pionero de los webs asociativos españoles
- √ Servicios profesionales
 - Asesoramiento profesional y legal
 - Peritajes, diagnósticos y certificaciones
 - Bolsa de Trabajo
 - Emisión en España del certificado profesional europeo EUCIP (*European Certification of Informatics Professionals*)
 - Emisión en España del certificado ECDL (*European Computer Driving License*) para usuarios
- √ Servicios personales
 - Los que ofrece la Mutua de los Ingenieros (Seguros, Fondo de pensiones, Servicios Médicos)
 - Los que ofrece la Caja de Ingenieros (gozar de las ventajas de ser socio de esta caja cooperativa)
 - Promociones y ofertas comerciales

¿Dónde está ATI?

- √ **Sede General y Capítulo de Catalunya** - Vía Laietana 46 ppal. 1ª, 08003 Barcelona - Tlf. 93 4125235; fax 93 4127713 / <secregen@ati.es>
- √ **Capítulo de Andalucía** - <secreand@ati.es>
- √ **Capítulo de Aragón** - Lagasca 9, 3-B, 50006 Zaragoza - Tlf./fax 976 235181 / <secreara@ati.es>
- √ **Capítulo de Galicia** - <secregal@ati.es>
- √ **Capítulo de Madrid** - Padilla 66, 3º dcha., 28006 Madrid - Tlf. 91 4029391; fax. 91 3093685 / <secremdr@ati.es>
- √ **Capítulo de Valencia y Murcia** - Universidad Politécnica de Valencia, ATI Edificio 1H - ETSINF Camino de Vera, s/n 46022 Valencia Tlf. 656 638 013 / <secreval@ati.es>
- √ **Revistas Novática, REICIS y UPGRADE** - Padilla 66, 3º, dcha., 28006 Madrid - Tlf. 91 4029391; fax. 91 3093685 / <novatica@ati.es>