# Memoria de Actividades
## ISMS Forum Spain

# 09

**Redacción:** ISMS Forum Spain

**Fotografía:** Roberto Pardo
Daniel Sastre

**Diseño:** Jon Arriaga

EQUIPO DE GESTIÓN:

**Directora:** Cristina Saura

**Coordinación general:** Joris Vredeling
Germaine Custers

**Management Assistant:** Esperanza Ruiz del Olmo
María Angelina Carabajal

**Colaboradores:** Antonio Sánchez (Web y BB.DD)
Oscar González (Asesor Fiscal)
Olga Torres (Administración)
Laura Díaz Bettarel (Periodista)

**Imprenta:** Emelar
Madrid, marzo de 2010

# Índice


Socios Fundadores 6

**Carta del Presidente** 7

Organos de Gobierno 8

Presentación de la Asociación 9

Colaboradores y patrocinadores 11

**Actividades 2009** 13

Jornadas Internacionales 13

V Jornada: La organización de la seguridad:
El laberinto del CISO. 14

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. 24

Otras iniciativas 34

Data Privacy Institute (DPI) 34

Otras sesiones formativas 35

Curso de Analista de Riesgos en Seguridad de la Información 35

Seminario intensivo DLP 36

Convenios de colaboración 37

CSA y ETICOM 37

Colaboración con otras organizaciones 38

Publicaciones 40

ISMS en los medios 41

Empresas asociadas 42

# Socios Fundadores












09

**Gianluca D'Antonio**
Presidente

*Estimados socios, colaboradores y amigos:*

*El año pasado finalicé la carta de presentación de la memoria agradeciendo el apoyo y la colaboración de todos los miembros del **ISMS Forum Spain**. Sin embargo, mientras me pongo a escribir estas líneas para presentar la nueva memoria y miro las iniciativas y actividades llevadas a cabo durante el tercer año de vida de nuestra Asociación, creo que en esta ocasión lo conveniente es empezar con los agradecimientos.*

*A nuestros Gold Sponsor y demás patrocinadores que, año tras año, siguen apostando por el trabajo que llevamos desarrollando para consolidar el rol de la Seguridad de la Información en las Organizaciones sobre los cimientos de una eficaz gestión de los riesgos y de profesionales capacitados y motivados.*

*A los Organismos Institucionales de ámbito Nacional e Internacional que, cada día más, están reconociendo el valor y la utilidad de una Asociación como la nuestra, comprometida con la sociedad y volcada en la tarea de concienciación y difusión de las mejores prácticas de Seguridad de la Información. Como el Ministerio de Industria, Turismo y Comercio (MITYC) que a través del programa AVANZA, ha concedido al ISMS Forum Spain la subvención para la realización del Portal Web de formación y divulgación sobre diferentes aspectos relativos a la seguridad de la información, dirigidos a particulares, profesionales, empresas e instituciones.*

*A todos los miembros que activamente han apostado por colaborar en beneficio de todos los profesionales de la Seguridad apoyando las iniciativas de la Asociación.*

*El ISMS Forum cumple tres años con la convicción de que el camino emprendido es el correcto, los resultados así lo demuestran, estamos creciendo en número de socios y apoyos institucionales. Hemos concluido el 2009 con la creación del Instituto de la Privacidad (DPI) y el lanzamiento de la primera Certificación para Profesionales de la Privacidad (CDPP).*

*Esta trayectoria nos refuerza en el compromiso que suscribimos hace tres 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. Es verdad, que como afirma Ron Collette, autor del libro CISO Soft Skills, nuestra profesión es joven y que la Seguridad de la Información como todas las disciplinas necesita tiempo para madurar. Sin embargo, precisamente para estas razones, los que formamos el ISMS Forum creemos que tanto el desarrollo de los sistemas de gestión como la capacitación de las personas que quieren trabajar en este ámbito es clave para alcanzar este nivel de madurez tan necesario.*

# Organos de Gobierno

El gobierno de ISMS Forum Spain se realiza por los siguientes Órganos:

## LA ASAMBLEA DE SOCIOS

La Asamblea es el órgano supremo de decisión y gobierno de ISMS y está constituida 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 2009, la Asamblea tuvo lugar el día 29 de enero y contó con un quórum de asistencia de 311 socios. En esta oportunidad se introdujeron algunos cambios en los Estatutos, entre los que destacan la creación de dos nuevos órganos de gestión y toma de decisiones como son el Comité Operativo y el Director Ejecutivo.

*En la imagen, de izda a dcha: Joan Camps Pons, Enrique Polanco, Gianluca D´Antonio, Alfonso Fernández, Ana Belén Santos, Antonio Ramos, Luis Buezo, Carlos A. Saiz, Álvaro R. de Roa, Juan Miguel Velasco López-Urda y Jesús Milán Lobo.*

## LA JUNTA DIRECTIVA

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

En la Asamblea General de 2009, se eligió a los siguientes titulares:

### Presidente:

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

### Vicepresidente y Secretario:

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

### Miembros:

**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.*

**Alfonso Fernández Jiménez.**
*Director de Desarrollo de Negocio de Seguridad e IT Management, Grupo SIA.*

**Jesús Milán Lobo*.** *Director de Seguridad de Sistemas, BANKINTER.*

**Fernando Pescador.**
*Director Servicios Informáticos. Universidad Complutense Madrid.*

**Enrique Polanco González.** *Director de Seguridad Corporativa y adjunto al Consejero Delegado, Grupo PRISA.*

**Ana Ramos.** *Responsable de Seguridad y Calidad de Sistemas, British Telecom (BT).*

**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.*

**Juan Miguel Velasco López-Urda.**
*Director Asociado de Servicios y Proyectos de Seguridad, grandes clientes, Telefónica España.*

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

## COMITÉ OPERATIVO Y DIRECTOR EJECUTIVO

El Comité Operativo es el órgano encargado 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. El Comité está formado por un grupo de miembros de la Junta Directiva. Por su parte, el Director Ejecutivo es el encargado de velar por la correcta ejecución de las decisiones tomadas en el seno de los Órganos de Gobierno, y de dirigir la gestión del día a día en ISMS Forum.

# 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.** Su finalidad 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 Sistemas de Gestión de Seguridad de la Información (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 en la actualidad a más de **100 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 **650 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.

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

DPI Data Privacy Institute
AN ISMS FORUM INITIATIVE

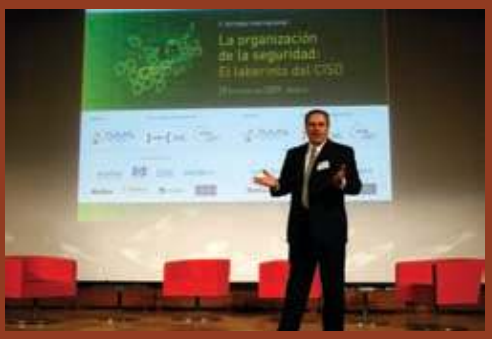
**ISMS Forum Spain** ha presentado recientemente el **Data Privacy Institute (DPI),** cuya vocación es aglutinar a todas las personas y organizaciones que tienen interés y responsabilidades en el ámbito de la Privacidad y Protección de datos personales, promoviendo la formación y excelencia en este área de creciente importancia. En este sentido ya ha puesto en marcha la certificación **CDPP (Certified Data Privacy Professional)** específicamente dirigida al área de la Privacidad y pionera en España. El DPI pretende asimismo ser una vía para la difusión de mejores prácticas en el uso y la protección de los datos personales entre las empresas y particulares españoles, y facilitar cauces de interlocución con las administraciones y autoridades de control.

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

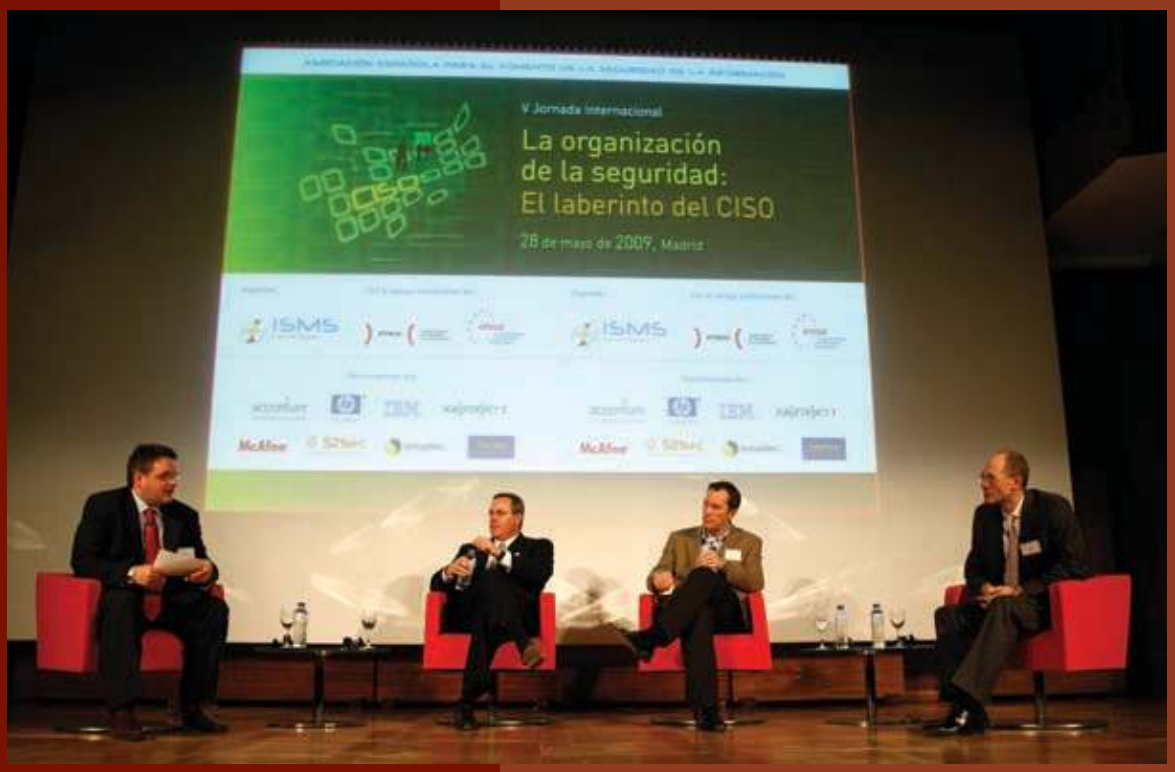
**Socios Fundadores:**

**BANKINTER • BT • CONSEJO GENERAL DE COLEGIOS DE MÉDICOS DE ESPAÑA • ECIJA • FCC • FUTURESPACE • GAS NATURAL • HEWLETT-PACKARD • SANITAS • S21SEC • SGS ICS • UNIVERSIDAD COMPLUTENSE DE MADRID**

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


La organización
de la seguridad:
El laberinto del CISO


ISMS


V Jornada Internacional
La organización
de la seguridad:
El laberinto del CISO
28 de mayo de 2009, Madrid
ISMS
ISMS

# Agradecimientos

## Apoyo institucional

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

Así mismo agradece al Ministerio de Industria, Turismo y Comercio por su apoyo para el desarrollo del portal "Protege tu informaciòn" 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 SPONSORS de la Asociación en 2009:

## 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.

# Actividades 2009,
# 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 1500 las personas que han participado en las 6 jornadas organizadas en 2007-2009,** 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.

En 2009, por primera vez organizamos una jornada en Sevilla. Consideramos 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.

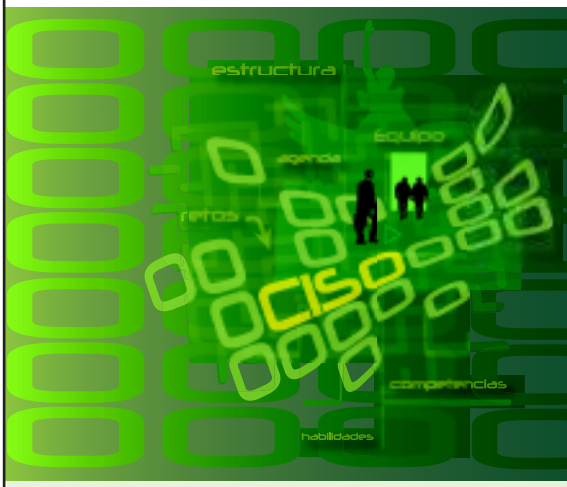
Asistencia a las Jornadas Internacionales de ISMS Fórum Spain

| | 2007 | | 2008 | | 2009 | |
|---|---|---|---|---|---|---|
| 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** |
| Nº de asistentes | 202 | 256 | 258 | 270 | 280 | 200 |

# Actividades 2009,
# V Jornada Internacional

ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN




V Jornada Internacional

## La organización de la seguridad: El laberinto del CISO

28 de mayo de 2009, de 9:00 a 18:00 h.

Auditorio Mutua Madrileña, Pº Castellana, 33, Madrid

### Objetivos:

- **Conocer** los modelos y estructuras más óptimas de la organización de la gestión de la Seguridad de la Información de la mano de reconocidos expertos españoles e internacionales.
- **Ampliar** conocimientos sobre la figura del CISO: cuáles son sus competencias, qué habilidades tiene que tener, cómo es la composición de su equipo ideal y cuáles son los retos más importantes que afronta.
- **Intercambiar** experiencias y hacer *networking* con cerca de 300 profesionales y expertos en seguridad de la información en sesiones muy participativas y abiertas al debate.

La **inscripción previa** es requisito imprescindible para acceder a la jornada y al almuerzo, así como para recibir la documentación.

Se facilitará traducción simultánea.

Pulse aquí para acceder al programa completo

Pulse aquí para ver los CVs de los ponentes

**Para más información: www.ismsforum.es**
**formacion@ismsforum.es 91 436 74 13**

Organiza: ISMS Forum Spain

Con el apoyo institucional de: INTECO (Instituto Nacional de Tecnologías de la Comunicación), enisa (European Network and Information Security Agency)

Patrocinadores Oro: accenture, hp invent, IBM, KASPERSKY, McAfee, S21sec, symantec, Telefónica

Patrocinadores Plata: GigaTrust, sia, SOPHOS

Media Partners: auditoría y seguridad, CincoDías, CIO, CSO, red seguridad

# ¿Por qué una Jornada sobre la figura del CISO?

En esta ocasión nos ha parecido necesario plantear un debate acerca de la organización óptima de la seguridad de la información desde la perspectiva de la preparación y competencias de los profesionales que se ocupan de protegerla en las organizaciones. La figura del CISO -*Chief Information Security Officer*-, todavía algo difusa y poco extendida en nuestro país, aparece como el eje vertebrador de un equipo que tiene la difícil misión de facilitar la transición entre la "seguridad informática" -que nos ocupó en los inicios de la profesión- y la gestión integral de la seguridad, a la que inevitablemente nos dirigimos.

Esta necesaria evolución requiere de profesionales cada vez más cualificados, versátiles y capaces de comunicarse e interactuar con todos los niveles de la organización, pues la seguridad, y nosotros lo sabemos bien, es una responsabilidad conjunta fruto de la concienciación y el apoyo de todos. El CISO de nuestros tiempos necesita entender y compartir las necesidades, objetivos, percepciones y hábitos de los demás. Esta proximidad con todas las áreas de la organización es el verdadero reto de nuestra joven profesión.

Lo cierto es que han pasado ya más de 15 años desde que se aprobara la primera regulación española en materia de datos automatizados (LORTAD) y lo que antes era una disciplina puramente técnica, orientada a la salvaguarda de los sistemas informáticos, se ha convertido en un área estratégica del gobierno de las organizaciones. La información, el conocimiento, son hoy los activos más valiosos para empresas e instituciones, y las amenazas a su integridad evolucionan y se multiplican a un ritmo veloz. Al frente de esta nueva función se consolida, pues, la responsabilidad del CISO, que debe contribuir además a la consecución de los objetivos del negocio. No es tarea fácil, al punto de que en esta V Jornada Internacional lo hemos situado, simbólicamente, en el interior de un laberinto.

Para encontrar la salida hemos pedido ayuda a expertos españoles e internacionales, y junto a ellos reflexionamos acerca de los retos y prioridades que debería marcarse el responsable de la seguridad de la información. Les hemos preguntado, también, qué habilidades y formación requieren el CISO y su equipo, y cuál sería la estructura más idónea para desarrollar su trabajo con la excelencia como meta. También reflexionamos acerca del actual contexto económico, en el que resulta más estratégica que nunca la capacidad del CISO para, con una visión generalista, implicar a la alta Dirección en una materia tan sensible y vital como es la Seguridad de la Información.

# Ponentes del máximo nivel

En esta V edición, volvimos a contar con ponentes españoles e internacionales del más alto nivel, que expusieron su visión acerca de la figura del CISO en el contexto actual.


*Ron Collette*

## Destacamos la presencia de:

El co-autor de libros como "CISO Handbook" y "CISO Soft Skills", y consultor **Ron Collette.**

Uno de los analistas más prestigiosos de Forrester Research, **Khalid Kark.**

**Serge Moreno,** CISO de Carrefour Bélgica.

Además de expertos de INTECO (**Victor Manuel Izquierdo**), Symantec Inc. (**Justin Soimani**), Steria (**Julio César Álvarez**), ONO (**Miguel Rego**) e ICM (**Raúl Avedillo**).

## Principales conclusiones / Por: Laura Díaz Bettarel

# La comunicación, el liderazgo y una medición más tangible de los beneficios de invertir en seguridad, retos clave en el desarrollo profesional del CISO.


*Victor Izquierdo*

**El auditorio del edificio de la Mutua Madrileña en Madrid reunió el pasado 28 de mayo a 270 expertos en seguridad de la información con motivo de la V Jornada Internacional de ISMS Forum Spain, titulada "La organización de la seguridad: El laberinto del CISO". Durante el encuentro se analizaron diferentes modelos y estructuras para la organización y gestión de la seguridad así como las características y atributos que debe tener el CISO para alcanzar sus objetivos dentro de la empresa. Las claves apuntadas por los expertos: tener capacidad de liderazgo y saber convertir sus estrategias en proyectos alineados con el desarrollo del negocio.**

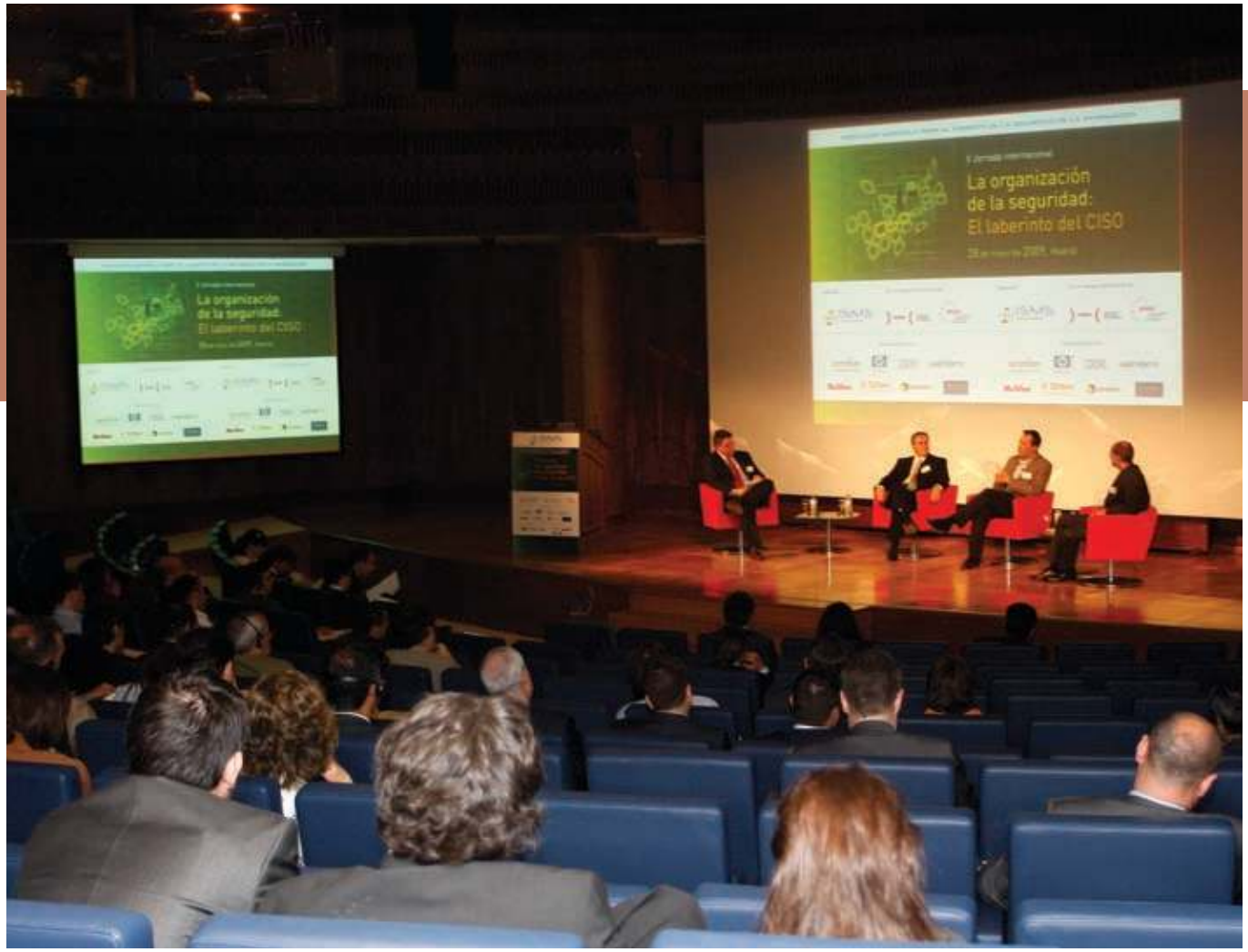
Más de 110 organizaciones y empresas públicas y privadas, de los más diversos sectores, estuvieron representadas en la V cita internacional organizada por ISMS Forum Spain.

## Aliar formación y concienciación

La V Jornada de ISMS Forum fue inaugurada por Víctor Izquierdo, director de INTECO, quien repasó las labores del Instituto y expuso los "Retos y Oportunidades para la organización de la Seguridad" desde el punto de vista del organismo que representa, del que destacó como líneas estratégicas la seguridad tecnológica, la accesibilidad y la calidad del software. A través de ellas INTECO ayuda a sus 'clientes' que van desde las administraciones públicas hasta las pymes y empresas que no pueden permitirse tener un CISO.

El representante del INTECO explicó que también prestan servicios de seguridad de la información a sus clientes a través de servicios y programas como el CERT (Centro de respuesta a incidentes en IT), orientado a pymes y ciudadanos; el Centro Demostrador de Tecnologías de Seguridad, la promoción del DNI electrónico y los servicios ofrecidos para su aplicación, y un Observatorio que permite conocer a través de investigaciones cómo evoluciona la situación de la seguridad de la información en España.

Este Observatorio se nutre de las encuestas que realiza, según explicó Izquierdo. "Pero a día de hoy recoge percepciones que a veces no coinciden con la realidad. Por ello hemos llegado a acuerdos con una muestra de pymes para instalar programas informáticos en sus ordenadores y efectuar un análisis mucho más estricto de lo que esta ocurriendo".




Según Izquierdo, las pymes instalan medidas de seguridad más tradicionales y de carácter pasivo. Destacó que la parte más vulnerable de la seguridad la encontramos en los empleados, y afirmó que más de la mitad de las pérdidas de información se debe a errores de trabajadores y no a ataques externos. El problema de robo y pérdida de información se ha agravado por la proliferación de dispositivos como los USB y la tecnología bluetooth.

En relación con el cumplimiento de la normativa en materia de protección de datos, INTECO contrastó en un estudio las declaraciones de pymes con datos obtenidos de otras fuentes: "Un 37% declara que ha notificado sus ficheros, pero sólo el 21% de ellas los ha presentado realmente al registro de la AEPD". ¿Pero puede INTECO ayudar a los CISO de grandes empresas?, se preguntó Izquierdo durante su ponencia. "Sí. Los desafíos de seguridad afectan a las empresas independientemente de su tamaño. Las grandes pueden estar mejor equipadas pero tienen que defenderse de más ataques y de mayor sofisticación".

## Recomendaciones para la industria

Combinar formación y concienciación es lo más eficaz para prevenir ataques, en opinión de Izquierdo. Entre los grandes desafíos están el robo de identidades on-line y las infraestructuras de información críticas; aspectos muy importantes para las administraciones, los gobiernos y las grandes empresas proveedoras de servicios. Para Izquierdo, una de las soluciones más eficaces es la autenticación electrónica. "En España contamos con el DNI electrónico, que supera ya los 9 millones de usuarios".

Desde la perspectiva de INTECO, la industria tiene que adaptar sus productos y sus servicios para que la Pyme pueda protegerse mejor. "Por ejemplo mediante sistemas de seguridad que se paguen por uso o por plazos". Igualmente, los precios deberían adecuarse al esquema y necesidades de estas organizaciones.

## Pasos para encontrar al equipo adecuado

Co-autor de los libros "CISO Handbook" y "CISO Soft Skills", auténticos manuales de referencia para la profesión, el experto norteamericano Ron Collete fue el encargado de exponer cuáles son las características y habilidades más importantes del CISO y de su equipo. Con un estilo muy dinámico, Collette dejó claro que no tenía una respuesta única sobre los atributos que son más importantes en el equipo de seguridad. Pues eso, sin duda, "depende de cada

**Combinar formación y concienciación es lo más eficaz para prevenir ataques, en opinión de Izquierdo. Entre los grandes desafíos están el robo de identidades on-line y las infraestructuras de información críticas; aspectos muy importantes para las administraciones, los gobiernos y las grandes empresas proveedoras de servicios.**

organización". Y explicó que en ello radica la dificultad, pues hay muchas influencias compitiendo. "La seguridad toca todo en una empresa. Hay requerimientos psicológicos, sociológicos y del entorno".

Los pasos a seguir para encontrar al candidato más adecuado: Primero hay que determinar el prototipo o perfil organizacional. Posteriormente determinar las áreas en las que operará el programa de seguridad y sus atributos: ¿Se trata de una organización centralizada de la seguridad o descentralizada? ¿Sus áreas de responsabilidad serán lógicas, físicas o ambas? ¿Se requiere que actúe como asesor o que tenga una participación más autoritaria? ¿Proactivo o reactivo? El tercer paso: construir una imagen para el rol dependiendo de la cultura de la organización y sus necesidades. Crear una matriz con el tipo de persona que se necesita: Arquitecto (orientado a soluciones), Policía (enfocado en el cumplimiento de los procedimientos), Auditor (enfocado en la comprobación), Hacker (detectar los fallos), Burócrata (centrado en la interpretación y desarrollo de procesos).

Collette repasó algunos de los atributos que deben tener los profesionales de la seguridad, tales como ser capaz de visualizar el programa antes de que esté terminado. Actuar como comandante y tener la habilidad de inspirar, motivar y liderar, un gurú técnico, un educador, un organizador, entre otros. Pero básicamente, Collete aclaró que se necesita alguien capaz de demostrar que usará esos atributos cuando se requiera, más allá de su experiencia previa. Y no olvidar que "encajar en la organización puede ser más importante que contar con una serie de habilidades".

## Paciencia y saber comunicar

Durante el espacio de preguntas se pusieron de manifiesto algunas de las preocupaciones de los CISOs presentes en el Auditorio de la Mutua Madrileña. ¿Tan importantes es que el CISO de una organización sea paciente? Collette dejó clara la relevancia de este atributo. "Hay dos cosas que le digo a un nuevo CISO: no tomes tu trabajo como algo personal. No puedes; morirás de un ataque cardíaco en una semana. Estás peleando con dos factores: uno es el riesgo, pero también tienes que ganarte a la organización. Si tienes una compañía de 2000 personas, todos ellos son vectores que tienes que proteger y que tienen que entender lo que haces. Toma años de entrenamiento lograrlo".


*Ron Collette*

Más preguntas del público: ¿Cómo puede el consejero delegado entender al CISO? "El consejero delegado no tiene que entender nada. La pelota está en el tejado del CISO, y su gran habilidad será traducir los riesgos que afronta su programa de seguridad en riesgos medibles y estratégicos para el negocio. En problemas que el Consejo de Dirección entiendan y que les preocupen".

## Fomentar la seguridad a través de la formación

Para finalizar la primera sesión, Carlos Alberto Sáiz, vicepresidente de ISMS Forum, habló de las próximas actividades de la asociación y presentó el primer curso de "Análisis de Riesgos para la Seguridad de la Información". Igualmente adelantó el tema de la próxima jornada del ISMS Forum que se llevará a cabo el mes de noviembre en Sevilla: "El efecto y el impacto de la crisis en el sector de la seguridad y los nuevos escenarios que afronta el sector".

## Una era de Renacimiento del CISO

Khalid Kark, analista principal de Forrester, abrió el segundo segmento de la mañana para hablar de organización: posicionamiento, estructura y equipo para el gobierno optimo de la seguridad. Kark inició su presentación explicando que los CISO habían pasado de un estado de ánimo alegre a uno sombrío y melancólico entre 2008 y 2009. "Por la disminución de los presupuestos, el CISO ha perdido visibilidad y siente que la seguridad no es una prioridad para los gestores de la empresa. Por ello hay que repensar su labor".


*Gianluca D'Antonio*

*Khalid Kark*

"Tenemos que ser hábiles para transmitir nuestros mensajes de una manera que sean entendidos por los gestores y necesitamos nuevas herramientas. Ahora estamos en un periodo de renacimiento. Un punto de inflexión en el que, si hacemos las cosas bien, seremos valorados dentro de la organización". En la actualidad el trabajo del CISO es la gestión del riesgo de la información, pero según Kark, en el futuro habrá que ayudar a la "transformación del negocio".

Kark expuso los resultados de un estudio de European Enterprise y SMB Security, en el que se consultó a una base de 285 personas encargadas de tomar decisiones en relación con la seguridad en empresas europeas. En el 41% de las empresas en Europa los CSO reportan al CEO o a la Dirección (en EEUU ese porcentaje es del 34%) y un 17% reporta al Comité Ejecutivo. Si se suman esas dos cifras, en Europa los CSO aun tienen mucha visibilidad en la organización. El estudio también determinó que los CISO "son responsables de casi todo". Por eso hay que saber cuáles son las competencias clave y en qué centrarse. En este sentido, explicó que quizá una de las tendencias que veamos en el futuro sea la externalización o delegación de ciertas responsabilidades operacionales, de forma que el CISO tendrá más tiempo para crear valor en la organización. "Es el único sector para el que se proyecta un crecimiento aproximado de un 10% en los próximos años".

Kark ve la organización de la seguridad estructurada en dos amplias áreas. Un lado estratégico de la seguridad, centrado en 'Políticas y gestión' y otro en "Gobierno y medidas". Además de proteger los datos, la principal función de los responsables de la seguridad de la información es asesorar a la empresa acerca de todos los problemas relacionados con el riesgo. "Hay que hacer marketing de la


*De izquierda a derecha: Antonio Ramos, Ron Collette, Justin Somaini y Nils Puhlmann*

seguridad. No puedes comunicar y esperar que la gestión de la empresa, a todos los niveles, entienda lo que estás diciendo", aseveró. Además de eso, el CISO debe supervisar el cumplimiento de las políticas de seguridad y asegurar que todos las ejecutan de manera efectiva.

En su propuesta de organización, Kark mencionó tres áreas y responsabilidades que deben existir de forma separada aunque interdependiente: Gobierno, riesgo y obediencia; Planificación y diseño; y Operaciones y aplicaciones.

**"Tenemos que ser hábiles para transmitir nuestros mensajes de una manera que sean entendidos por los gestores y necesitamos nuevas herramientas. Ahora estamos en un periodo de renacimiento. Un punto de inflexión en el que, si hacemos las cosas bien, seremos valorados dentro de la organización"**

**Khalid Kark,** ***Forrester Research.***

Para concluir, Kark propuso a los asistentes una serie de pasos a aplicar a la manera de un plan de acción para los próximos 90 días (encontrar aliados en otras áreas de la empresa, crear un consejo de seguridad en la organización, empezar a gestionar la seguridad como un negocio, identificar campos en los que se pueda delegar y asegurar la puesta en marcha de procesos de madurez en esas áreas), así como objetivos a largo plazo para estructurar y posicionar al equipo de seguridad de la información (como por ejemplo alinear la estructura organizativa con la cultura empresarial y el tamaño de la organización, ser creativo y asegurar la transparencia).

Ambos expertos, Collette y Kark, se reunieron después en un debate moderado por Antonio Ramos (S21sec) con Justin Somaini, vicepresidente y CISO global de Symantec, y Nils Pulmahnn, representante de la organización internacional Open Group y CISO de la compañía Qualys. Los cuatro aportaron sus experiencias y consejos a la audiencia. En un punto estuvieron todos de acuerdo: el CISO y su equipo deben dejar de ser, para la empresa, el departamento del NO y de las prohibiciones; y adoptar una postura mucho más colaborativa y positiva para lograr la implicación de todos.

## ¿Quién es CISO? ¿Lo soy yo?

Así tituló su exposición Serge Moreno, CISO de Carrefour Bélgica, quien repasó los distintos modelos organiza-


*De izquierda a derecha: Luis Buezo, Miguel Rego, Raúl Avedillo, Julio Cesar Álvarez y Guillermo Llorente.*

cionales que ha visto en los diferentes puestos que ha ocupado, y las funciones del CISO -muy diversas, ya que engloban aspectos financieros, de recursos humanos, de desarrollo, de marketing y comunicación, etcétera-. En cuanto a sus atributos, la honestidad y la integridad son fundamentales, como también lo es trabajar bien en equipo y ser comunicativo, negociador, intérprete, intuitivo, agente del cambio... Y teniendo en cuenta todo esto ¿Cómo debe ser el CISO? La respuesta para este CISO es: "Futurista, tiene que ser un evangelista, hablar con toda la gente de la organización y explicar los posibles peligros y riesgos, necesita ser un gestor de tecnología, un líder, mostrar entusiasmo aunque las cosas vayan mal". Y sobre todo: "hacer equipo" de todas las funciones de seguridad.

## Ser CISO en España ¿Una odisea?

Ese fue el punto de partida del debate de la tarde. Una discusión en la que el moderador Luis Buezo (director de la Práctica de Seguridad de HP), para retar a los participantes, estableció al inicio la prohibición del uso de ciertas palabras: marco estratégico, framework, alineamiento con el negocio, normativas. En el debate participaron Miguel Rego, director de Seguridad Corporativa de ONO; Raúl Avedillo, adjunto al director de Seguridad Corporativa de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid (ICM); Julio César Álvarez, Risk, Quality y MIS Manager de Steria España y Guillermo Llorente, director de Seguridad de Mapfre.

Al preguntar ¿Cuál es la figura del CISO en la organización y a quién reporta? Guillermo Llorente respondió que se trataba de una "pregunta trampa", pues se debe hablar de la figura del CISO en una organización específica. En el caso del CISO en Mapfre está dentro del Área de Seguridad y Medioambiente, a cargo de un director general que reporta al vicepresidente ejecutivo. "Yo soy responsable del área de Seguridad. En el organigrama está dentro de las áreas comunes: tecnología, medio ambiente. Una de nuestras responsabilidades es la protección de activos; la protección de la información está centrada en el cliente".

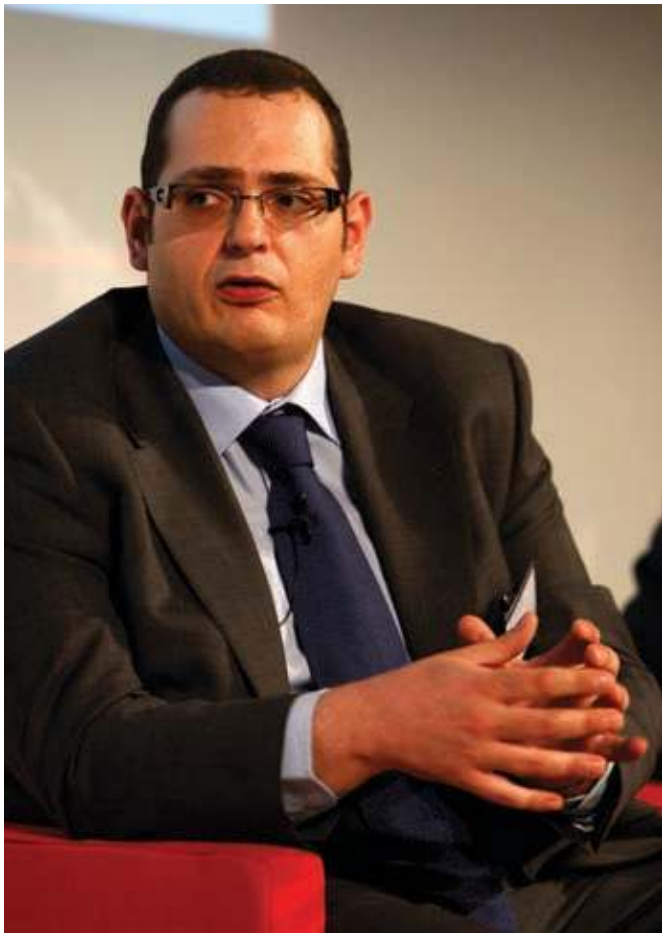
Sobre ONO, Rego explicó que la creación del CSO es relativamente reciente. Antes había un área de seguridad lógica y luego una de seguridad patrimonial y física. En junio del año pasado se decide crear una división que aglutine a ambas y que reporta al presidente. Julio César Álvarez, de Steria, explicó que en su caso, por tratarse de un grupo multinacional, en cada uno de los países se dan circunstancias específicas. En España la función del CISO la ejecuta la misma persona que hace la gestión de riesgos local y coordina la implantación de planes de investigación de riesgos corporativos. En España tiene presencia en el Comité de Dirección local. No obstante, a nivel corporativo no; reporta al director global de Riesgos y a la Dirección financiera. En el caso de ICM, Avedillo señaló que perte-

nece a la Dirección de Seguridad Corporativa, que engloba tanto la seguridad de activos y patrimonios como la información y la protección de datos.

El debate se animó al preguntar cómo es la relación en el día a día con el CIO de la empresa. Rego la calificó de excelente: "En ONO el área de seguridad lógica antes dependía del CIO y fue este quien decidió crear la división de CSO. Desde el punto de vista de la seguridad, el CIO tiene la implementación de políticas de seguridad y el CSO dice qué hacer y comprueba que se hace". Para Álvarez la relación es muy similar y cordial. "Nos ayuda tener una figura, la unidad de sistemas, que coordina la seguridad corporativa y la tecnológica". Por su parte, Julio César añadió que Steria creó un foro regulador a nivel internacional desde el que se definen las políticas. Llorente -en tono jocoso- explicó que la división de seguridad "es un chollo para los responsables de tecnologías, porque disminuye las posibilidades de que pase algo". "Cómo articulamos nuestras relaciones: a través de un Comité específico de Tecnología y Seguridad en el que se tratan todos los puntos en común. Puede haber fricciones, porque su interés es que salgan las aplicaciones y el nuestro que sean lo más seguras posible".

## ¿Cómo es la comunicación entre el CISO y su jefe directo?

Para Rego, la comunicación es fluida, pero hay que hacerle entender la función de seguridad. "Se asombran del grado de formalización de la seguridad. Es un tema cultural. Hay que aprender a trasladar las necesidades al director". Julio César Álvarez recordó que cuanto más background tecnológico tenga la otra parte más fácil es explicarle; en el caso del perfil financiero el mensaje debe regirse por el principio de la pérdida de productividad asociada a la perdida de información. Al respecto, Llorente aclaró nuevamente que en cada organización será de una manera y que depende de la capacidad de relación personal entre ambos. Pero a esa relación personal hay que ponerle un entarimado estable. Hay que poner por escrito el riesgo que hay. "Los consultores nos ayudan poco en esto: hay que dar un coste, una valoración a esos riesgos, una estimación de posibles daños o beneficios".



*Raúl Avedillo*

**"El CISO debe ser futurista, tiene que ser un evangelista, hablar con toda la gente de la organización y explicar los posibles peligros y riesgos, necesita ser un gestor de tecnología, un líder, mostrar entusiasmo aunque las cosas vayan mal, y sobre todo: hacer equipo de todas las funciones de seguridad"**

**Serge Moreno,**

***CISO de Carrefour Bélgica.***

Álvarez aclaró que esto era un punto clave y difícil. "En la medida en que podamos tener acceso a muchos casos reales, las estimaciones de riesgo serán buenas". Rego también señaló que "no se trata tanto de herramientas sino de ser capaz de medir el retorno en nuestra inversión".

Sobre la trayectoria para llegar a CISO o CSO y cómo consideran que se debería llegar, Rego, miembro de la armada, explicó que primero se especializó en seguridad más tecnológica y luego pasó a la gestión. "En mi opinión personal, la formación académica y la experiencia pueden ser muy heterogéneas. No hay vía única". Para Avedillo, en mayor o menor medida todos entran por el lado "tecnológico". "Creo que la evolución natural es conseguir la abstracción de esa parte tecnológica. Ser un intérprete al fin y al cabo, e interactuar con varios miembros de la organización". Para Julio Cesar Álvarez, es conveniente tener cierto background tecnológico y de gestión. Guillermo Llorente añadió que si se trata de una empresa pequeña probablemente sí hay que ser un tecnólogo, pero en una multinacional el perfil


*Jose Antonio Sainz*

tiene que corresponder más con el de un gestor capaz de liderar. Una persona con capacidad de entender lo que le dicen y facilidad para transmitirlo.

## ¿Y dónde está el límite en la carrera del CISO?

Para Rego el tope es ser un CSO, ser un buen gestor. A diferencia con otros directivos gestores, es más difícil moverte a otra área. Avedillo añadió que quizá la siguiente vía es pasar a una empresa especializada en seguridad. Julio César suscribió esto y añadió que el exceso de conocimiento es un handicap. Llorente comentó que si no hay posibilidades de crecer hacia arriba, se puede buscar que este todo mejor organizado y disminuir el riesgo al máximo posible, y quizá hay posibilidades de extender su alcance horizontal.

## Fluir, confluir e influir para lograr el éxito

Una vez más la clausura de la jornada rompió los cánones habituales y dio paso a una exposición dirigida a facetas mucho más relacionadas con la comunicación y las habilidades directivas que con los conocimientos tecnológicos. En esta ocasión fue el presidente del Instituto del Liderazgo en España y director de Eurotalent, José Antonio Sáinz, el encargado de hablar sobre el talento de liderar un equipo y proporcionó las claves de la capacidad directiva: liderar de forma versátil, fomentar un gran ambiente de trabajo, aprovechar tu intuición, escuchar con suma atención, y obtener resultados.

¿Cómo liderar? Para Sáinz "liderar podría compararse a jugar al golf... hay que saber qué palo usar en cada momento". Si se trata de una crisis, lo mejor es un "liderazgo de luz roja: dar instrucciones y generar imitadores". En épocas de bonanza, "liderazgo de luz verde: generar armonía y pedir sugerencias". Si hay que estar alerta al cambio constante, "liderazgo de luz amarilla: mostrar una visión (hacia dónde queremos ir) y capacitar al equipo para afrontar el cambio".

Sainz también ofreció una serie de recomendaciones útiles para mandar mejor. Primero: "toma decisiones: cuando toque, cuya responsabilidad te corresponda a ti, por ser el jefe". Asimismo el líder debe "controlar de cerca, sin abdicar, analizando el cumplimiento de los planes, de forma rápida y continuada. Los compromisos deben cumplirse en las fechas acordadas". Un buen jefe tiene que ser capaz de explicar qué es un trabajo bien hecho a cada uno de los miembros del equipo.

Desde el punto de vista del talento para dirigir un equipo, Sáinz expuso las capacidades que debe tener el "CISO actual ideal". Entre las competencias críticas: la confianza en sí mismo, orientación al logro, comunicación, liderazgo y visión global e integradora. Como competencias secundarias: integridad, optimismo, comprensión de los demás, orientación de servicio al cliente y conciencia política.

# Actividades 2009,
# VI Jornada Internacional

ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

VI Jornada Internacional

## Impactos de la Transformación Económica y Social en la Seguridad de la Información

El desafío de proteger los nuevos ámbitos y hábitos de trabajo

24 de noviembre de 2009, de 9:30 a 18:00 horas

Sevilla (Hotel Barceló Renacimiento - Isla de la Cartuja)

**Dirigida a todos los profesionales y expertos en Seguridad de la Información interesados en:**

- Los efectos de la crisis y los cambios producidos en la industria y el mercado sectorial.
- Cómo afrontar el incremento de la ciber delincuencia y de la fuga intencionada de información.
- Privacidad y seguridad en el camino hacia la Web 3.0; el fenómeno de las redes sociales; el auge del *cloud computing* y otras transformaciones en el uso de las TIC.

Conferencias y debates de expertos internacionales de primer nivel de representantes de **Accenture, Cloud Security Alliance, Forrester Research, GRUPO FCC, GRUPO PRISA, IBM, Infowatch, INTECO,** el **Ministerio Fiscal,** la **Policía Nacional, Tuenti** y **Verizon.**

La inscripción incluye documentación y almuerzo.
Se facilitará traducción simultánea.

**Pulse aquí para acceder al programa completo**

**Pulse aquí para los CVs de los participantes**

**Para más información: www.ismsforum.es**
**formacion@ismsforum.es 91 436 74 13**

Patrocinadores Oro:

accenture Alto rendimiento. Hecho realidad. · dintel · hp · IBM · KASPERSKY lab · McAfee · symantec · Telefónica

Con el apoyo institucional de:

enisa · CSA cloud security alliance · INTECO · Instituto Nacional de Tecnologías de la Comunicación · eticom

Media Partners:

Cinco Días · cibersur · CSO España · Dintel · red seguridad

# ¿Por qué jornada internacional sobre los Impactos de la Transformación Económica y Social en la Seguridad de la Información?

En esta ocasión quisimos plantear y debatir algunas de las principales cuestiones que marcan nuestra agenda en la actualidad, y que hemos englobado bajo un título que hace referencia a la transformación. Si bien todo se transforma y evoluciona en general, en nuestro sector estos cambios se suceden a menudo a una velocidad vertiginosa. Lo que ayer nos ocupaba hoy ha quedado obsoleto y desbancado por cuestiones que hace poco apenas intuíamos que estaban por llegar. Nuestra especialidad requiere, sin duda, una gran capacidad para fluir con la transformación, adaptarnos al cambio y estar en permanente alerta y contacto con lo que sucede a nuestro alrededor. Por ello nos fijamos hoy en varios fenómenos llegados de la mano de la web 2.0 que se han instalado en la vida de millones de usuarios en todo el mundo, y que tienen en común su importante repercusión en la materia que ocupa a los profesionales de la seguridad de la información y los responsables de privacidad de las organizaciones. Nos referimos tanto al auge de la nueva forma de trabajar "en la nube" como a las redes sociales (especialmente exitosas en España, donde ya hace un año se contabilizaban trece millones de usuarios). Recientemente se ha afirmado que España es, después de Brasil, el segundo país del mundo con mayor cantidad de usuarios de redes sociales en Internet, según la entidad pública Red.es. Hasta los ciudadanos han resaltado su creciente preocupación por los posibles usos fraudulentos de su información personal, como reflejaba el barómetro del CIS del pasado mes de octubre. Y es que las connotaciones de ambas "novedades" tecnológicas, en materia de protección de datos y seguridad, son notables y muy delicadas; pero no debemos olvidar que también constituyen importantes oportunidades para la mejora y la innovación en nuestro trabajo. Acerca de todo ello queríamos reflexionar en este encuentro y compartir de la mano de grandes especialistas las mejores formas de abordar estas cuestiones.

Por supuesto, también tratamos de contextualizar nuestro sector en el difícil momento económico que vivimos, y por ello revisamos también sus efectos en la industria de la seguridad. Muchas consecuencias de esta coyuntura global ya se han hecho notar, y pueden cuantificarse en términos de incremento de la ciberdelincuencia y de la fuga intencionada de datos; fusiones y compras de empresas del sector; impacto en tarifas y honorarios; aumento de la subcontratación de servicios (outsourcing) y reducción de presupuestos, en general, para la seguridad de la información en las empresas.

## Los ponentes

Como en anteriores ocasiones, ISMS Forum Spain contó en esta jornada con ponentes de máximo nivel, que expusieron sus conocimientos e ideas sobre los retos funcionales e internacionales del CISO, las implicaciones de seguridad en los modelos de outsourcing y cloud computing, los riesgos de la fuga de datos o las amenazas inherentes a las redes sociales.

### Destacamos la presencia de:

El cofundador y CISO de Cloud Security Alliance (CSA), **Nils Puhlmann.** Uno de los mayores expertos en cloud computing que hay en el mundo. CSA es una comunidad de más de 4000 expertos en seguridad que promueve el uso de mejores prácticas para ofrecer garantías de seguridad en cloud computing.

**Andrew Jaquith,** analista senior de Forrester Research. Hizo un análisis de la situación global de la industria. Sus 15 años de experiencia en TI y seguridad ayudaron a los asistentes de la jornada a comprender qué va a pasar en el sector en los próximos años.

El reconocido experto en Data Leak Prevention (DLP) **Oleg Mikhalsky,** director de la empresa rusa Infowatch, que se centró en la identificación de problemas y retos de la protección de la información sensible y la prevención de fugas de datos externas e internas mediante la tecnología DLP.

Además de otros 13 expertos nacionales e internacionales, todos máximos responsables de seguridad de la información de diversas empresas e instituciones públicas que compartieron sus experiencias y buenas prácticas en mesas redondas y ponencias.

## Principales conclusiones / Por ISMS Forum Spain

# Con la cabeza en las nubes y los pies en la tierra

### Los responsables de seguridad de la información deben ser capaces de asumir una gestión global del riesgo en entornos cambiantes.

**El entorno del Parque Tecnológico de La Cartuja, en Sevilla congregó el pasado 24 de noviembre a más de 200 expertos en Seguridad de la Información en torno a la VI Jornada Internacional de ISMS Forum Spain. Titulado "Impactos de la Transformación Económica y Social en la Seguridad de la Información", este encuentro facilitó el debate en torno a los retos funcionales e internacionales del CISO, las implicaciones de seguridad en los modelos de outsourcing y cloud computing, los riesgos de la fuga de datos o las amenazas inherentes a las redes sociales. La célebre frase "renovarse o morir" podría constituirse en lema del congreso, como veremos por las conclusiones de los distintos ponentes.**

La jornada estuvo poblada de comentarios y anécdotas que conformaron un adecuado análisis de la situación actual y de cómo la crisis mundial (todos los expertos internacionales admitieron que influía notablemente en el mercado de la seguridad) ha hecho evolucionar los riesgos tradicionales y a la vez plantea a la industria la necesidad de afrontar nuevos planteamientos.

La introducción de la jornada corrió a cargo de **Gianluca D'Antonio**, presidente de **ISMS Forum Spain** y CISO del **Grupo FCC**, quien recordó lo importante que es entender el pasado y el presente para comprender lo que puede deparar el futuro. Apuntó asimismo que ISMS Forum lleva ya tres años organizando dos jornadas internacionales anuales para reflexionar sobre el futuro de la sociedad de la información, en las que expertos internacionales colaboran aportando su experiencia acerca de lo que ocurre más allá de nuestras fronteras. Ya en la introducción se avanzó la sensación generalizada de que 2010 se anuncia duro, pues la crisis seguirá con nosotros, introduciendo así el contexto de las siguientes conferencias sobre el impacto de la crisis en el sector y cómo ésta afecta a la seguridad. Sobre el cloud computing, **D'Antonio** mencionó que, aunque lleva ya dos años entre nosotros, requerirá aún tiempo y conocimiento para aprovechar estas nuevas formas de hacer negocio, sabiendo gestionar el riesgo que esto también entraña. A este respecto, se entregó a todos los asistentes una llave USB con la nueva versión 2 del documento denominado "Guía para la Seguridad en áreas críticas de atención en Cloud Computing", que ha sido traducido por cortesía del ISMS Forum Spain desde el original en inglés de Cloud Security Alliance.

**Enrique Polanco**, director de Seguridad Corporativa del Grupo PRISA, impartió la conferencia inaugural, que analizó los desafíos de seguridad a los que se enfrentan las corporaciones españolas que tienen intereses en el extranjero y el reto de los cambios económicos y sociales. Entre los factores que potencian el riesgo destacó la diversidad de legislaciones -sobre todo en lo concerniente a seguridad privada- además de la inestabilidad política y los diferentes grados de corrupción o de libertad de expresión en algunos países. Todo ello puede comprometer las operaciones de las compañías españolas con intereses en Latinoamérica. Recomendó la implantación de un Sistema Integral de la Seguridad, fruto de unificar la gestión de la .Seguridad de la Información, Física, Laboral y Medioambiental. "El nuevo Director de Seguridad Corporativa es un "Risk Manager", resumió Polanco, enfatizando las funciones del CISO como gestor del riesgo global que debe abordar los cambios desde un punto de vista internacional. "El primer paso para poder dar con las soluciones adecuadas es conocer bien los problemas a los que nos enfrentamos" aseveró.

El caso expuesto del Grupo PRISA da una idea de este contexto. Presente en casi toda Iberoamérica, con una notable dispersión geográfica (y por tanto sujeta a entornos legales y sociales muy diversos), debe afrontar notables desafíos que hace 20 años se consideraban riesgos emergentes y ahora han pasado a ser estratégicos y operativos. "Y no podemos olvidar – aseveró Polanco- que hoy la amenaza es global, difícil de prever, y puede tardar sólo unos segundos en propagarse".

Sin embargo, el responsable de seguridad de PRISA añadió que algunos países latinoamericanos, como Argentina y Chile, destacan en asuntos como la protección de datos; de hecho, explicó que Argentina incorpora el concepto de "habeas data" en su Constitución, aunque por lo general existe poca regulación al respecto. Por último, habló acerca de los esfuerzos que se están realizando en el ámbito internacional en pro de un ambiente global más seguro y de una adecuada gestión de riesgos "global", principalmente desde la OTAN. Allí se estudia en profundidad lo que se conoce como el Futuro Ambiente de Seguridad (o

*Andrew Jaquith*

FSE por sus siglas en inglés), que valora el riesgo desde varios niveles, estratégico, regional y transnacional. La vulnerabilidad -acentuada por la crisis económica- y la amenaza creciente son los dos vectores a contemplar en esta gestión del riesgo.

La siguiente ponencia fue impartida por **Andrew Jaquith**, analista Senior de Forrester Research en Estados Unidos. Comenzó insistiendo en que la economía actual está realmente mal, y que las amenazas se incrementan a ritmos vertiginosos. Las consecuencias serán que el outsourcing forzará a las empresas a centrarse en proteger los datos, en vez de proteger los dispositivos, como venía siendo común hasta ahora; este cambio será debido a la tendencia hacia el outsourcing, la consultoría estratégica, y el incremento de relaciones con terceros. Adelantó algunos datos, como que la externalización mediante offshoring crecerá a un 25% en el 2010 en Europa, respecto al 20% actual; siendo un 23% la previsión para los Estados Unidos en este año próximo.

Por ello recomendó la realización de estrategias de protección de datos que no dependan de los dispositivos, mediante diversas fórmulas; en unos casos accediendo de forma remota a la información, mediante clientes ligeros; en otros casos con datos replicados y la posibilidad de eliminar los datos en caso de pérdida o robo; o bien utilizando procesos de información en "burbujas" de seguridad (con virtualización por ejemplo); bien protegiendo los datos con plantillas de confidencialidad de la información dentro del propio documento o, por último, realizando una monitorización de la red, permitiendo o bloqueando el intercambio de datos con marcas de agua de tipo hash y fingerprint y tecnología DLP. "Focalizarse en la protección de los datos, no en la de los dispositivos permite a los CISOs decir sí a las nuevas oportunidades emergentes, como el uso del cloud computing, que se está incrementando exponencialmente", indicó.

**Jaquith** presentó la clasificación de Forrester sobre cloud computing, en una torre de cuatro capas, desde de la infraestructura física IaaS hasta la prestación de servicios basados en web y el SaaS. Indicó, sin embargo, que los CISOS son aún cautelosos respecto a la nube, pues les preocupan las cuestiones de seguridad, privacidad y adecuación legal y normativa. Para resolver los miedos relativos a cada uno de los riesgos, sugería una posible solución. Además, los análisis muestran la tendencia de los responsables ejecutivos de las empresas (directores financieros, gerentes, ser-

**La imparable evolución tecnológica se suma a los trepidantes cambios en los hábitos y actitudes de las personas que utilizan las TIC en la vida personal y profesional. Todo ello plantea un constante reto a los profesionales que se encargan de salvaguardar la información sensible.**

vicios jurídicos...) a influir cada vez más en las decisiones de tecnología, que necesitan que esté perfectamente alineada con la estrategia empresarial. Además, problemas intrínsecamente tecnológicos se han convertido en problemas de negocio, como es el caso del fraude, la propiedad intelectual, el espionaje industrial, el gobierno corporativo, la retención de empleados, la integridad del negocio, e incluso la ética corporativa. Algunos de los consejos que dio a los presentes: "El Plan del año pasado conviene revisarlo y actualizarlo en aras de alinearlo con el negocio"; "Ser proactivo en la gestión de riesgos, y aplicar métricas y Gobierno Corporativo". **El analista** concluyó que las competencias clave del nuevo CISO incluyen ser capaz de darle la vuelta al concepto tradicional de seguridad, mirando al futuro respecto a las funciones que serán necesarias para este replanteamiento de la seguridad. "La nube será lo mejor que le habrá podido ocurrir a la industria de seguridad", llegó a pronosticar **Andrew Jaquith** adelantando el motor de dichos cambios evolutivos.

El siguiente ponente, **Carlos Alberto Saiz**, Vicepresidente del **ISMS Forum Spain**, adelantó los próximos proyectos y actividades, presentando el ISMS Forum Spain como asociación sin ánimo de lucro, con el objetivo de fomentar la seguridad de la información en España, como se demostraba en esta VI jornada, comenzada hace ya 3 años, con más de 1.500 asistentes a lo largo de las 6 jornadas celebradas. Resumió y asintió sobre el contenido de las intervenciones anteriores, donde se ha hablado de Adecuación Normativa y Legal, se ha hablado de Gestión de Riesgos y de la crisis económica global, así de cómo los CISOS deben acercarse al negocio, alejándose de la tecnología y acercándose

**"La nube será lo mejor que le habrá podido ocurrir a la industria de seguridad." Andrew Jaquith, *Forrester***

al lenguaje del negocio. **Carlos** comentó los números del ISMS Forum Spain, que cuenta con más de 90 empresas asociadas y 650 profesionales dados de alta; entre ellos los 245 profesionales que representan a 130 organizaciones que han participado en esta VI edición, provenientes de la industria, proveedores, instituciones y clientes finales, cifra que se va incrementando edición a edición. Se anunció la nueva fecha para la siguiente edición, el 25 de mayo de 2010 en el Palacio de Congresos de Madrid, en el marco del VII VI Jornada Internacional de ISMS Forum Spain; orientada a cómo vincular competitividad, innovación y tendencias en el mundo de la seguridad y cómo la tecnología, CIOs y CISOS podemos aportar al negocio.

Como actividades del **ISMS Forum Spain**, comentó que se han añadido y distribuido nuevas publicaciones gratuitas, actualizado el registro de profesionales certificados, se ha comenzado a realizar acciones formativas, etc. Precisamente destacó el reciente Curso de Analista de Riesgos en Seguridad de la Información, dirigido por Jesús Milán e impartido en septiembre de 2009, contando con unos 20 asistentes; anunciando que se realizaría una segunda edición para la primavera de 2010.


*Carlos Alberto Saiz*

Otra de las recientes actividades del **ISMS Forum Spain** es la creación del Data Privacy Institute, foro de referencia en la materia y abierto tanto a personas como a empresas; donde se celebrará, en junio de 2010, el primer examen de certificación, si bien existirá un esquema de "Grandfathering" para profesionales. Esta certificación, denominada "Certified Data Privacy Professional" está orientada a profesionales abogados, consultores, CISOs, responsables de LOPD en las Administraciones Públicas, etc. y contendrá un cuerpo común de dominios de conocimiento, incluyendo los fundamentos, un marco general, el marco sectorial, etc. Además, en este sentido, se están planteando las Segunda Jornadas de Privacidad en el Sector Sanitario, con fecha para el 21 de enero de 2010, en Madrid, donde se tratará sobre la historia clínica informatizada, la receta electrónica, etc.

Otra de las iniciativas que se lanzarán en breve, en concreto en enero de 2010 es el DLP Forum, incluyendo el sitio web http:///www.dlpforum.es y patrocinado por las compañías McAfee, Symantec e Infowatch para la promoción e intercambio de experiencias relacionada con la tecnología Data Leak Prevention.

Una tercera iniciativa presentada por ISMS fue el Proyecto Eifosi. Gracias a una importante subvención, concedida a través del programa AVANZA, del Ministerio de Industria, Turismo y Comercio (MITYC), ISMS Forum Spain está trabajando en la realización de un portal web de formación y divulgación sobre diferentes aspectos relativos a la seguridad de la información, dirigidos a particulares, profesionales, empresas e instituciones. El proyecto ha sido bautizado con el nombre "EIFOSI" porque abarca la Evaluación, Información, Formación y Orientación para mejorar la Seguridad de la Información. El lanzamiento del Portal está previsto para finales de 2010.

Además de las iniciativas para este nuevo año, **Carlos** finalizó su intervención con las ventajas de formar parte de ISMS Forum, que incluyen formar parte de la comunidad de profesionales de seguridad, acceso libre a las Jornadas Internacionales, descuentos en las acciones formativas, inclusión en el registro de profesionales, tasas de examen reducidas para la certificación en el Data Privacy Institute, poder participar en los grupos del Linkedin y foros de debate, acuerdos con Masters y Escuelas de Negocios, etc.

A continuación, el experto en Cloud Computing, **Nils Puhllman**, Cofundador y CISO de Cloud Security Alliance impartió una conferencia titulada "A New Landscape to Protect: What's Coming Up on Information Security Challenges?" Comenzó su exposición aludiendo que existe una novedosa tendencia de "consumerización" de la tecnología", algo que Gartner lo llamó en el 2005 la tendencia más significativa que afectará a IT en los próximos 10 años. Se refiere a que una nueva generación está creciendo con la tecnología de consumo, y esto hace que los dispositivos tecnológicos y los "gadgets" se incorporen al mundo laboral. De esta forma, las TIC se convierte en una herramienta para fomentar la creatividad. Sin embargo, entre las predicciones de las amenazas creadas por los consumidores IT se encuentran los ataques sobre aplicaciones SaaS y los ataques de Phishing originados desde las redes sociales.


*Enrique Polanco González*

**"No podemos olvidar que hoy la amenaza es global, difícil de prever, y puede tardar sólo unos segundos en propagarse."**

**Enrique Polanco,** ***Grupo Prisa***

Nils enumeró alguna cifras sobre los millones de usuarios de ebay (85,7 millones en 2008), Zynga (60 millones, Google Voice (1.419 millones de usuarios un 40% de uso diario), Skype (521 millones de usuarios registrados) además del dato de crecimiento del 700% anual de minutos invertidos en FaceBook. Los mayores riesgos en estos entornos se centran en que no es posible probar la identidad del usuario, existe la posibilidad de revelación de información sensible o la pérdida completa de la privacidad y la focalización de ataques en las redes sociales fomentan la facilidad para los ataques basados en ingeniería social, y en especialización de los frameworks de distribución de código malicioso para estas redes.

Por otro lado, el juego online, los mundos virtuales y las redes sociales tienden a converger, con los nuevos riesgos que ello acarrea, citando a anécdota del mundo virtual SecondLife, con 16 millones de residentes registrados, en que en un solo día de agosto cambiaron de manos 120 millones de dólares virtuales. Estas transacciones virtuales tienen su impacto en el mundo real, pues allí empresas como Nike y Adidas venden en realidad calzado; Pontiac y Toyota venden coches reales, se alquilan servicios de seguridad y

**"El mayor error que ha cometido la industria es que hasta ahora ha trabajado en solitario"**

**Nils Puhlmann,** ***CSA y Zynga.***

servicios de escort, y los perfiles se compran y venden en eBay con dólares reales. Este fenómeno de venta de perfiles, denominado Gold Farming, tiene como consecuencia el explotar a la juventud, principalmente de sudeste asiático, para generar dinero virtual que se blanquea posteriormente en moneda real.

Nils planteó la problemática que plantea la velocidad de infección respecto a la velocidad de defensa de estas amenazas. "Cada 4-5 segundos se descubre un nuevo sitio propagador de malware", comentó Nils. De las páginas afectadas, 85% se encuentran en sitios web legítimos que han sido hackeados y los ataques se incrementan de forma transversal por las redes sociales llegando a los puestos de usuario. Se dieron datos sobre los 14 millones de PCs que se comprometieron por "botnets" en el segundo trimestre de 2009, un incremento del 16% sobre el trimestre anterior. Sobre los 150.000 nuevos ordenadores vendidos, fueron infectados un 20% de cada uno de ellos. Según el número de bots continúa creciendo, se empieza a ofrecer Malware as a Service para controlar a todos estos equipos. Aparte que la protección antivirus no es suficiente, al requerirse entre 2 y 5 días para cada nueva firmas, y más de 14 días para analizar y contrarrestar nuevos algoritmos de infección. El crimen libera nuevo malware más rápido que las actualizaciones de sistema antivirus, y cada vez hay más mutaciones.

¿Cómo afecta esto respecto a los nuevos planteamientos de Seguridad TIC? En el viejo mundo, la gente utilizaba lo que le ofrecían, la infraestructura IT era estática, las webs se enlazaban unas a otras... Sin embargo, en el nuevo mundo, las tecnologías funcionan casi en el "Just-in-time", crecen los servicios SOA, la computación en la nube, los modelos de pago por uso), todo ello produce un adelgazamiento en las infraestructuras y potencia los entornos ágiles y las infraestructuras flexibles. El nuevo Internet trata sobre la gente, cómo ésta hace uso de Internet y cómo se interconectan entre sí. De esta forma, la seguridad es un paraguas común para todo ello adaptándose a las tendencias de agilidad y velocidad. La gente utiliza lo que le gusta.

¿Cuál es la parte mala en todo esto? **Nils** realizó un juicio crítico con el inmovilismo en la visión tradicional de la seguridad. Para los profesionales de la seguridad, la adecuación normativa y legal es el nuevo estándar, la nueva línea base. Solemos ser reacios al cambio y adversos a estructuras flexibles. Los fabricantes, por su parte, ofrecen soluciones para problemas antiguos, cada vez son menos y menos innovadores y comprenden la seguridad principalmente desde el punto de vista técnico. Nils sentenció que "los malos tiene todas las ventajas sobre los buenos; y además que son más participativos y colaborativos", finalizando su intervención con la idea de que "el mayor error que ha cometido la industria es que hasta ahora ha trabajado en solitario".

*Manuel Cortés*

Un debate posterior, en el que participaron **Vicente Aceituno**, Presidente de **ISSA Spain**; **Manuel Cortés Márquez**, de **Accenture**; **Peter Stremus**, de **IBM ISS Bélgica** y **Bart Vansevenant**, Director de estrategia de **Verizon Bélgica** y moderado por Nils Puhlmann, sacó a la luz algunos temas polémicos, como por ejemplo cuestionando si el mercado estaba realmente evolucionando.

Este debate postulaba si las cosas estaban o no cambiando; pues aunque las tecnologías de información habían cambiado los medios y los canales de comunicación, los problemas eran los mismos, las soluciones las mismas, la tecnología muy similar... Se plantea que el negocio actual en las redes sociales y de consumo es la publicidad, no los millones de usuarios registrados, comentándose que han cambiado los medios y los canales de comunicación con las nuevas tecnologías, pero se mantienen las expectativas de los usuarios, de las empresas, etc. También se apostó por un proceso gradual de concienciación en seguridad de la información, como un método más eficaz en

**Marcos Gómez indicó que se resuelven desde el INTECO unas 20.000 incidencias de seguridad anuales; de las que un 30% se refieren al fraude por internet.**

lugar de "endurecer" la legislación con sanciones ejemplares. **Bart Vansevenant**, por su parte, comentó algunas anécdotas relacionadas con las investigaciones en análisis forense que revelaron fugas de datos en empresas de transporte europeas, en que existía una rotación anual con sus vicepresidentes de ventas. A lo largo del debate también se llegaron a importantes conclusiones, pues tras alguna pregunta planteada sobre la necesidad normativa, se consensuó que es mucho mejor aplicar una política de concienciación en seguridad que vaya "calando" mejor que aplicar una sanción ejemplar. "Las PYMES son una gran oportunidad para hacer grandes cosas con pocos esfuerzos" se llegó a decir. Se cerró el debate comentando que el sector de la Pequeña y Mediana empresa constituye una gran oportunidad para hacer grandes cosas en seguridad con un pequeño esfuerzo.

La última intervención de la mañana, fue llevada a cabo por **Oleg Mikhalsky**, Director de Infowatch (Rusia) y se centró en la identificación de problemas y retos de la protección de la información sensible y la prevención de fugas de datos externas e internas mediante la tecnología Data Loss Prevention (DLP). Una de las anécdotas del día fue la pregunta al auditorio sobre aquellas empresas que están realizando actualmente implantaciones relacionadas con tecnología DLP. A pesar de que gran parte del sector coincide es que es uno de los nuevos puntales de generación de negocio, con tendencia actual en inversiones de seguridad con gran crecimiento, solamente un puñado de asistentes alzó la mano, lo que introdujo una paradoja entre las expectativas del mercado y los proyectos actuales que en realidad se están acometiendo en la materia.

Después del almuerzo, la conferencia de **Marcos Gómez Hidalgo**, Subdirector e-Confianza del **INTECO**, abordó su experiencia sobre los servicios y oportunidades para la Pyme española en Seguridad de la Información. Comenzó enumerando las actividades del **INTECO** respecto a Gestión de Incidentes de Seguridad , Centro Demostrador, Observatorio de la Seguridad, etc. y las perspectivas de extender el proyecto para darle continuidad en el largo plazo. Resumió el objetivo del INTECO en el hecho de formar y concienciar a la PYME en materia de seguridad informática, especialmente en Sistemas de Gestión de Seguridad de la Información y en la implantación de los estándares ISO 27001. En resumen, dar un impulso al SGSI en el tejido industrial español, ejerciendo de tercero de confianza en la industria. El planteamiento incluye ser centro verificador de las 144 empresas certificadoras, y certificar a empresas de entre 25 y 45 empleados, hasta 250 empleados en total.

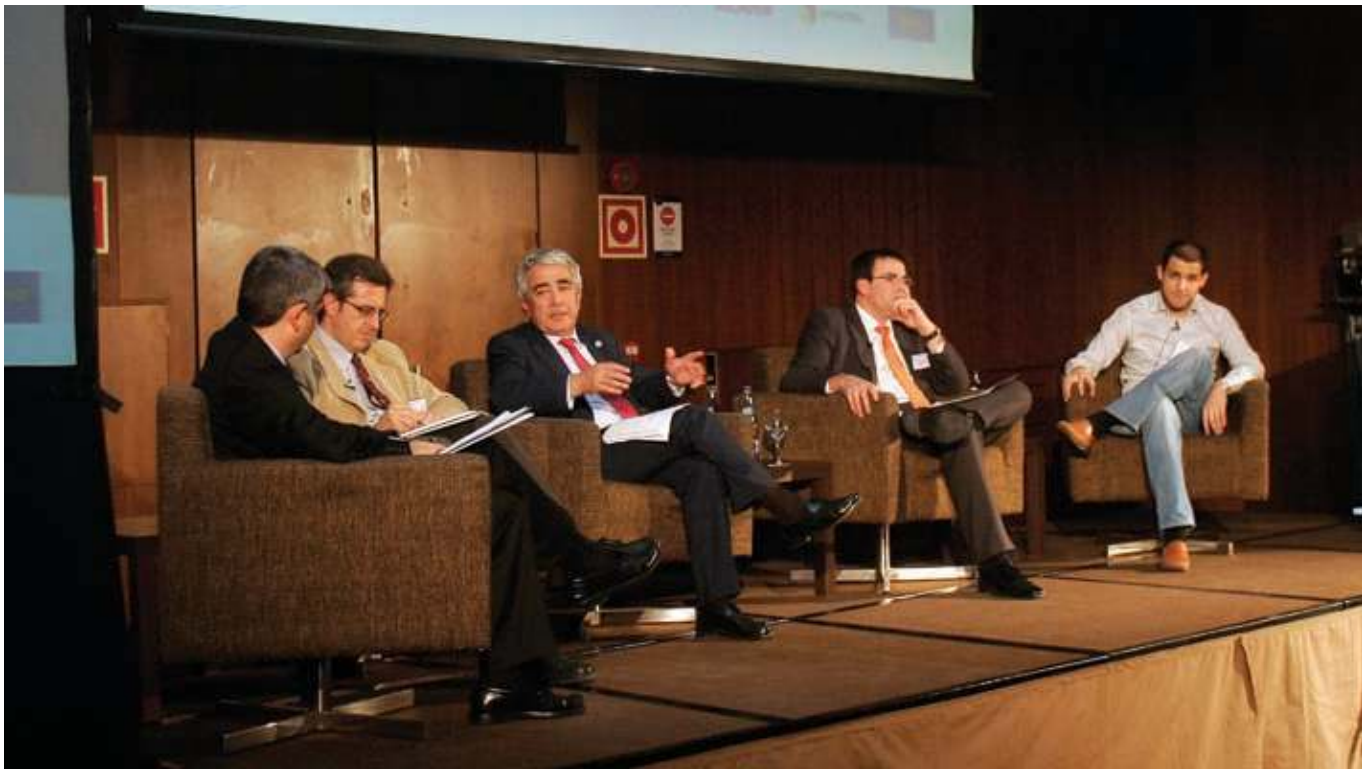
Tras una consulta lanzada sobre las principales motivaciones de las PYMES a la hora de certificar su SGSI, se comentó que el rasgo común sin duda ninguna es que a los directivos de las empresas se les había concienciado al asimilar el riesgo de las sanciones de la AEPD. Las recomendacio-

nes principales era elegir condicionantes tecnológicos y la existencia de un responsable de seguridad. Como resultado, un 98% de las empresas pasaron con éxito el proceso de certificación.

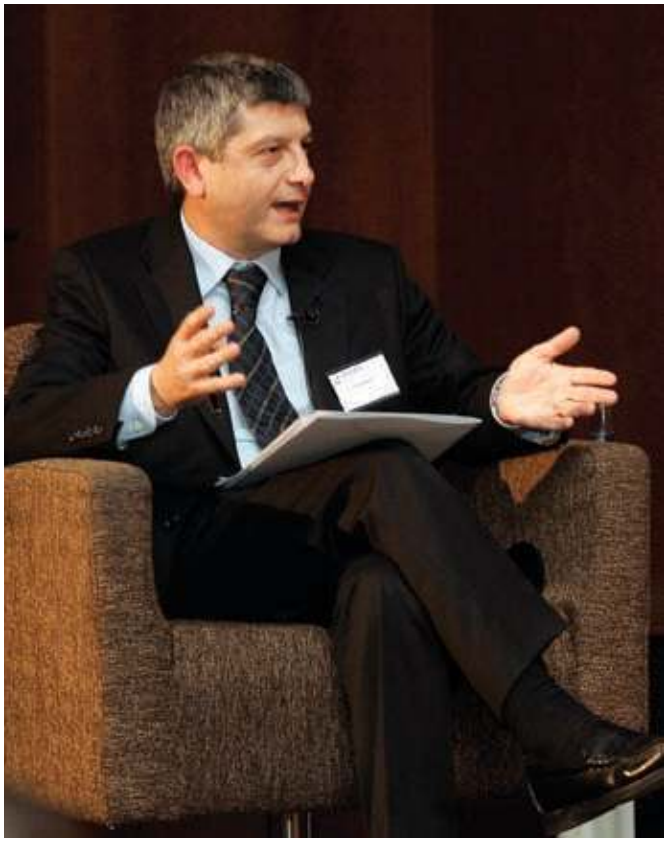
Marcos comentó, respecto al comportamiento medio de las micropymes en materia de seguridad, que su perfil de comportamiento es similar a cómo funcionaría un internauta individual; teniendo en cuenta el dato de que existen en España 3 millones de PYMES y 24 millones de internautas. El 30% de los encuestados dicen tener una deuda pendiente con el hecho de ponerse al día en seguridad; aparte, un 50% de los encuestados están familiarizados con términos como el "phishing"; aunque desconocen otros como malware, troyano o keylogger. **Marcos** finalizó su intervención con datos también interesantes; indicando que se resuelven desde el **INTECO** unas 20.000 incidencias de seguridad anuales; de las que un 30% se refieren al fraude por Internet.

A continuación se inició el debate de la tarde, que fue uno de los más interesantes y entretenidos del día, salpicado de anécdotas, chascarrillos y algo también de polémica; además de llegar a consensos, y conclusiones muy productivas. En este debate intervinieron **Francisco Hernández Guerrero**, Fiscal del Servicio de Criminalidad Informática del Ministerio Fiscal, **Rafael San Miguel Carrasco**, de Yumei, **Pedro Pablo Pérez**, Gerente de Marketing de Seguridad de Telefónica España y **Manuel Vázquez López**, Jefe de la Brigada de Investigación Tecnológica de la Comisaría General de Policía Judicial; moderado por **Antoni Bosch**, Director del Data Privacy Institute – ISMS Forum.

**Pedro Pablo** habló de las dificultades de detección y respuesta del crimen electrónico en redes sociales, derivadas de la captación, la acción a distancia y la internacionalización. **Manuel**, en base a su experiencia en la Brigada, nos contó que la lucha contra el cybercrimen se juega hoy en un ámbito global. "La acción preventiva suele corresponder a las empresas y organizaciones, pero cuando los controles fallan, es cuando entra en escena la acción policial", comentó. Añadió que las redes sociales han servido para iniciar movilizaciones, incluso a veces causas nobles; pero muchas otras veces se ha utilizado para la comisión de delitos. Los menores, por ejemplo, no tienen la personalidad formada, por lo que son objeto de delitos a través de estas redes sociales, como es el caso del Cyberbulling. "La ciencia es como un cuchillo", comentó. Las redes sociales son un elemento de nuestro tiempo; pero la tecnología va más rápido que las consideraciones morales y legales. Si se otorga capacidad a los menores, hay que ser coherentes en las formas de persecución. El debate cobró especial interés a raíz de comentar el éxito de inscripciones de menores en el portal de gestión de talentos del espectáculo **Yumei**, tras participar en el casting de un conocido programa de televisión, según comentó **Rafael Sanmiguel.** En este punto se abrió un interesante debate sobre legalidad, moralidad y responsabilidad de los padres, con aportaciones de todos los componentes de la mesa, y sentando cátedra en los temas por la autoridad y calidad de los ponente. Por ejemplo, **Francisco Hernández** realizó una interesante reflexión sobre el hecho de que "si se otorga capacidad a los menores, hay que ser coherentes en las formas de persecución en las redes sociales" respecto a la responsabilidad de los padres. **Manuel Vázquez** comentó el hecho de que si se dan demasiadas pistas para facilitar la ingeniería social; es posible por ejemplo mediante fotografías en diferentes situaciones, generar el perfil psicológico y anímico de una persona y



*De izqda. a dcha: Antoni Bosch, Francisco Hernández Guerrero, Manuel Vázquez López, Pedro Pablo Pérez y Rafael San Miguel Carrasco*



*Antoni Bosch*

**Francisco Hernández,** ***Fiscal del Servicio de Criminalidad Informática del Ministerio Fiscal,*** **realizó una interesante reflexión sobre el hecho de que "si se otorga capacidad a los menores, hay que ser coherentes en las formas de persecución en las redes sociales" respecto a la responsabilidad de los padres.**

las nuevas generaciones se aprovechan de las nuevas posibilidades de beneficiarse de ello. Aunque fue ecuánime en la utilización de estas redes: "prefiero que mis hijos estén en una red social que viendo determinados programas de la televisión que transmiten valores incorrectos" concluyó, como resumen de su planteamiento.

**Pedro Pablo** recordó respecto a la responsabilidad de los padres y la capacidad de filtrado de acceso a Internet, que los padres contratan para sus hijos un control parental para sus líneas ADSLs, en clara referencia al servicio Canguro.Net que presta Telefónica. **Toni Bosch** aprovechó el debate del filtrado de acceso para introducir el tema del paquete europeo de telecomunicaciones, lo que hacía cada vez más y más interesante el debate, a juzgar por los asistentes, que estaban tan concentrados en el interesante debate que no parpadeaban. A pesar de los puestos de responsabilidad y los cargos que ocupaban representando a sus respectivas organizaciones, los ponentes no dudaron en "mojarse" y entrar al trapo en la cuestión. **Francisco Hernández** sugirió que si tal vez las empresas de comunicaciones estaban inflando las necesidades de consumo de ancho de banda con grandes velocidades y orientadas a la descarga masiva; tal vez no debieran pretender cortar el acceso por descargar determinados contenidos. Todos los ponentes coincidieron en que existe un nuevo pacto social; en el que ni las empresas deben pretender extralimitarse en las restricciones, ni la sociedad debe por su parte parapetarse en posiciones radicales de desprecio a toda regulación. **Manuel**, matizó que desde la Policía nunca se han realizado investigaciones de forma directa contra usuarios de redes P2P, aunque sí sobre enlaces y propietarios de páginas. A lo largo del debate fueron varias las ocasiones en que surgió la polémica, sin miedo a expresar opiniones. Se comentó que "cualquier incidente informático se magnifica, porque es un asunto que vende. El problema es que los políticos hacen más caso a la prensa que a sus asesores, porque representan la opinión de los ciudadanos." En general, el debate de la tarde fue muy ameno, pero a la vez muy profundo y uno de los platos fuertes del día.

El resumen y el cierre de la jornadas fue responsabilidad de **Gianluca D'Antonio**, de nuevo como Presidente del **ISMS Forum Spain**. Comentó sobre la emisión, por parte de FCC, empresa de la que es Director de Seguridad de la Información, de un informe de vigilancia, con todas las publicaciones donde se hace referencia a la empresa, imagen y reputación corporativa, tanto para bien como para mal; y poder gestionar los riesgos que esto conlleva. Al respecto, comentó que la reputación en las redes sociales puede afectar a las distintas economías, pues orienta el consumo de los clientes como ha ocurrido con alguna empresa o producto. Insistió en que la seguridad de la información se trata hoy en día de vigilancia digital, de reputación corporativa. Son funciones transversales, no solamente tecnología.

Gianluca habló de las nuevas competencias del CIO, apuntando un 71% de gestión del riesgo y conformidad normativa. Entre los nuevos atributos del CISO habría que destacar los siguientes: jefe, visionario, escritor, vendedor, planificador, negociador, organizador, presentador CISO y las denominadas "soft skills" o habilidades directivas relacionadas con la inteligencia emocional y comportamiento. Los retos del CISO son ser aceptado, ser creíble, ser útil, ser eficiente, ser atractivo, ser competitivo, ser innovador. En resume, SER Y PARECER. Concluyó comentando que los CISOs estamos enfrascados en el día a día y no somos visibles; pareciendo que la empresa va por otros derroteros, instándonos a orientarnos más al negocio y a entremezclarnos con el lenguaje de la organización, como cierre de su intervención y de la jornada.

# Actividades 2009, otras iniciativas

DPI
Data Privacy Institute

## Nace el DATA PRIVACY INSTITUTE (DPI), una iniciativa de ISMS Forum que aglutinará a los expertos en privacidad y protección de datos personales

**"Es necesario potenciar la figura del Data Privacy Officer en las empresas españolas"**
**Artemi Rallo, director de la Agencia Española de Protección de Datos.**

Prácticamente a diario, los medios de comunicación llevan a sus portadas noticias referidas a la filtración, pérdida o publicación masiva de datos sensibles –incluso críticos- por parte de empresas e instituciones en los más diversos países. Informes recientes publicados por INTECO (Instituto Nacional de Tecnologías de la Comunicación) arrojan datos preocupantes, como que **sólo un 14% de las pymes españolas declara conocer el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos** (en vigor desde abril de 2008); o que **del total de pymes con ficheros automatizados, solo el 37% afirma haberlos declarado en el registro de la AEPD** (peor aún, pues contrastado este dato en la Agencia, sólo un 16% de las pymes los han declarado en realidad).

En contraste con esta falta de concienciación, los expertos están de acuerdo en que, tanto en el ámbito nacional como internacional, nos dirigimos a un entorno en el que la regulación relativa a protección de datos personales cobrará cada vez mayor importancia. Sin embargo, las organizaciones aún no prestan la necesaria atención a este capítulo y la figura del **Data Privacy Officer** (DPO) no está lo suficientemente reconocida y asentada en nuestro país, pese a que informes del **Article 29 Working Party** o de la propia **Comisión Europea** defienden desde hace años la necesidad de crearla. Tampoco existe una oferta formativa adecuada para la preparación de estos especialistas, ni una organización que los agrupe para dar visibilidad a su trabajo y facilitar su desarrollo y crecimiento profesional.

Por todo ello, conscientes de la importancia de la protección de datos y de su estrecho vínculo con el gobierno de la seguridad de la información, ISMS Forum Spain arrancó en julio de 2009 un nuevo proyecto, el **Data Privacy Institute** (DPI), cuya vocación es **aglutinar a todas las personas y organizaciones que tienen interés y responsabilidades** en la privacidad y la protección de datos personales, **promoviendo la formación y excelencia** de sus asociados y facilitándoles **cauces de interlocución con las administraciones y autoridades** de control. El DPI pretende asimismo ser una vía para la **difusión de mejores prácticas** en el uso y la protección de los datos personales entre las empresas y particulares españoles.

CDPP
Certified Data Privacy Professional
una certificación de DPI - ISMS Forum Spain

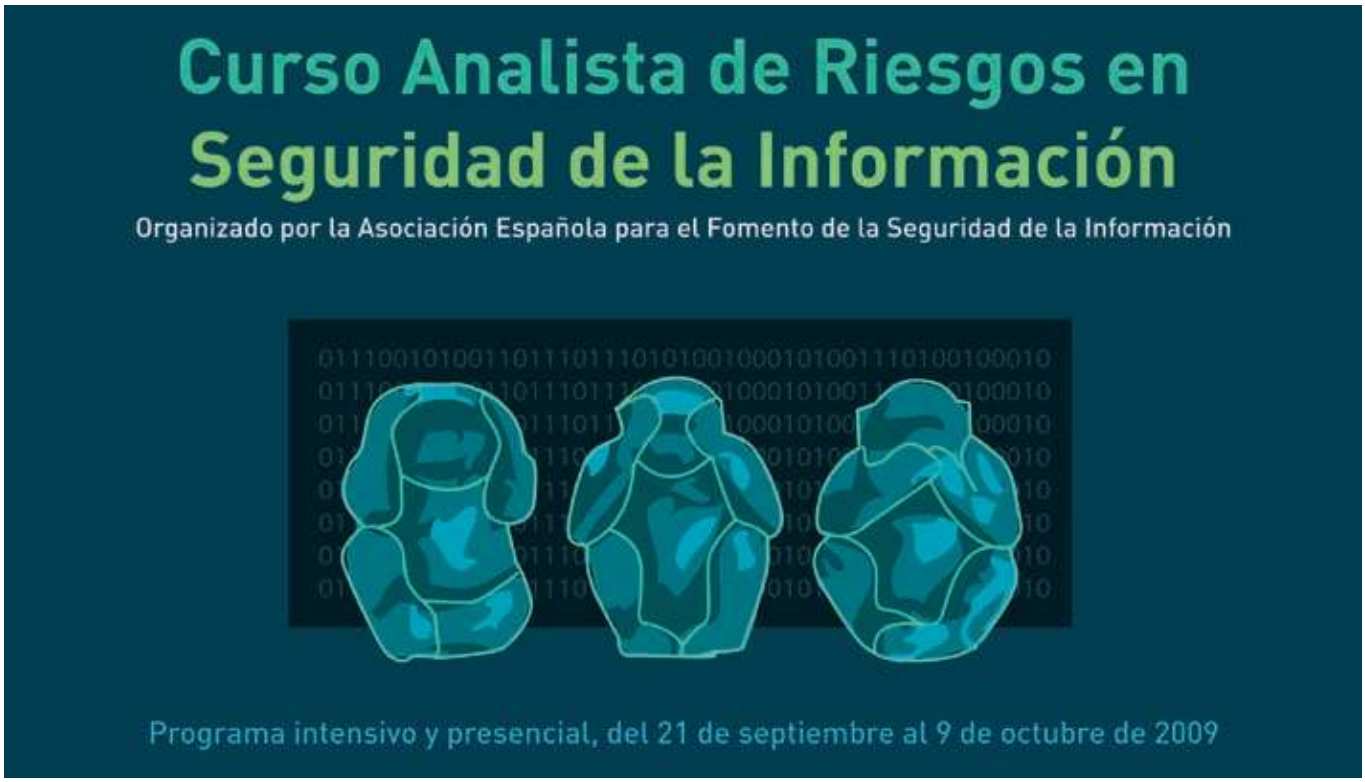
### Certified Data Privacy Professional

El Data Privacy Institute anunció el pasado mes de octubre la puesta en marcha de una **certificación específicamente dirigida al área de la Privacidad que será pionera en España**, denominada **CDPP (Certified Data Privacy Professional**).

Un comité de expertos ha trabajado en el programa, que se concreta en siete ámbitos o dominios que abarcará la Certificación para lograr una preparación completa de los profesionales en la materia.

La certificación CDPP se podrá obtener por dos vías: aquellos profesionales que acrediten tener sólidos conocimientos y experiencia podrán obtenerla, sin necesidad de presentarse al examen correspondiente, en virtud al programa de Grandfathering o superando una **prueba teórica** y acreditando además una **experiencia profesional** de al menos **3 años** en el ámbito de la Privacidad y la Protección de datos de carácter personal. El examen tendrá una validez de **3 años**, por lo que el candidato contará con este plazo para acreditar la experiencia requerida.

# Actividades 2009, otras sesiones formativas




Ayudar a los profesionales de la Seguridad de la Información a mejorar su preparación y actualizar sus conocimientos es una de las metas de ISMS Forum Spain. Y es una tarea prioritaria en el campo del Análisis de Riesgos, cuyos retos y soluciones están en constante cambio y evolución. Se trata de un área de trabajo compleja: era necesario crear un curso intensivo, especializado, con un enfoque práctico e interactivo que cubra 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, han diseñado el programa y buscado a los profesionales más adecuados para cada sesión. El resultado es el curso que aquí presentamos: durante diez días, y bajo una óptica basada en la experiencia del día a día empresarial, un profesorado con amplia experiencia aportará todas las claves para convertirse en un cualificado especialista en Análisis de Riesgos para la Seguridad de la Información, avalado por ISMS Forum Spain

## Objetivos:

•Adquirir los conocimientos teóricos y prácticos necesarios para el análisis y control de riesgos para la Seguridad de la Información en cualquier tipo de organización.

•Profundizar en las normas, herramientas, marcos y metodologías existentes.

•Conocer las tendencias y posible evolución de este campo profesional; identificar los retos y amenazas a afrontar en los próximos años y aprender del análisis casos prácticos y de la experiencia de especialistas que llevan años -en muchos casos décadas- ejerciendo responsabilidades en este ámbito.

Participa en este curso único y pionero en el ámbito de la Seguridad de la Información

Dirigido a: Auditores de Sistemas, Responsables de Seguridad, Responsables de Riesgos y profesionales que deseen adquirir conocimientos reales basados en la teoría y experiencia práctica en la Gestión y Análisis de Riesgos.

## Evaluación del Curso ARSI

La primera edición del Curso se organizo ,siguiendo el patrón de la Asociación para fomentar el contacto entre profesional de la seguridad de la información, de forma que quede un tiempo para que los participantes se relacionen y conozcan entre sí y puedan además acceder y comentar con los profesores sus inquietudes. Se contó con la presencia de 20 participantes de diferentes empresas relacionadas con la seguridad de la información que han evaluado, a través de un cuestionario de calidad, el curso dando como resultado, **una puntuación media de cuatro sobre cinco puntos** en lo que se refiere a organización, contenidos, profesores, etc.


Organizado conjuntamente por:

INFOWATCH

ISMS Forum Spain

# Seminario intensivo DLP: "Los últimos avances en Data Leak Prevention"

El 16 de abril ISMS Forum organizó, junto con Infowatch un Seminario Intensivo sobre Data Leak Prevention (DLP). Tanto los riesgos de fuga de datos sensibles como las opciones para combatirlos evolucionan y se multiplican a ritmo de vértigo. Este asunto está afectando gravemente a compañías de todo el mundo haciendo que DLP sea un tema prioritario en la agenda del responsable de seguridad de la información.

Por ello ISMS Forum Spain organizó este seminario que contó con un ponente de lujo, experto europeo en DLP, como es **Thomas Raschke**, y con otras valiosas exposiciones de **Rustem Khayretdinov** y **Vadim Sychev** de Infowatch. Siempre desde una óptica internacional, expusieron sus conocimientos, ejemplo útiles y de buenas prácticas. La sesión fue dinámica e interactiva y finalizó tras un animado debate entre los tres ponentes y Gianluca D´Antonio, con un almuerzo que a su vez fue una buena oportunidad para reflexionar e intercambiar experiencias.

Este seminario estuvo dirigido a CISOS y otros puestos de alta responsabilidad en Seguridad de la Información y contó entre el público con expertos internacionales y españoles de primer nivel.

# Actividades 2009,
# Convenios de colaboración

*Gianluca D'Antonio y Nils Puhlmann.*

## Con CSA

En octubre del pasado año, ISMS firmó un acuerdo de colaboración con Cloud Security Alliance en aras de fortalecer las relaciones que se han venido manteniendo entre ambas instituciones. Así, **Nils Puhlmann**, cofundador de CSA y CSO de Zynga ha participado en las dos jornadas internacionales de ISMS Forum de 2009. Además, en la jornada de noviembre se presentó oficialmente la versión española de la "*Guía para la Seguridad en áreas críticas de atención en Cloud Computing*". Este documento fue traducido por ISMS Forum y todos los asistentes a la VI Jornada Internacional recibieron un ejemplar gratis.

El acuerdo de colaboración establece las bases para participar en eventos e informes y de trabajar conjuntamente para mejorar la seguridad en cloud computing.

Cloud Security Alliance es una organización sin ánimo de lucro cuya misión es promover el uso de las mejores prácticas de seguridad dentro del cloud computing y brindar educación sobre los posibles usos de *Cloud Computing*. Esta Organización es liderada por profesionales de la industria y apoyada por más de 25 miembros corporativos. Entre sus miembros corporativos están la gran mayoría de multinacionales del sector.

## Con ETICOM

El 1 de septiembre de 2009 ISMS Forum Spain firmó un acuerdo de colaboración con ETICOM, La Asociación de Empresarios de Tecnologías de la Información y Comunicaciones de Andalucía, que es la patronal andaluza del sector de Tecnologías de la Información y Comunicaciones.

Este acuerdo busca acentuar las relaciones ante ambas instituciones y fomentar el intercambio de experiencias entre los distintos profesionales que las componen.

Eticom está creada por y para empresarios andaluces del sector. No tiene ánimo de lucro, su ámbito es regional y tiene como finalidad básica la defensa de los intereses del sector andaluz de las TICs.

En este sentido ETICOM es el representante natural del sector empresarial TIC ante la Administración Pública, ya sea comunitaria, nacional o regional, en el ámbito territorial de Andalucía.

# Actividades 2009, colaboración con otras organizaciones

## II Foro de Negocios Business TIC '09

**Dónde:** Centro Sevilla Congresos.

**Cuándo:** 25 y 26 de marzo de 2009.

**Organizado por:** ETICOM (Asociación de Empresarios de Tecnologías de Información y Comunicación de Andalucía).

Business TIC fue un evento B2B hecho por y para el propio sector, orientado a rentabilizar las áreas estratégicas generadoras de recursos económicos para las empresas TIC participantes. Se basó en un novedoso formato, alejado del clásico modelo ferial, e incluyo seis grandes áreas de trabajo: Ronda de negocios; Mercado del outsourcing; Área de I+D+i; Cluster TIC; Área Internacional y Meeting Point Partners. El evento incluyó una conferencia plenaria, desayunos y almuerzos de trabajo, sesiones monográficas, talleres y presentaciones, ponencias magistrales y una cena de gala.

## Seg2, I Encuentro de Seguridad Integral

**Dónde:** Hotel Eurobuilding, Madrid.

**Cuándo:** 25 y 26 de marzo de 2009.

**Organizado por:** Las publicaciones Red Seguridad y Securitecnia.

Las revistas de editorial Borrmart especializadas en seguridad lógica y seguridad física se unieron en la organización de este congreso, que trató en profundidad, precisamente, una de las tendencias que el sector de la Seguridad está constatando: la convergencia de ambos aspectos, que a menudo conforman las dos caras de una misma moneda, en la denominada seguridad integral. Contó con intervenciones de algunos de los máximos expertos del sector. **ISMS Forum Spain** fue una de las entidades colaboradoras.

## Forrester Security Forum EMEA 2009

**Dónde:** Millennium Gloucester Hotel, Londres.

**Cuándo:** 2 y 3 de abril de 2009.

**Organizado por:** Forrester Research.

Un año más, **ISMS Forum Spain** colaboró con el evento Security Forum que anualmente organiza Forrester en Europa. En esta ocasión la cita fue en Londres, y el tema de absoluta actualidad: se analizó la gestión del riesgo y de la seguridad en un contexto de incertidumbre mundial como es el actual. El forum se centró en algunos de los temas que más preocupan a los responsables de seguridad: Las arquitecturas de la seguridad del futuro, Gestionar un programa de seguridad orientado al negocio. Lograr unas políticas de cumplimiento normativo adecuadas y continuadas. Cómo acercarse al gobierno de la seguridad, Riesgo y cumplimiento de una forma sólidamente estructurada. Los socios de **ISMS Forum Spain** se beneficiaron de un descuento del 20% en la inscripción.

## Encuentros Tecnológicos E-Tic

**Dónde:** 22 de abril (Sevilla), 23 de abril (Málaga).

**Cuándo:** 22 y 23 de abril de 2009.

**Organizado por:** AVANTE Formación y Cibersur.

La definición de una política de seguridad empresarial debe considerarse como uno de los grandes valores a la hora de preservar los activos de la organización. A lo largo de la jornada los asistentes conocieron la importancia del análisis de riesgos, que permite identificar la vulnerabilidad de los sistemas y desarrollar estrategias orientadas a la protección de los mismos. Antonio Ramos, miembro de la Junta Directiva de **ISMS Forum Spain**, participó con una conferencia sobre la situación de la Seguridad en la empresa española y los principales retos que debe afrontar el sector. También hubo ponencias a cargo de expertos de Aidcon Consulting, BSI, Microsoft y Siemens. La asistencia fue gratuita.

**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.**

## Diálogo CxO: Gestión de Riesgos en TIC

**Dónde:** Madrid.

**Cuándo:** 16 y 17 de junio de 2009.

**Organizado por:** Econique Iberia.

Los responsables de seguridad y gestión de riesgos de las principales corporaciones españolas públicas y privadas se reunieron en la fechas antedichas en Madrid para participar en este encuentro organizado por Econique Iberia que congregó a la élite del sector y que contó con un panel de ponentes del más alto nivel, en el que se incluyeron expertos de Telefónica, Grupo Prisa, Grupo FCC, Grupo Iberdrola, la CNMV, Grupo Gas Natural, Caja Madrid, Sanitas, el Cuerpo Nacional de Policía, Bankinter, ONO y la Comunidad de Madrid. **ISMS Forum Spain** colaboró en este evento.

## Máster en Dirección y Gestión de Seguridad de la Información

**Dónde:** Escuela Técnica Superior de Ingenieros de Telecomunicaciones (ETSIT), Universidad Politécnica de Madrid.

**Cuándo:** Octubre 2009 a junio 2010.

**Organizado por:** ASIMELEC, UPM y FUNCOAS.

**ISMS Forum Spain** colaboró 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. Este Master cuenta con un programa detallado y un gran claustro docente, así como con algunos de los máximos expertos en la materia de nuestro país.

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

**Dónde:** Universidad Autónoma de Madrid.

**Cuándo:** Octubre 2009-Julio 2010.

**Organizado por:** Institute of Audit & IT-Governance y Universidad Autónoma de Madrid.

**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. El objetivo es 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.

## Expertos de USA, México, Cuba y España en el DISI 2009

**Dónde:** Campus Sur de la UPM, Madrid.

**Cuándo:** 30 de Noviembre 2009.

**Organizado por:** Cátedra UPM Applus+ de Seguridad y Desarrollo de la Sociedad de la Información.

La Cátedra UPM Applus+ de Seguridad y Desarrollo organizo la 4ª Edición del Día Internacional de la Seguridad de la Información, DISI 2009, que contó este año con la destacada presencia de Hugo Krawczyk de IBM Research (Estados Unidos), reconocido investigador que presentará la conferencia "Randomized Hashing: Secure Digital Signatures without Collision Resistance".

Desde su primera edición **ISMS Forum Spain** ha colaborado con esta interesante convocatoria anual de la cátedra de Seguridad de la Información de la Universidad Politécnica de Madrid.

# Publicaciones

## CSA e ISMS Forum Spain presentan la Guía para la Seguridad en áreas críticas en Cloud Computing

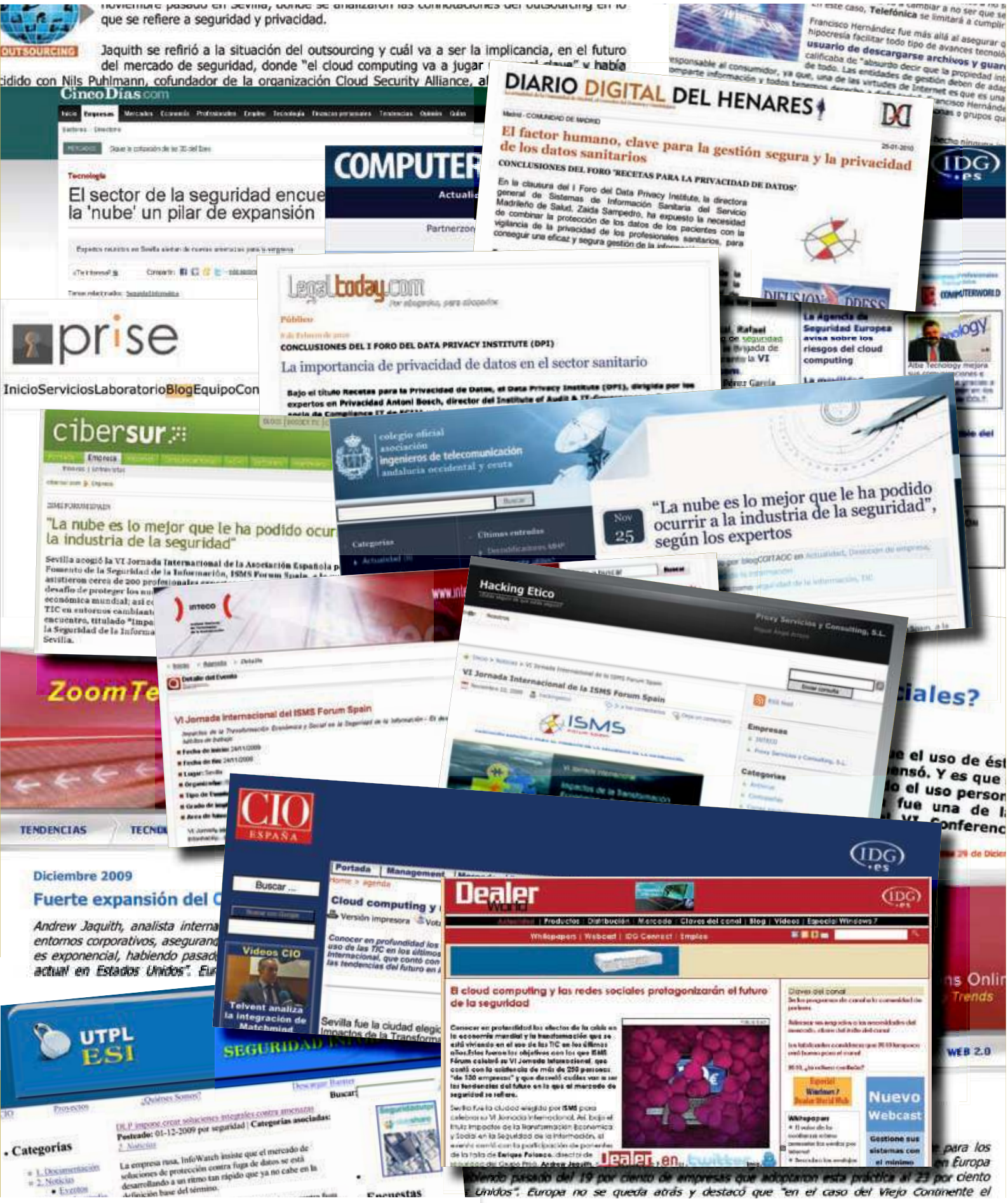

ISMS Forum ha presentado en la VI Jornada Internacional la Guía para la Seguridad en áreas críticas de atención en Cloud Computing, elaborada por los expertos de Cloud Security Alliance, CSA. Éste Resumen Ejecutivo es la primera entrega de una serie completa sobre seguridad en Cloud Computing que iremos poniendo a disposición de nuestros socios en los próximos meses.

Fué motivo de gran satisfacción para ISMS Forum Spain poder presentar en lengua española este amplio Resumen Ejecutivo de la Guía para la Seguridad en áreas críticas de atención en Cloud Computing de Cloud Security Alliance (CSA). En la línea ya iniciada con otras publicaciones, la Asociación tiene como objetivo acercar a los profesionales de la seguridad de la información herramientas de trabajo útiles y accesibles, sin ninguna barrera idiomática que dificulte su comprensión. Quisieramos agradecer, en nombre de todos los asociados de ISMS Forum Spain, a CSA (Cloud Security Alliance), a su director Jim Reavis y a su cofundador Nils Puhlmann, por habernos autorizado cortésmente a traducir y editar en castellano esta Obra.

Es para nosotros un reconocimiento más, a la labor de divulgación y fomento del conocimiento de las herramientas y Sistemas de Gestión de la Seguridad de la Información que nuestra Asociación está llevando a cabo. Seguimos, pues, consolidando la labor informativa que ISMS Forum Spain viene desarrollando desde su fundación en favor de todos sus asociados.

Este documento es el preludio de la segunda versión de esta Guía. La primera data de abril de 2009, y el volumen de contenidos de la misma se triplicará en la segunda edición, tal es la rápida evolución de la materia que nos ocupa, y que gana terreno por momentos a otras formas de trabajo que están quedando obsoletas frente a ella. Preparada por un amplio conjunto de expertos de CSA, la guía completa está aún en fase de corrección y edición final. Así, los distintos dominios que contiene el presente resumen ejecutivo –desarrollados en profundidad- se irán publicando a lo largo de los próximos meses hasta completar un manual que tendrá más de 350 páginas. Sin embargo, esto no es un mero aperitivo, sino una herramienta de trabajo verdaderamente útil: contiene perfectamente sintetizadas las claves a tener en cuenta para comprender los principios y procesos que rigen el Cloud Computing, los modelos a los que podemos adherirnos, y sobre todo, las áreas críticas que debemos tener en cuenta y las medidas que deberíamos tomar los responsables de seguridad de la información para que nuestras organizaciones puedan trabajar "en la nube" con la máxima confianza y con los mínimos riesgos posibles.

# ISMS en los medios



# Empresas asociadas

En diciembre de 2009, cerca de cien empresas y organizaciones de los más diversos sectores se han asociado, y más de 650 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
- Agaex Informática
- Agbar Servicios Compartidos
- Aidcon Consulting
- Applus+, Lgai Technological Center
- Ascêndia Reingeniería + Consultoría
- Asistencia Sanitaria Interprovincial, ASISA
- AEDCI Asociacion Española Destruccion Confidencial de Informacion
- Atos Origin
- 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
- Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya – CTTI
- Compañía Española De Petróleos, CEPSA
- Check Point
- Comparex España
- Consejo General de Colegios Oficiales de Médicos – CGCOM
- CPR Tecnologías de la Información
- Deloitte
- Destrucción Confidencial de Documentación DCD
- Destrudat
- Dintel
- EPDASA
- Ecija
- Endesa
- Ernst & Young
- Esa Security
- Eulen Seguridad
- Everis Spain
- Ever Team
- Firma, Proyectos y Formación
- Fomento de Construcciones y Contratas FCC
- Future Space
- Gas Natural Informática
- Giga Trust
- GFI Informática
- GMV Soluciones Globales Internet
- Grupo Ferrovial
- Grupo Generali
- Grupo Intermark 96
- Grupo S21sec Gestión S21sec
- Hewlett-Packard Española, HP
- IDN
- Indra Sistemas
- Instituto Nacional de Tecnologías de la Comunicación, INTECO
- International Business Machines, IBM
- Internet Security Auditors, ISECAUDITORS
- Interxion España
- Juniper Networks
- Kabel Sistemas De Información
- Krell Security
- Kaspersky Lab
- Leaseplan Servicios
- Lloyd's Register Quality Assurance, LRQA
- McAfee
- Mutua Madrileña
- Mnemo
- Nextel
- Nexus IT
- Ocaso
- Open3s Open Source And Security Services
- ONO
- OMC Consejo General de Colegios Oficiales de Médico
- Passwordbank
- Panda Software Spain
- Pricewaterhousecoopers, PWC
- Promotora de Informaciones, Grupo PRISA
- Red Seguridad
- Repsol
- Revista a+)) auditoria y seguridad
- S2 Grupo
- Sage Logic
- SGS ICS Iberica
- Sistemas Informáticos Abiertos, Grupo SIA
- Sophos Iberia
- Steria Ibérica
- Symantec
- Tecnocom Telecomunicaciones y Energía
- Telefónica
- T-Systems ITC Iberia
- Universidad Complutense de Madrid, UCM
- ...