ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Memoria de Actividades
ISMS Forum Spain

2010

Memoria de Actividades
ISMS Forum Spain

10

Redacción: ISMS Forum Spain

Fotografía: Daniel Sastre
Francesc Adelante

Diseño: jonarriaga1@gmail.com

EQUIPO DE GESTIÓN:

Directora General: Nathaly Rey Arenas

Coordinador General: Joris Vredeling

Management Assistant: María Angelina Carabajal

Colaboradores: Antonio Sánchez (Nuevoiris: Página web y BB.DD)
Oscar González (Gosán: Asesoría fiscal)
Laura Díaz Bettarel (Periodista)
Sol Núñez (Poweraxle: Periodista)

Publicación: Madrid, febrero de 2011

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.

OBJETIVOS PRINCIPALES

La finalidad primordial de **ISMS Forum Spain** es promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España, mediante la creación de un punto de encuentro donde profesionales y entidades públicas y privadas, con o sin ánimo de lucro, generen y compartan conocimiento, iniciativas, experiencias y puntos de vista sobre la Seguridad de la Información, tanto en el ámbito nacional como internacional.

A través de los cuatro valores adoptados por la Asociación – **independencia, neutralidad, objetividad** y **calidad y rigor profesional** – la Asociación se ha convertido en un referente a nivel nacional en cuanto a la Seguridad de la Información, no sólo por su labor como experto en la materia, sino también por haberse posicionado como foro de debate y estudio donde múltiples entidades ponen en común sus experiencias y puntos de vista sobre esta materia.

Gianluca D'Antonio
Presidente

Estimados socios, colaboradores y amigos:

Empiezo estas líneas de presentación de la memoria agradeciendo sinceramente el apoyo y la colaboración de todos los miembros de ISMS Forum Spain, que han hecho que el 2010 haya sido un gran año para la Asociación, que ya cumple cuatro años, y que sigue creciendo en número de socios, apoyos institucionales e iniciativas. Estamos orgullosos de haber pasado el umbral de las 100 empresas y 750 profesionales asociados en este año.

En primer lugar, gracias a nuestros Gold Sponsors y demás patrocinadores, quienes año tras año siguen apostando por las actividades que desarrollamos en la Asociación, con objeto de fomentar una cultura sólida de la Seguridad de la Información en España, mejorar la formación de los profesionales del sector y facilitar el intercambio de conocimientos y experiencias entre ellos.

También me gustaría agradecer especialmente a los colaboradores activos de la Asociación, quienes con su tiempo, esfuerzo y conocimientos, han hecho posible la puesta en marcha de proyectos de máxima trascendencia para la industria y pioneras en España, tales como la certificación Certified Data Privacy Professional (CDPP) y el Report sobre Compliance en la Nube, ambos enmacarcados respectivamente dentro de las iniciativas Data Privacy Institute (DPI) y Cloud Security Alliance-ES.

Asimismo quisiera dar las gracias a mis colegas, los CISOs, que constantemente apoyan nuestro esfuerzo por consolidar el rol de la Seguridad de la Información como una pieza clave dentro de las organizaciones sobre unos cimientos de una eficaz gestión de riesgos. Son ellos, quienes han hecho posibles iniciativas como el estudio sobre el Futuro de la Carrera del CISO en España, el cual muestra conclusiones muy interesantes sobre esta joven y apasionante profesión.

Durante el 2010, el ISMS ha dado un paso adelante enfocando también su atención sobre la difusión de la cultura de la Seguridad de la Información en la ciudadanía. Así, con el proyecto www.protegetuinformacion.com, hemos querido dirigir un mensaje a la población española para promover la seguridad y la protección de sus derechos, a la hora de interactuar con las nuevas tecnologías.

Esta trayectoria constituye para nosotros una gran motivación y sin duda, nos refuerza en el compromiso, que suscribimos hace cuatro años con nuestros socios y con la sociedad entera, de constituir el primer foro plural e independiente para el Fomento de la Seguridad de la Información.

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. En 2010, la Asamblea tuvo lugar el día 4 de marzo y contó con un quórum de asistencia de 77 socios. En esta oportunidad se introdujeron algunos cambios en los Estatutos, entre los que destacan la ampliación del número máximo de Miembros de la Junta Directiva de 15 a 20. Asimismo, se aprobó la incorporación de IBM y de Ono-Cableuropa a la Junta y el mantenimiento de las cuotas para el año 2011.

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 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)**.

Alain Karioty Responsable de la Práctica de Seguridad de **BT España**.

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

José Francisco Pereiro Seco Responsable de Servicios de Seguridad Tecnológica de **IBM** en España.

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

Enrique Polanco González Adjunto al Consejero Delegado y Director de Seguridad Corporativa 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 DIRECTOR EJECUTIVO

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 Ejecutiva de ISMS Forum es Nathaly Rey Arenas.

Asociación Española para el Fomento de la Seguridad de la Información

ISMS Forum Spain es una asociación española sin ánimo de lucro, cuyo principal objetivo es **fomentar la Seguridad de la Información**. Se constituye en 2007 como foro especializado para que todas las empresas, organismos públicos y privados y profesionales del sector colaboren, intercambien experiencias y conozcan los últimos **avances y desarrollos en materia de Seguridad de la Información**. Todo ello desde la **transparencia**, la **objetividad** y la **neutralidad**.

La Asociación está respaldada por algunas de las más representativas empresas y organizaciones comprometidas con la Seguridad de la Información. En la actualidad, la Asociación tiene a más de **100 empresas asociadas** (cada una de las cuales puede nombrar hasta 8 socios de pleno derecho). Además, numerosos expertos del sector se han asociado de manera independiente, por lo que ISMS Forum cuenta hoy con más de **750 profesionales** asociados. Por tanto, la Asociación para el Fomento de la Seguridad de la Información es ya la **mayor red activa española de expertos en SGSI.**

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.
- Participa en **foros nacionales e internacionales** y coopera con instituciones públicas y privadas, nacionales e internacionales, para impulsar la cultura de la Gestión de la Seguridad de la Información.
- Ha puesto en marcha el **Data Privacy Institute (DPI)** y la certificación **Certified Data Privacy Professional (CDPP).**
- Ha fundado el **Capítulo Español de Cloud Security Alliance (CSA-ES).**

Data Privacy Institute, el foro específico para los profesionales de la Privacidad

El **Data Privacy Institute (DPI)**, nació en 2009 con la vocación de aglutinar a todas las personas y organizaciones que tienen interés y responsabilidades en el ámbito de de la Privacidad y la Protección de Datos de carácter personal, promoviendo la formación y excelencia en esta área de creciente importancia. En este sentido, el DPI ha puesto en marcha la certificación **Certified Data Privacy Professional (CDPP)**, la certificación de referencia para los profesionales de la privacidad. En la actualidad ya hay 100 profesionales certificados, a través del programa de Grandfathering, y los exámenes celebrados en 2010.

CSA-ES, el capítulo español de Cloud Security Alliance

Con 91 miembros fundadores, representativos de los distintos actores de la industria del Cloud Computing en España, nació en mayo de 2010 el **Capítulo Español de Cloud Security Alliance (CSA-ES),** impulsado por ISMS Forum Spain y Barcelona Digital. Como es ya conocido, CSA es la organización internacional de referencia en la que expertos de alto nivel debaten y promueven el uso de mejores prácticas para garantizar la seguridad y privacidad en el entorno del Cloud Computing. Por su parte, el capítulo español ya cuenta con 200 miembros, siendo su ámbito de interés el "Compliance en la Nube". En este sentido, existen tres grupos de trabajo específicos como son: Privacidad y Cumplimiento Normativo en la Nube; Sistemas de Gestión de Seguridad de la Información, y Gestión de Riesgos en la Nube; y Contratación, Evidencias Electrónicas y Auditoría en la Nube. Los profesionales que conforman estos grupos están trabajando en el primer **Report español en materia de Cloud Compliance,** cuya publicación está prevista en primavera de 2011.

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


ISMS


Types of cloud

Agradecimientos

Apoyo institucional

La Asociación agradece expresamente a la **Agencia Europea para la Seguridad de las Redes y de la Información (ENISA),** al **Instituto Nacional de Tecnologías (INTECO)** y a **Cloud Security Alliance (CSA)** su apreciada colaboración y apoyo institucional.

Asimismo, agradece al **Ministerio de Industria, Turismo y Comercio** su apoyo para el desarrollo del portal **protegetuinformacion.com** en el marco del **Plan Avanza**.

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 2010:

Otros Patrocinadores y Colaboradores

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

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.

Actividades 2010,
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. Por supuesto, **la asistencia a estas jornadas es gratuita para los socios de ISMS Forum Spain,** incluida la documentación y la asistencia al almuerzo.

Las jornadas se organizan siempre de forma que quede un tiempo para que los participantes se relacionen y conozcan entre sí y puedan además acceder y comentar con los conferenciantes sus inquietudes. **Ya son 2.100 las personas que han participado en las 8 jornadas organizadas desde el 2007,** y han evaluado las mismas a través de cuestionarios de calidad que han dado siempre, como resultado, una **puntuación media de cuatro sobre cinco puntos** en lo que se refiere a organización, contenidos, escenario, ponentes y documentación.

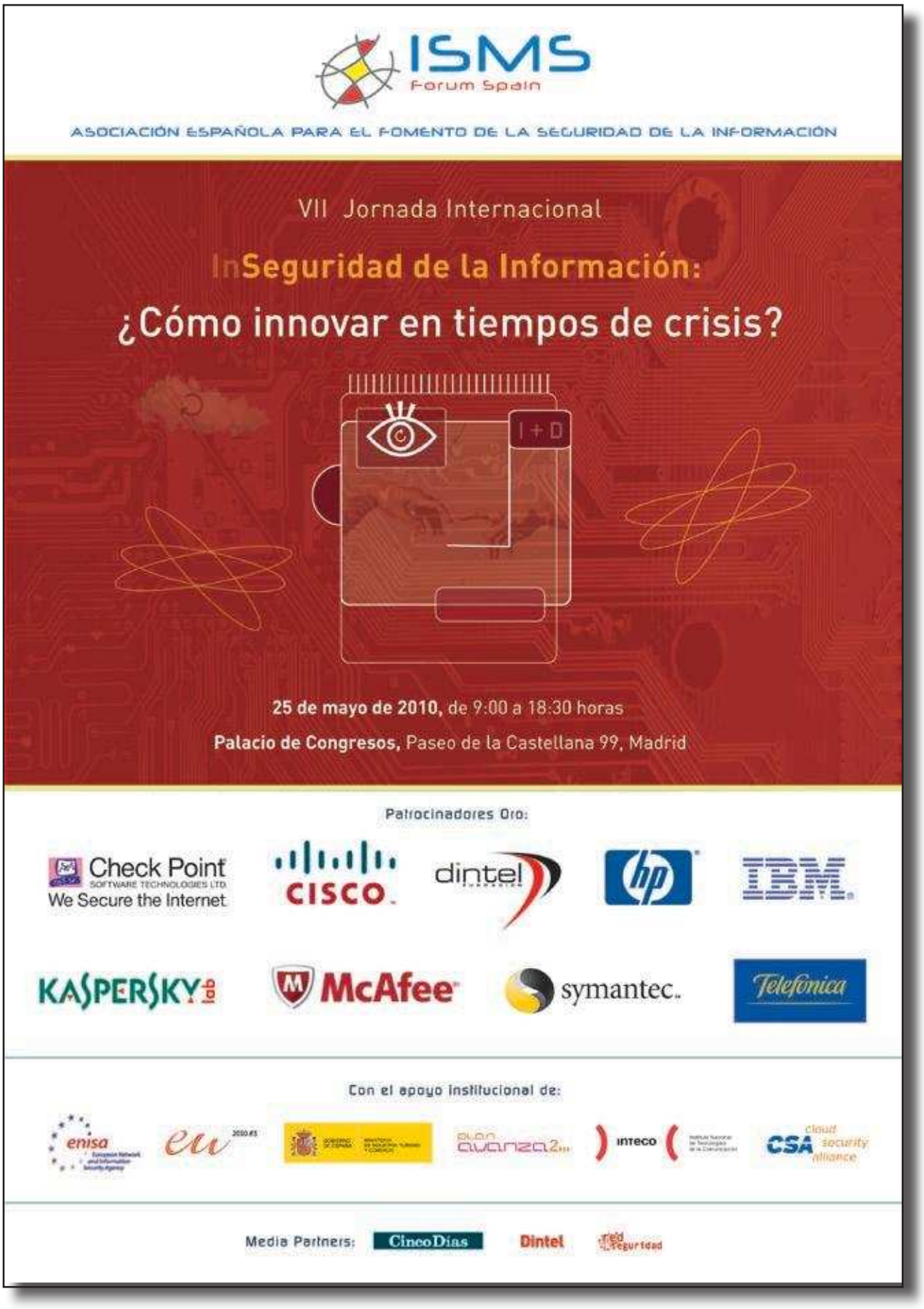
Al considerar que una asociación de ámbito nacional que quiere beneficiar a todos sus socios, y dinamizar el sector y fomentar la Seguridad de la Información, debe organizar eventos en todo el territorio español, se alternan jornadas en Madrid con jornadas en otras ciudades. En este sentido, se han celebrado ya dos jornadas en Barcelona, y una en Sevilla.

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	
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
Nº de asistentes	202	256	258	270	280	200	280	280

ctividades 2010,
VII Jornada Internacional



Programa VII Jornada ISMS Forum Spain

8:45 Acreditación – Welcome Coffee

9:15 Bienvenida
GIANLUCA D´ANTONIO, Director de Seguridad de la Información y Gestión de Riesgos, **Grupo FCC**; Presidente de **ISMS Forum Spain**; Asesor, Miembro del Consejo de Expertos (PSG) de la Agencia Europea de Seguridad de las Redes y de la Información (**ENISA**).

9:30 Conferencia inaugural
"Cómo innovar en Seguridad de la Información en tiempos de crisis".
UDO HELMBRECHT, Director General de la **Agencia Europea de Seguridad de las Redes y de la Información (ENISA)**.

10:00 Conferencia
"Midiendo la preparación tecnológica de España: Los resultados del Global Information Technology Report 2009-2010". IRENE MIA, Directora y Economista Senior del Global Competitiveness Network del **Foro Económico Mundial**.

10:30 Conferencia
"Cloud computing como método para innovar y mejorar la eficiencia".
CHRISTOPHER COGGRAVE, Director EMEA de Cloud Services de **HP**.

11:00 Coffee-break

11:30 esa redonda
"La visión del CIO acerca de la gestión de riesgos".
JOSÉ BOIXEDA DE MIQUEL, CTO de **Gas Natural Fenosa**.
JOAQUÍN CIDONCHA, CIO de **Grupo Telefónica**.
FRANCISCO JAVIER LÓPEZ COSTA, CIO de **Grupo FCC**.
IDOIA MAGUREGUI, Directora de Tecnología de **Bankinter**.
Modera: JOSÉ DE LA PEÑA, Director de la revista **SIC**.

12:30 Conferencia
"Balancing the costs of security and insecurity". FRED PIPER, Director del Information Security Group, **Royal Holloway (London University)**. Experto en ciberseguridad y criptografía.

13:00 Conferencia
"Proyectos y planes de ISMS Forum Spain". CARLOS ALBERTO SÁIZ, Vicepresidente de **ISMS Forum Sp** y Socio de **Ecija** responsable de Compliance IT.

13:30 esa redonda
"Innovación e Investigación en Seguridad de la Información: Retos y Desafíos".
MARK BREGMAN, CTO de **Symantec.**
NIKOLAY GREBENNIKOV, CTO de **Kaspersky Lab.**
SIMON HUNT, Vice President y CTO de **McAfee.**
Modera: JUAN MIGUEL VELASCO LÓPEZ-URDA, Director asociado de Servicios de Seguridad y Plataformas Comunes de **Telefónica Empresas.**

14:30 Almuerzo

16:00 esa redonda
"I+D y la seguridad como servicio a la ciudadanía".
MIGUEL ÁNGEL GARCÍA, Departamento de Promoción de la Innovación del **Centro para el Desarroll Tecnológico Industrial (CDTI)**.
CARLOS MARCOS MARTÍN, Subdirector General de Coordinación y Estudios del **Ministerio de la Presidencia.**
XABIER MITXELENA, Presidente del **Consejo Nacional Consultor sobre CyberSeguridad (CNCCS)** y Director General del Grupo **S21sec**.
PILAR SANTAMARÍA, Directora de Ciberseguridad para la Región Mediterránea de **CISCO.**
SALVADOR SORIANO MALDONADO, Subdirector General de Servicios de la Sociedad de la Informac **Ministerio de Industria, Turismo y Comercio**.
Modera: ANA BORREDÁ, Directora de **Red Seguridad**.

17:00 Conferencia
"Cumplimiento normativo en la Nube".
JOSHUA PENNELL, Cofundador de **Cloud Security Alliance (CSA)** y Consejero Delegado de **IOActive.**

17:30 Clausura
"Buenas prácticas de las compañías más innovadoras del mundo: Lecciones para nuestras empresas".
JOAQUIM VILÀ, Profesor de Dirección Estratégica y responsable de programas de formación para directivos sobre innovación, **IESE**.

Principales conclusiones / Por: Laura Díaz Bettarel

La importancia de no frenar el desarrollo de la Seguridad de la Información y la difícil labor de continuar innovando en tiempos de crisis

Udo Helmbrecht, ENISA.

La necesidad de generar confianza en la Nube y de promover la innovación, la formación y la colaboración global como gran motor para el desarrollo en materia de seguridad, fueron los principales mensajes de la VII Jornada internacional de la Asociación Española para el Fomento la Seguridad (ISMS Forum) en la que más de 280 profesionales del sector debatieron sobre la "Seguridad de la Información: ¿Cómo innovar en tiempos de crisis?". Una jornada que contó con un prestigioso panel de expertos nacionales e internacionales.

Soluciones globales

"Los desafíos para la Seguridad de la Información hoy también son globales. Todos sabemos que no hay fronteras para las amenazas y estas pueden llegar desde cualquier punto del planeta", fueron las palabras con las que **Gianluca D'Antonio** inauguró el evento en el que se analizó la innovación como factor clave para garantizar la Seguridad de la Información.

¿Cómo innovar si estamos en crisis?

Udo Helmbrecht, director general de la Agencia Europea de Seguridad de las Redes y de la Información (**ENISA**) fue el encargado de hablar sobre "Cómo innovar en Seguridad de la Información en tiempos de crisis". La técnica de Enisa: innovar a través de la investigación.

Helmbrecht repasó las iniciativas y estudios puestos en marcha por ENISA con el fin de combatir la inseguridad desde la prevención y la preparación. Por ello, han realizado estudios sobre el tratamiento de datos. Entre los más reciente citó "Procent" sobre las prioridades de estudio en seguridad de las tecnologías de la información y cuyas líneas de investigación son el "cloud computing" la detección y diagnosis en tiempo real, los futuros canales de comunicación *wireless*, los sensores de canales y la integridad de la cadena de suministro.

Otra de las investigaciones de ENISA es "Flying 2.0" sobre los problemas de seguridad y privacidad asociados al tráfico aéreo, y "Cloud Computing" que analiza los riesgos de los servicios que ofrece la "Nube".

"Los desafíos para la Seguridad de la Información hoy también son globales. Todos sabemos que no hay fronteras para las amenazas y estas pueden llegar desde cualquier punto del planeta".

Gianluca D´Antonio, *ISMS Forum*.

Para Helmbrecht, Internet ofrece muchas oportunidades para desarrollar negocios en tiempos de crisis, pero también tiene ciertos riesgos "por eso innovar en seguridad será siempre un buen negocio". Además, no se debe olvidar que los "atacantes" siempre están buscando nuevas vías para penetrar los sistemas de seguridad. Respecto a la tarea pendiente de las empresas e instituciones destacó la necesidad de armonizar las normas de seguridad.

Alto coste del acceso a las tecnologías de la información

Irene Mía, directora del Foro Económico Mundial, habló del posicionamiento de España según el Informe Global de Tecnologías de la Información. Para establecer el índice de preparación tecnológica de los países, o "Networked Readiness Index", el Foro evalúa 68 variables, que combinan datos y la percepción que tienen los altos cargos de empresas del país sobre la innovación tecnológica. Estas variables analizan aspectos del entorno como pueden ser

"Innovar en seguridad será siempre un buen negocio". Udo Helmbrecht, *ENISA*.

la existencia de "capital semilla" o la eficacia del marco legal, aspectos relacionados con la preparación como la calidad de la educación en ciencias y matemáticas o las tarifas de la conexión telefónica. También estudia aspectos ligados al uso como el número de personas con teléfonos móviles, el número de internautas o la capacidad para la innovación.

Respecto a los factores más problemáticos del ambiente de negocios para los empresarios españoles, de acuerdo con el estudio del Foro Económico Mundial, son "la dificultad del acceso a la financiación, lo restringido de las leyes en materia laboral y la ineficiencia de la burocracia gubernamental".

Según este índice España se ha mantenido en la posición número 34 en los últimos años (se analizan 133 países). "Lo más problemático es la preparación individual y el coste del acceso a las tecnologías de la información" explicó Mía, que entre las ventajas competitivas de nuestro país incluyó el desarrollo de la infraestructura, la preparación empresarial y el marco legal.

Cloud Computing

Christopher Coggrave, director de EMEA de Cloud Services de HP, habló del "Cloud computing como método para innovar y mejorar la eficiencia".

Coggrave empezó por definir la Nube, pues considera que hay mucha confusión sobre qué es y qué no es la Nube. "Los servicios de la Nube son altamente escalables y con tecnología que se puede adaptar a las necesidades del demandante. Se consume en Internet y sólo se paga por los servicios que se usan". Las tres principales Nubes: La pública como pueden ser Google o Amazon, la privada a la que se accede solo a través de invitación, y la interna o establecida por las organizaciones.

"Estas tres Nubes tienes implicaciones diferentes en términos de seguridad y el intercambio de información. En la pública te diriges al mercado masivo; la eficiencia, efectividad y el coste son críticos. En las Nubes privadas e internas hay más interés en los servicios específicos y por poder controlar las tecnologías de la información". De hecho, por ello "actualmente muchas organizaciones desconfían del área de la Nube pública y están mirando hacia el área privada e interna".

Coggrave destacó los beneficios que ofrece la Nube como el hecho de disponer de muchos servicios y solo pagar por los activos que se usan, la facilidad de manejo, la reducción de costes, la flexibilidad y que se trata de servicios escalables y con alto grado de adaptación, así como la posibilidad de seleccionar las fuentes de manera selectiva. En este sentido, "la organización tiene que saber qué servicios debe y puede dar y cuáles se pueden obtener externamente teniendo en cuenta los riesgos".

Entre los aspectos negativos del Cloud Computing para Coggrave está la longevidad ¿Qué pasa si el operador cierra? Pero el riesgo más importante, sin duda, la seguridad, puesto que cualquier problema en este sentido "puede dañar la imagen y disminuir la eficiencia de una organización".

En definitiva "todo se reduce a tener un buen entendimiento sobre lo que el proveedor de servicios puede ofrecer, pero tiene que haber un cierto grado de confianza y hacer un ajuste en términos de cuánto riesgo se está dispuesto a asumir".

"... no se trata de que el coste de la seguridad sea cero, sino de minimizar el coste de la suma de la seguridad y la inseguridad".
Fred Piper, *London University*.

"Hay que explicarse bien para que el riesgo pueda ser entendido por la pérdida de imagen y financiera que pueda representar para el negocio".

Joaquín Cidoncha, *Telefónica.*

Siete amenazas

El director de EMEA de Cloud Services de HP, citó los siete aspectos que pueden convertirse en amenazas para la Nube y que fueron identificados en un trabajo conjunto realizado por la CSA y HP. Estos son: los criminales (mal uso de los servicios de la Nube), interfaces (debilidad de la programación de las interfaces), los ataques por parte de empleados, la vulnerabilidad de las tecnologías compartidas, la pérdida o filtración de datos, la suplantación de credenciales o cuentas, y desde el punto de vista de los procesos, las amenazas pueden venir por el desconocimiento del perfil de riesgo del servicio recibido.

Las recomendaciones generales de Cogggrave para operar con confianza y seguridad en la Nube (las recomendaciones particulares para cada amenaza se pueden consultar en la presentación en la web de ISMS Forum): "Revisar las leyes y reglamentos, pues cambian dependiendo del país y la industria en la que estés; realizar una evaluación de la seguridad. Tener en cuenta los parámetros establecidos por organizaciones como la CSA y tratar de que cumplan o sean acordes con el *Service level agreement*. Pedir auditorías y tener en cuenta la opinión de organizaciones independientes e implementar controles que compensen los posibles riesgos".

Costes de la seguridad Vs. Inseguridad

Fred Piper, director del Information Security Group del Royal Holloway London University, inició su exposición en tono irónico y aclaró que había que ser conscientes de un hecho desafortunado "en teoría no hay diferencia entre la teoría y la práctica, pero en la práctica sí la hay". Por esta razón hay un profundo hueco entre idealismo y realismo "pero no sobrevives si solo haces eso. Tenemos que entender el negocio y cuándo entra el realismo".

Piper destacó que el reto actual no es diferente al de hace 30 años, todos saben que la seguridad es importante y es un acto de responsabilidad. "Si quieres seguridad tienes que pagarla", pero la inseguridad también tiene un precio pues "genera pérdidas y consecuencias directas como la mala reputación que adquiere la empresa. Por tanto, no se trata de que el coste de la seguridad sea cero, sino de minimizar el coste de la suma de la seguridad y la inseguridad".

No es protegerse de todos, es compartir la información sólo con quien quieres.

Piper definió la Seguridad de la Información con tres palabras: Confidencialidad, Integridad y Disponibilidad. "La confidencialidad porque nadie puede tener acceso sin autorización. Integridad porque los datos no pueden ser manipulados o modificados por extraños y disponibilidad para que los usuarios autorizados puedan acceder cuando la necesiten". En pocas palabras "compartir la información sólo con quien quieres".

En este sentido Piper destacó el desarrollo de políticas de seguridad, pero aclaró que estas sólo pueden ser efectivas si se desarrollan conforme a las leyes y son entendidas y aplicables por los empleados.

De izquierda a derecha: José de la Peña, Joaquín Cidoncha, Francisco Javier López Costa, Idoia Maguregui y José María Boixeda.

"El negocio no entiende de seguridad, ni de protocolo, pero entiende perfectamente de riesgos, clientes atacados y clientes bloqueados. Entiende siempre y cuando sea en términos de negocio".

Idoia Maguregui, *Bankinter.*

El reto

"La seguridad es importante y hay que actuar de manera global". Si bien no es un reto fácil, ha habido algunos pasos importantes. Entre los avances desarrollados hasta ahora, Piper citó los diferentes títulos que reconocen a los profesionales especializados en temas de Seguridad de la Información como el IISP (Institute of Information Security Professionals) de Reino Unido y centros similares en Malasia, Singapur, Holanda y Corea, así como la labor de las instituciones IMPACT (International Multilateral Programme against Cyber Threats) y ENISA (European Network and Information Security Agency).

Avances en materia de seguridad en España

Carlos Alberto Sáiz, vicepresidente de ISMS Forum Spain, fue el encargado de informar los planes de la asociación para los próximos meses. Sáiz anunció el nacimiento del **Capítulo Español del Cloud Security Alliance (CSA)** que promoverá las mejores prácticas y estándares para garantizar la Seguridad de la Información que se trata en la Nube y cuya área de interés será el cumplimiento normativo. Se trata del primer capítulo constituido por un país, ya que hasta ahora en el mundo sólo existían capítulos regionales de esta organización. En su desarrollo han participado activamente tanto la Asociación como Barcelona Digital.

Al frente del CSA Español estará Luis Buezo, responsable de EMEA para Seguridad de HP, quien detalló las "tres líneas de trabajo que seguirá la organización: Privacidad y cumplimiento normativo; sistemas de gestión de Seguridad de la Información y gestión de riesgos; y contratación, evidencias electrónicas y auditoría en la Nube".

Respecto a las novedades para el segundo semestre de 2010, se adelantaron los primeros detalles de la web **www.protegetuinformacion.com,** un portal que se lanzará a finales de este año y que formará e informará al ciudadano sobre distintos aspectos relacionados con la Seguridad de la Información. Este proyecto está siendo posible gracias al apoyo del Plan Avanza2 del Ministerio de Industria, Turismo y Comercio.

Además, Antoni Bosch, director del Data Privacy Institute de ISMS Forum, entregó las primeras certificaciones del **Certified Data Privacy Professional** (CDPP) bajo el programa de Grandfathering a las personas que acreditaron una experiencia cualificada en materia de Privacidad y Protección de datos de carácter personal. CDPP es la certificación de referencia, apoyada por los diferentes stakeholders en España para los profesionales de la Privacidad.

Irene Mía.

Gestionar los riesgos

En la primera mesa redonda de la jornada se debatió sobre "La visión del CIO acerca de la gestión de riesgos", y contó con la participación de **Joaquín Cidoncha**, Chief Information Officer (CIO) de Grupo Telefónica, **José María Boixeda**, Director de Planificación Tecnológica de Gas Natural Fenosa, **Francisco Javier López Costa,** CIO de Grupo FCC, **Idoia Maguregui**, Directora de Tecnología de Bankinter y con **José de la Peña**, Director de la revista SIC, como moderador.

Cada participante expuso su posición sobre cómo implicar a la empresa en la Seguridad de la Información. En estas grandes empresas las unidades de Seguridad de la Información tienen una gran importancia dentro del organigrama corporativo. No obstante, los debatientes estuvieron de acuerdo en que, sin importar el lugar que ocupen en la estructura de la empresa deben ser capaces de hablar el lenguaje del negocio.

"Muchas veces los peligros están dentro y los servicios externos en la Nube están mejor protegidos".

José María Boixeda, *Gas Natural Fenosa.*

Mark Bregman.

"Tienes que saber quién accede a la información adentro y fuera. Centrarnos en la información y la gente y no en la infraestructura". Mark Bregman, *Symantec.*

Para Joaquín Cidoncha (Telefónica) hay que "contextualizar la gestión del riesgo en la empresa. Se trata de capitalizarlo desde el punto de vista del negocio, no puedes hablarle de tecnología. Que el riesgo pueda ser entendido por la pérdida de imagen y financiera que pueda representar para el negocio".

En Bankinter el departamento de seguridad trabaja por el cometido de la compañía. "El negocio no entiende de seguridad, ni de protocolo, pero entiende perfectamente de riesgos, clientes atacados y clientes bloqueados. Entiende siempre y cuando sea en términos de negocio".

En el caso de FCC, que cuentan con proveedores de seguridad, consideran a los proveedores de tecnología una parte sustancial de la cadena de valor y hasta ahora las experiencias piloto que han desarrollado son satisfactorias. "Muchas veces los peligros están dentro y los servicios externos en la Nube están mejor protegidos", aclaró asimismo Boixeda de Gas Natural Fenosa, empresa que tampoco cuenta con tecnología propia.

Preocupación por la seguridad

Respecto a la pregunta de De la Peña sobre la valoración que hacen los CIOs de la gestión de riesgo de Seguridad de la Información en sus instituciones, Cidoncha explicó que "por ser una empresa eminentemente tecnológica, sabemos la importancia que tiene la Seguridad de la Información, por ello todo sistema o servicio tiene unas medidas de análisis proceso de evaluación". Respecto a la importancia de la gestión el riesgo destacó que para Telefónica el cliente y la seguridad del cliente son lo principal y por eso es de máxima importancia. En el caso de FCC, López Costa señaló que con la internacionalización de la empresa comenzó a darse importancia a la seguridad de sus sistemas de información. "Actualmente el 50% de su negocio es internacional y cuenta con empleados por todo el mundo", explicó. En el caso de Bankinter es "crucial y la apuesta por la seguridad es clara, decidida y constante", según Maguregui. Por ello, aparte de la presencia en las principales unidades de la organización, cuentan con un sistema propio desarrollado por la entidad: Bitácora.

En el caso de Gas Natural Fenosa, los riesgos principales están ligados a la naturaleza de su negocio pero con el inicio de operaciones a través de internet y la existencia de oficinas virtuales, la Seguridad de la Información ha ganado un puesto muy importante dentro de la organización lo que les ha llevado a crear figuras como el security manager.

En cuanto al futuro de la profesión, todos se mostraron convencidos de las posibilidades de crecimiento que ofrece, ya que, en un mundo cada vez más abierto, la Seguridad de la Información juega un papel cada vez más importante.

Vías para la innovación

La segunda mesa redonda trató de "Innovación e Investigación en Seguridad de la Información: Retos y Desafíos" y contó con la participación. **Mark Bregman**, Chief Technology Officer (CTO) de Symantec, **Nikolay Grebennikov**, CTO de Kaspersky Lab, **Simon Hunt**, Vicepresidente y CTO de McAfee. **Juan Miguel Velasco**, Director asociado de Servicios de Seguridad y Plataformas Comunes de Telefónica Empresas, actuó como moderador.

Para iniciar el debate entre los CTOs de tres de los fabricantes más importantes del mundo de la seguridad, Juan Miguel Velasco les preguntó sobre el desarrollo de los distintos procesos de innovación dentro de sus empresas.

Desarrollo interno + adquisición

En el caso de Symantec "la innovación forma parte de todas las unidades de negocio. Para nosotros hay dos elementos claves para la innovación, primero es la invención, la idea, pero no lo consideramos innovación hasta que la idea no tiene un impacto positivo en el mercado no lo consideramos innovación". Mark Bregman resumió las cuatro vías que usa su empresa para llegar a la innovación "la orgánica (desarrollo interno); a través de adquisiciones; colaboraciones o joint-ventures y el `harvest innovation', que es el valor añadido que aporta el uso y combinación del resto de tecnologías que no formaban parte de la decisión de compra de una compañía".

En el caso de Kaspersky Lab, la vía principal es el desarrollo interno a través de sus ingenieros expertos. "Afortunada o desafortunadamente, no podemos comprar muchas compañías. Para elaborar nuestros sistemas pensamos siem-

De izquierda a derecha: Juan Miguel Velasco, Mark Bregman, Nikolay Grebennikov y Simon Hunt.

pre en el triángulo de protección, desempeño y de fácil uso. Y, en el ámbito corporativo, tenemos en cuenta que sea fácil de administrar". Asimismo, destacó el hecho de que en su empresa cualquier trabajador puede enviar su idea al Consejo de Innovación.

En el caso de McAfee, Simon Hunt explicó que en su empresa se aplican ambas vías: desarrollo interno y por adquisición. Para fomentar la innovación dentro de la propia empresa mencionó la existencia de un programa para premiar a quienes envíen ideas al Consejo de Innovación si estas salen al mercado.

"Hoy día un notebook o smartphone por la mañana es de uso corporativo y por la tarde es de consumo de entretenimiento y aquí hay aspectos de seguridad que se deben gestionar y trabajar".

Nikolay Grebennikov, *Kaspersky lab.*

Innovar y educar

Una de las principales vías para innovar, sin duda es la colaboración con instituciones educativas. Symantec cuenta con programas en distintas universidades del mundo para patrocinar las investigaciones. Además la empresa practica la investigación y desarrollo realizando pruebas con grupos de consumidores. Bregman señalo que "los ingenieros tienen buenas ideas pero no siempre entienden las prioridades del cliente. De esta forma, trabajando juntos desde el principio, garantizan que conocen las necesidades del consumidor."

En el caso de Kaspersky Lab colaboran con universidades en Rusia, Alemania, Polonia, Reino Unido y Francia y desarrollan "programas especiales con ellas sobre Seguridad de la Información, tecnología antivirus, spam, etc, también hacemos competiciones entre equipos y diferentes instituciones", expuso Grebennikov.

En McAfee se da una mezcla y además de patrocinar programas en universidades contribuyen a través de planes para que la juventud sea consciente de la existencia del cibercrimen.

Respecto a la incorporación de la tecnología de las compañías adquiridas, todos estuvieron de acuerdo en la dificultad de esos procesos, pero destacaron la necesidad de lograr una integración que simplifique su uso para el usuario y que se dé en cada nivel de la solución.

Asimismo, sobre la adquisición de competidores hubo unanimidad al señalar que la compra de pequeñas empresas locales aporta más beneficio a su desarrollo que la adquisición de grandes competidores.

¿Las próximas innovaciones?

Para Symantec la innovación vendrá marcada por la importancia del gobierno de la información y de la identidad o autenticación del usuario. "Tienes que saber quién accede a la información adentro y fuera. Centrarnos en la información y la gente y no en la infraestructura. Cómo hacer negocio en Internet y saber que la persona con la que estamos tratando es quien dice ser", según Bregman.

Desde Kaspersky Lab el futuro está en satisfacer las necesidades reales de los clientes teniendo en cuenta el entorno actual de las tecnologías de la información. "Hoy día un notebook o smartphone por la mañana es de uso corporativo y por la tarde es de consumo de entretenimiento y aquí hay aspectos de seguridad que se deben gestionar y trabajar", comentó Grebennikov. Asimismo, los riesgos de las redes sociales y corporativas tanto desde el punto de vista del consumidor particular como corporativo es una vía a trabajar.

"El usuario final no está especializado en tecnología por lo que queremos hacer que esa innovación le ayude a protegerse". Simon Hunt, *McAfee*.

Entre las vías de desarrollo seguidas por McAfee está el objetivo de evitar que "salga" el spam, más que limitarse a frenar la entrada del mismo. Hunt especificó que "ante la proliferación de Ipads, Iphone y de otras tecnologías cada vez más accesibles, necesitamos saber que los datos están protegidos cuando se usan estos equipos. El usuario final no está especializado en tecnología por lo que queremos hacer que esa innovación le ayude a protegerse".

Seguridad para no expertos

La última mesa redonda de la jornada trató de "I+D y la seguridad como servicio a la ciudadanía" con **Miguel Ángel García**, de Departamento de Promoción de la Innovación del Centro para el Desarrollo Tecnológico Industrial (CDTI), **Xabier Mitxelena**, Presidente del Consejo Nacional Consultor sobre CyberSeguridad (CNCCS) y Director General del Grupo S21sec, **Carlos Marcos Martín**, Subdirector General de Coordinación y Estudios del Ministerio de la Presidencia, **Pilar Santamaría**, Directora de Ciberseguridad para la Región Mediterránea de CISCO, **Juan de Dios Llorens**, Consejero de Servicios de la Sociedad de la Información Ministerio de Industria, Turismo y Comercio (MITYC). Completando este panel, **Ana Borredá**, directora de Red Seguridad, actuó como moderadora.

Lograr que el ciudadano pueda navegar por la red sintiéndose seguro y respetando también las normas sin necesidad de ser un experto fue uno de los principales mensajes de esta mesa redonda.

¿Cómo conseguir que el ciudadano se sienta seguro en la Nube?

Desde el CDTI se destacó la necesidad de hacer un esfuerzo para adaptar los procesos al entorno y simplificarlos. "A veces la infracción de seguridad no viene por las herramientas sino por el uso que se hace de ellas", dijo García. Xabier Mitxelena, actual presidente del CNCCS comparó la navegación en Internet con la conducción. "Yo voy por una autopista y hago uso de ella, pero antes he hecho un curso de automoción. Los británicos ya lo están haciendo y educan sobre Seguridad de la Información desde la escuela". El representante del Ministerio de la Presidencia añadió que "como ciudadanos no tenemos que ser expertos. No hace falta ser mecánicos, pero sí tenemos que confiar en la máquina". De allí que la administración deba promover la confianza. En este sentido, a juicio de Carlos Marcos, "la ley en España está muy avanzada".

Pilar Santamaría destacó los esfuerzos de CISCO para trabajar en esta línea. La alta proliferación de la banda ancha y el crecimiento que se espera de la misma pone en evidencia la necesidad de brindar cada vez más protección al ciudadano y a las empresas.

Simon Hunt.

"Yo voy por una autopista y hago uso de ella, pero antes he hecho un curso de automoción. Los británicos ya lo están haciendo y educan sobre Seguridad de la Información desde la escuela". Xabier Mitxelena, *CNCCS*.

Para Juan de Dios Llorens del MITYC el ciudadano tiene que asimilar la Seguridad de la Información como la del automóvil. A su juicio y varios factores a tener en cuenta: "la complejidad debido al gran volumen de información, la virtualidad, la invisibilidad –un gran porcentaje de ordenadores de hogar están afectados, pero el 60% de sus dueños no es consciente de ello- y el *phishing*". Y aun más importante "incluso aunque no nos preocupe nuestro ordenador, nuestro PC puede estar dañando a otros". Por ello Llorens destacó lo positivo de iniciativas como el Plan Avanza, la oficina de seguridad del Internauta y la implantación del DNI electrónico.

Cómo aprovechar la inversión en seguridad

Los expertos ofrecieron cinco puntos de vista sobre un mismo aspecto. "No se trata de hacer cosas bonitas, sino rentables. En España hemos estado más preocupados por vender que por desarrollar tecnología en innovación", dijo Miguel Ángel García, quien también destacó que hay que pensar en el largo plazo: "la innovación es un estado mental. Hay que pensar constantemente "qué puedo desarrollar"".

Xabier Mitxelena explicó que la inversión en seguridad actualmente es alta pero que hay que ayudar a que no se pierdan las nuevas ideas y ahí es donde cobra un papel importante la Administración y su capacidad para comprar innovación. "Hay sector y es un sector capaz de generar PIB (Producto Interior Bruto)".

Para Carlos Marcos el desarrollo internacional es una vía. "Una vez que una empresa satisface los requisitos de una compañía en España, su producto se posiciona y esto le sirve de puente para entrar en Europa y Latinoamérica", especificó.

Santamaría habló de la pérdida de límites. "El trabajo ya no es un lugar, es una actividad. Cada vez hay más oportunidad de externalizar y por tanto hay más riesgo (...) La seguridad trabaja cada vez más en la vía de la prevención y esa es la mejor forma de aprovechar la inversión hecha".
El aprovechamiento de la seguridad, a juicio de Llorens "depende de la empresa, por eso es fundamental que haya un seguimiento" dentro de cada entidad.

Respecto al futuro de la innovación en seguridad en tiempos de crisis, si bien puede verse tocada, no se detendrá a juzgar por la apuesta que hicieron los participantes de la mesa redonda sobre la necesidad de continuar los desarrollos en esta materia debido a que, como recordó Llorens, "el atacante hace I+D todo el tiempo".

Transparencia y evolución ante los nuevos retos

Joshua Pennell, cofundador de Cloud Security Alliance (CSA) y Consejero Delegado de IOActive, habló sobre el "Cumplimiento normativo en la Nube". Destacó la labor del CSA como organismo que construye y promueve las mejores prácticas dentro del cloud computing. Entre las claves para lograr una armonización de la seguridad en la "Nube" destacó la necesidad de "adaptar los controles de seguridad a todos los mundos virtuales; resolver los retos que representan las distintas jurisdicciones y localizaciones geográficas, que los proveedores sean transparentes y que las herramientas evolucionen en línea con la Nube".

"El trabajo ya no es un lugar, es una actividad. Cada vez hay más oportunidad de externalizar y por tanto hay más riesgo (...) La seguridad trabaja cada vez más en la vía de la prevención y esa es la mejor forma de aprovechar la inversión hecha". Pilar Santamaría, *CISCO*.

Joaquím Vilà.

"Si la crisis hubiera llegado de manera más suave, hubiera sido perfecta para la innovación". Joaquím Vilà, *IESE*.

Por ello CSA ha desarrollado una serie de herramientas y cuestionarios disponibles, sin cargo, en su web con el fin de orientar y guiar a quienes quieran evaluar la seguridad de sus proveedores en la Nube.

Aprender de los que innovan

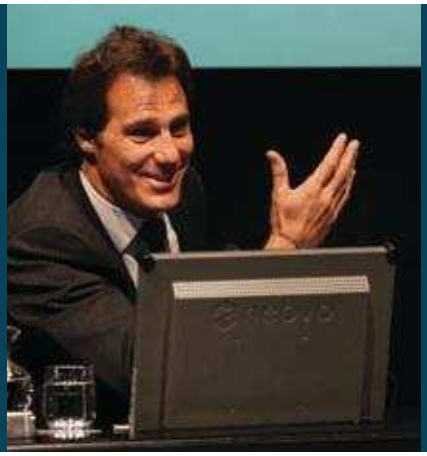
Joaquím Vilà, Profesor de dirección Estratégica y responsable de programas de formación para directivos sobre innovación de IESE, puso la guinda a la jornada identificando buenas prácticas de las compañías más innovadoras del mundo. Lo hizo analizando los casos de empresas como Ikea, Apple y Virgin, entre otras. Vilà ofreció sus cápsulas dinamizadoras de la innovación: diagnóstico de la salud de la compañía e identificar las claves para la innovación; definir el alcance del proyecto –Plan director-, formación para desarrollar habilidades, generación de ideas y resolución de problemas, valorización y priorización de proyectos detectando las oportunidades y, por último, realizar una implantación enfocada y una aplicación acotada.

Actividades 2010,
VIII Jornada Internacional

Programa VIII Jornada ISMS Forum Spain

8:45	**Acreditación – Welcome Coffee**
9:15 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 **ENISA** (European Network and Information Security Agency). **JOSEP ROF BUXÓ**, Chief Information Officer (CIO) de **Agbar.**
9:30 Keynote interview	THE FUTURE OF INFORMATION SECURITY. **David DeWalt**, Chief Executive Officer (CEO) and President of **McAfee;** Executive Keynote Interview by **Jim Reavis**, Executive Director of the **Cloud Security Alliance**.
10:00 Mesa redonda	HOW WILL CLOUD COMPUTING CHANGE ENTERPRISE IT? **Olivier Colinet**, Head of Technical Sales & Services EMEA of **Google Enterprise. Raimund Genes**, Chief Technology Officer (CTO) of **Trend Micro. Archie Reed**, Chief Technologist for Cloud Security of **HP.** Moderador: **Jim Reavis**, Executive Director of the **Cloud Security Alliance.**
11:00	**Coffee-break**
11:30 Keynote interview	SHAPING A STRATEGY FOR INFORMATION SECURITY: WHAT ARE THE KEYS? **John Brigden**, Senior Vice President EMEA of **Symantec;** Executive Keynote Interview by **Juan Miguel Velasco**, Associated Director of Security Services of **Telefónica Spain.**
12:00 Mesa redonda	SECURITY AS A BUSINESS: WHERE IS THE FUTURE? **Paolo Ardemagni**, Regional Director Southern Europe of **Check Point Software Technologies. John Brigden**, Senior Vice President EMEA of **Symantec. Natalya Kaspersky**, Chairperson of the Board of Directors of **Kaspersky Lab.** Moderador: **Juan Miguel Velasco**, Associated Director of Security Services of **Telefónica Spain.**
13:00 Ponencia	CROSS BORDER COOPERATION IN THE PROTECTION OF CRITICAL INFRASTRUCTURES. **Steve Purser**, Head of Technical Department of the **the European Network and Information Security Agency (ENISA).**
13:30 Ponencia	PROYECTOS Y ACTIVIDADES DE ISMS FORUM SPAIN. **Nathaly Rey**, Directora General de **ISMS Forum Spain.**
14:00 Ponencia	THE FUTURE OF THE CISO ROLE IN SPAIN: RESULTS AND ANALYSIS OF THE ISMS FORUM - FORRESTER IBEX35 CISO SURVEY. **Jinan Budge**, Senior Analyst of **Forrester Research.**
14:30	**Almuerzo**
16:00 Mesa redonda	EL PROYECTO DE LEY PARA PROTEGER LAS INFRAESTRUCTURAS CRÍTICAS: ¿CÓMO AFECTARÁ A LAS ORGANIZACIONES? **Miguel Ángel Abad Arranz**, Jefe del Servicio de Seguridad Lógica del **Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC). Josep Lluís Checa**, Director gerente del **Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) de la Generalitat de Catalunya. José Francisco Pereiro Seco**, Responsable de Servicios de Seguridad Tecnológica de **IBM España.** Moderador: **Jesús Milán Lobo**, Director de Riesgos Tecnológicos y Seguridad de **Bankinter.**
16:45 Mesa redonda	LA REFORMA DEL CÓDIGO PENAL: DELITOS INFORMÁTICOS Y LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS. **Elena Ballesteros**, Abogada Senior de **Ecija. Jorge Bermúdez**, Fiscal del Servicio de Criminalidad Informática de la **Fiscalía General del Estado. José Manuel Maza Martín**, Magistrado de la Sala Segunda del **Tribunal Supremo. Manuel Vázquez López**, Comisario del **Cuerpo Nacional de Policía** y la Jefe de la **Brigada de Investigación Tecnológica (BIT)** de la Comisaría General de la Policía Nacional. Moderador: **Carlos Alberto Sáiz**, Vicepresidente de **ISMS Forum Spain** y Socio de **Ecija,** Responsable del Área de Governance IT, Risk y Compliance.
17:30 Clausura	LA EVOLUCIÓN DEL RIESGO. **Victor Chapela**, CEO en **SM4RT Security Services.**

Principales conclusiones / Por Sol Núñez



El 30 de noviembre de 2010, el auditorio de la Torre Agbar de Barcelona acogió la VIII Jornada Internacional de ISMS Forum Spain bajo el título "*The Future of Information Security* – Nuevos Retos y Soluciones para un Futuro + Seguro". El evento, al que asistieron casi 300 personas, sirvió de punto de encuentro de grandes empresas e instituciones que intercambiaron experiencias y puntos de vista sobre el estado actual y futuro de la Seguridad de la Información.

La nueva era del "*networked intelligence*"

Gianluca D'Antonio, Presidente de ISMS Forum Spain y Chief Information Security Officer (CISO) del Grupo FCC, inauguró la VIII Jornada explicando el papel que la información y el conocimiento han tenido a lo largo de la historia como armas al servicio del poder y cómo los medios de información tradicionales han sido desplazados por los medios cibernéticos.

Para D'Antonio, la era de la colaboración de masa implica un '*networked intelligence*'. En el entorno actual, donde los ordenadores se parecen cada vez más a las personas y las redes a las sociedades, el reto es alcanzar un modelo de seguridad simple y transparente, aunque este planteamiento pueda resultar paradójico en un mundo cada vez más complejo.

Seguridad de la Información: Una estrategia en alza

La primera intervención del acto corrió a cargo de **Dave DeWalt,** CEO y Presidente de McAfee, quien, entrevistado por **Antonio Ramos,** Presidente de Isaca Madrid, puso sobre la mesa aspectos de máxima actualidad relacionados con la Seguridad de la Información, como la publicación de información sensible por parte de Wikileaks que ha incrementado la preocupación y el interés en la Seguridad de la Información. Según DeWalt, este interés en preservar un área tan vulnerable ha ido aumentando con el tiempo, de lo que es una clara muestra el crecimiento del sector de la seguridad en Silicon Valley durante los últimos 25 años.

"Existen muchos proveedores de seguridad porque hay muchas amenazas. Necesitamos plataformas para que todos los proveedores puedan conectarse a ellas, para comparar y relacionar las amenazas entre si".

Dave DeWalt, *McAfee.*

DeWalt explicó que al margen de las diferencias entre países y regiones del mundo con respecto a la seguridad, la inversión en la protección del ciberespacio y el desarrollo de nuevas armas defensivas en este ámbito demuestra la importancia que se está otorgando globalmente a la estrategia en Seguridad de la Información.

Para el ejecutivo, las industrias de infraestructuras son las más conscientes y preparadas para protegerse de las diferentes formas de amenazas, que han evolucionado de los iniciales hackers, que accedían desde un sótano a los sistemas ajenos por diversión, a las organizaciones sofisticadas que pueden diseñar malware complejos y orquestar fuertes ataques de phishing.

Según el ejecutivo, las nuevas tecnologías y dispositivos como móviles o pads se desarrollan de manera vertiginosa, de la misma manera que aumentan los niveles de vulnerabilidad, aspecto que se convierte en el objetivo de los criminales cibernéticos.

DeWalt expuso la necesidad de que existan plataformas que permitan la conexión de todos los proveedores para poder comparar y relacionar las amenazas existentes entre sí. "En McAfee", comentó, "recibimos al día alrededor de 5.000 millones de inputs que contienen algún tipo de malware."

Las ventajas y los retos del modelo de computing

El tema abordado en la primera mesa redonda, que contó con la participación de **Archie Reed,** Chief Technologist for Cloud Security de HP; **Olivier Colinet,** Head of Technical Sales & Services EMEA de Google y **Raimund Genes,** Chief

De izquierda a derecha: Raimund Genes, Olivier Colinet, Gianluca D´Antonio y Archie Reed.

Technology Officer (CTO) de Trend Micro, fue el modelo de Cloud Computing y la forma en que transformará a la empresa.

A este respecto, Olivier Colinet, explicó que Google está trabajando para desarrollar transparencia y confianza en materia de Cloud Computing para lo que en 2009 lanzó el dashboard, o cuadro de mandos, así como nuevos niveles de seguridad en los servicios.

Por su parte, Raimund Genes comentó las diferencias existentes entre la protección de datos europea y la norteamericana y señaló la debilidad que supone para Europa el hecho de que las directivas no estén unificadas entre sí. Esta realidad supone, según Genes, que no exista un acuerdo en el modo de fijar los estándares para el uso de las Nubes y su regulación.

Archie Reed aclaró que la gestión desde la Nube de dispositivos móviles como los pads, teléfonos móviles o blackberries, es diferente según incorporen distintas aplicaciones que puedan cambiar el aparato. Esto presenta un reto, que consiste en cómo gestionar todos estos dispositivos y sus aplicaciones sobre una base web o Nube.

Tras una primera intervención, los aspectos debatidos en la mesa se centraron en la definición del Cloud Computing, sus características, beneficios y desventajas.

Genes definió el término como "la posibilidad de tener todos los datos y el software donde uno quiera y cuando quiera", lo cual, en sus palabras, supone la "consumerización" de la informática. Sin embargo, pese a esta ventaja, las empresas se muestran en ocasiones reacias a utilizar este modelo, por lo que solicitan Nubes privadas, explicó Genes. La recomendación del CTO de Trend Micro para estas empresas es el uso de Nubes híbridas y de multipropiedad, aunque con el tiempo se impongan las de tipo público. En este punto, Reed indicó que las Nubes privadas no permiten aprovechar todos los beneficios de las Nubes, aunque sirven para desarrollar su conocimiento y acostumbrarse a la tecnología.

"Las Nubes privadas no permiten aprovechar todos los beneficios de las Nubes, pero sirven para desarrollar conocimiento y acostumbrarse a la tecnología". Archie Reed, *HP.*

Desde la perspectiva del Chief Technologist para Cloud Security de HP, la revolución de la Nube tiene mucho más que ver con el modelo de negocio y con lo que aporta a la gestión y el control del propio negocio, que con la tecnología de la misma Nube, ya que aparte de la seguridad, los temas que la afectan son más, y tienen que ver con el hecho de cómo poder mejorar su gestión. Además, explicó que se debe evaluar el riesgo de la Nube frente al valor que aporta a una compañía, ya que aunque no se puede afirmar que sea más segura que muchos otros entornos, supone grandes ventajas en costes y aporta gran agilidad al negocio: "Ya no tienes que esperar meses a que tu departamento de TI instale todos los recursos, la Nube permite elegir el menú propio de un catálogo de servicios", dijo.

"Las Nubes públicas son más seguras que muchos otros entornos hoy en día. Existe mucha confusión al respecto".

Olivier Colinet, *Google*.

Colinet defendió la seguridad de las Nubes públicas frente a la de otros entornos y destacó el inmenso avance que suponen en comparación con servicios de hosting ya existentes.

Con la vista puesta en las amenazas internas

Entrevistado por **Juan Miguel Velasco,** Director asociado de Servicios y Proyectos de Seguridad de Telefónica España, **John Brigden,** Senior Vice President EMEA de Symantec, aportó su visión sobre este tema. Según Brigden, la primera consideración para crear una estrategia de TI y de Seguridad de la Información es dar un paso atrás y hablar en el lenguaje del negocio, es decir, discutir los riesgos. En segundo lugar, hay que comprender el entorno externo de amenazas, que ahora son mucho más perniciosas, especialmente dirigidas y silenciosas. No hay que olvidarse tampoco, indicó Brigden, de evaluar las amenazas internas ya que, de forma intencionada o no, suponen importantes riesgos para la información.

Brigden lamentó que en la actualidad "la mayor amenaza para la información reside en nosotros mismos". El verdadero problema hoy, explicó, es que suele ser alguien desde dentro quien abre brechas en nuestra seguridad. Para combatirlo, propuso pasar a la acción y encontrar la manera de gestionar operativamente la seguridad. Dejó claro que para un CISO (Chief Information Security Officer) es imprescindible tener visibilidad y control y disponer de un cuadro de mandos, o dashboard que muestre dónde están sus datos críticos y sensibles y dónde están sus usuarios. La clave es disponer de políticas de acceso que no puedan ser saltadas por usuarios no autorizados.

Para Brigden, la planificación de la seguridad debe estar basada en una política concreta, ser operativa y estar centrada en la información y no en los dispositivos, para todo lo cual hay que diseñar una estrategia previa.

En relación con las diferentes normativas reconoció que no son populares en las empresas, ya que el foco de atención de éstas se centra en estimular su negocio y no en las regulaciones. No obstante, según Brigden, si una empresa está bien gestionada el cumplimiento con las regulaciones viene solo, por lo que todo consiste en llevar a cabo unas buenas prácticas de negocio.

El ejecutivo también mostró su opinión sobre los servicios de seguridad basados en la Nube e indicó que su implantación se está efectuando aún de modo lento en aquellos lugares que han empezado a adoptarlos, como Reino Unido y Escandinavia. Calculó que para 2014 el mercado de Nubes alcance unos 16.400 millones de dólares.

De izquierda a derecha: Natalya Kaspersky, John Brigden, Juan Miguel Velasco y Paolo Ardemagni.

La seguridad como negocio: ¿Hacia dónde vamos?

El futuro de la seguridad como negocio fue la temática de la segunda mesa de debate sobre la que aportaron sus opiniones **Paolo Ardemagni,** Director regional del Sur de Europa de Check Point; **Natalya Kaspersky,** Presidente del Consejo de Administración de Kaspersky y **John Brigden,** Senior Vicepresident EMEA de Symantec.

Kaspersky ve la tendencia actual de amenazas internas como un problema que aún no tiene solución ya que sólo podemos protegernos tecnológicamente con un 30 ó 40% de capacidad contra virus y amenazas externas. En cuanto a las internas, explicó que están relacionadas con los procesos, puesto que en ocasiones se implementan protecciones que posteriormente se olvidan.

En su intervención, se refirió también a los problemas potenciales de seguridad que se derivan del aumento de dispositivos, así como de entornos como las redes sociales: "Un mundo más conectado también es un mundo más inseguro". En este sentido, opina que la educación será probablemente la única vía para que la gente proteja la información que publica sobre sí misma. Esta misma idea fue compartida por Ardemagni al concluir que la educación y la formación "son críticas para conseguir que los humanos interactúen correctamente con las máquinas", lo que debería llevar a los proveedores de seguridad a promover y patrocinar la educación en las escuelas.

Ardemagni se refirió, asimismo, a los escenarios mixtos donde la Nube, los dispositivos y las tecnologías se comunican entre sí sin intervención humana, una intervención que es vista por Kaspersky como el factor malicioso. Ardemagni considera que es importante crear una plataforma de infraestructura donde vincular todas estas tecnologías así como dedicar un espacio o "contenedor de tecnologías", para aparcar las tecnologías maduras.

Brigden aseguró que la buena seguridad es invisible y eficaz y aconsejó deshacerse del factor humano de la tecnología, así como definir un nivel de automatización.

Kaspersky coincidió en que es mejor tener una seguridad invisible y que funcione a la perfección. Sin embargó, indicó que la seguridad es opuesta a la usabilidad, y que si se quiere seguridad se deben poner barreras adicionales, y se refirió a las medidas de algunas empresas que no permiten la conexión a Internet a sus trabajadores.

"Lo que se busca al proteger las infraestructuras críticas es asegurar los servicios. La solución depende de cómo reaccionan las personas, no de la tecnología".

Steve Purser, *ENISA*.

Paolo Ardemagni.

"La educación y la formación son críticas para conseguir que los humanos interactúen correctamente con las máquinas. Los proveedores de seguridad deberíamos promover y patrocinar la educación en las escuelas".

Paolo Ardemagni, *Check Point*.

Ardemagni aludió en este punto a la necesidad de establecer categorías de conexión. "Por ejemplo", explicó, "quizás debemos permitir al departamento de Marketing que utilice Youtube porque es una herramienta útil de trabajo para ellos, mientras que otros departamentos no la necesitan".

Protección de infraestructuras críticas: Cuestión de cooperación

El encuentro acogió la ponencia de **Steve Purser,** Jefe del departamento técnico de la Agencia Europea de Seguridad de las Redes y de la información (ENISA), organismo europeo que centraliza el expertise en protección de infraestructuras críticas y facilita el intercambio de información entre las instituciones públicas y privadas de la Unión Europea. Purser inició su discurso manifestando la necesidad de un enfoque colaborador entre todas las partes para conseguir proteger las infraestructuras críticas y de esta manera asegurar los servicios, puesto que la solución depende de cómo reaccionan las personas y no de la tecnología.

A continuación, Purser expuso algunas de las actividades clave desarrolladas por ENISA, entre las que se encuentran el Plan de Acción CIP (Critical Infrastructure Protection), cuyo objetivo es proteger a Europa de ciberataques a gran escala y que goza de un gran apoyo político en la Unión; el Partnership Público-Privado Europeo (PPP), que pretende crear un marco de colaboración; y el Simulacro CyberStorm, realizado con éxito el 4 de noviembre de 2010 y en la práctica difícil de gestionar, dado que en Europa no existe un mando centralizado para la defensa conjunta de un ataque cibernético.

ISMS Forum apuesta por el desarrollo de la Seguridad de la Información

La Directora General de ISMS Forum Spain, **Nathaly Rey,** fue la encargada de presentar a los asistentes el conjunto de actividades de ISMS Forum Spain, así como los proyectos en que se encuentra inmersa la Asociación.

Rey se remontó a 2007, año en el que ISMS Forum Spain nació como una asociación sin ánimo de lucro para promover el desarrollo, el conocimiento y la cultura de la Seguridad de la Información. Explicó que en la actualidad, la Asociación cuenta con más de 100 empresas asociadas y casi 750 socios, y que su creación fue posible gracias a la colaboración entre sus 12 socios fundadores: Bankinter, BT, Consejo General de Colegios de Médicos de España, Ecija, Grupo FCC, Futurespace, Gas Natural, Hewlett-Packard, Sanitas, S21sec, SGS ICS, Universidad Complutense de Madrid.

Sobre sus actividades, destacó la organización de 2 jornadas internacionales al año con más de 2.100 asistentes hasta la fecha; el **Data Privacy Institute** (DPI), creado para compartir buenas prácticas entre empresas y que otorga la certificación profesional en Data Privacy; el capítulo español de **Cloud Security Alliance** (CSA), que promueve la seguridad, la privacidad y el cumplimiento normativo en la Nube; la formación en materia de Seguridad de la Información; los diferentes estudios y publicaciones elaborados, como el estudio Forrester sobre la carrera del CISO en España; el registro de Profesionales Certificados; y la creación del portal **www.protegetuinformacion.com**, dirigido a los diferentes grupos sociales, dividido en áreas de interés y que fue puesto en marcha el 1 de noviembre de 2010 con el fin de informar y formar a los internautas en materia de seguridad.

"El lenguaje del CISO ha cambiado. Ahora los CISO hablan más del negocio de la tecnología, de las personas, de liderazgo y de cómo gestionar procesos".

Jinan Budge, *Forrester Research.*

Jinan Budge.

Ser CISO en España ¿Marcando la diferencia?

Para **Jinan Budge,** Analista senior de Forrester Research, el lenguaje del CISO en España ha cambiado. Explicó que ahora estos expertos hablan más del negocio de la tecnología, de las personas, de liderazgo y de cómo gestionar procesos.

Budge repasó los resultados del Estudio "The Future of the CISO Role in Spain", elaborado de manera conjunta con ISMS Forum, según el cual en España sólo el 30% de los CISO reportan a nivel C en la empresa, mientras que en otros países lo hacen el 55%; muchos dependen aún del departamento de TI; tienen formación técnica y estudios universitarios y dedican la mayor parte de su tiempo a asuntos estratégicos y del negocio.

El Proyecto de Ley para la protección de las Infraestructuras Críticas

La siguiente mesa de debate contó con la participación de **Miguel Ángel Abad,** Jefe del Servicio de Seguridad Lógica del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC); **Josép Lluis Checa,** Director gerente del Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) de la Generalitat de Catalunya; **José Francisco Pereiro,** Responsable de Servicios de Seguridad Tecnológica

De izquierda a derecha: Miguel Ángel Abad Arranz, Josep Lluís Checa, Jesús Milán y José Francisco Pereiro Seco.

de IBM España. El debate fue moderado por **Jesús Milán Lobo,** Responsable de Riesgos Tecnológicos y Seguridad de Bankinter.

Abad abrió el debate aportando una visión general sobre el CNPIC, encargado de definir las infraestructuras críticas (IC) en España, como las que soportan la provisión de servicios esenciales para la sociedad. El CNPIC cataloga los servicios, sectores y operadores de infraestructuras estratégicas en tres niveles de criticidad: Infraestructura complementarias, esenciales y críticas.

Desde el CNPIC se colabora de manera continua con los operadores críticos, es decir, empresas y organismos, para planificar la protección de las Infraestructuras Críticas, de las que las TI son sólo un tipo.

Abad recordó que el 11-S supuso un cambio de paradigma de seguridad con respecto a las infraestructuras críticas, al comprobar que ataques indiscriminados y directos podían hacer peligrar la provisión de servicios fundamentales para la sociedad.

Por su parte, Checa argumentó que el Proyecto de Ley sobre Infraestructuras Críticas aporta cosas positivas, como la normalización de las infraestructuras críticas y planes de actuación, inventarios o la existencia de un ente central de conocimiento de las ICs, pero también negativas, porque, como toda regulación, supone un incremento de los costes.

Pereiro añadió que la legislación debe cumplir con la protección de las infraestructuras críticas de forma integral,

"El 11-S supuso un cambio de paradigma de seguridad con respecto a las infraestructuras críticas".

Miguel Ángel Abad Arranz, *CNPIC.*

es decir, tanto físicamente como mediante sistemas lógicos porque las amenazas a la seguridad nacional pueden proceder de medios tradicionales o de ciberataques.

Una reforma del Código Penal insuficiente

La última mesa de esta Jornada tuvo como invitados a **José Manuel Maza,** Magistrado del Tribunal Supremo; **Jorge Bermúdez,** Fiscal del Servicio de Criminalidad Informática. Fiscalía Provincial de Guipúzcoa; **Manuel Vázquez,** Jefe de la Brigada de Investigación Tecnológica de la Policía Nacional; y a **Elena Ballesteros,** Abogada senior de Écija.

El tema abordado fue la reforma del Código Penal, así como los delitos informáticos y la responsabilidad penal de las personas jurídicas en esta materia.

La reforma, que entró en vigor el 23 de diciembre de 2010, fue planteada por Maza como una reforma imprescindible, pero a la vez con muchas carencias, principalmente en aspectos procesales, ya que no establece mecanismos de investigación para los delitos informáticos.

Bermúdez coincidió en este aspecto con Maza, al señalar que la reforma ha dejado sin tratar delitos como la suplan-

La reforma del código penal para incorporar delitos informáticos era muy necesaria, pero tiene muchas carencias."

José Manuel Maza, *Tribunal Supremo.*

tación de la identidad en Internet, objeto de numerosas denuncias; no ha modificado los delitos relacionados con la pornografía infantil y ha olvidado regular conductas que produzcan una denegación o limitación de servicio en los sistemas de información.

El fiscal explicó que para la Ley de Enjuiciamiento Criminal de 1988 no existen los ordenadores, por lo que estos son considerados "cajones de pruebas que nos llevamos para analizar". Asimismo, comentó la incapacidad existente para rastrear a distancia los delitos informáticos y los problemas que, con una ley llena de lagunas y carencias, implicaría trasladar la información a la Nube, donde todo hay que hacerlo a distancia.

En la misma línea, Vázquez denunció la falta de una regulación que contemple los delitos de suplantación de identidad a través de las redes sociales y reconoció que en este ámbito "seguimos rigiéndonos por parámetros de hace dos siglos". No obstante, aplaudió la iniciativa de Europol para crear un centro de Ciber Crimen, "pues la colaboración es la única manera de hacer efectiva la lucha contra estos delitos informáticos que cruzan fronteras".

Ballesteros reconoció también las deficiencias de una reforma necesaria para luchar contra fraudes como el phising "que no dejan de ser una estafa".

Para finalizar la charla, Maza señaló que la reforma de la responsabilidad penal de personas jurídicas se hace con el objetivo de equiparar a España con otros países del entorno. "No es para que la empresa responda de sus empleados, sino para que la persona jurídica responda por la posible falta de control de sus empleados en la comisión de delitos", expuso. Así, la persona jurídica, no los directivos, podrá ser condenada a ciertas penas o incluso a cierres parciales o totales de la actividad. El magistrado añadió que la reforma generará previsiblemente muchos problemas procesales y de tipo interno entre los consejos de administración, los accionistas y la dirección.

A continuación **Víctor Chapela,** CEO de Sm4rt Security Services abordó el tema de la evolución del riesgo desde la perspectiva de la evolución humana. Para Chapela, entender la evolución del riesgo supone entender tres premisas básicas: quien gestiona mejor el riesgo prevalece; no somos capaces de gestionar el riesgo digital y las entidades mejor preparadas para gestionar los riesgos serán las que perduren en el tiempo.

Chapela explicó en clave biológica cómo las mutaciones a veces son positivas y favorecen las posibilidades de supervivencia, para después explicar que los seres humanos disponemos de la capacidad para aprender a hacer aquello que nos hace mal, es decir, somos "reentrenables" y podemos transmitir nuestra experiencia para facilitar la supervivencia.

No obstante, "todo lo que pasa en Internet es inmediato y no podemos establecer patrones de actuación ante algo que es 100.000 veces más rápido que nuestro cerebro". En la actualidad, el número de conexiones crece de forma exponencial con lo que los riesgos también se incrementan

De izquierda a derecha: Manuel Vázquez, José Manuel Maza, Carlos Sáiz, Jorge Bermúdez y Elena Ballesteros.

Víctor Chapela.

en la misma medida. Por esta razón, Chapela llama alude a la experimentación como el medio para encontrar estrategias que los reduzcan.

La Jornada finalizó con una breve exposición de **Jim Reavis,** Executive Director de Cloud Security Alliance (CSA), sobre sus áreas de trabajo clave: auditorías y cumplimiento normativo de las Nubes, gestión de identidades y respuesta ante incidentes.

"Todo lo que pasa en Internet es inmediato y no podemos establecer patrones de actuación ante algo que es 100.000 veces más rápido que nuestro cerebro".

Victor Chapela, *Sm4rt Security Services.*

Conclusiones VIII Jornada Internacional

- La seguridad está creciendo como una prioridad para las empresas y para los gobiernos del mundo entero. Ello se refleja por ejemplo, en las inversiones en I+D+I y en los movimientos y operaciones societarias que se están produciendo y que se producirán en Sillicon Valley.

- La vigilancia a las amenazas internas de las organizaciones y la prevención de las fugas de información tendrán un papel fundamental en el futuro de la Seguridad de la Información.

- Para un CISO es imprescindible tener visibilidad y control de dónde están sus datos críticos y sensibles y de dónde están sus usuarios. La clave es disponer de políticas de acceso que no puedan ser saltadas por usuarios no autorizados y de un cuadro de mandos.

- Para 2014, el mercado de la Nube alcanzará unos 12.300 millones de euros.

- Las Nubes privadas no permiten aprovechar todos los beneficios de la Nube, aunque sirven para desarrollar su conocimiento y acostumbrarse a la tecnología.

- Un mundo más conectado es también un mundo más inseguro. La educación y la formación en seguridad son críticas para conseguir que los humanos interactúen correctamente con las máquinas, lo que debería llevar a los proveedores de seguridad a promover y patrocinar la educación en las escuelas.

- En la protección de las infraestructuras críticas, muchas veces la a solución depende de cómo reaccionan las personas y no de la tecnología, por ello es necesario un enfoque de máxima colaboración entre todas las partes.

- El lenguaje del CISO en España ha cambiado. Ya no se habla demasiado de cuestiones técnicas, se habla más del negocio, de la tecnología, de las personas, de liderazgo y de cómo gestionar procesos.

- La reforma del Código Penal era imprescindible, sin embargo tiene algunas carencias de orden sustantivo. Y es que ha dejado sin tratar delitos como la suplantación de la identidad en Internet, no ha modificado los delitos relacionados con la pornografía infantil, y ha olvidado tipificar conductas de denegación o limitación de servicio en los sistemas de información.

- La evolución del riesgo tiene que ver con la evolución humana. Todo lo que pasa en Internet es inmediato y actualmente no podemos establecer patrones de actuación ante algo que es 100.000 veces más rápido que nuestro cerebro. En el mundo digital, el número de conexiones crece de forma exponencial con lo que los riesgos también se incrementan en la misma medida.

Actividades 2010,
Data Privacy Institute (DPI)

El Data Privacy Institute (DPI) nació en 2009 con la vocación de aglutinar a todas las personas y organizaciones que tienen interés y responsabilidades en el ámbito de de la Privacidad y la Protección de Datos personales, promoviendo la formación y excelencia en esta área de creciente importancia. En este sentido, el DPI ha puesto en marcha la certificación **Certified Data Privacy Professional (CDPP)**, la certificación de referencia para los profesionales de la privacidad. Asimismo, en 2010 se celebraron tres foros enfocados en temas relacionados con esta materia a los que asistieron cerca de **250 profesionales**.

De izquierda a derecha: Elena Mora, Víctor Izquierdo, Antoni Bosch, Carlos Alberto Sáiz Peña, Emilio Aced y Fernando Ledrado durante el II Foro DPI.

Certified Data Privacy Professional (CDPP)

Tras su primer año de andadura, alrededor de **100 profesionales** en España se han certificado como **Certified Data Privacy Professional (CDPP).** La mayoría de ellos ha obtenido su Certificación mediante el programa de **Grandfathering,** acreditando tener sólidos conocimientos y experiencia relevante en el ámbito de la Privacidad y la Protección de Datos de carácter personal. Este proceso culminó a finales de 2010. Asimismo, se han celebrado dos convocatorias del **examen de certificación**; en junio y diciembre del pasado año.

CDPP es la primera Certificación española específicamente dirigida al área de la Privacidad. La obtención de esta Certificación acredita 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.

La Certificación está dirigida a directores de seguridad; responsables de privacidad; gestores de protección de datos; consultores; abogados y técnicos de seguridad y de sistemas con responsabilidades en esta área de creciente importancia en todo tipo de organizaciones.

Actividades 2010,
Foros del Data Privacy Institute

I Foro DPI 21-01-2010
Recetas para la Privacidad de Datos

El DPI inauguró su programación de eventos y foros para los profesionales de la Privacidad dirigiendo su mirada a uno de los sectores que más retos tiene ante sí en esta materia: el **sanitario**. La sede del Consejo General de Colegios Oficiales de Médicos de España (CGCOM) acogió a los más de 80 profesionales que asistieron a este foro titulado "**Recetas para la Privacidad de Datos**", que reunió a ponentes expertos del mundo médico y en privacidad de datos. Ellos compartieron conocimientos y experiencias en los asuntos que más preocupan tanto a los médicos como a los pacientes y a la propia Administración Pública. Se debatieron temas como la receta electrónica, el acceso a la **historia clínica** y la **convergencia e interoperabilidad en Europa**, entre otros.

Contamos con intervenciones de expertos de la Agencia de Protección de Datos de la Comunidad de Madrid (**APDCM**); de la **Unidad de Bioética y Orientación Sanitaria de la Comunidad de Madrid; Sistema Público de Salud de La Rioja (Rioja Salud);** del **Servei Català de Salut (CatSalut);** y de **AENOR.**

Asimismo, intervinieron el coordinador de la Comisión de Seguridad de la Información del Instituto de Salud Carlos III y el Coordinador de Prácticas Tuteladas de la Facultad de Farmacia de la Universidad San Pablo CEU. Este foro se celebró en colaboración con el **Consejo General de Colegios Oficiales de Médicos de España (CGCOM).**

II Foro DPI 23-05-2010
Dos años de Reglamento de la LOPD

En la víspera de la VII Jornada Internacional de ISMS Forum Spain, el DPI organizó su II Foro de Privacidad bajo el título "**Dos años de Reglamento de la LOPD**" en el Palacio de Congresos de Madrid. Este evento contó con 70 asistentes. Reuniendo a expertos de la administración pública y del sector privado, se analizaron las principales dificultades en la aplicación del nuevo Reglamento de la LOPD y los retos que presentan para las organizaciones en una mesa de debate. Este evento contó con la participación de Emilio Aced, Subdirector de la **APDCM**, Víctor Izquierdo, Director General de **INTECO**; Fernando Ledrado Gómez, Director de **Seguridad Corporativa de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid (ICM);** Elena Mora, Subdirectora de Marco Regulatorio de **MAPFRE**; y Carlos Sáiz Peña, Subdirector del DPI y Socio Director del Área Compliance IT de **Ecija**.

Asimismo, se presentaron todos los detalles de la certificación **Certified Data Privacy Professional (CDPP)**.

Por su parte, **Udo Helmbrecht**, el Director General de **ENISA**, impartió una conferencia sobre las principales modificaciones de la Directiva Europea relativa al tratamiento de los Datos Personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (2002/58/CE).

III Foro DPI 03-11-2010
Problemas actuales en Privacidad y la Seguridad de la Información

El III Foro del DPI se celebró nuevamente en la sede del CGCOM, bajo el título "**Problemas actuales de la Privacidad y la Seguridad de la Información**". Este evento contó con 70 asistentes y los temas clave que se debatieron fueron: el Impacto del Cloud Computing en la Privacidad; la Seguridad de la Información en el sector sanitario; y el Uso privado de los medios informáticos por parte de los trabajadores en las organizaciones.

Destacamos la participación de Ricard Martínez Martínez, Coordinador del Área de Estudios de la **Agencia Española de Protección de Datos (AEPD)**, representantes del **Servei Català de Salut (CatSalut),** el **CGCOM** y el **Servicio Madrileño de Salud (SERMAS)**, así como expertos del **Capítulo Español de Cloud Security Alliance (CSA-ES)**, y de empresas como **Bankinter, Check Point, Ecija, Grupo FCC** y **Microsoft**. Asimismo, participaron algunos de los primeros ***Certified Data Privacy Professionals***, que debatieron sobre los retos de los profesionales del sector.

En 2010, el DPI ha firmado acuerdos de colaboración con la APDCM y con ISACA Barcelona, con el objeto de estrechar la colaboración institucional ya existente con estas organizaciones y fomentar la certificación CDPP.

Más información en www.ismsforum.es/dpi

Actividades 2010, Cloud Security Alliance España (CSA-ES)

ISMS Forum Spain y Barcelona Digital Centro Tecnológico en colaboración con el Cloud Security Alliance (CSA), han puesto en marcha el **Capítulo Español de Cloud Security Alliance (CSA-ES).**

Como es ya conocido, CSA es la organización internacional de referencia en la que expertos de alto nivel debaten y promueven el uso de mejores prácticas para garantizar la seguridad y privacidad en el entorno del **Cloud Computing.**

Cada capítulo regional de CSA tiene un ámbito específico de interés en relación con el Cloud Computing. En este sentido, el Capítulo Español tiene como área de interés "Compliance en la Nube".

El Capítulo está organizado de la siguiente manera: **La Asamblea** es el órgano supremo de decisión y gobierno del capítulo y está por la totalidad de los miembros. La **Junta Directiva** está compuesta por diez miembros, con **Luis Buezo**, Director para EMEA de la práctica de seguridad de HP Technology Services y miembro de la Junta Directiva de ISMS Forum, como Presidente. Asimismo, CSA-ES cuenta con un Vicepresidente y ocho Vocales.

El **Consejo Asesor** es un órgano de alto nivel cuyo objeto es asesorar y proponer planes de acción al capítulo, así como liderar la interlocución con las autoridades de control, todo ello enmarcado en el desarrollo de las líneas de actividad fundacionales del capítulo. Actualmente, tres personas componen este Consejo, sin embargo, existe la posibilidad de que sean hasta seis, siempre manteniendo el equilibrio entre fabricantes, prestadores de servicios, administraciones públicas y usuarios.

El **Comité Operativo** es responsable del diseño, la implantación y el seguimiento en el día a día de las directrices y acuerdos alcanzados por la Junta Directiva en sus reuniones plenarias.

Las principales líneas de actividad del capítulo son:

- Privacidad y cumplimiento normativo en la Nube.
- SGSI y gestión de riesgos en la Nube.
- Contratación, evidencias electrónicas y auditoría en la Nube.

Estas líneas forman al mismo tiempo las áreas de atención para los tres **Grupos de Trabajo** del capítulo, que están trabajando en el primer **Report Español sobre Compliance en la Nube**, que será publicado en primavera del 2011.

cloud CSA security alliance Spanish chapter

I Encuentro Cloud Security Alliance-ES

Governance, Risk & Compliance en la Nube

29 de noviembre de 2010, Barcelona

El primer Encuentro oficial del capítulo se celebró el 29 de noviembre de 2010 en la Torre Agbar en Barcelona, bajo el título "**Governance, Risk & Compliance en la Nube**".

Este evento contó con la participación de **Jim Reavis**, Cofundador y Director ejecutivo de Cloud Security Alliance, así como de las tres Agencias autonómicas de Protección de Datos, así como de los líderes de los Grupos de Trabajo (Miguel Ángel Ballesteros, Antonio Ramos y María Luísa Rodríguez, que en dos sesiones de debate abordaron la visión del CSA-ES acerca de la Privacidad, los SGSI, la Contratación y las Evidencias en la Nube; y analizaron el control de las autoridades de protección de datos en la Nube.

El capítulo nació con **91 miembros fundadores** y en la actualidad cuenta con **200 profesionales asociados**.

Jim Reavis

Más información en:

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

Actividades 2010, Formación

Curso Analista de Riesgos en Seguridad de la Información (ARSI)

En octubre del pasado año, ISMS firmó un acuerdo En 2010 se celebró la II edición del Curso **Analista de Riesgos en Seguridad de la Información** (ARSI), un curso organizado por ISMS Forum para ayudar a los profesionales de la Seguridad de la Información a mejorar su preparación y actualizar sus conocimientos en el campo del Análisis de Riesgos, cuyos retos y soluciones están en constante cambio y evolución. La gestión de riesgos es un área de trabajo compleja: Por ello, creamos este curso intensivo, especializado, con un enfoque práctico e interactivo que cubre además el espectro teórico y metodológico necesario para afrontar un Análisis de Riesgos eficaz y exitoso.

Expertos de la Asociación, liderados por el Director Académico, diseñaron el programa y contaron con los profesionales más adecuados para cada sesión. El resultado fue un curso de cinco sesiones, enfocado en la experiencia del día a día empresarial, un profesorado con amplia experiencia aportó todas las claves para convertir a los profesionales en cualificados especialistas en Análisis de Riesgos para la Seguridad de la Información, avalado por ISMS Forum Spain.

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

En noviembre de 2010, se celebró la I Edición del Curso de **Gobierno Corporativo en Seguridad de la Información** (GCSI) 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 2011 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.

Más información en:
www.ismsforum.es/formacion

Actividades 2010, Protegetuinformacion.com

Un Portal Digital para aprender a utilizar las Nuevas Tecnologías con Seguridad

Con el objetivo contribuir a la difusión y la concienciación de la población en materia de seguridad así como fomentar el uso responsable de Internet y las Nuevas Tecnologías de la Información y la Comunicación (NTIC), **ISMS Forum** ha puesto en marcha el portal ***www.protegetuinformacion.com***, un proyecto que ha formado parte del Plan Avanza y que ha sido desarrollado con el apoyo del Ministerio de Industria, Turismo y Comercio (MITYC) junto con la participación de expertos en la elaboración de contenidos.

Esta nueva Web está dirigida a cinco grupos sociales concretos – **niños y adolescentes, padres, adultos, mayores y profesionales** – e incorpora información, consejos y otras herramientas divulgativas e informativas útiles para un aprovechamiento seguro y eficaz de la Red y de las nuevas tecnologías.

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. Así, ISMS Forum Spain pretende tratar de inculcar entre la población española, unos hábitos correctos que faciliten la seguridad de cada uno de los internautas a la hora de interactuar con las nuevas tecnologías.

> Enfocado a cinco grupos sociales: Niños y adolescentes; Padres; Adultos; Mayores; y Profesionales.

Como complementos formativos e informativos se han incorporado a la Web diversas herramientas que facilitan la comprensión de los mensajes transmitidos para cada uno de los grupos sociales:

- **Identificación de temas de interés**, donde se explican y abordan aspectos como el robo de identidad y fraude o las herramientas que existen para proteger el ordenador en el caso de los jóvenes, formas de controlar Internet o medidas técnicas de protección para los padres, phising y operaciones bancarias para adultos, compras en Internet o la utilización del DNI electrónico para mayores o los derechos y obligaciones relacionados con los equipos informáticos para profesionales, entre otros muchos.

- **Tests iniciales y finales**, que permiten comprobar a los internautas cómo evoluciona su comprensión de los riesgos y de los distintos temas recogidos en su grupo social.

- **Consejos y Avisos** para que el internauta pueda obtener de una forma más rápida información básica sobre los riesgos asociados a la utilización de Tecnologías de la información.

- **Actividades Interactivas** que hacen más amena y eficaz la comprensión de los mensajes como crucigramas, juego de tres en raya, entre otros.

- **Información adicional** para aquellos casos en los que se ha considerado necesario para que los usuarios más avanzados o con necesidades más profundas puedan encontrar la información que necesitan como, por ejemplo, recomendaciones para prevenir incidentes con virus y hackers u opciones de seguridad de Internet Explorer.

La Web ***www.protegetuinformacion.com*** se completa con un diccionario de términos y un buscador que facilitan al

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

planavanza2

Protegetuinformacion.com

La Banca Electrónica, las Redes Sociales y la Protección de Datos de carácter personal son tratados desde un lenguaje sencillo y accesible a los internautas.

usuario acceder a aquellos conceptos que desconoce o sobre los que quiere ampliar información.

Los mensajes, consejos y avisos incorporados a la Web, elaborados por expertos en Seguridad de la Información, están orientados a que el internauta pueda realizar una evaluación de riesgos adecuada y realista de sus actividades en Internet y que tome decisiones de forma responsable haciendo uso de la información disponible a través del portal ***www.protegetuinformacion.com.***

El microsite especialmente pensado para niños.

En la elaboración de los contenidos han participado:

Vicente Aceituno, Director del ISM3 Consortium.

Gianluca D'Antonio, CISO del Grupo FCC.

David Barroso, Director de e-crime de S21sec.

Kirian Bosch, Consultor.

Antoni Bosch, Director General del Institute of Audit & IT-Governance (IAITG) y Director del Data Privacy Institute (DPI).

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

Javier Carbayo, Asociado Senior del Área de Governance Risk management & Compliance (GRC) de Ecija.

Miguel Cebrián Lindström, Risk & Compliance Manager del Grupo FCC.

Leandro Nuñez, Asesor en Relaciones Internacionales de la Agencia Española de Protección de Datos (AEPD).

Agustín Palomo, Consultor de Seguridad de la Información de Ecija.

Román Ramírez, Arquitecto de Seguridad de Ferrovial.

Antonio Ramos, Presidente de Isaca Madrid.

Más información en:
www.protegetuinformacion.com

Diseñado para informar, formar y ayudar a la sociedad a utilizar de forma segura Internet y las Nuevas Tecnologías.

Actividades 2010, Colaboración en otros eventos

Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC

Dónde: Universidad Autónoma de Madrid (UAM).
Cuándo: de octubre de 2009 a julio de 2010.
Organizado por: Institute of Audit & IT-Governance (IAITG) y la UAM.

ISMS Forum Spain es una de las entidades colaboradoras en este Master multidisciplinar, que pretende formar y preparar a los alumnos para lograr con éxito la gestión y organización de la Auditoría y la Seguridad de los sistemas de información, el Gobierno de las TIC y realizar con éxito un mapa de cumplimiento normativo con especial énfasis en lo que hace referencia a los datos de carácter personal y a la legislación relacionada.

Este Master pretende formar a profesionales que puedan dirigir un Departamento de Sistemas de Información, que pueden llevar a término con todas las garantías una Auditoría de Sistemas y una Implantación y Auditoría de protección de datos y poder alcanzar la función de responsable de seguridad.

RootedCON 2010

Dónde: Auditorio del Centro de Convenciones Mapfre, Madrid.
Cuándo: 18 a 20 de marzo de 2010.
Organizado por: RootedCON.

ISMS Forum Spain colaboró en la organización y participó en la primera convocatoria de este congreso de seguridad que reunió a expertos, hackers y profesionales de todo el mundo, con el fin de aprender con ellos, desarrollar conocimientos y, sobretodo, disfrutar con la seguridad tecnológica. En el mundo inseguro en el que vivimos se producen miles de incidentes de seguridad al día. La mayoría de ellos nunca se harán públicos. Pero la realidad es que millones de ordenadores de usuarios se encuentran actualmente comprometidos y cientos de servidores son "**rooteados**" ("*hackeados*") cada día. Es necesario que todo el mundo esté concienciado sobre la importancia que tiene la seguridad informática hoy día y que nuestro conocimiento sobre dicha materia aumente y sea renovado con frecuencia. El presidente de ISMS Forum, Gianluca D´Antonio, impartió una ponencia titulada "¿Están preparadas las grandes empresas a los desafíos...?".

EuroDIG: El diálogo sobre la Gobernanza en Internet

Dónde: Madrid.
Cuándo: 29 y 30 de abril de 2010.
Organizado por: EuroDIG.

ISMS Forum y el Data Privacy Institute apoyaron esta iniciativa y participó en el evento impartiendo una presentación titulada "Managing Privacy Risk: Managing Trust?".

El Foro de la Gobernanza de Internet en España, junto con el Consejo de Europa, la Oficina Federal de Comunicación de Suiza (OFCOM) y otros actores clave en la gobernanza de Internet organizó la tercera edición del Diálogo Europeo sobre la Gobernanza de Internet (EuroDIG) en Madrid.

Conferencia Internacional de ISACA

Dónde: Cancún, México.
Cuándo: del 6 al 9 de junio de 2010.
Organizado por: ISACA.

Por primera vez, ISMS Forum participó en la **Conferencia Internacional** de ISACA, el principal evento educativo y de interrelacionamiento de esta organización en la que su comunidad de todo el mundo se reúne cada año. La Directora General de ISMS Forum, Nathaly Rey, impartió una conferencia titulada "Manejando el Riesgo de Privacidad: ¿Manejando la Confianza?".

En este foro global, se discutieron y debatieron los problemas más críticos que enfrentan los profesionales de TI y de negocios, y se descubrieron las diferentes formas en que se resuelven problemas similares alrededor del mundo. Esta conferencia atrajo a expertos, líderes, conferencistas de clase mundial, y profesionales de todo el mundo, y fue una oportunidad para colaborar y conectarse con un grupo internacional de colegas.

El fomento y difusión de una cultura sólida de la Seguridad de la Información es el fin fundacional de ISMS Forum Spain. La Asociación siempre está abierta a colaborar con proyectos y actividades que persigan este mismo objetivo a iniciativa de cualquier organización pública o privada. Por este motivo, a lo largo del año ISMS Forum Spain colabora con numerosos congresos, jornadas y reuniones organizados en torno a la Seguridad de la Información.

7th Annual CISO Executive Summit & Roundtable 2010

Dónde: Hotel Wellington, Madrid.
Cuándo: 9 y 11 de junio de 2010.
Organizado por: MIS Training Institute.

El 7º Congreso Anual CISO Executive Summit & Roundtable organizado por MIS Training Institute, tuvo lugar en Madrid.

Esta conferencia intensiva no sólo proporcionó información práctica sobre cómo se puede realizar (mejorar) la estrategia de la Seguridad de la Información en una empresa, sino que también ofreció una plataforma para el networking.

El presidente de ISMS Forum, Gianluca D´Antonio, participó en el debate *"Visionary Tips & Inspiration For Cisos Today: People, Processes & Technologies"*.

II Encuentro de la Seguridad Integral (II Seg2)

Dónde: Madrid.
Cuándo: 23 y 24 de junio de 2010.
Organizado por: Seguritecnia y Red Seguridad.

ISMS Forum participó en este evento representado por su Presidente, Gianluca D´Antonio, que aportó su visión en un debate titulado "¿Está preparado el profesional de la Seguridad para afrontar la Seguridad Global?".

Red Seguridad y Seguritecnia reunieron, por segundo año consecutivo, a los sectores de la Seguridad de la Información y la Seguridad Corporativa, en su "Encuentro de la Seguridad Integral (Seg2)". Seg2 es un evento centrado en la convergencia de la Seguridad y los planteamientos que conlleva sobre el desarrollo y la aplicación de una estrategia empresarial de Seguridad Integral.

Máster en Dirección y Gestión de Seguridad de la Información

Dónde: Escuela Técnica Superior de Ingenieros de Telecomunicaciones (ETSIT), Universidad Politécnica de Madrid.
Cuándo: de octubre de 2010 a septiembre de 2011.
Organizado por: ASIMELEC, UPM y FUNCOAS.

ISMS Forum Spain colabora con este curso de postgrado que se ha convertido ya en referente para aquellos profesionales que deseen adquirir una sólida formación que les capacite para asumir puestos de responsabilidad en el área de la seguridad de la información.

El claustro docente cuenta con algunos de los máximos expertos en la materia en nuestro país.

Día Internacional de la Seguridad de la Información, DISI 2010

Dónde: Madrid.
Cuándo: 30 de Noviembre 2010.
Organizado por: Cátedra UPM Applus+ de Seguridad y Desarrollo de la Sociedad de la Información.

ISMS Forum colaboró en la convocatoria del V Día Internacional de la Seguridad de la Información, DISI 2010. En esta edición, el Dr. Taher Elgamal pronunció la conferencia inaugural sobre el pasado, presente y el futuro del comercio electrónico.

Asimismo, participaron expertos del IRIS CERT, CCN CERT y CERT Inteco, representado por Marcos Gómez, Miembro de la Junta Directiva de ISMS Forum Spain, para debatir sobre el Esquema Nacional de Seguridad y sus los Centros de Respuesta a Incidentes de Seguridad.

Posteriormente hubo un debate sobre las Infraestructuras críticas, en el que participó entre otros David Barroso, de S21sec y también miembro de la Junta Directiva de ISMS Forum.

Actividades 2010,
Publicaciones

ISMS Forum y Forrester analizan el futuro de la Carrera del CISO en España

FORRESTER®

"El lenguaje del CISO ha cambiado. Ahora los CISO hablan más del negocio de la tecnología, de las personas, de liderazgo y de cómo gestionar procesos."

ntiene el presente resumen ejecutivo –desarrollados Durante los últimos años, los departamentos de seguridad han tenido que enfrentarse a un panorama de amenazas cada vez más complejo y a tener que desempeñar un papel mucho más visible dentro de las organizaciones, esto ha hecho que las expectativas del negocio con respecto a ellos, también hayan aumentado significativamente.

El departamento de seguridad ha pasado de tener una función técnica, y de desarrollar políticas de bajo nivel, a tener una función que debe entender y trabajar en estrecha colaboración con el negocio. Como resultado, los *Chief Information Security Officer* (CISO) necesitan tener más que nunca habilidades para entender el negocio y talento para el trato con las personas.

Para profundizar sobre esta tendencia, ISMS Forum Spain y Forrester Research han realizado una encuesta entre 24 CISOs y altos directivos de seguridad en España. En el marco de esta encuesta, se encontró que en España el CISO reporta a un nivel más bajo dentro de la organización en comparación con otros países, sin embargo, está bien posicionado para alinearse con la tendencia mundial de fomentar la existencia de departamentos de seguridad altamente visibles y orientados al negocio.

Con este estudio, ISMS Forum y Forrester concluyen que los CISOs en España:

- Reportan a niveles más bajos dentro de la organización. En comparación con otras encuestas de Forrester realizadas de manera global, en España el CISO no sólo reporta a un nivel inferior dentro de la organización, sino que además aún informa predominantemente dentro del área de Tecnología de la Información. Además, el CISO en España no es tan bien remunerado como otros CISOs a nivel mundial.

- Tienen carreras técnicas y por lo general son promovidos desde dentro de la organización. La mayoría de los CISOs tiene una formación en ciencias informáticas, en tecnologías de la información, o en seguridad y la mayoría fue promovida desde dentro del departamento de TI o de seguridad. Sin embargo, la mayoría también dijo pasar la mayor parte de su tiempo en actividades estratégicas y de negocio (planificación estratégica, desarrollo de políticas, gestión del equipo, y relaciones con el negocio).

- Se han fijado como objetivo alcanzar una posición de nivel C dentro de su organización. Ya sea en negocio, en riesgo, o en TI, los CISOs son ambiciosos y les gustaría estar en una posición de nivel C como su próximo paso en su carrera.

El Informe fue presentado por la analista senior en el marco de la VIII Jornada Internacional de ISMS Forum y el texto completo está disponible en la página web de la Asociación para sus asociados.

La publicación de herramientas divulgativas como informes y estudios monográficos, así como la traducción y la edición en castellano de manuales y guías de referencia, es una de las principales actividades de ISMS Forum Spain.

Empresas asociadas

En diciembre de 2010, cerca 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.

- A.C.S. Informaticos
- Abast Systems
- Abertis Infraestructuras
- Accenture
- Acens Technologies
- Agaex Informática
- Aguagest Services Company
- Allglobalnames
- Anyhelp International
- Applus+, LGAI Technological Center
- Ascêndia Reingeniería + Consultoría
- Asistencia Sanitaria Interprovincial (ASISA)
- Asociación Española de Destrucción Confidencial de Información (AEDCI)
- Asociación Española Seguridad en Sistemas de Información (ISSA España)
- Atos Origin
- Audisec Seguridad de la Información
- Auria Tecnología de la Información y el Conocimiento (AURIATIC)
- Bankinter
- BDO Auditores
- British Standards Institution España (BSI)
- BT España
- ONO
- Caixa Penedès
- Cajamar Caja Rural
- Campofrio Food Group
- Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI)
- Check Point Software Technologies
- Compañía Española de Petróleos (CEPSA)
- Comparex España
- Consejo General de Colegios Oficiales de Médico (OMC)
- Deloitte
- Destruccion Confidencial de Documentacion (DCD)
- Det Norske Veritas Business Assurance España (DNV)
- Ecija
- Empresa Publica Desarrollo Agrario y Pesquero (DAP)
- Endesa
- Ernst & Young
- Eulen Seguridad
- Everis Spain
- Ferrovial
- Fomento de Construcciones y Contratas (Grupo FCC)
- Future Space
- Gas Natural Informática
- Gigatrust Spain
- GMV Soluciones Globales Internet
- Grupo Generali
- Grupo Intermark 96
- Grupo S21sec Gestión
- Hewlett-Packard Española (HP)
- IDN Servicios Integrales
- Índigo Governance, Risk & Compliance
- Indra Sistemas
- Ingeniería e Integración Avanzadas (Ingenia)
- Instituto Nacional de Tecnologías de la Comunicación (INTECO)
- International Business Machines (IBM)
- Internet Security Auditors (ISecAuditors)
- Interxion España
- Ironwall Strategic Security Systems
- Juniper Networks
- Kabel Sistemas de Información
- Kaspersky Lab
- KPMG Asesores
- Krell Security
- Leaseplan Servicios
- Lloyd's Register Quality Assurance (LRQA)
- McAfee
- Mutua Madrileña
- Nexus IT
- Ocaso
- Oesia Networks
- Open3s Open Source And Security Services
- Panda Security
- Passwordbank Technologies
- Pricewaterhousecoopers (PWC)
- Promotora de Informaciones (Grupo PRISA)
- Red Seguridad
- Repsol
- Revista Dintel Alta Dirección
- S2 Grupo
- Sage Logic
- SGS ICS Ibérica
- Sistemas Informaticos Abiertos (Grupo SIA)
- Sophos Iberia
- Steria Ibérica
- Symantec
- Tecnocom Telecomunicaciones y Energía
- Telefónica
- Trend Micro
- T-Systems ITC Iberia
- Universidad Complutense de Madrid (UCM)
- Verizon Spain
- Zitralia Seguridad Informática


Seguridad de la información:
¿Cómo innovar
en tiempos de crisis?


OLIVIER COLINET


ISMS
Forum Spain


Creación del portal
Protegetuinformacion.com
ISMS
Forum Spain
ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO
DE LA SEGURIDAD DE LA INFORMACIÓN

Notas

Juan Bravo, 3-Portal A
28006 Madrid
Teléfono: +34 914 367 413
Fax: +34 914 367 365
Web: www.ismsforum.es

ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN