SECURMATICA

XVIII Congreso español de Seguridad de la Información

2007

24, 25 y 26 de abril

HOTEL NOVOTEL
CAMPO DE LAS NACIONES
MADRID

PROGRAMA

Securmática 2007, XVIII edición del Congreso español de Seguridad de la Información, organizado por la revista SIC, tendrá lugar los días 24, 25 y 26 de abril del presente en su tradicional sede del Campo de las Naciones de Madrid.

El ramo específico de protección de la información y de seguridad de las tecnologías y los sistemas que la tratan, se encuentra hoy en un momento crucial en el que por fin el amplio sector de TIC empieza a metabolizar la necesidad, manifestada reiteradamente por los usuarios, de encontrar soluciones integradas, interoperables y de calidad que puedan ayudar a gestionar la complejidad y contribuir al desarrollo de servicios electrónicos, informáticos y telemáticos fiables y aptos para servir al perfeccionamiento de actos de los que se deduzca el ejercicio de derechos y el cumplimiento de obligaciones.

Securmática 2007, a través de este programa, ofrecerá una visión profesional y panorámica de lo que se está haciendo en empresas y administraciones, a través de la presentación de proyectos de valor, expuestos por sus protagonistas.

ES HORA DE COMPARTIR EXPERIENCIAS >>> Y AVANZAR

Al tiempo, se tratarán asuntos de interés profesional específico en todos los órdenes de la protección y la seguridad de la información (organizativo, legal y tecnológico), y se debatirán dos realidades que marcan hoy la dinámica en la función profesional de los CISOS: de una parte, el de la incidencia del 'cumplimiento normativo', y de otra, el vinculado con la necesidad o no de disponer de herramientas evolucionadas de ayuda a la toma de decisiones en seguridad.

Copatrocinadores:

Deloitte. · Ernst & Young Quality In Everything We Do · germinus · Grupo Gesfor · gmv · hp invent · IBM · Indra · KPMG · PricewaterhouseCoopers · S21sec · sia · Siemens · Telefónica

Organiza:

Revista SIC seguridad en informática y comunicaciones

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

PRIMER MÓDULO 24 de abril

08:45h. Entrega de documentación.
09:15h. Inauguración.
Moderador: **Carlos Galán Pascual**, Presidente de la Agencia de Tecnología Legal y Profesor de la Universidad Carlos III de Madrid.
10:00h. Conferencia de apertura: **El proyecto de reglamento de desarrollo de la LOPD.**
Ponente: **Agustín Puente Escobar**, Abogado del Estado y Jefe del Gabinete Jurídico de la Agencia Española de Protección de Datos.
10:40h. Coloquio.
10:45h. Ponencia: **La credibilidad del CISO.**
Ponente: **Santiago Moral Rubio**, Director de Seguridad Lógica Corporativa del Grupo BBVA.
11:25h. Coloquio.
11:30h. Pausa-café
Moderador: **José Manuel Vidal Formoso**, Presidente de ASIA.
12:00h. Ponencia: **Mapfre: Plan de concienciación y sensibilización de seguridad de la información.**
Ponentes:
Juan Ignacio Sánchez Chillón, Jefe del Departamento de Seguridad de la Información de MAPFRE.
José María González Souto, Responsable del Área Internacional. Departamento de Seguridad de la Información de MAPFRE.
12:40h. Coloquio.
12:45h. Ponencia: **Desarrollo de una herramienta de auditoría informática a distancia para el Banco Popular.**
Ponentes:
José Antonio Rodríguez, Responsable de Auditoría Informática del Grupo Banco Popular.
Javier Urtiaga Baonza, Director de Technology and Security Risk Services de Ernst & Young.
13:25h. Coloquio.
13:30h. Debate: **La incidencia del cumplimiento normativo en la función del responsable de seguridad de la información.**
Moderador: **José de la Peña Muñoz**, Director de la revista SIC.
Intervienen:
• **Joaquín Álvarez Pérez**, Subdirector de Normativa y Coordinador de Seguridad de la Información. Endesa.
• **Daniel Barriuso Rojo**, Director de Seguridad de la Información para Europa. ABN AMRO.
• **José Antonio Castro González**, Director de Seguridad Corporativa del Grupo Santander.
• **Mar Sánchez Caro**, Directora de Seguridad Corporativa de BT España y Latinoamérica.
14:30h. Almuerzo.
Moderador: **Tomás Arroyo Salido**, Consultor independiente.
16:30h. Ponencia: **Basilea II: una aplicación de seguridad informática.**
Ponentes:
Ángel Torregrosa Salcedo, Jefe de Auditoría a Distancia. Caja de Ahorros del Mediterráneo.
Daniel Solís Agea, Gerente Senior. SPC (Security, Privacy & Continuity) IT Advisory KPMG.
1710h. Coloquio.
17:15h. Ponencia: **Gestión de seguridad operacional en Telefónica Móviles España.**
Ponentes:
José Luis Gilpérez López, Gerente de Seguridad de Redes y Servicios. Telefónica España.
Félix Martín Rodríguez, Jefe de Proyecto de la Práctica de Seguridad de HP Consulting & Integration.
17:55h. Coloquio.
18:00h. Pausa-café
18:15h. Ponencia: **Consolidación y simplificación de la arquitectura de comunicaciones y seguridad de la IGAE.**
Ponentes:
Francisco Javier González Rodríguez, Subdirector General de Explotación Informática en la Intervención General de la Administración del Estado (IGAE).
Jorge Hurtado Rojo, Subdirector de Desarrollo de Negocio de Servicios de Seguridad Lógica. Grupo Gesfor.
18:55h. Coloquio.
19:00h. Fin de la primera jornada.

EL PROYECTO DE REGLAMENTO DE DESARROLLO DE LA LOPD

Ponente:

< Agustín Puente Escobar es Licenciado en Derecho y Ciencias Económicas y Empresariales por la Universidad Pontificia Comillas (ICADE-Madrid) es Abogado del Estado desde 1994. Ha desempeñado los cargos de: Abogacía del Estado ante el Tribunal Superior de Justicia de Cataluña (1994-1996); Jefe del Gabinete del Subsecretario de Industria y Energía (1996-1998); Abogacía del Estado en el Ministerio del Interior (1998-1999), y Consejero Pre-Adhesión en Programa PHARE para el desarrollo legislativo de las normas comunitarias sobre protección de datos de carácter personal y la creación de la Oficina Checa para la protección de Datos (Praga, octubre de 2001 – septiembre de 2002).

LA CREDIBILIDAD DEL CISO

Sinopsis:
La credibilidad del CISO, como la de cualquier otro ejecutivo, está estrictamente relacionada con los aciertos y los "fracasos" de las decisiones que adopta y de la trascendencia de las mismas. Objetivar las decisiones, sabiendo *a priori* cuáles están basadas en "hechos reales" y cuáles en situaciones futuras que se supone que pueden darse, incorporando en las mismas la subjetividad de su propia corporación, se conforma como uno de los elementos fundamentales de la gestión del CISO.
La credibilidad del CISO debe ser mayor y gestionada con más firmeza que la del resto de los ejecutivos de tecnología, dado que su apuesta sobre el futuro no está ligada al devenir interno de la evolución de los sistemas, sino a la intencionalidad de un atacante externo; en este sentido, los "opinódromos" en el ámbito de la seguridad de la información, son una de las mayores amenazas a las que nos enfrentamos.

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 de ISACA, 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. Actualmente es director de Seguridad Lógica Corporativa del Grupo BBVA.

MAPFRE: PLAN DE CONCIENCIACIÓN Y SENSIBILIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Sinopsis:
El Plan de Concienciación y Sensibilización se lleva a cabo como desarrollo de las acciones resultantes del Plan Director de Seguridad. Dirigido a todo el personal de MAPFRE en España y sobre la base de un "Temario de Conocimientos", se desarrollaron los conceptos que, posteriormente, fueron trasladados a los distintos soportes utilizados para su divulgación, partiendo de la conocida premisa de que *"la cadena es tan débil como el más débil de sus eslabones"*, y teniendo en cuenta que, en este caso, dicho eslabón lo constituyen las personas de la Organización. Es evidente que un proyecto tan ambicioso como el Plan Director no podría tener éxito sin la participación e implicación del colectivo de empleados, por lo que se involucró a la práctica totalidad de empleados en España en alguna de las actividades desarrolladas.

Ponente:

< Juan Ignacio Sánchez Chillón es Licenciado en Informática por la Universidad Politécnica de Madrid (UPM), Master en Auditoría Informática por la UPM y Profesor Titular de los Master de Seguridad y Auditoría Informática de esta Universidad. Desde hace un año y medio desempeña el puesto de Jefe del Departamento de Seguridad de la Información de MAPFRE. Durante los diez años anteriores ha sido el Responsable de los Servicios de Auditoría Informática de MAPFRE en España y coordinador de las actuaciones en el exterior.

< José María González Souto es Responsable del Área Internacional de Seguridad de la Información de Mapfre, dentro del Departamento de Seguridad de la Información. Ingeniero de Telecomunicaciones por la Universidad de Vigo, posee un Máster en Gestión de empresas de telecomunicaciones de la EOI, un Máster en Gerencia de Riesgos y seguros en la Empresa de la Universidad Pontificia de Salamanca, y las certificaciones profesionales CISA y CISM, de ISACA, y CISSP, de ISC[2]. Con anterioridad a su actual responsabilidad, en la que lleva dos años, y durante los seis años anteriores, desempeñó diferentes puestos en Deloitte & Touche (antiguo Andersen), en los que participó en el desarrollo de múltiples proyectos relacionados con el ambito de control de las TI: definición y desarrollo de planes estratégicos de seguridad a nivel internacional, definición de marcos de referencia en seguridad de la información, mejora de procesos tecnológicos, establecimiento de organizaciones de seguridad y auditoría, evaluación, selección e implantación de soluciones.

DESARROLLO DE UNA HERRAMIENTA DE AUDITORÍA INFORMÁTICA A DISTANCIA PARA EL BANCO POPULAR

Sinopsis:

En esta conferencia se presentará la nueva herramienta de Auditoría a Distancia y Cuadro de Mandos de Seguridad, AUDITTA, desarrollada por el departamento de TSRS de Ernst&Young, en colaboración con Banco Popular. El objetivo fundamental de esta herramienta consiste en poder visualizar el estado y grado de evolución en seguridad de los sistemas de información de una entidad de una forma automatizada. Esta perspectiva se presenta contrastando los resultados en relación al cumplimiento de políticas y normativas tales como ISO-17799, CobiT, LOPD o Basilea II, etc. Del mismo modo, es posible conocer la situación de los sistemas de información frente a estándares reconocidos como ISO 27001, o cumplimiento de la ley Sarbanes-Oxley. La presentación se centrará en mostrar las funcionalidades de AUDITTA, sus métodos de recogida de datos de los sistemas y el modo en que éstos deben ser tratados para obtener indicadores precisos y fiables. Asimismo, se describirá la experiencia de la puesta en producción de AUDITTA en los sistemas de Banco Popular.

Ponentes:

< José Antonio Rodríguez González, es responsable de Auditoría Informática del Grupo Banco Popular. Técnico en Informática de Gestión y Técnico en Mantenimiento de Aeronaves, desde su incorporación al Grupo Banco Popular en 1991 ha desarrollado diversas funciones en Tecnologías de la Información, entre otras las correspondientes a la gestión del área de soporte técnico a usuario, la integración de sistemas y la de responsable de comunicaciones y redes.

< Javier Urtiaga Baonza es ingeniero de Telecomunicaciones por la UPC y Executive MBA por el Instituto de Empresa. Cuenta con amplia experiencia en el ámbito de la seguridad de la información, habiendo desempeñado su trabajo en este sector en los últimos ocho años. Actualmente ocupa el cargo de Director de Operaciones en el departamento de TSRS de Ernst & Young y responsable de la coordinación del Sector Financiero. Del mismo modo, coordina el Advanced Security Lab (Centro de Competencias de seguridad técnica avanzada para el sur de Europa). Adicionalmente, se encarga de coordinar el desarrollo de soluciones orientadas a los riesgos vinculados con la tecnología, tanto en el ámbito estratégico como en el técnico.

BASILEA II: UNA APLICACIÓN DE SEGURIDAD INFORMÁTICA

Sinopsis:

El Comité de Supervisión Bancaria de Basilea ha adaptado el marco de gestión de riesgos aplicable en general a todas las actividades bancarias a las características específicas de la Banca Electrónica en los Principios de Gestión de Riesgos para Banca Electrónica. Para ello, se han descrito 14 principios de gestión del riesgo divididos en tres grandes áreas: Controles de Gestión TI, Controles de Seguridad y Riesgos legales y reputacionales. En la ponencia se describirá el procedimiento seguido por la Caja de Ahorros del Mediterráneo para verificar el cumplimiento de dichos principios, adaptado a su idiosincrasia y a su perfil de riesgo, complementando esta revisión con otros estándares y códigos de buenas prácticas como: ITIL, ISO 17799, etc. Asimismo se describirá el valor proporcionado por esta iniciativa y las sinergias con otras iniciativas conducentes a perfeccionar la gestión de riesgos tecnológicos en la entidad.

> DEBATE

LA INCIDENCIA DEL CUMPLIMIENTO NORMATIVO EN LA FUNCIÓN DEL RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

Proposición: La mención en leyes generales o específicas –en diversas aproximaciones, y de forma explícita o implícita–, códigos de buen gobierno y estándares internacionales basados en prácticas aconsejables de la pertinencia de la protección de la información y la seguridad de los sistemas tecnológicos destinados a su tratamiento, obliga a que empresas y organismos orienten sus políticas y normas internas de tratamiento de la información al objetivo del cumplimiento. Algunas entidades multinacionales, incluso, tienen que encarar esta circunstancia en un ambiente multisectorial y multilegislativo.

En el debate se intentará profundizar en la identificación de lo que hay que entender por cumplimiento en el contexto, su incidencia en la función de seguridad de la información y en la función de auditoría y revisión, y la respuesta que está ofreciendo la industria de seguridad TIC para satisfacer las necesidades de las organizaciones en esta materia.

Intervienen:

< Joaquín Álvarez Pérez es Subdirector de Normativa y Coordinador de Seguridad de la Información de Endesa. Ha desarrollado parte de su carrera profesional en el ámbito de los sistemas de información, donde ha dirigido proyectos relacionados con diversas áreas de la compañía. Durante los últimos ocho años ha centrado su actividad profesional en el desarrollo organizativo, en el diseño de los procesos de negocio y en el desarrollo de la función de seguridad de la información. Además de en el sector de la energía, que es donde está actualmente, ha trabajado en el sector de las telecomunicaciones y en el de la electromedicina. Es Licenciado en Derecho, Ingeniero de Telecomunicaciones y Máster en Consultoría Estratégica de las Organizaciones.

< Daniel Barriuso Rojo es Director de Seguridad de la Información para Europa en ABN AMRO, donde tiene responsabilidad sobre la gestión de la seguridad en 28 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. Previamente a su actual puesto, ha sido Director del Departamento de Análisis de Riesgos Tecnológicos para Europa y Mercados Globales en ABN AMRO y Director del Departamento de Seguridad de Credit Suisse España. Desde 2002, imparte clases como profesor en el Master de Seguridad y Auditoría de la Universidad Politécnica de Madrid sobre el gobierno y la gestión de la inversión en seguridad. Es Ingeniero Superior en Informática por la Universidad Carlos III de Madrid y está certificado como Lead Auditor BS7799.

< 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 (19 años) en 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 en el ámbito de la seguridad de la información. Cuenta con trece 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.

< Mar Sánchez Caro es actualmente Directora de Seguridad Corporativa de BT España y Latinoamérica, y con anterioridad Country Security Manager de BT Global Services España. Entre sus responsabilidades se encuentran la coordinación del Comité de Seguridad Corporativo, la implantación de iniciativas de seguridad, la coordinación del Gabinete de Crisis, la responsabilidad en materia de protección de datos y la relación internacional con la empresa matriz.

Ponentes:

< **Ángel Torregrosa Salcedo** es Jefe de Auditoría a Distancia en Caja de Ahorros del Mediterráneo. Torregrosa inicia su carrera profesional en Caja de Ahorros de Alicante y Murcia, hoy Caja de Ahorros del Mediterráneo, y desde hace más de 20 años ha desempeñado su función como auditor interno de la entidad en Auditoría de Red Comercial, Control Interno, Auditoría de Servicios Centrales y Auditoría Informática. Actualmente es Jefe de Auditoría a Distancia con la función de auditoría de sistemas de información. Ha sido ponente en Convenciones de CECA de Auditores Internos, ha sido docente en varios cursos relacionados con LOPD y Auditoría de Sistemas de Información en la Universidad de Alicante y ha realizado estudios universitarios en esta Universidad, así como en la Universidad Oberta de Catalunya.

< **Daniel Solís Agea** es Senior Manager de KPMG. En la actualidad dirige la línea de servicios Security, Privacy and Continuity (SPC) en el área de IT Advisory. Ingeniero en Telecomunicaciones, ha participado en diferentes proyectos de seguridad desarrollando estrategias corporativas en materia de seguridad de la información, como planes directores de seguridad, expansiones internacionales de planes directores de seguridad, Sistemas de la Gestión de la Seguridad de la Información, etc. Por otro lado, Solís ha creado y formado equipos de consultores en seguridad de la información y de *hacking* ético en varias empresas del mercado. Es ISO 27001 Lead Auditor acreditado por IRCA y miembro activo del SC 27.

GESTIÓN DE SEGURIDAD OPERACIONAL EN TELEFÓNICA MÓVILES ESPAÑA

Sinopsis:

La Gerencia de Seguridad de Redes y Servicios –Dirección de Operaciones de Telefónica España– está llevando a cabo un programa para la gestión de amenazas, vulnerabilidades e incidentes de seguridad, un programa diseñado e implementado internamente por la propia HP, con base en el Programa Operacional Security Management (OSM). Este programa ha permitido a la Gerencia de Seguridad racionalizar los procesos y herramientas que utiliza y formalizar el trabajo y las tareas asignadas, definiendo claramente las responsabilidades y funciones que se deben llevar a cabo. El programa permitirá cubrir las necesidades de seguridad en el día a día, desde cómo gestionar proactivamente una amenaza grave a su infraestructura tecnológica, hasta cómo gestionar reactivamente un incidente ocasional o una crisis provocada por un problema de seguridad grave. Durante la ponencia se revisará el modelo y metodología del programa y la experiencia y proceso de implantación en Telefonica.

Ponentes:

< **José Luis Gilpérez López** es Responsable de Seguridad de Redes y Servicios en Telefónica España –Dirección de Operaciones, Supervisión y Operación–. Ingeniero Industrial por la UPM, trabajó en Telefónica de España desde 1998 con diferentes responsabilidades relacionadas con la Red, hasta el año 1997. Desde ese momento hasta 2000 presta sus servicios en Telefónica Móviles como responsable de Gestión Dinámica de Red, y de 2000 a 2002 como Responsable de Soporte y Operación de Firstmark Comunicaciones España. En 2002 fue nombrado Responsable de Seguridad de Redes y Servicios en Telefónica Móviles España –Dirección General de Red–, hasta el momento actual, en el que ocupa el puesto de Responsable de Seguridad de Redes y Servicios en Telefónica España.

< **Félix Martín Rodríguez** es Director de Proyectos de HP Consulting & Integration desde 1999. Ingeniero Superior en Telecomunicaciones, tiene 12 años de experiencia en el área de seguridad lógica. Posee diferentes certificaciones, entre las que pueden mencionarse CISSP e ITIL Service Manager, y experiencia en la implantación de Sistemas de Gestión de Seguridad. Su foco actual es el desarrollo y dirección de servicios de seguridad para clientes de HP. Antes de unirse a Hewlett-Packard Consulting, trabajó para Crisa, empresa de la industria aerospacial, donde fue el responsable de Sistemas de Información y CSO de la compañía.

CONSOLIDACIÓN Y SIMPLIFICACIÓN DE LA ARQUITECTURA DE COMUNICACIONES Y SEGURIDAD DE LA IGAE

Sinopsis:

En los últimos años se observa una tendencia imparable en el mercado de la seguridad hacia la simplificación y gestionabilidad de los sistemas de información. Los antiguos sistemas heterogéneos, las arquitecturas complejas y las redes inmanejables, dan paso a una nueva filosofía que permite reaccionar rápido ante la aparición de nuevas amenazas, y reducir el riesgo asociado a una infraestructura compleja. La Intervención General del Estado, dependiente del Ministerio de Hacienda, representa uno de los más importantes nudos gordianos en cuanto a administración electrónica, con conexiones y servicios telemáticos hacia todas las administraciones públicas, centrales, locales y autonómicas. En esta presentación se expondrán los antecedentes de la Intervención General del Estado y cómo se aborda un proyecto para consolidar, simplificar y monitorizar la arquitectura de seguridad que da servicio a aplicaciones críticas.

Ponentes:

< **Francisco Javier González Rodríguez** es Subdirector General de Explotación Informática en la Intervención General de la Administración del Estado (IGAE). Licenciado en Ciencias Económicas por la Universidad Autónoma de Madrid en 1981, accedió a la función pública por oposición al Cuerpo Superior de Interventores y Auditores del Estado en 1982, ocupando diversos puestos en la Dirección General de Presupuestos y en Intervenciones Territoriales y Delegadas. En 1999 fue nombrado Subdirector General de Explotación Informática en la Intervención General de la Administración del Estado, puesto que ocupa hasta la actualidad.

< **Jorge Hurtado Rojo** es Subdirector de Desarrollo de Negocio de Servicios de Seguridad Lógica de Grupo Gesfor. Ingeniero de Telecomunicaciones, anteriormente dirigió el Área Comercial de Germinus donde se incorporó en 2001, proveniente de SGI Soluciones Globales Internet, donde dirigió el Área de Seguridad Lógica desde 1998. Anteriormente desempeñó funciones técnicas relacionadas con las seguridad en Quark Software & Services y SGI.

SEGUNDO MÓDULO 25 de abril

09:15h. Entrega de documentación.
Moderador: **Jorge Dávila Muro**, Consultor independiente y Director del Laboratorio de Criptografía LSIIS de la Facultad de Informática de la Universidad Politécnica de Madrid.

09:30h. Ponencia: **¿Cómo abordar la seguridad en una Universidad? La experiencia de desarrollar un Plan Director de Seguridad.**
Ponentes:
Luis Padilla Visdómine, Responsable de Seguridad de la Información de la Universidad Complutense de Madrid.
Yolanda del Moral Armenteros, Jefe de Producto. Seguridad de la Información. Siemens Enterprise Communications.

10:10h. Coloquio.

10:15h. Ponencia: **Banco Sabadell: del Plan Director de Seguridad 2002-2006 al nuevo Plan 2007-2009.**
Ponentes:
Xavier Serrano Cossío, Responsable de Seguridad Tecnológica del Grupo Banco Sabadell.
Fernando Pons Ortega, Socio de Enterprise Risk Services-ERS. Deloitte.

10:55h. Coloquio.

11:00h. Pausa-café.
Moderador: **Paloma Llaneza González**, Socio de Llaneza y Asociados Abogados y co-editora de la norma ISO/IEC 27004.

11:30h. Ponencia: **SGSI 27001: el alcance es lo que importa.**
Ponentes:
Jesús Milán Lobo, Gerente de Seguridad. Departamento de Seguridad Informática de Bankinter.
Julio San José Sánchez, Jefe de Proyecto. Departamento de Seguridad Informática de Bankinter.

12:10h. Coloquio.

12:15h. Ponencia: **Departamento de Salud de la Generalitat de Cataluña: Plan Director de Seguridad.**
Ponentes:
Anna García Martínez, Responsable del Programa de Seguridad de la Información del Departamento de Salud de la Generalitat de Cataluña.
Jacobo van Leeuwen, Product Marketing Manager de Seguridad. Grupo SIA.

12:55h. Coloquio.

13:00h. Ponencia: **Grupo FCC: desarrollo del modelo de clasificación de la información.**
Ponentes:
Miguel Cebrián Lindström. Departamento de Seguridad de la Información y Gestión del Riesgo. Grupo FCC.
Alejandro García Nieto. IT Security Leader Spain. IBM

13:40h. Coloquio.

13:45h. Almuerzo.
Moderador: **Javier Areitio Bertolín**, Catedrático de la Facultad de Ingeniería ESIDE y Director del Grupo de Investigación Redes y Sistemas. Universidad de Deusto.

15:45h. Ponencia: **Alternativas tecnológicas para el desarrollo de servicios de seguridad gestionados desde la red.**
Ponente: **Juan Miguel Velasco López-Urda**, Director Asociado de Servicios de Seguridad en RED. UN Grandes Empresas. Telefónica España – Telefónica Soluciones.

16:25h. Coloquio.

16:30h. Ponencia: **EJIE: solución integral de seguridad gestionada.**
Ponentes:
Agustín Elizegi Etxeberria, Director General de EJIE.
Igor Unanue Buenetxea, Director de I+D+i de S21sec.

17:10h. Coloquio.

17:15h. Pausa-café.

17:30h. Ponencia: **Servicio de Monitorización y Alerta Temprana de RBC-Dexia.**
Ponentes:
Javier García Buergo, Jefe de Seguridad de RBC-Dexia.
Mariano J. Benito Gómez, Director de Seguridad / CISO de GMV Soluciones Globales Internet S.A.

18:10h. Coloquio.

18:15h. Fin de la segunda jornada.

20:00h. **Cena de la XVIII edición de Securmática y entrega de los IV Premios SIC.**

¿CÓMO ABORDAR LA SEGURIDAD EN UNA UNIVERSIDAD? LA EXPERIENCIA DE DESARROLLAR UN PLAN DIRECTOR DE SEGURIDAD

Sinopsis:
Los Servicios Informáticos de la UCM han iniciado un proyecto para elaborar un Plan Director de Seguridad de la Información manejada en sus principales actividades con la asistencia de una consultora externa, habiendo resultado Siemens S.A. la empresa adjudicataria del concurso correspondiente. En la conferencia se repasarán las actividades principales que se deducen del Plan y se identificarán aquéllas en las que es más necesaria la colaboración de la Dirección de la Universidad Complutense de Madrid, esencialmente las relacionadas con el análisis de la situación actual, el análisis y la gestión de riesgos y la continuidad de negocio.

Ponentes:

< Luis Padilla Visdómine es Responsable de Seguridad de la Información de la Universidad Complutense de Madrid. Licenciado en Ciencias Físicas por la Universidad Complutense de Madrid (UCM) -Tesis doctoral en el Departamento de Física Atómica, Molecular y Nuclear de la UCM en preparación-, trabaja en el Centro de Proceso de Datos de la UCM desde 1998, inicialmente como Analista de Sistemas especializado en aplicaciones y entornos Unix y supercomputación. Progresivamente se fue especializando en tecnologías relacionadas con la seguridad lógica, y posteriormente en la gestión de la seguridad de la información, hasta que en el año 2003 se hizo cargo del Departamento de Seguridad de los Servicios Informáticos de nueva creación.

< Yolanda del Moral Armenteros es Ingeniero Técnico en Informática de Sistemas por la Universidad de Alcalá de Henares. Trabaja en Siemens desde 1996, inicialmente como técnico y administrador de redes Windows. En la actualidad, y desde hace seis años, sus funciones son las de Jefe de Producto y Consultor Preventa de Soluciones de Seguridad Avanzada. Además, gestiona las relaciones con la casa matriz en Alemania para productos de Siemens que están bajo su responsabilidad.

BANCO SABADELL: DEL PLAN DIRECTOR DE SEGURIDAD 2002-2006 AL NUEVO PLAN 2007-2009

Sinopsis:
Banco Sabadell realizó, en el año 2003, su Plan Director de Seguridad Tecnológica, de la mano de Deloitte. Dicho Plan supuso la puesta en marcha de un total de 48 proyectos, encaminados a alcanzar el nivel de seguridad objetivo que establecía el Modelo de Seguridad del grupo Banco Sabadell. Durante el período 2004-2006 se procedió, con una detallada planificación, a la ejecución de todos estos proyectos, que adicionalmente debían convivir con los cambios propios de la organización (requerimientos normativos, nuevas tendencias y riesgos en seguridad) y con la integración de las nuevas Entidades (Banco Herrero, Banco Atlántico y Banco Urquijo). Una vez cumplidos los objetivos en lo concerniente a seguridad, Banco Sabadell ha decidido y ejecutado un nuevo Plan Director de Seguridad Tecnológica, de nuevo con la ayuda de Deloitte, que ha permitido definir la hoja de ruta del Banco en la materia para el período 2007-2009.

Ponentes:

< Xavier Serrano Cossío es Director de Seguridad Tecnológica del Grupo Banco Sabadell desde julio de 2002. Licenciado en Informática por la Universidad Autónoma de Barcelona, postgrado en Ingeniería de software, Máster en Telemática y MBA Internacional por la Universidad Ramón Llull-LaSalle, posee una amplia experiencia profesional en Seguridad Tecnológica, Telecomuinicaciones y Administración de Sistemas, habiendo desarrollado la mayor parte de su carrera profesional en el sector financiero. Xavier Serrano ha dirigido, desde su incorporación en 2002 al Banco Sabadell, la ejecución del Plan Director de Seguridad Tecnológica 2004-2006 y ha liderado la reciente realización del Plan Director de Seguridad Tecnológica 2007-2009.

< Fernando Pons Ortega es Socio de Deloitte responsable de la división ERS (Enterprise Risk Services) de las oficinas de Barcelona, Valencia, Baleares y Aragón. Ingeniero Técnico en Informática de Gestión por ICADE-ICAI, Máster en Auditoría Informática, CISA, CISM, Lead Auditor Certificado por BSI y Certificado ITIL Foundation, posee una amplia experiencia profesional en Seguridad Tecnológica, Auditoría Informática y Gestión de Riesgos Tecnológicos, Planes Directores de Seguridad, implantación de Sistemas de gestión de la seguridad, consultoría de adaptación para la obtención Certificación 27001 y Planes de Recuperación de Negocio en todo tipo de empresas.

SGSI 27001: EL ALCANCE ES LO QUE IMPORTA

Sinopsis:
Disponer en nuestras organizaciones de un Sistema de Gestión de la Seguridad es, *a priori*, y en la mayoría de los casos, un objetivo deseable, pero ¿a qué coste? Para su implementación es necesario definir procesos y actividades, analizar riesgos, involucrar a las distintas áreas afectadas, definir y gestionar modelos de relación con proveedores y prestatarios externos... y si encima, y ya que se hace el esfuerzo, se opta a la certificación los requerimientos formales, documentales y hasta en ocasiones burocráticos serán un inconveniente con el que tendremos que "lidiar" y por supuesto su coste y esfuerzo, tanto durante el proceso de implantación como de su mantenimiento en el día a día, no será baladí.
Todo ello nos hace llegar a preguntarnos... ¿Merece la pena? ¿Estoy preparado para ello? ¿Dónde me voy a meter? Y lo más importante, ¿podré salir con éxito del empeño? Todo responsable de Seguridad Informática, tarde o temprano, se realiza estas preguntas cuando tiene en mente un proceso de implantación de un Sistema de Gestión, y el elemento clave que le ayudará en su análisis, decisión y resultado final será el alcance. El alcance es la base sobre la cual se desarrollará nuestro SGSI, y su correcta elección no es una tarea sencilla, ya que éste no debe ser tan extenso como para no ser abarcable, ni tan acotado como para no aportar valor a la organización, y sin duda siempre será clave para el éxito del proceso.

Ponentes:

< Jesús Milán Lobo es Gerente de Seguridad Informática en Bankinter. Ingeniero en Informática con especialidad en Gestión por el ICAI-ICADE, certificado CISM, certificado Lead Auditor, es miembro del Subcomité Nacional de Seguridad de las TI (CTN 71 / SC27) y miembro WG1, habiendo colaborado en la redacción de varias normas, tanto nacionales como internacionales. En la actualidad representa al SC27 en las reuniones Internacionales ISO y colabora en la redacción de la norma 27004, Information Security Management Measurement. Milán Lobo es miembro de la Comisión de Seguridad de ASIA y miembro del Comité de Seguridad Informática y de la Comisión de Seguridad, Prevención y Fraude del CCI (Centro de Cooperación Interbancaria).

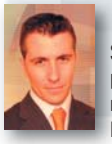
< Julio San José Sánchez forma parte del área de Seguridad Informática de Bankinter. Es CISM por ISACA y *Lead Auditor BS 7799* por Britihs Standard Institution. Es miembro de la Comisión de Seguridad de ASIA y Coordinador de subgrupo 2 (Criptografía) del Subcomité de Seguridad de las TI (CTN 71 / SC27), habiendo colaborado en la redacción de varias normas, tanto nacionales como internacionales. Así mismo es co-autor del libro *'Seguridad de las tecnologías de la información. La construcción de la confianza para una sociedad conectada',* editado por AENOR.

DEPARTAMENTO DE SALUD DE LA GENERALITAT DE CATALUÑA: PLAN DIRECTOR DE SEGURIDAD

Sinopsis:
Esta ponencia ilustrará el proceso de implantación del Plan Director de Seguridad llevado a cabo por el Departamento de Salud de la Generalitat de Cataluña, en colaboración con el Grupo SIA. Se trata de un proyecto estratégico orientado a una correcta gestión de la seguridad, a través de la aportación de métricas e indicadores de riesgo. Además, se ha conseguido un importante avance en la alineación de la seguridad con los SI y los requerimientos reales de los activos de información de los organismos sanitarios en Cataluña. El Plan Director de Seguridad ha facilitado una visión global del estado de la seguridad de las TIC, y permitirá garantizar, en paralelo, el cumplimiento de la LOPD en el tratamiento de datos clínicos así como los requerimientos de continuidad de los procesos de Catsalut.

Ponentes:

< Anna García Martínez es Responsable del Programa de Seguridad de la Información del Departamento de Salud de la Generalitat de Cataluña. Licenciada en Medicina y Cirugía por la Universidad de Barcelona y especialista en Medicina preventiva y Salud Pública, García es, además, Consultora en Seguridad Informática (UOC) y cuenta con un Postgrado de Economía de la Salud y Gestión de Servicios Sanitarios (Facultad de CC. Económicas y Empresariales de Barcelona). En su trayectoria profesional destaca como asesora técnica del Director Comisionado del Ministerio de Sanidad y Consumo en Catalunya así como por su amplia experiencia en diferentes cargos de responsabilidad en el Departamento de Sanidad de la Generalitat de Cataluña y el Área de Seguridad del Servicio Catalán de la Salud.



< Jacobo van Leeuwen es Product Marketing Manager de Seguridad en el Grupo SIA. Comenzó su experiencia en seguridad hace 10 años en Servicom/Retevisión, para pasar a la Gerencia de Seguridad de Telefónica de España como Jefe de Proyectos liderando, entre otros, el vinculado con la Gestión de Identidades. Posteriormente ejerció de Director Técnico en IP6 Seguridad (referente de seguridad perimetral y pen-test). Desde 2002 en el Grupo SIA, ha liderado como Jefe de Proyectos, los Planes Directores de Seguridad en el Grupo Cepsa y de Correos, así como los Servicios Gestionados para Telefónica Móviles, entre otros.

GRUPO FCC: DESARROLLO DEL MODELO DE CLASIFICACIÓN DE LA INFORMACIÓN

Sinopsis:
El Grupo FCC, en su afán por definir una estrategia de seguridad y como primer paso para un análisis de riesgos, ha decido realizar junto con IBM un proyecto de clasificación de la información que le permitiera obtener una visión más abstracta de su entorno TI. La complejidad de su entorno multientidad ha requerido de un estudio e inventario pormenorizado de los activos de información que permitirán al Grupo FCC un mejor trato de la información y, sobre todo, un conocimiento de las áreas más críticas en las que poner foco a la hora de afrontar futuros proyectos de seguridad. IBM ha proporcionado su enfoque consultivo para la definición de los modelos de clasificación y las posibles soluciones para garantizar dichos niveles. El estudio de los activos de la información permitirá al Grupo FCC alinear su estrategia de seguridad a lo largo de todas las organizaciones del Grupo, obteniendo en este sentido mejoras con respecto a la gestión de la seguridad y una visión más global de su situación actual para poder dirigir sus próximos pasos.

Ponentes:

< Miguel Cebrián Lindström es Consultor de Seguridad para el Grupo FCC. Dentro del Departamento de Seguridad de la Información y Gestión de Riesgos, dirige diferentes proyectos derivados de la implantación del Plan Estratégico de Seguridad. Experto en protección de datos personales y análisis de riesgo, comenzó su carrera profesional como desarrollador de software, participando en numerosos proyectos, desde el modelado 3D hasta la implantación de sistemas de control de red eléctrica. Cebrián, certificado como Lead Auditor ISO 27001 por IRCA, está interesado actualmente en las problemáticas relacionadas con la incorporación de la seguridad en los procesos de negocio.

< Alejandro García Nieto es el Responsable para España de los Servicios de Seguridad y Privacidad de la Información dentro de IBM. Licenciado en Administración y Dirección de Empresas e Informática de gestión por la Universidad de Lincoln, cuenta con una amplia experiencia en el sector de la seguridad de la información. García Nieto es CISA y CISM, y además participa en diversos foros de especialistas de seguridad TI.

ALTERNATIVAS TECNOLÓGICAS PARA EL DESARROLLO DE SERVICIOS DE SEGURIDAD GESTIONADOS DESDE LA RED

Sinopsis:
En un entorno de continuo crecimiento de Internet y de la apertura de sistemas hacia la red, la velocidad del entorno digital se contagia a las amenazas del mismo, generando entornos que sufren ataques de forma dinámica y casi inmediata. Los mecanismos perimetrales de protección y prevención no aportan soluciones adaptadas a la velocidad de aparición y propagación de los ataques y amenazas. ¿Existe alternativa a estas amenazas? En la presentación se intentarán analizar las nuevas alternativas que la tecnología nos aporta para prevenir, defender y contrarrestar en tiempo real y de forma ubicua dichas amenazas, las nuevas tecnologías y el futuro inmediato.

Ponente:

< Juan Miguel Velasco López-Urda es Director Asociado de Servicios de Seguridad en Red. UN Grandes Empresas Telefónica España-Telefónica Soluciones. Informático por la UPM y Master Executive de Gestión Empresarial por Insead-Euroforum, 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 Director Técnico y de Consultoría de la Agencia de Certificación Electrónica (ACE), sociedad filial de Telefónica DataCorp.

EJIE: SOLUCIÓN INTEGRAL DE SEGURIDAD GESTIONADA

Sinopsis:
La gestión de la seguridad abarca diferentes áreas críticas para las organizaciones. En el caso de la Administración Pública, conocer y gestionar adecuadamente la información sobre los diferentes sistemas constituye un requisito esencial. Gracias a la reciente implantación de la solución de gestión de *logs* de S21sec, Bitácora, el Gobierno Vasco está en condiciones de resolver la recolección, gestión de *logs* y eventos informáticos de manera eficaz. Esto le permite prevenir

internamente los riesgos de seguridad y facilita el análisis forense ante diversos incidentes que se suscitan en una infraestructura de sistemas que afecta a más de 6.000 ordenadores.
Con el objetivo de lograr una gestión de la seguridad más integral, EJIE ha decidido abordar un modelo externalizado 24x7. Para ello ha puesto en marcha un proyecto piloto, junto con S21sec, cuyos servicios se integrarán en un único portal con un cuadro de mandos desde donde se pueda tener acceso al estado de su seguridad en todo momento. Desde el centro de operaciones de seguridad (SOC) de S21sec, se realizará la monitorización y gestión de sus cortafuegos y detectores de intrusos, además de la gestión continua de las vulnerabilidades. Adicionalmente, se recogerán las alertas generadas por Bitácora en el mismo modelo de seguridad gestionada.

Ponentes:

< Agustín Elizegi Etxeberria es Director General de EJIE (Sociedad Informática del Gobierno Vasco). Ingeniero Industrial, actualmente está a cargo de la dirección general de EJIE. Antes de incorporarse a EJIE fue Gerente de cuenta en Ibermática, Director de Informática y Telecomunicaciones del Gobierno Vasco y Subdirector de Informática y Organización del Servicio Vasco de Salud-Osakidetza. Asimismo, trabajó como Jefe de Proyectos de Planificación de Sociedad de la Información de Interior y Jefe de Informática en el Gobierno Vasco.

< Igor Unanue Buenetxea es Director de I+D+i de S21sec. Diplomado en Ingeniería Técnica de Sistemas de Telecomunicaciones por la Universitat Politécnica de Catalunya, es socio fundador de Grupo S21sec Gestión, S.A. En la misma, ha sido con anterioridad Director Técnico y posteriormente Director de Organización, Sistemas y Calidad hasta ser nombrado en 2006 Director Gerente de S21sec Information Security Labs, S.L., empresa de I+D+i del Grupo S21sec Gestión, S.A. Antes de su incorporación a S21sec, Unanue fue Responsable del Departamento de Redes y Comunicaciones en Com&Media.

SERVICIOS DE MONITORIZACIÓN Y ALERTA TEMPRANA DE RBC-DEXIA

Sinopsis:
El crecimiento en número y tipo de SS.II. en las empresas derivado del uso intensivo de tecnologías de la información plantea nuevos retos a sus Responsables de Seguridad y Sistemas. Asimismo, surgen retos en escenarios de fusión de empresas, que requiere de respuestas inmediatas y eficaces, pero también seguras. Son por ello necesarias nuevas soluciones que permitan controlar y monitorizar adecuadamente estas infraestructuras y los servicios que a través suyo se prestan, dotando a los responsables de una rápida comprensión de qué está ocurriendo en las redes corporativas en cada momento. Esta necesidad es más patente ante la creciente amenaza interna, sea de usuarios "inquietos" que usen las redes corporativas como campo de juegos, como de empleados desleales, aspecto particularmente delicado en el regulado entorno financiero donde RBC-Dexia desarrolla sus actividades. Así, RBC-Dexia determinó la conveniencia de implantar en colaboración con GMV Soluciones Globales Internet S.A. medidas para la gestión y monitorización de seguridad en sus instalaciones, con el fin de identificar y detectar la ocurrencia de estas actividades.

Ponentes:

< Javier García Buergo es Responsable de Seguridad y Redes en RBC Dexia Investor Services España, S.A. Ingeniero Agrónomo por la UPM y Executive MBA por el Instituto de Empresa, ha desarrollado toda su carrera profesional en RBC Dexia Investor Services España, S.A. En 1995 se incorpora a la estructura de Seguridad de RBC Dexia (antes Bancoval), asumiendo las funciones de Responsable de Seguridad y otras empresas del Grupo, implantando y manteniendo en el banco todas la medidas de carácter técnico aparejadas a la función de seguridad informática y redes. García Buergo ha liderado en este periodo diversos proyectos, entre los que cabe citar el diseño e implantación del Centro de Respaldo del banco (2000), el proyecto de adecuación a LOPD de empresas del grupo (2002), la implantación avanzada de sistemas de seguridad y acceso en alta disponibilidad (2003), la coordinación técnica para *rebranding* de Bancoval (2005) y el servicio de monitorización de sistemas y alerta temprana (2006).

< Mariano J. Benito Gómez es Director de Seguridad / CISO de GMV Soluciones Globales Internet S.A. Ingeniero de Telecomunicaciones por la Universidad de Valladolid y CISSP por (ISC)^2, ha desarrollado toda su carrera profesional en Soluciones Globales Internet S.A. Desde 2004 asume las funciones de Director de Seguridad de GMV Soluciones Globales Internet S.A, dirigiendo el proceso de implantación del SGSI de la compañía, obteniendo su certificación en 2006 frente a ISO 27001, y en diciembre de 2004 frente a UNE 71502:2004, y realizando la monitorización del estado de seguridad de la compañía, establecimiento y definición de métricas e identificación de acciones de mejora. Anteriormente a esa fecha, Benito Gómez fue director de la Unidad de Negocio de Seguridad Lógica de Soluciones Globales Internet y Responsable del Área de Seguridad Perimetral y Auditoría. Participa activamente como colaborador en medios escritos, diversas tribunas de opinión y otros foros de seguridad lógica.

TERCER MÓDULO 26 de abril

09:15h. Entrega de documentación.
Moderador: **José Domingo Carrillo Verdún**, Profesor del Departamento LSIS, Facultad de Informática de la Universidad Politécnica de Madrid.

09:30h. Ponencia: **Continuidad de negocio: el "negocio" se pone las pilas.**
Ponente: **Carlos Bachmaier Johanning**, Gestión de Riesgo Corporativo. Sistemas Técnicos de Loterías.

10:10h. Coloquio.

10:15h. Ponencia: **El Plan de Continuidad de Negocio en el Grupo BBVA.**
Ponentes:
Pablo de Vera, Director de Continuidad de Negocio Corporativa. Grupo BBVA.
Elena Maestre García, Directora de los Servicios de Seguridad de PricewaterhouseCoopers.

10:55h. Coloquio.

11:00h. Pausa-café.

Moderador: **Arturo Ribagorda Garnacho**, Catedrático de Ciencias de la Computación e Inteligencia Artificial, y Director del Departamento de Informática de la Universidad Carlos III de Madrid.

11:30h. Ponencia: **De la seguridad de la información a la información de seguridad.**
Ponente: **Francisco Javier García Carmona**, Director de Seguridad de la Información y las Comunicaciones de Iberdrola.

12:10h. Coloquio.

12:15h. Ponencia: **El Centro de Respuesta a Incidentes del INTECO.**
Ponentes:
Enrique Martínez Marín, Director General del INTECO, Instituto Nacional de Tecnologías de la Comunicación.
Adrián Agudo Fernández, Gestor de Proyectos Consultoría de Seguridad. Indra.

12:55h. Coloquio.

13:00h. Debate: **La necesidad de herramientas de ayuda a la toma de decisiones en seguridad de la información.**
Moderador: **Luis Guillermo Fernández Delgado**, Editor de la revista SIC.
Intervienen:
- **José Luis Checa López**, Responsable de Seguridad de la Información. Grupo Gas Natural.
- **Gianluca D'Antonio**, Director del Servicio de Seguridad de la Información y Gestión de Riesgos. División de Informática. Grupo FCC.
- **Miguel Ángel Navarrete Porta**, Director del Departamento de Seguridad Informática de Caja Madrid.
- **Tomás Roy Catalá**, Director de Seguridad y Calidad. Centro de Telecomunicaciones y Tecnología de la Información (CTTI) de la Generalitat de Cataluña.

14:30h. Almuerzo.

Moderador: **Javier López Muñoz**, Coordinador del Grupo de Seguridad. Universidad de Málaga.

16:30h. Ponencia: **Servicios de respuesta a incidentes de seguridad para las Administraciones Públicas.**
Ponente: **Javier Candau Romero**, Jefe del Área de Inspección y Análisis de la Seguridad de las TIC. Centro Criptológico Nacional-CCN.

17:10h. Coloquio.

17:15h. Ponencia: **El descubrimiento de activos enfocado al análisis de riesgos de los sistemas de Información.**
Ponente: **José Antonio Mañas Argemí**, Catedrático de Ingeniería Telemática, ETSI de Telecomunicación de la Universidad Politécnica de Madrid, y consultor independiente.

17:55h. Coloquio.

18:00h. Pausa-café.

18:15h. Ponencia: **Errores de hoy, amenazas del mañana.**
Ponente: **Jorge Dávila Muro**, Director del Laboratorio de Criptografía. LSIIS. Facultad de Informática. Universidad Politécnica de Madrid.

18:55h. Coloquio.

19:00h. **Clausura de Securmática 2007**

CONTINUIDAD DE NEGOCIO: EL "NEGOCIO" SE PONE LAS PILAS

Sinopsis:
Los estímulos del entorno motivan a los gestores de las organizaciones a mejorar la continuidad de negocio, creando condiciones positivas para la correcta gestión de continuidad I/TIC. La aparición en UK de la norma BS 25999-1:2006, de "buenas prácticas de continuidad de negocio", con vocación de certificable, y orientada a todo tipo de empresa, marca un punto de inflexión. Los profesionales del sector debemos conocer cómo esta norma, y aspectos de gobierno corporativo asociados, pueden afectar a nuestra labor. En la conferencia se comentarán los siguientes aspectos: 1) Panorama del entorno relativo a continuidad de negocio: desafíos, incidentes y gobierno corporativo; situación normativa y de diligencia debida, particularmente en EEUU y UK, y en los diversos sectores (bancario, *trading*, salud, etc.). 2) Presentación de la norma BS 25999-1:2006 y evaluación de cómo su influjo puede afectar al campo I/TIC. 3) Marcos de gobierno I/TIC: relaciones y tensiones, y 4) posible influencia de los Códigos de Buen Gobierno y las responsabilidades de los Administradores sobre la atención a la continuidad de negocio en España.

Ponente:

< Carlos Bachmaier Johanning es Dr. Ingeniero Aeronáutico, 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 se centra en la Gestión de Riesgo Corporativo, que incluye la función de Auditoría Interna TIC y de 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 incorporó a STL en 1998, entidad en la que ha desarrollado actividades en las áreas de tecnología y protección de la información, así como de gestión del riesgo corporativo. Miembro de ISACA, mantiene activas sus certificaciones CISA y CISM. Publica regularmente artículos profesionales, y ejerce de profesor 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. Auditor Jefe SGSI (a falta de prácticas). Actualmente está interesado de forma particular en el Buen Gobierno TIC, y en la norma BS 25999, de continuidad de negocio.

EL PLAN DE CONTINUIDAD DE NEGOCIO EN EL GRUPO BBVA

Sinopsis:
En la actualidad los Planes de Continuidad de Negocio han pasado a ser uno de los grandes desafíos en materia de seguridad. En este entorno, se ha producido una importante evolución, entre otros, con el incipiente desarrollo de estándares internacionales en la materia o con la evolución regulatoria de algunos sectores, como el financiero, cuyo desarrollo se va a apuntar en esta ponencia. Adicionalmente, una entidad líder en el sector, como es Grupo BBVA presentará su visión particular en referencia a la Continuidad de Negocio y los grandes factores de éxito de su gestión.

Ponentes:

< Pablo de Vera es Director de Continuidad de Negocio Corporativa del Grupo BBVA. Su trayectoria profesional ha estado ligada desde sus inicios al Grupo BBVA, donde desde hace treinta años ha desempeñando diferentes puestos de responsabilidad en distintas áreas, como son: marketing, redes de ventas y negocio hipotecario. De Vera es licenciado en Ciencias Económicas y Empresariales por la UAM.

< Elena Maestre García es Directora responsable de los Servicios de Seguridad de la Información en 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 dieciséis años. Maestre es licenciada en Ciencias Económicas y Empresariales por la UAM y dispone de acreditación CISA y CISM.

DE LA SEGURIDAD DE LA INFORMACIÓN A LA INFORMACIÓN DE SEGURIDAD

Sinopsis:
La Seguridad de la Información, entre otro tipo de medidas, da lugar a la utilización de herramientas tipo antivirus, cortafuegos, contraseñas, cifrado, etc. A todas las Organizaciones estas referencias y otras muchas nos son sobradamente conocidas; son muchos los recursos que requieren en su implementación, operación y administración, pero, ¿hemos de seguir introduciendo nuevos elementos de seguridad en nuestros sistemas de información?, ¿se encuentran todos estos mecanismos debidamente adaptados a nuestras necesidades?, ¿cubren nuestras expectativas de seguridad?, ¿ya está todo hecho? Todas estas cuestiones y otras tantas más son a las que deberá dar respuesta una correcta Gestión de Riesgos de la Información.
La explotación adecuada de todas estas herramientas nos permitirá ofrecer garantías a los procesos de los negocios de la Organización, pero hemos de plantearnos dos cuestiones determinantes: primera, ¿lo estamos haciendo de la manera más adecuada?, y segunda, ¿están debidamente parametrizadas todas éstas para cubrir el objetivo para el que han sido implementadas?
Para dar respuesta a tales cuestiones, deberemos de soportarnos en datos, datos que son generados por cada una de estas herramientas. Pero de todos es conocida la interrelación que existen entre todos ellos. Casi ninguno de estos mecanismos tiene vida por sí; tenemos que relacionarlos entre sí, por lo que ha llegado ya el momento de trabajar con "la Información de Seguridad".

Ponente:

< Francisco Javier García Carmona es Director del Departamento de Seguridad de la Información y las Comunicaciones de Iberdrola. Inicia su actividad en 1982 en el sector de las Telecomunicaciones, pasando a dirigir este departamento en diversas empresas del ramo. Se incorporá al mundo de la seguridad en el año 1996, simultaneando la dirección de Operaciones con funciones técnicas. En el año 2001 se incorporá a Iberdrola como Director del Departamento de Seguridad de la Información y las Comunicaciones.

EL CENTRO DE RESPUESTA A INCIDENTES DEL INTECO

Sinopsis:
INTECO, Instituto Nacional de Tecnologías de la Comunicación, sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio, nace como iniciativa del Plan Avanza para contribuir a la convergencia de España con Europa en la Sociedad de la Información. El objetivo inmediato de INTECO consiste en la puesta en marcha de proyectos vinculados a la Sociedad de la Información, orientados a la innovación y la competitividad, con capacidad de concentrar talento y en un entorno institucional y empresarial sólido que devenga en un referente del ámbito de las Tecnologías de la Información y la Comunicación, especialmente en Seguridad Tecnológica, Accesibilidad e Innovación TIC. INTECO ofrece para ello servicios de seguridad tecnológica a los ciudadanos y la pequeña y mediana empresa española a través del Centro Nacional de Respuesta a Incidentes en Tecnologías de la Información, que ha lanzado recientemente con la ayuda de Indra. A lo largo de la ponencia se expondrá el proyecto de puesta en marcha del Centro, su organización y el catálogo de servicios prestados.

Ponentes:

< Enrique Martínez Marín es Director General del Instituto Nacional de Tecnologías de la Comunicación (INTECO), dependiente del Ministerio de Industria, Turismo y Comercio. Licenciado en Ciencias Políticas y Sociología por la Universidad Complutense de Madrid (UCM), funcionario del Grupo A de la Escala Técnica de Gestión de Organismos Autónomos, Master en Gestión Pública por el Centro Superior de Estudios de Gestión Análisis y Evaluación de la UCM y Master en Cooperación al Desarrollo (Centro Español de Estudios de América Latina), ha sido director del Centro de Estudios Jaime Vera entre 1995 y 2000. Desde 1999 es Vicepresidente para las Administraciones Locales del Observatorio para la Calidad de los Servicios Públicos, y de julio de 2000 hasta julio de 2004 fue miembro de la Ejecutiva Federal del Partido Socialista Obrero Español, en la que fue Secretario de Innovación y Comunicación Interna. En julio de 2004 fue nombrado Director del Observatorio de las Telecomunicaciones y para la Sociedad de la Información de la Entidad Pública Empresarial Red.es. Ha sido Director de la Oficina Técnica del Plan de Convergencia del Consejo Asesor para las Telecomunicaciones y la Sociedad de la Información (CATSI), y encargado de sistematizar sus propuestas para la redacción del Plan Avanza. Es Representante de Red.es en el Consejo Superior de Administración Electrónica (CSAE) del MAP y la Asociación XBRL España.

< Adrián Agudo Fernández es Gestor de Proyectos de Consultoría de Seguridad en Indra. En sus veintidós años de experiencia en el mundo de las TIC, ha desarrollado labores en todos los ámbitos de la función informática: desarrollo, administración de sistemas y explotación, en varias entidades financieras. Formó parte de la Auditoría Interna de SS.II. del Santander Central Hispano. Ha conocido de primera mano, la gestión de la seguridad en las .com, en una de las cuales se puso al frente del área de Auditoría y Seguridad. Desde 1999, forma parte de Indra, a la que se incorporó con el objetivo de abrir determinadas líneas de negocio de Consultoría de Seguridad.

SERVICIOS DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD PARA LAS ADMINISTRACIONES PÚBLICAS

Sinopsis:
Partiendo del conocimiento y la experiencia del Centro Criptológico Nacional sobre amenazas y vulnerabilidades a los sistemas de las tecnologías de la in-

formación y las comunicaciones, y con el objetivo de mejorar la seguridad de los sistemas de la Administración, se está desarrollando una capacidad de Respuesta ante incidentes gubernamental (CCN-CERT).
El CCN-CERT nace con la misión de ayudar a las Administraciones Públicas (General, Autonómica y Local) en la resolución de los incidentes mediante servicios de información y de investigación de los mismos. Esta actividad se va a desarrollar en torno al portal del CCN-CERT (www.ccn-cert.cni.es) y tiene por objetivo permitir el acceso de las diferentes administraciones a información sobre amenazas, vulnerabilidades, guías de configuración de las diferentes tecnologías (Series CCN-STIC), formación en diferentes tecnologías, herramientas de seguridad (herramienta de análisis de riesgos PILAR, entre otras) y mejores prácticas de seguridad.

Ponente:

< Javier Candau Romero es Jefe del Área de Políticas y Servicios del Centro Criptológico nacional (www.ccn.cni.es). Comandante de Artillería, Ingeniero Industrial (especialidad en Electrónica y Automática), especialista Criptólogo, dispone de diversas certificaciones de especialización en seguridad de las TIC (ISS, SANS, CRAMM, PILAR, OTAN, Curso de Auditoría del INAP...). Los principales cometidos del Área de Políticas y Servicios del CCN son: la formación del personal especialista de la Administración, el desarrollo de la normativa del CCN (elaboración de políticas, directrices y guías de seguridad TI para la Administración Pública –Series CCN-STIC–, la Herramienta PILAR, la supervisión de los procesos de acreditación de sistemas y la realización de auditorías de seguridad, y la Respuesta ante incidentes (CCN-CERT).

EL DESCUBRIMIENTO DE ACTIVOS ENFOCADO AL ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

Sinopsis:
Aunque la intuición de qué es un "activo" la tenemos todos, la definición formal es escurridiza y la determinación de qué activos nos deben interesar depende de la posición del interlocutor en la organización. Al tiempo, identificar correctamente los activos que contribuyen al éxito del sistema (cuidar la información y servirla donde y cuando sea requerida) es crítico pues no se puede proteger ni controlar que está protegido lo que se ignora, bien porque se ignora su existencia, bien porque se ignora su función. El inventario de activos es crítico; pero puede ser abrumador, y un análisis abrumador no permitirá identificar lo que es crítico, separándolo de lo que es opcional (y cuidaremos o no, a la vista del coste/beneficio) y olvidando lo que es accesorio.

Ponente:

< José Antonio Mañas Argemí es Catedrático de Ingeniería de Sistemas Telemáticos en la E.T.S.I. de Telecomunicación de la Universidad Politécnica de Madrid (UPM), consultor independiente, redactor de la versión 2 de la metodología Magerit de Análisis y Gestión de Riesgos de Sistemas de Información –del Ministerio para las Administraciones Públicas–, y autor de las herramientas PILAR/EAR de Gestión de Riesgos en colaboración con el Centro Critológico Nacional-CCN.

ERRORES DE HOY, AMENAZAS DEL MAÑANA

Sinopsis:
Aunque el determinismo estricto desapareció de la física a principios del siglo XX, las relaciones sociales suelen seguir el principio clásico de la acción y la reacción y, sobre todo, el de relación causal; de modo que las cosas son siempre consecuencia y causa de algo. La sociedad de la información se mueve dentro de ese marco y todas las amenazas que hoy sufre son consecuencias de acciones y decisiones tomadas anteriormente por profesionales como los que hoy la dirigen. En esta ponencia intentaremos ver si el análisis de las opciones actuales permitiría ver qué amenazas estamos invocando con las tendencias actuales, y cómo, con este proceder, poder mitigar los futuros riesgos cuya eliminación es imposible.

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 NECESIDAD DE HERRAMIENTAS DE AYUDA A LA TOMA DE DECISIONES EN SEGURIDAD DE LA INFORMACIÓN

Proposición: El modelo actual del proceso de gestión y de toma de decisiones en materia de seguridad de la información y, en consecuencia, en materia de seguridad TIC, en el contexto global de una organización, relaciona el análisis de riesgos, los sistemas de gestión de la seguridad de la información y la creación de sistemas de indicadores, medida y cuadro de mando como las herramientas idóneas para ayudar a los gestores, en los distintos estratos, a tomar decisiones en los terrenos organizativo y tecnológico cuya puesta en práctica, a menudo, comporta inversión y gasto.
En el debate se tratará de que los participantes ofrezcan sus opiniones profesionales acerca de si este modelo es el único posible para la toma de decisiones documentadas (sobre todo es su dimensión predictiva), si es perfeccionable en alguno de sus componentes (análisis de riesgos, descubrimiento de amenazas y vulnerabilidades, creación de indicadores, cuadro de mando, SGSI...), en qué y si se echan en falta otro tipo de herramientas orientadas a la toma de decisiones en el ámbito de la gestión de la seguridad de la información que pudieran ser suministradas por la industria de seguridad TIC.

Intervienen:

< José Luis Checa López es Responsable de Seguridad de la Información del Grupo Gas Natural. Ingeniero Técnico Industrial por la Universidad Politécnica de Cataluña (UPC), cuenta con 18 años de experiencia en el sector informático en diversas áreas, 11 de ellos en Digital Equipment Corporation. Fue durante 7 años Jefe de Arquitectura de Sistemas y Software de Base de Gas Natural con responsabilidad en proyectos de diseño e implementación de infraestructuras en esta compañía, etapa profesional en la que afrontó, entre otros, retos tan significativos como el despliegue de una solución corporativa de gestión de sistemas basada en Tivoli, la migración de la plataforma Microsoft a Windows 2000/XP y Exchange 2000, el despliegue de las infraestructuras SAP, Siebel, Gestión Documental, Output Management, EAI, Portales y Datawarehouse, y el Plan Director de Seguridad y entorno de acceso con *logon* único (SSO).

< Gianluca D'Antonio es Director del Servicio de Seguridad de la Información y Gestión de Riesgos en la División de Informática del Grupo FCC. Su principal misión es promover, impulsar y desarrollar la Política de Seguridad de la Información del Grupo. Es miembro de ISACA desde 2003 y posee las certificaciones CISM y CISA. Licenciado en Derecho, experto en derecho de las nuevas tecnologías, desde el comienzo de su vida profesional ha trabajado en proyectos de seguridad de la información. Tras una breve etapa en Motorola España, ha sido Consultor Senior de Seguridad Informática en Centrisa y posteriormente Responsable de Protección y Recuperación de Datos en el Grupo DIA hasta finales de 2005. Es miembro fundador de ISMS Forum España.

< Miguel Ángel Navarrete Porta es Director del Departamento de Seguridad Informática de Caja Madrid. Ha trabajado como informático desde hace veintiún 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 de Madrid, donde se ubica el departamento de Seguridad Informática, que dirige desde el año 1999.

< Tomás Roy Català es, desde junio de 2004, Director del Área de Calidad y Seguridad en el Centro de Telecomunicaciones y Tecnologías de la Información de la Generalitat de Cataluña. 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. Con anterioridad, en 2001, en tanto Responsable de un centro de investigación, dirigió proyectos de I+D en el ámbito del documento de identidad electrónico italiano. Tiene patentes sobre criptografía y autenticación fuerte. En 2000 fue Responsable del primer Master Italiano en Seguridad de los Sistemas, Informaciones y Aplicaciones. Complementa su formación en el area de Seguridad en los ámbitos de auditoría CISA, la Gestion de Seguridad CISSP, Seguridad de Sistemas Operativos MCSE y Certificaciones Cisco.

> SECURMATICA, a escena

Panorámica de SECURMÁTICA 2006

> Premios SIC 2007

En coincidencia con la celebración de la XVIII edición de Securmática, tendrá lugar el acto de entrega de los IV 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 tercera edición de los premios SIC

LA HORA DEL REENCUENTRO Y LOS RECONOCIMIENTOS

> Cena de celebración

SECURMATICA

XVIII Congreso español de Seguridad de la Información 2007

AFORO LIMITADO

> Fechas y lugar

SECURMÁTICA 2007 tendrá lugar los días 24, 25 y 26 de abril de 2007 en el hotel NOVOTEL*. Campo de las Naciones de Madrid.

> Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2007 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 Celebración y entrega de los IV Premios SIC (25 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 teléfono: +34 91 575 83 24/25
- Por fax: +34 91 577 70 47
- Por correo electrónico: info@securmatica.com
  info@codasic.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)

- Abone 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 DE 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 2007

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 24 ❑ MÓDULO 2 DÍA 25 ❑ MÓDULO 3 DÍA 26 ❑ Deseo inscribirme a SECURMATICA 2007

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**