ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Memoria de Actividades
ISMS Forum Spain

2008

Redacción: Dirección de Comunicación de ISMS Forum Spain

Fotografía: Ángel Martínez
Miguel Ruiz
Miguel Torres

Diseño: Jon Arriaga

Madrid, enero de 2009

Índice

Carta del presidente 7

Socios Fundadores, Junta Directiva y Equipo de Gestión 8

Presentación de la Asociación 9

Colaboradores y patrocinadores 11

Actividades 2008 13

Jornadas Internacionales 13

- III Jornada: Compliance en Seguridad de la Información 14
- IV Jornada: Amenazas Internas y Externas a la Seguridad de la Información hoy 24

Otras sesiones formativas 32

- Conferencia de Eugene Kaspersky 32

Otras iniciativas 34

- Breakfast & Workshop "Data Leak Prevention" 34
- Consultoría estratégica 34
- Registro de Profesionales Certificados Online 34

Convenios de colaboración 35

Colaboración con otras entidades 36

Publicaciones 38

Reconocimientos 38

Empresas asociadas 39

Memoria de Actividades
ISMS Forum Spain

08

0 8

Gianluca D'Antonio
Presidente

Estimados socios, colaboradores y amigos:

Finaliza el segundo año de actividad de la Asociación, y todos los que estamos trabajando en la organización de sus actividades tenemos la sensación de que algo ha cambiado en nuestro sector desde que comenzamos a desarrollar esta iniciativa a la que se han unido, desde entonces, más de cien empresas y de 600 profesionales. Los socios asisten a nuestras jornadas internacionales y nos evalúan con muy buenas calificaciones, trasmitiéndonos así un mensaje de satisfacción que nos llena de optimismo y nos impone la obligación de seguir mejorando. Las empresas nos responden y apoyan en la financiación de nuestras iniciativas, que de otro modo serían sencillamente irrealizables, pues las cuotas de los miembros asociados se mantienen, como todos sabéis, en el ámbito de lo simbólico. Nos llegan mensajes y sugerencias para que traigamos a debatir con nuestros socios a gurús y expertos mundiales de muy diversas especialidades, mensajes siempre expresados en la seguridad de que, si nos lo proponemos, lograremos traer a dichos expertos. Claramente, desde el comienzo de nuestra andadura nos hemos centrado en la calidad, y me enorgullece decir que hemos recibido por ello numerosas felicitaciones por parte de las distintas partes implicadas.

Y es que, en dos años, los participantes en nuestras conferencias (en Madrid y, por primera vez en 2008, también en Barcelona) han asistido a charlas y debates con expertos de renombre mundial como Bruce Schneier, Howard Schmidt o Eugene Kaspersky; con altos responsables de los organismos nacionales de referencia en nuestra materia (como INTECO, el CNI, la AEPD, la Guardia Civil, AENOR y, por supuesto, el MITYC) y de algunas de las principales organizaciones internacionales relacionadas con la seguridad de la información (Consejo de Europa, ISACA, OCEG, ISSA, IRCA, RAISE Forum, por citar algunas) y, cómo no, con responsables de seguridad de la información de grandes corporaciones y empresas que han compartido con nosotros su experiencia y conocimientos. Todo ello conforma uno de los objetivos que nos marcamos en su día los fundadores de la Asociación: queríamos abrir en nuestro sector –a veces demasiado endogámico- una ventana al exterior, y establecer nuevos vínculos internacionales que nos dieran una perspectiva más global de nuestra industria, de sus retos y preocupaciones, y de las soluciones que afloran desde las distintas aproximaciones al problema en los cinco continentes. Queríamos fomentar la creación de un "espíritu sectorial" del que nos parecía que carece la Seguridad de la Información en España, y crear vías de comunicación y encuentro para que las redes de contactos y la información circulen con fluidez entre los profesionales y expertos del sector. Queríamos, en definitiva, dar un impulso a la internacionalización y a la búsqueda de la excelencia de nuestro ámbito profesional. Sería absurdo decir que lo hemos conseguido en los dos años que han pasado desde que se firmó el acta fundacional de ***ISMS Forum Spain****: esta es una tarea que requiere su tiempo y sus etapas. Pero sí creo que estamos en la vía acertada para ir progresando en esas líneas de trabajo, y desde luego afirmo que nos sobran el entusiasmo y las ganas de avanzar por este camino.*

Tras dos años, llega la hora de evolucionar, de crecer, y de ofrecer más valor añadido a los socios. Espero sinceramente que los nuevos proyectos que queremos arrancar en 2009 tengan la misma aceptación entre los asociados. No quiero despedir estas líneas sin agradecer profundamente su colaboración a todos los que han hecho posibles los logros de ***ISMS Forum Spain****: a nuestros Gold Sponsor y demás patrocinadores; a los miembros de nuestra Junta Directiva; a todas las entidades que nos han prestado su valiosa colaboración; al excelente equipo de gestión y, por supuesto, a todos los socios que con sus ideas y sugerencias, y -por encima de todo- con su participación, dotan de sentido a este proyecto.*

Socios Fundadores

Junta Directiva 2008

En la imagen, parte de la Junta Directiva. De izda a dcha: Andreu Bravo, Luis J. Buezo, Mar Sánchez, Gianluca D'Antonio, Carlos A. Sáiz, Jesús Milán, Antonio Ramos.

Presidente:

Gianluca D'Antonio*. *CISO del Grupo FCC.*

Vicepresidente y Secretario:

Carlos Alberto Saiz Peña*. *Socio del Área de Nuevas Tecnologías, Protección de Datos y Compliance de Écija.*

Vicesecretaria:

Mar Sánchez Caro. *Security Manager Spain and LatAm, BT España.*

Vocales:

Luis J. Buezo*. *Director de la Práctica de Seguridad, HEWLETT-PACKARD Española.*
Andreu Bravo*. *Responsable de Seguridad de la Información, GAS NATURAL.*
Joan Camps Pons. *Director de Proyectos y de la Unidad Tecnológica del Consejo General de Colegios de Médicos de España.*
Daevid A. Lane. *Director de Seguridad, FUTURESPACE.*
Enrique Martín Menéndez. *Responsable de Seguridad Informática. SANITAS.*
Jesús Milán*. *Director de Seguridad de Sistemas, BANKINTER.*
Fernando Pescador. *Director Servicios Informáticos. Universidad Complutense Madrid.*
Antonio Ramos*. *Director de la Unidad de Consultoría y Auditoría Informática, S21SEC.*
Álvaro Rodríguez de Roa. *Director de Certificación de Servicios, SGS ICS IBÉRICA.*
Ana Belén Santos Pintor. *Responsable de Proyectos en el área de e-Confianza de INTECO.*

** Miembros del Comité Operativo de la Junta Directiva.*

Equipo de Gestión:

Directora: **Cristina Saura**
Coordinadora de Eventos: **Germaine Custers**
Colaboradores: **Antonio Sánchez** *(Web y BB.DD)*, **Jon Arriaga** *(Diseño y Maquetación)*, **Olga Torres** *(Administración)*, **Javier Sánchez** *(Asesor Fiscal)*, **Paloma García Cámara** *(Atención a socios)*.

Asociación Española para el Fomento de la Seguridad de la Información

ISMS Forum Spain es una asociación sin ánimo de lucro, creada en 2007, **para el Fomento de la Seguridad de la Información en España.** Además, **ISMS Forum Spain** es el Capítulo Español de **ISMS International User Group (IUG),** organización que promueve el conocimiento e implementación de los Sistemas de Gestión de la Seguridad de la Información en todo el mundo, de acuerdo con los estándares ISO 27000.

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

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

ISMS Forum Spain tiene ya a **95 empresas asociadas** (cada una de las cuales puede nombrar hasta ocho socios de pleno derecho). Además, numerosos expertos del sector se han asociado de manera independiente. ISMS Forum Spain cuenta hoy con más de **500 profesionales asociados,** ya sea a través de sus empresas o por iniciativa individual. La Asociación para el Fomento de la Seguridad de la Información es ya, por tanto, 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, que se ampliará en breve con un nuevo **Registro de Empresas Certificadas en ISO27001 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.

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


III Jornada
Claves y
Una visión glob


rvice Providers
ISMS


FORRESTER


III Jornada Internacional
Compliance en Seguridad de la Información
Claves y Tendencias
Una visión global del presente y una mirada al futuro
29 de mayo de 2008, Madrid
ISMS
accenture
IBM
LOPD

Agradecimientos

Apoyo institucional

La Asociación agradece expresamente al organismo público **INTECO (Instituto Nacional de Tecnologías de la Comunicación)** su apreciada colaboración y apoyo institucional.

INTECO
Instituto Nacional
de Tecnologías
de la Comunicación

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 SPONSORS de la Asociación en 2008:

accenture — Alto rendimiento. Hecho realidad.
dintel FUNDACIÓN
ERNST & YOUNG — Quality In Everything We Do
FCC
hp invent
IBM
McAfee
symantec
Telefónica

Otros Patrocinadores y Colaboradores

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

Agbar
a+ auditoría y seguridad
COMPUTERWORLD
ECIJA
ESA Security — Seguridad de la Información
FORRESTER
funcoas
ISACA
ISSA España
OCEG
PANDA
Reed Exhibitions
red seguridad
S21sec — La seguridad digital del futuro, hoy
sia
steria

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

Actividades 2008, 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. **Cerca de mil participantes en las cuatro jornadas organizadas en 2007 - 2008** 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, etcétera.

En 2008, por primera vez, se organiza una Jornada Internacional fuera de Madrid. Elegimos para ello un escenario privilegiado en Barcelona, el impresionante auditorio de la vanguardista Torre AGBAR. Fue el 13 de noviembre y se batió el **récord de asistencia** con 270 participantes.

Asistencia a las Jornadas Internacionales de ISMS Fórum Spain

Eventos	2007		2008	
	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**
Número de Asistentes	202	256	258	270

Actividades 2008,
III Jornada Internacional

ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Organiza: ISMS Forum Spain

Con la colaboración de: INTECO — Instituto Nacional de Tecnologías de la Comunicación

Ponentes del más alto nivel nos aportarán, a lo largo de una completa jornada, su visión del *estado del arte* en cumplimiento normativo en un contexto global pero muy centrado en tres ámbitos geográficos: **España, Europa** y **Estados Unidos**.

Objetivo: comprender las líneas estratégicas que seguirá la regulación en los próximos años y obtener unas pautas claras para liderar la implementación de las **mejores prácticas** en *Compliance*.

Programa completo e inscripción: www.ismsforum.es , hasta el 19 de mayo de 2008.
Tasas: Socios de ISMS Forum Spain: **gratuito**. No socios: 360€. **Se admitirán las inscripciones por riguroso orden de llegada**, hasta cubrir el aforo. La jornada incluye documentación, coffee-break y almuerzo.
Se facilitará traducción simultánea inglés-español.

Patrocinadores Oro:

accenture — High performance. Delivered. · dintel · ECIJA · ERNST & YOUNG — Quality In Everything We Do · ESA Security — Seguridad de la Información · FCC · hp invent · IBM · S21sec — La seguridad digital del futuro, hoy · SGS · steria · symantec · Telefónica

Media Partners: auditoría y seguridad · COMPUTERWORLD · infosecurity IBERIA · red seguridad

¿Por qué una Jornada sobre Cumplimiento Normativo?

En primer lugar, a petición de los propios asociados, que habían manifestado repetidamente su interés en el análisis de este tema. Por otro lado, la regulación y el cumplimiento normativo salieron a relucir como **asuntos clave para el futuro de la seguridad de la información** a lo largo de las ponencias de la II Jornada Internacional organizada por la Asociación.

Así, nos enfrentamos a tiempos empresariales de normativa, regulación y control. El desarrollo económico de estos años, la globalización de productos y/o servicios en las empresas y el fomento de las redes de comunicación social conllevan el necesario impulso de cautelas para respetar los derechos e intereses de clientes, trabajadores y accionistas. Esa búsqueda de transparencia en la actividad de las empresas y las administraciones públicas se garantiza a través de normas y leyes, así como de estándares y buenas prácticas equilibradas y seguidas para aproximarse a los mejores niveles posibles de Responsabilidad Social Corporativa.

Por todo ello la Seguridad de la Información ocupa un lugar importante en el llamado *Compliance* o Cumplimiento Normativo. La toma de decisiones y los procesos son cada vez más automáticos gracias a la tecnología, basándose de forma preponderante en la información que maneja el negocio. Ello conlleva la proliferación de más normas y leyes de obligado cumplimiento (Como la LOPD y su Reglamento, LISI, Conservación de datos, Firma y Facturación Electrónica, Basilea, SOX o MiFID) y la necesidad de establecer controles para proteger la información del negocio, a pesar de no ser obligatorio por ley: trazabilidad de la identidad digital, normas de uso de correo electrónico, normas de clasificación de la información, etcétera.

¿Qué depara el futuro a las organizaciones empresariales en lo que se refiere a normativa y legislación, tanto en el ámbito global como en el local? ¿Cuándo deja la certificación de ser una opción voluntaria, para convertirse en un requisito legal o, simplemente, una condición indispensable para competir en el mercado? ¿Es la regulación una asignatura pendiente de la seguridad de la información? ¿O lo son los mecanismos para asegurar su implantación y cumplimiento? Son, sin duda, cuestiones importantes para todos los profesionales del sector.

De todo ello se habló en la III Jornada Internacional con el **objetivo** de obtener una completa visión del estado del arte en cumplimiento normativo y comprender las líneas estratégicas que seguirá la regulación en los próximos años. Y obtener a partir de esa información pautas para liderar la implementación de las mejores prácticas en *Compliance*.

Ponentes del máximo nivel

ISMS Forum Spain buscó para esta jornada a ponentes del más alto nivel, que expusieron la actualidad y las tendencias futuras del Compliance en un contexto global pero muy centrado en tres ámbitos geográficos: España, Europa y Estados Unidos. Para ello se invitó en esta ocasión a conferenciantes procedentes, además de **España**, de **EE.UU, Grecia, Colombia, Hong Kong** (China), **Reino Unido, Holanda** y **Dinamarca.**

Pierre Noel (IBM).

Destacamos la presencia de:

- Prestigiosos analistas internacionales especialistas en el tema (como **Thomas Raschke,** de Forrester Research y **Pierre Noel** de IBM).

- El máximo responsable de OCEG - **Open Compliance & Ethics Group,** una de las organizaciones norteamericanas referentes a nivel mundial en cumplimiento normativo- **Scott L. Mitchell.**

- Representantes de la Administración española (**Enrique Martínez,** director de INTECO, **Ricard Martínez,** Coordinador Área de Estudios de la AEPD y **Antonio Alcolea,** experto del MITYC).

- Uno de los expertos en liderazgo y gestión de personas más reconocidos en nuestro país, **Santiago Álvarez de Mon,** que aportó su humanista visión de la organización empresarial y expuso cómo la comunicación es un elemento clave en las organizaciones.

Principales conclusiones

Buen Gobierno, Seguridad de la Información, Gestión del Riesgo y Cumplimiento Normativo, claves para la empresa del siglo XXI.


Lucio A. Molina (ISACA)

Casi una veintena de ponentes de media docena de países se dieron cita el 29 de mayo de 2008 en el céntrico hotel Husa-Princesa de Madrid, que albergó la III Jornada Internacional de ISMS Forum Spain. Scott L. Mitchell, Pierre Noel, Hervé Gabadou o Samantha Bruyn fueron algunos de los prestigiosos ponentes que construyeron una densa jornada de información ante 258 asistentes del ámbito de los Sistemas de Gestión de la Seguridad de la Información (SGSI) y del área de Compliance.

El presidente de **ISMS Forum Spain**, Gianluca D'Antonio, introdujo la jornada destacando que "estamos inmersos en una proliferación de normas que impulsan la seguridad de la información" debido a su importancia estratégica para empresas y países. "No tiene sentido enfocar la seguridad de la información desde ámbitos nacionales -dijo- cuando el crimen y las amenazas son globales, y por eso necesitamos acometer las acciones sin fronteras". Estas palabras precedieron la intervención del ingeniero colombiano experto en Auditoría de Sistemas **Lucio Augusto Molina** (ex vicepresidente internacional de ISACA, en la imagen superior), quien, en la misma línea, señaló que "la importancia del cumplimiento de las normativas internas y externas en Seguridad de la Información es fundamental en pleno auge del cibercrimen, un problema cada vez más frecuente cuyos efectos y consecuencias hay que mitigar". Colombia se ha convertido en uno de los referentes en materia de SGSI debido a su compleja situación política con la amenaza de las FARC. Molina denunció que los problemas se derivan de la falta de controles y de colaboración de algunas entidades, sobre todo financieras, y del incumplimiento de las normativas como Basilea II. "El riesgo existe. Lo hemos visto en la tragedia del World Trade Center y en otras catástrofes. La informática no es inmune y hay que mitigar los daños". Añadió, además, que ahora es más fácil delinquir "virtualmente", ya que "en los años 80 los *hackers* necesitaban experiencia y pericia; a día de hoy cada vez se requieren menos conocimientos para crear virus y se puede descargar el software necesario para ello de Internet". El asesor externo de la Bolsa bogoteña apuntó también que se trata de un fenómeno social: "los niños -dijo- aprenden en su casa, de sus padres, que la piratería no es mala" y hay que educarles. En otro orden de cosas señaló que "todavía la mayoría de usuarios de una *blackberry* o un *pendrive* no usa claves, ignoran su debilidad". Y advirtió que "el riesgo es evidente y, aunque hay niveles, la III Guerra Mundial probablemente será informática, basada en ataques informáticos, en aislar los sistemas de comunicaciones... ¿Qué tenemos que proteger? La información, su confidencialidad, su sensibilidad. La mayor parte de la población confía en que las empresas que guardan sus datos los custodian, pero pueden caer en malas manos".

Sobre la legalidad del software en las empresas y las sanciones señaló que para el cumplimiento normativo es fundamental tener apoyo interno y externo, "de forma que el cliente pueda depositar en nosotros su confianza y estar tranquilo". Departió también Molina sobre la oportunidad del uso de herramientas de prevención y detección, y destacó finalmente que las leyes y reglamentaciones deben acompañarse de "la educación al usuario en estas prácticas, la implementación de políticas de seguridad y gestión

De izda. a dcha: Eduardo Ruiz (HP), Antonio Alcolea (MITYC), Hervé Gabadou y Álvaro Ecija (Ecija).

de riesgos, llevadas a cabo por personal cualificado para ello en las empresas, y la capacitación al *security officer* para ejercer el poder con autoridad". Otras alternativas a la hora de gestionar la seguridad para el colombiano pasan por la externalización de estos trabajos, de forma que puedan desarrollarse con independencia y objetividad. Tras repasar los procesos de auditoría interna, los planes de control y recuperación y la necesidad de documentar los procesos, Molina señaló que es fundamental compartir las experiencias, porque "la seguridad es del mundo, no de las personas. Y tenemos que cumplir y ampliar la normativa para luchar contra el cibercrimen".

Las palabras de Molina dieron paso al debate abierto entre los abogados **Álvaro Écija** (Écija Abogados), especialista en Derecho y TIC; **Hervé Gabadou**, director de TI y Telecomunicaciones en el bufete francés Courtois Lebel; y **Antonio Alcolea**, Jefe del Área de seguridad de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del MITYC. Moderados por **Eduardo Ruiz** de HP Ibérica, recibieron la pregunta clave del debate: "¿Hacia dónde va el desarrollo normativo y de cumplimiento en materia de Seguridad de la Información?" Écija fue el primero en señalar que "todos sabemos que las normas están para cumplirlas, pero la norma de cumplimiento se caracteriza por imponer obligaciones técnicas además de las jurídicas"; en

"Una vez convencida la alta Dirección de la importancia de la Seguridad de la información, hay que pensar cómo integrarnos en la estrategia y en la marca"

Ramiro Mirones, *Ernst&Young*

Francia, sin embargo, según explicó Gabadou, "la normativa se impone mientras que los estándares son apoyos. La Agencia de Protección de Datos transpone las directivas europeas en la materia, pero en Gran Bretaña y España es diferente, lo que complica en alto grado la actividad de las multinacionales". Para Écija "estas diferencias en Europa traerán problemas, por ello se intenta que haya unos estándares mínimos comunes. El control de la información es una preocupación global y el conflicto entre Seguridad Pública y Privacidad requiere coordinación entre los países", dijo. Así pues, todos estuvieron de acuerdo en la necesidad de imponer estándares y en la esperanza depositada

"El riesgo es evidente y, aunque hay niveles, la III Guerra Mundial probablemente será informática, basada en ataques informáticos, en aislar los sistemas de comunicaciones... ¿Qué tenemos que proteger? La información, su confidencialidad, su sensibilidad. La mayor parte de la población confía en que las empresas que guardan sus datos los custodian, pero es obvio que pueden caer en malas manos"

Lucio Molina, *ex vicepresidente de ISACA*

en el Grupo del Artículo 29 de la Comisión Europea que próximamente será presidido por el actual Presidente de la Agencia francesa de Protección de Datos.

La próxima revisión de la Directiva europea sobre protección de datos y confidencialidad fue otro de los temas "calientes" del debate por las posibles contradicciones entre Seguridad Pública y Derecho a la intimidad y la Privacidad. Desde EE.UU. quieren una normativa excesivamente estricta, "quieren saberlo todo -dijo Gabadou- y en Francia queremos un sistema proporcional. Y, además, hay otro problema: la tecnología avanza mucho más rápido que las autoridades". Écija señaló también que "en España, por ejemplo, la videovigilancia está incluida en la Ley de Protección de Datos, mientras que en Francia no. La proporcionalidad es la clave en esta carrera que no podemos perder contra la ciber delincuencia organizada. Se necesita energía, sostenibilidad y confianza". Lo más destacable del modelo, a juicio de estos expertos, es "buscar normas compartidas y que se pretendan cumplir por empresas y ciudadanos. Compartir y ser compatibles para evolucionar".

A la pregunta del moderador sobre el exceso normativo, el representante de la Administración señaló que "analizamos los sectores que más afectan al ciudadano y de ahí ha surgido la Ley para la Sociedad de la Información, LISI, que se supervisa desde la Secretaría de Estado, ya sea por demandas o de oficio". Écija, por su parte, apuntó que "hay muchas leyes pero pocas herramientas para hacer que se cumplan", mientras el francés indicó que "el problema es que hay que educar a la ciudadanía en el cumplimiento de estas leyes y en sus derechos". Sobre otras iniciativas como el DNI o la firma electrónicos, Alcolea señaló que "intentamos favorecer y promover que los empresarios se comprometan con estos temas para impulsar la eSociedad en España". Muchas eran las manos alzadas para hacer preguntas, pero el tiempo

apremiaba y **Samantha Bruyn**, responsable de Compliance de ING Real Estate comenzó su ponencia explicando la ventaja competitiva que supone integrar esta área en el plan estratégico y en el día a día de las compañías. Inició con dos palabras "Honestidad" y "Transparencia". Según Bruyn "hay que ser sincero a la hora de gestionar y mitigar el riesgo, los encargados de Seguridad y *Compliance* no son agentes, son consultores que tratan no sólo de que se cumpla la ley sino también los compromisos". Bruyn dedicó su presentación a demostrar que el cumplimiento es un coste necesario pero también, y más importante, constituye una ventaja competitiva ya que "la crisis de las *subprime* ha demostrado la importancia de ser transparente ante el riesgo de perder una reputación granjeada durante años. Mantener la confianza de todos los agentes implicados (accionistas, inversores, proveedores, clientes, empleados...) es fundamental y no puede hacerse sin *compliance*". Según señaló, es un departamento que debe ser firme y debe depender del área de riesgo y no del Departamento Legal, porque hay que valorar y cuantificar el riesgo de cumplimiento, que "supone riesgo reputacional, financiero, de seguridad..." La responsable ING Real Estate apuntó algunas claves para asegurar la eficacia de estos departamentos, como aumentar los recursos dedicados a *compliance*, marcar objetivos y tener reglas claras (con políticas globales y locales). Para ella, "en España hay pocos empleados formados en estas materias y no hay apenas cursos de formación específicos en Europa; pese a que los directivos son conscientes de la importancia de cumplir las normativas de sistemas, no las implementan con tiempo suficiente"; a su juicio, "el mercado va a demandar cada vez más este tipo de profesionales, capaces de cuantificar los riesgos, hacer que se cumplan normas y

Pierre Noel (IBM).

Samantha Bruyn (ING Real State).

saber explicarlo" auguró. "El responsable de cumplimiento se ve en la obligación de multiplicarse porque tendrá que estar en varios sitios a la vez y no es fácil encontrar personal para asumir el cumplimiento basado en el riesgo" reconoció para finalizar.

Tras un café llegó la presentación de **Pierre Noel**, Worldwide Information Security & Risk Management Evangelist de IBM Corp, sobre la Seguridad y la Gestión del Riesgo. "Pensar que no tendrás incidencias es una ridiculez, cada vez más la seguridad es la gestión del riesgo", comenzó Noel, animado y convincente. "La formación y la educación son lo más importante y sin embargo es a lo que dedicamos menos dinero; de la misma forma, tenemos que evitar ser conocidos como "la gente de los antivirus", tenemos que elevar el discurso para dar a la seguridad la importancia que tiene". En una escalada desde la inexistencia de seguridad a la división del departamento en Sistemas, por un lado, y Gestión del Riesgo, por otro, sólo hay tres pasos: blindarse, prevenir y consolidar.

Con profusión de ejemplos, datos (como que el 43,5% de los incidentes proviene del interior de las corporaciones y, la mayor parte de ellos de empleados varones) y metáforas, Noel señaló que los buenos SGSI se basan en una matriz de riesgos, una base de datos de pérdidas, controles mitigadores, mediciones constantes que demuestren los hechos y la elaboración de informes "legibles" y "comunicables". Coincidió, pues con Bruyn en señalar que tanto la gestión del riesgo como la capacidad de comunicación son claves a la hora de posicionar a los departamentos de Seguridad y Compliance en el lugar que les corresponde.

El público lanzó numerosas preguntas en los coloquios.

Scott L. Mitchell tomó el relevo y comenzó su intervención presentando el *think thank* norteamericano que preside, el Open Compliance & Ethics Group, OCEG, que cuenta con más de 13.000 miembros de muy diversos sectores, ya que, según explicó "la Seguridad de la Información y Compliance no es una labor aislada, pues muchos profesionales miden riesgos en su trabajo". ¿Qué tienen en común? ¿Por qué no se trata como algo que afecta a todos los departamentos de la empresa?" se preguntaba; y la respuesta es clara para el norteamericano "nosotros hablamos de resultados orientados al riesgo, trabajando sobre objetivos y auditando los resultados, como el resto de trabajadores. Cualquier labor tiene riesgos, límites y restricciones y ya ha llegado el tiempo en que todo eso se va sabiendo e incluso Standard&Poors está "quitando el velo" de la "caja negra" que era hasta ahora la Gestión de Riesgos", afirmó. Explicó Mitchell que hasta ahora la RSC no se ocupaba de la Seguridad de la Información y, dada su importancia actual para el desarrollo empresarial, ha surgido una nueva forma de entender la empresa, la GRC, que basa la estrategia en el Buen Gobierno, la Gestión del Riesgo y el Cumplimiento Normativo (GRC). Coincidiendo con Noel señaló que se trata de un concepto en el que el análisis de riesgos es la base de la actividad profesional de cualquier entidad y en el que los objetivos se estructuran en función de los límites externos (normativas) e internos (principios); y donde la base de todo es la información, el elemento más sensible y, por tanto, el que se debe controlar con mayor celo.

"Hay que dejar de ser el departamento del "No", pero una organización sin límites puede hacer verdaderas barbaridades", apuntó, "somos los frenos que te permiten correr tranquilo y seguro, un mecanismo que permite ralentizar o frenar en caso necesario", precisó. La clave del nuevo concepto es su valor añadido ante las exigencias crecientes de los accionistas, el aumento de la volatilidad y la complejidad y el coste cada vez mayor de las equivocaciones. Criticando la multiplicación de normativas en EEUU, marcó

"Ha surgido una nueva forma de entender la empresa, la GRC, que basa la estrategia en el Buen Gobierno, la Gestión del Riesgo y el Cumplimiento Normativo (GRC). Se trata de un concepto en el que el análisis de riesgos es la base de la actividad profesional de cualquier entidad y en el que los objetivos se estructuran en función de los límites externos (normativas) e internos (principios); y donde la base de todo es la información, el elemento más sensible y, por tanto, el que se debe controlar con mayor celo"

Scott L. Mitchell, *OCEG.*

Carlos A. Saiz, vicepresidente de ISMS Forum Spain (Ecija).

Scott L. Mitchell (Open Compliance & Ethics Group, OCEG).

como grandes retos de la GRC "tener una única versión de la verdad, saber si realmente cumples todas las normativas e integrar la gestión para que la empresa sea un todo cohesionado" y concluyó que la única forma de hacerlo es "asociando el programa de control de riesgos al de gestión de clientes y a los procesos de negocio, de forma que el cumplimiento se convierta en un propulsor del negocio." Así, según el norteamericano, se mejoran los resultados reduciendo los costes y la GRC es un paso más allá de los SGSI y *Compliance*. El OCEG que preside ha elaborado un *Red book* de reglas y técnicas novedosas -que se puede descargar de su web- donde se describe la GRC como la columna que vertebra toda la actividad empresarial, ya que, para él "existe solapamiento en el 75% de los procesos" al hablar de gestión de clientes, protección de datos, seguridad de la información de empleados y clientes, privacidad, etc. Para Mitchell, la importancia del control de la información es la oportunidad para que los SGSI y *Compliance* den el salto definitivo para aumentar su influencia en las corporaciones.

Pero, una vez convencida la alta Dirección de la importancia de la Seguridad de la información, "hay que pensar cómo integrarnos en la estrategia y en la marca" señaló **Ramiro Mirones**, de Ernst&Young, para comenzar el segundo debate. Según **Floris Van den Dool**, EALA Security Lead de Accenture, "hay que conseguir que se entienda que es holístico e importante aliar las iniciativas entre informático y Gobierno corporativo, por medio de la transparencia de la información" que debe fluir entre el Chief Information Officer (CIO) y el Chief Information Security Officer (CISO).

El debate se quedó corto debido a lo apretado de una agenda que obligó a **Teresa Serrano**, de Citibank España, a sintetizar las claves de la función del *Compliance Officer* en la protección de datos, una labor especialmente delicada en una entidad financiera. Especialmente interesante fue su exposición de los "especiales riesgos" como las listas Robinson, los ficheros de solvencia patrimonial o la gestión y protección de datos de clientes nacionales e internacionales y, en su caso las transferencias de datos internacionalmente en cumplimiento de todas las normativas de los países en liza. Abierta a la posibilidad de que compliance sea una labor de control externa, concluyó que, en cualquier caso, "debe ser independiente, aunque en colaboración con otras áreas" e indudablemente "exige permanente vigilancia dado el riesgo legal y regulatorio, así como los daños a la reputación de la entidad".

En línea similar al resto de los expertos, el analista de Forrester **Thomas Raschke**, apuntó que la promesa del incremento de la productividad y la reducción de costes y riesgos han obligado a los SGSI y compliance a trabajar juntos para entender y mitigar los riesgos, tras un largo camino plagado de equivocaciones en el que cada uno trabajaba por su lado sin cooperar. Para el danés GRC es el engranaje perfecto al incluir la cultura corporativa, políticas de empresa, legislación, normativas, relaciones insti-

tucionales y procesos con la valoración del riesgo, basado en una gestión bidireccional de la información. También dedicó tiempo a la importancia de la gestión basada en el riesgo, añadiendo el enfoque de los nuevos canales y servicios que ofrece la Web 2.0, la movilidad y, en definitiva, las nuevas herramientas que conforman la Sociedad de la Información en la que estamos inmersos. Aunque con cierta prisa, explicó el camino recorrido entre los SGSI y la Gestión centrada en el Riesgo para derivar en el "ecosistema GRC" y en la importancia de los flujos de información en la empresa, que señaló como tendencia evidente en el mundo empresarial de los próximos años. Describió para terminar "un modelo de empresa en el que GRC estará alineando estrategias y objetivos, con métricas bien definidas e informes bien comunicados, en un ambiente de cooperación y mejora constante basado en el análisis de los datos" afirmó.

Tras una mañana intensa, los asistentes pudieron almorzar y compartir sus impresiones en un cóctel. Una breve presentación del vicepresidente de ISMS Forum Spain, **Carlos Alberto Sáiz**, dio paso a las ponencias de la tarde. El coordinador del área de estudios de la Agencia Española de Protección de Datos, **Ricard Martinez**, explicó los objetivos de la nueva estrategia de la Agencia, que "no pretender actuar contra los responsables de la custodia de datos sino a su lado, ayudándoles a cumplir la Ley", en parte como resultado del encuentro internacional sobre Protección de Datos celebrado en Londres en 2006. Para Martínez, "la Agencia no busca sancionar y de hecho en 2007 se han producido menos sanciones y más procesos tutelares; hemos editado en cambio más guías y hemos

Teresa Serrano (Citibank).

modernizado la información on line para facilitar la tarea a la empresas y ciudadanos". Esta nueva estrategia se basa en que "nuestra labor es garantizar los derechos, el derecho fundamental a la protección de datos. Es una labor preventiva en un 20%", aunque no restó importancia a las inspecciones. Indicó, además, que la Agencia está realizando un notable esfuerzo para hacerse más visible en positivo con apariciones en la prensa no sólo por las sanciones impuestas. Y, finalmente hizo un llamamiento a la "precisión en las consultas, cuestiones, dudas y preguntas que se envían a la Audiencia para poder recomendar con mayor conocimiento de cada caso".

"La formación y la educación son lo más importante, y sin embargo es a lo que dedicamos menos dinero. De la misma forma, tenemos que evitar ser conocidos como "la gente de los antivirus", debemos elevar el discurso para dar a la seguridad la importancia que tiene. En una escalada desde la inexistencia de seguridad a la división del departamento en Sistemas, por un lado, y Gestión del Riesgo, por otro, sólo hay tres pasos: blindarse, prevenir y consolidar"

Pierre Noel, ***IBM Corp.***

Rápida fue también la intervención de **Enrique Martínez**, director del Instituto Nacional de Tecnologías de la Comunicación, INTECO: su presentación reivindicó la importancia necesaria de los estándares para crear un mercado sólido. "La industria de la informática se ha desarrollado basándose en estándares. Esta condición le ha permitido alcanzar el grado de adelanto experimentado a la fecha. Diferentes fabricantes de *hardware* y *software* se adhieren a estándares definidos por diferentes organizaciones para lograr la interoperabilidad de diferentes componentes y partes", afirmó rotundo para explicar que "al aplicar los estándares, los proveedores ayudan y aseguran que sus productos y servicios sean consistentes, compatibles y efectivos", dijo, mencionando a continuación algunos de los errores garra-

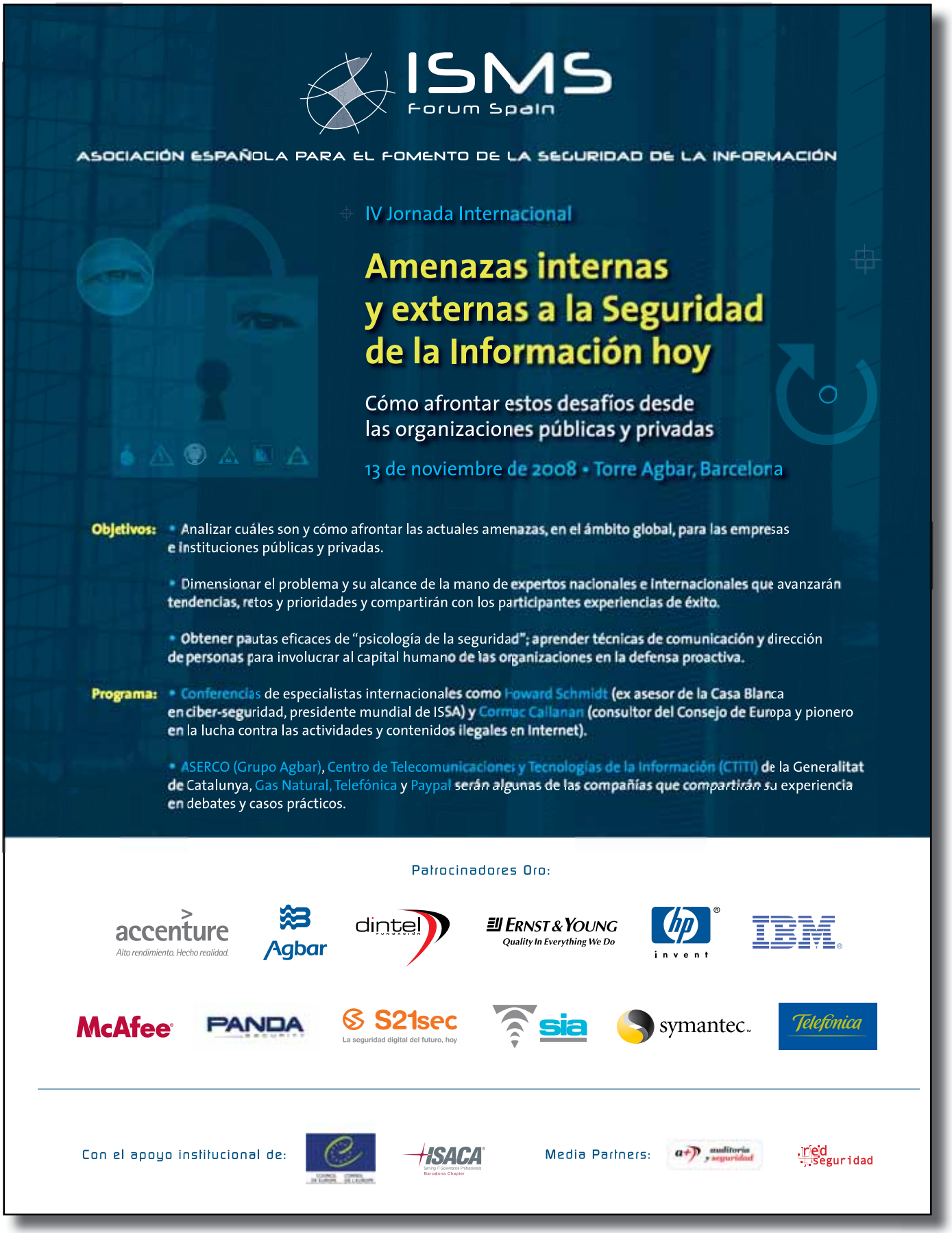
De izda. a dcha: Ramiro Mirones (Ernst&Young), Scott Mitchell (OCEG), Floris Van den Dool (Accenture) y Lucio Molina (ISACA).

fales del pasado como la proliferación momentánea del sistema BETA de video o la más reciente batalla *BlueRay Vs. HD DVD*, así como algunos aciertos que pusieron a Europa en la vanguardia como el estándar GSM de la telefonía móvil. Para Martinez, "si el sector de la Seguridad de la Información quiere realmente prosperar y ganar la importancia que merece tiene que fijarse en la demanda del mercado, muy segmentada y desinformada (siguen hablando de los virus, que son sólo el 8% de las amenazas), y adecuar su oferta a esa demanda con unos estándares que impulsen esta industria", según se deduce de algunos de los últimos informes elaborados por INTECO. Repasó Martínez otras intervenciones recientes del Instituto en procesos como el DNI electrónico o la seguridad de la información en los ayuntamientos para finalmente volver a su idea inicial: "los mercados se crean con regulación y estándares y hay que prever lo que van a necesitar los usuarios".

Fernando Hervada comenzó su intervención sobre la auditoría interna de los Sistemas de Información implementada en Endesa desde 1998, obligados por la Ley Sarbanes-Oxley, que más tarde les ha facilitado el cumplimiento de la normativa italiana tras la compra por Enel y que afirmó "ha dado muy buenos resultados en un proceso que comienza por la planificación y promoción entre la alta Dirección y finaliza con la revisión de resultados (*Plan-Do-Check-Act*). La jornada tocó a su fin con la intervención del comunicador y experto en coaching, **Santiago Álvarez de Mon**, autor de diversos libros sobre liderazgo y comunicación empresarial quien comenzó su alocución, amena y distendida, poniendo en duda que nos encontremos en la Sociedad del Conocimiento, "conozco gente sabia que no sabe escribir y gente discapacitada que recibe 500 mails al día". Enlazó Álvarez de Mon con el liderazgo y las capacidades que debe ostentar un buen directivo, empezando por aprender a jerarquizar y priorizar, así como identificar carencias y dar importancia a la comunicación e interacción entre empleados y directivos; y es que, todos los ponentes destacaron la importancia de las habilidades de comunicación para integrar la gestión de la Seguridad de la Información y Compliance en la alta Dirección, una de las grandes lecciones de esta jornada.

Santiago Álvarez de Mon (IESE).

Actividades 2008,
IV Jornada Internacional



¿Por qué una jornada internacional sobre Amenazas?

La información se ha convertido en uno de los activos que toda empresa debe proteger y salvaguardar frente a un entorno adverso que atenta contra su confidencialidad, integridad y disponibilidad. Gestionar adecuadamente la seguridad de la información debería minimizar las amenazas a las que esta se expone, **optimizar la inversión en seguridad que la empresa afronta e incluso mejorar las oportunidades de negocio**.

Hay amenazas con las que convivimos desde hace muchos años; pero en el mundo actual cada día surgen nuevas amenazas y las existentes, además, **mutan y de readaptan constantemente para poder causar su impacto**. Existen amenazas domésticas, cuyo origen se encuentra en la propia organización, y otras que provienen de causas y factores externos; algunas están claramente **ligadas al factor humano**, otras son atribuibles a la tecnología y muchas otras encuentran su causa en **desastres y fenómenos naturales**. Un empleado desleal, un *hacker* desde un país lejano, los programas maliciosos, los virus, la desactualización de *software*, una inundación, un incendio, un acceso indebido y no controlado de un usuario a nuestra red; todas ellas son amenazas que una organización tiene que conocer para calcular sus niveles de riesgo y saber cómo pueden afectar e impactar en su información y en sus procesos de negocio.

La tendencia nos empuja a pensar en el **tránsito del concepto de seguridad informática a seguridad de la información**, y la realidad nos convence de que **se inicia la era de la Gestión Responsable de la Información**. En España queda mucho trabajo por hacer y desde ISMS Forum quisimos contribuir con esta IV Jornada Internacional a compartir experiencias y fomentar el conocimiento de las últimas amenazas y los retos para contrarrestar los impactos que pueden generar en las organizaciones. Para ello, contamos con expertos internacionales de primer nivel y con un inmejorable abanico de profesionales españoles que analizaron las amenazas a las que se enfrentan organizaciones públicas, cómo combatir el cibercrimen, formas de concienciar al personal de una organización con **políticas adecuadas para evitar ataques internos**, y reflexionar sobre las formas de combatir los desafíos internos y externos que afrontamos. Con la participación de un experto en dirección de personas en las organizaciones quisimos, también, **obtener pautas eficaces de "psicología de la seguridad"**; aprender técnicas de comunicación y dirección de personas para involucrar al capital humano de las organizaciones en la defensa proactiva.

Los ponentes

Como en anteriores ocasiones, ISMS Forum Spain contó en esta jornada con conferenciantes del más alto nivel, que expusieron las tendencias en cuanto a amenazas en un contexto global, hablando tanto de las que provienen del exterior como de las que surgen en el mismo seno de la empresa, tan importantes como las primeras y a menudo algo olvidadas.

Destacamos la presencia de:

- El reconocido experto en ciber terrorismo y ex asesor de la Casa Blanca en este ámbito, **Howard Schmidt.** Además, es presidente mundial de ISSA (Information Security Sistems Association) y anteriormente fue Chief Security Officer de Microsoft Corp, jefe del Computer Exploitation Team de la FBI, y Chief Security Strategist en eBay.

- **Cormac Callanan,** consultor del Consejo de Europa en temas de ciber delincuencia, ha colaborado en la elaboración de la normativa de la UE en este ámbito. Es CEO de Aconite Internet Solutions, una empresa que se especializa en la lucha contra el ciber crimen internacional y la seguridad en Internet. Facilita formación a instituciones como la Interpol, Europol y otras agencias similares por el mundo.

- Uno de los expertos en organisational behaviour más reconocidos en nuestro país, el profesor del IESE **Guido Stein,** que aportó con su conferencia pautas sobre cómo involucrar al capital humano de una organización en la defensa proactiva contra las amenazas a la seguridad de la información.

- Además, los máximos responsables de seguridad de la información de diversas empresas e instituciones públicas compartieron sus experiencias y buenas prácticas en debates y presentaciones de casos prácticos.

Principales conclusiones

Howard Schmidt: "Recortar inversión en seguridad en el actual contexto de crisis sería un grave error que pasaría factura a las organizaciones a medio y largo plazo"

El ex asesor de la Casa Blanca en ciber seguridad fue uno de los participantes en la IV Jornada de ISMS Forum Spain el 13 de noviembre.

El auditorio de la Torre Agbar, en Barcelona, estaba repleto a primera hora del 13 de noviembre de 2008. El programa de la IV Jornada Internacional de ISMS Forum Spain atrajo a más de 270 expertos y profesionales de la seguridad de la información procedentes de toda la geografía española, y no era para menos, pues el abanico de ponentes conformaba un cúmulo de experiencia y de know-how internacional como para no perdérselo. Surgieron muchas ideas a lo largo de la jornada, pero destacaremos una que aparecía una y otra vez: parece que hay acuerdo en que la clave para combatir las amenazas no reside en la tecnología, sino en las personas.

Cada día surgen nuevas amenazas a la seguridad de la información y las existentes, además, mutan y se readaptan constantemente para poder causar su impacto. Algunas están claramente ligadas al factor humano, otras son atribuibles a la tecnología y muchas otras encuentran su causa en desastres y fenómenos naturales. Esta jornada, titulada "Amenazas internas y externas a la Seguridad de la Información hoy", analizó los desafíos a los que actualmente se enfrentan los responsables de proteger la información de las organizaciones. Entre los ponentes destacó el reconocido experto en ciber terrorismo y ex asesor de la Casa Blanca en este ámbito, **Howard Schmidt**, quien ha sido Chief Security Officer de Microsoft, jefe del Computer Exploitation Team del FBI, y Chief Security Strategist en eBay. Además en la actualidad es el presidente mundial de ISSA (Information Security Systems Association).

Schmidt dejó bien claro desde el inicio de su exposición que en el mundo global de las telecomunicaciones -en el que realmente no hay una autoridad mundial a cargo, sino que todos somos responsables al tiempo que nadie lo es de manera determinante- las amenazas actuales constituyen un problema de seguridad nacional. Un problema crítico que puede afectar directamente, además, al corazón económico de nuestras sociedades. Esto se agrava por el hecho de que la propiedad y la gestión de la mayoría de las infraestructuras críticas, en casi todos los países, está en manos privadas, como también lo está la garantía y supervisión de su seguridad física y lógica.

Chris Kenworthy (McAfee).

Howard Schmidt.

La concienciación internacional, gracias a diversas iniciativas y organismos –citó como ejemplo al ENISA-, va mejorando. Así, por ejemplo –y a raíz de los sucesos del 11 de septiembre de 2001 en Nueva York- se ha creado la alianza público-privada internacional IMPACT (International Multilateral Partnership Against Cyber-Threats), plataforma con sede principal en Malasia, que aúna a gobiernos, empresas e investigadores para combatir el ciberterrorismo a escala global, intercambiar información, estandarizar el cumplimiento de buenas prácticas, etcétera.

Para dar una idea del crecimiento exponencial del número de equipos a vigilar y proteger, Howard Schmidt recordó en en 2008 se alcanzó la cifra de mil millones de dispositivos de todo tipo conectados a la red (cifra a la que se llegó tras 25 años de evolución de las TIC), pero se estima que en sólo cinco años más esta cantidad se habrá duplicado. Cada vez serán más en proporción los dispositivos móviles, y hacia ellos se dirigirán la mayoría de los ataques en los próximos años, quitando el protagonismo en este triste asunto a su titular actual, el PC.

El gobierno de la seguridad, recordó, no es sólo un problema de tecnología, sino que implica y mucho a las personas (por ejemplo: la lucha contra el phishing ha traído consigo notables mejoras tecnológicas y eficaces filtros, pero el factor hu-

Cormac Callanan (European Council).

H. Schmidt dejó claro que las actuales amenazas a la seguridad de la información constituyen un problema de seguridad nacional. Un problema crítico que puede afectar directamente, además, al corazón económico de nuestras sociedades.

Sólo hasta septiembre, en 2008 Telefónica manejó un tráfico de 5.000 millones de e-mails . Pero más del 95% de ese tráfico de correo electrónico lo compone el malware (spam, virus, spyware...) Juan Miguel Velasco resaltó que en 2008 el phishing en España se duplicó con respecto al año anterior y que en Reino Unido se ha multiplicado por diez.

mano sigue ahí, y las personas siguen "picando"). El presidente de ISSA apuntó que la concienciación, y el establecimiento de procesos guiados por las mejores prácticas podrían ser factores clave a la hora de mejorar la seguridad, mientras que a menudo las organizaciones se centran en lanzar mensajes negativos de amenaza, vulnerabilidad, etcétera.

A continuación se celebró un debate moderado por **Marcos Gómez Hidalgo**, director de e-Confianza de INTECO, que fue pasando la palabra a **Juan Miguel Velasco** (director asociado de Servicios y Soluciones de Seguridad de Telefónica), **Juan Salom** (comandante jefe del Grupo de Delitos

Marcos Gómez (INTECO) moderó la mesa redonda en la que participaron Howard Schmidt, Juan Salom (GDT) y Juan Miguel Velasco (Telefónica).

Temáticos de la Guardia Civil) y al propio Howard Schmidt que se unió al debate.

Velasco resaltó algunos datos que desde su observatorio privilegiado del tráfico puede aportar Telefónica. Así, frente a la cantidad total de 700 millones de correos que contabilizaron en el año 2004, en 2008 se llegó a la cifra de 5.000 millones (y eso sólo hasta el mes de septiembre). Pero más del 95% de ese tráfico de correo electrónico lo compone el *malware* (*spam, virus, spyware*...). También resaltó que en 2008 el *phishing* en España se duplicó con respecto al año anterior, y en Reino Unido se ha multiplicado nada menos que por 10. También la suplantación de identidad crece de manera preocupante, y además –recordó- sigue existiendo un "gap" importante, un plazo de tiempo excesivo, entre el delito y la investigación del mismo, y muchas lagunas legales en lo que se refiere a las evidencias electrónicas, lo que da una clara ventaja a los ciberdelincuentes.

Por su parte el experto de la Guardia Civil Juan Salom aseguró que España estaría preparada para un eventual ataque a infraestructuras críticas o estratégicas, y que un comité de expertos del Ministerio del Interior trabaja para combatir estas posibles amenazas, que aún no ha sufrido España como sí ha ocurrido en otros países (Georgia, Estonia o los Estados Unidos). Habló de los "paraísos informáticos que todos conocemos", refiriéndose claramente a países en los que el cibercrimen campa más o menos a sus anchas, amparado en una sensación incluso de impunidad: sin poner nombres concretos, sí que dejó caer que Europa del Este y algunos países sudamericanos estarían en cabeza. Así actualmente uno puede comprar, mencionó como ejemplo, los datos de una tarjeta de crédito en vigor por entre uno y cinco dólares. El panorama no es demasiado alentador.

Cormac Callanan, consultor del Consejo de Europa, reconoció que eran necesarios esfuerzos adicionales para coordinar, mejorar procedimientos, estandarizar y, en definitiva, simplificar y lograr un eficiente gobierno internacional de la Seguridad de la Información.

La segunda parte de la mañana contó con otras dos intervenciones de alto nivel. **Chris Kenworthy**, alto directivo internacional de McAfee, y **Cormac Callanan**, consultor del

Marcos Gómez Hidalgo, director de E-Confianza de INTECO.

Juan Salom, de la Guardia CiVil, habló de los "paraísos informáticos que todos conocemos", refiriéndose a países en los que el cibercrimen campa más o menos a sus anchas, amparado en una sensación incluso de impunidad. Europa del Este y algunos países sudamericanos estarían en cabeza. Así actualmente se pueden comprar los datos de una tarjeta de crédito en vigor por entre uno y cinco dólares. El panorama no es demasiado alentador.

Consejo de Europa y de otros organismos internacionales como la INTERPOL en materia de seguridad de las TIC y de Internet.

Kenworthy insistió en uno de los mensajes básicos de esta jornada: "la seguridad no es una cuestión de tecnología sino, sobre todo, de personas", y en que el principal objetivo de los cibercriminales es hoy la obtención masiva de datos sensibles (como datos de acceso online a cuentas bancarias) para su venta y uso posterior por parte del comprador. Se trata de un lucrativo negocio y ya no tiene nada que ver con el hacker de los viejos tiempos que saltaba barreras para ponerse a prueba a sí mismo, o para ganar en imagen frente a la comunidad de expertos en Internet. Hoy se trata de ganar dinero y permanecer anónimo, tan simple como eso.

Por su parte, Callanan desgranó las distintas líneas de trabajo que está desarrollando el Consejo de Europa para luchar contra las diversas amenazas a la seguridad de la información. El panorama no es excesivamente optimista pues él mismo reconocía que eran necesarios esfuerzos adicionales para coordinar, mejorar procedimientos, estandarizar y, en definitiva, simplificar y lograr un eficiente gobierno internacional de la seguridad. Animó a todos los presentes a visitar la web del Consejo de Europa sobre cibercrimen para recabar más información al respecto de la normativa europea y de las iniciativas que está llevando a cabo este organismo internacional.

La mañana terminó con una excelente exposición de un caso práctico a cargo del director general en España de Paypal, **Fernando Aparicio**, que reconoció que su compañía es objetivo constante de tácticas de fraude tipo phishing y explicó las estrategias que están utilizando para combatirlo y para asegurar la autenticación de los usuarios y la integridad de los sensibles datos que maneja Paypal.

La sesión de la tarde comenzó con la exposición de un exhaustivo análisis de la situación actual de la seguridad en las Pymes en España. Su autor no podía ser otro que **Pablo Pérez**, gerente del Observatorio de Seguridad de la Información de INTECO, pues este organismo posee sin duda estudios e información de sobra para poder elaborar esta radiografía. Todavía queda mucho camino para que pueda considerarse en términos generales que estas organizaciones -que conforman la gran mayoría del tejido empresarial español- cumplen con la LOPD, se preocupan activamente por la seguridad de la información o han implementado un SGSI en condiciones. Su presentación se acompañó de gráficos muy ilustrativos al respecto.

Guido Stein puso el toque más humanista de la jornada a continuación. El profesor del IESE, experto en gestión de personas en las organizaciones, disertó acerca de conceptos como la confianza, el liderazgo o la comunicación, tan importantes y a menudo tan olvidados en los departamentos de Seguridad de la Información de las organizaciones. Utilizando el salto de un pequeño caracol como metáfora visual, aportó muchas ideas y sobre todo hizo reflexionar al público acerca de estos conceptos, cuya aplicación excede el ámbito profesional y abarca también, sin duda, el personal.

El profesor de IESE Guido Stein

La jornada terminó con una mesa redonda en la que participaron responsables de seguridad de la información de Gas Natural, de ASERCO (Grupo Agbar), del Banco Sabadell y del Centro de Telecomunicaciones y Tecnologías de la Información (CTiTI) de la Generalitat de Catalunya. El debate giró en torno a las políticas internas como herramienta de generación de actitudes proactivas y contramedidas a las amenazas. De nuevo, las personas y su importancia a la hora de combatir las amenazas, o el factor humano y psicológico de la seguridad.

Resposables de Seguridad de la Información de Gas Natural (Andreu Bravo), ASERCO-Grupo Agbar (Cristina Segura), Banco Sabadell (Xavier Serrano) y del Centro de Telecomunicaciones y Tecnologías de la Información (CTiTI) de la Generalitat (Tomás Roy) participaron en la mesa redonda de la tarde.

Actividades 2008, otras sesiones formativas

Organizado conjuntamente por:

infosecurity IBERIA

ISMS Forum Spain

Conferencia de Eugene Kaspersky: "El cibercrimen contra la industria de prevención de amenazas"

El 11 de junio, en un programa organizado por ISMS Forum Spain en el seno de la feria especializada del sector, Infosecurity, **Eugene Kaspersky**, CEO y co-fundador de Kaspersky Lab, impartió la conferencia ***iCrime vs Threat Prevention industry***. En ella expuso las principales tendencias y focos de interés en la seguridad de la información y las razones por las que se generan los problemas relativos a la seguridad. Además habló del desarrollo de la industria y hacia donde evolucionará. Por último, prestó especial atención a las amenazas más preocupantes -la más peligrosa de las cuales es el ciberterrorismo- y aportó algunos recientes e impactantes ejemplos.

La actividad, celebrada en el Palacio Municipal de Congresos y Exposiciones, continuó con una demostración práctica a cargo del director de la Unidad de e-Crime de S21sec, **David Barroso**, quien dirigió la sesión "**Una experiencia práctica sobre *malware***". Barroso es uno de los expertos en informática forense más reconocidos en nuestro país.

David Barroso (S21sec) finalizó la jornada con una sesión práctica sobre malware.

Principales conclusiones de la sesión

"Con la sofisticación de los sistemas y tecnologías y la proliferación de terminales móviles, el problema del cibercrimen está lejos de tener solución"

La multiplicación progresiva del número de ataques a las empresas, unida a la falta de formación y precaución de los empleados de las compañías, hacen que el problema de la lucha contra el cibercrimen esté lejos de ser resuelto y requiera de inversiones cada vez más millonarias. De hecho, al crearse cada día nuevos servicios en la Red, cada vez hay más dinero, más información y más datos personales circulando por Internet, lo que lógicamente actúa como reclamo para el crimen organizado. Así lo aseguró Eugene Kaspersky en la sesión organizada por ISMS Forum Spain y Reed Exhibitions en el seno de la feria Infosecurity 2008, a la que asistieron más de 200 profesionales

En su conferencia, titulada "El cibercrimen contra la industria de prevención de amenazas", el CEO y co-fundador de Kaspersky Lab, uno de los máximos expertos mundiales en antivirus, expuso las principales tendencias y focos de interés en la seguridad de la información y las razones por las que se generan los problemas relativos a la seguridad, y habló a continuación del desarrollo y previsible evolución del sector.

Kaspersky recordó que según los datos de sus analistas, en 2007 aparecieron en Internet más de 2.227.000 nuevos programas nocivos (virus, gusanos y troyanos), cifra que supone cuatro veces más que en 2006; y previsiblemente los resultados de 2008 superarán todas las expectativas, pues los expertos de Kaspersky Lab pronostican que podría multiplicarse por diez, con respecto al año anterior, el número de nuevos programas nocivos, cuya cantidad superaría los 20 millones. "El problema es que no solo crece la cantidad, sino también la calidad, complejidad y sofisticación de estos programas", señaló. La ya denominada como generación "*malware 3.0*" está haciendo ganar millonadas a los cibercriminales.

Es un hecho que, con la excepción de algunas zonas de África, en general nuestras sociedades viven ya permanentemente conectadas a Internet, y cada vez más a través de dispositivos móviles. Por supuesto también las empresas, que siguen mostrando grandes vulnerabilidades. Y el asunto es mucho más complejo que un simple "usuario víctima versus ciber delincuente": "Los criminales compran, venden, negocian, se asocian y ofrecen sus servicios personalizados en la Red", aseguró Kaspersky, quien ilustró su explicación con variados ejemplos de sitios de ciber delincuentes en los que se podían leer desde notas de prensa enfatizando la eficacia de sus servicios hasta listados de tarifas por ejecutar distintas actividades como crear una botnet o realizar espionaje industrial... "Estos servicios en general son caros, pero como pueden observar, se ofrecen descuentos a partir del segundo encargo profesional: el sector también fideliza a sus clientes", ironizó Kaspersky. "Ya no hablamos de B2B en la Red –continuó-, sino de un próspero mercado de C2C (*Criminals to Criminals*), y lo que es aún peor, de C2T (*Criminals to Terrorists*), pues en la Red numerosos grupos criminales y terroristas internacionales comercian, cooperan y establecen redes entre ellos". De nuevo Kaspersky apoyó sus afirmaciones con el repaso de casos recientes, algunos bastante espeluznantes, que iban frunciendo el semblante de los asistentes en un gesto que denotaba preocupación. Después de preguntarles qué creían que nos deparaba el futuro, Kaspersky les recomendó el visionado de la película "*Die Hard*", cuarta entrega, en la que la factoría de Hollywood desarrolla muchísimas ideas "para inspirar a los malos".

A continuación, David Barroso, director de la Unidad de e-Crime de S21sec, dirigió la sesión "Una experiencia práctica sobre *malware*". Barroso presentó en esta sesión todos los pasos para conseguir una *botnet* con miles de ordenadores infectados: la infección, el comportamiento y análisis del código malicioso, el control de los ordenadores infectados, el funcionamiento de los paneles de control e incluso datos sobre quién está detrás. Se trataba de comprobar en vivo qué fácil es infectar un ordenador que no cumple con requisitos básicos de seguridad, así como la infraestructura que hay detrás, cada vez más compleja, para garantizar el éxito de toda la operación

Actividades 2008, otras iniciativas

Data Leak Prevention Workshop

El 6 de marzo ISMS Forum organizó, en colaboración con Forrester Research, el seminario "Data Leak Prevention and Data-Centric Security" en un céntrico hotel de Madrid. El ponente de este taller, que se desarrolló íntegramente en inglés, fue el analista de Forrester **Bill Nagel**, experto en seguridad de la información, que se desplazó desde Amsterdam para compartir con los socios de ISMS Forum una práctica sesión, en la que diálogo y debate fueron protagonistas, que se prolongó durante tres horas.

La pérdida de información sensible a causa del extravío, robo o ataques a los dispositivos móviles, cada vez más presentes e importantes en la gestión empresarial de nuestros días, y foco de atención para los delincuentes en la Red, fue uno de los temas que centró el debate. Pero también el enorme volumen de información sensible que se pone en peligro constante por parte de los empleados de las organizaciones sin que éstos sean siquiera conscientes, es decir, de una manera involuntaria, fruto del desconocimiento y de la falta de sensibilización, formación, y unas políticas internas adecuadas.

Consultoría para la planificación estratégica 2009-2011

Tras año y medio de actividad, la Asociación entra en fase de consolidación. Se debe priorizar en esta fase la creación de una estructura de gestión más sólida, la redefinición de procesos y procedimientos y la formulación de ejes estratégicos, todo ello con un único objetivo: crear más valor añadido para los asociados. Por todo ello ISMS Forum Spain contrató en junio los servicios de una Consultora Estratégica especializada en el Tercer Sector, que nos ayudó, tras varios meses de trabajo, a redefinir la visión, misión y valores de la asociación, establecer los objetivos y retos pata 2009-2011 y elaborar un plan estratégico y una planificación anual para 2009.

Registro de Profesionales Certificados

Más de cien asociados se han dado de alta ya en el **Registro *online* de Profesionales Certificados**, un servicio público y gratuito de ISMS Forum Spain a los profesionales que trabajan en seguridad de la información y a las empresas, organizaciones e instituciones que puedan necesitar de sus servicios.

Los **objetivos** de este Registro son:

- Promover e incentivar la certificación de primer nivel y la adopción de estándares para las mejores prácticas de gestión de la seguridad de la información entre las empresas y profesionales españoles.
- Dar visibilidad al esfuerzo en formación continua y actualización constante de conocimientos realizados por los profesionales que ejercen su trabajo en este sector.
- Mantener una base de datos actualizada y verificada del talento profesional disponible y en ejercicio en nuestro país en materia de seguridad de la información.

Las certificaciones contrastan, evalúan y validan conocimientos teóricos y prácticos en campos específicos de la seguridad de la información, de forma que para cada perfil profesional requerido será más oportuno buscar una u otra certificación. Muy orientados a la práctica, estos títulos son complementos indispensables, hoy en día, en la formación de especialistas en la materia. Para obtener las certificaciones más exigentes, además de superar exámenes teóricos y prácticos es necesario poseer experiencia profesional previa, dependiendo de cada caso. Y para mantenerlos, los profesionales deben "revalidar" periódicamente la Certificación, mediante exámenes y/o documentando el ejercicio profesional. Contar con especialistas certificados asegura el dominio y aceptación de determinados estándares de mejores prácticas, ética y actuación profesional

Mediante una sencilla búsqueda, el Registro permite comprobar qué certificaciones posee un profesional dado de alta, u obtener el listado de profesionales dados de alta que posean determinada certificación, así como sus datos de contacto.

Actividades 2008,
Convenios de colaboración

Gianluca D'Antonio y Martín Pérez Sánchez.

Gianluca D'Antonio y Fernando Bahamonde.

Con FUNCOAS

Martín Pérez Sánchez, presidente del patronato de FUNCOAS (Fundación para la Transferencia del Conocimiento de ASIMELEC) y el presidente de ISMS Forum Spain, **Gianluca D'Antonio**, firmaron a comienzos del año un acuerdo marco de colaboración, en virtud del cual ambas organizaciones cooperan en la difusión y promoción de la seguridad de la información en España, así como en otras iniciativas que contribuyan a mejorar la formación de los profesionales del sector. Ambas instituciones tienen metas comunes y aunarán esfuerzos para lograr estos objetivos, con especial interés en la concienciación de las Pymes españolas acerca de la importancia estratégica de la seguridad de la información. El acuerdo, de vigencia anual prorrogable, prevé la cooperación en la organización de actividades de carácter divulgativo, editorial y/o formativo, y se concretó ya en enero, cuando ASIMELEC cedió seis becas para cursar el **Master en Dirección y Gestión de la Seguridad de la Información** organizado por ASIMELEC/FUNCOAS, que se sortearon entre los asociados de ISMS Forum Spain. El sorteo se celebró en la sede de ASIMELEC, y los socios agraciados con estas seis becas (la única condición para participar en el sorteo era trabajar en una Pyme) fueron José **Miguel Rosell, Pablo Blanco, Antonio Cerezo, Daniel Rodríguez, Esther Arenales** y **Ricardo Cañizares.**

El Master en Dirección y Gestión de la Seguridad de la Información está respaldado académicamente por la Universidad Pontificia de Salamanca. La beca para los seis socios de ISMS Forum ha sido completa, es decir, ha cubierto los 9.000 euros que cuesta el master en su versión completa (módulo de Gestión + módulo de Dirección). El programa consta de 460 horas lectivas.

Con ISSA España

La Asociación Española para la Seguridad de los Sistemas de Información, ISSA España, es desde 2004 Capítulo Oficial de ISSA, la mayor Asociación mundial de profesionales de seguridad de Sistemas de la Informacion, formada por más de 12.000 profesionales de la seguridad de la información en todo el mundo. ISSA tiene como principal objetivo promover la educación contínua de sus miembros y el desarrollo de sus cualidades referentes a la seguridad en los sistemas de información así como difundir entre las empresas, organismos, particulares y la sociedad en general el uso y necesidad de las buenas prácticas en seguridad informática.

En mayo, los presidentes de ambas asociaciones (**Gianluca D'Antonio** y **Fernando Bahamonde**), conscientes de que las organizaciones que representan comparten objetivos y trabajan en pro de metas muy similares, firmaron un convenio de colaboración en virtud del cual ambas asociaciones cooperarán en distintas líneas de trabajo. El acuerdo tiene una vigencia anual prorrogable.

Los expertos de ISSA España han colaborado desde entonces aportando su experiencia, ideas y contenidos para las jornadas de ISMS Forum Spain, y ayudando a la vocalía de Grupos de Trabajo a coordinar la cooperación online de los mismos a partir de la reunión presencial que se organizó con todos los inscritos en los GTs el 12 de mayo en el Instituto Internacional (c/Miguel Ángel, Madrid). Además, el presidente mundial de ISSA, **Howard Schmidt**, fue el ponente encargado de inaugurar la IV Jornada Internacional que se celebró en Barcelona en noviembre.

Actividades 2008, colaboración con otras organizaciones

Seguridad 2008. VII Conferencia Internacional sobre Seguridad TIC de IDC

Cuándo: 26 de febrero (Madrid) y 28 de febrero (Barcelona).

Dónde: Hotel Palace, en Madrid, y Hotel Juan Carlos I, en Barcelona.

Organizado por: IDC.

ISMS Forum Spain colaboró con este encuentro anual, una cita de referencia para el sector, donde se analizaron los retos que los sistemas de IT y su seguridad generarán en los próximos años a los CIOS y Managers de IT en toda Europa. La convergencia de las tecnologías, la multiplicación de los puntos de acceso o el factor humano de los empleados fueron algunos de los puntos de análisis en el programa de esta conferencia. Los asociados de ISMS Forum Spain disfrutaron de un 25% de descuento en el precio de inscripción.

Forrester's Security Forum EMEA 2008

Cuándo: 2 y 3 de abril.

Dónde: Hotel Mövenpick, Amsterdam, Holanda.

Organizado por: Forrester.

El foro europeo anual de seguridad de Forrester tuvo lugar este año en Amsterdam con un panel de participantes de lujo. Además de sesiones y talleres a cargo de analistas de la firma, el evento contó con ponencias de directivos de Unilever, Reuters, Rolls-Royce, Alliance & Leicester, ING o Barclays. Esta cita se dirigía a profesionales con cargos de responsabilidad en las áreas de seguridad y gestión de riesgos que desearan conocer el estado del arte, los retos a los que se enfrenta el sector y las prácticas, principios, estrategias y herramientas que les ayudarán a guiar a sus organizaciones hacia la excelencia en seguridad de la información, gestión de riesgos y buen gobierno. Los socios de **ISMS Forum Spain** se beneficiaban de un 20% de descuento en la inscripción.

Gestión de la Seguridad Corporativa

Cuándo: 20 de Mayo.

Dónde: Hotel Holiday Inn, Madrid.

Organizado por: Intereconomía Conferencias.

La jornada contó con reconocidos profesionales del sector que analizaron, entre otros temas, la importancia de analizar los riesgos y gestionarlos de una forma adecuada a la hora de definir la estrategia de seguridad; la gestión conjunta de la seguridad física y lógica; la inteligencia competitiva aplicada en materia de seguridad y las tendencias actuales de delincuencia, forma de gestionar estos incidentes y análisis de las pérdidas sufridas. **ISMS Forum Spain** fue entidad colaboradora en esta jornada. Por ello, todos nuestros socios se beneficiaron de un 10% de descuento en la inscripción.

II Foro de Seguridad Avanzada

Cuándo: 5 de junio.

Dónde: Hotel Carlton (Bilbao).

Organizado por: Ernst&Young y Computerworld.

En el transcurso de este foro tuvo lugar una presentación de **ISMS Forum Spain** para dar a conocer a las empresas y profesionales del entorno geográfico del norte peninsular sus proyectos, iniciativas y filosofía de trabajo en favor del desarrollo y fomento de la seguridad de la información en España. La Asociación quiso acercarse así a todos los profesionales que tienen inquietudes por intercambiar experiencias con otros expertos, mejorar su formación y acceder a conferencias y debates con ponentes de primer nivel en el ámbito internacional.

El fomento y difusión de una sólida cultura de la seguridad de la información en España es el fin fundacional fundamental 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 colaboró con numerosos congresos, jornadas y reuniones organizados en torno a la seguridad de la información

I Congreso Nacional PCI - DSS

Cuándo: 17 de junio.

Dónde: Hotel NH Eurobuilding, Madrid.

Organizado por: AKJ Associates.

PCI – DSS (Payment Card Industry – Data Security Standard) es una iniciativa mundial que regula el proceso de pago por tarjeta en cualquier ámbito con el fin de preservar la integridad de la información y los datos personales de los usuarios, evitando el robo de éstos o el fraude financiero. Este congreso se celebró en 2008 en diferentes localizaciones europeas. Su objetivo era dar a conocer los requerimientos del estándar, la información crítica para su implementación y las herramientas y servicios disponibles en la industria para su ejecución y las buenas prácticas de mano de grandes compañías que ya lo han implementado. **ISMS Forum Spain** fue una de las entidades colaboradoras y por ello nuestros socios se beneficiaron de un 30% de descuento en la inscripción.

ENISE II

Cuándo: del 22 al 24 de octubre

Dónde: Parador Nacional San Marcos, León.

Organizado por: Instituto Nacional de Tecnologías de la Comunicación (INTECO).

INTECO convocó por segundo año a la industria de la Seguridad en un foro que reunió a sus principales protagonistas; tanto los que la impulsan desde el lado de la oferta como a los que le dan soporte desde el lado de la demanda. Con cerca de 200 ponentes, cada día se estructuró en torno a un ámbito sectorial (sector financiero el primer día, Defensa y Administración Pública el segundo, y la última jornada, el 24 de octubre, se dedicó a utilities, transporte e industria), y comenzó con una sesión plenaria de carácter estratégico que dio paso a la celebración de diversos talleres con un enfoque más técnico y muy práctico. **ISMS Forum Spain** participó en varias sesiones y colaboró en la difusión de esta iniciativa entre sus socios, que disfrutaron de unas condiciones de inscripción ventajosas.

Foros FAST de Fundación Dintel

Cuándo: 9 de abril y 1 de octubre

Dónde: Club Financiero Génova, Madrid.

Organizado por: Fundación DINTEL

En abril tuvo lugar la primera edición 2008 del Foro FAST (Foro de la «Auditoría y Seguridad de la Información y las TIC) organizado por Dintel. Su primera sesión técnica del día se dedicó a indicadores y métricas de seguridad, y la segunda a la gestión de la continuidad de negocio. La segunda edición se celebró en octubre, con las políticas de seguridad como eje temático.

ISMS Forum Spain ha colaborado con esta iniciativa, cuyo objetivo es sensibilizar a las organizaciones acerca de la criticidad de la información almacenada en sus sistemas, aportando expertos para sus distintos debates y colaborando en el diseño de su programación.

Día Internacional de la Seguridad de la Información DISI 2008

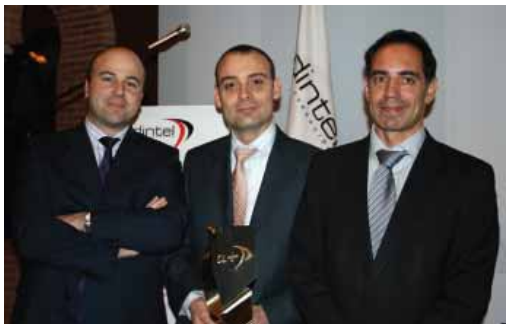
Cuándo: 1 de diciembre

Dónde: Universidad Politécnica de Madrid.

Organizado por: Cátedra CAPDESI Applus+ de la Universidad Politécnica de Madrid.

ISMS Forum Spain fue una de las organizaciones colaboradoras en la III jornada con motivo del Día Internacional de la Seguridad de la Información (DISI) que Jorge Ramio, responsable de la Cátedra anfitriona, viene organizando con gran éxito. La sesión tuvo como invitada de honor a Radia Perlman, CTO de Sun Microsystems en la actualidad e incansable investigadora en seguridad y redes desde hace décadas. Perlman, que ya ha pasado a la historia de las telecomunicaciones por su autoría del STP (Spanning Tree Protocol) habló de sus actuales trabajos y de algunas claves para enfocar adecuadamente el trabajo de I+D en su campo.

Reconocimientos



Luis Buezo, Gianluca D'Antonio y Andreu Bravo.

Publicaciones

Premio de la revista a+)) auditoría y seguridad al "Mejor foro TIC de los Profesionales y Empresas"

La Asociación recibió en enero el Premio 2008 al **"Mejor Foro TIC de los profesionales y empresas"** otorgado por la Revista a+)) auditoría y seguridad, que edita la **Fundación DINTEL**.

Estos galardones reconocen cada año, en sus distintas categorías, la labor de los profesionales, organizaciones y empresas que más han destacado en su contribución al sector de la seguridad de la información y las tecnologías de la información y la comunicación. La entrega de los premios 2008 de a+)) auditoría y seguridad tuvo lugar en el transcurso de un acto organizado por la Fundación DINTEL en el Palacio de la Misión (Casa de Campo, Madrid). Presidido por el vicepresidente económico y consejero de Economía y Empleo de Castilla y León, **Tomás Villanueva**; su clausura corrió a cargo de **María José López**, consejera de Justicia y Administración Pública de la Junta de Andalucía, que habló en nombre de todos los premiados en esta edición.

El presidente de ISMS Forum Spain recibió el premio en nombre de la Asociación de manos del director de la Agencia de Protección de Datos de la Comunidad de Madrid, **Antonio Troncoso**.

Guía de Medidas y Métricas para una Capacidad Integrada de GRC de OCEG

En la línea ya iniciada con otras publicaciones, y con el objetivo de acercar a los profesionales de la seguridad de la información herramientas de trabajo útiles y accesibles, sin ninguna barrera idiomática que dificulte su comprensión, en 2008 ISMS Forum Spain ha traducido y editado en castellano un nuevo manual. Se trata de la **"Guía de Medidas y Métricas 2007"** de OCEG (Open Compliance & Ethics Group, EEUU), subtitulada **"Una propuesta para la evaluación de resultados y métricas para disponer de una capacidad integrada de GCR (Governance, Risk, Compliance and Ethics)"**.

Ahora más que nunca, la comunidad empresarial siente la necesidad de integrar buen gobierno, gestión del riesgo, controles, cumplimiento normativo y ética en el día a día del negocio — y utilizar esas prácticas para impulsar "resultados con principios". La Guía de Medidas y Métricas de OCEG ayuda a medir estos procesos e informar acerca del rendimiento y de las capacidades de GRC en las organizaciones.

Además, los socios de ISMS Forum Spain tienen acceso a muchísimos más contenidos *online* de OCEG, normalmente restringidos a socios de este *think tank* norteamericano, en virtud de un acuerdo alcanzado entre ambas instituciones.

Empresas asociadas

En diciembre de 2008, cerca de cien empresas y organizaciones de los más diversos sectores se han asociado, y más de 500 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.

- Abertis Infraestructuras
- Accenture
- Acens Technologies
- Adesis Netlife (Alaro Avant)
- Agaex Informática
- Agbar Servicios Compartidos, ASERCO
- Aidcon Consulting
- Applus+, Lgai Technological Center
- Ascêndia Reingeniería + Consultoría
- Asistencia Sanitaria Interprovincial, ASISA
- Audisec Seguridad de la Información
- Bankinter
- Breyer Sistemas De Información
- British Standards Institution España
- Bt España
- Caixa D'estalvis Del Penedès CEP
- Cajamar Caja Rural
- CC.AA. Región De Murcia
- Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya – CTTI
- Cisco
- Compañía Española De Petróleos, CEPSA
- Comparex España
- Consejo General de Colegios Oficiales de Médicos – CGCOM
- CPI Consultoría T.I.
- CPR Tecnologías de la Información
- Cuatrecasas Abogados
- Deloitte
- Destrucción Confidencial de Documentación DCD
- Dintel
- Ecija
- Endesa
- Ernst & Young
- Esa Security
- Eulen Seguridad
- Everis Spain
- Evidian
- Firma, Proyectos y Formación
- Fomento de Construcciones y Contratas FCC
- Future Space
- Gas Natural Informática
- Giga Trust
- GFI Informática
- GMV Soluciones Globales Internet
- Grup Andbanc Mora
- Grupo Ferrovial
- Grupo Generali
- Grupo Intermark 96
- Grupo Millar 2
- Grupo S21sec Gestión S21sec
- Hewlett-Packard Española, HP
- Indra Sistemas
- Instituto Nacional de Tecnologías de la Comunicación, INTECO
- International Business Machines, IBM
- Internet Security Auditors, ISECAUDITORS
- Interxion España
- Kabel Sistemas De Información
- Krell Security
- Leaseplan Servicios
- Live Data Security
- Lloyd's Register Quality Assurance, LRQA
- McAfee
- Microsoft Ibérica
- Mnemo
- Morse Spain
- Network Centric Software, NCS
- Nextel
- Ocaso
- Open Source Security Information Management
- Open3s Open Source And Security Services
- Panda Software Spain
- Pricewaterhousecoopers, PWC
- Promotora de Informaciones, Grupo PRISA
- Proyectopyme Consultores
- Quest Software España
- Red Seguridad
- Reed Exhibitions Iberia
- Repsol
- Revista a+)) auditoria y seguridad
- S2 Grupo
- Sanitas de Seguros
- Seguridad Informática D´Guardian
- SGS ICS Iberica
- Sistemas Informáticos Abiertos, Grupo SIA
- Smart Access
- Sophos Iberia
- Steria Ibérica
- Symantec
- Tecnocom Telecomunicaciones y Energía
- Telefónica
- T-Systems ITC Iberia
- Unitronics Comunicaciones
- Universidad Complutense de Madrid, UCM
- Viajes Marsans
- Zeppelin Televisión

Nueva sede en Madrid

Juan Bravo, 3-Portal A
28006 Madrid
Teléfono: +34 914 367 413
Fax: +34 911 412 626

ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN