ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Memoria de Actividades
ISMS Forum Spain

2011

Redacción: ISMS Forum Spain

Fotografía: Daniel Sastre
Toni Maicas

Diseño: jonarriaga1@gmail.com

EQUIPO DE GESTIÓN:

Directora General: Nathaly Rey Arenas

Coordinador General: Daniel Felipe García Sánchez

Management Assistant: María Angelina Carabajal

Colaboradores: Juan Antonio Ibáñez (Comunicación)
Óscar González (Gosán: Asesoría fiscal)
Laura Díaz Bettarel (Periodista)
Webimpacto

Publicación: Madrid, febrero de 2012

Índice

Socios Fundadores

ISMS Forum Spain nació en enero de 2007, respaldada por algunas de las más representativas empresas y organizaciones comprometidas con la Seguridad de la Información en España. Los socios fundadores ejercen su labor en muy diversos ámbitos que van desde la enseñanza superior y la I+D hasta la Consultoría, pasando por los sectores de Banca, Construcción, Energía, Seguros, Servicios Jurídicos, Tecnologías de la Información o Telecomunicaciones.

Agradecimientos

Apoyo institucional

La Asociación agradece expresamente a la **Agencia Europea para la Seguridad de las Redes y de la Información (ENISA)** su apreciada colaboración y apoyo institucional.

Gold Sponsors

ISMS Forum Spain ha desarrollado su labor gracias al generoso apoyo económico, logístico y profesional de las siguientes compañías e instituciones que han adoptado la fórmula de **GOLD SPONSOR** de la Asociación en 2011:

Otros Patrocinadores y Colaboradores

A lo largo del año nos han prestado su apoyo y colaboración puntual otras muchas empresas y organizaciones:

Memoria de Actividades
ISMS Forum Spain

2011

Gianluca D'Antonio
Presidente

Estimados socios, colaboradores y amigos:

Me complace enormemente poner a su disposición esta nueva memoria en la que damos cuenta de las actividades e iniciativas puestas en marcha desde la Asociación durante 2011.

En primer lugar, debo agradecer la participación de socios, patrocinadores y colaboradores, pues sin ellos no sería posible consolidar cada año el gran nivel que han alcanzado las actividades organizadas por ISMS Forum. Hemos cumplido 5 años y durante este tiempo no hemos dejado de crecer y aunar más y más voluntades que no hacen otra cosa que enriquecer nuestra red activa y abierta de profesionales y empresas comprometidas con la Seguridad de la Información.

Actualmente, ISMS Forum engloba cinco áreas especializadas. Así, nuestras Jornadas Internacionales, que inauguraron la Asociación, se han visto complementadas por las actividades del Data Privacy Institute, el capítulo español del Cloud Security Alliance y el proyecto Protegetuinformacion.com, que continúan desarrollándose.

Para el próximo año entre nuestros objetivos está la creación de la Fundación Española de la Privacidad e implantar el Instituto Español de Ciberseguridad. Este último es una apuesta decidida por ISMS Forum en vista al gran interés que se demuestra en la sociedad ante estos aspectos, ya que resultan vitales para asegurar la seguridad nacional, el crecimiento económico y el suministro de los servicios esenciales a la sociedad, provistos por las Infraestructuras Críticas. Un tema extensamente tratado en nuestra última Jornada Internacional de Valencia.

Desde ISMS Forum queremos seguir apostando por una sociedad más segura y un sector fuerte y comprometido. Para ello, desde nuestro carácter abierto y neutral animamos a la participación de todos los actores implicados para abordar los nuevos retos derivados del progreso tecnológico y la globalización, fomentando la inteligencia colectiva y el networking entre todos los miembros de la Asociación.

Asociación Española para el Fomento de la Seguridad de la Información

ISMS Forum Spain es una asociación sin ánimo de lucro, creada en 2007 para promover el **desarrollo, conocimiento y cultura de la Seguridad de la Información en España** y actuar en beneficio de toda la comunidad implicada en el sector. Se constituye como un foro especializado de debate para que todas las empresas; organismos públicos y privados; investigadores y profesionales **colaboren, intercambien experiencias y conozcan los últimos avances y desarrollos** en el ámbito de la Seguridad de la Información. Todo ello desde la **transparencia**, la **objetividad** y la **neutralidad**.

ISMS Forum Spain nació respaldada por empresas representativas y organizaciones comprometidas con la Seguridad de la Información. Los socios fundadores proceden de muy diversos ámbitos que van desde la enseñanza superior y la I+D hasta la Consultoría, pasando por los sectores de Banca, Certificación, Seguros, Construcción, Servicios Jurídicos o Telecomunicaciones. La asociación se ha creado con una vocación **plural y abierta**; que quiere representar a todos los sectores implicados. Por ello **invita a todos los profesionales, empresas e instituciones involucrados en la gestión de la Seguridad de la Información a asociarse**.

ISMS Forum Spain tiene en la actualidad más de **100 empresas asociadas** (cada una de las cuales puede nombrar hasta ocho socios de pleno derecho) y más de **750 profesionales asociados**, ya sea a través de sus empresas o por iniciativa individual. Además, numerosos expertos del sector se han asociado de manera independiente. La Asociación para el Fomento de la Seguridad de la Información es ya, por tanto, la **mayor red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España**.

Entre los principales objetivos de ISMS Forum Spain destacan:

- Dar **visibilidad** a un sector **estratégico** para el desarrollo económico, como es la Seguridad de la Información, y **difundir** el **talento** de los profesionales que trabajan en él.
- Situar a las empresas y organizaciones españolas a la **vanguardia de conocimientos** e implementación de SGSI.
- Ser **interlocutores** en España de diversas asociaciones y foros internacionales relacionados con la Seguridad de la Información.

Para ello, entre otras actividades, ISMS Forum Spain:

- Organiza **eventos** y **actividades formativas** para sus asociados.
- Prepara **herramientas divulgativas** (informes y estudios monográficos; traducción y edición en castellano de manuales y guías de referencia) **e informativas** (newsletter).
- Ha creado el primer **Registro *online* de Profesionales Certificados** en España, el **Data Privacy Institute (DPI)** y el capítulo español de **Cloud Security Alliance (CSA)**. Trabaja en la puesta en marcha de la **Fundación de la Privacidad** y el **Instituto Español de Ciberseguridad**.
- Participa en **foros nacionales e internacionales** y coopera con instituciones públicas y privadas, nacionales e internacionales, para impulsar la cultura de la Seguridad de la Información.

Más información en: www.ismsforum.es

Síguenos en:

twitter LinkedIn

El trámite para hacerse socio de ISMS Forum Spain se realiza online en www.ismsforum.es

ISMS Forum Spain está inscrita en el Registro Nacional de Asociaciones Grupo I, Sección I, Número Nacional 588718

Iniciativas

1. Jornadas Internacionales:

ISMS Forum Spain organiza dos Jornadas Internacionales por año. Se han convertido en referencia del sector y suponen un escenario compartido por los actores más influyentes del sector, siendo además un foro de aprendizaje e intercambio de experiencias para todos sus asociados. Reúnen a ponentes de alto nivel, autoridades de control nacionales e internacionales, grandes compañías españolas comprometidas con la Seguridad de la Información, fabricantes, proveedores de servicios globales y expertos de primer nivel. Se han celebrado 10 ediciones, con 200 ponentes y más de 2.500 asistentes hasta hoy.

2. Data Privacy Institute:

Aglutina a todas las personas y organizaciones que tienen responsabilidades e interés en el cumplimiento de la normativa sobre Privacidad y la Protección de Datos de carácter personal. Su objetivo es promover la formación y la excelencia en esta área de creciente importancia. Por ello, ha puesto en marcha la Certified Data Privacy Professional (CDPP), que acredita un alto nivel de especialización en la normativa española en materia de Protección de Datos de carácter personal, así como un dominio de los fundamentos que rigen la Seguridad de la Información. Se trata la primera certificación española dirigida a los profesionales de la Privacidad y se obtiene tras la superación de una prueba teórica, o acreditando una experiencia profesional de al menos 10 años, entre otros criterios.

3. Cloud Security Alliance:

El capitulo español de Cloud Security Alliance reúne a miembros representativos de los distintos actores de la industria del Cloud Computing en España. Se trata de un foro de debate que promueve el uso de buenas prácticas para garantizar la seguridad y privacidad en el entorno del Cloud Computing, siendo una de sus áreas de interés específico el 'Compliance en la Nube'. ISMS Forum pondrá en marcha el Certificate of Cloud Security Knowledge (CCSK) en castellano, que acredita a título individual a profesionales con conocimientos en materia de seguridad en el Cloud Computing, incluyendo gestión de riesgos y buenas prácticas.

4. Workshops:

ISMS Forum organiza workshops donde se abordan aspectos concretos de la Seguridad de la Información y donde las empresas pueden intercambiar conocimientos, buenas prácticas y casos de éxito. Se trata de un punto de encuentro que fomenta la inteligencia colectiva en aras de una excelencia en la gestión.

5. Protegetuinformación.com:

Es una herramienta didáctica e interactiva que divulga la cultura de la Seguridad de la Información y de la Protección de Datos entre la ciudadanía en general. Está dirigida a todos los grupos sociales (niños, jóvenes, adultos, mayores, padres y profesionales), el Portal presenta distintos mensajes y aplicaciones adaptadas a cada perfil, siempre en un lenguaje sencillo y accesible.

6. Formación:

ISMS Forum Spain apuesta por la formación continua de los profesionales de la Seguridad de la Información. De este modo se organizan distintos cursos como los de Analista de Riesgos en Seguridad de la Información y el Curso de Gobierno Corporativo de la Seguridad de la Información. Seguirán creándose nuevos cursos y nuevas convocatorias.

7. Registro de Profesionales Certificados:

Es un servicio público y gratuito para socios de ISMS Forum Spain dirigido a los profesionales que trabajan en Seguridad de la Información y a las empresas, organizaciones e instituciones que puedan necesitar de sus servicios.

Órganos de Gobierno

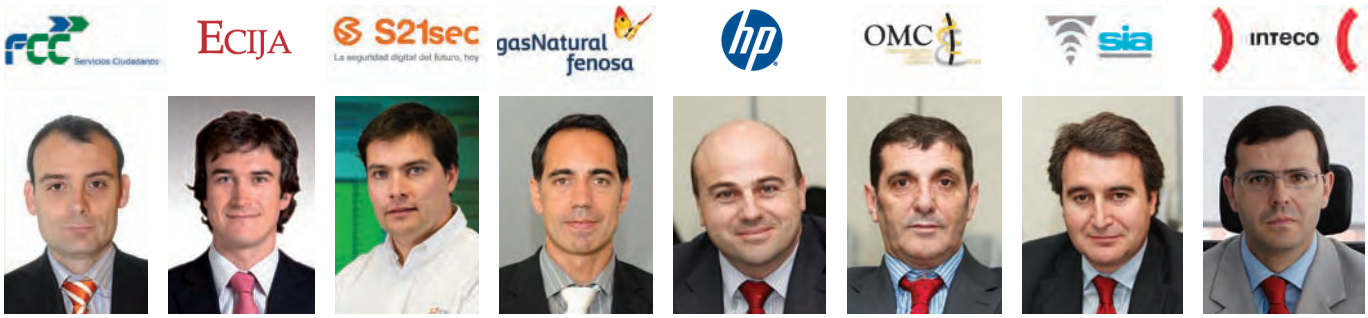
LA ASAMBLEA DE SOCIOS

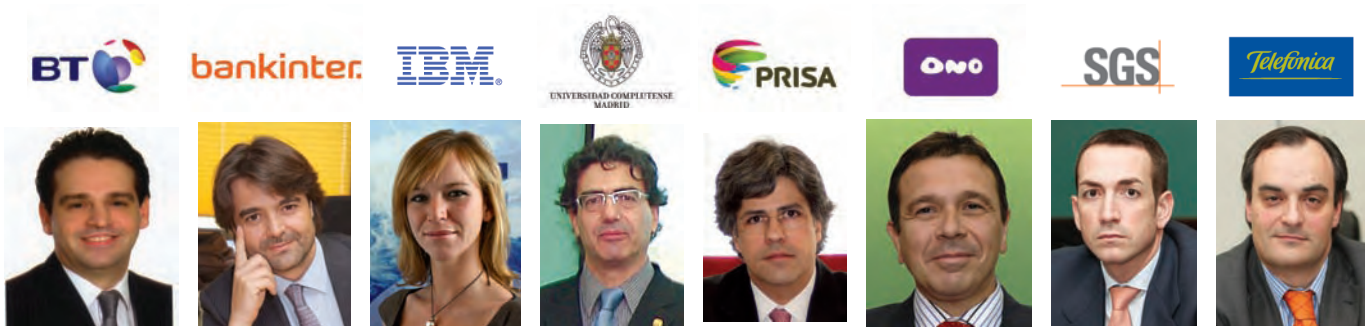
La Asamblea es el órgano supremo de decisión y gobierno de ISMS Forum y está constituida por todos sus asociados. A la Asamblea corresponde la aprobación de las directrices a seguir por la Asociación, así como la aprobación de los resultados financieros de la misma.

LA JUNTA DIRECTIVA

La Junta Directiva es el órgano de representación y administración de la Asociación. Está compuesta por un Presidente, un Vicepresidente, un Secretario, un Vicesecretario y vocales. Sus miembros son elegidos por la Asamblea, mediante votación libre y secreta.

Actualmente, la Junta Directiva está compuesta por:





Gianluca D'Antonio* Chief Information Security Officer (CISO) del **Grupo FCC.** *Presidente de* ***ISMS Forum Spain.***

Carlos Alberto Saiz Peña* Socio Director del Área Compliance IT de **Ecija**. *Vicepresidente y Secretario de* ***ISMS Forum Spain***.

David Barroso Director de **S21sec** E-crime.

Andreu Bravo Responsable de Seguridad de la Información de **Gas Natural-Fenosa**.

Luis Buezo* Director para EMEA de la Práctica de Seguridad de **HP Technology Services.**

Joan Camps Pons Director de Proyectos y de la Unidad Tecnológica del **Consejo General de Colegios Oficiales de Médicos de España (CGCOM)**.

Alfonso Fernández Jiménez Director de Desarrollo de Negocio de **Sistemas Informáticos Abiertos (Grupo SIA)**.

Marcos Gómez Subdirector de Programas del **Instituto Nacional de Tecnologías de la Comunicación (INTECO)**.

José Francisco Pereiro Head of Security Practice de **BT España y Portugal**.

Jesús Milán Lobo* Responsable de Riesgos Tecnológicos y Seguridad de **Bankinter**.

Jessica Valderrama Sales Security Leader de **IBM** España y Portugal.

Fernando Pescador Director de los Servicios Informáticos de la **Universidad Complutense de Madrid (UCM)**.

Jaime Corró Bestard (Director de Seguridad Lógica del **Grupo PRISA**.

Miguel Rego Fernández* Director de Seguridad y Riesgos Corporativos de **ONO**.

Álvaro Rodríguez de Roa Director de Seguridad de la Información y Gobierno TI de **SGS ICS Ibérica**.

Juan Miguel Velasco López-Urda Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Clientes de **Telefónica España**.

** Miembro de Comité Operativo de la Junta Directiva.*

COMITÉ OPERATIVO Y DIRECCIÓN

El Comité Operativo es el órgano encargado de tomar decisiones de manera ágil por delegación de la Junta Directiva, teniendo una implicación directa e inmediata en la marcha de la Asociación y en el seguimiento de sus actividades. Actualmente, el Comité Operativo está formado por los siguientes miembros: Gianluca D'Antonio, Carlos Alberto Saiz Peña, Luis Buezo, Jesús Milán y Miguel Rego. La actual Directora General de ISMS Forum es Nathaly Rey Arenas.

Empresas asociadas

En diciembre de 2011, más de 100 empresas y organizaciones de los más diversos sectores se han asociado, y más de 750 profesionales forman parte de ISMS Forum Spain, ya sea como miembros independientes o a través de sus empresas. Es muy amplia la variedad de empresas y organizaciones, de los más diversos tamaños y sectores de actividad: proveedores y clientes de servicios relacionados con la implantación y gestión de SGSI se están reuniendo en torno a ISMS Forum Spain como punto de encuentro neutral, pero también instituciones y organismos profesionales, investigadores y expertos académicos. Los conocimientos, la experiencia, el alto nivel y la profesionalidad de sus miembros constituyen el gran valor de la Asociación.

- Abast Systems
- Abertis Infraestructuras
- Accenture
- Acens Technologies
- Agaex Informática
- Agbar
- Anyhelp International
- Applus+, LGAI Technological Center
- Arbor Network
- Asistencia Sanitaria Interprovincial (ASISA)
- Asociación Española de Destrucción Confidencial de Información (AEDCI)
- Audisec Seguridad de la Información
- Bankinter
- BDO Auditores
- Blancco
- British Standards Institution España (BSI)
- BT España
- Cajamar Caja Rural
- Compañía Española de Petróleos (CEPSA)
- Consejo General de Colegios Oficiales de Médico (OMC)
- Deloitte
- Destruccion Confidencial de Documentacion (DCD)
- Ecija
- Endesa
- Ernst & Young
- Eulen Seguridad
- Everis Spain
- Ferrovial
- Fomento de Construcciones y Contratas (Grupo FCC)
- Fortinet
- Future Space
- Gas Natural Informática
- Gigatrust Spain
- GMV Soluciones Globales Internet
- GNET
- Grupo Generali
- Grupo Intermark 96
- Grupo Mahou-San Miguel
- Grupo S21sec Gestión
- Hewlett-Packard Española (HP)
- IDN Servicios Integrales
- Indra Sistemas
- Ingeniería e Integración Avanzadas (Ingenia)
- Innovery (Innovation Discovery)
- Instituto CIES
- Instituto Nacional de Tecnologías de la Comunicación (INTECO)
- International Business Machines (IBM)
- Internet Security Auditors (ISecAuditors)
- Interxion España
- Ironwall Strategic Security Systems
- Isaca
- Juniper Networks
- Kaspersky Lab
- KPMG Asesores
- Leaseplan Servicios
- Lloyd's Register Quality Assurance (LRQA)
- McAfee
- Mutua Madrileña
- Numara Software
- Ocaso
- Oesia Networks
- ONO
- Open3s Open Source And Security Services
- Panda Security
- Pricewaterhousecoopers (PWC)
- Promotora de Informaciones (Grupo PRISA)
- Prosegur
- Red Seguridad
- Repsol
- Revista Dintel Alta Dirección
- S2 Grupo
- Sage Logic
- SGS ICS Ibérica
- Sistemas Informaticos Abiertos (Grupo SIA)
- Sm4rt Security Services
- Spamina (Cloud Email & Web Security)
- Steria Ibérica
- Symantec
- Tecnocom Telecomunicaciones y Energía
- Telefónica
- Trend Micro
- Unidad Editorial
- Verizon Spain

Jornadas Internacionales
ISMS Forum Spain

I Jornada
Balance mundial y retos de la gestión profesional de la Seguridad de la Información en España.

II Jornada
Seguridad de la Información: Una cuestión de Responsabilidad Social Corporativa.

III Jornada
Compliance en Seguridad de la Información: Claves y tendencias
Una visión global del presente y una mirada al futuro.

IV Jornada
Amenazas internas y externas a la Seguridad de la Información hoy.

V Jornada
La organización de la seguridad: El laberinto del CISO.

VI Jornada
Impactos de la transformación económica y social en la Seguridad de la Información.
El desafío de proteger nuevos ámbitos y hábitos de trabajo.

VII Jornada
Seguridad de la Información: ¿Cómo innovar en tiempos de crisis?.

VIII Jornada
The Future of Information Security: Nuevos retos y desafíos para un futuro + seguro.

IX Jornada
Amenazas, compliance, riesgos y privacidad:
A Global Approach.

X Jornada
Ciberdefensa y Ciberseguridad: La evolución de la amenaza frente a la protección
de las infraestructuras críticas.

Actividades 2011,
Jornadas Internacionales

ISMS Forum Spain organiza **dos jornadas internacionales anuales** que, ya desde su primer año de actividad, se han convertido en citas de referencia del sector y sirven como foro de aprendizaje e intercambio de experiencias para todos sus asociados. La vocación de estos seminarios es presentar a **ponentes de alto nivel**, en un contexto que facilite además el encuentro y la comunicación entre los asociados, y con un **componente internacional** representativo. L**a asistencia a estas jornadas es gratuita para los socios de ISMS Forum Spain,** incluyendo el almuerzo.

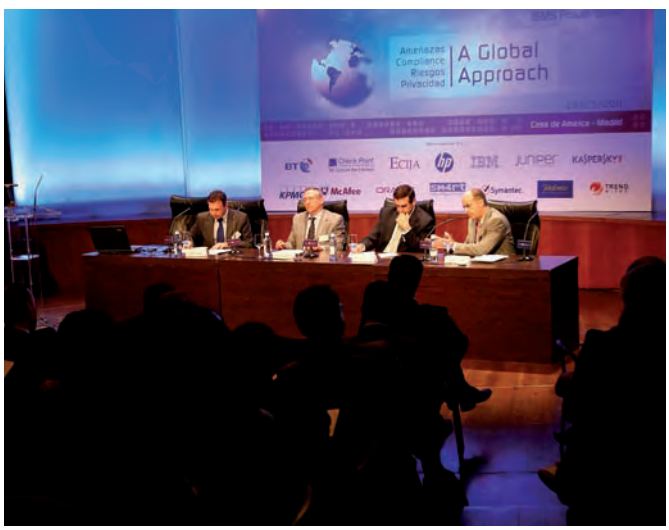
Las jornadas se organizan siempre de forma que quede un tiempo para que los participantes se relacionen entre sí y puedan además acceder y comentar con los conferenciantes sus inquietudes. **Ya son más de 2.500 las personas que han participado en las 10 jornadas organizadas desde 2007,** quienes han evaluado las mismas a través de cuestionarios de calidad que han dado como resultado siempre una **puntuación media de cuatro sobre cinco puntos,** en lo que se refiere a organización, contenidos, escenario, ponentes y documentación.

Al considerar que una asociación de ámbito nacional debe beneficiar a todos sus socios, dinamizando el sector y fomentando la Seguridad de la Información, ISMS Forum organiza eventos en todo el territorio español. Se alternan jornadas en Madrid con jornadas en otras ciudades. Así, se han celebrado ya jornadas en Barcelona, Sevilla y Valencia.

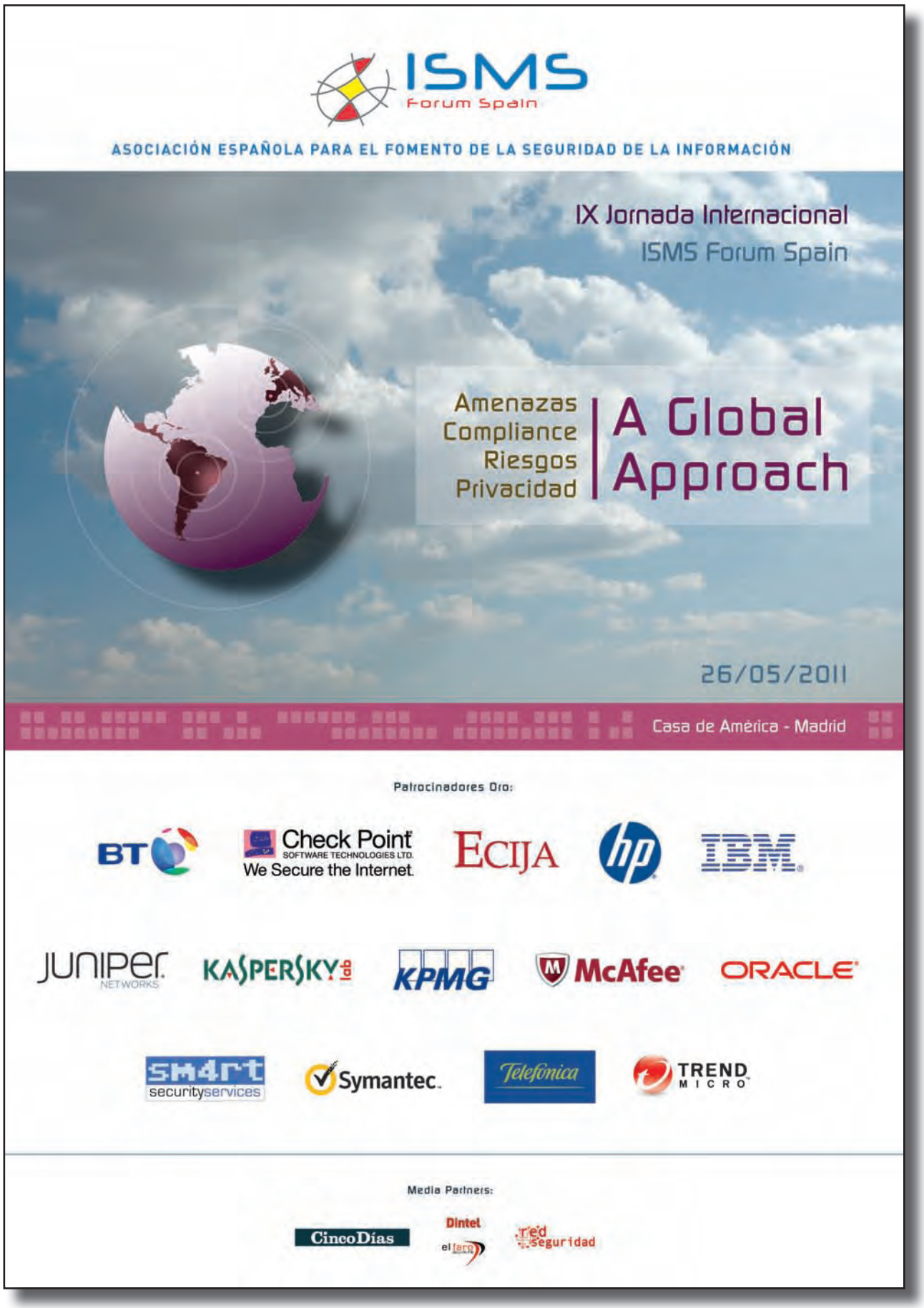
Como puede observarse en el cuadro de asistencia, estas Jornadas Internacionales cuentan con entre 250 y 300 asistentes, todos profesionales y expertos en Seguridad de la Información, ejecutivos y altos directivos representando a las empresas más importantes de España.

Asistencia a las Jornadas Internacionales de **ISMS Forum Spain**

	2007		2008		2009		2010		2011	
Eventos	I Jornada 17/05/2007 Madrid **Museo Reina Sofía**	II Jornada 20/11/2007 Madrid **Palacio Municipal Congresos**	III Jornada 29/05/2008 Madrid **Hotel Husa Princesa**	IV Jornada 13/11/2008 Barcelona **Torre Agbar**	V Jornada 28/5/2009 Madrid **Auditorio Mutua Madrileña**	VI Jornada 24/11/2009 Sevilla **Hotel Barceló Isla de la Cartuja**	VII Jornada 25/5/2010 Madrid **Palacio Municipal Congresos**	VIII Jornada 30/11/2010 Barcelona **Torre Agbar**	IX Jornada 26/05/2011 Madrid **Casa de América**	X Jornada 29/11/2011 Valencia **Ciudad de las Artes y las Ciencias**
Nº de asistentes	202	256	258	270	280	200	280	280	250	255



Actividades 2011,
IX Jornada Internacional

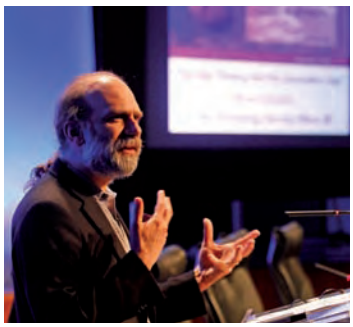


Programa IX Jornada ISMS Forum Spain

8:45	**Acreditación**
9:00 Bienvenida	**Palabras de Bienvenida.** **Gianluca D'Antonio,** Presidente de **ISMS Forum Spain**; Chief Information Security Officer (CISO) del **Grupo FCC**; Asesor de Seguridad (PSG) de la **European Network and Information Security Agency** (**ENISA**). **Imma Turbau Fuertes,** Directora General de la **Casa de América**.
9:15 Inaugural Keynote	**Security, Privacy and the Generation Gap.** **Bruce Schneier,** Chief Security Technology Officer de **BT**.
9:45 Mesa redonda	**¿Cómo Implantar un Modelo de Seguridad Global que Conviva con las Necesidades y Requerimientos en Europa y Latinoamérica?** **Manuel Carpio,** Director de Seguridad de **Telefónica**. **Guillermo Llorente,** Director de Seguridad de **Mapfre**. **Enrique Polanco,** Adjunto al Consejero Delegado y Director de Seguridad Corporativa del **Grupo PRISA.** Moderador: **Miguel Rego,** Director de Seguridad y Riesgos Corporativos de **ONO**.
10:45	**Coffee-break**
11:15 Keynote	**Information Security Metrics - Information that Matters to the Business.** **John Rakowski,** Analyst & Advisor de **Forrester Research**.
11:45 Debate	**Internal Threats: Does Wikileaks Testify to the Need for Improved Network Visibility?** **Pedro Cutillas,** CTO Enterprise EMEA & Vice-President Strategic Alliances EMEA de **Juniper Networks**. **Rick Miller,** Global Managed Security Services Leader de **IBM**. **John Rakowski,** Analyst & Advisor de **Forrester Research**. Moderator: **Juan Miguel Velasco,** Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Clientes de **Telefónica España**.
12:45 Debate	**Cross Border Data Flows vs. Multiple Privacy Regulations and Jurisdictions.** **Giovanni Buttarelli,** European Data Protection Assistant Supervisor, **EDPS**. **Peter Fleischer,** Global Data Privacy Officer de **Google**. **Ronald Koorn,** Partner, Global Privacy Leader de **KPMG**. **Daniel Pradelles,** EMEA Privacy Officer de **HP**. Moderadora: **Nathaly Rey,** Directora General de **ISMS Forum Spain.**
13:45 Presentación	**Proyectos y Actividades de ISMS Forum Spain.** Junta Directiva de **ISMS Forum Spain**.
14:30	**Almuerzo - Lunch**
16:00 Debate	**Marcos Normativos de Protección de Datos en Europa y en Latinoamérica.** **Raúl Ferrada,** Director General del **Consejo para la Transparencia**, Chile. **María Marván,** Comisionada del **Instituto Federal de Acceso a la Información** (**IFAI**), México. **Artemi Rallo,** Director de la **Agencia Española de Protección de Datos** (**AEPD**). Moderador: **Carlos Alberto Sáiz Peña,** Vicepresidente de **ISMS Forum Spain**; CDPP, Socio Director Compliance IT de **Ecija**.
16:45 Debate	**Reputación Corporativa en Internet.** **Álvaro Ecija,** Socio de **Ecija**; Consejero de **Playtelevision**. **José Antonio Gallego,** Presidente de la **Asociación Española de Responsables de Comunidad** (**AERCO**). **José Manuel Velasco,** Director General de Comunicación y Relaciones Corporativas del **Grupo FCC**. Moderador: **Alfredo Reyes Krafft,** CDPP, Vicepresidente **Asociación Mexicana de Internet**; Director de Negocios Digitales e Industria Bancaria en **BBVA Bancomer**, México.
17:30 Clausura	**A New Security Risk Approach for Privacy Regulations.** **Víctor Chapela,** CEO de **SM4RT Security Services**, México.

Principales conclusiones / Por: Laura Bettarel

La respuesta a las crecientes amenazas y riesgos de seguridad y de privacidad debe tener una aproximación global y flexible



Bruce Schneier.

ISMS Forum reunió el 26 de mayo a 28 expertos en seguridad de empresas nacionales e internacionales para debatir sobre los nuevos retos que enfrentan las compañías en materia de Seguridad de la Información y analizar las distintas estrategias a seguir, en un entorno donde la movilidad y los servicios basados en Internet, hacen que sea más difícil establecer cuál es el perímetro y definir fronteras para los flujos de información.

Con el objetivo de analizar las distintas estrategias jurídicas y organizacionales que están influyendo en la regulación de la privacidad bajo el entorno actual, la IX Jornada Internacional ISMS Forum Spain, reunió a cerca de 30 ponentes de primer nivel, expertos en seguridad en organizaciones como Forrester Research, Ecija, Google, Grupo PRISA, Grupo FCC, HP, IBM, Juniper Networks, KPMG, Mapfre, ONO, y Telefónica.

En este evento se debatió sobre aspectos como el "gap", o hueco generacional generado por Internet y la manera de entender la seguridad y la privacidad, "¿Cómo Implantar un Modelo de Seguridad Global que Conviva con las Necesidades y Requerimientos en Europa y Latinoamérica?", los marcos Normativos de Protección de Datos en Europa y en Latinoamérica y la Reputación Corporativa en Internet, entre otros temas.

Gianluca D'Antonio, Presidente de ISMS Forum Spain y CISO del Grupo FCC, resumió al principio del evento la importancia de debatir sobre la Seguridad y Privacidad en un momento como el actual. "El emergente ecosistema digital está generando muchos riesgos y desafíos. Igual que cualquier ecosistema sostenible permite a sus actores interactuar en beneficio de todos, un ecosistema digital debe permitir a sus participantes comerciales crear valor económico y al mismo tiempo ofrecer bienestar al conjunto de la sociedad". Para ello se debe encontrar un equilibrio de factores críticos como la seguridad, la privacidad, la capacitación del usuario, la estructura en las reglas del mercado y el derecho a la propiedad intelectual.

"Un ecosistema digital debe permitir a sus participantes comerciales crear valor económico y al mismo tiempo ofrecer bienestar al conjunto de la sociedad".

Gianluca D'Antonio,

Presidente de ISMS Forum.

Como parte de la celebración de este encuentro, que contó con más de 250 asistentes expertos en materia de seguridad, ISMS Forum premió a HP, IBM y Symantec por su firme compromiso con el desarrollo de la Seguridad de la Información en España. Asimismo, se presentó el primer informe: 'Cloud Compliance Report', elaborado por el capítulo español de CSA-ES, que constituye prácticamente la única referencia en nuestro país del análisis del Cloud desde la perspectiva de España.

Gap generacional: Los jóvenes tienen fluidez social, pero no tecnológica

Bruce Schneier, Chief Security Technology Officer de BT, habló de la Privacidad y el "gap" o distancia generacional. Schneier, calificado por la revista "The Economist" como uno de los gurús de la seguridad explicó que "para el promedio de las personas la seguridad es principalmente algo relacionado con el control de la información (...) Todos esperamos ser capaces de controlar la información; ya sea la del e- mail, la información bancaria o nuestra ubicación". Pero el desarrollo de la tecnología ha hecho públicas cosas que antes no lo eran.

"Antes de Facebook nadie tenía la necesidad de una política de seguridad, ni de escribirla". Es aquí donde Internet pone en evidencia las diferencias entre las distintas generaciones: "Los jóvenes tienen una fluidez social, pero no tecnológica. La socialización pertenece a los jóvenes; para ellos vivir la vida en público es normal".

De izquierda a derecha: Manuel Carpio, Guillermo Llorente, Enrique Polanco y Miguel Rego.

"No somos clientes. Los usuarios somos los productos de Facebook para sus clientes". Bruce Schneier, *BT.*

Y ese es el negocio de Facebook y de otras redes sociales, hacer negocio con lo que compartimos. "No importa si no son nuestros secretos más íntimos", mientras más usuarios cuenten lo que hacen, más compartan y más digan qué sitios frecuentan, más gana la red social. "No somos clientes. Los usuarios somos los productos de Facebook para sus clientes".

Según Schneier, existen seis tipos de datos que Facebook recopila sobre sus usuarios: los datos de servicio o básicos para la apertura de la cuenta; los datos que se van sumando con el paso del tiempo: posts, fotos subidas por el usuario, etc.; en qué perfiles has entrado; los datos secundarios (la información que otro sube acerca de ti; datos sobre tus hábitos; y datos derivados (las coincidencias con el 70% de tus amigos: lugar, aficiones, tendencias, etc). Por tanto, lidiar con la privacidad de esos seis tipos de datos es complicado y las redes son débiles en privacidad.

Dos reflexiones de la intervención de Schneier: "Si la gente cree que tiene control, comparte, si no, son menos propensos a compartir". Pero, la mayoría de los usuarios que entran en una red se quedan con la seguridad que viene por defecto en la página web a la que se afilia; y estas suelen ser muy débiles.

¿Cómo Implantar un Modelo de Seguridad Global?

La primera mesa redonda del día giró en torno a cómo se debe implantar un Modelo de Seguridad Global. En ella, participaron Guillermo Llorente, Director de Seguridad de Mapfre; Manuel Carpio, Director de Seguridad de Telefónica; y Enrique Polanco, Adjunto al Consejero Delegado y Director de Seguridad Corporativa del Grupo PRISA, con Miguel Rego, Director de Seguridad y Riesgos Corporativos de ONO, como moderador.

Los participantes de esta mesa redonda defendieron la importancia de compartir inteligencia de seguridad a fin de diseñar de manera eficaz las políticas de seguridad a las que deben sujetarse los activos de información, para Manuel Carpio: "hemos pasado del *need to know* al *need to share*.

¿Cómo entienden la seguridad global? En el caso de Mapfre, Guillermo Llorente comentó que ven a la organización como un todo donde quiera que esté y, desde una perspectiva funcional, valoran las actividades corporativas encaminadas a un fin. "Por ejemplo, recursos humanos, seguridad, tecnología, asuntos legales. En esa función agrupamos un conjunto de actividades: que van desde los controles de seguridad ya sean físicos o lógicos, las acreditaciones, la protección de los bienes, etc. Pero es una función corporativa que engloba múltiples actividades".

Manuel Carpio explicó que el caso de Telefónica era muy similar. "Tenemos un modelo corporativo que se basa en el principio de delegación de autoridad de parte de la dirección del negocio. Implantamos nuestro modelo en cada uno de los países en los que estamos, pero somos muy respetuosos con la cultura. Un modelo es un espejo en el que mirarse pero no una fotocopia".

En este sentido, Enrique Polanco incidió en la importancia de que las propias empresas respeten la seguridad, pues si no, no se pueden atender las amenazas. "Tenemos que entender que la amenaza es global, es internacional".

Respecto a qué nivel de reporte tener dentro de la organización, Llorente comentó el caso de MAPFRE donde Seguridad es una de las áreas corporativas que dependen de la presidencia. "Existe un comité en el cual yo actúo como secretario y están presentes las máximas autoridades de cada una de las unidades de negocio.

"Es importante que participen las distintas áreas de negocio, pues ellas serán las encargadas de implementarla". Guillermo Llorente, *MAPFRE.*

En este comité se presentan y se definen los criterios de seguridad. Por ello es importante que participen las distintas áreas de negocio, pues ellas serán las encargadas de implementarlas".

En el caso de Telefónica, Carpio comentó que la empresa fue una de las primeras en aplicar el concepto de seguridad integral a su esquema corporativo, donde el CSO reporta al presidente de Telefónica. No obstante, como empiezan a aparecer los chief risk officer, el chief tecnical security officer, etc., es muy importante tener una coordinación de todos.

Polanco explicó uno de los problemas que ha identificado a través de su trabajo en Prisa: elevar demasiado la seguridad. "No me gusta mi modelo. El responsable máximo de seguridad está en niveles muy elevados y puede caer en el error de estar en una línea jerárquica separada de quienes deciden y aplican las órdenes. Por lo cual te conviertes en consejero". Hay que estar en la línea jerárquica y cerca de quienes toman la decisión y la aplican.

"¿Qué pueden hacer las empresas que no tienen un modelo global?", preguntó Rego. "No existe modelo receta", respondió Llorente. Lo seguro, según sus palabras, es que no debe estar 100% centralizada. "Hay que identificar qué medidas puedes centralizar y cuáles no, establecer responsables funcionales en cada área. Después definir el nivel de riesgo corporativo y el nivel de riesgo asumible en cada país; hay que ser capaz de amoldarse a un escenario cambiante y complejo". "No hay un modelo único pero sí una línea única adaptable".

Dejando claro lo complicado de la pregunta, Polanco aclaró que es muy importante tener en cuenta las peculiaridades locales y el nivel de delegación; pero alguien tiene que tener la responsabilidad y decir cómo se hace, tienen que existir "órganos colegiados para la toma de decisiones tácticas, no estratégicas".

En conclusión para lograr una seguridad global idónea hay que "conseguir el equilibrio adecuado entre la centralización de la seguridad y su adaptación en el ámbito local".

"20 minutos para generar un impacto"

John Rakowski, Analyst & Advisor de Forrester Research habló de las métricas en Seguridad de la Información durante su conferencia "Information Security Metrics - Information that Matters to the Business". Explicar la seguridad cuando hay problemas presupuestarios puede ser un gran reto. "Tenemos que generar un amplio impacto para los directivos de seguridad, dar en la diana". Para explicarlo puso el ejemplo de Ozzy Osbourne que, para llamar la atención de los directivos de una discográfica que sólo le habían dado 20 minutos para reunirse con él, se sacó una paloma de su bolsillo y le arrancó la cabeza. "La moraleja es que si tú eres un ejecutivo de seguridad sólo tienes 20 minutos para estar frente a los directivos, por tanto tienes que usar la métrica adecuada para impactarles".

Se trata de generar la información interesante en el tiempo adecuado y en la cantidad correcta. "Tenemos que lograr alinear la función de seguridad con el negocio. Subir su valor ante los directivos. Que se convierta en un valor añadido".

Los pasos propuestos por Rakowski para crear un alto impacto son:

1) Comprender las capacidades de los informes actuales. Como profesionales de la seguridad tenemos que dar una serie de métricas que podemos usar potencialmente. Hay que empezar con una documentación con toda la métrica y decidir qué métricas son más interesantes de cara al ejecutivo.

2) Calibrar qué quieren ellos en cuanto a informes, averiguar qué les interesa. Disminuir la brecha de la seguridad por un lado y la dirección por el otro.

3) Planificar y diseñar el informe. Organizar un marco para escribir el informe.

4) Poner en práctica este informe sin perder de vista el aspecto de estar alineado con el negocio, alineación funcional, eficiencia y eficacia, niveles de calidad y de servicio, medición de procesos, innovación, y alineación en el cumplimiento de las leyes.

De izquierda a derecha: Juan Miguel Velasco, Rick Miller, Pedro Cutillas y John Rakowski.

"Tenemos que lograr alinear la función de seguridad con el negocio. Subir su valor ante los directivos. Que se convierta en un valor añadido". John Rakowski, *Forrester Research*.

Pero el proceso no termina en el paso 4. Tiene que ser circular, de retroalimentación para entrar y generar el nivel adecuado de seguridad de la comunicación. "Tienes 20 minutos para un impacto dales un buen diagrama conceptual y céntrate en los beneficios de ponerlo en práctica".

Después de Wikileaks ¿Deberíamos mejorar nuestra NAV?

Juan Miguel Velasco, Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Clientes de Telefónica España, moderó la mesa redonda "Internal Threats: Does Wikileaks Testify to the Need for Improved Network Visibility?" en la que participaron Pedro Cutillas, CTO Enterprise EMEA & Vice-President Strategic Alliances EMEA de Juniper Networks; Rick Miller, Global Managed Security Services Leader de IBM, y John Rakowski, Analyst & Advisor de Forrester Research.

La cultura y la formación del personal fueron destacadas como otra de las variables a tener en cuenta en la aplicación de la seguridad. "El problema surge cuando alguien tiene acceso autorizado y malas intenciones" aclaró Rakowski quien añadió que casos como los de Wikileaks surgen todos los días, la diferencia es que ésta ha llegado a los medios.

Los participantes de la mesa redonda estuvieron de acuerdo en que hay que impedir que sea fácil la fuga de información definiendo qué información es sensible y quién tiene acceso a qué, que cada persona dentro de la organización tenga el nivel de acceso adecuado.

¿Reducir el acceso a redes sociales o a Internet para disminuir los riesgos? Esa no parece ser una solución efectiva. Miller explicó que se podría tener un enfoque muy restrictivo, pero hay que tener en cuenta que los profesionales de hoy en día han cambiado "tenemos que tener en consideración el riesgo de controles excesivos" pues no están acostumbrados a ellos.

"La solución es tener servicios y productos que tengan aportaciones de valor y que detecten problemas de seguridad fácilmente y que podamos darnos cuenta de que algo se escapa de nuestra red". Pedro Cutillas, *CTO*.

John Rakowski.

Cutillas explicó que la solución es tener servicios y productos que tengan aportaciones de valor y que detecten problemas de seguridad fácilmente y que podamos darnos cuenta de que algo se escapa de nuestra red.

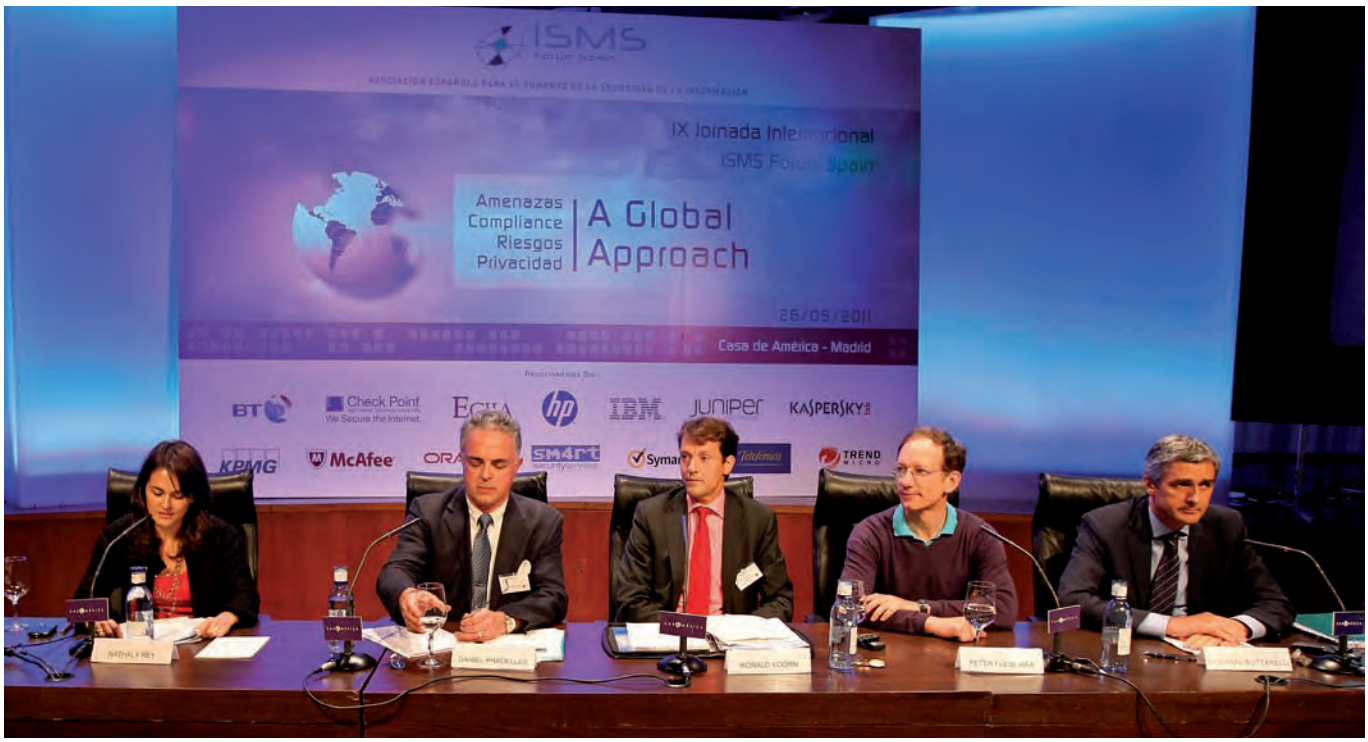
Para Rakowski más que prohibir, hay que "implicarse con la gente y ser proactivo. Preguntar qué aplicaciones usas en tu Ipad o en tu móvil, entonces les puedes explicar cómo deben usarlo y, si no lo pueden hacer, darles una razón".

La necesidad de armonizar la ley

Giovanni Buttarelli, European Data Protection Assistant Supervisor; Peter Fleischer, Global Data Privacy Officer de Google; Ronald Koorn, Partner y Global Privacy Leader de KPMG y Daniel Pradelles, EMEA Privacy Officer de HP, participaron en la mesa redonda "Cross Border Data Flows vs. Multiple Privacy Regulations and Jurisdictions", bajo la moderación de Nathaly Rey, Directora General de ISMS Forum Spain.

Para los participantes en la mesa redonda es un gran momento para trabajar por armonizar la ley, pues el crecimiento exponencial de los flujos de datos transfronterizos representa un gran reto en la privacidad. Un punto importante dentro de la discusión fue no centrar el debate sobre en qué lugar están los datos sino en que quienes controlan los datos respeten las regulaciones de privacidad, sin importar donde estén.

En materia de regulación de la privacidad, la mayoría de los expertos coincidieron en la necesidad de ir hacia un marco homo-



De izquierda a derecha: Nathaly Rey, Daniel Pradelles, Ronald Koorn, Peter Fleischer y Giovanni Buttarelli.

"El marco actual no es algo totalmente eficaz ni efectivo. Hay tendencias por tanto a una mayor armonización no sólo a nivel europeo".

Daniel Pradelles, *HP.*

géneo de protección de datos, aunque para Artemi Ralló: "no es algo que vayamos a lograr a corto ni a medio plazo". Peter Fleischer, por su parte, indicó que a él también le gustaría que hubiera una armonización global, "porque sería la mejor manera de proteger la privacidad, pero es muy complicado porque hay países mucho más estrictos en sus normas que otros".

Buttarelli explicó que "el marco actual no es algo totalmente eficaz ni efectivo. Hay tendencias por tanto a una mayor armonización a nivel europeo. También hay expectativas de un marco más moderno con una regulación de mayor flexibilidad, con menos cargas administrativas". Entre las dificultades Pradelles comentó que "el problema de la directiva actual es que cada país de Europa la interpreta de una manera distinta". Además, tampoco se puede regular de manera excesiva, Según Fleischer "en un futuro habrá más flujos de datos y la pregunta es quién va a escribir una ley para regular todo eso".

Como cierre al debate se propuso la posibilidad de que la privacidad esté presente desde el principio para que cualquier dispositivo de software sea concebido en vistas a minimizar los procesamientos no necesarios de datos personales.

Pradelles apuntó a la investigación en tecnologías como condición para garantizar de manera satisfactoria la gestión de la privacidad. Butarelli coincidió con el responsable de HP en este punto, afirmando que cualquier software que se desarrolle habría de contar con lo que se denomina "privacidad por defecto". No obstante, Pradelles apuntó que la privacidad va mucho más allá que la seguridad: "la privacidad por defecto o por diseño será importante y no solo se refiere al software, sino también a servicios y procesos dentro de las empresas".

Marcos Normativos de Protección de Datos en Europa y en Latinoamérica

Para encontrar los puntos en común de las diferentes leyes en relación con la privacidad, Artemi Rallo, Director de la Agencia Española de Protección de Datos (AEPD); Raúl Ferrada, Director General del Consejo para la Transparencia de Chile; y María Marván, Comisionada del Instituto Federal de Acceso a la Información (IFAI) de México, debatieron junto a Carlos Alberto Sáiz Peña, Vicepresidente de ISMS Forum Spain; CDPP, Socio Director Compliance IT de Ecija, sobre los Marcos Normativos de Protección de Datos en Europa y en Latinoamérica.

Tanto el representante de Chile como la de México reconocieron el importante aporte del modelo creado en España para la garantía del derecho a la protección de datos. Respecto a las peculiaridades de los modelos de sus países, Ferrada comentó que en Chile el Consejo de la Transparencia es el encargado de verificar que el derecho de acceso a la información pública no contradice aspectos relacionados con la seguridad nacional, el interés público o temas relativos a derechos de las personas. "En un 30% de los casos estudiados por el Consejo hemos tenido que ponderar ambos derechos: el derecho a acceder a información pública frente al derecho de la protección de datos".

En el caso de México, Marván explicó que el sistema aprobado en la Ley de 2010 "es un sistema fuerte en términos de multas

"En un 30% de los casos estudiados por el Consejo hemos tenido que ponderar ambos derechos: el derecho a acceder a información pública frente al derecho de la protección de datos". Raúl Ferrada, *Consejo para la Transparencia en Chile.*

que podrían llevar a multas de hasta 300.000 euros". A diferencia del modelo español el instituto no se refinanciará a través de las multas.

La comisionada del IFAI indicó que en el contenido de la citada ley se establece un equilibrio entre protección de la información personal y la libre circulación de la misma. Añadió que "es una legislación moderna que reconoce y protege los llamados derechos de tercera generación". Comentó, por ejemplo, que facilita las transferencias de datos personales dentro y fuera del país, siempre y cuando el responsable informe en el aviso de privacidad la realización, la finalidad de las transferencias y el titular acepte o consienta éstas.

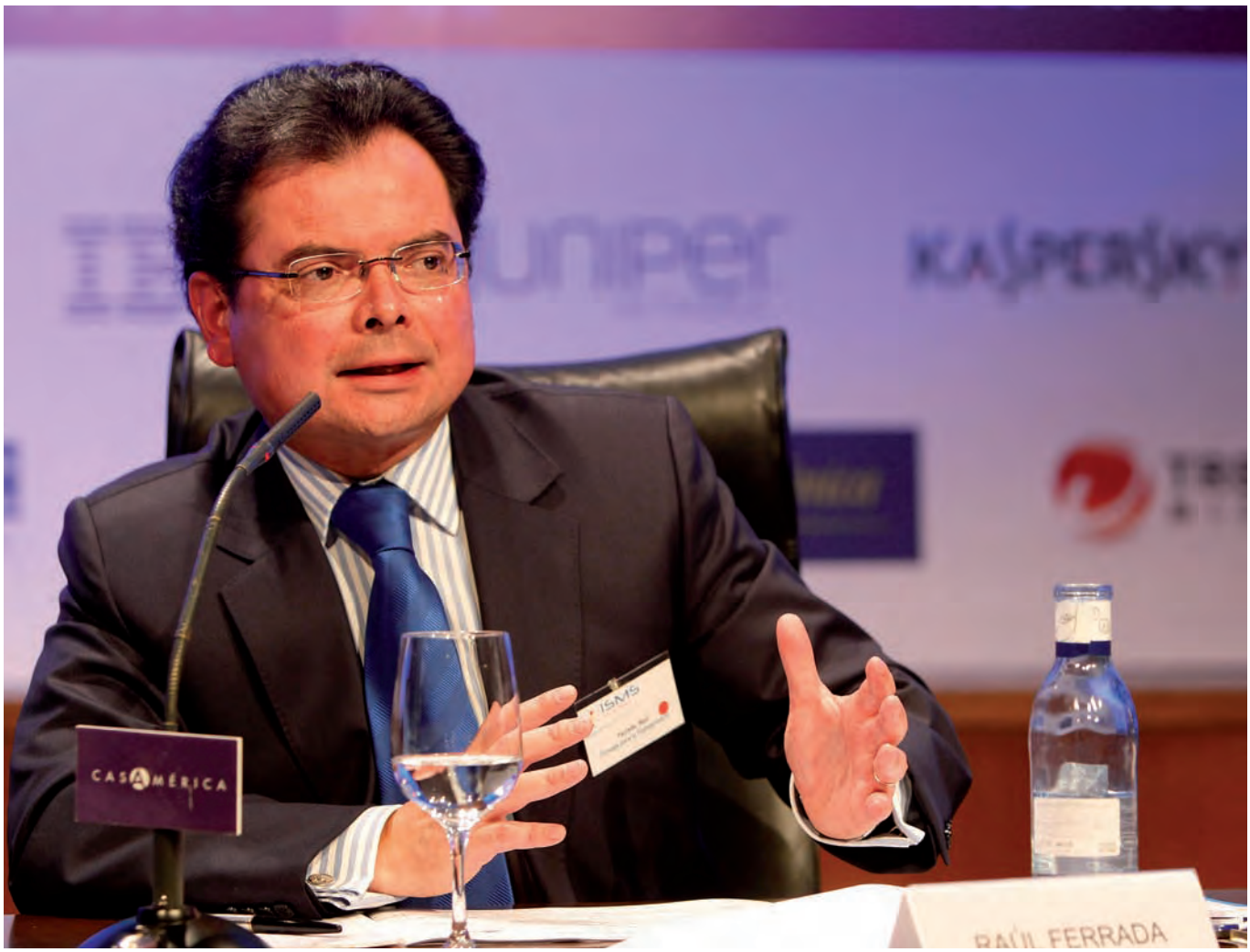
Respecto a los retos para las corporaciones encargadas de la seguridad, Rallo comentó que la AEPD está trabajando en como verificar y forjar modelos de responsabilidad empresarial de carácter preventivo. Marván añadió que los modelos futuros deben ser "tecnológicamente neutrales con una nueva disciplina del análisis de riesgo donde la protección sea proporcional al tipo de datos, el número de datos que se manejan, el tiempo y la sensibilidad de los mismos".

Reputación Corporativa en Internet

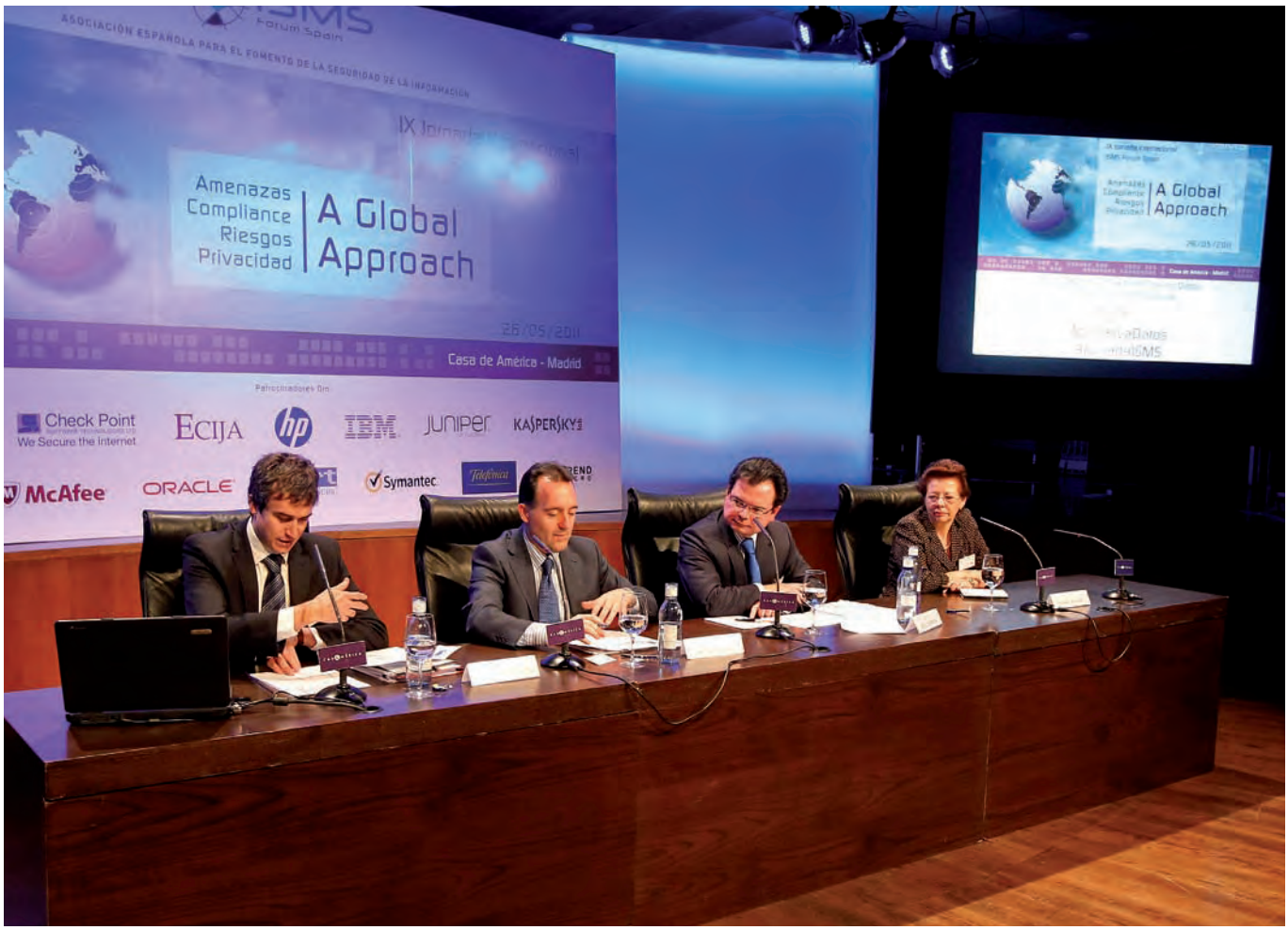
José Manuel Velasco, Director General de Comunicación y Relaciones Corporativas del Grupo FCC, Álvaro Ecija, Socio de Ecija; Consejero de Playtelevision; y José Antonio Gallego, Presidente de la Asociación Española de Responsables de Comunidad (AERCO), debatieron sobre la Reputación Corporativa en Internet, con la moderación de Alfredo Reyes Krafft, CDPP, Vicepresidente de la Asociación Mexicana de Internet; Director de Negocios Digitales e Industria Bancaria en BBVA Bancomer, México.

La mesa redonda empezó con tres formas distintas de entender la imagen corporativa y la reputación.

Para Velasco "la reputación es el premio a una buena gestión de la comunicación. Entendiendo la comunicación como el diálogo con los



Raúl Ferrada.



De izquierda a derecha: Carlos Alberto Saiz, Artemi Rallo, Raúl Ferrada y María Marván.

"Si estás en una organización que es centro de atención, se van a generar contenidos sobre ti, así que la estrategia básica es la anticipación".
José Manuel Velasco, *Grupo FCC.*

grupos de interés. Por tanto yo creo que no se debe gestionar la reputación, sino la comunicación para lograr una buena reputación".

Gallego entiende la imagen corporativa como lo que "los medios transmiten sobre una empresa y la reputación lo que sus clientes opinan de ella". Para Ecija, "una cosa es lo que la empresa quiere decir de ella misma y otra lo que opinen los demás. Claramente con Internet y los medios sociales una empresa está obligada a escuchar lo que están diciendo, ya sea bueno o malo".

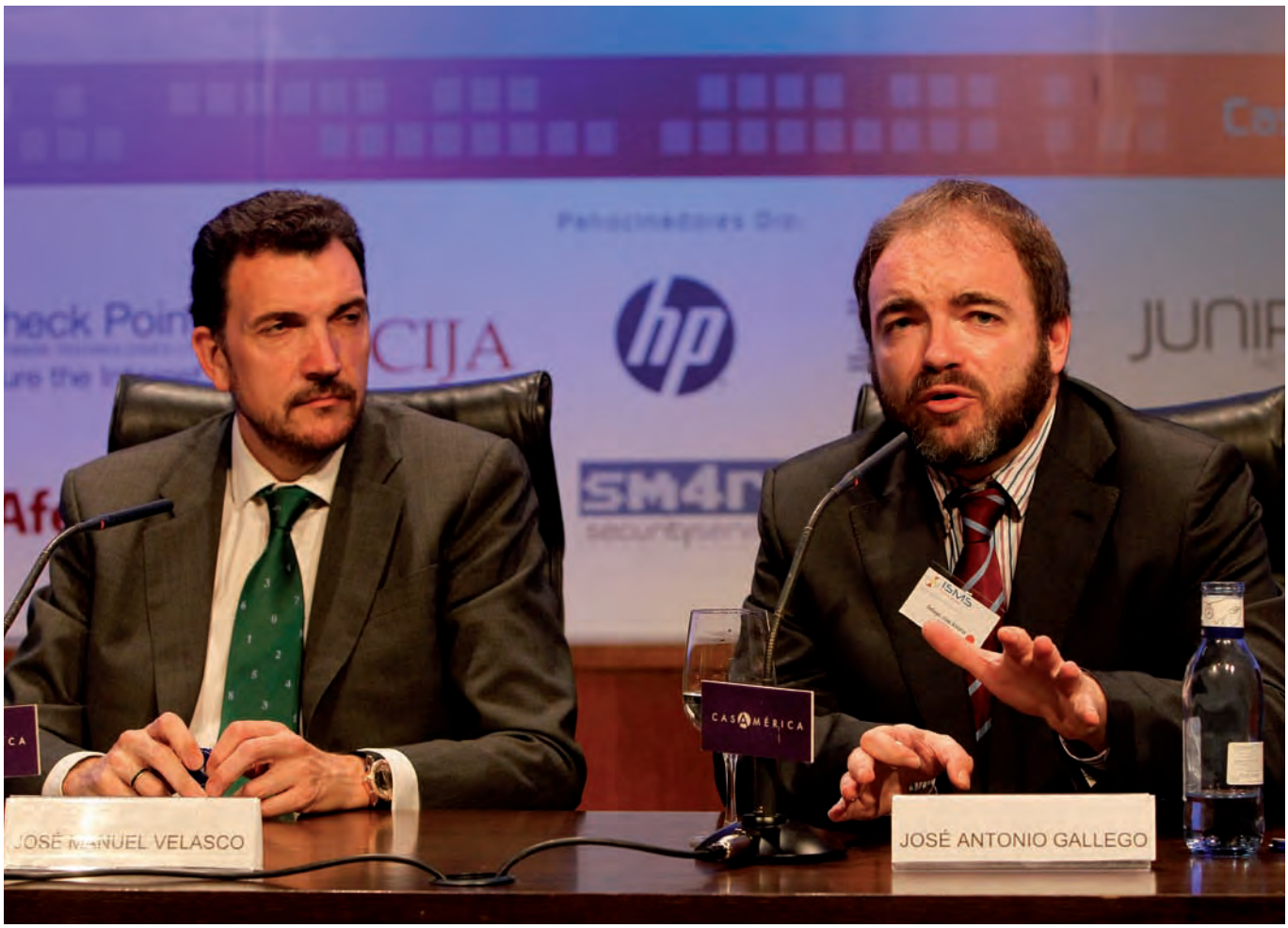
Teniendo claro que las redes sociales han dado pie para que las personas opinen más abiertamente e influyan en la imagen corporativa de una entidad ¿Cómo gestionar las crisis? Los tres participantes estuvieron de acuerdo en que la anticipación, la proactividad y un mensaje bien estructurado son esenciales.

Velasco explicó que con todas las vías de comunicación actual "o comunicas o eres comunicado. Por tanto si estás en una organización que es centro de atención, se van a generar contenidos sobre ti, así que la estrategia básica es la anticipación". Por ello es más importante que nunca la estrategia de mensaje. Según Velasco "tenemos que definir bien qué es lo que vamos a comunicar. Si acertamos, acertaremos mucho, pero si nos equivocamos el error se multiplicará exponencialmente".

Un reglamento eficiente para las empresas y eficaz para las personas

Víctor Chapela, CEO de SM4RT Security Services en México, habló de la "Nueva aproximación del riesgo en seguridad para los reglamentos de privacidad". Chapela aclaró que la clave para que las empresas puedan aplicar las medidas establecidas es que sean fáciles de implementar. De esta manera las empresas "gestionarán la seguridad de la forma más eficiente para ellos, sin que esté en perjuicio la efectividad de esas medidas para el individuo o los titulares a los que queramos proteger".

¿Cómo hacer algo eficiente y efectivo que pueda estar en un reglamento? Chapela explicó varias consideraciones a tener en cuenta con el fin de poder abordar el tema de la privacidad de una manera más sencilla. Primero la Autoregulación de Seguri-



De izquierda a derecha: José Manuel Velasco y Antonio Gallego.

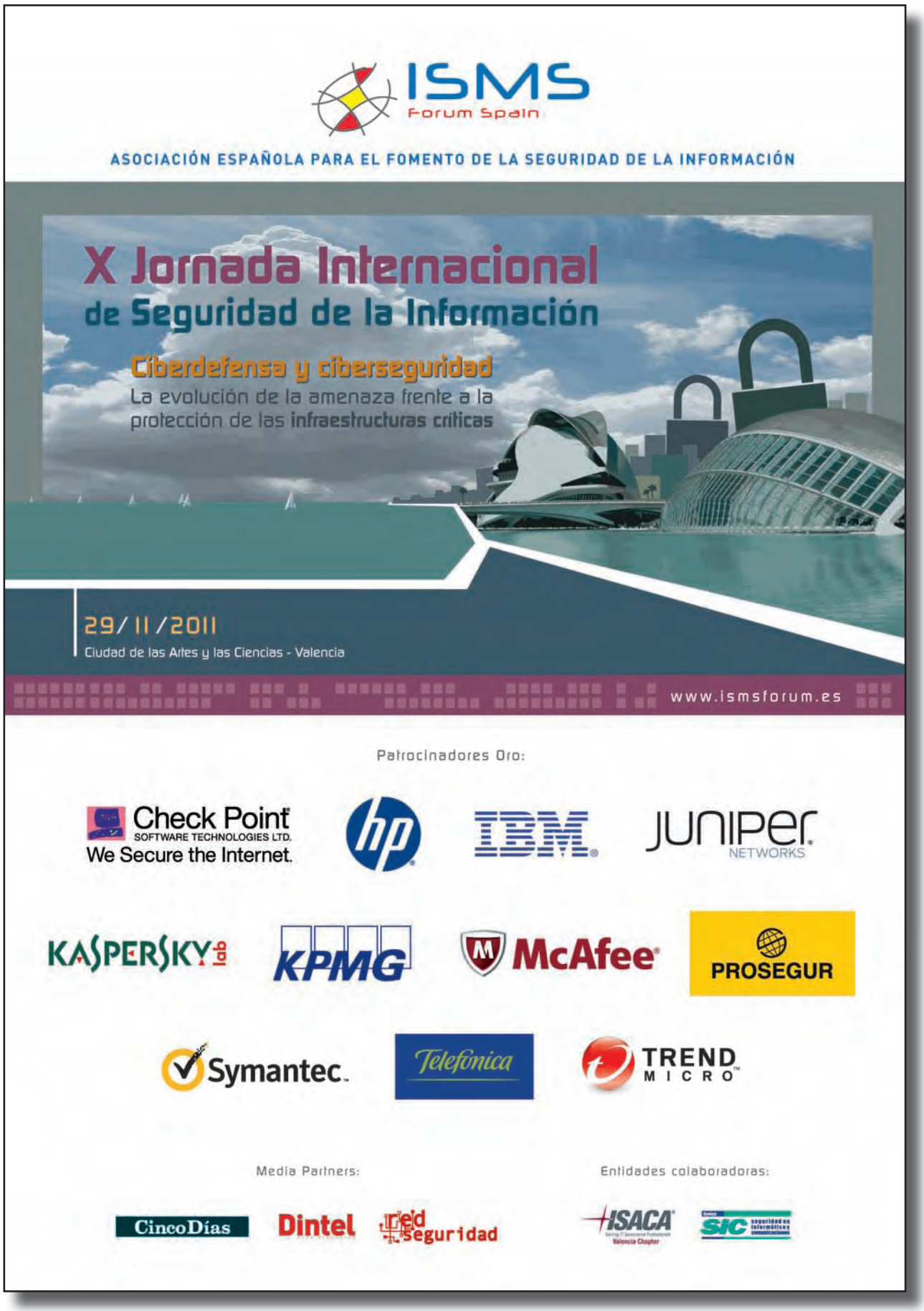
"Las empresas gestionarán la seguridad de la forma más eficiente para ellos, sin que esté en perjuicio la efectividad de esas medidas para el individuo o los titulares a los que queramos proteger".
Víctor Chapela, *SM4RT Security Services.*

dad a través de una tabla de equivalencias. "Por ejemplo: el PSI y el DSS para las tarjetas de crédito. Si yo ya cumplo con PSI entonces por ende ya tengo el mínimo necesario de acuerdo con la ley". Como segundo paso hay que tener en cuenta los tipos de datos que son más sensibles. "En México el secuestro es un problema, entonces hay que proteger los datos que en su conjunto pudieran conllevar un secuestro". La tercera consideración es el cloud computing: no podemos proteger el lugar donde está, pero sí los puntos de acceso a la información. Y, finalmente, el tiempo. "Hay que darles seis meses para definir qué controles necesitan y un año entero para implementarlo".

Se trata de crear un reglamento "que sea eficiente para las empresas y eficaz para las personas".

Víctor Chapela.

Actividades 2011,
X Jornada Internacional



Programa X Jornada ISMS Forum Spain

8:30	**Registro**
9:00 Inauguración	**Palabras de Bienvenida.** **GIANLUCA D'ANTONIO,** Presidente de, **ISMS Forum Spain**; Chief Information Security Officer (CISO) del **Grupo FCC**; Miembro del Consejo de Expertos (PSG) de (**ENISA**). **BRUNO BROSETA DUPRÉ,** Secretario Autonómico del Sector Empresarial, en representación de la **Generalitat Valenciana**.
10:00 Mesa redonda	**Information Security: Setting the Vision and Strategy for the Next Decade.** **BRUNO DARMON,** Vicepresidente, EMEA, **Checkpoint.** **ILIJANA VAVAN,** Vicepresidenta Senior de Ventas Corporativas de Europa, **Kaspersky.** **SIMON YOUNG,** General Manager, Server Security EMEA, **Trend Micro.** Preside: **RAMÓN POCH,** Head of IT Advisory, Risk Consulting **KPMG.**
11:00	**Coffee-break**
11:30 Ponencia	**La Estrategia Española en materia de Ciberseguridad.** **JAVIER CANDAU,** Subdirector General Adjunto del Centro Criptológico Nacional, **CCN.**
12:00 Ponencia	**Why security breaches are ocurring? The Data Breach Investigations Report 2011.** **JELLE NIEMANTSVERDRIET,** Principal Consultant Forensics and Investigative Response, **Verizon Business Security.**
12:30 Mesa redonda	**La Industria de la Seguridad de la Información en España. Retos y oportunidades.** **JOAQUÍN REIXA,** Director General para el sur de Europa, **Check Point.** **JESÚS SÁNCHEZ,** Director General para España y Portugal, **McAfee.** **MARCO BAVAZZANO,** Director Security Strategist Organization, **Symantec.** Preside: **GIANLUCA D'ANTONIO,** Presidente de, **ISMS Forum Spain**; Chief Information Security Officer (CISO). del **Grupo FCC**; Miembro del Consejo de Expertos (PSG) de (**ENISA**).
13:30 Presentación	**Proyectos y actividades de ISMS FORUM SPAIN.** Comité Operativo, **ISMS Forum Spain**.
14:00	**Almuerzo**
15:45 Mesa redonda	**La entrada en vigor de la normativa española en materia de infraestructuras críticas.** **FERNANDO SÁNCHEZ GÓMEZ,** Director Centro Nacional de Protección de Infraestructuras Críticas, **CNPIC.** **MANUEL CANALEJAS,** Director de Consultoría, **Prosegur.** **MANUEL CARPIO,** Director de Seguridad de Infraestructuras y Prevención del Fraude, **Telefónica.** **JOSÉ LUIS BOLAÑOS,** Director de Seguridad y Protección, **Gas Natural Fenosa.** Preside: **JOSÉ DE LA PEÑA,** Director, **Revista SIC.**
16:45 Mesa redonda	**El nuevo panorama de ciberamenazas. Casos de éxito y buenas prácticas.** **MANUEL CORNEJO,** Director de Ingeniería de Sistemas, **Juniper Networks.** **JAVIER SEVILLANO,** Responsable de Seguridad Tecnológica, **Bankia.** **FELIX MARTÍN,** Responsable de desarrollo de negocio de Servicios de Seguridad, **HP.** **JESSICA VALDERRAMA,** , **IBM** Sales Security Leader. Preside: **JESÚS MILÁN LOBO,** Director de Riesgos Tecnológicos y Seguridad Informática, **Bankinter.**
17:45 Ponencia	**El *headhunting* de profesionales y directivos de la Seguridad ¿Qué está demandando el mercado?** **MIGUEL PORTILLO,** Associate Director, **Michael Page Executive Search.**
18:15 Clausura	**Palabras de cierre.**

Principales conclusiones / Por: Juan Antonio Ibáñez

La Ciberseguridad debe considerarse un bien público y requiere la implicación de los Estados y las empresas

Fernando Sánchez Gómez.

La X Jornada Internacional de Seguridad de la Información de ISMS Forum reunió en Valencia a expertos, profesionales, instituciones y empresas de primer nivel para debatir sobre el estado actual de la Ciberseguridad en España. Celebrada en la emblemática Ciudad de las Artes y las Ciencias de Valencia, tuvo como eje principal los retos que se presentan para el sector, con especial hincapié en las nuevas ciberamenazas y la recientemente publicada normativa sobre Protección de Infraestructuras Críticas. Contó con más de 250 asistentes, procedentes de 120 empresas e instituciones.

La bienvenida corrió a cargo de Gianluca D'Antonio, Presidente de ISMS Forum Spain; Chief Information Security Officer (CISO) del Grupo FCC; y Miembro del Consejo de Expertos (PSG) de ENISA; y de Bruno Broseta Dupré, Secretario Autonómico del Sector Empresarial, en representación de la Generalitat Valenciana.

La sesión partió de una idea: la Ciberseguridad debe considerarse como un Bien Público. El Presidente de ISMS Forum abrió la jornada argumentando que la Ciberseguridad es "un deber de Estado" que consiste en garantizar la seguridad y la protección de los derechos y libertades en el ciberespacio. Tal y como plantea la profesora de Berkeley University, Deirdre K. Mulligan, la Ciberseguridad tiene que ser tratada como un Bien Público, equiparable a la Salud Pública. De este modo, el Estado tiene la obligación de asumir un papel rector, estableciendo un marco para el fomento del estado positivo de la seguridad y para el manejo de la inseguridad, una vez que las ciberamenazas se han materializado. En este sentido, España necesita de una estrategia de Ciberseguridad que defina unas metas y objetivos claros, y en la que se establezcan aspectos clave como: a quién se va a asegurar, contra qué amenazas; con qué medios técnicos, educativos, regulatorios; y bajo qué modelo de financiación.

"Existen sectores estratégicos que también necesitan protección, pues ofrecen servicios muy importantes a la sociedad y su fallo puede causar importantes problemas".

Javier Candau, *CCN.*

Esta X Jornada Internacional de ISMS Forum contó con la participación de dos instituciones claves en materia de Ciberseguridad como son el Centro Criptológico Nacional (CCN) y el Centro Nacional de Infraestructuras Críticas (CNPIC), quienes aportaron valoraciones, y expusieron las estrategias estatales de su competencia. Los demás ponentes, representantes de empresas de primer nivel nacional e internacional, tuvieron la oportunidad de debatir y mostrar sus posiciones ante ellas. Así supuso un foro de debate abierto e integrador y, por ello, de gran valor para los asistentes. Participaron multinacionales que lideran el I+D de seguridad como Check Point, HP, IBM, Juniper Networks, Kaspersky, KPMG, McAfee, Symantec, Trend Micro; y empresas españolas de referencia como Bankia, Bankinter, Gas Natural Fenosa, Grupo FCC, Prosegur o Telefónica.

La estrategia española en materia de Ciberseguridad

Javier Candau, Subdirector General Adjunto del CCN argumentó que España ha establecido una "línea mínima de defensa" donde todas las administraciones tienen que verse reflejadas. Se trata de un paso importante, destacó, pero Candau no escatimó argumentos para recalcar que es necesaria una dotación presupuestaria suficiente. Debemos estar en "permanente vigilancia y pensar que la red puede estar comprometida", pero "todo pasa por recursos materiales y económicos", sentenció.

Javier Candau.

Candau explicó que se trata de "la primera referencia que se hace a la ciberamenaza" como un peligro real, haciendo referencia a la estrategia de seguridad aprobada el pasado junio en el Congreso de los Diputados. Así en "las políticas sobre amenazas y riesgos para los próximos cinco años figuran las ciberamenazas", incluyéndose una mención especial a las Infraestructuras Críticas. Precisamente, la X Jornada se centro en buena parte en el análisis del nuevo panorama de ciberamenzas derivadas del rápido progreso tecnológico, en particular las que podrían poner en peligro servicios esenciales para la sociedad, provistos por estas Infraestructuras Críticas del país. El tema tiene una relevancia máxima, pues como consecuencia de fallos de seguridad o de ciberataques terroristas, por ejemplo, se podrían producir, además de millones de euros en pérdidas, víctimas humanas.

Por ello, Candau comentó que hay que proteger las Infraestructuras Críticas, pero éstas, en sentido estricto, son sólo las consideradas y clasificadas como críticas para el Estado, existiendo otras infraestructuras que aún no "siendo apellidadas como críticas" también hay que protegerlas. Por eso hay que matizar que hay sectores muy relevantes que "pueden no ser clasificados como 'críticos' desde la Administración; y sufren muchos ataques". Por eso "existen sectores estratégicos que también necesitan protección", pues ofrecen servicios muy importantes a la sociedad y su fallo puede causar importantes problemas" explicando la visión global de la estrategia aprobada.

"Se requiere de una colaboración público-privada, que es la base de un adecuado estado de seguridad".
Fernando Sánchez Gómez, *CNPIC*.

Colaboración público-privada en la protección de IC

Este año 2011 ha sido clave para establecer el marco legal en materia de Infraestructuras Críticas, ya que se publicaron la Ley 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas y el Real Decreto 704/2011 por el que se aprueba el Reglamento para la Protección de las Infraestructuras Críticas, que son definidas como "el conjunto de recursos, servicios, tecnologías de la información y redes, que en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación".

El análisis de la normativa recientemente aprobada correspondió a Fernando Sánchez Gómez, Director del Centro Nacional de

"Es más imprescindible que nunca unirse para encontrar la mejor forma de defenderse en la próxima década".

Bruno Darmon, *Checkpoint*.

Protección de Infraestructuras Críticas, CNPIC; Manuel Canalejas, Director de Consultoría, Prosegur; Manuel Carpio, Director de Seguridad de Insfraestructuras y Prevención del Fraude, Telefónica; y José Luís Bolaños, Director de Seguridad y Protección, Gas Natural Fenosa; en un debate conducido por José de la Peña, director de la revista SIC. Los ponentes trataron temas relacionados con la implantación de la normativa, el nivel de madurez de las empresas españolas en seguridad, y la necesaria interlocución público-privada, uno de los retos fundamentales para los próximos años, ya que como aseguró el director de CNPIC: "El espíritu de la ley es la coordinación de todos los actores", ya que no en vano en la protección de las Infraestructuras Críticas intervienen tanto la Administración como las empresas. Por ello, se requiere de una colaboración público-privada, que es "la base de un adecuado estado de seguridad".

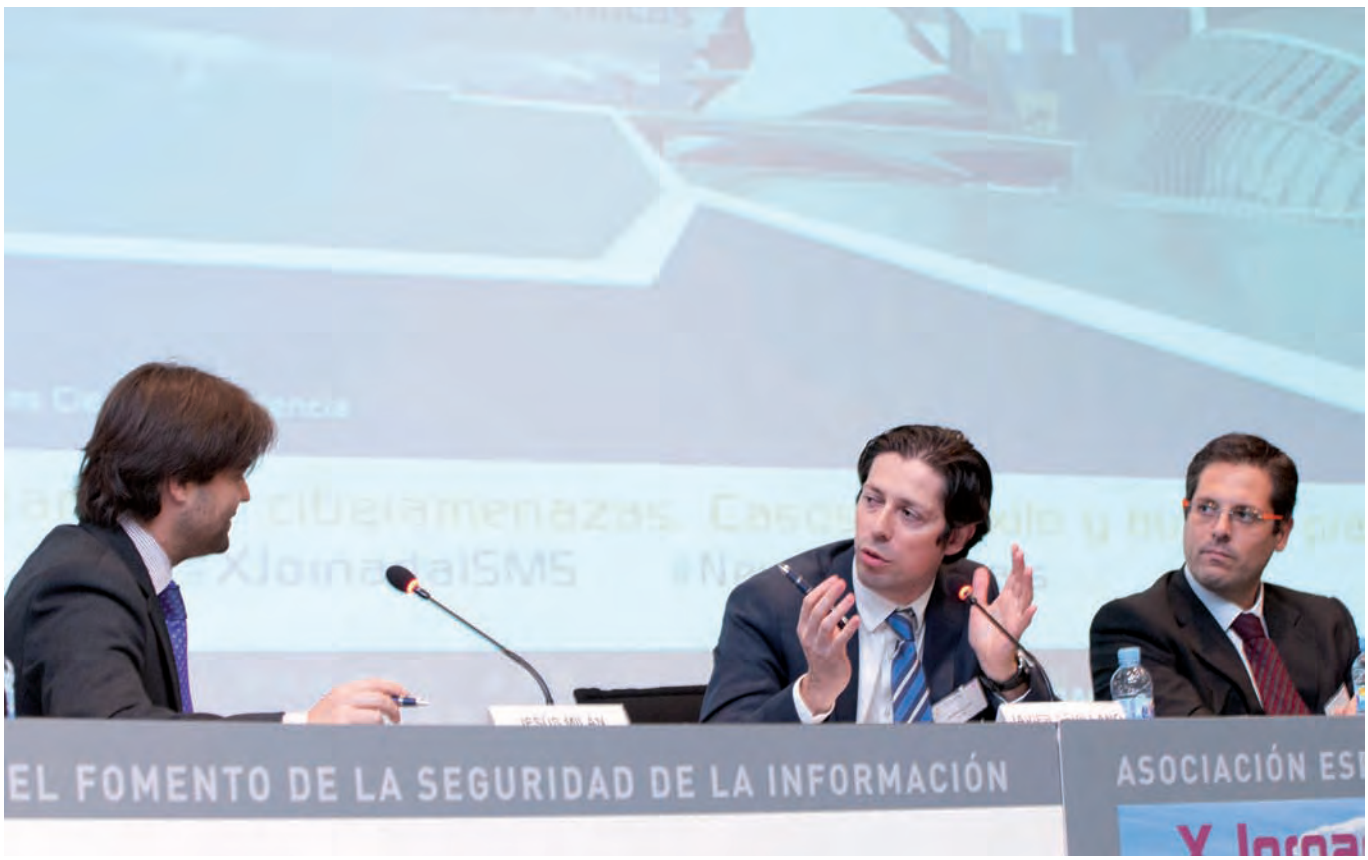
De hecho, las empresas protegen sus Infraestructuras Críticas desde que se crean, por lo que cuentan con una experiencia muy valiosa. Como comentó Manuel Carpio, desde los años 20 Telefónica "se ha ocupado de proteger las Infraestructuras Críticas para ofrecer el servicio y para garantizar la continuidad del negocio. En este sentido el impacto de la Ley es mínimo".

Según Sánchez la Ley sólo establece "un sistema de mínimos y no entra a valorar" los mecanismos que ponen en marcha las empresas para proteger sus Infraestructuras Críticas, si son eficaces, eficientes y si están probados. Y es que se trata de una gestión vital para ellas, ya que garantizan la prestación del servicio y la respuesta ante los daños originados por posibles ciberataques. "No vamos a decir a una empresa con mucha experiencia al respecto cómo lo tiene que hacer", aseguró.

"Esta no es una Ley más, no es una ley convencional. Tiene unas características que la diferencia de las demás. No es una carga impositiva más. Si no que es algo que va más allá. De lo que se trata es de crear una política de protección de Infraestructuras Críticas en la que participemos todos". Así, aseguró que el Real Decreto impulsa toda esta política de cooperación para enmarcar un camino, sin que exista un ánimo de sanción.

Desde el punto de vista de las empresas, en general, se mostró su acuerdo a las afirmaciones del director del CNPIC. José Luís Bolaños destacó que efectivamente la colaboración de las administraciones públicas es esencial. "El problema no se resuelve con medios y recursos de las empresas proveedoras", si no que es necesaria la colaboración de la administración, estableciendo unas bases y reglas del juego, y el "apoyo efectivo de las fuerzas de seguridad el Estado y de las autonomías en la prevención y reacción cuando ocurren las cosas y para que no se vuelvan a repetir", aseveró. "Las empresas han invertido, pero eso no resuelve la película".

En cuanto al cumplimiento normativo, Manuel Carpio comentó que "estamos preparados de acuerdo a lo que dice la Ley".



De izquierda a derecha: Jesús Millán, Javier Sevillano y Manuel Cornejo.

"Los Estados necesitan controlar la seguridad para facilitar que las economías crezcan".

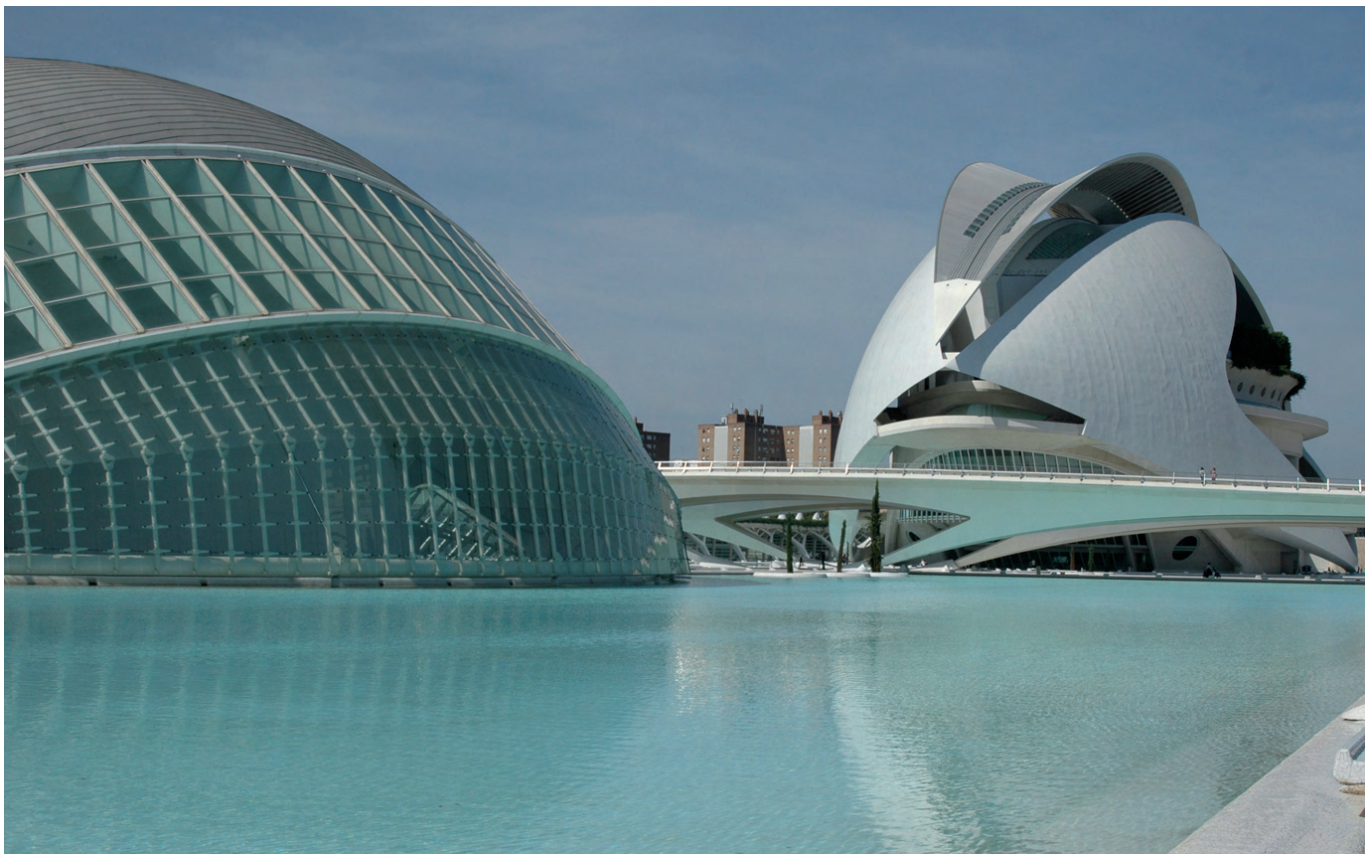
Simon Young, *EMEA*.

Jelle Niemantsverdriet.

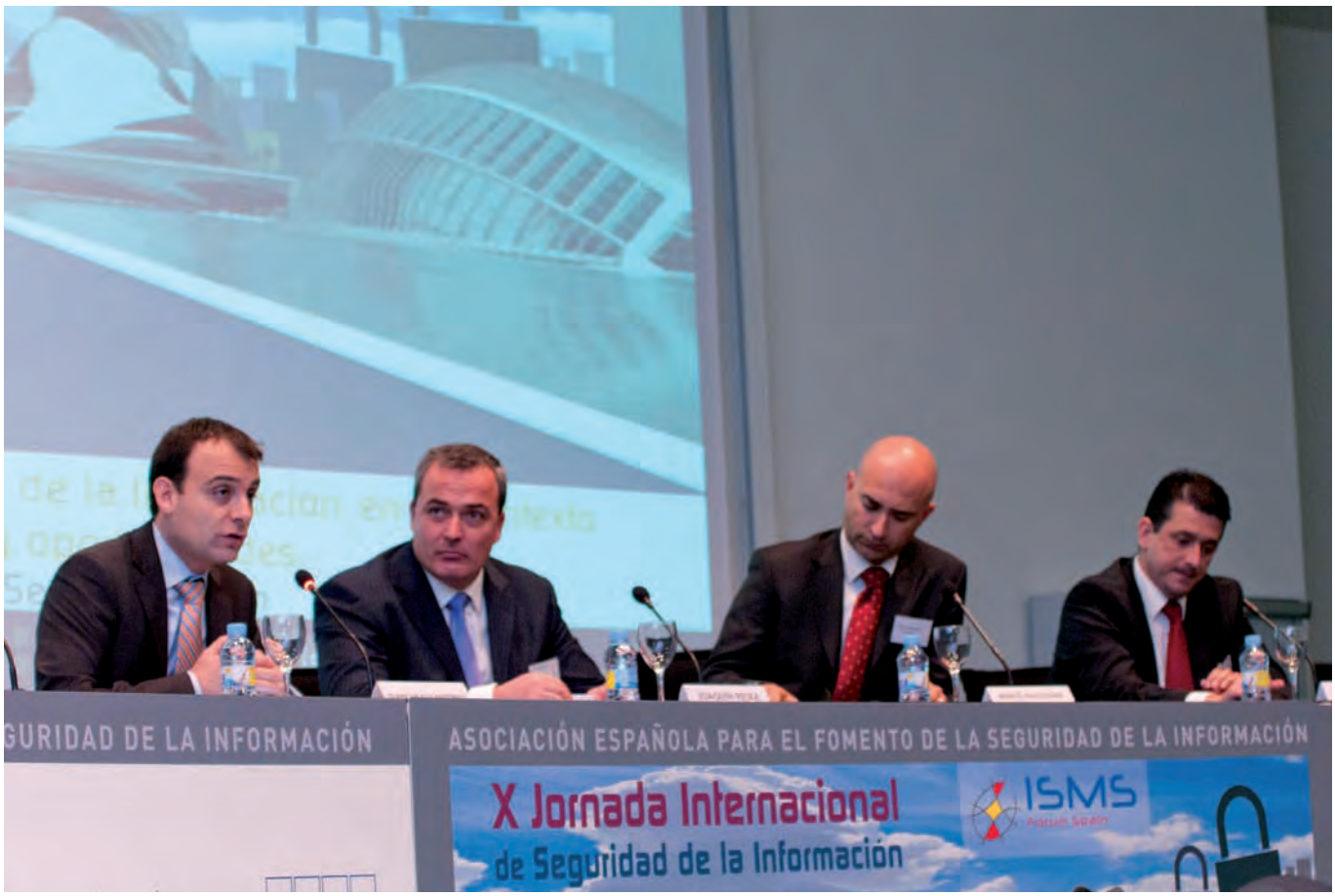
Bolaños valoró además que el "concepto de Infraestructuras Críticas para nosotros tiene un matiz especial con respecto a nuestros clientes y los servicios que proporcionamos a la sociedad", quien también destacó la importancia de llevar a cabo una gestión global dentro de las empresas. "No podemos estar en departamentos estancos". En este sentido también se pronunció Manuel Canalejas: "Si todas las estrategias no forman parte de una estrategia global de seguridad nunca llegaremos al punto final que es conseguir que la empresa o la infraestructura sea segura".

Con respecto a la legislación aplicable, Canalejas interpeló al CNPIC: "me gustaría ver mucha más concreción en la exigencia" y "me encantaría ver muy concreto y desarrollado como va ser el tema de coordinación. Cómo nos vamos a comunicar unos con otros y cómo vamos a actuar en casos de emergencia".

Por último, para el director del CNPIC "el grado de madurez de la protección en España es muy alto a nivel general", ya que debido a la amenaza del terrorismo ha sido necesario en las últimas décadas prepararse ante posibles ataques. "De lo que se trata es de impulsar un tema que a medio y largo plazo propicie un cambio de cultura de la seguridad que algunos lo perciben de una forma más intensa y otros no lo perciben o no quieren percibir", concluyó.



Ciudad de las Artes y las Ciencias de Valencia, lugar donde se celebró el evento.



De izquierda a derecha: Gianluca D'Antonio, Joaquín Reixa, Marco Bavazzano y Jesús Sánchez.

Nuevo panorama de ciberamenazas

El rápido progreso tecnológico y los nuevos usos generan nuevas amenazas de seguridad. De gran actualidad son aquellas vinculadas a la tendencia de la movilidad y el denominado cloud computing, que permite, entre otras cosas, almacenar información en servidores de forma deslocalizada, que puede ser consultada a través de Internet y mediante múltiples dispositivos. Así se han producido fenómenos como la desaparición de los tradicionales perímetros corporativos y la generalización de los movimientos de la información, incluso con carácter transfronterizo. Esto representa un reto tanto para los Estados, las empresas y para la ciudadanía en general.

Durante la X Jornada Internacional también se abordó el panorama actual de la ciberamenaza, que Félix Martín, Lead Solution Consultant, HP, describió como "un nuevo paradigma", provocado por un mayor interés de los negocios hacia el ciberespacio, una tendencia cultural a dar más información en detrimento de la privacidad y el cambio tecnológico unido a la globalización. Entre los problemas más debatidos en la sesión, además de los vinculados a la movilidad y al cloud, se encontraron los ataques dirigidos, los ataques de denegación de servicios (DDoS), los ataques persistentes (APT) y las vulnerabilidades del software, entre otros.

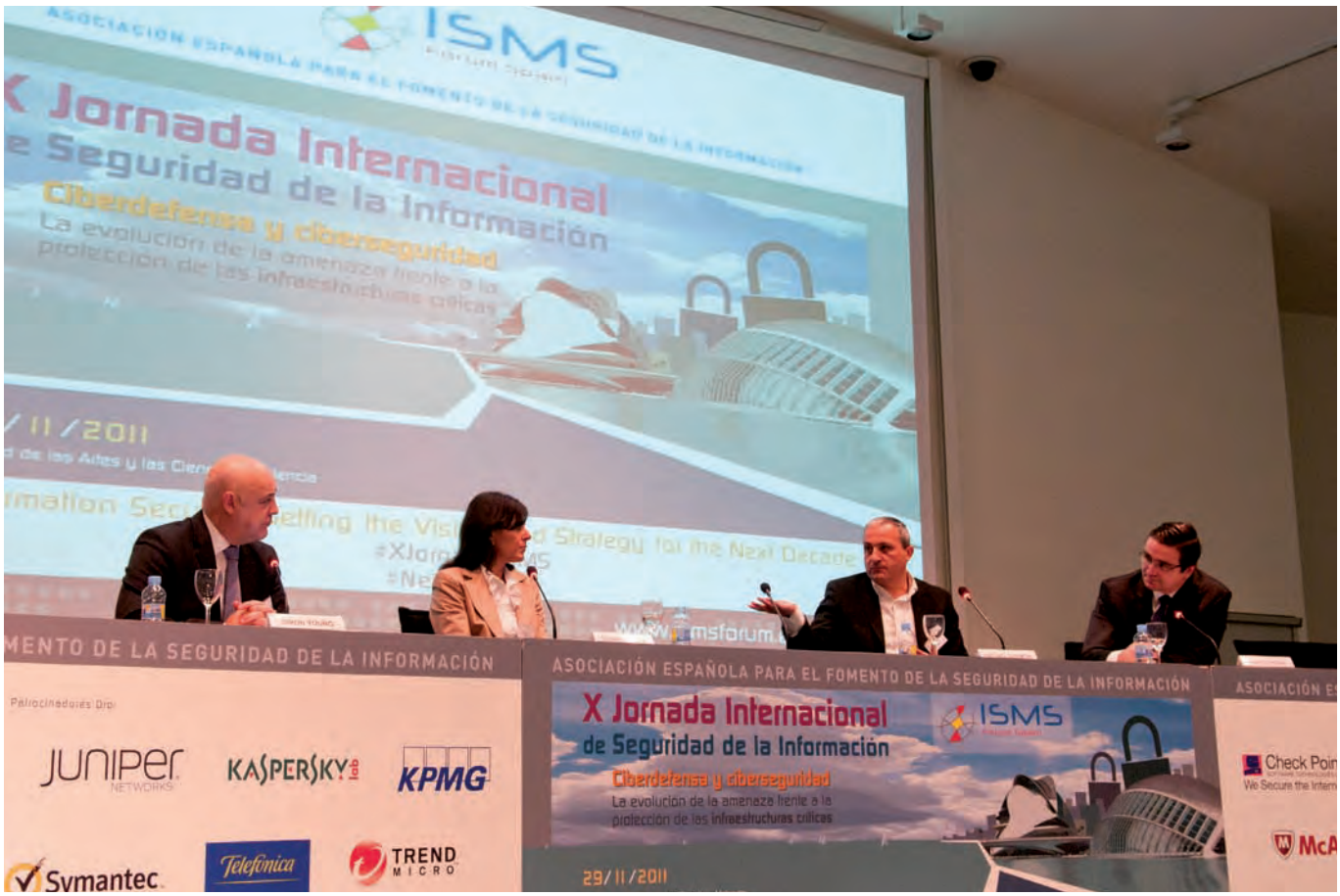
"En cuanto a la madurez de las empresas españolas en materias de seguridad estamos algún paso por delante con relación al control de fugas de información".

Jesús Sánchez, *McAfee*.

Félix Martín participó en un debate conducido por Jesús Milán, miembro de la Junta Directiva de ISMS Forum, Director de Seguridad, Bankinter; junto a Manuel Cornejo, Director de Ingeniería de Sistemas, Juniper Networks; Javier Sevillano, Responsable de Seguridad Tecnológica, Bankia y Jessica Valderrama, IBM Sales Security Leader.

En lo referente a vulnerabilidades, Martín confirmó que se mantiene la tendencia desde 2006. Las vulnerabilidades decrecen en número, sobre todo en software comercial, según datos recogidos por HP. El punto crítico lo aportó Javier Sevillano. "¿Por qué llevamos muchos años tapando agujeros y nunca conseguimos que estén tapados?", se preguntó. Así, argumentó que cree que hay un problema de modelo, porque "a nuestro juicio el que tiene la responsabilidad de los agujeros no es aquel que es capaz de arreglarlo".

Con respecto a la movilidad, Manuel Cornejo resaltó los cambios de comportamiento de los usuarios ante los nuevos dispositivos. Es un reto importante para los próximos años "securizar esos nuevos entornos", ya que se demuestra que, en general, los usuarios están menos concienciados y no tienen en cuenta los aspec-



De izquierda a derecha: Simon Young, Ilijana Vavan, Bruno Darmon y Ramón Poch.

tos de seguridad. Por ello, consideró pertinente recordar que "el usuario es el eslabón más débil de la cadena".

Otro aspecto importante destacado por Cornejo es la necesidad de compartir la información sobre los ciberataques sufridos. "Para poder crear una inteligencia, para ser más proactivo; o compartimos información o no funciona", aseveró.

Los ciberdelincuentes sofistican sus ataques a empresas y Estados

Los retos de la Seguridad de la Información para la próxima década fueron debatidos en una mesa internacional formada por Bruno Darmon, Vicepresidente, Checkpoint; Ilijana Vavan, Directora Corporativa en Europa, Kaspersky; Simon Young, Director General, EMEA, Trend Micro; y conducida por Ramón Poch, Head of IT Advisory, KPMG.

Los ponentes coincidieron en destacar que todos los agentes implicados deben comprometerse y colaborar, tanto a nivel local como global, para mejorar la seguridad. Si se quiere alcanzar un grado de prevención óptimo "necesitamos trabajar todos juntos: las empresas, los gobiernos y los individuos", opinó Ilijana Vavan.

Los ciberdelincuentes forman un colectivo poderoso, que cuentan con organizaciones criminales y motivaciones económicas detrás. Se ha producido, además, una sofisticación de la amenaza en los últimos años. "Es más imprescindible que nunca unirse para encontrar la mejor forma de defenderse en la próxima década", continuó Bruno Darmon, destacando que han aumentado los ataques selectivos; mientras que Simon Young alertaba sobre los grandes riesgos que surgen del uso de los medios sociales, la movilidad y el cloud computing.

"En España el sector de la Seguridad de la Información probablemente sea uno de los menos afectados por la crisis porque las empresas tienen la necesidad de proteger sus activos".
Joaquín Reixa, *Checkpoint*.

De este modo, una red más regulada podría ser una ayuda para mejorar la seguridad. Young destacó que los requerimientos legales para las empresas, destinados a garantizar la seguridad de la información y la protección de datos personales, "deberían ser más fuertes" y también que los gobiernos tendrían que desarrollar nuevos marcos legales para servicios como el cloud. De la misma opinión fue Vavan, quien propuso, además, crear mecanismos para "la identificación de quien entra en Internet". Por su parte, Darmon matizó que es muy importante ligar la implementación de la regulación a la concienciación de los empleados para conseguir la protección adecuada.

Tal y como destacó Vavan, es muy necesario educar a toda la ciudadanía sobre qué riesgos hay en Internet. La colaboración de los gobiernos es imprescindible en este sentido, quienes, por otro lado, se están empezando a dar cuenta de que las amenazas y riesgos son reales y graves, tanto para las personas como para las empresas.

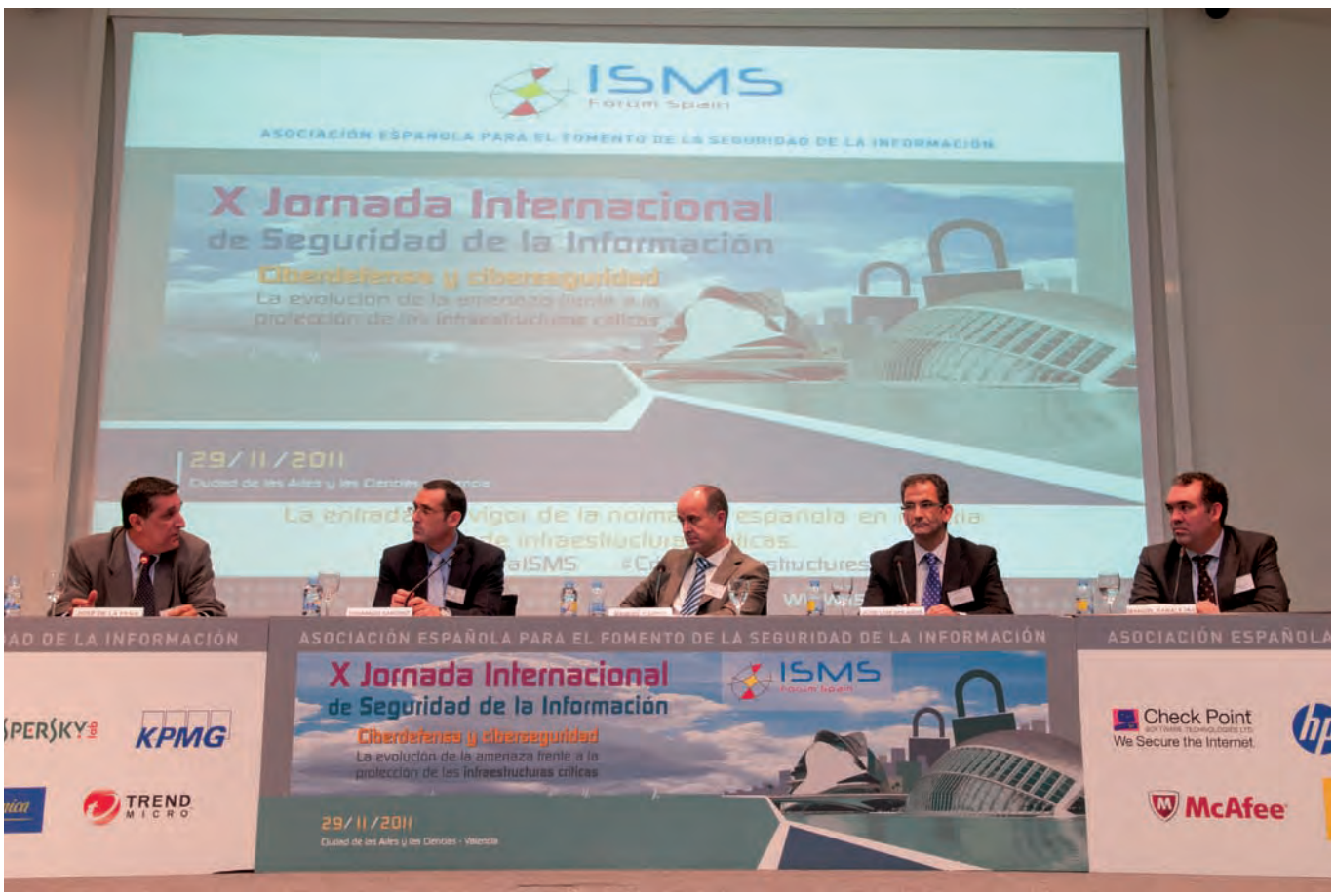
Auditorio.

En este sentido, los Estados "necesitan controlar la seguridad para facilitar que las economías crezcan. Todo depende del conocimiento y la información", declaró Young, poniendo como ejemplo la estrategia nacional aprobada en Gran Bretaña, que incluye políticas activas e importantes partidas presupuestarias.

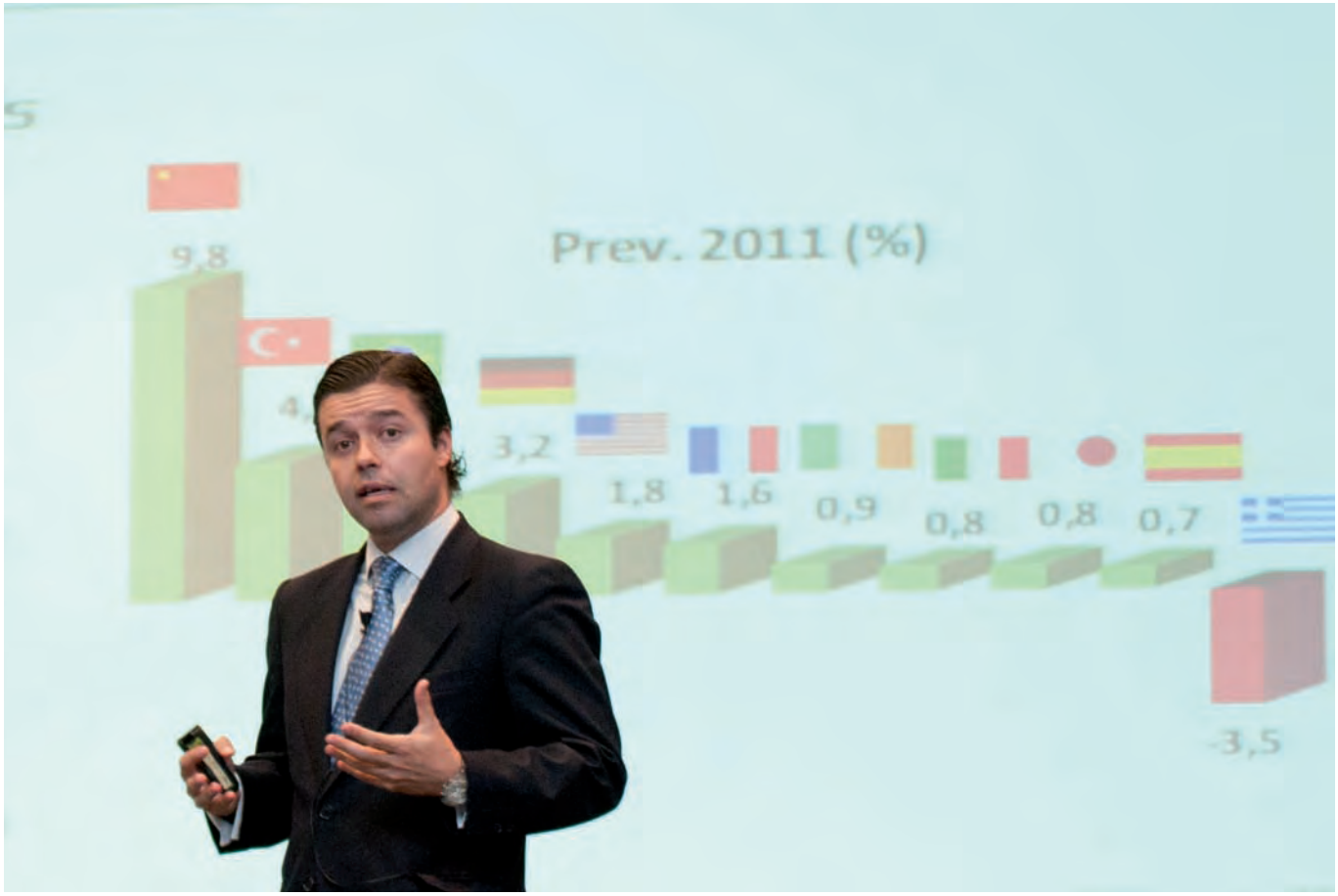
La industria en España

En la mesa dedicada a las oportunidades de la industria de la Seguridad de la Información en el contexto nacional, Marco Bavazzano, Director Security Strategist Organization, Symantec, y Gianluca D'Antonio, Presidente de ISMS Forum Spain; Chief Information Security Officer (CISO), Grupo FCC; y Miembro del Consejo de Expertos (PSG), ENISA; también situaron como punto de referencia el modelo inglés por su búsqueda de un espacio ciberseguro como garantía y atracción para los negocios.

Ambos compartieron mesa con Joaquín Reixa, Director General para el sur de Europa, Checkpoint; y Jesús Sánchez, Director General para España y Portugal, McAfee; quien destacó, en cuanto a la madurez de las empresas españolas en materia de seguridad, que "estamos algún paso por delante" con relación al control de fugas de información. También España es pionera en la aplicación de algunas medidas como el cifrado, coincidió Reixa, quien relacionó además esta situación con el grado de regulación, que es muy alto, con respecto a otros países del entorno, en especial, en materia de protección de datos de carácter personal.



De izquierda a derecha: José de la Peña, Fernando Sánchez, Manuel Carpio, José Luis Bolaños y Manuel Canalejas.



Miguel Portillo.

Por otro lado, Bavazzano opinó, tomando como referencia la demanda del mercado, que se debe de ir hacia soluciones integradas y convergentes. "Como proveedor, encontramos que vamos algunos pasos por delante de la necesidad. Desde un punto de vista de convergencia la necesidad creo que existe", explicó.

Desde un enfoque económico, Joaquín Reixa opinó que en este momento en España el sector de la Seguridad de la Información "probablemente sea uno de los menos afectados por la crisis porque las empresas tienen la necesidad de proteger sus activos". "Aunque siempre existe el riesgo de la falta de presupuesto", matizó.

Brechas de seguridad

Jelle Niemantsverdriet, Principal Consultant Forensics and Investigative Response, Verizon Business Security, analizó la materialización de brechas de seguridad en las organizaciones, ayudándose de las conclusiones del "Data Breach Investigations Report 2011". Según éste, se robaron 3,8 millones de registros en 2010, una cifra significativamente más baja con respecto a estudios previos (en 2009, por ejemplo, se registraron 143,6 millones), comentó.

En su opinión, un elemento reseñable es que se está mostrando un cambio de tendencia en los robos. Debido a la presión, se sospecha que los nuevos delincuentes "van a por los pequeños conejos, no a por el gran elefante", declaró. Es decir, ahora los ciberdelincuentes atacan muchas pequeñas compañías, a quienes sustraen menos datos. El problema grave que surge es que "se está extendiendo esta práctica y es mucho más difícil de detectar que las anteriores".

Por otro lado, Niemantsverdriet resaltó la relevancia de los logs en la investigación de las brechas de seguridad. "Es fácil. Todo lo que se necesitan son logs. Todo está en esos logs", declaró, por lo que resulta vital leerlos y saberlos interpretar adecuadamente. Para la prevención, recomendó centrarse en un conjunto de medidas básico, basándose en los procesos y las personas antes que en aumentar la inversión y mejorar la tecnología. "Mucho se podría haber evitado cumpliendo sólo con lo básico", comentó. También hizo hincapié en la necesidad de monitorizar al personal interno, elaborar un plan de respuesta revisable anualmente y colaborar con la policía y los servicios secretos para compartir información.

El profesional de la Seguridad de la Información

En la jornada también se dedicó un espacio al profesional de la Seguridad de la Información, en el que se habló de perfiles y la situación del mercado laboral. Para ello, se contó con Miguel Portillo, Associate Director, Michael Page Executive Search, quien explicó que debido a la crisis "hay menos procesos de selección pero son muy buenas oportunidades". También destacó que cada vez hay una mayor concentración geográfica, sobre todo hacia Madrid. En cuanto a salarios comentó que "en España se paga mal, entre un 20 o 30 % por debajo de los vecinos de la Unión Europea".

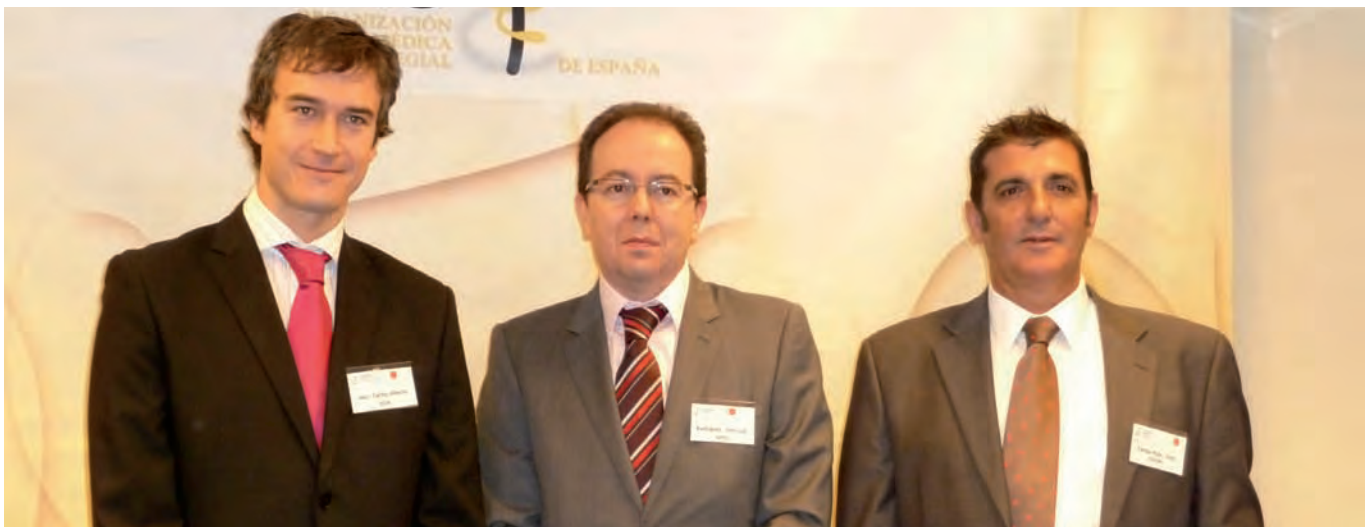
Actividades 2011, Data Privacy Institute (DPI) /

Por: Juan Antonio Ibáñez

I Foro DPI 21-01-2010	Recetas para la Privacidad de Datos.
II Foro DPI 23-05-2010	Dos años de Reglamento de la LOPD.
III Foro DPI 03-11-2010	Problemas actuales en Privacidad y la Seguridad de la Información.
IV Foro DPI 18-10-11	Estado actual de la Protección de Datos y próximos retos.

Conclusiones del IV Foro DPI

La protección de datos ante las grandes transformaciones tecnológicas y la globalización

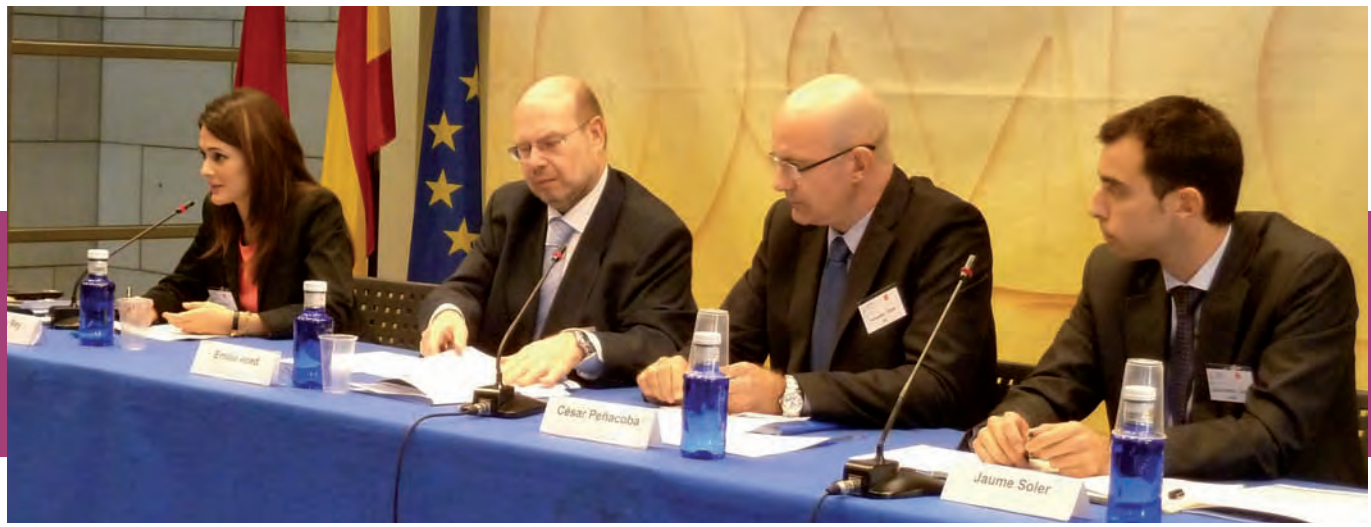


De izquierda a derecha: Carlos Alberto Saiz, José Luis Rodríguez y Joan Camps Pons.

La Protección de Datos se enfrenta a retos que hace muy pocos años eran impensables. El progreso tecnológico y la globalización, han hecho emerger un nuevo escenario donde surgen riesgos y debates sobre conceptos como el derecho al olvido o la aplicación de la normativa en entornos en los que la información fluye a nivel internacional y los datos están deslocalizados bajo modelos de cloud computing. Como escenario de reflexión y debate, el Data Privacy Institute (DPI) de ISMS Forum Spain reunió en el IV Foro de la Privacidad, que tuvo lugar en Madrid el 18 de octubre en Madrid, a varios de los actores implicados en el sector, tanto empresas de referencia (**Écija, Tuenti, KPMG, Telefónica, HP, Mapfre, Cepsa, Symantec, Grupo Prisa**) como expertos y representantes de organismos públicos (**Agencia Española de Protección de Datos, la Agencia Madrileña de Protección de Datos y la Agencia Catalana de Protección de Datos**).

Bajo el título de "Estado actual de la protección de datos y próximos retos", el evento hizo especial hincapié en los cambios normativos y en los desafíos que presentan los nuevos servicios y prácticas en Internet, como el cloud computing, el behavioral marketing o las redes sociales; que han crecido de forma exponencial, tanto en el ámbito empresarial como en el personal. Además se analizaron las primeras resoluciones tras la reforma del régimen sancionador de la Ley Orgánica de Protección de Datos (LOPD). La sede del Consejo General de Colegios de Médicos, miembro fundador de ISMS Forum acogió este IV Foro de la Privacidad debido a la importancia que para el colectivo tiene la Protección de Datos de los pacientes y de su compromiso con la privacidad.

"Estamos necesitados de una actualización del marco legal". José Luís Rodríguez Álvarez, ***Agencia Española de Protección de Datos (AEPD).***



De izquierda a derecha: Nathaly Rey, Emilio Aced, César Peñacoba y Jaume Soler.

El director de la **Agencia Española de Protección de Datos** (AEPD), José Luís Rodríguez Álvarez, fue el encargado de la apertura de honor con una ponencia sobre los retos de la Protección de Datos en los próximos años, aunque hizo énfasis en el estado actual, caracterizado por una normativa que podría haber quedado obsoleta para algunos problemas surgidos por un progreso tecnológico acelerado. "Estamos necesitados de una actualización del marco legal", haciendo referencia a la Directiva 95/46/CE. "Los avances tecnológicos plantean continuamente nuevos retos para todas las instituciones que no son fáciles de abordar con las normativas actuales", explicó. Aunque precisó que en España "contamos con un alto nivel de garantía de los datos personales, por encima de muchos países de nuestro entorno". También apeló a la responsabilidad de las empresas en el respecto a la protección de los datos personales, así como a la ciudadanía general a exigir el cumplimiento de la legislación. "Yo creo que la conciencia de los ciudadanos de todos estos riesgos moverá a incrementar los niveles de protección. Lo será más cuando haya una mayor competencia", apostilló a modo de comentario personal.

Con respecto a las redes sociales, declaró que es imprescindible un mayor compromiso de las compañías en la protección de los menores de la red, urgiendo que se perfeccionen metodologías que permitan comprobar la edad mínima exigida para participar en ellas. Asimismo, para Rodríguez Álvarez, el cloud computing no se puede convertir en una vía para eludir la normativa de Protección de Datos y advirtió a los usuarios que "quien contrata responde con arreglo a la legislación española", haciendo referencia a la necesidad de revisar de forma exhaustiva las cláusulas contractuales.

"Hay posibilidad de que las autoridades de control españolas actúen en cloud computing". Emilio Aced, ***subdirector general de la Agencia Madrileña de Protección de Datos.***

Precisamente el respeto a la privacidad y la seguridad en el cloud computing fue uno de los aspectos abordados profusamente en la jornada, ya que se trata de un fenómeno emergente que permite transferencias internacionales de datos personales y el almacenamiento de estos en servidores repartidos en distintos países del mundo, con legislaciones distintas. De ahí que tanto los miembros de la práctica de seguridad de **HP** y **KPMG**, César Peñacoba y Jaume Soler, respectivamente, como el subdirector general de la **Agencia Madrileña de Protección de Datos**, Emilio Aced, destacaran, en línea con la opinión del director de la AEPD, el valor de la auditoría y la contratación de proveedores fiables, cuyos propios contratos incluyan el respeto explícito a la ley nacional sobre Protección de Datos, allí donde los datos se gestionen. "Hay posibilidad de que las autoridades de control españolas investiguen y actúen porque contractualmente debe de estar contemplado", aseguró Aced.

"Tenemos que saber qué información nuestra se está publicando". Ramón Miralles, ***coordinador de Auditoría y Seguridad de la Información de la Agencia Catalana de Protección de Datos.***

El concepto de derecho al olvido fue uno de los más discutidos en la jornada. El director de la AEPD, alertó que lo "que está en juego es qué tipo de sociedad queremos. Una en la que las personas puedan cambiar o una sociedad en la que el recuerdo permanente del pasado impida la reinserción o nos coarte o no nos deje desarrollarnos como personas". En lo estrictamente legal Rodríguez Álvarez explicó que las personas deben de poder ejercer los derechos de cancelación también en Internet. Se trata de retos que apelan al legislador, pero también a la industria que está obligada a "atender las peticiones de los ciudadanos con respecto a la Ley de Protección de Datos".

Otros ponentes, durante la jornada aportaron perspectivas diferentes al respecto. El coordinador de Auditoría y Seguridad de la Información de la **Agencia Catalana de Protección de Datos**, Ramón Miralles, a título personal, habló de la idea de la "autodeterminación informativa". "El Derecho al Olvido no existe",

De izquierda a derecha: Ricard Martínez y José López Calvo.

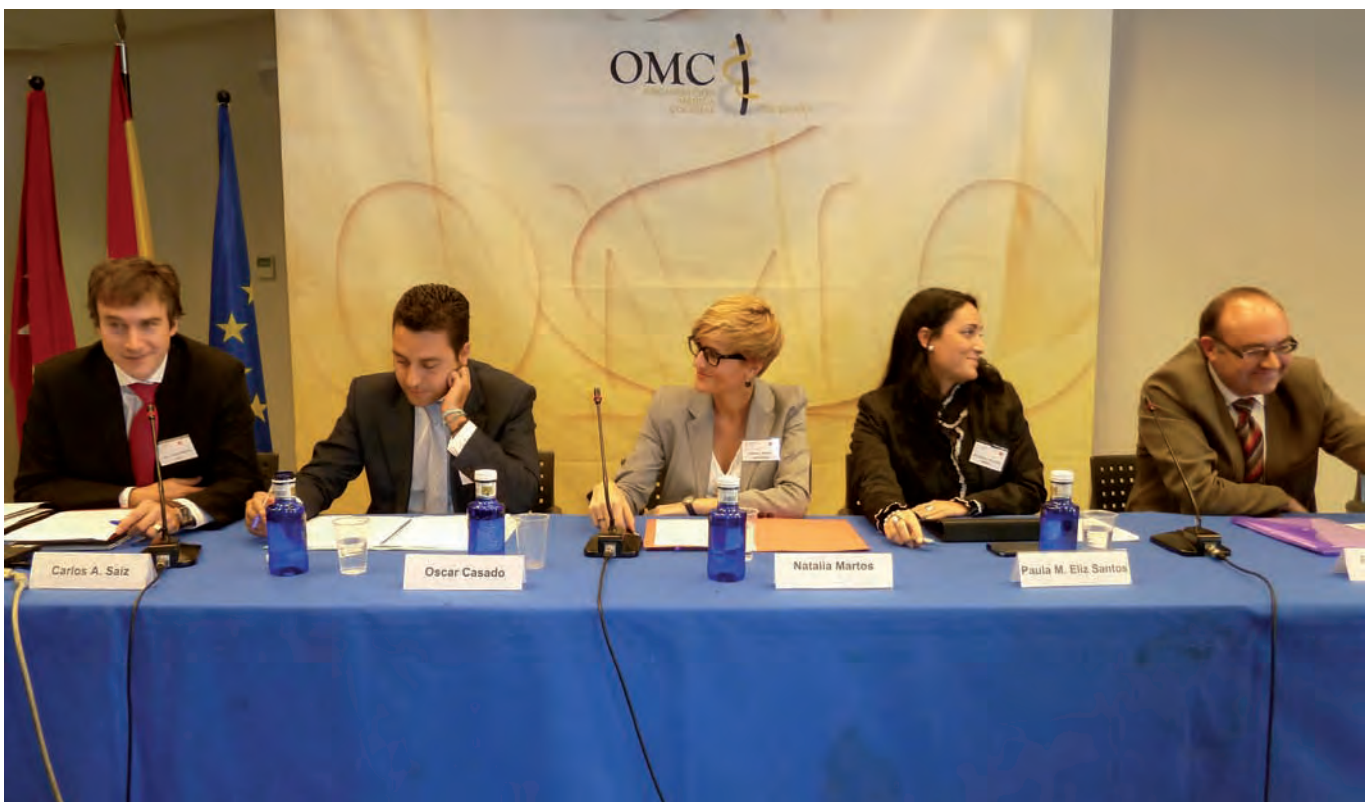
comentó, haciendo referencia a que las personas deberían tener acceso a toda la información disponible sobre ellos, siendo éste un derecho a la información de cualquier ciudadano. "Tenemos que saber qué información nuestra se está publicando y así podemos actuar", concluyó. Otro matiz fue introducido por Natalia Martos, Directora de Privacidad en el **Grupo Prisa** y Consejera General de Prisa Digital, al diferenciar entre información publicada como noticia en un medio de comunicación a "lo publicado en una red social donde la persona puede cancelar lo que ha dado", mostrándose "contraria a la sobrerregulación".

"Hay que buscar soluciones que no sólo sean costosas para el que está prestando el servicio". Paula Mª Eliz Santos, ***Letrada de la Dirección de Asesoría Jurídica de lo Consultivo en Telefónica España,***

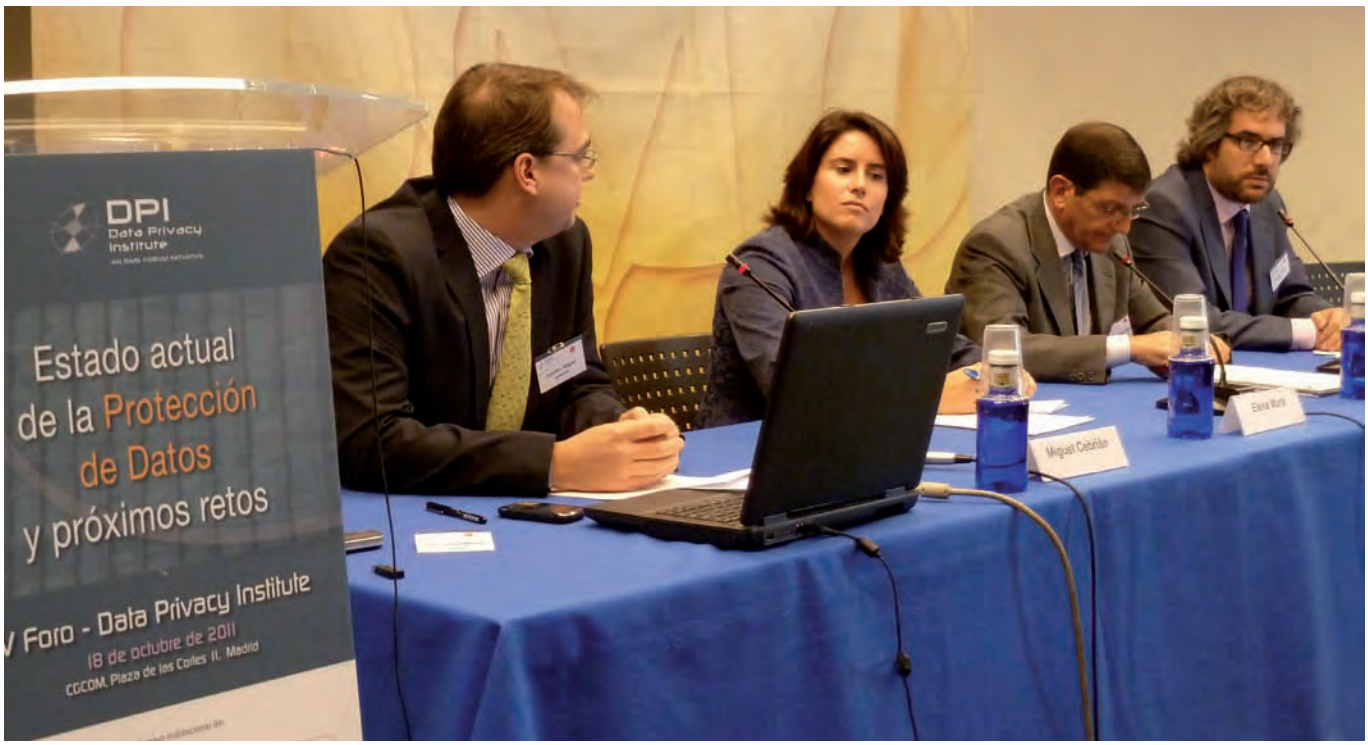
En esta misma mesa dedicada al panorama normativo nacional de la privacidad en Internet, también se abordaron los protocolos de seguridad utilizados por las empresas de servicios, destacando la dificultad tecnológica actual como por ejemplo para identificar menores. "La diligencia de nuestros profesionales es máxima para identificar perfiles que son potenciales menores de 14 años" y proceder a su identificación real a través de documentos acreditativos verificados o de sus propios padres, comentó Óscar Casado, Director Jurídico y de Privacidad en **Tuenti**. Ante la dificultad de crear mecanismos fiables "lo que hace falta es que "se sienten todos los actores para buscar soluciones que no sólo sean costosas para el que el está prestando el servicio", declaró Paula Mª Eliz Santos, Letrada de la Dirección de Asesoría Jurídica de lo Consultivo en **Telefónica España**.

"No se tiene en cuenta la diligencia del responsable como causa de exención", Ricard Martínez. ***Presidente de la Asociación Profesional Española de Privacidad (APEP) y Profesor de Derecho Constitucional en la Universitat de Valencia.***

Por otro lado, se analizaron las primeras resoluciones tras la reforma del régimen sancionador de la Ley Orgánica de Protección de Datos derivada de la Ley de Economía Sostenible, a cargo del subdirector de Inspección de la **Agencia Española de Protección de Datos**, José López Calvo, quien comunicó que



De izquierda a derecha: Carlos Alberto Saiz, Óscar Casado, Natalia Martos, Paula M. Eliz Santos y Ramón Miralles.



De izquierda a derecha: Miguel Cebrián, Elena Mora, Miguel Ángel Ballesteros y Javier Carbayo..

desde el tres de marzo se habían producido un alto número de apercibimientos, 213, siendo muy destacable que 144 estuvieran relacionados con la videovigilancia. Ricard Martínez, Presidente de la **Asociación Profesional Española de Privacidad** (APEP) y Profesor de Derecho Constitucional en la **Universitat de València** incidió sobre "el fruto de la modulación de las sanciones". "No se tiene en cuenta la diligencia del responsable como causa de exención", aseguró, abriendo debate con López Calvo, quien mostró su desacuerdo, matizando la afirmación de Martínez.

"La principal misión de la auditoría es la concienciación". Miguel Ángel Ballesteros, *Auditoría interna en Cepsa.*

Las estrategias para la aplicación efectiva de las medidas de seguridad establecidas en el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de carácter personal (RLOPD) fueron analizadas por Miguel Ángel Ballesteros, Auditoría interna en **Cepsa**; Elena Mora, Marco regulatorio en **Mapfre**; Javier Carbayo, Asociado Senior en **Ecija**, y Miguel Cebrián, Senior Systems Engineer en **Symantec**, como moderador. Todos ellos estuvieron de acuerdo en destacar el gran valor de concienciación que tiene la auditoría. "Desde mi experiencia la principal misión de la auditoría es la concienciación", aseveró Ballesteros. Además esa obligación se debe "aprovechar para convertirla en un valor diferencial", en forma de certificaciones, por ejemplo, comentó Carbayo. Por su parte, Mora incidió en la necesidad del apoyo de la alta dirección y el plan de acción. "Es más efectivo incluir aspectos desde el momento de concepción de la idea que a posteriori", argumentó.

Certified Data Privacy Professional (CDPP) y Fundación de la Privacidad

En su ponencia Nathaly Rey, directora de ISMS Forum Spain, anunció la creación de una **Fundación de la Privacidad**, que estará abierta a empresas e instituciones e informó de la buena marcha de la primera certificación española dirigida a los profesionales de la privacidad, creada por ISMS Forum, el **Certified Data Privacy Professional (CDPP)**. Un certificado que permite acreditar un alto nivel de especialización en la normativa española en materia de Protección de Datos de carácter personal, tanto en un contexto local, como en un contexto europeo e internacional, así como un dominio de los fundamentos que rigen la Seguridad de la Información.

Clausuró el acto su Secretario General del **Consejo General de Colegios de Médicos** (miembro de ISMS Forum y sede del IV Foro de la Privacidad del DPI), Serafín Romero, quien aludió a Hipócrates para visibilizar el compromiso tradicional de la comunidad médica con la Protección de Datos de los pacientes, un sector que se enfrenta actualmente a "importantes retos" derivados del progreso tecnológico ya que, por ejemplo, es posible "desde Argentina estar informando de una resonancia hecha aquí", comentó.

Más información en: www.ismsforum.es/dpi

Actividades 2011, Cloud Security Alliance España (CSA-ES)

Cloud Security Alliance publica el primer Informe Cloud Compliance para España

El capítulo español de Cloud Security Alliance (CSA-ES) ha publicado el primer Informe Cloud Compliance. Este informe ha sido la principal línea de trabajo de la división desde su inicio en 2010 durante la VII Jornada Internacional de ISMS Forum Spain. Uno de los principales objetivos de este informe es proveer de unas pautas metodológicas que ayuden a abordar la necesidad de Compliance en Cloud Computing.

El informe se centra en tres áreas principales:

- Grupo de trabajo 1: Privacidad y Compliance en la Nube, conducido por Miguel Ángel Ballesteros.
- Grupo de trabajo 2: Sistemas de Management en Seguridad de Información y Gestión de Riesgos en la Nube, bajo la dirección de Antonio Ramos.
- Grupo de trabajo 3: Contratación, evidencias electrónicas y auditoría en la Nube, dirigido por María Luisa Rodríguez.

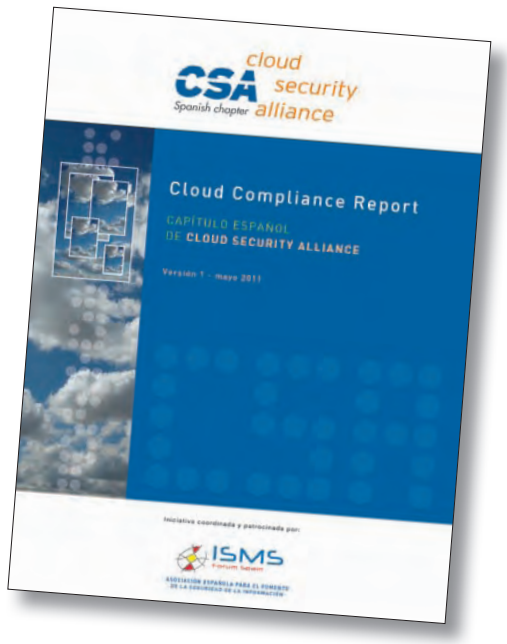
"Compliance es un componente crítico en el trabajo que CSA desarrolla, y que provoca que la adopción de buenas prácticas de seguridad en Cloud Computing sea cada vez más lejana", afirma Jim Reavis, co-fundador y director ejecutivo de CSA, "Cada división de CSA en el mundo concentra sus esfuerzos en esta iniciativa, que es clave para nosotros".

Este primer informe de ámbito nacional ha prestado especial interés a la privacidad y a aspectos relacionados con la contratación y las auditorías como claves fundamentales de la relación entre cliente y proveedor de servicios en "la nube". También se proponen diferentes recomendaciones y se especifica que una empresa cliente establecida en el territorio del Espacio Económico Europeo, independientemente de dónde esté ubicado su proveedor de servicios, será la responsable en términos de protección de datos y le será de aplicación la ley del Estado en que está establecida.

Luis Buezo, Presidente del Capítulo Español Cloud Security Alliance, explica que no conviene ver sólo beneficios en la computación en la nube y olvidar los riesgos y las obligaciones legales. La cuestión es buscar un equilibrio entre ambos aspectos ya que, "la simple determinación de la legislación aplicable ya es un reto".

"La evolución de la Nube será gradual, y las exigencias de Compliance serán ser uno de los parámetros principales que determinarán la velocidad de esta evolución", valora Buezo. "Estamos muy satisfechos de haber completado el primero los muchos objetivos que la división española de CSA se había propuesto".

El capítulo español de CSA trabaja para ampliar el alcance del informe a otras áreas que no han sido cubiertas en esta versión y para implementar la certificación CCSK en castellano.



"Las exigencias de Compliance serán uno de los parámetros principales que determinarán la velocidad de la evolución del Cloud Computing". Luis Buezo, *presidente de CSA-ES.*

Más información en:

www.cloudsecurityalliance.es y www.ismsforum.es/csa

Actividades 2011, Formación

Curso de Gobierno Corporativo de la Seguridad de la Información (GCSI)

En marzo y junio de 2011 se celebraron la II y III Edición del Curso de **Gobierno Corporativo en Seguridad de la Información** de ISMS Forum. Este curso nació con el objetivo de formar y especializar a profesionales en las metodologías, estrategias, estándares y las técnicas relacionadas con el gobierno de la Seguridad de la Información, de forma que adquieran la capacidad de definir, desarrollar e implantar un plan estratégico de Seguridad de la Información dentro de cualquier organización.

El profesorado está compuesto por expertos de la Asociación y en 2012 el curso contará con nuevas convocatorias, dirigidas a profesionales que trabajan en Seguridad de la Información, o en la gestión de las tecnologías de la información y la comunicación, sea en el sector privado, o para las Administraciones Públicas. Este curso ofrece la oportunidad de adquirir nuevos conocimientos para desempeñar puestos y roles de mayor responsabilidad en el ámbito de la seguridad.

En sus diferentes ediciones, los cursos de ISMS Forum han sido valorados muy positivamente por los alumnos con una alta puntuación en los cuestionarios de calidad. Ya son casi 60 los profesionales que han pasado por las aulas de ISMS Forum. De esta manera, la Asociación confirma su apuesta por la formación, una rama que seguirá creciendo con nuevas convocatorias y nuevos cursos.

Programa

DÍA 1

Estándares y buenas prácticas de referencia

- Objetivos, estructura y elementos.
- Modelos de referencia:
  - ISO 27014 / ISACA.
- Estándares y buenas prácticas:
  - ISO 27001/ISO 27002.
  - ITIL V3.
  - COBIT.
  - ISO 38500.
  - CMMI.
  - SABSA.

DÍA 2

Organización, roles y responsabilidades

- Modelos organizativos y funcionales.
- El Comité de Dirección.
- El CISO.
- El Comité de Seguridad.
- El propietario del proceso o del activo.
- Los usuarios.

DÍA 3

La identificación y gestión de riesgos

- La gestión de riesgos tecnológicos en la gestión de riesgos corporativos.
- El proceso de análisis y gestión de riesgos de seguridad.
- Metodologías y herramientas de referencia.

DÍA 4

Cumplimiento legal

- Gobierno de seguridad y cumplimiento.
- Normativa nacional de referencia:
  - LOPD.
  - LSSICE.
  - Propiedad Intelectual.
  - Código Penal.
  - Otra legislación de interés.
- Normativa internacional de referencia:
  - SOX.
  - Basilea III.

DÍA 5

El proceso de definición estratégica en la empresa

- Elementos para la definición estratégica:
  - Misión, visión.
  - Los valores y la cultura corporativos.
  - Objetivos estratégicos, tácticos y operativos.
- El proceso y desarrollo de la planificación:
  - Planes estratégicos, tácticos y operativos.
- Gestión, revisión y mejora:
  - Métricas e indicadores.
  - El balance Scorecard.

DÍA 6

El desarrollo de la estrategia de Seguridad

- Definición de objetivos de seguridad.
- La política de seguridad de la información.
- Desarrollo y ejecución del Plan Director de Seguridad.
- Revisión y mejora. ISO 27004.

DÍA 7

El arte de presentar

- Cómo planificar, estructurar, diseñar y exponer presentaciones.

DÍA 8

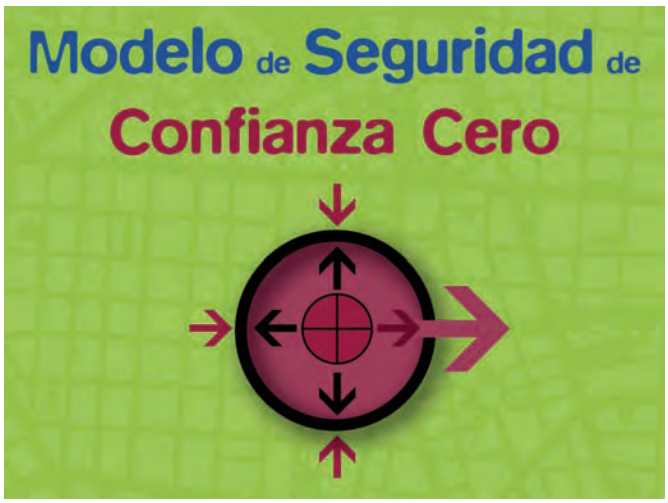
Caso Práctico

- Diseño de un modelo de gobierno corporativo.

Más información en:
www.ismsforum.es/formacion

ISMS organiza un debate sobre el Modelo de Seguridad de Confianza Cero

ISMS Forum celebró el 28 de abril un encuentro para discutir sobre el planteamiento defendido por Forrester Research y su "Zero Trust" o "Confianza Cero", según el cual, el tráfico generado por los empleados y colaboradores que se encuentran dentro de la organización, debe ser objeto del mismo nivel de desconfianza que el tráfico generado desde fuera del entorno corporativo.



La desaparición progresiva del perímetro, la necesidad de centrar la seguridad en el dato, la importancia de conocer en tiempo real los riesgos y problemas de seguridad, la monitorización del tráfico y la concienciación sobre el uso de la red y todos los dispositivos que se conecten a ella, así como el conocimiento de las debilidades de cada organización desde el punto de vista de la seguridad, fueron las principales conclusiones de la jornada organizada por ISMS Forum.

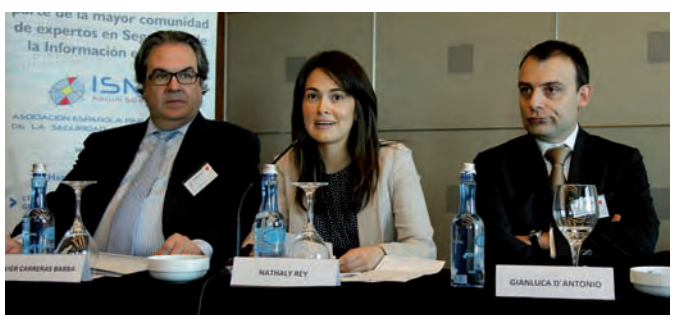
El evento contó con la participación de 14 ponentes de primer nivel, responsables de la seguridad en organizaciones como Telefónica España, Cepsa, la Guardia Civil, ONO, Endesa, junto a expertos de las empresas Arbor Networks Iberia, Buguroo, Blancco Iberia y Swivel Iberia.

Gianluca D'Antonio, Presidente de ISMS Forum Spain y CISO del Grupo FCC, inauguró la conferencia con la explicación del Modelo de Seguridad de Confianza Cero y su aplicación en grandes corporaciones. Según D´Antonio, se ha pasado del modelo "trust but verify" –una estrategia reactiva focalizada en la estructura de red- al "verify and never trust" o confianza cero.

"Verificar siempre. Se trata de un modelo proactivo, centrado en el dato y focalizado en el usuario, ver qué puede hacer este usuario de la red y saber cuáles son sus privilegios".

D'Antonio explicó que cada vez es mayor el robo de datos por parte de "insiders" que no necesariamente son empleados de la organización sino identidades suplantadas. Según el "2010 Data Breach Investigations Report" de Verizon Business, el robo de datos por parte de insiders ha aumentado un 26% y ya alcanza el 48% de las incidencias relacionadas con este tipo de delitos.

"Necesitamos construir un Network Analysis & Visibility (NAV). Es decir, capacidad para proteger el acceso a la información, monitorizar toda la actividad, filtrar el contenido para que no sea accesible a todo el mundo. Tengo que ser capaz de saber: ¿Quién navega por mi red? ¿Por qué tiene acceso a mi red? ¿Cómo? ¿Cuándo? ¿Con qué dispositivo? ¿A qué información accede?".



De izquierda a derecha: Javier Carreras, Nathaly Rey y Gianluca D'Antonio.

"Se ha pasado del modelo 'trust but verify' al 'verify and never trust'.

Gianluca D'Antonio, *presidente de ISMS Forum.*

Gianluca D'Antonio.

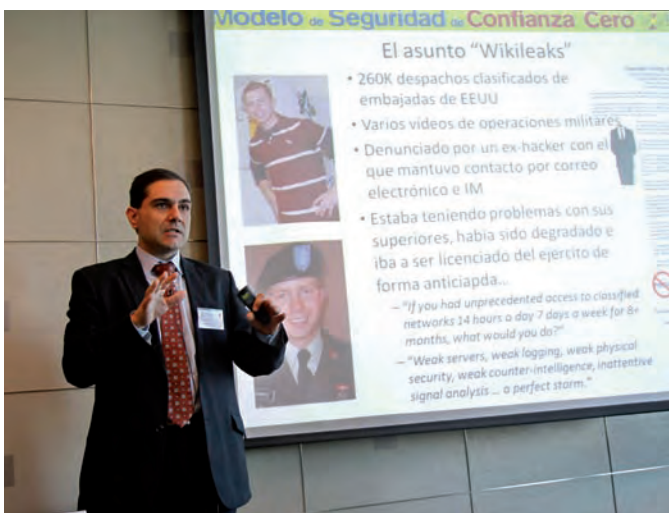
Seguridad Vs. Wikileaks

Alberto Cita, Consulting Engineer de Arbor Networks Iberia, empleó el caso de Wikileaks para introducir su conferencia "Los riesgos de seguridad de las organizaciones y la necesidad de mejorar el análisis y la visibilidad de lo que está pasando en la Red corporativa".

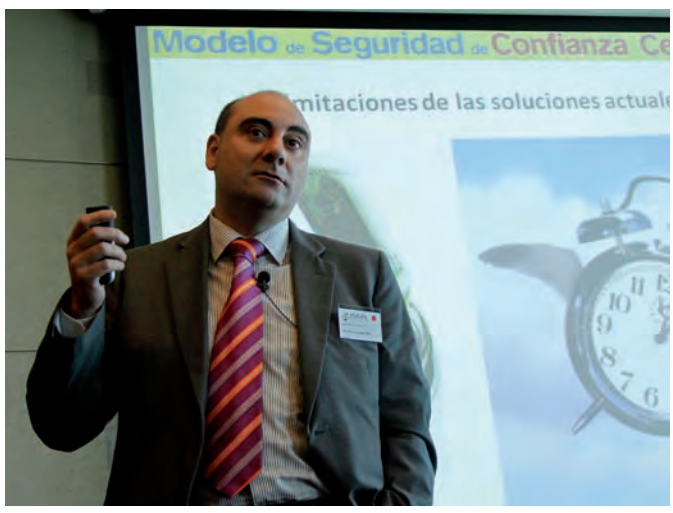
Cita quiso dejar claro que tanto los sistemas en línea como aquellos offline corren riesgos de filtración de los datos de una organización. Un ejemplo son los llamados "Bots" que se instalan en el sistema sin conocimiento de su propietario y contactan con otro sistema para ponerse a su disposición. Es así como un botmaster envía instrucciones a los bots para realizar "tareas" como convertirse en un site de phishing, envío de spam o proporcionar datos de cuentas bancarias, etc.

"El 'trusted' ya no es válido tenemos que ir a un modelo de seguridad de confianza cero, ahora hay que monitorizar todo el tráfico. Este es el desafío porque estas redes dan servicio a un centenar de empleados". Cita presentó una solución que lo facilita: Peakflow X, de Arbor Networks. A través de la exportación de datos de flujos IP en los dispositivos de red se puede medir a distancia lo que está ocurriendo y hacer un "Network Behavioral Analysis". Esta solución provee de información de red a nivel transaccional más datos del plano del control de red. De esta manera se crean líneas base (estadísticas y relacionales) que permiten la identificación de anomalías en tiempo real.

Para Cita, la implementación de un modelo de Seguridad de Confianza Cero requiere "visibilidad y seguridad de red global para detectar la anormalidad".



Alberto Cita.



Abel González Lanzarote.

Seguridad desde el código fuente

Abel González Lanzarote, Business Development Manager de Buguroo, se centró en el Modelo de confianza cero aplicado a la estructura al código fuente. "Más del 90% de las vulnerabilidades están en el código. El problema es que no tenemos en cuenta la seguridad al desarrollar las aplicaciones, ya sea por tiempo o por coste. La solución es implantar desde la base el desarrollo seguro: gestionar la seguridad desde el origen, desde el código fuente".

González propuso una tecnología para poder cumplir con los objetivos de seguridad: Buguroo Boy Scout, que audita simultáneamente varios códigos y detecta más del 94% de sus vulnerabilidades. Discrimina falsos positivos y facilita el acceso desde la nube para cualquier organización, grande o pequeña, con un coste adecuado a su nivel de uso". Para él la clave está en tener "acceso desde la nube con escalabilidad ilimitada y poder determinar por perfiles quién puede acceder a qué y no esperar a que el código esté terminado".

Se acabaron los usuarios de confianza

Alex Rocha, Country Manager de Swivel Iberia, explicó que "las contraseñas ya no son seguras: Sabemos que hay password muy sencillas como 12345...al menos el 50% de las personas usa contraseñas de menos de 7 caracteres; es decir poco seguras. Igual la seguridad corporativa es fuerte dentro de mi organización, pero la de mi gmail no...Entonces, si yo me envío el trabajo a mi gmail, ya no todo es seguro...". Con esta acción tan simple se puede debilitar la cadena de seguridad de la empresa.

Rocha también habló de la frecuencia con la que las contraseñas se dejan debajo del teclado o del monitor como otra evidencia de la debilidad de las contraseñas. Algo que tampoco puede solventarse con los datos de autenticación, pues no ofrecen una gran seguridad debido a su carácter estático y permanente.

Para evitar problemas Rocha explicó el modelo PinSafe basado en cuatro dígitos que nunca cambian, pero que pueden ofrecer cuatro millones y medio de posibilidades y hacer nuestras contraseñas más seguras.

"PinSafe es una solución de autenticación fuerte. La clave está en que nunca tenemos que teclear nuestro pin, pero tenemos un pin. Funciona con un protocolo patentado que asocia un pin a cada uno de los usuarios. Este pin va cambiando de posición según el uso de una cadena de seguridad. El pin no cambia, cambia la cadena de seguridad".

Destrucción de datos

La posibilidad de que los datos que han sido borrados de un disco duro puedan ser recuperados representa un riesgo para las organizaciones que deben buscar soluciones para garantizar la destrucción de esos datos pues "formatear no es borrar de manera definitiva" según explicó Javier Carreras Amorós, Managing Director de Blancco Iberia en su conferencia "Retos en la gestión del ciclo de vida del dato: Control de dispositivos y borrado seguro".

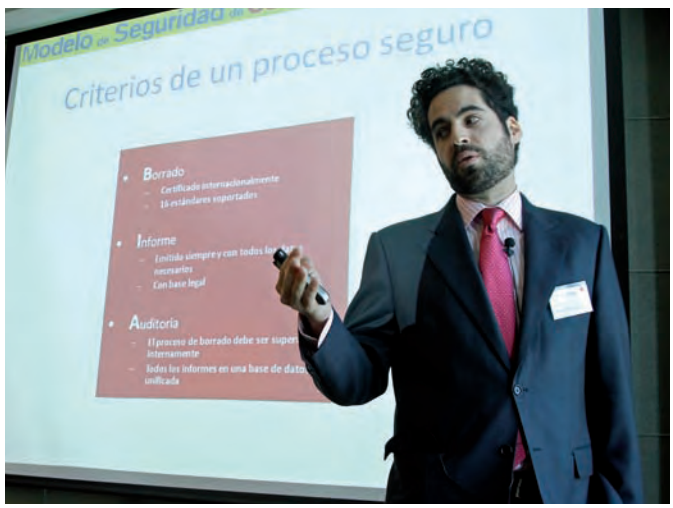
Carreras propuso el borrado de la información con un protocolo seguro. "Se necesita un software de sobrescritura que destruya toda la información y realice un informe de borrado que dice qué, quién, cuándo, cómo y por qué se ha borrado. Actualmente –añadió- la información está dispersa en múltiples dispositivos, proponemos una solución independiente del hardware. Para todas debe haber un informe de borrado".

La clave, según Carreras, está en el "borrado", es decir, la creación de un protocolo seguro para el borrado de la información; el "informe", que consiste en la emisión de un reporte con todos los datos necesarios y con base legal; y la "auditoría". Este último aspecto se refiere a que el proceso de borrado debe ser supervisado internamente y todos los informes deben incluirse en una base de datos unificada. De esta manera, si todos los datos están en una base común, se podrán realizar auditorías con mayor facilidad. "Si no se ha hecho nada hasta ahora no es una cuestión de dinero, sino de concienciación"; añadió el representante de Blancco.

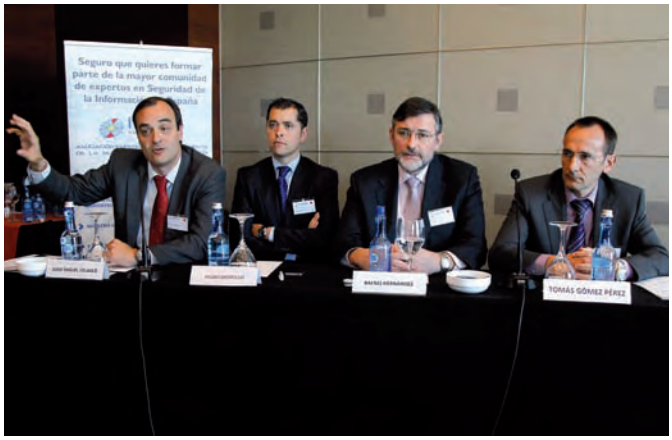
El fin de la perimetralidad interna y externa

En la mesa redonda "Estrategias y claves para la implantación de los pilares de modelo" participaron Pedro Morcillo, Comandante, Jefe área de Redes y Seguridad de la Guardia Civil; Rafael Hernández, Responsable de Seguridad DSI de Cepsa; Tomás Gómez Pérez, Subdirector de informática del Sistema

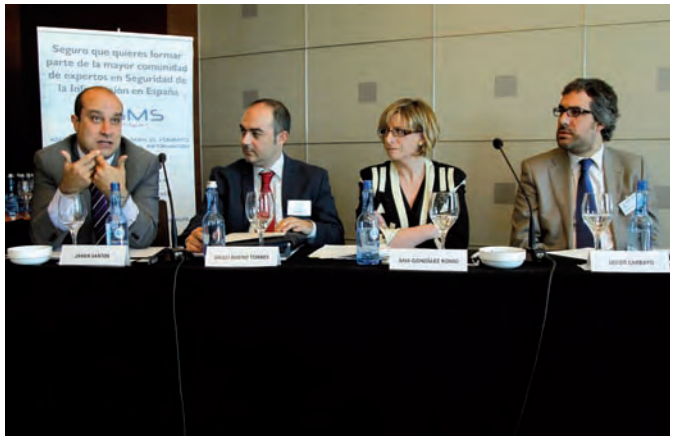
Alex Rocha.



Javier Carreras Amorós.



De izquierda a derecha: Juan Miguel Velasco, Pedro Morcillo, Rafael Hernández y Tomás Gómez Pérez.



De izquierda a derecha: Javier Santos, Diego Bueno Torres, Ana González Romo y Javier Carbayo.

Público de Salud de la Rioja; con la moderación de Juan Miguel Velasco, Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Clientes de Telefónica España.

En este debate quedó claro que han desaparecido los perímetros y que no hay diferencias por tipos de usuarios internos y externos. El uso de dispositivos móviles, tablets, smartphones, que se conectan a la red de una organización ha hecho que haya aún más riesgos de seguridad que deben gestionarse.

Velasco introdujo el debate analizando la situación de Sony tras el robo de datos y cómo afectó al valor de la compañía en bolsa y planteó la primera duda: "¿Tenemos un perímetro? ¿Hay usuarios buenos y usuarios malos?". En el caso de Cepsa, Hernández comentó que la perimetralidad interna y externa se está acabando. "Cada vez se usan más dispositivos móviles. El dispositivo personal-de empresa cada vez está más extendido. Hay herramientas que ayudan a hacer ese trabajo pero es muy importante tener en cuenta la tecnología y la gestión de la tecnología".

Para el subdirector de informática del Sistema Público de Salud de la Rioja, la dificultad de establecer un perímetro, principalmente por el uso de dispositivos que se conectan a la red, ha obligado a la organización a impedirlos. "De momento solo podemos gestionar los positivos que nosotros entregamos. Por lo que no damos acceso a los dispositivos que no controlamos".

Pedro Morcillo de la Guardia Civil comentó que "en nuestro proyecto tenemos un ordenador de internet y otro de intranet".

¿Se puede monitorizar al empleado?

En la mesa redonda "Implicaciones legales de la monitorización de la actividad de los empleados" que contó con la participación de Javier Carbayo, Asociado Senior del Área de Governance, Risk & Compliance, de Ecija; Ana González Romo, del departamento de Seguridad de la Información de Endesa, Diego Bueno, Senior Manager IPBR, IT Advisory en KPMG; Javier Santos, Gerente de Operaciones de Seguridad de ONO; y la moderación de Antonio Ramos, presidente de ISACA Madrid; se llegó a la conclusión de que la clave está en establecer una normativa de uso que sea conocida por el empleado. "La concienciación es necesaria pero tiene que ser de arriba abajo", explicó Ramos en relación con el cumplimiento de los protocolos de seguridad por parte de todos los empleados.

Respecto a si la monitorización de los empleados es un tema técnico o jurídico, hay diversidad de opiniones. Para Carbayo, de Ecija, "es un tema legal que normalmente se articula a través de medidas tecnológicas. Se busca tener una capacidad para cumplir una normativa y que en el cumplimiento de la misma no se viole otra". En el caso de Endesa, González considera que se trata de "un tema organizativo que pasa por las políticas y las normas que establece la empresa". Desde KPMG, Bueno explica que es un tema técnico que depende de la estrategia de seguridad: "Hay que analizar los riesgos a los que se está sometido y tomar las medidas adecuadas". Santos, de Ono, lo ve como jurídico-organizativo: "En nuestro caso tener más capacidad de monitorización nos hace tener que hacer menos esfuerzo tecnológico. Tiene que haber concienciación y que el usuario sepa que lo estamos monitorizando".

En cualquier caso como explicó Javier Carbayo "la normativa nos da unas ciertas fronteras. Que cada vez están más definidas y nuestro trabajo es identificar cuáles son las fronteras, según la actividad del empleado y saber que no tienen que superar ciertos límites".

Gianluca D'Antonio concluyó el evento haciendo énfasis sobre la importancia de permitir el uso privado y moderado de la red y los sistemas de la organización a cambio de poder monitorizar a los usuarios, pero sin correr el riesgo de que el CISO se tome más atribuciones. "El negocio es el que tiene que prohibir. El departamento de seguridad hace el análisis de riesgo, propone controles y aconseja al negocio sobre cómo controlar estos riesgos. Somos un asesor interno que facilita la toma de decisiones, pero no somos los propietarios de la información".

Protegetuinformacion.com premiado con el Trofeo de la Seguridad TIC

El proyecto Protegetuinformacion.com ha sido reconocido en 2011 con el Trofeo de la Seguridad TIC de la revista Red Seguridad, en la categoría de Trofeo a la Formación, Capacitación, Divulgación o Concienciación en Seguridad TIC. El premio se entregará en una ceremonia que se celebrará en los primeros meses de 2012.

Protegetuinformacion.com es el resultado de una iniciativa de ISMS Forum Spain, con la ayuda del Ministerio de Industria, Turismo y Comercio en el marco del Plan Avanza aprobado en Consejo de Ministros en 2005 y cuyo objetivo es generalizar el uso de las Nuevas Tecnologías en la sociedad.

El portal nació para contribuir a la difusión y la concienciación de la población en materia de seguridad así como para fomentar el uso responsable de Internet y las Nuevas Tecnologías. Para ello, se dirige a cinco grupos sociales concretos (jóvenes, adultos, mayores, padres y profesionales), ofreciendo información, consejos y otras herramientas divulgativas e informativas útiles para un aprovechamiento seguro y eficaz de la red.

A través de un lenguaje sencillo y accesible a los ciudadanos se tratan temas de especial relevancia como la banca electrónica, las redes sociales y la protección de datos personales. ISMS Forum inculca hábitos entre la población española, que fomentan la seguridad de los internautas a la hora de interactuar con las Nuevas Tecnologías.

Más información en:
www.protegetuinformacion.com

Actividades 2011, Otras noticias

ISMS Forum premia a HP, IBM y Symantec por su compromiso con la Seguridad de la Información

Durante la IX Jornada Internacional de ISMS Forum, la Asociación entregó sendos premios a HP, IBM y Symantec en reconocimiento a su firme compromiso con el desarrollo de la seguridad de la información en España y a su incondicional apoyo a ISMS Forum, desde su constitución en el año 2007.

Los premios fueron entregados por Gianluca D'Antonio, Presidente de ISMS Forum, a Damián Paredes, General Manager de HP; Isidro Carrasco, Director de Servicios Tecnológicos y Mantenimiento de IBM SPGI (España, Portugal, Grecia e Israel) de IBM y Gabriel Martín, Director General de Symantec Ibérica.

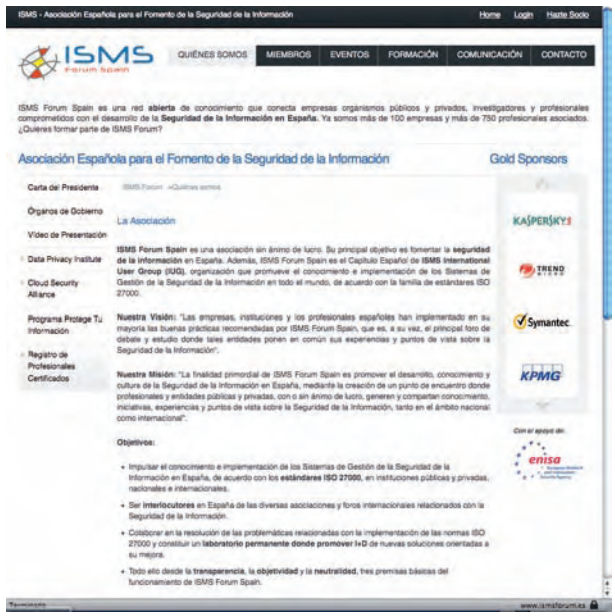
Entrega de premios.

Enrique Polanco, miembro del Consejo Asesor de ISMS Forum

ISMS Forum Spain ha nombrado a Enrique Polanco como el primer miembro de su Consejo Asesor, un órgano creado para apoyar los procesos de toma de decisión de la Asociación y contribuir en su desarrollo estratégico y excelencia operacional. Su valiosa aportación reside en el reconocido prestigio profesional, destacada experiencia y los conocimientos avanzados tanto del sector como de la propia Asociación, ya que fue miembro con anterioridad de la Junta Directiva de ISMS Forum.

ISMS Forum Spain lanza nueva web

ISMS Forum ha desarrollado su nueva web con motivo de mejorar de forma eficaz la comunicación con todos sus públicos internos y externos, haciendo especial hincapié en sus socios, patrocinadores y colaboradores. Se trata de una página intuitiva y dinámica con la que se busca difundir las novedades, proyectos y demás información interesante generada en la Asociación. Además, se incluyen funcionalidades como la posibilidad de hacerse socio online, la inscripción en eventos o la descarga de documentos. www.ismsforum.es.



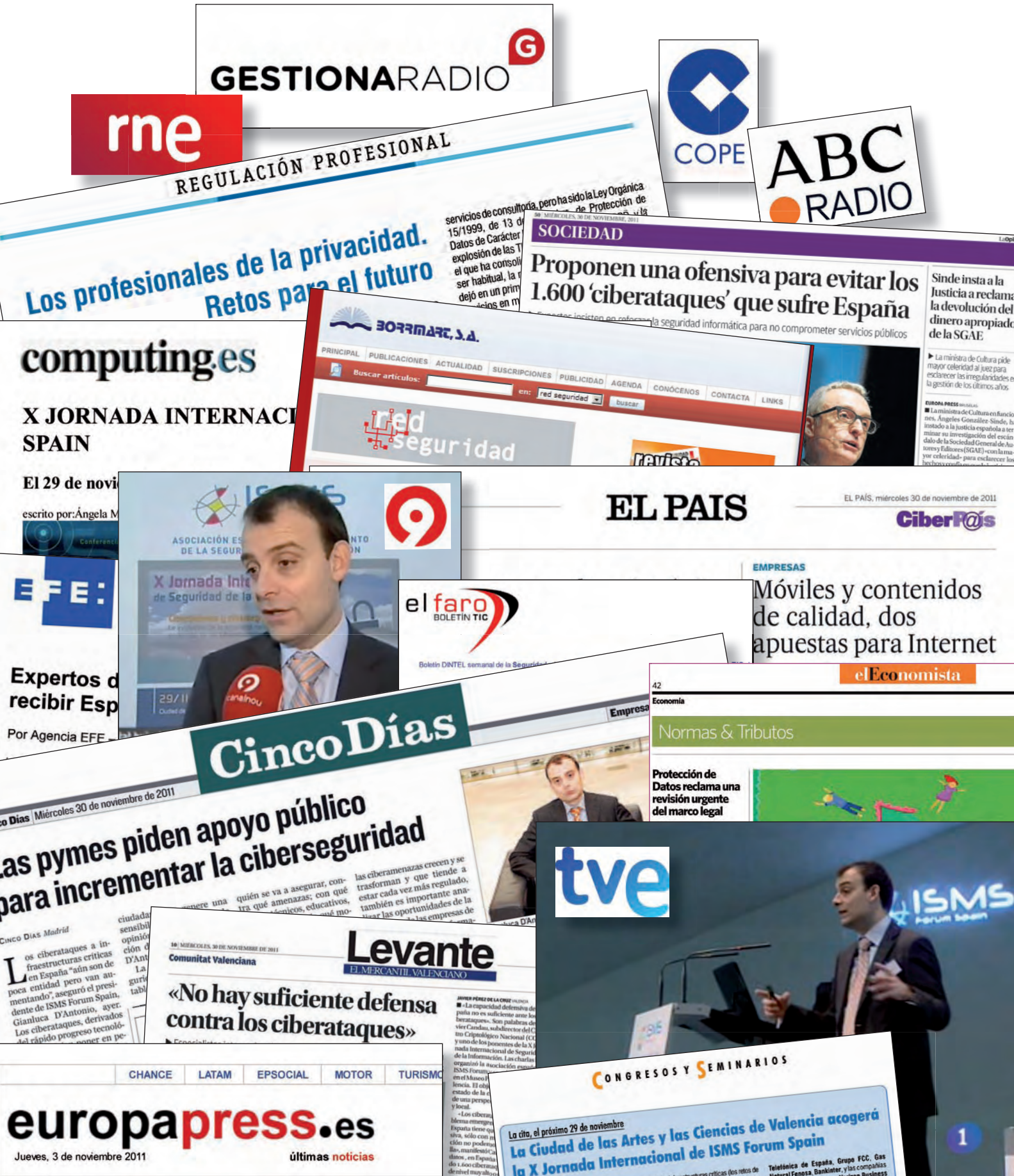
Web ISMS Forum.

Juniper Networks, KPMG y Prosegur, nuevos Gold Sponsors de ISMS Forum

En 2011, ISMS Forum ha incorporado tres nuevos Gold Sponsors: Juniper Networks (NYSE: JNPR), empresa especializada en el negocio de la innovación de la red; KPMG, red global de firmas de servicios profesionales que ofrecen servicios de Audit, Tax y Advisory; y Prosegur, empresa líder en servicios integrales de seguridad en España. A través de una colaboración anual se unen al resto de Gold Sponsors de la Asociación: Check Point, HP, IBM, Kaspersky, McAfee, Symantec, Telefónica y Trend Micro.

Gracias al respaldo de estas compañías y al apoyo puntual recibido por parte de numerosas empresas y organizaciones del sector, la Asociación puede organizar actividades de gran calidad como sus Jornadas Internacionales, que se han convertido ya en referencia para el sector de la Seguridad de la Información en España.

Actividades 2011,
ISMS en los medios



Notas

Castelló 24, 5º dcha. esc. 1
28001 Madrid
Teléfono: +34 91 186 13 50
Fax: +34 91 186 13 54
Web: www.ismsforum.es

ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN