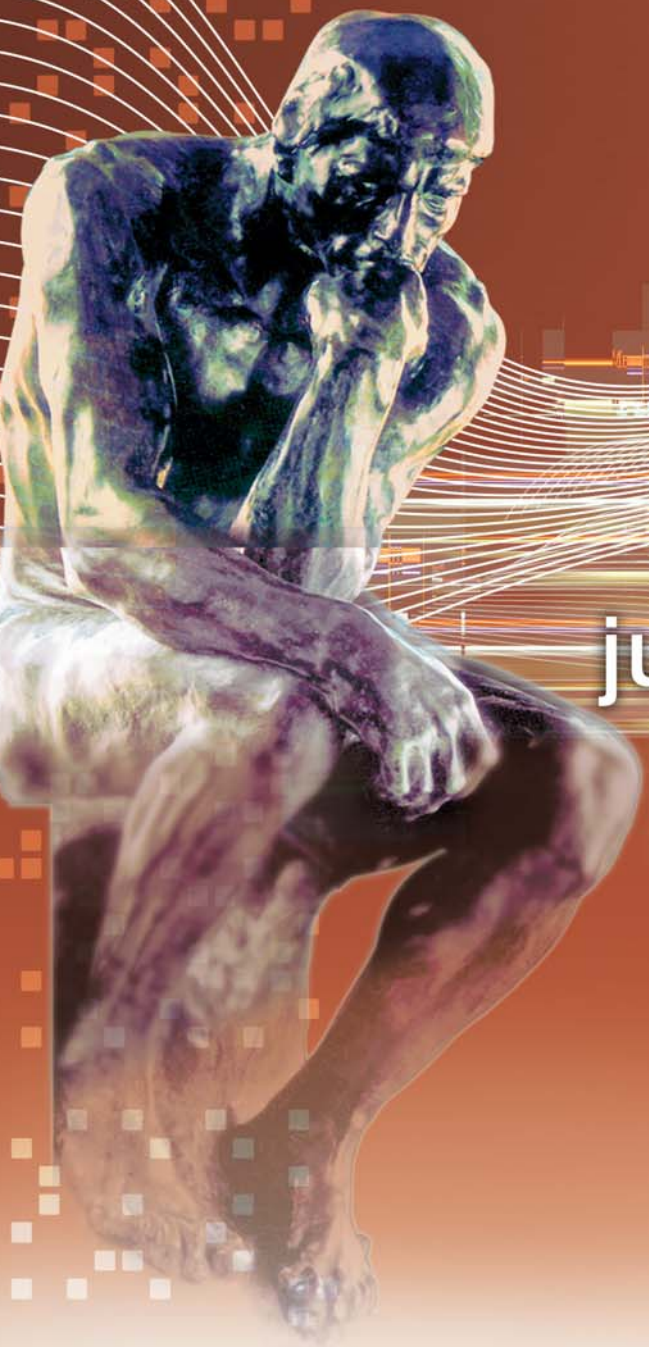
SECURMATICA 2010

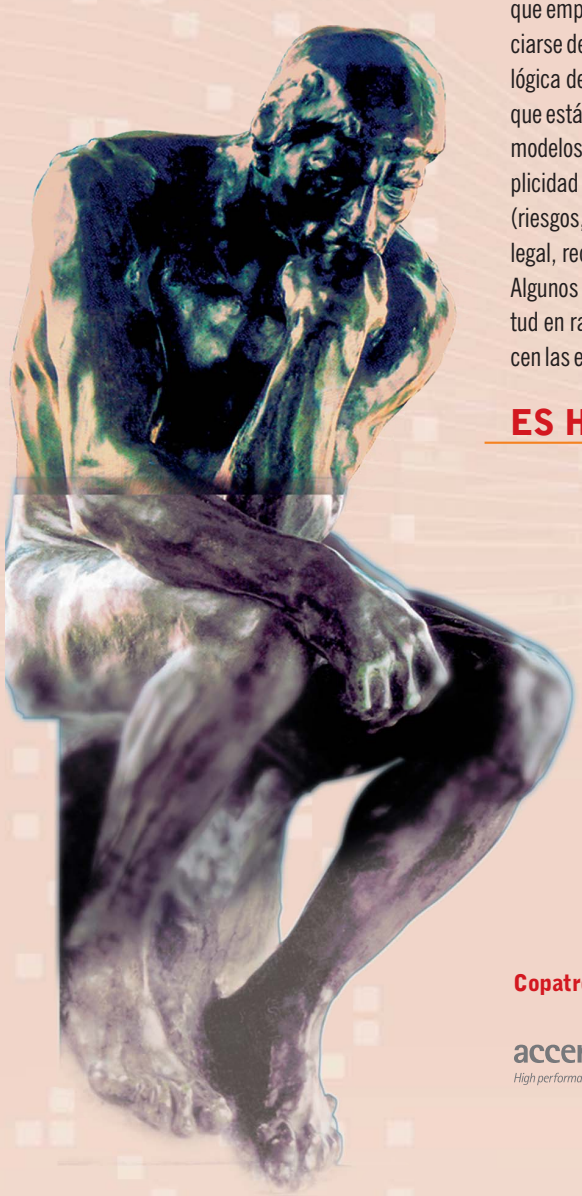
XXI Congreso español de Seguridad de la Información

27.28.29 | abril



Seguridad
invisible
justificada
útil

PROGRAMA



Securmática 2010, XXI edición del Congreso español de Seguridad de la Información organizado por la revista SIC, tendrá lugar los días 27, 28 y 29 de abril en su tradicional sede del Campo de las Naciones de Madrid.

Las distintas actividades que conforman la protección de la información tratada en sistemas tecnológicos se encuentran actualmente a las puertas de una nueva fase evolutiva, en la que empiezan a encontrar acomodo y a diferenciarse de un modo palpable la dimensión tecnológica de otras también de corte corporativo, lo que está dando lugar a la aplicación de distintos modelos de gestión en los que se asume la mutiplicidad de frentes que abarca esta disciplina (riesgos, control, tecnología, cumplimiento legal, recursos humanos, imagen, auditoría...). Algunos de estos modelos guardan una similitud en razón de los sectores a los que pertenecen las entidades (caso, por ejemplo, del sector financiero), y otros son producto del punto de partida y de la cultura de cada empresa. Y todos, eso sí, tienen que alcanzar el punto óptimo de eficiencia, especialmente en estos tiempos en los que los órganos de gobierno de los grupos empresariales, tratan de reducir con trazo fino la complejidad, la dispersión y los costes, optando por la externalización de todas aquellas actividades que no consideran nucleares.

Por otra parte, al del tratamiento legal de los datos personales, se están uniendo otros frentes que plantean retos importantes a las entidades públicas y las privadas, como es el caso del de las evidencias electrónicas, o el del intento de control de la información empresarial en las redes sociales o la defensa frente a una delincuencia crecientemente organizada y con conocimientos de los procesos de negocio y el comportamiento de las personas.

A ellos se viene a sumar otro, el de la protección de las infraestructuras críticas, particularmente las de información –hoy en sus albores regulatorios–, que junto con la denominada "ciberguerra", va a ir demandando más atención.

ES HORA DE COMPARTIR EXPERIENCIAS >>> Y AVANZAR

Securmática pretende ser un fiel reflejo de lo que se está haciendo en, entre otras, estas materias. Y en este sentido, el programa de su XXI edición incluye una calibrada selección temática en la que expertos de reconocido prestigio relatarán proyectos tecnológicos relevantes (no pocos de vanguardia), justificarán cambios organizativos de gran calado, y realizarán aportaciones en asuntos capitales para la profesión y la práctica de la seguridad de la información y la seguridad TIC.

Copatrocinadores:

accenture High performance. Delivered. · BULL · ERNST & YOUNG Quality In Everything We Do · gmv · GRUPO GESFOR 25 años · hp · IBM · indra · inteco Instituto Nacional de Tecnologías de la Comunicación · PRICEWATERHOUSECOOPERS · S21sec · Telefónica · unitronics

Organiza:

Revista SIC seguridad en informática y comunicaciones

SIC Seguridad en Informática y Comunicaciones es desde hace diecinueve años la revista española especializada en seguridad de los sistemas de información. Perteneciente a Ediciones CODA, esta publicación organiza SECURMÁTICA, el acontecimiento profesional por excelencia de este pujante ramo de las TIC en nuestro país.

PRIMER MÓDULO 27 de abril

08:45h. Entrega de documentación
09:15h. Inauguración Oficial.
09:55h. **Ponencia: La nueva organización de seguridad de la información del Grupo BBVA.**
Ponente: Santiago Moral Rubio, Director de Seguridad de la Información del Grupo BBVA.
10:30h. Coloquio
10:35h. **Ponencia: Maximización del valor de las competencias en seguridad.**
Ponente: Tomás Roy Catalá, Director del Área de Calidad, Seguridad y Relaciones con Proveedores del Centro de Telecomunicaciones y Tecnologías de la Información-CTTI de la Generalitat de Cataluña.
11:10h. Coloquio.
11:15h. Pausa-café.
11:45h. **Ponencia: Compartiendo información de seguridad: reto y oportunidad.**
Ponente: Daniel Barriuso Rojo, CISO y Responsable Global de Riesgos TI de Credit Suisse.
12:20h. Coloquio
12:25h. **Ponencia: La amenaza interior.**
Ponente: Miguel Ángel Navarrete Porta, Director de Seguridad Informática de Caja Madrid.
13:00h. Coloquio.
13:05h. **Ponencia: El modelo Mapfre de seguridad. Del Plan de Contingencias a la Continuidad de Negocio.**
Ponentes:
• **Juan Ignacio Sánchez Chillón**, Director de Planificación y Procesos de Seguridad. Mapfre.
• **Lionel Güitta Abellán**, Subdirector de Continuidad de Negocio y Contingencia Informática. Mapfre.
13:40h. Coloquio.
13:45h. Almuerzo.
15:45h. **Ponencia: Enfoque corporativo para la gestión del cumplimiento regulatorio e implantación de herramientas de soporte en el Grupo Iberdrola.**
Ponentes:
• **Adolfo Merino Cañas**, Departamento de Seguridad de la Información y las Comunicaciones de Iberdrola.
• **Manuel Cortés Márquez**, Responsable de Ventas de Seguridad de Accenture.
16:20h. Coloquio.
16:25h. **Ponencia: Caja de Ahorros del Mediterráneo: seguridad gestionada y estrategia.**
Ponentes:
• **Francisco Galdames Gómez**, Director de Planificación Tecnológica de la Caja de Ahorros del Mediterráneo-CAM.
• **Javier Megias Terol**, Director Regional de Levante de GMV.
17:00h. Coloquio.
17:05h. Pausa-café.
17:20h. **Ponencia: Redes y Procesos: monitorización integral de la seguridad.**
Ponentes:
• **Miguel Ángel Fernández Martín**, Director de Producción de Redes y Procesos.
• **Mariano Largo del Amo**, Director de Desarrollo de Negocio de S21sec.
17:55h. Coloquio.
18:00h. Fin de la primera jornada.

LA NUEVA ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL GRUPO BBVA

Sinopsis: El Grupo BBVA, durante el año 2009, ha trasformado su organización de Seguridad de la Información. Los objetivos fundamentales son mejorar la capacidad de gestión global de los ámbitos funcionales del Gobierno del Riesgo Tecnológico, unificar la gestión de la prevención tecnológica del fraude y la globalización en la gestión de las tecnologías de seguridad de la información.
La función de Seguridad de la Información se ha desarrollado en tres planos: estratégico, funcional y geográfico.
• El estratégico refleja qué entendemos por seguridad de la información en el Grupo BBVA y qué departamentos son los interlocutores naturales en los procesos de gestión cotidianos.
• El funcional describe las diez funciones en las que estructuramos la Seguridad de la Información y su forma de gestión.
• El geográfico describe qué funciones se hacen en un único punto para todas las empresas, qué funciones deben hacerse en cada empresa y como los CISO locales deben liderar la función en su ámbito geográfico.

Ponente:

• **Santiago Moral Rubio** es Director de Seguridad de la Información del Grupo BBVA. Con más de una década de experiencia en seguridad y protección de la información, este Ingeniero Técnico Informático, poseedor de las certificaciones CISA y CISM, inició su andadura profesional en el Grupo BBVA en mayo de 2000 como Responsable de Seguridad de Sistemas de uno-e Bank. Nueve meses después, en marzo de 2001, se responsabilizó de la Seguridad Lógica de BBVA, para pasar posteriormente a ocupar la Dirección de Seguridad Lógica Corporativa del Grupo BBVA hasta su nombramiento en 2009 como CISO.

MAXIMIZACIÓN DEL VALOR DE LAS COMPETENCIAS EN SEGURIDAD

Sinopsis: La actual tesitura económica pone de relieve la extrema necesidad de reducir ineficiencias, generar ingresos y mejorar la productividad. Esto va a llevar a eliminar solapamientos de funciones, industrializar la producción y detectar oportunidades de mejora. Aquellas empresas que hayan hecho los deberes en épocas favorables saldrán de la situación demostrando que pueden ser ciertos los tópicos de que las crisis son una oportunidad y que lo importante es prepararse para la postcrisis. Este pensamiento es aplicable también a las funciones de una organización, e incluso a cada profesional. La función de seguridad captura de forma natural –debido a la complejidad de los problemas a resolver– personas con alto potencial y versatilidad de competencias. A través de un análisis de los servicios TI se descubren nuevas áreas de responsabilidad o soporte de la función de seguridad. Maximícese el valor de las competencias de seguridad afrontando con ellas nuevos retos y nuevos éxitos.

Ponente:

• **Tomás Roy Catalá** es Director del Área de Calidad, Seguridad y Relaciones con Proveedores en el Centro de Telecomunicaciones y Tecnologías de la Información (CTTI) de la Generalitat de Cataluña. Desde 2004 dirige un equipo en el área de la Calidad y la Seguridad destacando la gestión de los servicios externalizados. Desde 2006 lidera la gestión de la Calidad y la Seguridad en proyectos y aplicaciones, y desde septiembre de 2007 ha integrado en sus funciones la Dirección del Área de Relación con Proveedores. Ingeniero Superior en Telecomunicaciones, Ingeniero Superior en Electrónica y Licenciado en Ciencias de la Educación, Roy Catalá ha desarrollado su carrera profesional en Italia, en la *joint venture* Fiat GM Powertrain, en la que fue Responsable de Seguridad de la Información y de Privacidad de Datos. Complementa su formación en el área de seguridad en los ámbitos de auditoría –CISA–, gestion de seguridad –CISSP–, gestión de servicios –ITIL–, mejora continua –6sigma– y seguridad de sistemas operativos y redes.

COMPARTIENDO INFORMACIÓN DE SEGURIDAD: RETO Y OPORTUNIDAD

Sinopsis: El mundo de la seguridad se encuentra inmerso en una carrera de amenazas cambiantes, nuevas tecnologías y constante innovación en los métodos de defensa. En tan cambiante entorno, estar preparados es sinónimo de tener la información adecuada en el momento oportuno. La ponencia aborda preguntas claves tales como: ¿es beneficioso compartir información de seguridad vs. ventaja competitiva?, ¿qué información aporta valor y por qué?, ¿cuáles son los retos y barreras que limitan la compartición de la información?, ¿cuáles son los principales grupos que pueden (¡y deben!) compartir información? y ¿qué modelos funcionan y cuáles podrían aportar luz en el futuro?

Ponente:

• **Daniel Barriuso Rojo** es CISO y responsable Global de Riesgos TI en Credit Suisse, donde es responsable de la seguridad de la información y riesgo tecnológico a través de más de 50 países. Con una experiencia de más de 10 años en Seguridad y TIC, la prioridad de Barriuso está centrada en los aspectos organizativos de la seguridad, tales como el gobierno, la estrategia y la gestión del riesgo. Desde 2002, imparte clases como profesor en el Master de Seguridad y Auditoría de la Universidad Politécnica de Madrid. En la actualidad, Barriuso reside en Londres y es el presidente del grupo de Seguridad en la Banca de Inversión (UK IBSIG), que agrupa a los 30 mayores bancos en Reino Unido.

LA AMENAZA INTERIOR

Sinopsis: Desde su creación, las empresas han tenido que afrontar amenazas internas clásicas como el fraude, el robo de información, de mercancías, etc. Para combatirlas han aplicado normas, procedimientos y herramientas específicos en un contexto contractual adecuado. No obstante, el cambio cultural, la universalización de las herramientas, los nuevos modelos de negocio y la explosión tecnológica han aumentado los riesgos provocados por estas amenazas, por lo que reevaluar y actualizar los controles existentes y generar nuevos ajustados al cambiante escenario es una necesidad para todo tipo de organizaciones, independientemente de su ámbito de actuación y de su tamaño. En este contexto, la conferencia está dirigida a compartir ideas sobre la importancia del riesgo específico que presentan las personas que acceden a la red interna de las entidades, en relación con la seguridad de las mismas, y cómo tratar ese riesgo para procurar minimizarlo.

Ponente:

• **Miguel Ángel Navarrete Porta** es Director del Departamento de Seguridad Informática de Caja Madrid. Ha trabajado como informático desde hace veintitrés años en diferentes entidades financieras. Desde su primer contacto en Explotación y hasta su llegada al mundo de la seguridad de la información, ha recorrido casi todas las áreas de las TI (Técnica de Sistemas, Gestión Presupuestaria, Recursos y Proyectos, Metodología, Arquitectura y Desarrollo de Software), donde ha dirigido numerosos proyectos. Actualmente se enmarca en Planificación e Innovación Tecnológica de Caja Madrid, donde se ubica el departamento de Seguridad Informática, que dirige desde el año 1999.

EL MODELO MAPFRE DE SEGURIDAD. DEL PLAN DE CONTINGENCIAS A LA CONTINUIDAD DE NEGOCIO

Sinopsis: En el año 1996, Mapfre decidió apostar por un enfoque integral de la seguridad, que plasmó en el, entonces novedoso, Plan Director de Seguridad, en el que se establecieron los criterios de actuación, definiendo la estructura y concretando las funciones a desempeñar. Dicho enfoque integral contempla todas las amenazas y riesgos, así como el uso coordinado de recursos técnicos, humanos y organizativos, que se instrumenta en un control centralizado de los medios electrónicos. Tras una década de experiencia, surge la pregunta: ¿es ésta la seguridad que Mapfre necesita? A la mencionada concepción integral, con alcance global y carácter permanente, se añade algo no considerado en el modelo: garantizar la operativa del negocio, iniciándose así la inmersión de Mapfre en lo que se ha venido en denominar "Continuidad de Negocio".

Ponentes:

• **Juan Ignacio Sánchez Chillón** es desde el 1 de enero de 2010 Director de Planificación y Procesos de Seguridad en la Subdirección General de Seguridad y Medio Ambiente de Mapfre, cargo en el que tiene responsabilidades básicas de ámbito corporativo en las áreas de seguridad de la información, continuidad de negocio, cumplimiento normativo relacionado con la Seguridad y las Tecnologías, y la coordinación de los Jefes de Seguridad de la Información de las entidades Mapfre. Licenciado e Ingeniero en Informática por la UPM, es Máster en Auditoría y Seguridad Informática por la UPM, experto en Gerencia de Riesgos y Seguros por el Instituto de Ciencias del seguro de la Fundación Mapfre, Director de Seguridad en Empresas por la Universidad Pontificia de Comillas (ICADE), y posee las certificaciones CISA e IT Service Management (ITIL). De 2005 a 2008 desempeñó el puesto de Jefe del Departamento Corporativo de Seguridad de la Información de Mapfre, y durante los diez años anteriores (1996 a 2005) fue Responsable de los Servicios de Auditoría Informática de Mapfre, reportando directamente al Director General de Auditoría Interna.

• **Lionel Güitta Abellán** es desde el 1 de enero de 2010 Subdirector de Continuidad de Negocio y Contingencia Informática en la Subdirección General de Seguridad y Medio Ambiente de Mapfre, cargo en el que tiene como responsabilidades básicas de ámbito coporativo la responsabilidad y la coordinación de la Continuidad de Negocio y la Contingencia Informática. Licenciado en Informática por la UPM y Experto Universitario en seguridad y Comercio Electrónico por la UNED, Güitta fue con anterioridad y desde 2007 Subdirector de Explotación de Tecnologías de Seguridad de Mapfre. Previamente –entre 1993 y 2001 fue Técnico de Sistemas y Responsable de Técnica de Sistemas en Banco Mapfre, y de 2001 a 2007 desempeñó labores de Jefe de Seguridad de la Información en las empresas tecnológicas de Mapfre.

ENFOQUE CORPORATIVO PARA LA GESTIÓN DEL CUMPLIMIENTO REGULATORIO E IMPLANTACIÓN DE HERRAMIENTAS DE SOPORTE EN EL GRUPO IBERDROLA

Sinopsis: La casuística concreta de Iberdrola y los requerimientos en materia de cumplimiento regulatorio llevó a la Dirección de Seguridad Corporativa a establecer un modelo para gestionar dichos requerimientos de la forma más eficaz y eficiente. A partir de ese modelo, Iberdrola, con el apoyo de Accenture, ha llevado a cabo la implantación de una herramienta de soporte que centraliza su gestión, pero que establece la realización de ciertas tareas por parte de los responsables según su ámbito de actuación en el tratamiento de Ficheros de Carácter Personal. El sistema implantado mejora la gestión de la información, tanto en el ámbito de los requerimientos legales (registros frente a la AEPD, Documento de Seguridad, procedimientos…), como en el ámbito de la información interna que le da soporte.

Ponentes:

• **Adolfo Merino Cañas** es Licenciado en Ciencias Físicas por la UCM. Comenzó su carrera profesional como consultor, para incorporarse posteriormente en 1998 a Iberdrola, compañía en la que ha desempeñado diferentes puestos siempre ligados a la seguridad de la información y a la calidad. Actualmente forma parte del Departamento de Seguridad de la Información y las Comunicaciones, centrándose su labor tanto en la protección de datos de carácter personal como en otros aspectos normativos. Es el jefe del proyecto de implantación de la herramienta en Iberdrola.

• **Manuel Cortés Márquez** es Responsable de Ventas de Seguridad en Accenture. Ingeniero Informático de Sistemas por la Universidad Pontificia de Salamanca, CISA, CISM y CGEIT, viene desempeñando su carrera profesional en el ámbito de la seguridad de la información desde hace catorce años. Desde hace dos trabaja en la práctica de seguridad de Accenture. Anteriormente ha trabajado en organizaciones como el Grupo SIA, donde ocupó el cargo de Director de Consultoría, o en PricewaterhouseCoopers, donde ocupó el puesto de Gerente de la práctica de Seguridad.

CAJA DE AHORROS DEL MEDITERRÁNEO: SEGURIDAD GESTIONADA Y ESTRATEGIA

Sinopsis: La Caja de Ahorros del Mediterráneo (CAM) se planteó hace dos años la necesidad de disponer de un Servicio de seguridad gestionada que le permitiera incorporar a su estrategia diversa información sobre múltiples aspectos relacionados con la Seguridad de la Información, con el fin último de proteger de forma proactiva a sus clientes. En este contexto, GMV presta a través de su servicio de seguridad gestionada, ofrecido desde el SOC de la compañía, un alto nivel de inteligencia de seguridad y servicios gestionados asociados. Dichos servicios permiten a la Caja de Ahorros del Mediterráneo extraer conclusiones relevantes del análisis cruzado de la información de sistemas, dispositivos de comunicaciones, *middleware,* e incluso aplicaciones propias. Dicha información realimenta los procesos de la compañía para mejorar la calidad y seguridad de sus servicios. Asimismo, el servicio incluye la respuesta temprana ante incidentes de seguridad, la realización de análisis de seguridad, *tests* de intrusión y la protección ante amenazas específicas para el sector bancario, donde se hace especial foco en amenazas como el *phishing* y derivados.

Ponentes:

• **Francisco Galdames Gómez** es Director de Planificación Tecnológica de la Caja de Ahorros del Mediterráneo-CAM. Licenciado en Ciencias Físicas y MBA por el IE, ha desarrollado su carrera profesional en distintas compañías y proyectos, tanto nacionales como internacionales, pero siempre relacionados con el mundo de las Entidades Financieras.

• **Javier Megias Terol** es Director Regional de la multinacional española GMV para la zona de Levante. Ingeniero Técnico Informático, ha complementado su formación con las titulaciones CIT y ADIT por la Universidad de Cambridge, y posee las certificaciones PMP en Dirección de Proyectos, CGEIT en Gobierno de las TIC, CISA, CISSP e ITIL Foundations. Tiene más de 15 años de experiencia en el sector TIC, especialmente en las áreas de Seguridad, Innovación, Gobierno de tecnología y Dirección de grandes proyectos. Ha trabajado en diversas organizaciones relevantes en el panorama nacional, colabora con varios medios como escritor y ponente, imparte periódicamente clases en diversas Universidades y actúa como asesor y evaluador de proyectos de I+D+i para la Comisión Europea.

REDES Y PROCESOS: MONITORIZACIÓN INTEGRAL DE LA SEGURIDAD

Sinopsis: En la presentación se mostrará cómo en el momento actual el impulso de las tecnologías de seguridad se revela fundamental para la disponibilidad de negocio, y más en un ámbito transaccional como el de Redes y Procesos, empresa que gestiona millones de transacciones. Entre otras cosas, se expondrá el porqué de la decisión de monitorizar su capa de gestión de la seguridad lógica, y a continuación se explicará cómo desde S21sec se aborda esta tipología de proyectos y cuáles son los aspectos más destacados para dotar de valor a los clientes en los servicios de monitorización de los dispositivos de seguridad, como comienzo de un camino que puede llevar al *outsourcing* de la función de las unidades de seguridad digital.

Ponentes:

• **Miguel Ángel Fernández Martín** es Director de Producción de Redes y Procesos, y entre sus responsabilidades se encuentra la de la Seguridad Corporativa. Licenciado en Ciencias Físicas por la Universidad Complutense de Madrid, inició su carrera profesional en el Banco Español de Crédito, S.A., y en Construcciones Aeronáuticas, S.A. Posteriormente se incorporó a la disciplina de Sistema 4B, S.A., organización en la que ha ocupado diferentes puestos siempre relacionados con la actividad empresarial ligada a los medios de pago.

• **Mariano Largo del Amo** es Director de Estrategia y Desarrollo de Negocio de S21sec. Previamente ocupó el cargo de Director de Proyectos Estratégicos, y se encargó de la definición y puesta en marcha de los proyectos críticos de la compañía, como la creación del Centro de Operaciones de Seguridad Gestionada 24 horas (SOC) y la definición de la línea de servicios de seguridad gestionada. Cuenta con una reconocida experiencia de más de 25 años en el sector de las TI en las áreas de desarrollo de negocio, ventas y marketing.

SEGUNDO MÓDULO 28 de abril

09:00h. Entrega de documentación.

09:15h. **Ponencia: Ferrovial: la gestión de vulnerabilidades como proceso continuo.**
Ponentes:
• **Juan Cobo Páez**, Jefe del Departamento de Seguridad de la Información y Continuidad de Negocio de Ferrovial.
• **Juan Ramón Fontán Lago**, Senior Manager dentro de la práctica IT Risk and Assurance (ITRA) y Responsable de la red de Centros Avanzados de Seguridad de Ernst & Young.

09:50h. Coloquio.

09:55h. **Ponencia: El proceso de autorización como marco integrador de aplicaciones corporativas. Experiencia de Generali e IBM en gestión de accesos web.**
Ponentes:
• **Josep Guijarro García**, Jefe de Proyectos de Seguridad. Departamento de Supervisión de Servicio y Seguridad. Generali España.
• **Vicente Gozalbo Moragrega**, Líder de Ventas de Productos de Seguridad Tivoli. IBM Software Group. Tivoli Software. Seguridad. IBM España.

10:30h. Coloquio.

10:35h. **Ponencia: Prevención del fraude en línea. Aproximación pragmática basada en el CRM de Seguridad.**
Ponente: Jesús Milán Lobo, Director de Riesgos Tecnológicos y Seguridad Informática de Bankinter.

11:10h. Coloquio.

11:15h. Pausa-café.

11:45h. **Ponencia: Los tiempos cambian. Uso inteligente de la información de seguridad.**
Ponente: Casimiro Juanes Calvo, Responsable de Seguridad TI del Grupo Ericsson.

12:20h. Coloquio.

12:25h. **Debate: La dinámica de relación entre la función de Seguridad en Tecnología y Sistemas y las corporativas de Auditoría y Riesgos.**
Participantes:
• **Carlos Bachmaier Johanning**, Gestión de Riesgo Corporativo y Auditoría TI de Sistemas Técnicos de Loterías.
• **Mariano de la Cruz Molina**, Senior Manager de Seguridad Corporativa de Grupo Santander y Responsable de la Estrategia de Seguridad.
• **Carolina de Oro Gómez**, IT Compliance & Risk Management Manager para la Región Mediterránea y Latinoamérica de Axa Seguros.
• **Alejandro Rembado Mendizábal**, Director Corporativo de Auditoría TI de Telefónica.

14:00h. Almuerzo.

16:00h. **Ponencia: CEPSA: externalización de la seguridad TI a escala internacional.**
Ponentes:
• **Rafael Hernández González**, Responsable de Seguridad TI de Cepsa.
• **Juan Miguel Velasco López-Urda**, Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Clientes de Telefónica España.

16:35h. Coloquio.

16:40h. **Ponencia: Monitorización y control de eventos para la Gestión Integral de la seguridad. La experiencia en ONO.**
Ponentes:
• **Francisco Javier Santos Ortega**, Gerente de Gestión Operativa de Seguridad de ONO.
• **Félix Martín Rodríguez**, Gerente de Seguridad de Technology Services. Hewlett-Packard.

17:15h. Coloquio.

17:20h. Pausa-café.

17:40h. **Ponencia: El Centro de Seguridad de la Información de Cataluña-CESICAT, un año después.**
Ponentes:
• **Josuè Sallent i Ribes**, Director General de la Sociedad de la Información. Secretaría de Telecomunicaciones. Generalitat de Cataluña.
• **Jordi Rodríguez Mauri**, Director de Unitronics Information Management.

18:15h. Coloquio.

18:20h. **Ponencia: Soluciones de seguridad a medida en 20:20 Mobile Group: una apuesta por el software de código abierto.**
Ponentes:
• **César Colado Rodríguez**, Director de IT de 20:20 Mobile Group.
• **Joaquín Crespo Pérez**, Responsable de Producción. Subdirección de Seguridad de Grupo Gesfor.

18:55h. Coloquio.

19:00h. Fin de la segunda jornada.

20:00h. **Cena de la Seguridad y entrega de los VII Premios SIC.**

FERROVIAL: LA GESTIÓN DE VULNERABILIDADES COMO PROCESO CONTINUO

Sinopsis: El Departamento de Seguridad de la Información de Ferrovial, dependiente de la Dirección de Control y Gestión de la Dirección General de Sistemas de Información, ha establecido, a través del Plan Director de Seguridad, la estrategia de seguridad de la compañía, alineada con sus objetivos tecnológicos, funcionales y estratégicos y considerando los requisitos de tipo legal a los que se encuentra sometido su modelo de negocio en relación con la explotación de las tecnologías de la información. Dentro del Plan Director de Seguridad, Ferrovial ha abordado un proyecto a través del cual se establecen las bases para construir sistemas seguros. Dicho objetivo general se vertebra en tres ejes: definición de guías para la configuración segura de sistemas, elaboración de guías para el desarrollo seguro de los nuevos Sistemas de Información e implantación de una herramienta que permita automatizar el proceso de comprobación del estado de los sistemas y de cumplimiento de las políticas internas de seguridad.

Ponentes:

• **Juan Cobo Páez** es Jefe del Departamento de Seguridad de la Información y Continuidad de Negocio de Ferrovial. Ingeniero Técnico Informático por la Universidad Politécnica de Madrid y PDD por IESE, dispone también de las certificaciones CISA y CISM de ISACA. Tiene más de 18 años de experiencia en el sector de las TI, en los que ha trabajado en compañías tales como Indra, IECISA o Telefónica y gran experiencia en la definición, despliegue y evolución de marcos, modelos y procesos de organización y control de la función de TI. En 2005 se incorporó a Ferrovial.

• **Juan Ramón Fontán Lago** es Senior Manager dentro de la práctica IT Risk and Assurance (ITRA) de Ernst & Young, y Responsable de la red de Centros Avanzados de Seguridad de esta firma en España. Fontán Lago, Ingeniero de Telecomunicaciones por la Universidad de Vigo y en posesión de las certificaciones CISA, CISM, CISSP e ISO 27001 Lead Auditor, ha desarrollado su carrera profesional en compañías como Symantec –donde dirigió la práctica de Consultoría de Seguridad–, Deloitte y Arthur Andersen.

EL PROCESO DE AUTORIZACIÓN COMO MARCO INTEGRADOR DE APLICACIONES CORPORATIVAS. EXPERIENCIA DE GENERALI E IBM EN GESTIÓN DE ACCESOS WEB

Sinopsis: IBM y Generali presentarán el proyecto de Gestión de Accesos a las aplicaciones web que Generali implantó hace 7 años con la tecnología Tivoli Access Manager. Además de los aspectos de estrategia de sistemas y los puramente relacionados con seguridad y cumplimiento normativo, se revisarán otros beneficios aportados, como son la mejora de rendimiento de las aplicaciones; la habilitación de sistemas de auditoría y seguimiento; la facilidad de integración de las aplicaciones *legacy* en un proceso y sistema de acceso a la web diseñado desde el principio, y la transparencia del sistema para empleados, administradores y desarrolladores.

Ponentes:

• **Josep Guijarro García** es Jefe de Proyecto de Seguridad en el departamento de Supervisión de Servicio y Seguridad de Generali España. Licenciado en Filosofía y Ciencias de la Educación (Sección de Psicología) por la Universidad de Valencia, Guijarro García cuenta con la titulación CISA de ISACA. Vinculado al ámbito de las TI desde hace más de 25 años, ha ejercido su actividad profesional sucesivamente en las áreas de Desarrollo de Aplicaciones, Estudios y Metodologías, y Seguridad.

• **Vicente Gozalbo Moragrega** es Responsable de ventas de productos de Seguridad Tivoli en IBM España, donde ha desempeñado su trabajo en distintas posiciones desde 2007, partiendo como Gerente de Desarrollo de Negocio de Servicios Gestionados de Seguridad. Gozalbo posee una experiencia en el sector de la seguridad TI de más de 10 años, habiendo desarrollado su carrera en compañías como RSA Security (responsable para España y Portugal) o Selesta (como Gerente de preventa de la unidad de negocio de Seguridad), y anteriormente en Bull, BMC Software e IBM Global Services. Por su experiencia, tiene un profundo conocimiento en áreas como las de gestión de identidades y SSO, gestión de accesos a la web, sistemas de autenticación robusta, protección de seguridad perimetral, forénsica, correlación y gestión de eventos de seguridad y herramientas de análisis de cumplimiento normativo.

PREVENCIÓN DEL FRAUDE EN LÍNEA. APROXIMACIÓN PRAGMÁTICA BASADA EN EL CRM DE SEGURIDAD

Sinopsis: Desde hace ya varios años el uso de la banca a distancia se ha extendido y universalizado, y sus usuarios, cada vez más, disfrutan de las ventajas, flexibilidad, comodidad e inmediatez que el canal conlleva. Ahora bien, esta realidad también trae consigo otros aspectos no tan positivos que las entidades financieras han de gestionar, como el crecimiento exponencial de los riesgos inherentes al canal; como el *efraude* y la suplantación de los clientes. Aspectos que los "amigos de lo ajeno" no han dudado en explotar y profesionalizar, principalmente mediante técnicas de *phishing* y/o caballos de Troya bancarios, con el fin de obtener rápidos y cómodos réditos. Hasta la fecha, las áreas de control y seguridad de las entidades financieras lidiaban con estas amenazas a través de la experiencia pasada, es decir, sé qué es malo y lo busco. Este planteamiento, si bien efectivo y nada desdeñable, implica ir siempre un paso por detrás, amén de la exposición al riesgo que conlleva el intervalo de tiempo que pasa entre que se pone en producción un nuevo vector de ataque y la capacidad para detectarlo y controlarlo. Por ello, avanzar en nuevos sistemas de control, que no se preocupen en saber qué es malo, sino en lo que es normal, permitiría, por primera vez, no tener que estar un paso por detrás. Bajo esta premisa se concibe y desarrolla el concepto CRM de Seguridad.

Ponente:

• **Jesús Milán Lobo** es Director de Riesgos Tecnológicos y Seguridad Informática en Bankinter. Ingeniero en Informática con especialidad en Gestión por el ICAI-ICADE, cuenta con la certificación CISM y es Lead Auditor ISO27001 - BS25999. Es miembro del Subcomité Nacional de Seguridad de las TI (CTN 71 / SC27) y miembro WG1, y colaborador en la redacción de normas internacionales. Igualmente, es miembro de la Junta Directiva de ISMS Forum Spain; de la Comisión de Seguridad del Capítulo de Madrid de ISACA; y del Comité de Seguridad Informática y de la Comisión de Seguridad, Prevención y Fraude del Centro de Cooperación Interbancaria.

LOS TIEMPOS CAMBIAN. USO INTELIGENTE DE LA INFORMACIÓN DE SEGURIDAD

Sinopsis: La realidad externa, el entorno corporativo y las necesidades y objetivos de la propia empresa ponen retos que deben saberse gestionar. Es importante conocer hacia dónde se quiere ir y qué prioridades se deben tomar para ser útil a la compañía. El uso inteligente de la información de seguridad, tanto para gestionar los riesgos de la información como para apoyar los objetivos corporativos, se hace más y más necesario. En la ponencia, Juanes Calvo explicará cómo Ericsson afronta la gestión de la información de seguridad para la toma de decisiones, y cómo justifica su utilidad.

Ponente:

• **Casimiro Juanes Calvo** es Responsable de Seguridad TI del grupo Ericsson. Nombrado para dicho puesto en enero de 2008, trasladó su residencia a Estocolmo (Suecia), sede central de la compañía. Ingeniero Técnico Superior de Telecomunicaciones por la Universidad Politécnica de Madrid, Juanes Calvo ha estado ligado en toda su carrera profesional –más de diez años–, a Ericsson, habiendo ocupado diversos puestos, principalmente en el área de IT y de seguridad, siendo anteriormente el Responsable de Seguridad para la Market Unit Iberia (España y Portugal). Colaborador de SIC y ponente en Securmática, cuenta con la certificación CISSP, y la concentración de gestión de seguridad ISSMP, siendo colaborador de ISC^2 en la preparación de los exámenes. Actualmente forma parte del Permanent Stakeholders' Group (PSG) de la Agencia Europea de Seguridad de las Redes y la Información, ENISA.

CEPSA: EXTERNALIZACIÓN DE LA SEGURIDAD TI A ESCALA INTERNACIONAL

Sinopsis: CEPSA, tras 4 años de consolidación de la gestión y operación de la seguridad del Grupo en España y Portugal, apoyado en la tecnología y servicios del Centro de Operaciones de Seguridad (SOC) de Telefónica Grandes Clientes, afronta la internacionalización de su modelo al resto del Grupo CEPSA en 3 continentes, con una enorme diversidad de comunicaciones, arquitecturas y organizaciones en cada país, y todo ello extendiendo el modelo de servicios de Seguridad operativo en España de la mano de Telefónica Grandes Clientes, con toda la normalización de plataformas, servicios y planes de acción en 24x7 y con la misma calidad de servicio y tiempos de atención que en España, pero trasladada a África, LATAM y América del Norte y Europa.

Ponentes:

• **Rafael Hernández González** es Responsable de Seguridad IT en CEPSA. Ingeniero Superior de Telecomunicación por la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid, está especializado en el área de Telemática. Ha desarrollado su carrera profesional en CEPSA, siempre asociado al ámbito de los Sistemas de Información, participando en proyectos de integración entre los sistemas de fabricación y los sistemas TIC, así como en la definición e implantación del Plan Director de Seguridad del Grupo CEPSA (2003). Ha llevado a cabo el desarrollo de los Servicios de Seguridad Gestionada en CEPSA.

• **Juan Miguel Velasco López-Urda** es actualmente Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Clientes de Telefónica España. Anteriormente ejerció en Telefónica Empresas como Subdirector de Arquitecturas y Servicios de Seguridad de la Línea de Outsourcing, Subdirector de Arquitecturas y Planificación de Infraestructuras, y antes como Subdirector de Ingeniería de Proyectos y Servicios de Protección de la Información de la UN Hosting y ASP, así como CTO Director Técnico y de Consultoría de la Agencia de Certificación Electrónica (ACE), sociedad filial de Telefónica DataCorp. Cursó sus estudios de Informática en la Universidad Politécnica de Madrid y, entre otros, es Master Executive de Gestión Empresarial por INSEAD-EUROFORUM.

MONITORIZACIÓN Y CONTROL DE EVENTOS PARA LA GESTIÓN INTEGRAL DE LA SEGURIDAD. LA EXPERIENCIA EN ONO

Sinopsis: ONO posee un Centro de Control de Seguridad (CCS) operado y gestionado internamente, donde realiza actividades de supervisión, monitorización y gestión en tiempo real de incidentes de seguridad física y seguridad lógica con el objetivo de poder garantizar la protección de sus infraestructuras críticas. Dentro de su plan estratégico, la compañía tiene como objetivo explotar los servicios del Centro de Control de Seguridad en modo 24x7 y ofrecer estos servicios a sus clientes como valor añadido sobre los tradicionales servicios de líneas e infraestructuras de comunicación. Durante el último año, ONO ha desarrollado un proyecto de revisión, diseño, implantación y despliegue de mejoras sobre las herramientas de Gestión de Seguridad (SIM) que ayudará a la consecución de sus objetivos estratégicos. La ponencia describirá el proceso llevado a cabo, la metodología utilizada y destacará las iniciativas de implantación y despliegue de mejoras más relevantes: la integración de las infraestructuras críticas y los sistemas de seguridad física en la plataforma de monitorización, y la renovación tecnológica con un nuevo equipamiento más potente y con alta disponibilidad que proporcione la capacidad requerida y ofrezca con garantías los servicios del CCS.

Ponentes:

• **Francisco Javier Santos Ortega** es Gerente de Gestión Operativa de Seguridad de ONO, puesto que desempeña desde octubre de 2008 y donde es responsable de la operación de seguridad de ONO tanto lógica como física, así como de la Gestión del Fraude tecnológico y de los Requerimientos de Información. Ingeniero Industrial Eléctrico con especialización en Electrónica, Informática y Sistemas de Control por la Universidad de Zaragoza, tiene más de 15 años de experiencia en seguridad de la información. Antes de su incorporación a ONO, trabajó en Wisekey, Ernst &Young, Atos Origin, SchlumbergerSema y Europa Management Consulting, siempre en el ámbito de la consultoría de seguridad de la información. Posee diferentes certificaciones, entre las que destacan CISM e ITIL.

• **Félix Martín Rodríguez** es Gerente de la práctica de Seguridad y Gestión de Riesgos de HP TS. Se incorporó como consultor de seguridad en el departamento de consultoría de HP en 1999. Ingeniero de Telecomunicaciones y Executive MBA por el Instituto de Empresa, tiene más de quince años de experiencia en seguridad de la información. Posee diferentes certificaciones, entre las que destacan las siguientes: CISSP, PMP e ITIL Service Manager, y dispone también de amplia experiencia en la implantación de Sistemas de Gestión de Seguridad de la Información-SGSI. Su foco actual es el desarrollo y la dirección de servicios de seguridad para clientes de HP. Antes de unirse a Hewlett-Packard, trabajó para CRISA Astrium España, empresa de la industria aeroespacial, donde fue el responsable de Sistemas de Información y CSO de la compañía.

EL CENTRO DE SEGURIDAD DE LA INFORMACIÓN DE CATALUÑA-CESICAT, UN AÑO DESPUÉS

Sinopsis: El Centro de Seguridad de la Información de Cataluña (CESICAT) es el organismo ejecutor del Plan Nacional de impulso de la seguridad TIC aprobado por el gobierno de la Generalitat de Cataluña en marzo de

2009. La misión de este plan es la de garantizar una Sociedad de la Información Segura Catalana para todos, operando un centro de seguridad, como herramienta para la generación de un tejido empresarial catalán de aplicaciones y servicios de seguridad TIC que sea referente nacional e internacional. Entre los objetivos estratégicos de CESICAT están los de crear un CERT para dar respuesta a los diferentes incidentes de seguridad, un Centro de Operaciones de Seguridad (SOC) para prestar servicios de seguridad gestionada con el propósito de aumentar el nivel de seguridad, y la realización de programas de difusión, comunicación y concienciación a las diferentes comunidades a quien se dirige.

Ponentes:

• **Josué Sallent i Ribes** es Director General de la Sociedad de la Información de la Secretaría de Telecomunicaciones y Sociedad de la Información del Departamento de Gobernación y Administraciones Públicas de la Generalitat de Cataluña, y Presidente de la comisión ejecutiva del Centro de Seguridad de la Información de Cataluña (CESICAT). Doctor en Ciencias Físicas por la Universidad de Barcelona y Diplomado en Ciencias Empresariales por la Universitat Oberta de Catalunya, es Profesor Asociado de la Universidad Pompeu Fabra. Tiene una larga experiencia profesional en el ámbito de las TIC, tras su paso por el Grupo Telefónica y como gerente de negocio en DOXA. Ha sido Coordinador de Proyectos Estratégicos del CTTI y Coordinador del Plan Director de Infraestructuras de Telecomunicaciones del 2004 al 2006.

• **Jordi Rodríguez Mauri** es Director de Unitronics Information Management. Ingeniero Técnico Informático y Master en Gestión y Dirección de Empresas por el ICT/UPC, cuenta con más de 20 años de experiencia en el sector de las TI, 15 de ellos en el seno del Grupo ADD. Rodríguez ha ocupado con anterioridad la Dirección de Desarrollo de Nuevos Mercados del Grupo ADD (1999-2001), la Dirección de la oficina de ADD en Portugal (2001-2002), así como la Dirección de Davinci Consulting en Madrid (2002-2004) y la Dirección de la sede de Barcelona (2004-2008). A finales del 2008, Davinci es absorbida por Unitronics y se convierte en la marca de Seguridad del Grupo Unitronics. A partir de entonces pasa a ocupar las siguientes responsabilidades: Director de Seguridad y Contenidos (2009) y actualmente Director de la unidad de negocio Unitronics Information Management.

SOLUCIONES DE SEGURIDAD A MEDIDA EN 20:20 MOBILE GROUP: UNA APUESTA POR EL SOFTWARE DE CÓDIGO ABIERTO

Sinopsis: Todas las organizaciones requieren de soluciones tecnológicas seguras, robustas, y fiables que sirvan de base para ofrecer servicios de calidad a sus clientes finales al tiempo que se protege la información de la compañía. ¿Es posible que este tipo de soluciones estén basadas en software de código abierto? ¿Qué ventajas y desventajas suponen este tipo de soluciones? ¿Hay diferencias al abordar proyectos con esta base tecnológica? Analizando un caso particular de apuesta decidida por el software de código abierto dentro de una empresa internacional, se valorarán las circunstancias en las que este tipo de soluciones pueden ser las más adecuadas. Igualmente se describirán otros aspectos relevantes, como el papel y la presencia de los responsables TIC en los órganos principales de la compañía, la definición de una estrategia clara, y el apoyo tecnológico de integradores de confianza.

Ponentes:

• **César Colado Rodríguez** es Director de IT de la filial española de 20:20 Mobile Group, donde se incorporó en el año 2008. Ingeniero de Telecomunicaciones por la UPM y Executive MBA por el Instituto de Empresa, cuenta con más de 10 años de experiencia en el sector de las TI en distintas áreas: redes, seguridad y desarrollo de aplicaciones específicas para empresas de telecomunicación. Anteriormente trabajó como Jefe de Proyecto en HP realizando proyectos de mediación y gestión de facturación para operadoras de telecomunicaciones.

• **Joaquín Crespo Pérez** es Responsable de Producción en la Subdirección de seguridad de Grupo Gesfor. Ingeniero Técnico de Telecomunicación con la especialidad en Telemática por la Universidad de Alcalá de Henares, cuenta con 10 años de experiencia en el sector de la Seguridad IT. Comenzó su carrera profesional en el año 2000 en SGI (Soluciones Globales Internet), como Ingeniero de Proyectos del Área de Seguridad Lógica. Posteriormente se incorporó a Germinus XXI, (desde 2006 dentro del Grupo Gesfor) como Jefe de Proyectos e Ingeniero Senior de la División de Seguridad e Infraestructuras de Redes Corporativas. Desde 2008 realiza la coordinación técnica y administrativa de todas las tareas de producción del área.

DEBATE

LA DINÁMICA DE RELACIÓN ENTRE LA FUNCIÓN DE SEGURIDAD EN TECNOLOGÍA Y SISTEMAS Y LAS CORPORATIVAS DE AUDITORÍA Y RIESGOS

Proposición: Al igual que sucede en otros frentes derivados de la actividad de las organizaciones, el de la seguridad de la información tratada en sistemas tecnológicos se cimenta en la dinámica de relación entre la función de Seguridad TIC y aquellas otras de control, también de alcance corporativo, como son la de Auditoría y la de Riesgos. El objetivo del debate es poner en valor las finalidades de cada uno de estos actores e intentar marcar las fronteras de sus atribuciones en la consecución del objetivo común perseguido: la eficiencia en la protección de los datos.

Intervienen:

• **Carlos Bachmaier Johanning** es Doctor Ingeniero Aeronáutico por la UPM, Profesor Titular de Universidad (excedente) y Diplomado en el Programa de Dirección en Responsabilidad Corporativa por el Instituto de Empresa (primera convocatoria). Su actividad profesional actual se desarrolla en Sistemas Técnicos de Loterías del Estado (STL) y Loterías y Apuestas del Estado (LAE), y está centrada en la Gestión Integrada (procesos, calidad y seguridad de la información) y la Gestión de Riesgo Corporativo, que incluye la función de Auditoría Interna TIC/Seguridad de la Información. Fue socio fundador de GMV y SGI Soluciones Globales Internet. Tras más de veinte años de actividad profesional se incorporó a STL en 1998. Miembro de ISACA, mantiene activas sus certificaciones CGEIT, CISA y CISM. Publica regularmente artículos profesionales, y ejerce de profesor sobre seguridad, auditoría y buen gobierno corporativo y de sistemas de información en cursos de másteres y de preparación CISA y CISM. Es representante de LAE en el SC27 de AENOR y en el Grupo de Trabajo de Seguridad y Gestión de Riesgos de la Asociación Mundial de Loterías. También es Auditor Jefe SGSI (a falta de prácticas).

• **Mariano de la Cruz Molina** es Senior Manager de Seguridad Corporativa de Grupo Santander y Responsable de la Estrategia de Seguridad. Licenciado en Informática por la Universidad Politécnica de Madrid, ha participado en diversos programas de desarrollo directivo del Grupo Santander, entre los que cabe destacar el impartido por el Instituto de Empresa. Dispone de un amplio conocimiento en el sector de las TIC y cuenta con una dilatada experiencia de más de 15 años en diferentes disciplinas de la seguridad de la información, ocupando diversos puestos de responsabilidad, como el de Responsable de Infraestructuras de Seguridad, Responsable de Análisis de Riesgos de Seguridad y Responsable de Estrategia de Seguridad Corporativa. Ha participado activamente, entre otros, en la creación y el despliegue del Modelo de Seguridad del Grupo Santander, en el desarrollo de planes corporativos para la prevención y detección del fraude electrónico y en el desarrollo de los Planes Directores de Seguridad del Grupo Santander. Antes de su incorporación a Grupo Santander trabajó en otras prestigiosas firmas, entre las que destaca IBM, estando ligado al desarrollo del comercio electrónico, las tecnologías Internet y la seguridad.

• **Carolina de Oro Gómez** es IT Compliance & Risk Management Manager para la Región Mediterránea y Latinoamérica de Axa Seguros. De Oro realizó sus estudios de Ingeniería Superior de Telecomunicación en la UPM y formación de postgrado en Administración de Empresas por la Universidad de Alcalá de Henares. Instructora habitual de diversos cursos relacionados con la seguridad lógica, posee amplia experiencia en proyectos de alto valor añadido en el campo TI. Con anterioridad ha prestado sus servicios en BT Global Services como Responsable de Desarrollo de Negocio del área de Seguridad BCSG (Business Continuity, Security & Governance) y fue Jefe de Producto y Coordinadora de la unidad de negocio de seguridad de Siemens.

• **Alejandro Rembado Mendizábal** es Director Corporativo de Auditoría TI de Telefónica. Nacido en Buenos Aires (Argentina), se graduó como Licenciado en Informática en la Universidad Argentina de la Empresa (UADE), donde posteriormente cursó el Master en Administración Estratégica, y en la Universidad Torcuato di Tella (UTDT) la especialización en Economía. Dispone de la certificación internacional CGEIT (Certified in the Governance of Enterprise IT). En el año 1995 ingresó en Telefónica de Argentina donde alcanzó la Gerencia en Auditoría Informática, para posteriormente ser convocado desde la Corporación en España a efectos de desarrollar la actividad en todo el Grupo Internacional. Desde noviembre de 2008 es Presidente de ISACA Capítulo de Madrid. Ha sido ponente en numerosos congresos sobre auditoría (IIR, Marcus Evans, ISACA, etc.). Rembado es coautor del libro "El Gobierno de las Tecnologías y Los Sistemas de Información" (ed. RA-MA, Madrid 2007) y ha apoyado la publicación por el Capítulo de Madrid de ISACA del volumen "Marco para la Auditoría de los Sistemas de Información".

TERCER MÓDULO 29 de abril

09:15h. Entrega de documentación.
09:30h. **Ponencia: La concentración de riesgos en grandes centros corporativos: Plan de Continuidad de Negocio de Distrito C.**
Ponentes:
• **José Miguel González González**, Gerente de Seguridad Lógica de Telefónica de España, S.A.U.
• **Juan José Míguez Iglesias**, Director del Área de Riesgos Tecnológicos de PricewaterhouseCoopers.
10:05h. Coloquio.
10:10h. **Ponencia: Análisis de riesgos de seguridad de la información en la externalización de la infraestructura y operativa TI del Grupo FCC.**
Ponente: Gianluca D'Antonio, Director de Seguridad de la Información y Gestión de Riesgos del Grupo FCC.
10:45h. Coloquio.
10:50h. **Ponencia: HERMES: Sistema para la Gestión del Catálogo Nacional de Infraestructuras Estratégicas.**
Ponentes:
• **Miguel Ángel Abad Arranz**, Jefe de Sección de Seguridad TIC. Centro Nacional de Protección de Infraestructuras Críticas. CNPIC.
• **Jorge López Hernández-Ardieta**, Ingeniero Senior. Sistemas de Seguridad. Indra.
11:25h. Coloquio.
11:30h. Pausa-café.
12:00h. **Ponencia: Iberdrola: gestión de las infraestructuras críticas de información.**
Ponente: Francisco Javier García Carmona, Director de Seguridad de la Información y las Comunicaciones del Grupo Iberdrola.
12:35h. Coloquio.
12:40h. **Debate: La batalla de las evidencias.**
Participantes:
• **José María Anguiano Jiménez**, Socio Director del Departamento de Nuevas Tecnologías de J&A Garrigues Abogados.
• **José Antonio del Cerro Esteban**, Fiscal. Secretaría Técnica. Fiscalía General del Estado.
• **Paloma Llaneza González**, Presidenta de la Asociación Española de Evidencias Electrónicas, AEDEL.
• **Pedro Pablo López Bernal**, Gerente de Infraestructura de Seguridad, Auditoría y Normalización. Rural Servicios Informáticos.
• **Juan Salom Clotet**, Jefe del Grupo de Delitos Telemáticos (GDT) de la Guardia Civil.
14:05h. Almuerzo.
16:00h. **Ponencia: Hacia una sociedad de la información más confiable, Plan Avanza2.**
Ponente: Marcos Gómez Hidalgo, Subdirector de Programas de INTECO, Instituto Nacional de Tecnologías de la Comunicación.
16:35h. Coloquio.
16:40h. **Ponencia: Seguridad integral de los puestos de trabajo de usuario de Osakidetza-Servicio Vasco de Salud.**
Ponentes:
• **Alberto González Hierro**, Responsable de Microinformática y Seguridad. Osakidetza-Servicio Vasco de Salud.
• **Rodrigo Blanco Rincón**, Director de la Oficina de Proyectos de Bull España.
17:15h. Coloquio.
17:20h. Pausa-café.
17:45h. **Ponencia: El control de la seguridad de la información en la web 2.0.**
Ponente: Jorge Dávila Muro, Consultor Independiente y Director del Laboratorio de Criptografía LSIIS – Facultad de Informática de la Universidad Politécnica de Madrid.
18:20h. Coloquio.
18:25h. **Clausura de Securmática 2010.**

LA CONCENTRACIÓN DE RIESGOS EN GRANDES CENTROS CORPORATIVOS: EL PLAN DE CONTINUIDAD DE NEGOCIO DE DISTRITO C

Sinopsis: La tendencia actual en las grandes organizaciones es la creación de grandes centros corporativos con el objetivo de maximizar las sinergias derivadas de la concentración del personal y, por lo tanto, de las operaciones del negocio, a la vez que se minimizan los costes derivados de las infraestructuras y su mantenimiento. Se trata, en muchas ocasiones, de algo más que una agrupación de edificios: los nuevos centros corporativos se asemejan cada vez más a pequeñas ciudades. Este escenario de concentración de las operaciones del negocio acarrea, asimismo, una concentración de los riesgos a los que se exponen las operaciones críticas del negocio. En este sentido, la materialización de una amenaza podría generar un impacto que afectase seriamente la sostenibilidad del negocio. Para mitigar este riesgo se hace necesario abordar un Plan de Continuidad de Negocio.

Ponentes:

• **José Miguel González González** es Gerente de Seguridad Lógica de Telefónica España. Certificado CISM, cuenta además con 23 años de experiencia en TI. Su trayectoria profesional abarca la operación, la administración, el desarrollo, la tecnología y la arquitectura de sistemas, en áreas tales como comunicaciones, bases de datos, sistemas operativos y *middleware*, en entornos *mainframe* y *open*, ocupándose de la gestión e implementación de la seguridad de TI durante 7 años. En el terreno de la continuidad de negocio implantó el Plan de Contingencia del CPD de sistemas de gestión de Telefónica de España.

• **Juan José Míguez Iglesias** es Director del Área de Riesgos Tecnológicos de PricewaterhouseCoopers. Es Ingeniero de Telecomunicación en la especialidad de Telemática y certificado como CISA, CISM y CGEIT por ISACA, y Lead Auditor ISO 27001 y Lead Auditor BS25999-2 por BSI. A lo largo de su trayectoria profesional de más de 14 años en el mundo de la consultoría de seguridad y auditoría informática ha realizado multitud de trabajos, entre los que cabe destacar: Planes Directores de Seguridad, Planes de Continuidad de Negocio, Análisis de Riesgos, implantación de Gestión de Identidades o Auditorías técnicas informáticas en grandes compañías de diversos sectores a nivel nacional e internacional.

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN LA EXTERNALIZACIÓN DE LA INFRAESTRUCTURA Y OPERATIVA TI DEL GRUPO FCC

Sinopsis: La ponencia ilustrará los productos de las fases finales del proyecto llevado a cabo en FCC a lo largo del segundo semestre de 2009, orientado a analizar los riesgos de seguridad de la información en el contexto de su iniciativa de externalización de la infraestructura y operativa de TI: definición de una metodología de análisis de riesgos orientada a servicios IT, basada en un catálogo específico de amenazas derivadas de la gestión externalizada de servicios TIC. La catalogación de dichas amenazas (41 en total) se ha realizado teniendo como referencia los dominios clásicos de los marcos de gobierno TIC.

Ponente:

• **Gianluca D'Antonio** es Director de Servicio de Seguridad de la Información y Gestión de Riesgos del Grupo FCC. Licenciado en Derecho (experto en nuevas tecnologías y en seguridad de la información) y PDD por el IESE Business School, es fundador y presidente de ISMS Forum Spain, capítulo español de ISMS International User Group, además de miembro del Security and Risk Management Council de Forrester. Posee las certificaciones CISM, CISA y CGEIT, de ISACA, y es Lead Auditor ISO 27001 acreditado por IRCA. Su experiencia profesional se inició en Motorola España como Security Advisor. Posteriormente fue consultor *senior* en Centrisa, y hasta finales de 2005, año en el que se incorporó al Grupo FCC, fue Responsable de Protección y Recuperación de Datos en el Grupo DIA. Actualmente forma parte del Permanent Stakeholders' Group (PSG) de la Agencia Europea de Seguridad de las Redes y la Información, ENISA.

HERMES: SISTEMA PARA LA GESTIÓN DEL CATÁLOGO NACIONAL DE INFRAESTRUCTURAS ESTRATÉGICAS

Sinopsis: El Proyecto HERMES surge con el objetivo de desarrollar un sistema robusto que permita al Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) la gestión eficiente del Catálogo Nacional de Infraestructuras. Según el Acuerdo de Consejo de Ministros de 2 de noviembre, el Catálogo tiene consideración de secreto. No obstante, debido a que uno de los pilares en el que se fundamentan las actividades del CNPIC es el intercambio de información, ha sido necesaria la división del Sistema en dos plataformas bien diferenciadas que puedan gestionar distintos niveles de clasificación de la información. Ello posibilita, por un lado, la colaboración de todos los agentes involucrados en la gestión de las Infraestructuras y su seguridad, y por otro, que el acceso a la información estratégica y sensible del Catálogo esté limitado al CNPIC. El Sistema HERMES se ha diseñado cumpliendo unos requisitos de seguridad fuertes. Cada Plataforma se certificará de acuerdo a la norma *Common Criteria*, con el objetivo final de obtener la Acreditación del Centro Criptológico Nacional (CCN) para manejar información nacional clasificada en el nivel que corresponda.

Ponentes:

• **Miguel Ángel Abad Arranz** es Jefe de la Sección de Seguridad TIC del Centro Nacional de Protección de Infraestructuras Críticas, CNPIC. Capitán de la Guardia Civil e Ingeniero Informático por la Universidad de Comillas ICAI-ICADE, posee el título de Máster de Investigación en Inteligencia Artificial por la Universidad Politécnica de Madrid, y actualmente se encuentra desarrollando la tesis doctoral en el ámbito de las "Tecnologías para el Desarrollo de Sistemas de Software Complejos". Trabajó desde 1999 en distintas compañías del sector tecnológico desempeñando distintas funciones técnicas en proyectos dirigidos a operadores de telefonía móvil principalmente. En el año 2005 ingresó en la Guardia Civil y fue destinado al Servicio de Informática de este Cuerpo.

• **Jorge López Hernández-Ardieta** es Ingeniero Senior en la División de Seguridad de Indra Sistemas. Ingeniero Informático por la UAM (2003), obtuvo el Diploma de Estudios Avanzados en el programa de Doctorado de Ingeniería Informática y Telecomunicaciones en el año 2005 por la misma Universidad. Es Profesor Asociado y miembro del Grupo de Investigación en Seguridad de la Universidad Carlos III de Madrid, donde se encuentra finalizando su tesis doctoral. Ha trabajado en consultoría e investigación en seguridad desde el año 2002, participando en diversos proyectos de I+D+i tanto nacionales como europeos. Posee diversas publicaciones científicas en su haber, así como una patente solicitada en la USPTO. Participa en múltiples iniciativas industriales, siendo miembro del IEEE, IETF y de IRTF.

IBERDROLA: GESTIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN

Sinopsis: La aparición de las nuevas tecnologías en la vida diaria de las personas en todos los ámbitos productivos y sectores económicos, incluyendo la Administración, ha traído también consigo la aparición de nuevos riesgos que tienen su impacto en nuestra sociedad. Una de las amenazas emergentes asociadas a la dependencia de los sistemas de las Tecnologías de la Información y las Comunicaciones es la posible utilización de los medios informáticos asociados a las recientemente definidas infraestructuras críticas de un país para la realización de delitos, y más en concreto, su utilización por grupos terroristas con el objeto de realizar atentados que provoquen el máximo daño a la sociedad y consecuentemente a la economía de un país. A partir de este punto tenemos que desgranar tres nuevos conceptos: "infraestructuras esenciales, infraestructuras críticas, interdependencias". Además, replantearnos la validez de los modelos actuales de riesgos y vulnerabilidades así como su evaluación; en fin, todo un nuevo mundo.

Ponente:

• **Francisco Javier García Carmona** es Director del Departamento de Seguridad de la Información y las Comunicaciones de Iberdrola. Maestro Industrial (Eléctrica), Ingeniero de Telecomunicaciones y Director de Seguridad Privada por el Ministerio del Interior, García Carmona inició su actividad en el sector de las Telecomunicaciones en 1979, en cuyo ámbito ha prestado servicios en áreas de implantación y mantenimiento en sistemas de telecontrol y voz, dirección de Redes y Sistemas y Gerencia en diversas compañías de Telecomunicaciones. En 2000 se incorporó al ramo de la seguridad TIC como Director de Operaciones de una compañía de desarrollo de software de protección en el sector de Defensa. En el año 2001 se incorporó a Iberdrola como Director del Departamento de Seguridad de la Información y las Comunicaciones, integrado en la División de Seguridad Corporativa.

HACIA UNA SOCIEDAD DE LA INFORMACIÓN MÁS CONFIABLE, PLAN AVANZA2

Sinopsis: El horizonte que se vislumbraba hace tan solo un lustro ya está aquí con toda su realidad. En el 2005 se empezaron a sentar las bases de un ambicioso y estratégico plan que debía armonizar numerosas actuaciones y proyectos enfocados principalmente a fomentar el desarrollo de una Sociedad de la Información convergente con los principales líderes europeos: el Plan Avanza. Este Plan se dotaba y articulaba con piezas esenciales en el ámbito económico, con importantes dotaciones, pero también en el ámbito tecnológico y legislativo. Fruto de estos esfuerzos y ya en el ámbito de la confianza nacía y daban sus primeros pasos potentes proyectos como el DNIe en la identidad digital, o el Centro de Respuesta a Incidentes de Seguridad de la Información INTECO-CERT y la Oficina de Seguridad del Internauta en la Seguridad de la Información. Echando la mirada atrás se ha desarrollado un importante esfuerzo, pero ahora queda con este Plan Avanza2 una tarea de consolidación, y que los más de 25 millones de internautas, los más de 15 millones de ciudadanos con DNIe, y las más de 3 millones y medio de empresas, confíen en esta Sociedad de la Información que se les brinda y de la que forman parte ineludiblemente. Pero esta vez habrá que conjugar los tres pilares fundamentales de la confianza: la seguridad, la accesibilidad y la calidad. Con este nuevo horizonte, y sin dejar de lado las importantes influencias derivadas de los Esquemas Nacionales de Seguridad e Interoperabilidad, y la protección de las Infraestructuras Críticas, habrá que seguir avanzando y responder decididamente a las preguntas y necesidades que se planteen.

Ponente:

• **Marcos Gómez Hidalgo** es Subdirector de Programas de INTECO. Licenciado en CC. Matemáticas por la UCM, inició su carrera profesional en el ámbito de los sistemas de información en Atos Origin como administrador de bases de datos. En Red.es desempeñó diversos puestos de responsabilidad, entre ellos el de Responsable de Sistemas de Información. Ya en el ámbito de la seguridad de la información asumió también en Red.es el puesto de Responsable del Centro de Alerta Temprana Antivirus. Continúa su carrera actualmente como Subdirector de Programas de INTECO, sociedad dependiente del Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, dirigiendo entre otros proyectos el INTECO-CERT y la Oficina de Seguridad del Internauta. Ha sido también profesor de Ingeniería Informática en la Universidad Camilo José Cela, imparte clases en diversos másteres y seminarios de seguridad de la información, y actualmente forma parte del Permanent Stakeholders' Group (PSG) de la Agencia Europea de Seguridad de las Redes y la Información, ENISA.

SEGURIDAD INTEGRAL DE LOS PUESTOS DE TRABAJO DE USUARIO DE OSAKIDETZA-SERVICIO VASCO DE SALUD

Sinopsis: Osakidetza, Servicio Vasco de Salud, ha puesto en marcha un proyecto de seguridad integral para garantizar la seguridad de toda su red. El objetivo es proteger tanto los servidores como los puestos de trabajo a través de la detección, bloqueo y reacción ante cualquier tipo de amenaza de seguridad. Se protege tanto frente a virus, código malicioso y otros ataques (externos o internos), como frente a amenazas contra la integridad y confidencialidad de la información, tanto transmitida como almacenada. La solución cumple con todos los requisitos internos y regulatorios; es flexible, escalable y reduce costes al centralizar la gestión en una única plataforma.

Ponentes:

• **Alberto González Hierro** es actualmente Responsable de Microinformática y de Seguridad de Microinformática en Osakidetza-Servicio Vasco de Salud. Licenciado en Informática por la Universidad de Deusto, es un profesional de amplia experiencia en la materia.

• **Rodrigo Blanco Rincón** es Director de la Oficina de Proyectos de Bull España. Ingeniero Superior de Telecomunicaciones por la Universidad Politécnica de Madrid, y Máster de Gestión y Dirección de la Seguridad de la Información por la Universidad Pontificia de Salamanca y Asimelec, está certificado como CISA por ISACA y PMP por el Project Management Institute. Colabora como profesor en el Máster de Gestión y Dirección de la Seguridad de la Información anteriormente citado, y es ponente habitual en los foros y conferencias de la industria de seguridad.

EL CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA WEB 2.0

Sinopsis: La Web 2.0 nació en 2004 y aún perdura. Se trata de un termino relacionado con aplicaciones web diseñadas para facilitar el compartir interactivamente información, la interoperabilidad global y la colaboración universal, siendo el usuario el centro neurálgico indiscutible de su diseño (software social). Ejemplos de ello los hay para aburrir: comunidades basadas en la web, servicios hospedados, aplicaciones web, redes sociales, foros para compartir vídeos y fotos, *wikis* de todo tipo, *blogs*, *mashups* y *folcsonomías*. Aunque el término 2.0 insinúa tratarse de una nueva versión de la web, en realidad no supone ninguna actualización técnica, sino una mera acumulación de cambios ideados según iban haciendo falta. Al igual que en el caso de la Web 1.0, la versión 2.0 se ha ideado de espaldas a la seguridad, por lo que carece completamente de ella; sin embargo, su carácter social ha despertado un furor desmedido que ha entrado de lleno en el mundo social y empresarial desactivando cualesquiera medidas de seguridad que se hubiesen tomado. ¿Demostrará la Web 2.0 que realmente no es necesaria la seguridad en los sistemas empresariales del futuro?

Ponente:

• **Jorge Dávila Muro** es Profesor Titular de la Facultad de Informática de la Universidad Politécnica de Madrid (UPM) y desarrolla sus actividades académicas en el ámbito de la Criptología, la Seguridad Informática y en el diseño de nuevos sistemas avanzados para la sociedad de la información. Desde 1993, el profesor Dávila dirige el Laboratorio de Criptología de la UPM en el que, además de desarrollar sus investigaciones, se dedica a la formación y capacitación de nuevos profesionales de la seguridad informática. El profesor Dávila es, desde su inicio y en concepto de experto, miembro de la representación española en el 7º Programa Marco de la UE, en el programa de Seguridad.

DEBATE

LA BATALLA DE LAS EVIDENCIAS

Proposición: El uso de la informática y las telecomunicaciones, y el éxito del medio telemático para canalizar el grueso de las relaciones en la sociedad, y particularmente aquellas en las que se ejercitan derechos y se cumplen obligaciones entre partes, ya sean éstas personas físicas o jurídicas, obliga a preparar los sistemas de información tecnológicos para que generen datos que debidamente extraídos y tratados puedan presentarse, si llega el caso, ante árbitros y tribunales para que éstos enjuicien su valoración como pruebas. ¿Qué posibilidades hay de conseguir este fin en un mundo de sistemas tecnológicos interconectados y gestionados por distintas entidades en distintos territorios? ¿Qué medidas técnicas razonables pueden tomarse para controlar este riesgo de alcance creciente?

Intervienen:

• **Jose María Anguiano Jiménez** es Socio Director del Departamento de Nuevas Tecnologías de J&A Garrigues Abogados. Asimismo, es Consejero Delegado de Logalty (*joint venture* constituida por Garrigues y T-Systems) y Secretario General de la Asociación Española de Derecho de la Propiedad Intelectual. Es igualmente colaborador habitual de varias universidades, así como conferenciante y columnista para distintos medios de comunicación.

• **José Antonio del Cerro Esteban** es Fiscal de la Secretaría Técnica de la Fiscalía General del Estado. Licenciado en Derecho, ha cursado estudios de Doctorado y Grado Académico de Experto Comunitario en la UPM. Ejerció la Abogacía en Madrid entre los años 1980 y 1985. En este último ingresa en la Carrera Fiscal, habiendo prestado servicios en las Fiscalías de Bilbao, Toledo, Madrid y en la Fiscalía Especial Antidroga. Dispone de una amplia experiencia como miembro de Tribunal de Oposiciones y Profesor de formación de cursos de acceso a la Carrera Fiscal. Ha sido Director y ponente en numerosos cursos, seminarios y proyectos nacionales e internacionales (Méjico, Uruguay, Chile, Nicaragua, Bolivia, Ecuador, Perú, Colombia y Francia) sobre delincuencia organizada, delitos contra la salud pública, blanqueo de capitales, delitos informáticos y cooperación internacional, y ha realizado publicaciones sobre drogas, blanqueo de capitales y cooperación internacional.

• **Paloma Llaneza González,** socio de Razona Legaltech, es Abogado, CISA y experta en seguridad. Editora de diversos estándares de seguridad (IEC/ISO 27004:2009, ESI TS on Registered E-Mail, y CEN CWA on Data Protection Good Practices), preside en la actualidad AEDEL (Asociación Española de Desarrollo de las Evidencias Electrónicas). Como coordinadora del Grupo Ad-Hoc del SC27 de AENOR sobre evidencias electrónicas, participa en el desarrollo de dos normas nacionales, la 71505 sobre el sistema de gestión de evidencias, y la 71506 sobre análisis forense. Actualmente está participando como experta en seguridad en diversos grupos internacionales sobre "Interoperability issues on REM", "e-signatures and e-documents Long Term Preservation", y "EU Commission Mandate on RFID".

• **Pedro Pablo López Bernal** es el Gerente de Infraestructura de Seguridad, Auditoría y Normalización de Rural Servicios Informáticos, empresa que presta los Servicios de *outsourcing* global, desde 1986, a las Cajas Rurales y empresas participadas que forman el Grupo Caja Rural, en total más de 73. Técnico Informático con Máster en Auditoría Informática desde 1991, CISA y Máster en Seguridad Global en la Universidad Europea y Belt Ibérica, ha trabajado en los últimos 25 años en los servicios informáticos de empresas tales como: Entel (hoy Indra), Citibank, Banco Santander y RSI, en las que ha desarrollado diversos puestos y funciones relacionadas con las TIC (Auditoría, Seguridad, Calidad, Procesos, Sistemas, Fraude). Además, participa en diversos comités, foros y grupos internos y externos al Grupo, relacionados con Gestión de Continuidad, Riesgos, Seguridad, Auditoría, Fraude y Calidad, y forma parte del Grupo de Seguridad y de la Comisión de Seguridad, Prevención y Fraude del Centro de Cooperación Interbancaria (CCI), en representación de la UNACC (Unión Nacional de Cooperativas de Crédito), grupo de trabajo pionero en la lucha contra el fraude *online* en España; así como de CECON (Consorcio Español de Continuidad de Negocio), en el que participan Entidades Financieras, Bolsa, Valores, Seguros y Banco de España, entre otros; y Grupos de Normalización de AENOR. Es uno de los miembros fundadores del ICON (nuevo Instituto de Continuidad de Negocio español).

• **Juan Salom Clotet** es Comandante de la Guardia Civil. Desde el año 2000 dirige el Grupo de Delitos Telemáticos (GDT) de la Guardia Civil. Titulado del Curso Superior de Informática del Ejército y Máster de Seguridad de la Información para la Defensa por la Universidad Rey Juan Carlos, cuenta con numerosos cursos de especialización en el campo de las nuevas tecnologías, así como cursos profesionales sobre investigación policial. Participa en numerosos foros y másteres como experto en la investigación de la delincuencia informática y ha impartido cursos de formación a personal de la judicatura y a otras policías internacionales. Mantiene relaciones con las ciberpolicías de casi todos los países europeos, apoyado en instituciones como Europol e Interpol, y es fundador del Foro Iberoamericano de Encuentro de Ciberpolicías (FIEC), referente para los países iberoamericanos. Además es, desde su fundación, Vicepresidente del Grupo de Trabajo Latinoamericano sobre delitos tecnológicos de Interpol.

> SECURMÁTICA, a escena

Panorámica de SECURMÁTICA 2009

> Premios SIC 2010

En coincidencia con la celebración de la XXI edición de Securmática, tendrá lugar el acto de entrega de los VII Premios SIC, una iniciativa de la revista SIC con periodicidad anual.

La pretensión de estos galardones no es otra que la de hacer público reconocimiento del buen hacer de significativos protagonistas de un sector –el de la seguridad de la información y de la seguridad TIC en nuestro país– cuyo estado de madurez y proyección han alcanzado un punto crítico.

Los galardonados en la sexta edición de los premios SIC

LA HORA DEL REENCUENTRO Y LOS RECONOCIMIENTOS

> Cena de la Seguridad

SECURMATICA 2010

XXI Congreso español de Seguridad de la Información

27.28.29 | abril

AFORO LIMITADO

> Fechas y lugar

SECURMÁTICA 2010 tendrá lugar los días 27, 28 y 29 de abril de 2010 en el hotel NOVOTEL*. Campo de las Naciones de Madrid.

> Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2010 recibirán las carpetas de congresista con el programa oficial y toda la documentación –papel y CD-ROM– referente a las ponencias.
- Almuerzos y cafés.
- Cena de la Seguridad y entrega de los VII Premios SIC (28 de abril).
- Diploma de asistencia.

> Cuota de inscripción

La inscripción se podrá realizar para todo el congreso o por módulos (uno por día de celebración), con lo que se pretende ajustar al máximo la oferta de contenidos a las distintas necesidades formativas e informativas de los profesionales asistentes.

Cuota	Hasta el 31 de marzo	Después del 31 de marzo
1 Módulo	661 € + 16% IVA	760 € + 16% IVA
2 Módulos	961 € + 16% IVA	1.105 € + 16% IVA
3 Módulos	1.141 € + 16% IVA	1.313 € + 16% IVA

Descuentos:

– Dos inscripciones de una misma empresa: 10% dto. cada una.
– Tres inscripciones y siguientes: 15% dto. cada una.
– Universidades: 25% dto. cada una.

> Proceso de solicitud de inscripción

- Por fax: +34 91 577 70 47
- Por correo electrónico: info@securmatica.com
- Por sitio web: **www.securmatica.com**
- Por correo convencional: envíe el boletín adjunto o fotocopia del mismo a:

EDICIONES CODA / REVISTA SIC
Goya, 39
28001 Madrid (España)

- Abono de la cantidad correspondiente mediante cheque nominativo a favor de **Ediciones CODA, S.L.**, que deberá ser remitido a la dirección de Ediciones CODA, o
- Transferencia bancaria, cuya fotocopia deberá ser remitida vía fax o correo, a nombre de:

EDICIONES CODA, S.L.
CAJA MADRID
Oficina: Avda. de Felipe II, 15
28009 Madrid (España)
C.C.C.: 2038 1726 67 6000477427

- * Existen descuentos del hotel Novotel para los congresistas que deseen alojarse en el mismo con motivo de su asistencia a Securmática.
- Las inscripciones solo se considerarán formalizadas una vez satisfecho el importe de las mismas antes de la celebración del Congreso.
- Las cancelaciones de inscripción sólo serán aceptadas hasta 7 días antes de la celebración del Congreso, y deberán comunicarse por escrito a la entidad organizadora. Se devolverá el importe menos un 10% por gastos administrativos.

> Boletín de inscripción a Securmática 2010

Nombre y apellidos _____

Nombre y apellidos _____

Nombre y apellidos _____

Empresa _____ C.I.F. _____

Cargo _____

Dirección _____ Población _____

Código Postal _____ Teléfono _____ Fax _____

Correo-e _____

Persona de contacto, departamento y teléfono para facturación _____

_____

❑ MÓDULO 1 DÍA 27 ❑ MÓDULO 2 DÍA 28 ❑ MÓDULO 3 DÍA 29 ❑ Deseo inscribirme a SECURMÁTICA 2010

Firma:

Forma de pago: ❑ Talón ❑ Transferencia

Los datos personales que se solicitan, cuya finalidad es la formalización y seguimiento de su solicitud de inscripción al Congreso, serán objeto de tratamiento informático por Ediciones Coda, S.L. Usted puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición, expresados en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el domicilio del responsable del fichero: Ediciones Coda, S.L., C/ Goya, 39. 28001 Madrid.

> Información e inscripciones:

Revista SIC seguridad en informática y comunicaciones

Ediciones CODA / Revista SIC
Goya, 39 - 28001 Madrid (España)
Tel: 91 575 83 24/25 · Fax: 91 577 70 47
Correo-e: info@securmatica.com / info@codasic.com
Sitio: **www.securmatica.com**