**Más de 150 personas asistieron a la ceremonia de entrega de los "Trofeos de la Seguridad TIC 2008" de RED SEGURIDAD**

# El secretario de Estado, Alberto Saiz, presidió la III edición de los premios

*A la izquierda, José Ramón Borredá, editor de RED SEGURIDAD, recibe a Alberto Saiz, secretario de Estado director del CNI, a su llegada a la celebración, junto con Alfonso Mur, presidente del Consejo Técnico Asesor de la revista (a la derecha).*

**SeMarket, el Centro Criptográfico Nacional (CCN) del Centro Nacional de Inteligencia (CNI), Lexmark, S21sec e Hispasec Sistemas fueron los triunfadores de unos galardones muy competidos. El acto también contó con la presencia de Enrique Martínez, director general del Instituto Nacional de Tecnologías de la Comunicación (INTECO), así como autoridades de la Comunidad de Madrid, la Agencia Española de Protección de Datos (AEPD), el CCN y la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM).**

Tx: Mercedes Oriol Vico.
Ft: Fermín Sánchez González.

EL PASADO 19 de noviembre, RED SEGURIDAD celebró, en el Hotel Meliá Castilla, la entrega de los "Trofeos de la Seguridad TIC", bajo la presidencia del secretario de Estado del Ministerio de Defensa y director del Centro Nacional de Inteligencia (CNI), Alberto Saiz. La tercera edición de estos premios se convirtió en todo un éxito, ya que al acto institucional asistieron más de 150 profesionales del sector, procedentes de empresas, organismos públicos y asociaciones. Otras autoridades que compartieron presidencia, junto con José Ramón Borredá, editor de la revista y presidente de Editorial Borrmart, y Alfonso Mur, presidente del Consejo Técnico Asesor (CTA) de RED SEGURIDAD, fueron: Enrique Martínez, director general del Instituto Nacional de Tecnologías de la Comunicación (INTECO); Fermín Montero, subdirector general de Innovación Tecnológica de la Comunidad de Madrid; Mª José Blanco, subdirectora general del Registro de Protección de Datos de la Agencia Española de Protección de Datos (AEPD); Emilio Aced, subdirector general de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM); Luis Jiménez, subdirector adjunto del Centro Criptológico Nacional (CCN); y Mercedes Pérez, directora del Gabinete del secretario de Estado.

### Premiados de la tercera edición

Los ganadores de esta tercera edición han sido: la firma SeMarket, por su producto de control de acceso biométrico "BioSeLogOn"; el Centro Criptográfico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI), por los servicios que ofrece desde su CERT; la empresa Lexmark, por los sistemas de seguridad implantados en sus dispositivos multifunción; la compañía S21sec, por sus planes de formación continua en tecnología de seguridad; e Hispasec Sistemas, por el fomento de la divulga-


*En la imagen, los premiados -flanqueados por Alfonso Mur y José Ramón Borredá-. De izquierda a derecha: Antonio Ropero, socio co-fundador de Hispasec Sistemas; Guillermo Morales, CEO de SeMarket; Luis Jiménez, subdirector adjunto del CCN; Alberto Saiz, secretario de Estado; Juan Carlos Rodríguez, director de Formación de S21Sec; y José Luis Domínguez, director de Marketing de Lexmark.*

ción de la seguridad informática y por su trayectoria empresarial. El jurado declaró desierto el "Trofeo a la Investigación en Seguridad".

## Progreso de la sociedad

"Si de algo tenemos que estar convencidos es de que la seguridad de las tecnologías de la información y las comunicaciones es tan importante para la seguridad y el bienestar de los ciudadanos como lo es la protección de los propios ciudadanos, sus intereses y el progreso de su modelo de sociedad". Con estas palabras, Alberto Saiz, secretario de Estado del Ministerio de Defensa y director del Centro Nacional de Inteligencia (CNI), describió la importancia que posee en la actualidad la protección de las comunicaciones electrónicas, en las que basamos la mayor parte de nuestro día a día.

Además, Saiz destacó que la garantía de esta seguridad, depende directamente de "una responsabilidad compartida que afecta a gobiernos, empreas y todo tipo de organizaciones y usuarios individuales", puesto que "el alcance de la seguridad de la información es tan amplio que atañe a cualquier agente que desarrolle, posea, provea, gestione o utilice sistemas de información y redes de comunicación en general".

Asimismo, el secretario de Estado puso de relieve la necesidad de "una cooperación entre todos los agentes implicados, incluidas las administraciones públicas": "De dicha cooperación, surgida en foros como este, saldrán soluciones innovadoras que nos permitirán hacer frente a los nuevos desafíos".

Por su parte, José Ramón Borredá, presidente de Editorial Borrmart y editor de RED SEGURIDAD, mostró su orgullo por el desarrollo de los premios de la revista que, en su opinión, "han consolidado su prestigio e importancia merced a la limpieza de los mismos y a la independencia e imparcialidad del Jurado a la hora de otorgarlos, según las bases del certamen".

José Ramón Borredá resaltó la importancia de conseguir el compromiso que se marcó la editorial, desde el primer número de la revista, "promover e impulsar la cultura de la seguridad de la información", al igual que "abogar por la seguridad integral". En este sentido, Borredá recordó a los asistentes, el evento que a finales de marzo celebrará Editorial Borrmart, con sus dos cabeceras, RED SEGURIDAD y SEGURITECNIA: el "I Encuentro de Seguridad Integral. Seg$^2$". Una puesta en común del sector de la Seguridad Privada y la Seguridad Lógica, imprescindible, porque, tal y como indicó el presidente de la editorial, "entendemos que ambas seguridades están condenadas a entenderse y deben formar un todo en aras de la prevención y de la seguridad integral que se pretende".

Un paso hacia dicho fin tan prometedor fue que, en esta tercera edición de los "Trofeos de la Seguridad TIC" de RED SEGURIDAD, estuvieron presentes los presidentes y gerentes de las asociaciones nacionales más importan-

*Enrique Martínez (a la izquierda), director de INTECO, junto con José Ramón Borredá y Alberto Saiz, disfrutaron de una distendida comida.*

tes de la Seguridad de la Información y de la Seguridad Privada, a quienes José Ramón Borredá agradeció muchísimo haber aceptado la invitación.

### Un trabajo bien hecho

Para Guillermo Morales, CEO de SeMarket, quien recogió el trofeo al mejor producto de seguridad, este premio "es una clara recompensa a una labor y un trabajo de fondo", que confirma la máxima que defiende este joven directivo: "El trabajo bien hecho siempre está recompensado".

José Luis Domínguez, director de Marketing de Lexmark, expresó su "satisfacción por recibir este premio de una cabecera tan prestigiosa como es RED SEGURIDAD" y añadió que "supone un aliciente de cara a la inversión que todo fabricante debe hacer en aras no solamente al lanzamiento de nuevos productos, sino también de soluciones dentro de las TIC y de la propia seguridad".

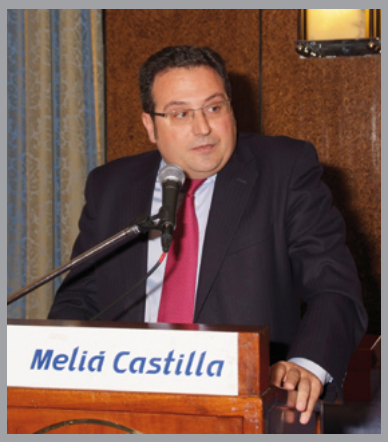
Por su parte, Juan Carlos Rodríguez, director de Formación de S21sec, felicitó la iniciativa de haber "incluido el premio a la Formación como algo a destacar dentro de la seguridad TIC -algo no muy habitual-", que para su compañía es "un pilar en la gestión de la seguridad" y que, en esta ocasión, "ha sido valorada".

Antonio Ropero, socio co-fundador de Hispasec Sistemas, manifestó su alegría diciendo: "Este reconocimiento, viniendo además de quien viene, solo nos puede animar a seguir en la misma línea y tratar de hacerlo cada vez mejor".


*De izquierda a derecha, Mercedes Pérez, Emilio Aced, Enrique Martínez, Alberto Saiz, Alfonso Mur, Fermín Montero, Luis Jiménez y Mª José Blanco, durante el discurso de José Ramón Borredá.*

El secretario de Estado, como portavoz del CCN-CNI, explicó: "Aunque somos conscientes de que queda mucho por hacer, y que los logros conseguidos necesitan consolidarse, este premio nos dará , sin duda, renovadas fuerzas para afrontar, junto con el resto de organismos de la Administración, los nuevos retos que tenemos ante nosotros".

Alberto Saiz finalizó agradeciendo a Editorial Borrmart la organización de "unos premios que tienen el valor de reconocer públicamente la labor de quienes, día a día, se afanan en mejorar los niveles de seguridad en un sector tan sensible y crítico como es el de las TIC". De ahí, que Alberto Saiz dejara patente su "agradecimiento y felicitación a la revista RED SEGURIDAD por animar a todos los presentes a progresar en este difícil campo", así como por "su encomiable labor y compromiso con la difusión de los conocimientos e innovaciones que se producen dentro del sector de la seguridad de las TIC". ■




## Discurso de Alfonso Mur, presidente del Consejo Técnico Asesor y del Jurado de los Trofeos de la Seguridad TIC de RED SEGURIDAD

"Hace ya más de tres años que me dejé embaucar por un señor, que es el presidente de Editorial Borrmart, don José Ramón Borredá, y para mí es un honor haber hecho una vez más de presidente del Consejo Técnico Asesor y de presidente de este jurado que va a otorgar los premios.

Me gustaría destacar, especialmente, el esfuerzo, dedicación y cariño con que el jurado que ha participado en la elección de estos premios, ha estado trabajando a lo largo de los últimos meses. También me gustaría destacar el criterio en la selección de los trofeos que vamos a entregar hoy, porque demuestra un alto conocimiento profesional del mercado y, sobre todo, agradecerles la dedicación que han tenido en la lectura, examen y evaluación de los distintos expedientes de las candidaturas.

Una prueba inequívoca de que estos trofeos se están consolidando en el mundo de la seguridad es, primero, que es su tercera edición (no es fácil llegar a tres ediciones), segundo, llegar a esta tercera edición con esta afluencia de personas y de profesionales del sector, y por supuesto, acompañados por esta mesa de autoridades que nos honra con su visita.

A los trofeos de este año 2008 hemos tenido la suerte de poder evaluar 25 candidaturas, es decir, ha habido 25 optantes a los cinco premios. Desafortunadamente se nos ha quedado desierta una candidatura este año, que al jurado nos sorprende sobremanera que se haya quedado desierta, que es la candidatura a la innovación en materia de seguridad. Los que nos dedicamos a vender seguridad sabemos que con las "duras" que vienen en el mercado y como está la economía, hay que aguzar el ingenio, hay que innovar, hay que ser innovadores a la hora de presentar productos, para que nos permita estar posicionados en el mercado. Y nos ha sorpendido sobremanera que haya quedado desierta esta candidatura.

Como va a seguir lloviendo, y va a llover mucho, a lo largo de los próximos años, vamos a tener que remar mucho, incluido en el mundo de la seguridad, estamos convencidos que en la cuarta edición de los "Trofeos de la seguridad TIC" de RED SEGURIDAD, que desde ya queda abierta, tendremos un montón de candidaturas relacionadas con la innovación de la seguridad.

Por último, quería destacar que el CTA de la revista y los miembros del jurado hemos decidido hacer algunos pequeños cambios en el formato de las candidaturas, para hacerlos un poco más atractivos y más simples en el momento de su presentación, que en breve veremos publicados en la revista para que todos os animéis y presentéis candidaturas a la edición 2009.

Gracias a todos por acompañarnos hoy, enhorabuena anticipada a los premiados.

# Distinguidos de la convocatoria 2008

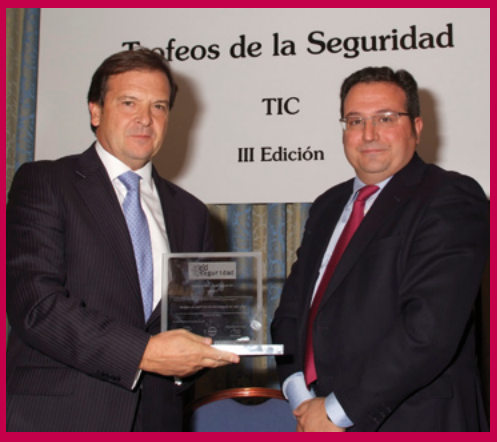
Acompañada de un respetuoso silencio por parte de los asistentes al acto institucional, Mª Victoria Gómez, directora de Relaciones Institucionales de Editorial Borrmart, pronunció unas palabras ya tradicionales en este sector: "Reunido el pleno del Consejo Técnico Asesor de la revista RED SEGURIDAD, en su calidad de jurado del certamen y bajo la presidencia de don Alfonso Mur Bohigas, una vez estudiadas y analizadas las candidaturas presentadas a las distintas categorías, ha otorgado los siguientes Trofeos de la Seguridad TIC en esta tercera edición".

## "Trofeo al Producto de Seguridad TIC 2008" — SEMARKET

A la empresa SeMarket, por su producto "BioSeLogOn", una solución de control de acceso biométrico, que reemplaza al actual proceso que requiere de un *login* y una contraseña, por un sistema biométrico basado en el reconocimiento biométrico multimodal al que se añade un sistema de identificación adicional mediante tarjeta criptográfica. Utiliza el reconocimiento de la identidad a través de voz, cara y huellas dactilares, con el objetivo de autorizar el acceso a un determinado usuario, si este ha sido dado de alta previamente, teniendo como principales ventajas poseer un nivel máximo de seguridad, comodidad y facilidad de uso.

Recibió el trofeo Guillermo Morales, CEO de SeMarket, de manos de Fermín Montero, subdirector general de Innovación Tecnológica de la Comunidad de Madrid.

## "Trofeo al Servicio de Seguridad TIC de 2008" — CCN-CERT




Al Centro Criptológico Nacional (CCN), por el servicio que ofrece el Equipo de Respuesta a incidentes de Seguridad de la Información (CERT) a la Administración Pública, cuyo principal objetivo es el de contribuir a la mejora del nivel de seguridad en los sistemas de información de las administraciones públicas españolas, y afrontar, de forma activa, las nuevas amenazas a las que hoy en día están expuestas. Funciona como un centro de alerta nacional que coopera y ayuda a las administraciones a responder de una forma rápida y eficiente ante los incidentes de seguridad que puedan surgir.

Alberto Saiz, secretario de Estado del Ministerio de Defensa y director del CNI, recogió el premio que le entregó Alfonso Mur, presidente del Consejo Técnico Asesor (CTA) y del jurado de los trofeos.

# III EDICIÓN PREMIADOS III EDICIÓN PREMIADOS III EDICIÓN

## "Trofeo al Sistema de Seguridad TIC más innovador de 2008" LEXMARK

A Lexmark, por su sistema de seguridad en dispositivos multifunción. Complejos dispositivos que basan su seguridad en la protección del producto multifunción, la red y los datos involucrados en el uso. Los productos de dicha empresa están equipados con numerosas funciones de seguridad que permiten garantizar la protección del equipo y de la información que se procesa en ellos, tanto a través de red como de su uso.

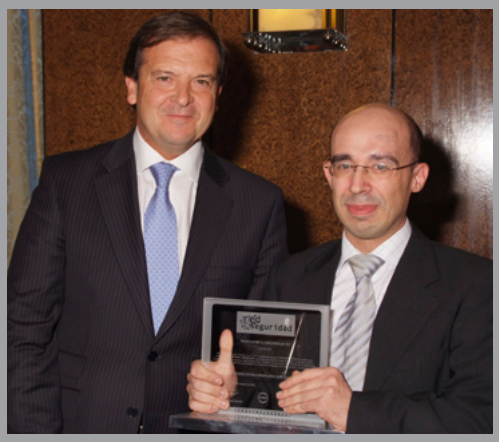
Recogió el trofeo José Luis Domínguez, director de Marketing de Lexmark, de manos de Enrique Martínez, director general del Instituto Nacional de Tecnologías de la Comunicación (INTECO).

## "Trofeo a la Formación y Capacitación de 2008" S21SEC

A la empresa S21SEC, por la formación continua en tecnología de seguridad que ofrecen, creando una cultura de seguridad digital en la totalidad de los usuarios de sistemas, utilizando para ello diferentes metodologías: jornadas breves de divulgación y concienciación, distribución de mensajes y recomendaciones diarias a través de pequeños módulos didácticos, llamados "bites de formación", etcétera.

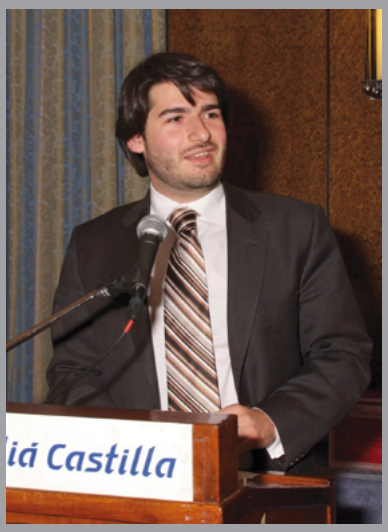
Juan Carlos Rodríguez, director de Formación de S21sec, recogió el trofeo que le entregó Luis Jiménez, subdirector adjunto del Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI).

## "Trofeo Extraordinario del Jurado 2008" HISPASEC SISTEMAS



A Hispasec Sistemas, que desde hace diez años viene prestando un servicio público y gratuito para la comunidad, con el propósito de divulgar y concienciar a los usuarios de la importancia que tiene la seguridad en el campo de las nuevas tecnologías de la información. En un año que coincide con el aniversario de "una-al-día", su boletín de noticias diario, especializado en informaciones de seguridad, que fue el origen del nacimiento de esta empresa española.

Recogió el trofeo Antonio Ropero, socio y co-fundador de Hispasec Sistemas, de manos de Alberto Saiz, secretario de Estado.




# "Este premio representa el esfuerzo y la apuesta en I+D+i realizada por SeMarket, en los últimos años"

Guillermo Morales
CEO de SeMarket

**¿Qué ha supuesto ganar el premio al mejor producto de seguridad TIC del año, con su solución "BioSeLogOn"?**
La entrega de este premio tan significativo para SeMarket, es una clara recompensa tras la incansable labor de toda la compañía por buscar soluciones de seguridad que ayuden al mundo actual a ser más seguro. Este premio representa el esfuerzo y la apuesta en I+D+i realizada por SeMarket, en los últimos años, y refleja nuestro objetivo de ofrecer al mercado las mejores soluciones de biometría y seguridad.

**¿Nos podría describir brevemente esta solución?**
La solución premiada es un sistema de control de acceso lógico que reemplaza al actual proceso, que requiere de un usuario y una contraseña, por un sistema basado en el reconocimiento biométrico (voz, cara y huella dactilar), al que se añade un sistema de identificación adicional mediante tarjeta criptográfica. Una solución de máxima seguridad y modular que garantiza el acceso seguro a equipos informáticos en dominio o bien a estaciones de trabajo aisladas.

**¿Qué aporta "BioSeLogOn" de novedoso e innovador al sector respecto a otros sistemas similares del mercado?**
La principal novedad es el uso simultáneo de diferentes biometrías (voz, cara y huella), lo que aumenta exponencialmente la seguridad del sistema. Con "BioSeLogOn" se alcanza el nivel de seguridad más alto al combinar los siguientes tres factores:

+ Algo que tienes: la tarjeta inteligente.
+ Algo que sabes: la clave personal.
+ Algo que eres: la verificación de las distintas biometrías de voz, cara y huella.

**¿De qué manera presentaría su empresa a alguien que aún no les conoce?**
SeMarket es una empresa española, especializada en asegurar la identidad de las personas y organizaciones, mediante biometría y certificación digital.

Con más de diez años de experiencia acumulada, SeMarket fue la primera empresa de I+D+i en biometría en España, y continua invirtiendo constantemente en esta área con el objetivo de ofrecer las mejores soluciones al mercado.

**Su equipo está formado por jóvenes profesionales, pero respaldada por grandes expertos en seguridad de la información y las TIC, como Manel Medina. ¿Es esta la clave del éxito de su tecnología?**
En SeMarket trabajamos con un equipo de profesionales expertos que cuenta con más de 20 años de experiencia en PKI y biometría. Al mismo tiempo, nuestro deseo constante de ver las cosas desde distintas perspectivas, nos lleva a apostar fuerte por un equipo joven que aporta frescura, dinamismo y nuevas visiones. Las personas son, sin temor a equivocarme, el activo más importante de la compañía.

**Sus soluciones, sistemas y productos se basan en la biometría y en la identificación por firma electrónica. En todos los casos, ustedes se mueven entre la seguridad física y la lógica: ¿cuál es su concepto de la seguridad integral?**
Sin duda, la seguridad física y lógica convergen. Cada vez nos encontramos con más organizaciones en las que ambas seguridades se unifican bajo una única Dirección Corporativa, que integra todas las disciplinas relacionadas con la Seguridad.

Cada día, cualquier empleado realiza multitud de procesos de identificación y autenticación: abrir una puerta, acceder al ordenador, entrar en una aplicación, fichar en el trabajo, etc. Todos estos actos están relacionados y deben de estar centralizados en un único punto; es aquí cuando unificamos la seguridad física y lógica en lo que llamamos Seguridad Integral.

**Desde la filosofía que predican con sus productos para asegurar identidades, ¿cómo creen que se puede mejorar la confianza en Internet y en las comunicaciones móviles?**
La autenticación de las personas y usuarios es fundamental para garantizar la confianza, nuestras soluciones hacen posible que las empresas creen sistemas fiables y seguros para el comercio electrónico, Internet y el comercio a través de teléfonos móviles. ■

# "Intentamos dar solución a los problemas de las empresas para asegurar la confidencialidad de su información"

José Luis Domínguez
Director de Marketing de Lexmark

**¿Qué ha supuesto ganar el premio al sistema de seguridad TIC más innovador?**
El hecho de que nuestras soluciones de seguridad para dispositivos multifunción hayan sido reconocidas como el sistema de seguridad más innovador del año por una publicación tan prestigiosa como RED SEGURIDAD, nos llena de orgullo y de satisfacción. Además, nos demuestra que estamos siguiendo el camino correcto a la hora de proporcionar a nuestros clientes soluciones que se adapten realmente a sus necesidades.

**¿Qué es para ustedes la seguridad de la información?**
La seguridad de la información es fundamental para cualquier empresa. En Lexmark intentamos dar una solución a los problemas con los que las empresas se pueden enfrentar a la hora de asegurar la confidencialidad de su información, y hemos diseñado herramientas que ayudan a proteger esta información. Es muy importante implantar políticas de seguridad para las impresoras, al igual que se hace con los ordenadores o con cualquier otro dispositivo informático. La necesidad de contar con un acceso a red controlado y la necesidad de una gestión remota segura son las mismas para impresoras que para estaciones de trabajo en empresas que quieran proteger la información clave para sus clientes y empleados.

**¿Nos puede describir, lo más detallado posible, los sistemas de seguridad que han integrado en sus dispositivos?**
Los productos multifunción y de conexión a red de Lexmark incluyen un amplio abanico de características relacionadas con la seguridad.

Los productos multifunción en red funcionan de manera independiente y pueden ser puntos focales de información confidencial. Asegurarlas puede compararse, a veces, con asegurar otros dispositivos de red convencionales, como los ordenadores. La necesidad de un acceso controlado a la red y la necesidad de una administración remota segura son, en lo fundamental, iguales para productos multifunción que para estaciones de trabajo. En otras áreas, las consideraciones de seguridad de los productos multifunción son muy diferentes. Los productos multifunción generalmente no ejecutan sistemas operativos convencionales, el concepto de autenticación del usuario se aplica de una manera diferente, no tienen recursos compartidos de archivos en red que haya que proteger y probablemente no necesitan o admiten *software* antivirus.

Para administrar de forma práctica un conjunto de productos multifunción conectados a una red, es imprescindible la administración remota y ésta debe ser segura. El dispositivo debe permitir que las personas con autorización lo puedan configurar y las que no tengan autorización, sean rechazadas. Además, el proceso de administración del dispositivo debe ser seguro, de forma que el tráfico de red asociado a la administración remota no pueda ser interceptado, robado o usado para fines nocivos.

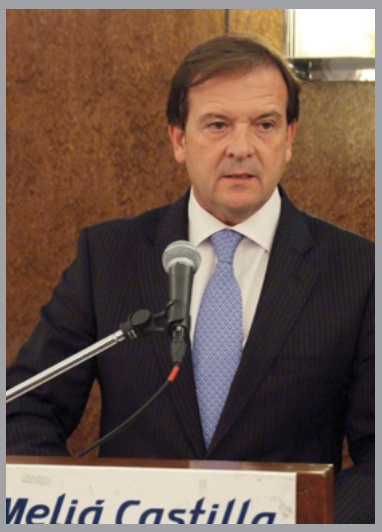
**¿Desde cuándo Lexmark toma conciencia de la importancia de la seguridad en las tecnologías que desarrolla?**
Desde el primer momento, Lexmark ha visto la necesidad de implantar seguridad en sus productos. Desde el momento en que las compañías se puedan ver perjudicadas por algo tan simple como olvidar información confidencial en la impresora.

Olvidar documentos confidenciales en las bandejas de las impresoras puede suponer, en muchos casos, un riesgo para los empleados de toda empresa, y lo que es más importante, puede acarrear pérdidas económicas para la misma. Es ahí cuando Lexmark ve la necesidad de crear soluciones para evitar el problema, y desarrolla soluciones que ayudan a proteger los documentos confidenciales mediante sencillos procedimientos que se diseñan desde el momento en el que se crean los primeros conceptos del dispositivo.

**Como grandes conocedores del mundo de la impresión física, ¿cuál ha sido la evolución que han experimentado respecto a la protección de la información con los sistemas electrónicos, Internet, las comunicaciones móviles, etc.?**
La seguridad de la información se empieza a considerar como un elemento importante para todas las compañías y usuarios de las comunicaciones. Hoy en día, hay mayor responsabilidad y más programas que ofrecen mayor seguridad tanto en los sistemas como en Internet. Cada vez hay más soluciones que protegen los datos de los usuarios y la información que se comparte día a día. Lexmark, a través de los años, ha visto un incremento en la necesidad de protección de datos, y es por esta razón por la que cada vez se preocupa más por la seguridad de los datos de sus clientes, por lo que diseña dispositivos que incluyen seguridad y herramientas que permitan una impresión segura.

La Web 2.0 ha facilitado increíbles posibilidades de compartir información y de estar en contacto con todo el mundo. Sin embargo, esta tendencia posibilita que esa información pueda ser utilizada con fines no lícitos, por lo que también se deben mejorar las medidas de seguridad de Internet.

**¿Qué otras claves consideran imprescindibles para proteger la información confidencial de las organizaciones?**
Sin duda, es necesaria cierta concienciación. De poco sirven las medidas de seguridad si nos seguimos dejando documentos confidenciales en las bandejas de impresión, o si no tenemos cuidado a la hora de facilitar nuestros datos bancarios en ciertos sitios de Internet. Obviamente, el sentido común siempre es necesario. ■



# "A día de hoy, más de 1.300 responsables de seguridad de toda la Administración están registrados en el CCN-CERT"

Alberto Saiz
Secretario de Estado y director del CNI

**¿Qué supone para ustedes ganar el premio al servicio de seguridad TIC, por el Equipo de Respuesta ante Incidentes de Seguridad de la Información (CERT) del Centro Criptológico Nacional (CCN)?**
Para nosotros es un reconocimiento a la labor emprendida hace ya más de tres años, cuando se empezó a fraguar la Capacidad de Respuesta ante incidentes de Seguridad de la Información (CCN-CERT). Entonces, y gracias al conocimiento adquirido sobre amenazas, vulnerabilidades y riesgos de los sistemas de información y comunicaciones durante toda su historia por el Centro Nacional de Inteligencia (CNI), y a través del Centro Criptológico Nacional (CCN), se decidió crear un nuevo servicio con el que contribuir, de forma activa, a la mejora del nivel de seguridad en los sistemas de información de las administraciones públicas españolas (general, autonómica y local).

Este premio, junto con la buena acogida que ha tenido entre los responsables de seguridad de toda la Administración, nos confirma que estamos en el camino adecuado y nos da nuevas fuerzas para afrontar, junto con el resto de organismos, los nuevos retos que tenemos ante nosotros.

**¿Cuántos organismos están utilizando ya este servicio y se están beneficiando del CCN-CERT?**
En realidad, podríamos decir que todas las administraciones públicas españolas y sus distintos organismos están utilizando, de una u otra manera, alguno de nuestros servicios e, incluso, y de forma colateral, todos los ciudadanos que acceden a nuestro portal (www.ccn-cert.cni.es). De hecho, mensualmente recibimos una media de 50.000 visitantes únicos que pueden acceder a una parte importante de la información publicada por el CCN-CERT, cuya principal función es reducir los riesgos de seguridad de cualquier sistema.

No obstante, y centrándonos en nuestra "comunidad" (en el ámbito de los CERT, se entiende por tal los miembros del grupo a los que se presta el servicio), a día de hoy, son más de 1.300 los responsables de seguridad de toda la Administración los que están registrados en la parte privada del portal, que no olvidemos que es nuestra principal herramienta y punto de contacto con todos ellos. A través de este registro reciben todo tipo de información de primera mano, no sólo sobre el modo de abordar cualquier incidente, sino también -y sobre todo- sobre cómo evitarlo a través de guías, herramientas y alertas de vulnerabilidades actualizadas diariamente. De este número, aproximadamente el 65 por ciento pertenece a la Administración General del Estado (AGE); el 23 por ciento, a la autonómica; el 18 por ciento, a la local; un tres por ciento a universidades; y un uno por ciento, a organizaciones internacionales con las que mantenemos una estrecha colaboración.

En cuanto a la gestión de incidentes, y dada la política del CCN-CERT de mantener la confidencialidad sobre cualquier información de la Administración solicitante de ayuda, no podemos ofrecer datos concretos, pero sí señalar que han sido numerosos los organismos que han recurrido a nuestro equipo para afrontar algún incidente en estos dos últimos años (particularmente de fraude, código malicioso, intentos de intrusión o ataques DoS y DDoS).

Otro de nuestros servicios más solicitado es la formación. El CCN ha ofertado desde el año 2006 cursos a más de 1.200 funcionarios, procedentes de 110 organismos diferentes y repartidos en los 18 cursos y 1.300 horas lectivas que lleva a cabo de forma presencial (a los que hay que sumar los cursos impartidos a distancia). De igual forma, en las jornadas y seminarios de concienciación y sensibilización, así como en las presentaciones del CCN-CERT realizadas por diversas autonomías (Madrid, Comunidad Valenciana, Aragón, Asturias, Cantabria, Castilla y León...), han sido más de 700 los responsables de seguridad que han asistido a las mismas.

Pero además, y conviene no olvidarlo, el CCN-CERT tiene un papel muy importante en el ámbito internacional. Al actuar como CERT gubernamental español está presente en las principales organizaciones internacionales en las que se aborda continuamente la forma y el modo de atajar cualquier posible ataque o incidente (ENISA, OTAN, FIRST, TERENA...). Esta participación nos lleva a colaborar activamente junto con otros equipos e instituciones en la resolución de incidentes transfronterizos en los que se nos pide ayuda y colaboración y que, por supuesto, siempre prestamos.

**¿Qué aporta este servicio a la Administración?**
Son numerosas las aportaciones y servicios del CCN-CERT puestos a disposición de toda la Administración. No obstante, yo destacaría las siguientes, en función del momento y la forma en que se actúe ante un incidente: servicios reactivos (gestión de incidentes; información sobre vulnerabilidades, alertas y avisos; o análisis de código dañino remitido por las diferentes administraciones), proactivos (boletines e informes restringidos, auditorías y evaluaciones de seguridad de los servicios web que así lo requieren; desarrollo de herramientas de seguridad y detección temprana de intrusiones) y de gestión (análisis de riesgos, sensibilización y formación).

En definitiva, el CCN-CERT mantiene entre sus metas el facilitar una gestión

de incidentes de seguridad centralizada; coordinar una respuesta a unos tipos de incidentes específicos; proporcionar asistencia técnica directa que se requiera y las referencias en configuraciones de seguridad; forzar a proveedores a una respuesta adecuada ante vulnerabilidades detectadas y establecer relaciones con otros CERT y con las Fuerzas y Cuerpos de Seguridad del Estado.

**En un mundo interconectado, en el que la seguridad debería plantearse como una estrategia global, ¿no sería óptimo llegar a aunar todos los CERT de seguridad en uno solo que controlase todas las incidencias?**

Un único CERT no puede afrontar por sí solo el número creciente de amenazas a los que, hoy en día, están expuestos los sistemas de información de un país o, en este caso, de toda la Administración Pública. No obstante, sí que es cierto que resulta imprescindible la colaboración no sólo de los CERT de un país, sino de los equipos de todo el mundo para afrontar unas amenazas que no tienen fronteras. Por este motivo, uno de nuestros objetivos es ofrecer información, formación y herramientas para que las distintas administraciones, particularmente las autonomías, puedan desarrollar sus propios CERT (u otros servicios de gestión de seguridad centralizada, llámense CSIRT, COS o de otra forma), permitiendo al CCN-CERT actuar de catalizador y coordinador de CERT a nivel gubernamental. Nuestra voluntad, además, es la de apoyar a todos ellos, colaborar en la medida de nuestras posibilidades a su formación (facilitando información, herramientas de seguridad...) y, llegado el caso, ayudarles en la resolución de incidentes e, incluso, fomentar su participación en foros internacionales.

Por poner un ejemplo, en países como Alemania o Reino Unido el número de CERT se eleva hasta los 19 y 17, respectivamente (incluidos equipos de organizaciones privadas).

**¿De qué manera mantienen la colaboración o el cruce de información, tanto con servicios de seguridad TIC privados, como con otros públicos existentes?**

Antes de nada, debo decir que para el desarrollo de las funciones establecidas en el Real Decreto de su constitución (RD 421/2004) , el Centro Criptológico Nacional (CCN) debe establecer la coordinación oportuna con las Comisiones Nacionales a las que las leyes atribuyan responsabilidades en el ámbito de los sistemas de las Tecnologías de la Información y de las Comunicaciones (TIC). Esto implica mantener un contacto permanente con diversas instituciones y organismos implicados en la seguridad de la información. Así, mantenemos relaciones con la Administración Pública, infraestructuras críticas (CNPIC) y sectores estratégicos, Fuerzas y Cuerpos de Seguridad del Estado, otros CERT, ISP, empresas de *hosting*, registradores, etc. En este sentido, formamos parte del Grupo de CERT españoles públicos y privados reconocidos (CSIRT.es) y del Foro ABUSES (equipos ABUSE de ISP españoles promovido por RedIRIS). Además, hemos venido firmando diversos acuerdos con distintos organismos con el fin de colaborar mutuamente (FEMP, INTECO, etc.).

En cuanto al ámbito internacional, somos miembros de pleno derecho del FIRST (principal organismo que aglutina a los CERT de todo el mundo), del *NATO Cyber Defense Workshops*, del *European Government CERT Group* (EGC), del Terena TF-CSIRT y del Grupo de Trabajo de CERT Nacionales de ENISA. Asimismo, pertenecemos al *AntiPhishing WG* y al Programa SCP de Microsoft.

**¿Está la Administración española preparada para defenderse ante un posible ciberataque?**

Desgraciadamente, ningún sistema está libre de sufrir algún ataque, e incluso la mejor infraestructura de seguridad de información no puede garantizar que una intrusión acabe por afectar a un equipo. Pese a ello, y pese a que somos conscientes de la existencia de estos riesgos y amenazas y de la necesidad de que todos los organismos tomen conciencia de ello, podemos decir que la Administración española está preparada para defenderse ante un posible ciberataque.

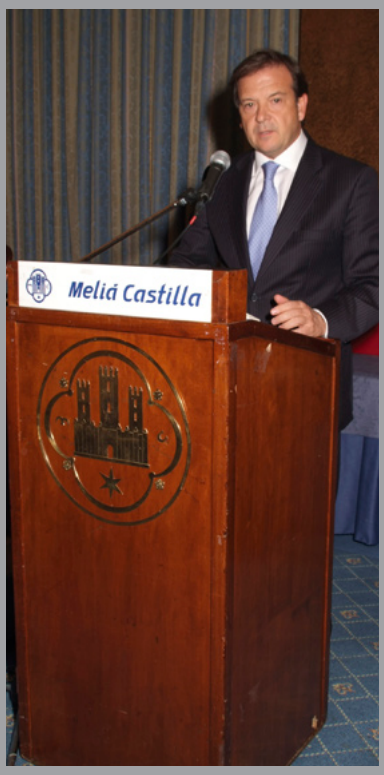
La iniciativa del CCN-CERT, junto con otras desarrolladas en los últimos años, sigue la línea trazada en materia de seguridad de las TIC por los países más avanzados y por las organizaciones internacionales OTAN y Unión Europea, con quienes colaboramos activamente y con quienes mantenemos una estrecha relación para actuar, tanto de forma preventiva como reactiva, ante cualquier hipotético ataque.

**Para afrontar las amenazas que se producen a través de las TIC, además de tecnología, ¿qué claves son necesarias?**

El principal obstáculo con el que nos enfrentamos a la hora de afrontar estas amenazas es, por paradójico que resulte, la falta de concienciación en materia de seguridad de los usuarios de las TIC. De hecho, la ingenuidad, los errores y omisiones del personal autorizado y bienintencionado -pero desconocedor de buenas prácticas de seguridad- y la falta de concienciación existente sobre la necesidad de preservar la seguridad de la información constituyen una fuente principal de amenazas, que todos, en mayor o menor medida, conocemos (robo, pérdida o extracción de dispositivos de almacenamiento; versiones descifradas de archivos confidenciales, claves de acceso públicas, etc.).

No hay que olvidar que a medida que las tecnologías empleadas para proteger la información se hacen más sofisticadas, los ataques centrados en explotar las debilidades de la persona se incrementan.

Por ello, consideramos que uno de los pilares básicos de la seguridad de la información es la formación y concienciación del personal. Para luchar contra la ingenuidad, la ignorancia de buenas prácticas y la falta de concienciación, es preciso tomar conciencia de los riesgos (con medidas procedimentales, organizativas y técnicas), utilizar herramientas de seguridad (medidas técnicas) y mantener inspecciones que acrediten el buen uso de estas prácticas y herramientas. ■




"Consideramos que uno de los pilares básicos de la seguridad de la información es la formación y la concienciación del personal"


# "La seguridad informática es nuestro 'hobby', afición, pasión, y hemos hecho de todo ello nuestro trabajo"

Antonio Ropero
Socio y co-fundador de Hispasec Sistemas

**¿Qué ha supuesto ganar el Premio Extraordinario del Jurado?**
Tenemos que reconocer que a todos los que integramos Hispasec nos ha hecho mucha ilusión y lo hemos acogido con gran satisfacción. Justo ha coincidido con nuestro décimo aniversario, y si durante diez años hemos publicado y distribuido gratuitamente una noticia de seguridad todos los días, y hemos trabajado para formar y concienciar a los usuarios de la importancia de la seguridad, este reconocimiento por parte de la revista RED SEGURIDAD sólo nos puede animar a seguir en la misma línea y tratar de hacerlo cada vez mejor.

**¿En qué cree que radica el éxito de Hispasec Sistemas como empresa?**
Entendemos que son varios los factores diferenciadores de Hispasec como empresa. El primero fue el de su nacimiento. Nacimos como empresa a demanda del propio mercado, lo que nos permitió un crecimiento con una fuerte base tecnológica más que empresarial, ya que el mercado demandaba nuestro conocimiento. En la actualidad, seguimos dando gran importancia a la base tecnológica; nuestro Laboratorio Técnico es el valor más importante dentro de la compañía.

En segundo lugar, nuestro crecimiento se ha basado siempre en la excelencia de nuestro trabajo, priorizando la labor técnica a la comercial o gerencial. Y apoyándonos en un capital humano al que Hispasec siempre estará agradecido por su dedicación, y por poner su talento a disposición de la empresa y, por consiguiente, a disposición de nuestros clientes; sin este binomio trabajador/cliente, no seríamos lo que somos.

En tercer lugar, y columna vertebral de nuestra filosofía empresarial, es el favorecer a la comunidad en general, con parte de nuestro conocimiento y desarrollos I+D, siendo recompensados por parte de la comunidad con prestigio, apoyo y con el propio *know-how* de la comunidad.

**¿Qué proyecto es la "niña bonita" de Hispasec?**
Es difícil decidirnos por uno. Es como cuando a un niño le preguntan: "¿A quién quieres más, a papá o a mamá". A "una-al-día" le tenemos un especial cariño, porque este servicio ha significado el nacimiento de Hispasec como empresa, nuestra forma de darnos a conocer entre muchos técnicos y nuestra principal "tarjeta" de presentación.

Por otra parte, VirusTotal es un servicio desarrollado íntegramente por el Laboratorio de Hispasec, que en poco tiempo, ha crecido hasta obtener un reconocimiento mundial. En muchos foros y países conocen VirusTotal (el servicio está disponible en 23 idiomas), sin embargo, no conocen Hispasec. La cifra de más de 50.000 archivos analizados diariamente por los 38 antivirus que actualmente integran el servicio (más de 20 análisis por segundo), ya nos llena de satisfacción.

Y por qué no decirlo también; actualmente, estamos muy orgullosos con nuestro último "niño", el libro que acabamos de publicar -*Una al día*-, que recoge todo lo ocurrido durante los últimos diez años en el mundo de la seguridad informática, y un buen número de entrevistas a personas relevantes dentro de nuestro sector.

**¿Cómo describiría su compañía?**
Nos gusta definirnos como un laboratorio especializado en Seguridad TIC. Desde 1998, el equipo de Hispasec se ha especializado en diferentes áreas dentro del mundo de la seguridad. Actualmente, nuestras principales líneas de negocio son: Auditoría, Servicio de información y alertas, Consultoría y Antifraude.

Nos gusta vernos como una empresa joven y ágil, por lo que nuestro laboratorio siempre intenta estar a la vanguardia en cuanto a nuevas tendencias de ataque, fraudes, etc., con el fin de proporcionar a los clientes el mayor grado posible de seguridad.

Para quien todavía no conozca Hispasec Sistemas, lo mejor que puede hacer es ver lo que hacemos con sus propios ojos. Solo puedo recomendarle que se pase por nuestra web (www.hispasec.com); se subscriba a "una-al-día", nuestro *newsletter* que diariamente envía una noticia de seguridad informática; visite VirusTotal (www.virustotal.com), donde de forma gratuita podrá enviar cualquier archivo para que sea escaneado por 38 antivirus; o nos consulte sobre cualquiera de los servicios que prestamos (auditorías, consultoría, antifraude…).

**¿Qué es para ustedes la seguridad informática?**
Si hace diez años ya estábamos convencidos de la importancia de la seguridad informática, imagina en la actualidad. Con frecuencia solemos decir que la seguridad es nuestra razón de ser. Desde nuestro origen nos hemos centrado en la investigación de los problemas de seguridad informática y en proporcionar soluciones correctivas y preventivas. Creemos que la seguridad es algo que incumbe a todos, y que necesitamos tanto empresas, Administración como usuarios.

En otras palabras, la seguridad informática es nuestro *hobby*, afición, pasión, y hemos hecho de todo ello nuestro trabajo.

**¿Cuál es el mayor peligro que existe hoy?**
En más de una ocasión, en "una-al-día" hemos escrito que "la seguridad es como una cadena: siempre se rompe por el eslabón más débil". Frase a la que habría que añadirle que el eslabón más débil suele ser el factor humano. Por eso es tan importante la formación y concienciación de todos los usuarios en materia de seguridad. Pero ello no debe implicar descuidar, desde luego, ninguno de los demás factores; tenemos que procurar que todos los eslabones de esa cadena que componen la seguridad sean lo más robustos posible.

**Y pensando en utopías, para que un día llegásemos a estar cien por cien protegidos, ¿en qué línea es necesario trabajar?**
No se puede descuidar tampoco ninguna línea de trabajo, y nosotros seguimos apostando por todas ellas. "una-al-día" es un buen medio para la concienciación y promoción de la seguridad y, por eso, seguimos prestando el servicio gratuitamente, y seguiremos haciéndolo, incluso lo hemos ampliado con el apoyo del *blog* del laboratorio, donde tienen cabida aspectos o tratamientos de la información que posiblemente quedan fuera de "una-al-día". Igualmente, nuestra apuesta e inversión en I+D+i es fuerte y dedicamos grandes recursos a ello. ■

# "En S21sec, siempre se ha considerado la formación como un elemento determinante para alcanzar los objetivos de seguridad"

Juan Carlos Rodríguez
Director de Formación de S21sec

**¿Qué ha supuesto para su compañía ganar el premio a la formación y capacitación en seguridad TIC?**
Para todo el equipo que formamos parte del departamento de Formación, ganar este premio nos ha supuesto obtener un reconocimiento al trabajo que llevamos desarrollando desde hace seis años, donde la innovación y la satisfacción de nuestros clientes son nuestro medio y objetivo. Este premio nos ayuda a seguir adelante ya que, si bien es difícil llegar, no lo es menos mantenerse y, por ello, uno de nuestros objetivos para el próximo año será precisamente conseguir ser merecedores de nuevo de este galardón.

**¿Qué papel tiene para ustedes dicho ámbito?**
En S21sec, siempre se ha considerado la formación y la concienciación en seguridad como uno de los elementos fundamentales y determinantes para poder alcanzar los objetivos de seguridad de las empresas. Estos objetivos están fijados por el cumplimiento de las políticas de seguridad ya que, como muchas veces se ha señalado, "la seguridad es una cadena tan fuerte como el más débil de sus eslabones", y es precisamente la actitud y conocimiento de seguridad de los profesionales lo que podemos considerar el "eslabón más débil" de la cadena.

Actualmente trabajamos ocho personas en el departamento de Formación, entre formadores, desarrolladores y diseñadores, pero contamos con la colaboración y participación de personas de cada departamento que nos ayudan en la actualización, renovación y adecuación de los contenidos. La aportación de estas personas nos ofrece un punto de vista muy importante basado en su experiencia y su trabajo en áreas especializadas.

**¿Nos puede detallar cómo es el proceso de formación continua de S21sec?**
En S21Sec hemos desarrollado un plan de formación interno de seguridad adaptado a los diferentes perfiles de trabajo dentro de la compañía. Este plan de formación contempla un curso multimedia para todos los trabajadores sobre "concienciación y sensibilización en seguridad" que muestra cómo adquirir "buenas prácticas en seguridad" en nuestro trabajo diario.

Posteriormente, y para aquellos trabajadores que por su puesto de trabajo así lo necesiten, se imparten diferentes cursos *on-line* basados en la metodología de *e-learning*. El *e-learning* está apoyado con contenidos multimedia y tutorización remota que facilita la adquisición de conocimientos y capacidades para perfiles de tecnología, auditoría y gestión de la seguridad. Estos cursos son tutorizados por personal del departamento de Formación especializado en cada área. Con este sistema, cada trabajador planifica, en función de su disponibilidad, su tiempo diario de dedicación al curso.

Los trabajadores que realizan los tres cursos base (Tecnología, Auditoría y Gestión) reciben la titulación de "Máster en Sistema de Gestión de la Seguridad de la Información", que es un título propio de S21sec.

En departamentos concretos, y en función de su actividad, sus componentes reciben formación especializada oficial de fabricantes de *hardware* y *software*, que acreditan su capacitación como expertos conocedores de la solución a implementar en el cliente. Ejemplo de ello es la formación realizada por fabricantes de soluciones de *firewall*, IPS, antivirus...

**¿Cuál es el perfil de los trabajadores de S21sec?**
El perfil mayoritario de los trabajadores de S21sec es el de licenciado, ingeniero y técnico de grado superior -una gran parte ellos en Ingeniería Informática o Telecomunicaciones-. Puesto que en la actualidad no existe una titulación que forme profesionales específicamente en el mundo de la "Seguridad Digital", a lo largo de su trabajo en S21sec, una parte de ellos se preparan para la obtención de certificaciones internacionales reconocidas en seguridad como pueden ser: CISSP, CISM, CISA... De esta forma, a su formación técnica de base se añade la acreditación como especialistas en "Seguridad Digital" avalada por la obtención de títulos reconocidos internacionalmente.

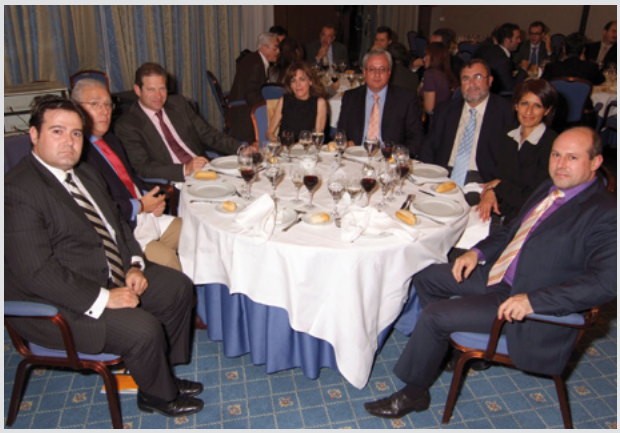
**¿Cuánto invierten en formación?**
Actualmente, la inversión realizada en la formación interna de empleados se sitúa en torno al cuatro por ciento anual sobre la masa salarial. Esta inversión se destina a: formación interna, ofrecida por expertos de la propia compañía al resto de trabajadores a través de los cursos *on-line*; formación externa, impartida por los fabricantes y proveedores de soluciones de seguridad integradas por la compañía; preparación y pruebas de certificación como CISM, CISA, CISSP…

**¿Cuál es su opinión sobre el "matrimonio" Universidad-Empresa?**
Desde el mundo universitario constatamos cada vez un mayor interés por establecer colaboraciones con el mundo profesional de las empresas. Prueba de ello, es que en S21sec hemos establecido numerosos acuerdos con universidades para la realización de trabajos de investigación, cátedras o desarrollo de formación de postgrado que posibiliten la especialización de los alumnos de carreras universitarias tecnológicas en la "Seguridad Digital". En la actualidad, esta formación solo puede ser realizada como una especialización, a través de estudios de postgrado o másteres, si bien desde nuestra perspectiva, entendemos que la formación en "Seguridad Digital" debería desarrollarse como una carrera universitaria propia, con un título específico.

Desde este convencimiento, y por la ausencia actual de esta formación oficial en seguridad, hemos desarrollado la línea de formación "S21sec University", desde la que presentamos un itinerario completo de formación en seguridad a lo largo de tres años y que contempla la adquisición de las competencias necesarias para desarrollar las labores como el responsable de seguridad de nivel más alto de cualquier empresa.

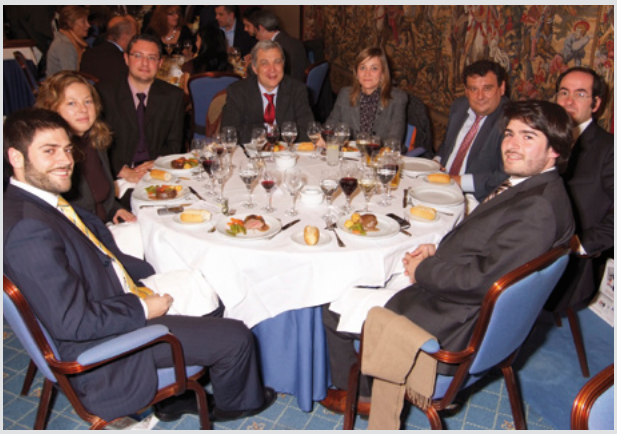
La formación profesional es también una línea a tener en cuenta, puesto que determinadas tareas específicas se pueden llevar a cabo satisfactoriamente con una especialización en seguridad dentro de la formación profesional, y ayudaría a cubrir las carencias de profesionales en el sector. ■

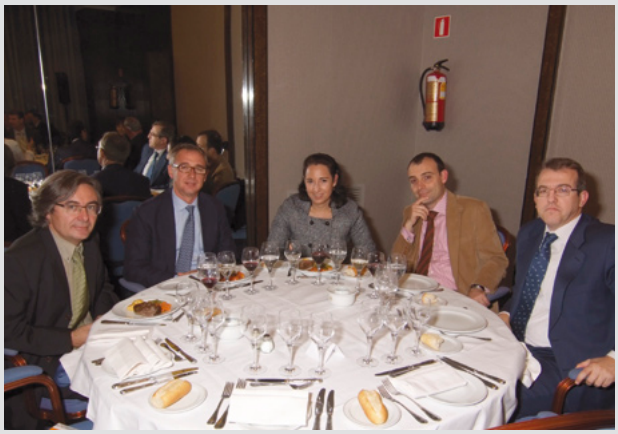
# ALMUERZO INSTITUCIONAL ALMUERZO INSTITUCIONAL ALMUERZO

# INSTITUCIONAL ALMUERZO INSTITUCIONAL ALMUERZO INSTITUCIONAL








III edición