SECURMATICA 2009

21.22.23/abril

XX Congreso español de Seguridad de la Información

Las reglas del juego: prioridad y eficiencia

+ con –

20 aniversario

PROGRAMA

20 aniversario

Securmática 2009, XX edición del Congreso español de Seguridad de la Información, organizado por la revista SIC, tendrá lugar los días 21, 22 y 23 de abril del presente en su tradicional sede del Campo de las Naciones de Madrid.

La protección de la información que se trata en los sistemas tecnológicos de uso en organizaciones ha llegado a un punto de madurez crítico que tiene reflejo en la profusión de normas técnicas, en la continua alusión a las mismas y a otros principios y mandatos consagrados en la legislación de la UE y específica española, y en la naturaleza y velocidad de implantación de los modelos de gestión y administración de la seguridad que han ido adoptando las entidades en función del sector de actividad al que pertenecen y de su propia cultura interna.

La seguridad de la información está llamada a formar un cuerpo único con las otras "seguridades" en el correspondiente nivel corporativo de abstracción; en tanto que los directores de sistemas de información deberán cuidar de la existencia en sus departamentos de la función específica de seguridad TIC, a fin de que en todos los planes y proyectos TIC se incluyan siempre controles de seguridad, cuya calidad de implantación y eficiencia deberán ser, además, verificadas y auditadas por especialistas.

Y es en este contexto en el que se va a celebrar la XX edición de Securmática, un momento apasionante tanto desde la óptica profesional como desde el punto de vista de la aplicación de la disciplina en organizaciones.

ES HORA DE COMPARTIR EXPERIENCIAS >>> Y AVANZAR

El programa que se propone este año incluye una visión fidedigna de lo que se está haciendo y de por dónde habrá que aplicar el esfuerzo para obtener los mejores resultados en tiempos tanto de contención presupuestaria como de preocupación real por el control de los riesgos de seguridad de la información.

Copatrocinadores:

accenture High performance. Delivered. · BULL · dominion · ERNST & YOUNG Quality In Everything We Do · gmv · GRUPO GESFOR · hp · IBM · indra · PRICEWATERHOUSECOOPERS · SIEMENS · Telefónica · unitronics

Organiza:

Revista SIC seguridad en informática y comunicaciones

SIC Seguridad en Informática y Comunicaciones es desde hace dieciocho 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 21 de abril

08:45h. Entrega de documentación.
09:15h. Inauguración oficial.
09:55h. **Ponencia: Centros de Servicios de Seguridad Gestionados en el Grupo Santander.**
Ponente: José Antonio Castro González, Director de Seguridad Corporativa del Grupo Santander.
10:30h. Coloquio.
10:35h. **Ponencia: El modelo de gestión y administración de la seguridad TIC en Iberia. Alcance del SGSI ISO/IEC 27001.**
Ponente: María Antonia García Redondo, Jefe de la Unidad de Seguridad Informática de Iberia.
11:10h. Coloquio.
11:15h. Pausa-café.
11:45h. **Ponencia: El proyecto de Centro de Seguridad de la Información de Cataluña.**
Ponentes:
• **Josuè Sallent i Ribes**, Director General de la Sociedad de la Información. Secretaría de Telecomunicaciones. Generalitat de Cataluña.
• **José Luis Checa López**, Director Gerente del Centro de Telecomunicaciones y Tecnologías de la Información de la Generalitat de Cataluña.
12:20h. Coloquio.
12:25h. **Ponencia: La mejora continua de los controles de seguridad: un juego a varias bandas.**
Ponente: Miguel Ángel Navarrete Porta, Director de Seguridad Informática de Caja Madrid.
13:00h. Coloquio.
13:05h. **Ponencia: Grupo Gas Natural: ¿gestión del riesgo o gestión de oportunidades?**
Ponente: Andreu Bravo Sánchez, Responsable de Seguridad de la Información de Gas Natural.
13:40h. Coloquio.
13:45h. Almuerzo.
15:45h. **Ponencia: Grupo Iberdrola: Plan de ciclo continuo para la concienciación en seguridad de la información.**
Ponente: Francisco Javier García Carmona, Director de Seguridad de la Información y las Comunicaciones del Grupo Iberdrola.
16:20h. Coloquio.
16:25h. **Ponencia: Ministerio de Economía y Hacienda: gestión efectiva de la seguridad.**
Ponentes:
• **Óscar Robledo Pascual**, Subdirector General de la Subdirección General de Tecnologías de la Información y las Comunicaciones del Ministerio de Economía y Hacienda (MEH).
• **Jesús Casado Viejo**, Gerente de Seguridad de Accenture Technology Solutions.
17:00h. Coloquio.
17:05h. Pausa-café.
17:20h. **Ponencia: Telefónica: Estrategia de Seguridad y Cuadro de Mando Integral.**
Ponentes:
• **José Luis Gilpérez López**, Gerente de Supervisión y Operación de Seguridad de Telefónica.
• **Félix Martín Rodríguez**, Gerente de la práctica de Seguridad y Gestión de Riesgos de Hewlett-Packard.
17:55h. Coloquio.
18:00h. **Ponencia: Fira de Barcelona: gestión de la seguridad entendida como Gestión de TI. ¿Es lo mismo?**
Ponentes:
• **Miguel Ángel Iglesias**, Director de Tecnologías de la Información y Comunicaciones de la Fira de Barcelona.
• **Javier Zubieta Moreno**, Director de Desarrollo de Negocio de Seguridad de Unitronics.
18:35h. Coloquio.
18:40h. Fin de la primera jornada.

CENTROS DE SERVICIOS DE SEGURIDAD GESTIONADOS EN EL GRUPO SANTANDER

Sinopsis: Cualquier empresa o institución basa gran parte de su actividad o negocio en los datos o en la información que posee acerca de clientes, ciudadanos, empleados, productos… La protección de la información, o seguridad de la información, se ha convertido en un eje fundamental de actividad en compañías e instituciones y ha crecido y evolucionado de manera significativa en el último decenio. Dentro de la protección de la información, al igual que en la mayoría de actividades, se pueden distinguir al menos dos funciones bien diferenciadas, el diseño o estrategia y la operación o ejecución. ¿Cuál es más importante de las dos? Si hacemos un símil con el cuerpo humano, la estrategia podría ser el cerebro y la operación el sistema nervioso. ¿Podemos vivir sin alguna de las dos? Por otra parte, si tratáramos de definir la seguridad de la información con una palabra, vendrían automáticamente a nuestra mente vocablos como prevenir, controlar, proteger, administrar, monitorizar, eficacia… Al realizar algo análogo con el concepto negocio, utilizaríamos palabras del tipo beneficio, ahorro de costes, rentabilidad, optimización, eficiencia… La piedra filosofal de la seguridad de la información sería el combinar ambos intereses y conceptos. La clave para resolver este enigma está en si podemos gestionar la seguridad de forma eficiente sin que ello suponga un riesgo adicional para nuestras entidades. En esta tesitura nos deberíamos plantear preguntas como ¿Podemos hacer de esta fusión de conceptos una oportunidad? ¿Hasta qué punto estamos dispuestos a ceder el control de nuestra seguridad a un tercero? No existe una respuesta ni solución única, cada empresa es una realidad diferente y la seguridad de la información debe ser "un traje a medida" con el que nos sintamos confortables.

Ponente

• **José Antonio Castro González** es Director de Seguridad Corporativa de Grupo Santander. Ha desarrollado la práctica totalidad de su carrera profesional en tecnologías de la información (21 años) en el Grupo Santander, en el que ha ocupado los puestos de Consultor del Área Internacional, de responsable de diferentes áreas técnicas y de Director de Seguridad Informática, hasta su nombramiento como Director de Seguridad Corporativa vinculada a la seguridad de la información. Cuenta con catorce años de experiencia en la Gestión de Riesgos de información en ámbitos como la continuidad operativa, la seguridad en canales alternativos, las infraestructuras de clave pública y las arquitecturas de seguridad .Net.

EL MODELO DE GESTIÓN Y ADMINISTRACIÓN DE LA SEGURIDAD TIC EN IBERIA. ALCANCE DEL SGSI ISO/IEC 27001

Sinopsis: La Gestión del Riesgo en las organizaciones es un proceso continuo que requiere esfuerzos de adaptación y gestión. El alineamiento de este proceso con las buenas prácticas establecidas en la norma ISO 27001 y la correspondiente certificación, beneficia adicionalmente a las organizaciones en imagen, que llega a clientes, proveedores, accionistas, y empleados. Iberia, consciente de la importancia de proporcionar una imagen corporativa de compromiso con la seguridad, ha trabajado durante los últimos años en la implantación de un SGSI y su posterior certificación. El alcance inicial ha sido definido de acuerdo a criterios de carácter estratégico, y establece las bases sobre las que debe sustentarse la estrategia de seguridad corporativa.

Ponente

• **María Antonia García Redondo** es Directora de la Unidad de Seguridad de la Información en Iberia Líneas Aéreas de España. Licenciada en Ciencias Económicas y Empresariales y Master en Gestión Empresarial y Técnico de Aviación Comercial, cuenta con una dilatada experiencia en el negocio del transporte aéreo. Actualmente es la Directora de la Unidad de Seguridad Informática en Iberia, cargo que lleva desempeñando desde 1993. Es colaboradora habitual en grupos de trabajo de seguridad de la información y ha participado activamente en foros de legislación y técnicos.

EL PROYECTO DE CENTRO DE SEGURIDAD DE LA INFORMACIÓN DE CATALUÑA

Sinopsis: La intervención versará sobre el plan nacional de impulso de la seguridad TIC de Cataluña, proyecto liderado por la Dirección General de la Sociedad de la Información de la Secretaría de Telecomunicaciones y Sociedad de la Información de la Generalitat de Cataluña. Se presentará el contexto del plan nacional, las líneas estratégicas aprobadas, las principales actuaciones previstas en los próximos cuatro años y el modelo organizativo propuesto, con especial atención a la propuesta de creación del Centro de Seguridad de la Información de Cataluña, CESICAT, entidad instrumental de la Secretaría de Telecomunicaciones y Sociedad de la Información que gestionará las principales actuaciones del plan nacional de impulso de la seguridad TIC. Al tiempo, se tratará de la evolución de los servicios gestionados de seguridad que actualmente ofrece el CTTI dentro del ámbito corporativo de la Generalitat y el sector público vinculado. A partir de la industrialización de una parte de dichos servicios, se ha podido trabajar su evolución y extensión al resto de entidades públicas catalanas, universidades, empresas y ciudadanos, mostrando cómo la colaboración entre los diversos agentes del sector permite incrementar la seguridad global del sistema y diseñar políticas corporativas embrionarias

de nuevos servicios públicos dirigidos a todos. Estas iniciativas representan el embrión de los servicios que prestará el CESICAT convirtiendo a la propia Generalitat en el primer y gran cliente de la iniciativa.

Ponentes

• **Josuè 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. Doctor en Ciencias Físicas por la Universidad de Barcelona y Diplomado en Ciencias Empresariales por la Universidad Oberta de Catalunya, ha sido 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.

• **Josep Lluís Checa López** es Director Gerente del Centro de Telecomunicaciones y Tecnologías de la Información, CTTI, de la Generalitat de Cataluña. Ingeniero Técnico Industrial por la UPC, ha cursado postgrados PDG-IESE en la Universidad de Navarra, PDG Gas Natural y CISM por Isaca. Cuenta con 22 años de experiencia en el sector informático con diversas responsabilidades, 11 de ellos en Digital Equipment Corporation y 9 en el Grupo Gas Natural. En su última etapa en esta compañía ocupó el cargo de Director de Administración y Seguridad de la Información.

LA MEJORA CONTINUA DE LOS CONTROLES DE SEGURIDAD: UN JUEGO A VARIAS BANDAS

Sinopsis: ¿Quiénes son los actores que intervienen y en qué medida participan en la mejora de los controles de seguridad? ¿Conoces a "los buenos" y a "los malos"? ¿Cómo ayudan unos y otros a la mejora continua? ¿Qué significa que un control sea mejor? ¿Qué hay que hacer para mejorar? ¿Y para hacerlo continuamente? ¿Cómo podemos medir cuán buenos somos? ¿Hasta qué punto nos ayuda en la mejora continua un análisis de riesgos? ¿Debe ser éste el eje de nuestra gestión? Y sobre todo, una cosa es que los controles que tenemos sean buenos e incluso los mejores, y otra que sean los que el negocio necesita. ¿Cómo es posible mejorar este encaje? Responder a estas y otras cuestiones nos ayudará a configurar el paquete de soluciones que precisaremos para trabajar en el nuevo escenario de la SEGURIDAD 2.0 (esa que va más allá de los controles de la ISO). El conferenciante tiene algunas ideas al respecto. Y en su intervención las compartirá con la audiencia y, al tiempo, recabará su opinión.

Ponente

• **Miguel Ángel Navarrete Porta** es Director del Departamento de Seguridad Informática de Caja Madrid. Ha trabajado como informático desde hace veintidós 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.

GRUPO GAS NATURAL: ¿GESTIÓN DEL RIESGO O GESTIÓN DE OPORTUNIDADES?

Sinopsis: Vivimos una época de crisis global económica en la que los errores se pagan muy caro; la prudencia e incertidumbre frena y descarta decisiones de negocio que podrían suponer claras oportunidades de mejora no sólo para los intrépidos; y la optimización de procesos se ha convertido en un proyecto obligatorio para todas las empresas. Abordar una gestión del riesgo de todos los activos de la información y definir una estrategia de implantación rápida y global es la clave para ofrecer una herramienta de soporte al negocio capaz de aportar argumentos fiables y efectivos que respalden sus tomas de decisiones, permitan priorizar acciones y optimicen los costes y los beneficios de los proyectos de seguridad. Partiendo de este enfoque, se presentan las tácticas desplegadas en el Grupo Gas Natural para ofrecer los mejores resultados a todas las áreas de negocio en el menor tiempo.

Ponente

• **Andreu Bravo Sánchez** es Responsable de Seguridad de la Información del Grupo Gas Natural y cuenta con más de 20 años de experiencia profesional en las diferentes áreas de las tecnologías de la información (desarrollo, sistemas, comunicaciones, arquitectura y seguridad). Certificado CISSP, CISM e ISO-27001 lead auditor, es también miembro de la junta directiva de ISMS Forum Spain y de otras organizaciones internacionales como $(ISC)^2$ e ISACA. Ha participado en la definición, gestión e implantación de seguridad de la información de la compañía, incluyéndose entre los proyectos concernidos la gestión de identidades, la definición de políticas de seguridad, la clasificación de activos, la gestión de riesgos, el diseño de seguridad perimetral, la certificación digital y la firma electrónica.

GRUPO IBERDROLA: PLAN DE CICLO CONTINUO PARA LA CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Sinopsis: En mayor o menor medida, dirigimos acciones a concienciar y formar en el uso del Activo de Información a todos los profesionales que conforman nuestras organizaciones, intentando llegar a cada colectivo con un contenido y un continente, adaptando éstos al máximo a sus actividades y entornos, intentado en ello que sientan este Activo más próximo, como algo propio y al cual contribuyen aportando valor en cada momento. Ahora somos las direcciones de Seguridad quienes debemos tomar conciencia de la realidad de la Organización: entornos cambiantes, complejidad de los procesos, mayor relación entre los entornos productivos de ésta, etc.; es decir, un entorno no estático al cual, igualmente, deberemos de responder por una parte, midiendo la eficacia de nuestras acciones formativas y por otra, adaptando éstas a cada nueva realidad sobre la base de las anteriores mediciones; o dicho de otro modo: dotar de vida a nuestro Plan de Concienciación de Protección de la Información.

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 inicia 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. Y 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.

MINISTERIO DE ECONOMÍA Y HACIENDA: GESTIÓN EFECTIVA DE LA SEGURIDAD

Sinopsis

Dentro de las iniciativas prioritarias en materia de seguridad lanzadas por la Subdirección General de Tecnología de la Información y las Comunicaciones (SGTIC) del Ministerio de Economía y Hacienda, está el control y seguimiento de la implantación de su Sistema de Gestión de la Seguridad de la Información (SGSI). Hasta la fecha, son pocas las organizaciones que disponen de herramientas de gestión y control de un SGSI. En este sentido, la SGTIC junto con Accenture ha definido y desarrollado una solución de gestión y control, que le permite la recogida y la explotación de todos los datos sobre los que se sustenta un SGSI, de forma ordenada, automatizada y repetible. Se revisarán durante la conferencia los pilares y capacidades de la herramienta de gestión y control SGSI: Activos de información y su relación con otras herramientas, Planes y Proyectos, Gestión del Marco Normativo de Seguridad, Controles de Seguridad, Auditorías, Indicadores (estratégicos y automatizados con otras herramientas de gestión de *logs*), estadísticas, estructura organizativa, así como sus mecanismos de parametrización y posibilidades de integración.

Ponentes

• **Óscar Robledo Pascual** es Subdirector General en la Subdirección General de Tecnologías de la Información y las Comunicaciones del Ministerio de Economía y Hacienda-MEH, y Vicepresidente de la Comisión Permanente de la Comisión Ministerial de Administración Electrónica. Licenciado en Informática por la Facultad de Informática de la UPM, dispone de las certificaciones CISM, CCN-STIC e ITIL. Ha desempeñado diversos puestos de responsabilidad en el Ministerio de Fomento, el Ministerio de Administraciones Públicas y en el Ministerio de Economía y Hacienda.

• **Jesús Casado Viejo** es Gerente de la línea de seguridad dentro del Grupo de Tecnología de Accenture Technology Solutions. Licenciado en Ciencias Físicas por la Universidad Complutense de Madrid posee las certificaciones CISSP y BS7799 Lead Auditor por BSI. A lo largo de su carrera profesional en el mundo de la consultoría de seguridad, ha trabajado en diferentes tipologías de proyectos, Planes de Continuidad de Negocio, Análisis de Riesgos, Planes Directores de Seguridad, Sistemas de Gestión de Seguridad de la Información-SGSI y auditorías LOPD.

TELEFÓNICA: ESTRATEGIA DE SEGURIDAD Y CUADRO DE MANDO INTEGRAL

Sinopsis: Como parte del programa de Gestión de la Seguridad Operacional (GSO) llevado a cabo desde la Dirección de Operaciones de Telefónica España, se ha desarrollado el área de informes como parte de los procesos de administración de la Gerencia de Seguridad. Durante el último año, se ha llevado a cabo un proyecto para la implantación de un cuadro de mando integral. La implantación del cuadro de mando ha supuesto la creación de diferentes perspectivas: la financiera, la de cliente, la de recursos y excelencia operativa, que a través de diferentes vistas ofrece información a diferentes agentes con distintas necesidades. Como parte de la implantación del programa HP OSM, la construcción del cuadro de mando supone el colofón a la implantación de los procesos de seguridad operativa de Telefónica Operaciones, ayudando a la consolidación de la información para facilitar la toma de decisiones y el seguimiento de la estrategia de seguridad. Durante la conferencia, se describirá la metodología y la experiencia en la implantación del cuadro de mando y el área de informes.

Ponentes

• **José Luis Gilpérez López** es Responsable de Seguridad de Redes y Servicios de la Dirección de Operaciones, Supervisión y Operación de Telefónica España. Ingeniero Industrial por la UPM, trabaja en Telefónica de España desde 1988, compañía en la que ha ocupado diferentes responsabilidades relacionadas con la red, hasta el año 1997; desde 1997 hasta 2000 fue responsable de gestión dinámica de red en Telefónica Móviles; y de 2000 a 2002 ocupó el cargo de responsable de soporte y operación de Firstmark Comunicaciones España. Desde 2002 hasta incorporarse a su actual cargo, fue responsable de Seguridad de Redes y Servicios en Telefónica Móviles España, Dirección General de Red.

• **Félix Martín Rodríguez** es Gerente de la práctica de Seguridad y Gestión de Riesgos de Hewlett-Packard. 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 catorce 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, empresa de la industria aeroespacial, donde fue el responsable de Sistemas de Información y CSO de la compañía.

FIRA DE BARCELONA: GESTIÓN DE LA SEGURIDAD ENTENDIDA COMO GESTIÓN DE TI. ¿ES LO MISMO?

Sinopsis: Fira de Barcelona ha abordado el proyecto "Beleroforte" para gestionar de forma global a través de un único proveedor todos los servicios de red para cubrir las necesidades de conectividad y acceso a internet de los usuarios propios de Fira, de los expositores que acuden a los eventos y de los organizadores externos. Desde su concepción, este proyecto está basado en la prestación de servicios remotos en donde la seguridad está embebida desde el punto de vista tecnológico y su gestión es intrínseca a la gestión de la infraestructura crítica. En la ponencia se repasarán los aspectos relevantes del proyecto así como los beneficios que obtiene Fira al contar con Unitronics como prestador único de servicios de seguridad, aplicando las metodologías y procedimientos que rigen los servicios de red. Se demuestra así la simbiosis operativa entre la gestión de TI y la gestión de seguridad, desde un mismo prisma.

Ponentes

• **Miguel Ángel Iglesias** es director de Tecnologías de la Información y Comunicaciones en Fira de Barcelona. Licenciado en Ingeniería Informática, es MBA por la Universidad Politécnica de Cataluña y PDD por la IESE Business School. Como consultor y director de proyectos, ha pasado por diferentes empresas relacionadas con la consultoría, banca y la prestación de servicios tecnológicos. Actualmente, su actividad se centra no sólo en la gestión del plan TIC para Fira, sino también en la definición e implantación de metodologías de gestión y reingeniería de procesos para toda la organización.

• **Javier Zubieta Moreno** es Director de Desarrollo de Negocio de Seguridad y Optimización y CISO de Unitronics. Licenciado en Informática por la Universidad Politécnica de Madrid, tiene 14 años de experiencia en seguridad. Sus actuales funciones incluyen la gestión del portafolio de soluciones y servicios de seguridad de la compañía, decidiendo su contenido, planteamiento comercial, provisión de recursos internos y liderando la definición de servicios y las relaciones con los proveedores con los que Unitronics firma alianzas estratégicas. Como CISO, es miembro permanente del Comité de Dirección de Seguridad y su responsabilidad es la organización de todas aquellas actuaciones que en la materia Unitronics aborda. Anteriormente trabajó en empresas como SIA, fue profesor adjunto de la Universidad Camilo José Cela y becado en el CERN.

SEGUNDO MÓDULO 22 de abril

09:00h.	Entrega de documentación.
09:15h.	**Ponencia: Euskaltel: Plan Director Integral de Riesgo Corporativo.** **Ponentes:** • **Juan Carlos Uranga**, Responsable de Seguridad Física de Euskaltel. • **Rafael Ortega García**, Socio Director de T&SRS de Ernst & Young.
09:50h.	Coloquio.
09:55h.	**Ponencia: ¿Hacia dónde apunta la evolución de la figura del CISO?** **Ponente: Santiago Moral Rubio**, Director de Seguridad Lógica Corporativa del Grupo BBVA.
10.30h.	Coloquio.
10:35h.	**Ponencia: SGSI/SGCN - Seguridad y disponibilidad, dos caras de un mismo sistema.** **Ponentes:** • **Julio San José Sánchez**, Gerente de Seguridad Informática de Bankinter. • **Ana Belén Galán López**, Responsable SGSI/SGCN. Área de Seguridad Informática de Bankinter.
11:10h.	Coloquio.
11:15h.	Pausa-café.
11:45h.	**Ponencia: STL y LAE: certificaciones ISO/IEC 27001 de alcance global.** **Ponentes:** • **Julio Sánchez Fernández**, Director de Seguridad de la Información de STL-Sistemas Técnicos de Loterías. • **Carlos Bachmaier Johanning**, Gestión de Riesgo Corporativo y Auditoría TI de STL-Sistemas Técnicos de Loterías.
12:20h.	Coloquio.
12:25h.	**Debate: Un reto para el CISO: aminorar la complejidad de operación de la infraestructura tecnológica de seguridad TIC.** **Intervienen:** • **Pedro Sánchez Cordero**, Responsable de Seguridad de la Información y de Sistemas de Información de ATCA (Asociación Técnica de Cajas de Ahorro). • **Santiago Minguito Santos**, Responsable de Seguridad Tecnológica del Grupo Banco Sabadell. • **Casimiro Juanes Calvo**, Responsable de Seguridad TI del Grupo Ericsson. • **Gabriel Arriero Salcedo**. Área de Seguridad. Inspección General CIS. Ministerio de Defensa.
13:55h.	Fin del debate.
14:00h.	Almuerzo.
16:00h.	**Ponencia: Grupo FCC: proyecto de prevención de fugas de información.** **Ponentes:** • **Gianluca D'Antonio**, Director de Seguridad de la Información y Gestión de Riesgos del Grupo FCC. • **Juan Miguel Velasco López-Urda**, Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Empresas de Telefónica España.
16:35h.	Coloquio.
16:40h.	**Ponencia: Ministerio de Economía y Hacienda. Intervención General de la Administración del Estado (IGAE): experiencia de *single-sign on* y *workflow* de gestión de identidades.** **Ponentes:** • **María Jesús Casado Robledo**, Responsable de Seguridad de la Información de la IGAE. • **Rodrigo Blanco Rincón**, Gerente de la Línea de Seguridad de Bull España.
17:15h.	Coloquio.
17:20h.	Pausa-café.
17:40h.	**Ponencia: Gestvul y tendencias en la gestión de 'securización' de plataformas tecnológicas.** **Ponentes:** • **Luis Saiz Gimeno**, Responsable de Prevención de Delitos Tecnológicos de BBVA. • **Isidro Ramón Labrador Rodríguez**, Jefe de Sección de Auditorías Técnicas de GMV Soluciones Globales Internet.
18:15h.	Coloquio.
18:20h.	**Ponencia: Circuito de Montmeló-Cataluña: Sistema integral de seguridad física y accesos.** **Ponentes:** • **Jordi Urquijo Otero**, Director del Departamento de Tecnología. Circuito de Montmeló-Cataluña. • **Víctor Llorente Gómez**, Gerente de la Línea de Seguridad. Dominion Soluciones Tecnológicas.
18:55h.	Coloquio.
19:00h.	Fin de la segunda jornada.
20:00h.	**Cena de la Seguridad y entrega de los VI Premios SIC.**

EUSKALTEL: PLAN DIRECTOR DE RIESGO CORPORATIVO

Sinopsis: Hoy en día, la mayoría de las organizaciones gestionan el riesgo interno de forma independiente en diferentes áreas. Realizar una gestión del riesgo descentralizada implica que los esfuerzos que realiza la organización a nivel corporativo no se encuentren coordinados y los costes de identificar, evaluar y corregir los riesgos se vean duplicados. Por esta razón, las organizaciones tienden con la experiencia que disponen en la gestión del riesgo a unificar en una sola todas las áreas de riesgo. Las áreas de mayor riesgo identificadas por las organizaciones son las relacionadas con el departamento económico financiero, los sistemas de información y las instalaciones físicas. Euskaltel, siendo consciente de su situación particular y de la evolución en la gestión del riesgo en empresas de su mismo sector y tamaño, decidió acometer un Plan Director Integral del Riesgo Corporativo, que empezase a planificar el riesgo asociado a la seguridad fisica o patrimonial, seguridad de la información y fraude. El factor crítico de éxito ha sido seleccionar un único modelo de referencia para las tres áreas: la ISO 27002, estrechamente relacionada con los sistemas de información. Para ello se ha adaptado dicha norma a los requerimientos de las áreas de seguridad física y fraude, obteniendose un único e integrado Plan Director.

Ponentes

• **Juan Carlos Uranga** es Responsable de Seguridad Física de la compañía Euskaltel desde el año 2000 hasta la fecha. Dispone de una gran experiencia en proyectos de dimensión corporativa en el frente de la protección global. Miembro de la Ertzaintza (período 1983 – 2000) es Director de Seguridad (nº. 01723).

• **Rafael Ortega García** es Socio Director de T&SRS (Technology and Security Risk Services) de Ernst & Young. Con anterioridad ha ocupado diversos cargos en firmas como Infosafe, Unisys, Deloitte y Azertia Consulting. Posee una larga experiencia en el sector de la protección TIC y de la información, ámbitos en los que ha dirigido y participado en numerosos proyectos, centrados en la planificación estratégica de sistemas de información, planes estratégicos de seguridad, PKI, desarrollo y soporte a planes de contingencia TIC, planes de continuidad de negocio, diagnósticos de seguridad, análisis de riesgos y creación de cuadros de mando.

¿HACIA DÓNDE APUNTA LA EVOLUCIÓN DE LA FIGURA DEL CISO?

Sinopsis: En los últimos años, las responsabilidades de las áreas de Seguridad Lógica han ido evolucionando hacia otras funciones que tienen un denominador común: el alto grado de conocimiento y especialización en la Seguridad Lógica. La primera que nos encontramos históricamente fue la Seguridad de la Información. Dado que no toda la información está en soporte electrónico, hay una serie de responsabilidades en la Seguridad de la Información que no son tecnológicas, que no encajan bien dentro de departamentos de TI. Pero el problema es que para poder asumir la responsabilidad de la Seguridad de la Información sí es necesario tener un conocimiento muy profundo sobre la Seguridad Lógica (o Seguridad TI). Si analizamos lo que sucede con la Prevención del Fraude, en cualquier tipo de industria o administración pública, es que hay tipos de fraudes que no son tecnológicos; pero hoy en día es imposible trabajar sobre prevención del fraude sin unos conocimientos muy sólidos de Seguridad Lógica. Pasa exactamente igual cuando hablamos de Control Interno de TI, cuando hablamos de Riesgo Operacional en TI o cuando, de forma incipiente, se comienzan a tratar los temas de Gobierno del Riesgo Tecnológico, entroncado con las estrategias de Responsabilidad Social Corporativa. ¿Vamos hacia un "SuperCISO" con responsabilidades en Seguridad TI, Control Interno, Riesgo Operacional, Prevención del Fraude y Riesgo Tecnológico, o vamos hacia un "MiniCISO" que dé servicio a los responsables de Seguridad de la Información, Control Interno TI, Riesgo Operacional TI, Prevención del Fraude Tecnológico y Gobierno del Riesgo Tecnológico?

Ponente

• **Santiago Moral Rubio** es Director de Seguridad Lógica Corporativa 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.

SGSI / SGCN: SEGURIDAD Y DISPONIBILIDAD, DOS CARAS DE UN MISMO SISTEMA

Sinopsis: Con la publicacion a principios de 2007 de la BS 25999-2, Bankinter se planteó la creación, implantación y operación de un Sistema de Gestion de Continuidad de Negocio que le permitiera la mejora de la resiliencia de su negocio, haciéndolo de forma proactiva, y que incrementara su capacidad de gestión de la interrupción de negocio, y que asegurara a sus clientes que el banco trabaja con los estándares más elevados de calidad y rigor profesional en la gestión de la continuidad de negocio en sus plataformas y sistemas. En este contexto, aparecieron de nuevo algunas de las preguntas planteadas allá por 2006 con la implantación de la ISO 27001 ¿Podremos llevarlo a cabo? ¿Sistemas independientes? Las respuestas a estas y otras cuestiones fueron apareciendo gracias a que entonces se sentaron las bases de un sistema de gestión que permitiera a la entidad mejorar de manera continua y uniforme. Este planteamiento de disponer de un único sistema ha permitido al banco tener un proceso de implantación muy eficiente y corto –menos de 6 meses–, llevando a Bankinter a ser la primera empresa española en obtener la certificacion BS 25999-2 otorgada por la British Standard Institution (BSI).

Ponente

• **Julio San José Sánchez** es Gerente de Seguridad Informática de Bankinter. Con una trayectoria de más de veinte años en seguridad de la información, desde su incorporación al banco en 1997 ha desempeñado varios puestos: Responsable de Seguridad de Aplicaciones y Responsable Técnico de Seguridad Informática. Es CISM por ISACA, *Lead Auditor* BS 7799 y BS 25999 por BSI. Igualmente, es coordinador de subgrupo 2 (Criptografía) del Subcomité de Seguridad de las TI (CTN 71/SC27), habiendo colaborado en la redacción de varias normativas, tanto nacionales como internacionales. Representante del SC27 en el *Grupo Especial de Análisis de Riesgos GET 13*. Vocal del CTN 71/SC7/WG25, *IT Service and Operations Management, ITIL,* es también miembro del Grupo de Expertos de la Cátedra de Gestión de Riesgo del Instituto de Empresa y profesor del Máster en Dirección y Gestión de la Seguridad de la Información de Asimelec. Asimismo es co-autor del libro *'Seguridad de las tecnologías de la información. La construcción de la confianza para una sociedad conectada'*, editado por AENOR.

• **Ana Belén Galán López** es Responsable de SGSI/SGCN en el Área de Seguridad Informática de Bankinter. Ingeniera Técnica Informática por la Universidad Politécnica de Madrid, posee las certificaciones CISA, CISM de ISACA y Lead Auditor ISO 27001 de Applus. Comenzó su trayectoria profesional en Red.es y trabajó como consultora de seguridad en Telefónica Soluciones y T-Systems, desarrollando e implantando Sistemas de Gestion de Seguridad de la Información, así como Planes de Continuidad de Negocio.

STL Y LAE: CERTIFICACIONES ISO/IEC 27001 DE ALCANCE GLOBAL

Sinopsis: Parece evidente que proyectos pequeños de corta duración tengan mayores posibilidades de éxito que proyectos grandes de larga duración, para complejidades equivalentes de los asuntos abordados. Este pensamiento se traslada de forma regular a la forma de abordar un proyecto de creación y despliegue de un SGSI, fijando un alcance parcial, normalmente pequeño y acotado que excluye grandes partes de la organización, pero bien conocido y controlado. Por otra parte, la implantación de un SGSI debe servir para reducir el riesgo de una organización de forma eficiente (coste-beneficio); un razonable análisis de riesgos (corporativo y TIC) y coste beneficio permitirá seleccionar el alcance más conveniente, lo demás será tirar el dinero. Parece haberse convertido en conocimiento convencional (el alcance es lo que importa) que se debe desplegar paso a paso, partiendo desde un alcance pequeño e incluir en expansiones posteriores nuevos procesos y activos. Sin embargo, un alcance limitado también introduce otras problemáticas. ¿Existen alternativas viables a esta forma de proceder? ¿Pueden ser mejores? ¿Es conveniente y viable abordar un alcance completo para una organización grande? Se compartirán las experiencias de LAE y STL, que han implantado la gestión de la seguridad con alcance completo –todas las actividades de la organización se exponen simultáneamente– en un corto periodo de tiempo y cuyos sistemas han sido certificados con éxito.

Ponentes

• **Julio Sánchez Fernández** es Responsable de Seguridad de la Información en Sistemas Técnicos de Loterías del Estado, STL. Ingeniero de Telecomunicación por la UPM y CISM, desarrolló funciones de desarrollo de software y técnica de sistemas durante 10 años en la industria y la administración pública; se incorporó en 1987 a GMV, donde se hizo cargo de la Dirección de Software Engineering hasta 1993, año en el que participó en la novedosa GMV Soluciones Globales Internet desde su creación, entidad en la que estuvo hasta 1998, año de su incorporación a Sistemas Técnicos de Loterías del Estado.

• **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, donde inició su labor profesional en los campos del desarrollo, la seguridad y el control. Tras más de veinte años de actividad profesional se incorpora 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 Másteres y en cursos de preparación CISA y CISM. Forma parte del "Grupo de Expertos de la Cátedra GMV/Oracle de Gestión de Riesgo" del Instituto de Empresa, y 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. Auditor Jefe SGSI (a falta de prácticas).

■ GRUPO FCC: PROYECTO DE PREVENCIÓN DE FUGAS DE INFORMACIÓN

Sinopsis: Se presentará durante la conferencia la primera iniciativa DLP específica registrada en España, emprendida por el Grupo FCC como parte de su Plan Director de Seguridad de la Información, desplegado y operado por el equipo de Telefónica Grandes Clientes en 24x7 desde el SOC de Telefónica desde la RED. Este proyecto completa el conjunto de servicios que el AN. Seguridad de Telefónica GG.EE. puso en marcha tras el concurso de adjudicación de FCC en 2008. La tecnología DLP es la evolución de las tecnologías DRM y presenta elementos de control exhaustivo sobre cualquier dato o información electrónica de la organización de forma transparente y no intrusiva. Este proyecto permite a FCC el control de la información y documentos críticos para su organización en un mercado sensible a la fuga de información confidencial y el correcto uso de los medios electrónicos en la empresa. Por su parte este nuevo servicio incorporado al SOC y la RED de Telefónica el año pasado es una nueva muestra de la apuesta tecnológica de la Compañía por la seguridad en los mercados en que opera.

Ponentes

• **Gianluca D'Antonio** es Director de Servicio de Seguridad de la Información y Gestión de Riesgos del Grupo FCC. Licendiado en Derecho (experto en nuevas tecnologías y en seguridad de la información) y PDD por el EISE 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.

• **Juan Miguel Velasco López-Urda** es Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Empresas 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 UPM y, entre otros, es Master Executive de Gestión Empresarial por INSEAD-EUROFORUM.

■ MINISTERIO DE ECONOMÍA Y HACIENDA. INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO (IGAE): EXPERIENCIA DE *SINGLE-SIGN ON* Y *WORKFLOW* DE GESTIÓN DE IDENTIDADES

Sinopsis: En la conferencia se expondrá el caso específico de la implantación en la Intervención General de la Administración del Estado (IGAE) de una solución de Control de Accesos y de Gestión de Identidades. Se analizarán las necesidades de la IGAE, y cómo la solución propuesta ha aportado valor a la organización en las distintas fases del ciclo de vida de la identidad de los usuarios. Se describirán, además, la arquitectura y los componentes adoptados (E-SSO, *Provisioning* y Flujo de Trabajo de Aprobación). Por último, se valorarán las dificultades encontradas durante el desarrollo del proyecto y las soluciones aplicadas en cada caso.

Ponentes

• **María Jesús Casado Robledo** es Responsable de Seguridad de la Información en la Secretaría General de Presupuestos y Gastos y de la Intervención General de la Administración del Estado, en el Ministerio de Economía y Hacienda. Pertenece al Cuerpo Superior de Sistemas y Tecnologías de la Información, es miembro de ASTIC (Asociación del Cuerpo Superior de Sistemas y Tecnologías de la Información), y dispone de las certificaciones CISA y CGEIT. Es miembro de ISACA y de su capítulo en Madrid, ASIA.

• **Rodrigo Blanco Rincón** es Responsable de la línea de Negocio de Seguridad de Bull (España). Ingeniero Superior de Telecomunicaciones por la UPM y Máster de Gestión y Dirección de la Seguridad de la Información por la Universidad Pontificia de Salamanca y ASIMELEC, posee la certificación CISA y PMP por el Project Management Institute. Actualmente trabaja en Bull España, donde es el responsable de la línea de negocio de Seguridad. También es profesor en el Máster de Gestión y Dirección de la Seguridad de la Información de ASIMELEC y la UPM.

DEBATE

■ UN RETO PARA EL CISO: AMINORAR LA COMPLEJIDAD DE OPERACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE SEGURIDAD TIC

En no pocas organizaciones, grupos empresariales y servicios comunes o compartidos, el crecimiento a veces incontenible en muchos frentes y durante estos últimos años de la infraestructura tecnológica orientada específicamente a la protección de la información de negocio y actividad y al entorno tecnológico heterogéneo en que se trata, ha traido aparejado un incremento de la complejidad de operación, al que se viene a añadir el producido por la interconexión en línea con clientes y con proveedores. ¿Existen hoy fórmulas aceptables con base tecnológica que permitan frenar o aminorar dicha complejidad sin menoscabo del control de riesgos de seguridad de la información?

Intervienen:

• **Pedro Sánchez Cordero** es Responsable de Seguridad de la Información en Asociación Técnica de Cajas de Ahorros (ATCA). Ingeniero Informático, ha trabajado anteriormente en empresas como consultor de seguridad informática especializado en métodos forenses, redes trampa, detección de intrusiones, cortafuegos, desarrollo de normas y metodologías sobre arquitecturas de seguridad. Asimismo ha liderado la implantación de la ISO 27001 en ATCA. Cuenta con la certificación de Visa y Mastercard en la implantación del estándar de seguridad PCI-DSS. También ha colaborado con expertos de seguridad a nivel gubernamental y otras organizaciones comerciales. Actualmente escribe y da conferencias nacionales e internacionales en eventos especializados. También posee las certificaciones CISM y CHFI.

• **Santiago Minguito Santos** es Responsable de Seguridad Tecnológica del Grupo Banco Sabadell. Ingeniero Técnico de Telecomunicaciones por la UPC, CISA, CISM, CISSP, BS17799 Lead Auditor y certificado ITIL Foundation, posee amplia experiencia profesional en seguridad de la información, habiendo desarrollado gran parte de su carrera profesional en Deloitte durante 11 años, como *Senior Manager* del departamento de Gestión de Riesgos Tecnológicos, en tareas de planificación y ejecución de proyectos relacionados con la seguridad informática. Desde su incorporación a Banco Sabadell en mayo de 2007, ha gestionado proyectos estratégicos de seguridad tecnológica relacionados, entre otros frentes, con la aplicación de la firma electrónica, la gestión del fraude en Internet y la gestión de identidades.

• **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 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 ISC² en la preparación de los exámenes.

• **Gabriel Arriero Salcedo** es Teniente Coronel de Cuerpo General de las Armas del Ejército de Tierra. Diplomado en Informática Militar y Máster en Dirección y Gestión de la Seguridad de la Información por la Universidad Pontificia de Salamanca, actualmente está destinado en el Área de Seguridad de la Información de la Inspección General CIS perteneciente a la Dirección General de Infraestructura del Ministerio de Defensa.

GESTVUL Y TENDENCIAS EN LA GESTIÓN DE 'SECURIZACIÓN' DE PLATAFORMAS TECNOLÓGICAS

Sinopsis: La detección y posterior gestión de las vulnerabilidades tecnológicas se ha convertido en uno de los procedimientos de seguridad más efectivos en la lucha contra el fraude en línea y el ciberdelito. En este sentido, toda entidad que realiza análisis de vulnerabilidades se encuentra con el problema de que, una vez obtenidos los resultados, bien a través del lanzamiento de herramientas automatizadas, bien a través de análisis manuales, el procedimiento no finaliza sino que hay que efectuar diversas tareas de gestión: distribución de resultados entre los distintos responsables, comparación con resultados de anteriores análisis, descarte de falsos positivos, soporte a la resolución de vulnerabilidades y verificación de la resolución. Estas tareas, entre otras, se pueden automatizar con el servicio GestVul, siendo el objetivo de esta ponencia explicar el aprovechamiento de GestVul por parte de BBVA dentro del marco de su Plan Director de Seguridad.

Ponentes

• **Luis Sáiz Gimeno** es Responsable de Prevención de Delitos Tecnológicos del Grupo BBVA dentro del departamento de Seguridad Lógica, siendo su ámbito de actuación la prevención, detección e investigación de los delitos cometidos por medios telemáticos. Uno de los proyectos actuales que dirige es el constituido por el Plan Estratégico de Prevención de Fraude Electrónico. Ingeniero de Telecomunicación por la UPM, certificado CISA y CISSP, tiene más de 10 años de experiencia en diferentes áreas de seguridad de la información y viene trabajando en este campo en el Grupo BBVA desde el 2000.

• **Isidro R. Labrador Rodríguez** es Jefe de la Sección de Auditorías Técnicas de GMV Soluciones Globales Internet S.A. Ingeniero Industrial por la Universidad de Oviedo, CISA y CISSP, ha desarrollado su carrera profesional dentro del ámbito de la seguridad lógica y pertenece a GMV desde 2001. En 2008 asumió las funciones de Jefe de Sección de Auditorías Técnicas de GMV Soluciones Globales Internet S.A, dirigiendo el equipo encargado de realizar proyectos de análisis de seguridad y *hacking* ético. Anteriormente participó como consultor de seguridad, jefe de proyecto e ingeniero en diversos proyectos relacionados con *test* de intrusión e infraestructuras de seguridad para usuarios de los sectores de telecomunicaciones, financiero, industrial y administración pública. Antes de su incorporación a GMV, trabajó en varias empresas del ámbito de las TIC, realizando labores de definición, desarrollo e integración de soluciones relacionadas con la seguridad lógica.

CIRCUITO DE MONTMELÓ - CATALUÑA: SISTEMA INTEGRAL DE SEGURIDAD FÍSICA Y ACCESOS

Sinopsis: El objetivo principal de la solución integral implementada por el Circuito de Montmeló de Cataluña, consiste en dar una solución a todos los niveles y en todos los aspectos de una empresa, abarcando el abanico más amplio de posibilidades, e intentando unificar todas las soluciones, elementos y dispositivos ya implementados o previstos en futuras instalaciones. Dicha solución integral hace referencia a los distintos entornos como son las entradas, pases, socios, visitas y empleados, quedando enmarcados en una solución global, que comparte espacio con las tecnologías de seguridad de última generación, destacando sobre todas ellas, por su alto grado de eficacia y seguridad, la biometría facial en 3D, implantada en puntos estratégicos de seguridad dentro del Circuito de Montmeló de Cataluña.

Ponentes

• **Jordi Urquijo Otero** es Director del Departamento de Tecnología del Circuito de Montmeló de Cataluña. Cuenta con más de 20 años de experiencia en los diferentes campos en los que ha participado, desde la industria gráfica hasta la televisión, pasando por la seguridad, la administración, la hostelería, el desarrollo y el diseño y gestión de sistemas. Algunas de las compañías y organismos con los que ha colaborado son: Micronet, G&D, Schlumberger, Servei Catalá de la Salut, Ferrocarrils de la Generalitat, Kaba, Roca, Gestmusic, Cambra de Comerç de Barcelona, Bertelsmann, Port Aventura, Ajuntament del Prat, Principado de Asturias, Microsoft, Hospital de Cruces, CajaAsturias, Hotel Fira Palace, Selección Nacional de Waterpolo, SL Benfica, entre otros.

• **Víctor Llorente Gómez** es Gerente de la Línea de Seguridad Lógica, Técnica y Física de Dominion. Licenciado en Informática por la Universidad de Deusto, es máster de Ingeniería del Software y Seguridad de Sistemas por la Universidad de Deusto–Eside, y cuenta con las certificaciones Clarify, CISA y Certificación SGSI. En Dominion ha sido desde 2003 gerente de la línea de Seguridad de Sistemas de Información y con anterioridad ha trabajado en Ibermática y en DMR Consulting –actual Everis–, en esta última en numerosos proyectos de seguridad técnica y consultoría, así como Gerente del Área de Seguridad Lógica de DMR Consulting.

TERCER MÓDULO 23 de abril

09:15h. Entrega de documentación.

09:30h. **Ponencia: Negocios diversos, el reto de una Seguridad Corporativa: el Plan Director de ICM.**
Ponentes:
• **Fernando Ledrado Gómez**, Director de Seguridad Corporativa de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid.
• **Elena Maestre García**, Directora de Riesgos Tecnológicos de PricewaterhouseCoopers.

10:05h. Coloquio.

10:10h. **Ponencia: La gestión de la seguridad TIC en el ámbito sanitario: el caso de la Comunidad de Madrid.**
Ponentes:
• **José Manuel Laperal González**, Responsable de Seguridad, Planificación e Innovación de la Dirección General de Sistemas de Información Sanitaria del Servicio Madrileño de Salud.
• **Alfonso Martín Palma**, Gerente *Senior* del Departamento Sistemas de Seguridad de Indra.

10:45h. Coloquio.

10:50h. **Ponencia: El día a día del gobierno de la seguridad en un entorno de multiexternalización.**
Ponente: Tomás Roy Catalá, Director del Área de Calidad, Seguridad y Relaciones con Proveedores del Centro de Telecomunicaciones y Tecnologías de la Información de la Generalitat de Cataluña.

11:25h. Coloquio.

11:30h. Pausa-café.

12:00h. **Ponencia: ONO: el Plan de Seguridad 2009-2011. Fundamentos, orientación y alcance.**
Ponente: Miguel Ángel Rego Fernández, Director de Seguridad Corporativa de ONO.

12:35h. Coloquio.

12:40h. **Debate: Prioridades de actuación en la agenda del responsable de seguridad TIC.**
Intervienen:
• **Rafael Hernández González**, Responsable de Seguridad TI de Cepsa.
• **Tomás Villalba de la Luz**, Coronel Jefe de la Oficina de Seguridad de los Sistemas de Información y Comunicaciones, y del Servicio de Innovación Tecnológica. Guardia Civil.
• **Marcos Gómez Hidalgo**, Subdirector de eConfianza de Inteco.
• **Juan Ignacio Sánchez Chillón**, Adjunto al Director General de Seguridad y Medio Ambiente. Mapfre.

14:00h. Fin del debate.

14:05h. Almuerzo.

16:00h. **Ponencia: Grupo FCC: la experiencia del usuario en la puesta en marcha de una solución de auto-servicio para la gestión de accesos.**
Ponentes:
• **José Luis Tortajada Pastor**, Director de Tecnología. División de Sistemas y Tecnologías de la Información de Grupo FCC.
• **Juan Nemiña Gantes**, SWG Tivoli Technical Sales Specialist de IBM.

16:35h. Coloquio.

16:40h. **Ponencia: Banco de España: evolución de la normativa de seguridad.**
Ponentes:
• **Santiago Calvo Cueto**. Unidad de Seguridad Informática, División de Gestión Interna y Seguridad. Banco de España.
• **Javier Fernández-Sanguino Peña**. Subdirector de Seguridad TIC. Germinus XXI (Grupo Gesfor).

17:15h. Coloquio.

17:20h. Pausa-café.

17:45h. **Ponencia: Adecuación y adaptación NAC de la red de acceso y núcleo de los servicios de la Consejería para la Igualdad y Bienestar Social de la Junta de Andalucía.**
Ponentes:
• **Martín Ayastuy López**, Jefe del Servicio de Informática de la Consejería para la Igualdad y Bienestar Social de la Junta de Andalucía.
• **Raúl Díaz Pérez**, Gerente de Soluciones de Datos de Siemens Enterprise Communications.

18:20h. Coloquio.

18:25h. **Clausura de Securmática 2009.**

NEGOCIOS DIVERSOS. EL RETO DE UNA SEGURIDAD CORPORATIVA: EL PLAN DIRECTOR DE ICM

Sinopsis: El Comité de Dirección de ICM –la Agencia que, en el marco de la Comunidad de Madrid, tiene como misión dar respuesta a las necesidades de su administración en el ámbito de la informática y las comunicaciones–, a través de su Dirección de Seguridad Corporativa, decidió abordar la ejecución de un Plan Director de Seguridad Corporativo e Integral, en las diferentes Consejerías e incluyendo aspectos relativos a seguridad de los activos de información, regulatorios y del patrimonio. La metodología empleada por PricewaterhouseCoopers, que le apoyó durante todo el proceso, se basa en el estándar ISO 27002, en el análisis de la legislación vigente aplicable, así como en las mejores prácticas de mercado, incluyendo la seguridad de las personas y el patrimonio. El enfoque desarrollado tuvo en cuenta la estrategia de cada Consejería y las líneas de servicio que ICM ofrece a cada una de éstas, con la finalidad de priorizar los requisitos de seguridad alineados a los objetivos estratégicos de la Comunidad de Madrid, a las líneas de servicio ofrecidas al ciudadano y a los planes de sistemas de información sectoriales. El resultado del proyecto es una gestión integral de la seguridad a través del Marco Normativo y de Gobierno de la función de seguridad basado en el riesgo y gestionado a través de un sistema de control que permite medir la mejora de los niveles de madurez de la Seguridad de la Información en la Comunidad de Madrid.

Ponentes

• **Fernando Ledrado Gómez** es el Director de Seguridad Corporativa de la Agencia de Informática y Comunicaciones de la Comunidad dde Madrid (ICM). Su trayectoria profesional se inició en el Área de Derecho y Asesoramiento de la TI de ICM, hasta ocupar su actual responsabilidad en materia de seguridad de la tecnologías de la información, cumplimiento normativo y seguridad de los activos y el patrimonio. Ledrado es licenciado en Derecho por la Universidad Autónoma de Madrid y ha cursado diferentes Másteres en Asesoría y Consultoría de Derecho de las Tecnologías de la Información, Dirección de Seguridad de la Información y Relaciones Laborales.

• **Elena Maestre García** es la Directora responsable en España del Área de Riesgos Tecnológicos de PricewaterhouseCoopers. Su trayectoria profesional se inició en el área de auditoría informática de una Entidad Financiera, para posteriormente desarrollarse en el ámbito de la consultoría de seguridad, donde tiene una trayectoria profesional de más de diecinueve años. Elena Maestre es licenciada en Ciencias Económicas y Empresariales por la Universidad Autónoma de Madrid y dispone de las certificaciones CISA, CISM, CGEIT y Lead Auditor BS 25999-2.

LA GESTIÓN DE LA SEGURIDAD TIC EN EL ÁMBITO SANITARIO: EL CASO DE LA COMUNIDAD DE MADRID

Sinopsis: Proporcionar servicios TIC a una organización de la envergadura de la Consejería de Sanidad de la Comunidad de Madrid, con una realidad compleja, conformada por una Red de Centros Sanitarios de características variadas, teniendo en cuenta la alta criticidad de dichos servicios en lo que su importancia para la prestación asistencial sanitaria se refiere, hacen que se multiplique la dificultad para una adecuada gestión de la seguridad TIC. A esto hay que sumar otros factores de especial relevancia, sobre todo desde el punto de vista de la Seguridad TIC: la sensibilidad de los datos que se manejan en el sector de la Sanidad, tal y como viene demostrando la legislación en materia de protección de datos de carácter personal; la preocupación por preservar los derechos de los ciudadanos, que tiene su reflejo en la Ley de Autonomía del Paciente; las iniciativas para implantar la Libre Elección de Médico o la Historia Clínica Única y su impacto en los actuales sistemas de información y en la cultura de los usuarios de los mismos. En esta ponencia se describirán las medidas que, en el ámbito de la Seguridad TIC, se están tomando en la Consejería para afrontar los retos que suponen todos estos cambios, para gestionar la seguridad de los datos y de los sistemas de información que los tratan.

Ponentes

• **José Manuel Laperal González** ejerce desde su puesto en la Agencia de Informática y Comunicaciones de la Comunidad de Madrid, las funciones de Responsable de Seguridad, Planificación e Innovación de la Dirección General de Sistemas de Información Sanitaria del Servicio Madrileño de Salud. Ingeniero Informático por la Universidad Pontificia de Salamanca ha desarrollado su carrera profesional en grandes organizaciones como Digital Equipment Corporation, Oracle Ibérica, PricewaterhouseCoopers o la propia Comunidad de Madrid. Cuenta con más de 20 años de experiencia profesional en el ámbito de los sistemas de información y consultoría, la mayor parte de ellos en ámbito de la seguridad.

• **Alfonso Martín Palma** Gerente Senior en el departamento de Sistemas de Seguridad de Indra. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid, CISA, CISM y GGEIT por la ISACA, ha desarrollado su carrera profesional en GFI, Thales, Magari, Azertia y actualmente en Indra. Cuenta con más de 14 años de experiencia en seguridad de la información habiendo dirigido proyectos de gestión de identidades y acceso, consultoría de seguridad, securización de infraestructuras TI, PKI, sistemas de gestión de seguridad de la información y oficinas técnicas de seguridad.

EL DÍA A DÍA DEL GOBIERNO DE LA SEGURIDAD EN UN ENTORNO DE MULTIEXTERNALIZACIÓN

Sinopsis: El gobierno de la seguridad consiste en un proceso de gestión y de liderazgo, a través de una gerencia constante, políticas cohesivas, procesos y toma de decisiones en el área de responsabilidad de la seguridad. El necesario equilibrio entre eficiencia y participación, interacción entre funciones que no obedecen a una subordinación jerárquica, sino a una integración sistémica compleja, se traslada a lo largo de la organización, departamentos y se realiza en sus recursos internos y externos. El modelo de relación en la externalización es fuertemente de subordinación jerárquica, dificultando, en el día a día, la traslación de los logros de integración sistémica de la organización. En un entorno multiexternalizado el reto es arduo, y la mejor estrategia es la concreta orientación a la provisión e innovación de los servicios del cliente.

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.

ONO: EL PLAN DE SEGURIDAD 2009-2011. FUNDAMENTOS, ORIENTACIÓN Y ALCANCE

Sinopsis: En junio de 2008, ONO decide afrontar un modelo de gestión de la seguridad capaz de integrar la protección de sus activos de información con la de los activos patrimoniales. Para alcanzar este objetivo, se crea una dirección de Seguridad Corporativa basada en un modelo organizativo orientado a procesos, que busca la segregación de funciones y la integración completa entre las áreas tradicionales de seguridad. Desde entonces se ha venido trabajando en la definición de un plan de seguridad, cuya ejecución ya ha comenzado, que tiene líneas de acción orientadas a la revisión y mejora de las políticas de seguridad, la integración del modelo de seguridad en la compañía y la mejora de las infraestructuras de seguridad lógica y física. El objetivo final es optimizar la gestión de los incidentes de seguridad y contribuir a la prevención del fraude.

Ponente

• **Miguel Ángel Rego Fernández** es Director de Seguridad Corporativa de ONO desde junio de 2008. Hasta su incorporación a este operador de telecomunicaciones, y desde 2003, ocupó el cargo de Responsable de Seguridad TIC en la Inspección General CIS del Ministerio de Defensa. Rego es Oficial de la Escala Superior del Cuerpo de Intendencia de la Armada, Diplomado en Estudios Avanzados en Ingeniería Informática (Universidad Pontificia de Salamanca), Especialista en Seguridad Corporativa y Protección del Patrimonio (Universidad Europea de Madrid), Máster en Auditoría de Sistemas, Analista de Sistemas Rama de Gestión (Escuela de Informática de La Armada) y Especialista en Criptología (CCN-Centro Criptológico Nacional). Actualmente es Director Académico del Máster en Dirección y Gestión de Seguridad organizado por Asimelec y la UPM. Posee las siguientes certificaciones: ISO/IEC 2000 Foundation, ITIL Service Manager, Foundation Certificate in IT Service Management, CISM y CISA.

GRUPO FCC: LA EXPERIENCIA DEL USUARIO EN LA PUESTA EN MARCHA DE UNA SOLUCIÓN DE AUTO-SERVICIO PARA LA GESTIÓN DE ACCESOS

Sinopsis: FCC detectó un problema en la gestión de usuarios que había provocado una falta de actualización en los datos de los mismos. La necesidad de cumplir con la Responsabilidad Social Corporativa aconsejaba corregir las discrepancias para poder asegurar la identidad de los usuarios que introducen datos en los sistemas Económico-Financieros. FCC lanzó un Proyecto de Gestión de Identidades, unido a otro de Auditoría de los Accesos a la Información para solventar el problema. Se comenta el desarrollo del proyecto, las incidencias que se experimentaron y los logros que se consiguieron.

Ponentes

• **José Luis Tortajada Pastor** es Director de Tecnología en la División de Sistemas y Tecnologías de la Información de Grupo FCC. Empleado de FCC (antes FOCSA) desde hace 33 años, Tortajada siempre ha ocupado puestos relacionados con la Ingeniería de Sistemas. Desde la fusión de FOCSA y CYCSA ocupó el cargo de Director de Sistemas y Comunicaciones. En la actualidad desarrolla proyectos especiales y participa en el equipo de Reingeniería de Procesos.

• **Juan Nemiña Gantes** es SWG Tivoli Technical Specialist de IBM. Ingeniero Superior de Telecomunicaciones por la UPB, trabaja en IBM desde 1990, año en el que se incorpora al Centro Internacional de Desarrollo de Barcelona. A partir de 1994 pertenece a distintas unidades de servicios de IBM, desempeñando diferentes roles en proyectos siempre relacionados con la gestión de sistemas y la seguridad, hasta su incorporación en 2000 a la division de software Tivoli de IBM España. Dentro de la organización de Tivoli, ha desempeñado funciones de técnico especialista, arquitecto y consultor en productos de seguridad para finalmente, en los últimos tres años, ser responsable comercial de la venta de software de seguridad en distintos sectores del mercado español.

BANCO DE ESPAÑA: EVOLUCIÓN DE LA NORMATIVA DE SEGURIDAD

Sinopsis: Las funciones desempeñadas por el Banco de España, órgano supervisor y regulador del sistema financiero español, han sufrido una serie de transformaciones a lo largo del tiempo. Algunas de ellas consecuencia de la integración en el Sistema Europeo de Bancos Centrales y otras fruto de las demandas internas y externas. El desarrollo de nuevos servicios, así como la aparición de estándares internacionales (como ISO 27001 o ITIL) y estándares propios del Banco Central Europeo han tenido un impacto significativo en el proceso de revisión de las normas de seguridad propias del Banco en sus distintos entornos. La presentación describirá este proceso de evolución, las fuerzas, los actores y las experiencias que de él se derivan.

Ponentes

• **Santiago Calvo Cueto** es responsable de Proyectos de Seguridad en Redes del Banco de España, entidad de la que forma parte desde hace más de 20 años. Licenciado en Ciencias Físicas por la UAM, su trayectoria profesional ha estado siempre ligada al campo de la seguridad en sistemas de información. Sus principales funciones como miembro de la Unidad de Seguridad Informática han sido la realización de análisis de riesgos de aplicaciones y nuevas tecnologías, auditoría de los entornos tecnológicos, y el desarrollo de proyectos de integración de plataformas de seguridad con nuevos servicios y aplicaciones en los entornos de interconexión con redes privadas y con internet del Banco.

• **Javier Fernández-Sanguino Peña** es Subdirector de Seguridad TIC del Grupo Gesfor. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid (UPM), desde hace diez ha liderado y desarrollado, como jefe de proyecto, consultor y auditor, multitud de proyectos de seguridad en diversos sectores: administraciones públicas, banca y operadores de telecomunicación. Antes de unirse a Germinus XXI, empresa integrada dentro del Grupo Gesfor en el año 2008, trabajó en Soluciones Globales Internet S.A.

ADECUACIÓN Y ADAPTACIÓN NAC DE LA RED DE ACCESO Y NÚCLEO DE LOS SERVICIOS DE LA CONSEJERÍA PARA LA IGUALDAD Y EL BIENESTAR SOCIAL DE LA JUNTA DE ANDALUCÍA

Sinopsis: La Consejería para la Igualdad y Bienestar Social de la Junta de Andalucía, tiene como objetivo sentar las bases para la aparición de nuevos escenarios de intervención y participación en la búsqueda de respuestas a las necesidades de las personas mayores, personas con discapacidad, familias, drogodependencia, violencia de género, menores y jóvenes desde cualquier condición o situación especial. Para el desarrollo de sus planes, la interacción con las entidades y los ciudadanos, la Consejería ha implantado una oficina virtual, con un principio fundamental de funcionamiento: un alto nivel seguridad de los datos personales, al ser de carácter personal que regula las medidas de seguridad de los ficheros automatizados de este tipo el Real Decreto 994/1999, de 11 de junio. No es de extrañar que los requerimientos exigidos para la infraestructura de comunicaciones sean los mismos: seguridad, calidad y disponibilidad, criterios que sólo pueden ser asumidos por una basada en Control de Acceso (NAC). La red de comunicaciones finalmente implantada, se basa en la filosofía Secure Networks de Enterasys, que autentica y autoriza granularmente el acceso a los servicios y los datos por parte de los usuarios, según sus perfiles y roles dentro de la organización. El análisis de los servicios, la integración con los roles corporativos, y la traslación a conceptos de Control de Acceso a la Red (NAC) ha sido realizada por Siemens Enterprise Communications.

Ponentes

• **Martín Ayastuy López** es Jefe de Informática de la Consejería para la Igualdad y Bienestar Social de la Junta de Andalucía. Licenciado en Matemáticas en la especialidad de Estadística e Investigación Operativa por la Universidad de Sevilla, es funcionario de carrera Grupo A superior facultativo especialidad A2019 Informática. Anteriormente a su puesto actual –que desempeña desde 2001– ha sido, sucesivamente, Jefe de Proceso de Datos de las Consejerías de Agricultura y Pesca, y de Igualdad y Bienestar Social en la delegación provincial de la Junta de Andalucía en Málaga. Asimismo, ha trabajado en el Departamento de Investigación y Desarrollo de Fujitsu España.

• **José Raúl Díaz Pérez** es Gerente de Soluciones de Datos de Siemens Enterprise Communications. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid, en los más de 10 años colaborando en Siemens, ha liderado varias áreas tecnológicas como responsable y desarrollador de negocio, entre las que cabe destacar las áreas de sistemas y soluciones de gestión de redes y servicios IP, soluciones y servicios de *datacenters*, y actualmente en el área de Data Solutions.

DEBATE

PRIORIDADES DE ACTUACIÓN EN LA AGENDA DEL RESPONSABLE DE SEGURIDAD TIC

Los tiempos actuales están marcados, además de por una preocupación creciente por la seguridad de la información, la prevención del fraude y el cumplimiento legal y normativo, por la contención presupuestaria, la búsqueda de eficiencia, la reutilización, la optimización, la simplificación de procesos y la tendencia incipiente en algunos sectores a la convergencia de los distintos frentes de la seguridad. En esta coyuntura, ¿qué prioridades se marcan a corto y medio plazo los responsables de seguridad de la información y TIC? ¿Qué proyectos tienen en cartera? ¿Qué revisiones se están planteando o se han planteado en los Planes Directores aprobados en sus organizaciones?

Intervienen

• **Rafael Hernández González** es Responsable de Seguridad TI del Grupo CEPSA. Ingeniero Superior de Telecomunicaciones por la UPM, dispone de una larga experiencia profesional, que inició en 1988 como Ingeniero de Desarrollo en Amper Datos. En 1989 ingresó en Cepsa como Técnico de Desarrollo y, posteriormente, Ingeniero de Redes (infraestructuras y Sistemas de Red). Desde 2003 viene desarrollando diferentes funciones en el Área de Seguridad dentro de la Dirección de Sistemas de Información. En la actualidad es reponsable del Sistema de Gestión de Seguridad de la Información-SGSI del Grupo Cepsa.

• **Marcos Gómez Hidalgo** es Subdirector de eConfianza del Instituto Nacional de Tecnologías de la Comunicación (INTECO), dependiente del Ministerio de Industria, Turismo y Comercio. Como tal, dirige la línea de seguridad de la entidad, en la que se encarga de los servicios del INTECO-CERT, Centro de Respuesta a Incidentes en TIC, y del Centro Demostrador de Tecnologías de Seguridad. Licenciado en Ciencias Matemáticas por la UCM, ha desempeñado diversos puestos de responsabilidad en Sema Group (Atos Origin). Trabajó en Red.es como Responsable del Centro de Alerta Temprana sobre Virus y Seguridad Informática y Responsable de Sistemas de Información, y como profesor de Ingeniería Informática de la Universidad Camilo José Cela de la Institución educativa SEK, así como en diversos másteres de postgrado en seguridad de la información.

• **Tomás Villalba de la Luz** es el Coronel Jefe de la Oficina de Seguridad de los Sistemas de Información y Comunicaciones de la Guardia Civil y del Servicio de Innovación Tecnológica. Posee gran experiencia (desde 1980) en el ámbito de las TIC, tanto en el área de sistemas, como en las de comunicaciones y explotación. Es Diplomado en Informática Militar, en Análisis Informático de la Guardia Civil, Especialista en Estadística Militar, con estudios de informática en la Universidad Pontificia de Salamanca, y ha asistido a multitud de congresos y cursos en organismos privados nacionales e internacionales, y de la Administración Pública.

• **Juan Ignacio Sánchez Chillón** es Adjunto al Subdirector General de Seguridad y Medio Ambiente de Mapfre, cargo en el que tiene dos responsabilidades básicas, la de Dirección de Continuidad de Negocio de Mapfre en el ámbito corporativo, y la de Coordinación de los Jefes de Seguridad de las entidades de Mapfre. Licenciado en Informática (actualmente Ingeniero en Informática) por la UPM, es Máster en Auditoría Informática por la UPM, experto en Gerencia de Riesgos y Seguros y posee las certifcaciones CISA y IT Service Management (ITIL). Es profesor titular de los másteres de Seguridad y Auditoría Informática de la UPM. 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. Antes de su incorporación a esta multinacional del sector asegurador desempeñó diversos puestos de responsabilidad en el sector de la consultoría y los servicios profesionales en Eria (actualmente Indra), Norsistemas (actualmente Indra) y PricewaterhouseCoopers.

> SECURMATICA, a escena

Panorámica de SECURMÁTICA 2008

> Premios SIC 2009

En coincidencia con la celebración de la XX edición de Securmática, tendrá lugar el acto de entrega de los VI 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 quinta edición de los premios SIC

LA HORA DEL REENCUENTRO Y LOS RECONOCIMIENTOS

> Cena de la Seguridad

SECURMATICA 2009

21.22.23/abril

XX Congreso español de Seguridad de la Información

AFORO LIMITADO

> Fechas y lugar

SECURMÁTICA 2009 tendrá lugar los días 21, 22 y 23 de abril de 2009 en el hotel NOVOTEL*. Campo de las Naciones de Madrid.

> Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2009 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 VI Premios SIC (22 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 sólo 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 2009

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 21 ❑ MÓDULO 2 DÍA 22 ❑ MÓDULO 3 DÍA 23 ❑ Deseo inscribirme a SECURMATICA 2009 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**