SECURMATICA 2006

XVII Congreso español de Seguridad de la Información

PROGRAMA

Una vez más Securmática se cita con su audiencia natural: los responsables de seguridad de la información, la industria y los servicios relacionados con la protección TIC. La XVII edición del congreso, que anualmente organiza la revista SIC, se celebrará los días 25, 26 y 27 de abril en su tradicional sede del Campo de las Naciones de Madrid.

ES HORA DE COMPARTIR EXPERIENCIAS Y AVANZAR >

La organización del Congreso español de la Seguridad de la Información ha conformado un programa en el que puede traslucirse el avance imparable de la función de seguridad y el mayor calado y complejidad de los proyectos que se están realizando, en todos los órdenes, bajo la dirección de los departamentos específicos de protección TIC y de gestión de riesgos de información. Al tiempo, ofrecerá una visión global de la seguridad a través de los trabajos realizados por expertos españoles que prestan sus servicios en organizaciones multinacionales y despejará dudas sobre algunas iniciativas de gran calado nacional. Igualmente, el congreso prevé concitar la máxima atención alrededor de un debate singular: las ventajas e inconvenientes derivados del uso de software de seguridad propietario vs. software de seguridad de libre disposición y código abierto.

También la edición 2006 de Securmática, en su ya histórica línea de dejar apuntados asuntos que marcarán el inmediato devenir en la materia, va a abordar -de la mano de dos de las máximas autoridades de nuestro país- el espinoso asunto de las vulnerabilidades asociadas a la tecnología, así como los nuevos retos profesionales que representa la instauración a medio plazo de la identidad federada.

Copatrocinadores:

Deloitte. · Ernst & Young Quality In Everything We Do · germinus

hp invent · IBM · Indra · KPMG

S21sec · SECUWARE · SGI

sia · SIEMENS · Telefónica

Organiza:

Revista SIC seguridad en informática y comunicaciones

ANIVERSARIO XV SIC

SIC Seguridad en Informática y Comunicaciones es desde hace quince 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 25 de abril

08:45h. Entrega de documentación.
09:15h. Inauguración oficial.
10:00h. Conferencia de apertura: **Consideraciones al respecto del borrador del Reglamento de la LOPD.**
Ponente: **Jesús Rubí Navarrete**, Adjunto al Director de la Agencia Española de Protección de Datos.
10:40h. Coloquio
10:45h. Ponencia: **El modelo de gestión de riesgos en sistemas de información en el Banco Central Europeo.**
Ponente: **Alberto Partida Rodríguez**, Experto en Seguridad de Sistemas de Información. División de Gestión de Tecnologías de la Información. Banco Central Europeo.
11:25h. Coloquio
11:30h. Pausa-café
12:00h. Ponencia: **Grupo Santander: modelo de organización de seguridad.**
Ponente: **José Antonio Castro González**, Director de Seguridad Corporativa. Grupo Santander.
12:40h. Coloquio
12:45h. Ponencia: **Outsourcing, offshoring y otros retos de la seguridad global.**
Ponente: **Daniel Barriuso Rojo**, Director de Análisis de Riesgos Tecnológicos para Europa y Mercados Globales. ABN AMRO.
13:25h. Coloquio
13:30h. Ponencia: **Grupo FCC: establecimiento de la función de gestión de riesgos y plan estratégico de seguridad.**
Ponente: **Gianluca D'Antonio**, Director del Servicio de Seguridad de la Información y Gestión de Riesgos. División de Informática. Grupo FCC.
14:10h. Coloquio
14:15h. Almuerzo
16:15h. Ponencia: **Nuevas herramientas de prevención de fraude.**
Ponentes: **Pedro Pablo López Bernal**, Grupo de Seguridad. CCI, Centro de Cooperación Interbancaria, y **Mariano Largo del Amo**, Director del SOC (Security Operations Center) de S21sec.
16:55h. Coloquio
17:00h. Ponencia: **Programa de gestión de riesgos para los Centros Tecnológicos del Grupo PRISA.**
Ponentes: **Pablo Rivera Villaverde**, Director de Tecnologías de la Información. Grupo PRISA, y **Luis J. Buezo Bueno**, Gerente de la Práctica de Seguridad de HP Consulting & Integration.
17:40h. Coloquio
17:45h. Pausa-café
18:00h. Ponencia: **Los servicios gestionados de seguridad en Grupo Antolín.**
Ponentes: **Susana Cuevas Arce**, Responsable de Comunicaciones y Seguridad del Grupo Antolín, y **Roberto López Navarro**, Consultor de Seguridad. División de Auditoría y Planificación estratégica de Soluciones Globales Internet.
18:40h. Coloquio
18:45h. Fin de la primera jornada.

CONSIDERACIONES AL RESPECTO DEL BORRADOR DEL REGLAMENTO DE LA LOPD

Ponente:

< **Jesús Rubí Navarrete**, Adjunto al Director de la Agencia Española de Protección de Datos. Abogado desde 1977, Rubí Navarrete ha ocupado hasta la fecha diversos cargos en la Administración General del Estado. Fue Director del Gabinete del Ministro de Justicia de 1982 a 1986; Secretario General Técnico del Ministerio de Relaciones con las Cortes en 1988, Director General de Relaciones con las Cortes de 1989 a 1994, y Vocal del Tribunal de la Competencia de 1996 a 1999. De 1999 a 2002 ocupó el cargo de Adjunto al Director de la Agencia de Protección de Datos, y de 2002 a 2005 el de Subdirector General de Inspección de Datos. Actualmente ocupa el cargo de Adjunto al Director de la Agencia Española de Protección de Datos.

EL MODELO DE GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN EN EL BANCO CENTRAL EUROPEO

Sinopsis:
La ponencia evidenciará los puntos de mayor interés didáctico de una iniciativa de gestión de riesgos en sistemas de información en una organización multicultural y no-comercial como es el Banco Central Europeo, cuya misión es mantener la estabilidad de precios en la zona del euro y, de este modo, el poder adquisitivo de más de 308 millones de ciudadanos europeos. Este proceso de gestión de riesgos está basado en el estándar ISO 17799 (ISO 27002 a partir de 2007) y en la metodología de gestion de riesgos de la información del Information Security Forum (ISF). Su objetivo es ofrecer un servicio estructurado, consistente y práctico al propietario de la información y de los procesos de negocio a los que los sistemas de información dan soporte. Los cinco pasos principales de este servicio comienzan con un análisis de la criticidad del proceso de negocio, seguido de la identificación de los requisitos de seguridad necesarios. Posteriormente, se seleccionan e implementan los requisitos acordados, se identifica el riesgo remanente y se informa al propietario de la información. La experiencia acumulada en esta iniciativa revela la importancia de considerar la seguridad en sistemas de información como un elemento indispensable dentro del gobierno corporativo de toda organización, especialmente en la gestión del riesgo estratégico.

Ponente:

< **Alberto Partida Rodríguez** es Experto de Seguridad en Sistemas de Información en el Banco Central Europeo desde 2001. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid, comenzó su andadura profesional en seguridad de la información en la propia Universidad y en la empresa Atos para, posteriormente, incorporarse como consultor de seguridad dentro del Grupo Telefónica. Entre otros campos, Partida centra su actividad profesional en la seguridad en el desarrollo de aplicaciones, en la provisión de sistemas de información seguros y en el análisis de riesgos en procesos estratégicos de negocio. Participa en el grupo de trabajo de Seguridad Informática del Sistema Europeo de Bancos Centrales desde 2001 y posee las certificaciones CISA y CISSP, así como SANS GIAC Gold GSEC, GCFW y GCFA. En la actualidad, Partida estudia la relación entre la gestión del riesgo operacional y la seguridad de la información en el mundo empresarial.

GRUPO SANTANDER: MODELO DE ORGANIZACIÓN DE SEGURIDAD

Sinopsis:
La gestión de la seguridad de la información se cimenta en tres pilares: las personas, la organización y la tecnología. En la ponencia se describirá a grandes rasgos el modelo de organización de seguridad por el que está optando el Grupo Santander con el fin de obtener una eficacia y una eficiencia adecuadas en la gestión de los riesgos de información en todas las áreas de actividad y de negocio que desarrolla en los distintos países en los que opera, cubriendo la unificación de políticas y el cumplimiento de requisitos normativos y legales.

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 (18 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 doce años de experiencia en el mundo de la gestión de riesgos de la información en áreas como la continuidad operativa, la seguridad en canales alternativos, las infraestructuras de clave pública y las arquitecturas de seguridad .Net.

OUTSOURCING, OFFSHORING Y OTROS RETOS DE LA SEGURIDAD GLOBAL

Sinopsis:
El mundo de la seguridad se enfrenta al reto de gestionar un entorno tecnológico cada vez más disperso desde un punto de vista tanto geográfico como organizativo. La globalización de la economía ha puesto al alcance del mundo corporativo nuevos mercados y oportunidades de negocio, así como nuevas maneras de proveerse de servicios. Esto, unido a la continua reducción de los márgenes operativos, ha dado lugar a la necesidad de explorar nuevas oportunidades de ahorro de costes mediante servicios globales que incluyen *outsourcing* y *offshoring*. Recientemente, ABN AMRO ha sido protagonista de uno de los mayores y más ambiciosos procesos de *outsourcing* tecnológico en el sector financiero. La presentación aborda, desde la experiencia del ponente, cuestiones tales cómo las claves organizativas para gestionar la seguridad en un entorno global externalizado, qué aspectos se deben tener en cuenta desde el punto de vista de los riesgos tecnológicos, y las principales oportunidades, amenazas y tendencias en este campo.

Ponente:

< **Daniel Barriuso Rojo** es Director del Departamento de Análisis de Riesgos Tecnológicos para Europa y Mercados Globales en ABN AMRO, donde tiene responsabilidad global sobre la gestión de riesgos en los sistemas, proyectos y nuevas soluciones tecnológicas. 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 incorporación a ABN AMRO, ha sido 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 áreas tales como 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.

GRUPO FCC: ESTABLECIMIENTO DE LA FUNCIÓN DE GESTIÓN DE RIESGOS Y PLAN ESTRATÉGICO DE SEGURIDAD

Sinopsis:
A lo largo de la ponencia se ilustrarán las directrices del Plan Estratégico de Seguridad adoptado por el GRUPO FCC. La heterogeneidad de las áreas de actividad del Grupo requiere un enfoque específico, orientado a la implementación de modelos de madurez distintos según la actividad. Partiendo de estas premisas, el GRUPO FCC se está dotando de nuevos medios técnicos y organizativos para soportar tecnológicamente su ambicioso desarrollo internacional. En los próximos tres años se llevará a cabo un plan de convergencia hacia el estándar ISO 17799, que sucesivamente permitirá la certificación del Sistema de Gestión de la Seguridad de la Información según la ISO 27001 para aquellas áreas de actividad que lo requieran.

Ponente:

< **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.

NUEVAS HERRAMIENTAS DE PREVENCIÓN DE FRAUDE

Sinopsis:
El grupo de Seguridad del Centro de Cooperación Interbancaria-CCI y la Comisión de Seguridad, Prevención y Fraude presenta el estudio de evolución del fraude *online* en el sector durante 2005 y los primeros meses de 2006. En base a las experiencias y conclusiones obtenidas de este estudio, se presentarán en la conferencia un conjunto de iniciativas orientadas a la lucha contra el delito económico, intentando ofrecer soluciones en todos los niveles y puntos de actuación, es decir a nivel sectorial, a nivel de entidad y llegando incluso al eslabón mas débil, el usuario.

Ponentes:

< **Pedro Pablo López Bernal** es Gerente de Infraestructura de Seguridad, Auditoría y Normalización de Rural Servicios Informáticos, empresa que presta los servicios de *outsourcing* global, desde 1986, a las cajas rurales y empresas participadas que forman el Grupo Caja Rural (en total más de 73). Técnico Informático con Master en Auditoría Informática desde 1991 y CISA, en la actualidad cursa el Master en Seguridad Global en la Universidad Europea y Belt Ibérica. Ha trabajado en los últimos 21 años en los servicios informáticos de empresas como Entel, Citibank, Banco Santander y RSI. En RSI, desde 1988 ha desempeñado funciones diversas, siendo en la actualidad responsable a nivel corporativo de Grupo Caja Rural de la Infraestructura de Seguridad, Auditoría y Normalización. Además participa en el Comité de Seguridad y Salud, Comités de Informática, Organización y Banca a Distancia, Comité de Calidad y Grupos y Comisiones de Trabajo de CCI (miembro del Grupo de Seguridad), IBM, Swift y Banco de España, así como en distintos foros y publicaciones. Como Responsable de Seguridad Corporativa, ha diseñado y está llevando a cabo la implantación del Plan Director de Seguridad Corporativa tanto para RSI como para las entidades en que ésta presta sus servicios, conforme a los requerimientos y objetivos marcados y en base a una política y metodología de implantación alineadas con las principales normas de gestión de la seguridad.

< **Mariano Largo del Amo** es Director del Security Operations Center de S21sec, compañía a la que se incorporó en 2003. Con anterioridad había desempeñado la Dirección Comercial de la Agencia de Certificación Electrónica. Bajo su dirección, S21sec lidera los servicios antifraude en el mercado de habla hispana y es co-redactor del Informe Anual de Phishing del año 2005 donde se analizan más de 600 casos distintos sufridos por diversas entidades.

PROGRAMA DE GESTIÓN DE RIESGOS PARA LOS CENTROS TECNOLÓGICOS DEL GRUPO PRISA

Sinopsis:
El Grupo Prisa está integrado por un Centro Corporativo y más de 130 Sociedades agrupadas en Unidades de Negocio, que desarrollan su actividad en los sectores de educación, editorial, prensa, radio, televisión, Internet y medios musicales. Las Tecnologías de la Información son un componente esencial para las diferentes unidades de negocio, coordinándose a través de sus respectivos Centros Tecnológicos, como es el caso de El Pais, Grupo Santillana, Unión Radio, Prisacom, GMI, GDM y el Centro Tecnológico Corporativo. Atendiendo a la diversidad, el tamaño y la interrelación de sus empresas, el Grupo Prisa estima crítico realizar un Programa de Gestión de Riesgos que catalogue los activos de información para el negocio junto con sus dependencias tecnológicas, realice un análisis de riesgos de dichos activos e inicie formalmente un Programa de Seguridad a través de la definición de un Plan Operacional de Seguridad.

Ponentes:

< **Pablo Rivera Villaverde** es Director de Tecnologías de la Información de Grupo Prisa desde 2001. Licenciado en Derecho y Económicas por la Universidad Autónoma de Madrid, ha sido profesor de Servicios Financieros *online* en el Máster de Economía Financiera de ICADE (Madrid) y en el Center for Financial Innovation (Londres). Rivera ha sido responsable del proyecto de creación del Marco de Regulación y Supervisión de Servicios Financieros *online*.

< **Luis J. Buezo Bueno** es Ingeniero Industrial del ICAI, tiene un Executive MBA por el Instituto de Empresa, está certificado CISSP por el ISC^2 y GIAC 7799 por el SANS Institute. Como Gerente de la Práctica de Seguridad en HP Consulting & Integration actualmente es responsable del negocio de consultoría en las áreas de seguridad de HP en España. Previamente, ha participado y dirigido diversos proyectos en las áreas de Planificación y Gobierno de la Seguridad, Arquitectura de Seguridad, Gestión de Identidad, Seguridad en entornos militares, Planes Directores de Seguridad y otros proyectos realacionados con la gestión de la seguridad para grandes empresas y organizaciones de este país.

LOS SERVICIOS GESTIONADOS DE SEGURIDAD EN GRUPO ANTOLÍN

Sinopsis:
El concepto de servicio gestionado de seguridad propone a las organizaciones un modelo de externalización selectiva de la función de seguridad de la información que poco a poco se va consolidando como una alternativa a los modelos tradicionales. La presente ponencia estudiará un caso de éxito, exponiendo el proceso completo partiendo de la identificación de la necesidad, al despliegue y operativa de los servicios gestionados.

Ponentes:

< **Susana Cuevas Arce** es Responsable de Comunicaciones y Seguridad de Grupo Antolín, en el que empezó a prestar sus servicios en el año 2000. Licenciada en Ingeniería Superior de Telecomunicaciones por la Universidad de Valladolid, ha trabajado anteriormente en Hewlett-Packard en el Reino Unido y Telefónica I+D (diversos proyectos).

< **Roberto López Navarro** es Consultor de Seguridad en la División de Auditoría y Planificación Estratégica de Soluciones Globales Internet. Certificado CISA *(Certified Information Systems Auditor)* y CISM *(Certified Information Security Manager)* por ISACA, López Navarro es Ingeniero Superior de Telecomunicación por la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid, especializado en el área de Telemática. Ha desarrollado toda su carrera profesional en Soluciones Globales Internet, S.A., siempre asociado a la seguridad lógica.

SEGUNDO MÓDULO 26 de abril

09:15h. Entrega de documentación

09:30h. Ponencia: **La unificación de la seguridad tecnológica en el Grupo Banco Sabadell.**
Ponente: **Xavier Serrano Cossío**, Responsable de Seguridad Tecnológica del Grupo Banco Sabadell.

10:10h. Coloquio

10:15h. Ponencia: **Modelo de servicios gestionados en la seguridad de Caja Castilla La Mancha.**
Ponentes: **Faustino Villarrubia Carmona**, Jefe de Seguridad y Control de Proceso de Datos de Caja Castilla La Mancha, y **Javier Jarauta Sánchez**, Responsable de Ventas de Seguridad de Grupo SIA.

10:55h. Coloquio

11:00h. Pausa-café

11:30h. Ponencia: **El valor de la gestión de identidades en el contexto del Banco de España**
Ponentes: **Antonio Rafael Fernández Lupiáñez**, Responsable de proyectos de Seguridad. Banco de España, y **Dídac Marín Lozano**, Consultor Senior de Morse.

12:10h. Coloquio

12:15h. Ponencia: **Caja Madrid: el camino hacia la BS-7799. Lecciones aprendidas y evolución de los controles.**
Ponente: **Miguel Ángel Navarrete Porta**, Director del departamento de Seguridad Informática de Caja Madrid, y **Miguel Hoyo Nájera**, Consultor de Seguridad del Departamento de Seguridad Informática de Caja Madrid.

12:55h. Coloquio

13:00h. Debate: **El uso de software de seguridad propietario vs. software de seguridad de libre disposición y código abierto en la empresa. Ventajas e inconvenientes.**
Intervienen:
- **Pedro Castillo Muro**, Director Técnico de Seguridad Informática de Bankinter.
- **José Manuel Cea Vieira**, Director General de Check Point Software Technologies.
- **Jorge Dávila Muro**, Director del Laboratorio de Criptografía LSIIS. Facultad de Informática. Universidad Politécnica de Madrid.
- **Luis Jiménez Muñoz**, Subdirector General Adjunto del Centro Criptológico Nacional. Centro Nacional de Inteligencia.
- **Héctor Sánchez Montenegro**, Director de Seguridad Corporativa de Microsoft Ibérica.

14:20h. Coloquio

14:30h. Almuerzo

16:30h. Ponencia: **Evolución de los servicios antiphishing y de seguridad en red. La experiencia del Grupo Banco Popular.**
Ponente: **Juan Miguel Velasco López-Urda**, Director Asociado. Desarrollo de Plataformas Comunes y Servicios de Seguridad. Outsourcing de Sistemas. Telefónica Empresas.

17:10h. Coloquio

17:15h. Ponencia: **Aspectos de seguridad en el Plan de Renovación Tecnológica de la Oficina Española de Patentes y Marcas (O.E.P.M.).**
Ponentes: **José Antonio Martín Pérez**, Vocal Asesor. Jefe de la Dependencia de Informática. Oficina Española de Patentes y Marcas, y **Aurelio Martín Gómez**, Responsable de Línea de Producto Seguridad de la Información. Siemens.

17:55h. Coloquio

18:00h. Pausa-café

18:15h. Ponencia: **Mejora y consolidación de la infraestructura de seguridad del Colegio de Registradores.**
Ponentes: **Luis Alberto Lahoz Sevilla**, Director Técnico. Servicio de Sistemas de Información. Colegio de Registradores de España, y **Alfonso Franco Gómez**, Responsable de Preventa y Tecnología. División de Seguridad Lógica. Germinus.

18:55h. Coloquio

19:00h. Fin de la segunda jornada.

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

LA UNIFICACIÓN DE LA SEGURIDAD TECNOLÓGICA EN EL GRUPO BANCO SABADELL

Sinopsis:

El objetivo de la presentación es mostrar cómo la dinámica de un grupo empresarial continuamente cambiante afecta a los planes establecidos dentro del marco de un Plan Director a 3 años, que es el resultado de una foto estática, y cómo ayuda a mantener los objetivos de dicho Plan el hecho de disponer en el mismo de una metodología y un modelo de seguridad claramente establecidos. Adicionalmente, se verá cómo en el curso de una serie de transformaciones acontecidas por fusiones de empresas, se unen y conviven dos modelos diferentes de organizar la seguridad. Las transformaciones acontecidas incluyen la fusión de Banco Herrero, de Activobank, de Banco Atlántico, la disgregación de una serie de departamentos para crear una filial tecnológica a la que se externalizan un determinado grupo de sistemas y servicios y, finalmente, la externalización a un proveedor del principal Centro de Proceso de Datos, el Host y el correo electrónico. En todo este camino, se han aprendido muchas cosas que nos ayudarán en futuras dinámicas empresariales.

Ponente:

< Xavier Serrano Cossío es Responsable de Seguridad Tecnológica del Grupo Banco Sabadell. Licenciado en Informática por la Universidad Autónoma de Barcelona (postgrado en Ingeniería del Software), Master en Telemática (Universidad Politécnica de Cataluña) y en Telecomunicaciones de Empresa (Universidad Pompeu Fabra), dispone de un MBA por La Salle Bonanova. Serrano Cossío tiene una experiencia profesional de siete años como Responsable de Telecomunicaciones del Grupo Bankpyme y de tres años y medio como Responsable de Seguridad Tecnológica en este mismo Grupo. Desde hace tres años y medio ocupa el puesto de Responsable de Seguridad Tecnológica en el Grupo Banco Sabadell.

MODELO DE SERVICIOS GESTIONADOS EN LA SEGURIDAD DE CAJA CASTILLA LA MANCHA

Sinopsis:

Tras un diagnóstico de seguridad realizado el pasado año según la política de CCM, se identificaron diferentes actuaciones en materia de mejora de la seguridad, algunas orientadas a Proyectos y otras a Servicios Gestionados. Los Servicios Gestionados de Seguridad en CCM se constituyen como elemento de control efectivo de la seguridad, entendido como la puesta en marcha de un sistema exhaustivo de monitorización de todos los eventos reales y potenciales, así como la gestión de las acciones que deben ser ejecutadas ante dichos eventos para mantener un nivel de seguridad adecuado en los Sistemas de Información. Este nuevo modelo establece Acuerdos de Nivel de Servicio exigentes, que se traducen en una mejora tangible de la seguridad, tanto proactiva (mediante el seguimiento exhaustivo y periódico de vulnerabilidades) como reactiva (gracias a la detección temprana de incidentes de seguridad). El principal objetivo es la consecución de una mejora sustancial de la gestión de la seguridad, preservando los entornos claves para el negocio y simplificando de modo significativo el esfuerzo y recursos de Caja Castilla La Mancha para llevar a cabo la labor de control.

Ponentes:

< Faustino Villarrubia Carmona, Jefe de Seguridad y Control de Proceso de Datos de Caja Castilla La Mancha. Licenciado en Informática por la Universidad Politécnica de Madrid, es auditor CISA y Decano del Colegio de Ingenieros en Informática de Castilla La Mancha. Ha desarrollado su labor profesional como auditor en Caja Castilla La Mancha y Jefe de Seguridad, coordinando la definición de políticas e implantación de proyectos estratégicos de Seguridad. Ha colaborado con la Universidad Politécnica en la impartición del Master de Seguridad y Auditoría, y ha sido ponente de Securmática en anteriores ediciones. Asimismo, Villarrubia ha participado en diversos cursos, seminarios y publicaciones de seguridad en el ámbito de las Cajas de Ahorros, especialmente en el comité de Seguridad Lógica de las Cajas de Ahorros para la elaboración del Libro Blanco de Seguridad.

< **Javier Jarauta Sánchez**, Security Sales Manager de Grupo SIA. Ingeniero de ICAI por la Universidad Pontificia de Comillas, cuenta con veinte años de experiencia en el sector de la seguridad informática, liderando proyectos emblemáticos en grandes organizaciones e instituciones de la Administración Pública. Jarauta ha participado en congresos nacionales e internacionales de Seguridad y Criptografía, así como en seminarios y Masters de diferentes organismos y universidades. En la actualidad asume la responsabilidad de dirigir y coordinar el desarrollo de la venta especializada en materia de Seguridad, como Security Sales Manager, de Grupo SIA.

EL VALOR DE LA GESTIÓN DE IDENTIDADES EN EL CONTEXTO DEL BANCO DE ESPAÑA

Sinopsis:

El Banco de España, como órgano supervisor y regulador del sistema financiero español, precisa de un nivel de gestión de la seguridad que permita asegurar y garantizar el cumplimiento y alineación con la legislación vigente, su política de seguridad interna y con la política de seguridad en vigor en el sistema europeo de bancos centrales. La solución de gestión de identidades implementada, basada en IBM Tivoli Identity Manager, ha permitido y facilitado al Banco de España la consecución de sus objetivos.

Ponentes:

< **Antonio Rafael Fernández Lupiáñez** es Responsable de Proyectos de Seguridad en el Banco de España, entidad en la que lleva 15 años en su Unidad de Seguridad Informática. Como responsable del Z/OS Security Server, ha realizado diversos proyectos orientados a la integración, dentro de este componente, de distintas aplicaciones en el entorno de ordenadores centrales así como su interoperación con otras plataformas. Ha estado directamente implicado en la definición e implementación de la Política de Seguridad Informática en la entidad emisora, de su modelo descentralizado de Gestión y Administración de Seguridad Informática y su Metodología de Gestión de Riesgos. Dentro del grupo de expertos de seguridad del Sistema Europeo de Bancos Centrales (SEBC), Fernández Lupiañez ha participado en la definición de su Política de Seguridad, y en la creación y aplicación de Metodologías de Gestión de Riesgos para sistemas de información de ámbito europeo (TARGET).

< **Dídac Marín Lozano** es Consultor Senior de Seguridad en Morse. Licenciado en Informática por la UPC, ha desarrollado su carrera profesional como técnico especialista y consultor senior experto en las áreas de integración de sistemas y seguridad informática corporativa. Como consultor experto en integración de sistemas, Marín ha sido responsable del análisis, diseño e implantación de proyectos de integración y seguridad de sistemas y aplicaciones en grandes organizaciones y es co-autor de los *redbooks* de IBM "GPFS: A Parallel File System" y "High Availability and Scalability with Domino Clustering and Partitioning on AIX". Como consultor senior en seguridad, y trabajando en el área comercial de Morse desde 2000, se encarga del diseño de soluciones de seguridad corporativa en las áreas de la gestión de identidades centralizada, sistemas centralizados de autenticación y control de accceso web, sistemas de consolidación y tratamiento de eventos de seguridad, diseño e implementación de SGSIs, de sistemas de cifrado basados en estándares, etc.

CAJA MADRID: EL CAMINO HACIA LA BS-7799. LECCIONES APRENDIDAS Y EVOLUCIÓN DE LOS CONTROLES

Sinopsis:

Caja Madrid obtuvo la certificación en el estándar internacional BS-7799 en Seguridad de la Información en abril de 2005, tras un proyecto en el cual se revisaron y adaptaron los procesos de gestión de la seguridad de la Oficina Internet y de la Oficina Internet Empresas. Durante este proceso, en el que Seguridad Informática lideró

DEBATE

EL USO DE SOFTWARE DE SEGURIDAD PROPIETARIO VS. SOFTWARE DE SEGURIDAD DE LIBRE DISPOSICIÓN Y CÓDIGO ABIERTO EN LA EMPRESA. VENTAJAS E INCONVENIENTES.

Propósición: En los últimos años se ha ido conformando una polémica centrada en las posturas creadas en torno a dos posiciones-opciones de los usuarios en relación con el uso de software: la formada por los que defienden la creación-producción de software de libre disposición y código abierto, y los que defienden la creación-producción de software de propietario. En la mesa redonda se debatirá acerca de las ventajas e inconvenientes de optar unilateralmente por una de estas dos opciones, o bien hacerlo de modo selectivo, pero aplicando la supuesta disyuntiva al software con propósitos específicos de seguridad TIC y exclusivamente en escenarios empresariales.

Intervienen:

< **Pedro Castillo Muro** es Director Técnico del departamento de Seguridad Informática en Bankinter. Estudió Ciencias Químicas en la Universidad Complutense de Madrid, y desde 1992 hasta 1996 trabajó en los servicios de Informática de la Universidad Complutense como administrador de sistemas. Desde 1996 hasta diciembre de 1999 trabajó en Webline S.L. empresa fundada junto a otros compañeros y dedicada al desarrollo de aplicaciones Internet y consultoría de sistemas y seguridad. Desde enero de 2000 es Director Técnico del departamento de Seguridad Informática en Bankinter.

< **José Manuel Cea Vieira** es Director General de Check Point Software Technologies Iberia. Licenciado en Informática, está en posesión de un Master en Diseño de Sistemas y ha cursado sus estudios en EEUU. Antes de su incorporación a Check Point, desempeñó distintos puestos de responsabilidad en AT&T, Cray Research y Airtel. Posteriormente fue director de Tecnología y Desarrollo de Negocio en Bea Systems Ibérica y responsable de Desarrollo de Negocio para grandes sistemas en Sun Microsystems.

< **Jorge Dávila Muro** es Director del Laboratorio de Criptografía en la Facultad de Informática de la Universidad Politécnica de Madrid. Doctor en Ciencias Químicas por la Universidad Complutense de Madrid. Desde 1991 trabaja como Profesor Titular de Universidad en la Facultad de Informática de la UPM en temas de Seguridad Informática y Criptografía. Dávila es fundador y director del Laboratorio de Criptografía de dicha facultad y en él, desde entonces, se han formado numerosos profesionales de la seguridad informática a la vez que se desarrollan diferentes proyectos de I+D+I sobre los aspectos mas avanzados de ese ámbito.

< **Luis Jiménez Muñoz** es Subdirector General Adjunto del Centro Criptológico Nacional y Jefe del Área de Certificación del Organismo de Certificación. Entre 1991 y 1992 recibió cursos de especialización en Matemáticas y Criptología, siendo destinado al Centro Criptológico Nacional (CCN). En dicho organismo ha trabajado como especialista criptólogo entre 1992 y 1998, como especialista en seguridad de las TIC entre 1998 y 2002, y como jefe de la Unidad de Políticas y Servicios de Seguridad de las TIC entre 2002 y 2004. Desde estos puestos ha participado como representante nacional en diversos grupos de trabajo internacionales, y ha sido profesor en los cursos de especialización de Criptología y Seguridad de las TI que imparte el CCN para la Administración. Dispone de diversas certificaciones de especialización en seguridad de las TIC, incluida la de CISA por ISACA. Actualmente es el representante nacional en los Comités INFOSEC del Consejo de la Unión Europea y de la OTAN, y entre los principales cometidos de su actual puesto se encuentra el desarrollo del Esquema Nacional de Evaluación y Certificación de la Seguridad de las TIC, y la elaboración de políticas, directrices y guías de seguridad TI para la administración pública.

< **Héctor Sánchez Montenegro** es Director de Seguridad Corporativa de Microsoft Ibérica. Licenciado en Ciencias Físicas por la Universidad Autónoma de Madrid, Sánchez Montenegro, ha ocupado anteriormente diversos puestos de responsabilidad en Dinsa, Level Data y tecnología del Grupo INI. Tras su incorporación a Microsoft Ibérica en 2000, como Director de Ingeniería de Preventa de Soluciones, impulsó la firma de importantes acuerdos de compartición de código de la multinacional norteamericana con el Gobierno español. Es coautor de libros sobre protección de datos de carácter personal.

la participación de diferentes departamentos tanto de tecnología, como de negocio y de soporte de la Entidad, no sólo se realizó dicha adaptación, sino que también surgieron nuevos procedimientos y nuevas formas de actuación. La presentación pretende transmitir esta experiencia.

Ponentes:

< **Miguel Ángel Navarrete** 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.

< **Miguel Hoyo Nájera** es Ingeniero Superior de Telecomunicaciones por la Universidad Politécnica de Madrid. Ha recorrido diferentes departamentos desde que ingresara hace seis años en el Grupo Caja Madrid: Banca de Negocios, CajaMadrid e-Business y finalmente la Unidad de Organización y Sistemas, donde actualmente es consultor de Seguridad, dentro del Área de Planificación e Innovación Tecnológica, y específicamente en el Departamento de Seguridad Informática, ubicándose en el equipo de Normativas y Directrices, desde donde ha coordinado el proyecto de certificación BS-7799.

EVOLUCIÓN DE LOS SERVICIOS ANTIPHISHING Y DE SEGURIDAD EN RED. LA EXPERIENCIA DEL GRUPO BANCO POPULAR

Sinopsis:

En la conferencia se describirá la evolución de los servicios de prevención y bloqueo de ataques en red y la evolución del *phishing*, así como algunas nuevas funcionalidades que se incorporarán, fruto de la experiencia y la gestión de clientes que se realiza desde el SOC de gestión de plataformas y servicios de seguridad de Telefónica Empresas. Posteriormente, se procederá a relatar el ejemplo de actuación y defensa proactiva del servicio en el Grupo Banco Popular.

Ponente:

< **Juan Miguel Velasco López-Urda** es Director Asociado de Desarrollo de Plataformas Comunes y Servicios de Seguridad de Outsourcing de Sistemas. Telefónica Empresas. Anteriormente ha sido Subdirector de Arquitecturas y Servicios de Seguridad de la Línea de Outsourcing de Sistemas de Telefónica Empresas, Subdirector de Ingeniería de Proyectos y Servicios de Protección de la Información de la UN Hosting y ASP de Telefónica Data y Director Técnico y de Consultoría de la Agencia de Certificación Electrónica (ACE), sociedad filial de Telefónica DataCorp. Velasco ha cursado estudios de Informática en la Universidad Politécnica de Madrid y es Master Executive de Gestión Empresarial por Insead-Euroforum.

ASPECTOS DE SEGURIDAD EN EL PLAN DE RENOVACIÓN TECNOLÓGICA DE LA OFICINA ESPAÑOLA DE PATENTES Y MARCAS (O.E.P.M.)

Sinopsis:

En el último año, la Oficina Española de Patentes y Marcas ha emprendido un ambicioso Plan de Renovación Tecnológica abarcando no sólo la actualización de sus infraestructuras sino también la revisión y optimización concienzuda de todos sus procesos de negocio. Dentro de este Plan hay una serie de aspectos a los que la OEPM ha dado una importancia vital: los relativos a la seguridad. Por ello, el proyecto de Renovación Tecnológica de la OEPM, junto a Siemens actuando como socio tecnológico, ha incluido las soluciones más actuales en prevención activa de la seguridad de los sistemas, garantizando el correcto funcionamiento de su negocio.

Ponentes:

< **José Antonio Martín Pérez** es Vocal Asesor - Jefe del Departamento de Informática de la Oficina Española de Patentes y Marcas (O.E.P.M.). Licenciado en Ciencias Físicas (Automática e Informática), Martín Pérez pertenece al Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado. Anteriormente ha sido Subdirector General Adjunto de Coordinación Institucional e Infraestructura Científica en el Mº de Ciencia y Tecnología (2003-2004), Jefe de Área de Coordinación y Planificación Informática en el Mº de Justicia (2000-2003) y Responsable de Informática de la Dirección General de Objeción de Conciencia (1997-2000).

< **Aurelio Martín Gómez** es Responsable de la Línea de Producto de Seguridad de la Información de Siemens. Licenciado por la ETS de Industriales de la UNED, Martín Gómez cuenta con una extensa trayectoria en el campo de la seguridad de la información. Desde 1998 es responsable en Siemens de la Línea de Producto de Seguridad de la Información, habiendo prestado anteriormente sus servicios en Winmat como Director de Operaciones y en Eltec como Responsable de Proyectos. Es Master en Gestión y Dirección de Seguridad de la Informacion por la Universidad Pontificia.

MEJORA Y CONSOLIDACIÓN DE LA INFRAESTRUCTURA DE SEGURIDAD DEL COLEGIO DE REGISTRADORES

Sinopsis:

El proyecto de migración de la infraestructura de seguridad del Colegio de Registradores tuvo como principales objetivos actualizar la solución de seguridad y comunicaciones con los Registros de la Propiedad y Mercantiles de toda España (aproximadamente 1.000), mejorando igualmente la gestión global. La solución elegida consistió en el despliegue de una infraestructura que consolidara las necesidades de *firewalling* y redes privadas virtuales con los citados Registros, que cuentan a su vez con una solución tipo SoHo para habilitar su conexión. Toda la gestión se realiza de forma agregada, simplificándola y reduciendo errores y el tiempo necesario para dicha tarea. Germinus ha participado en el diseño de la solución y en su dimensionamiento y planificación, y ha realizado la instalación y configuración de todos los elementos que forman parte de la solución en las oficinas centrales del colegio de Registradores, tanto de los elementos de seguridad como de la plataforma de gestión.

Ponentes:

< **Luis Alberto Lahoz Sevilla** es Director Técnico del Servicio de Infraestructura y Nuevas Tecnologías del Colegio de Registradores de España. Ingeniero en Informática e Ingeniero Industrial –especialidad de Organización Industrial– es auditor de sistemas CISA por Isaca y master en sistemas y comunicaciones móviles por la Escuela de Telecomunicaciones de la UPM. Lahoz viene desempeñando sus funciones como Director Técnico del Servicio de Infraestructuras y Nuevas Tecnologías en el Colegio de Registradores, entidad donde ingresó en 2000, en donde ha sido responsable sucesivamente de los departamentos de sistemas, telecomunicaciones, infraestructuras y nuevas tecnologías. Durante los últimos años su actividad se ha centrado fundamentalmente en desarrollar proyectos de mejora en áreas como la seguridad corporativa y la firma electrónica.

< **Alfonso Franco Gómez** es Responsable de Preventa y Tecnología de la División de Seguridad Lógica de Germinus. Franco Gómez estudió Ingeniería Informática en la Universidad Politécnica de Madrid, cuenta con más de ocho años de experiencia en el campo de la Seguridad TIC y, desde el año 2001, con un conocimiento exhaustivo de la oferta tecnológica del sector, lidera la labor de preventa en la División de Seguridad de Germinus, realizando igualmente dirección de proyectos estratégicos y participando en la selección de las apuestas tecnológicas de la compañía.

TERCER MÓDULO 27 de abril

09:15h. Entrega de documentación

09:30h. Ponencia: **FNMT: Análisis de Riesgos (Magerit 2) y Plan Director de Seguridad.**
Ponentes: **Víctor Jiménez Jiménez**, Responsable de Seguridad y Auditoría Informática de la FNMT, y **Ramón Poch Vilaplana**, Director de IRM –Information Risk Management– de KPMG.

10:10h. Coloquio

10:15h. Ponencia: **Telefónica Móviles España: Plan Estratégico de Seguridad: análisis y seguimiento.**
Ponentes: **Jesús Arango Riego** es Director de División de Supervisión y Operación de Red y Presidente del Subcomité de Seguridad de Telefónica Móviles España, y **Luis Carro Martínez**, Socio de ERS - Enterprise Risk Services-de Deloitte.

10:55h. Coloquio.

11:00h. Pausa-café

11:30h. Ponencia: **Proyecto de tecnología SIM (Security Information Management) en el ámbito del Ministerio de Defensa.**
Ponentes: **Miguel Ángel Rego Fernández**, Responsable de Seguridad TIC en el Área de Seguridad de la Inspección General CIS. Ministerio de Defensa, y **Francisco Javier Santos Ortega**, Senior Manager de T&SRS –Technology & Security Risk Services– de Ernst & Young.

12:10h. Coloquio

12:15h. Ponencia: **Modelo de relación entre servicios y aplicaciones. Seguridad y calidad en el ciclo de vida.**
Ponente: **Tomás Roy Catalá**, Director de Calidad y Seguridad. Centro de Telecomunicaciones y Tecnología de la Información (CTTI) de la Generalitat de Cataluña.

12:55h. Coloquio

13:00h. Ponencia: **Infraestructuras de Certificación y Registro del DNI electrónico.**
Ponentes: **José Luis Díez Aguado**, Jefe de Unidad de Análisis y Programación de la Subdirección General de Gestión y RRHH de la Dirección General de la Policía. Ministerio del Interior, y **Ascensio Chazarra Navarro**, Gestor de Proyectos de Certificación y Firma Electrónica de Indra.

13:40h. Coloquio

13:45h. Almuerzo

15:45h. Ponencia: **Alternativas de identidad corporativas: DNI electrónico y la tarjeta corporativa de Iberdrola.**
Ponentes: **Francisco Javier García Carmona**, Director de Seguridad de la Información y las Comunicaciones de Iberdrola, y **Carlos Jiménez Suárez**, Presidente de Secuware.

16:25h. Coloquio

16:30h. Ponencia: **Tecnología y vulnerabilidades: ¿un divorcio posible?**
Ponente: **Jess García Jiménez**, Experto en Seguridad e Instructor del Instituto SANS.

17:10h. Coloquio

17:15h. Pausa-café

17:30h. Ponencia: **Identidad federada: una nueva ruta hacia la confianza.**
Ponente: **José Antonio Mañas Argemí**, Catedrático de Ingeniería Telemática. ETSI de Telecomunicación de la Universidad Politécnica de Madrid.

18:10h. Coloquio

18:15h. **Clausura de Securmática 2006**

FNMT: ANÁLISIS DE RIESGOS (MAGERIT 2) Y PLAN DIRECTOR DE SEGURIDAD

Sinopsis:

Afrontar ambiciosos proyectos relativos a Planes de Seguridad es una tarea complicada teniendo la diversidad de herramientas puestas a disposición de los profesionales de la seguridad. En este sentido, la FNMT decidió afrontar el proyecto de establecer un Plan Director de Seguridad basado en herramientas de análisis de riesgos novedosas, siendo este ejercicio uno de los pioneros utilizando Magerit 2 y Pilar. Sin duda, una gran variedad de experiencias se han sucedido a lo largo del proyecto, siendo el resultado final un excelente Plan Director soportado que tras la mejora de algunas de su funcionalidades, debe permitir servir como base para otros proyectos en otros sectores distintos al público. La ponencia establecerá los factores clave a tener en cuenta en el desarrollo de Planes de Seguridad, ofreciendo una visión practica de las áreas cubiertas y entregables a ser utilizados por parte las empresas.

Ponentes:

Víctor Jiménez Jiménez es Responsable de Seguridad y Auditoría Informática de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda. Tiene una larga experiencia en esta organización, en cuyo ámbito informático lleva trabajando más de 30 años durante los cuales ha desempeñado los cargos de Responsable de Desarrollo, Responsable de Sistemas, y Responsable Técnico del Proyecto Ceres, hasta la actualidad, en la que es Responsable de Seguridad y Auditoría Informática en el departamento de Sistemas de Información de la FNMT-RCM.

Ramón Poch Vilaplana es Director de Information Risk Management de KPMG. Economista por la Universidad de Barcelona y por la Universidad Central Lancashire de UK, es Master en Auditoría Informática y CISA así como Vocal de la Isaca en Barcelona. Inició su carrera profesional en Nestlé, siendo trasladadado como responsable de Auditoría Interna Informática a la sede mundial de Nestlé en Suiza. Posteriormente se incorporó a KPMG como Gerente del grupo de Information Risk Management en Barcelona. Actualmente es Director de la actividad en España. Poch es ponente habitual en materia de Auditoría Informática en el Instituto de Auditores Censores Jurados de Cuentas de España, así como del Instituto de Auditores Internos. Finalmente es profesor de Auditoría Informática de la Universidad de Barcelona, así como en otros foros.

TELEFÓNICA MÓVILES ESPAÑA: PLAN ESTRATÉGICO DE SEGURIDAD. ANÁLISIS Y SEGUIMIENTO

Sinopsis:

Telefónica Móviles España, alineada con la estrategia de seguridad del Grupo Telefónica, puso en funcionamiento el Subcomité de Seguridad. En dicho Subcomité están representadas todas las Direcciones Generales de TME (Red, Sistemas, Tecnología, Servicios, Ventas y Secretaría General) para opinar en materia de seguridad de la información. El principal objetivo del Subcomité es facilitar la evolución e implantación de procesos de seguridad para incrementar la seguridad de las personas, activos y sistemas de la Compañía. En este sentido, una de las primeras tareas del Subcomité de Seguridad fue poner en marcha el Plan Estratégico de Seguridad. El proyecto de Telefónica Moviles España sobre el Plan Estratégico de Seguridad en el que ha colaborado Deloitte, ha consistido en un análisis de dicho Plan contrastándolo con los estándares de seguridad del mercado (ISO 17799), posicionando los proyectos del Plan en las áreas de la ISO y cuantificando la evolución en términos de seguridad para cada uno de los proyectos. Asimismo, con el trabajo realizado, el Subcomité de Seguridad dispone de un conjunto de métricas que le permiten conocer el estado, coste, avances, etc., de los proyectos que constituyen el Plan Estratégico de Seguridad.

Ponentes:

< **Jesús Arango Riego** es Director de División de Supervisión y Operación de Red y Presidente del Subcomité de Seguridad de Telefónica Móviles España. Arango, que ha desarrollado su trayectoria profesional en el sector de las Telecomunicaciones, empezó su carrera en Telettra en el año 1982, donde desarrolló labores en áreas de Instalaciones e Ingeniería. Durante 10 años ocupó varias responsabilidades en operaciones de redes móviles en Motorola, donde fue responsable de la Cuenta de Telefónica Móviles. En el año 2000 inició su carrera en Telefónica Móviles España, donde ha estado siempre relacionado con la operación de la red y garantía del servicio.

< **Luis Carro Martínez** es socio del grupo ERS (Enterprise Risk Services) de Deloitte y lidera la línea de Seguridad de la Información. Ha trabajado desde el comienzo de su carrera profesional hace 16 años en el mundo de la auditoría y la seguridad de los sistemas de información. Entre los proyectos de seguridad más relevantes en los que ha participado destacan los relacionados con la gestión centralizada de seguridad, los planes de continuidad de negocio, *profiling* de ERP y "securización" de plataformas. Carro Martínez ha trabajado durante dos años en Deloitte USA en proyectos relacionados con la seguridad y la ley Sarbanes-Oxley y sus implicaciones con la seguridad de los sistemas de información que procesan información financiera en grandes compañías.

PROYECTO DE TECNOLOGÍA SIM (SECURITY INFORMATION MANAGEMENT) EN EL ÁMBITO DEL MINISTERIO DE DEFENSA

Sinopsis:

El Ministerio de Defensa, desde la Inspección General CIS y dentro del marco del Plan Director CIS, inició en junio del 2005 un ambicioso proyecto de implantación de una solución de tecnología SIM (*Security Information Management*) que permitiera dotar a los responsables de seguridad lógica del Ministerio de una herramienta de control y gestión de la seguridad tanto en tiempo real como en diferido, consiguiendo la centralización de la información de los *logs* de la diversidad de plataformas tecnológicas que se hallan en el Departamento y proporcionando información homogenea del estado de seguridad de los sistemas e infraestructuras. Dicho proyecto tiene como objetivo la implantación de la solución, en una primera fase, en el Centro de Comunicaciones, Explotación y Apoyo del Ministerio de Defensa, para ir aumentando su despliegue en sucesivas etapas.

Ponentes:

< **Miguel Ángel Rego Fernández** es Responsable de Seguridad TIC en el Área de Seguridad de la Inspección General CIS del Ministerio de Defensa. Anteriormente ha sido Jefe del Centro de Apoyo Informático Central, en el Cuartel General de la Armada, y profesor de la Escuela de Informática de la Armada. Rego Fernández es Comandante de la Armada (CINA) y posee los títulos de postgrado de Diplomado en Seguridad Corporativa y Protección del Patrimonio, Master en Auditoría de Sistemas de Información y Especialista en Criptología. Posee las certificaciones Fundation Certificate in IT Service Management-ITSMF (2006), CISM (2004) y CISA (2002). En la actualidad dirige el Master en Dirección y Gestión de Seguridad de la Información, organizado por Asimelec y por la Universidad Pontificia de Salamanca (Campus de Madrid).

< **Francisco Javier Santos Ortega** es responsable de proyectos de Consultoría de Seguridad y Tecnología en TSRS de Ernst & Young. Ingeniero Superior Industrial Eléctrico, especialidad en Informática, Electrónica y Sistemas de Control, por el Centro Superior de la Universidad de Zaragoza, Santos es Senior Manager del departamento de TSRS en Ernst & Young desde el 1 de enero de 2005. Cuenta con una experiencia de más de 8 años en el sector de la Seguridad Informática, tras su paso por Europa MC, SchlumbergerSema y Atos Origin. Actualmente es responsable de proyectos de Consultoría de Seguridad y Tecnología en TSRS de Ernst & Young, destacando los relativos a la gestión de la información de seguridad (SIM), gestión de identidades y servicios de certificación digital.

MODELO DE RELACIÓN ENTRE SERVICIOS Y APLICACIONES. SEGURIDAD Y CALIDAD EN EL CICLO DE VIDA.

Sinopsis:

Las organizaciones TIC buscan mejorar la calidad, fiabilidad y los costes de sus servicios confiando en que ello les permitirá incrementar la confianza, credibilidad, alineamiento y relación con el negocio. Está de moda y bien visto invocar estándares de facto: ITIL, CMMI, CobiT, UNE 71502, Six Sigma, eSCM-SP, eSCM-CL... Ninguno de ellos se solapa con los demás. Pero ninguno de ellos se conecta con los demás de forma inmediata. La falta del hilo conductor es el mayor riesgo en estos marcos de referencia que pueden llevar a ser fines en sí mismos en vez de un medio. El hilo conductor es el ciclo de vida de los productos TIC: los servicios y aplicaciones. Construir soluciones sin tener en cuenta lo que pide el cliente, es un error clarísimo. Muchas organizaciones TIC no se dan cuenta de que es igual de peligroso construir sin contemplar quién y cómo va a mantener y operar el resultado o si éste es seguro y fiable. Sólo a través de una metodología que se adapte e integre a nuestra propia organización permitiremos tales beneficios. Un solo proceso a lo largo de todo el ciclo de vida del producto, en el que todos los actores no sólo resuelven con éxito sus funciones sino que, además, dejan conectores preparados para que los próximos actores se conecten con economía (eficiencia y eficacia) de recursos. La calidad y la seguridad son óptimos candidatos a ser conectores, ya que su presencia durante todo el ciclo de vida no sólo es deseable sino también necesaria para garantizar la mejora continua del rendimiento del negocio con el mínimo de recursos.

Ponentes:

< **Tomàs 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.

INFRAESTRUCTURAS DE CERTIFICACIÓN Y REGISTRO DEL DNI ELECTRÓNICO

Sinopsis:

La aprobación del Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica, ha sentado las bases para la implantación definitiva del Documento Nacional de Identidad electrónico en España. En su virtud, todos los españoles mayores de edad que gocen de plena capacidad de obrar podrán firmar documentos de manera electrónica produciendo dicha firma los mismos efectos que la consignada en el papel. Como consecuencia de lo expuesto anteriormente, la Dirección General de la Policía, como Centro Directivo encargado de la gestión y expedición del nuevo Documento Nacional de Identidad, se convierte en prestador de servicios de certificación de firma electrónica a lo que es de aplicación la Ley 59/2003, de 19 de diciembre, de firma electrónica. La presente ponencia describe la infraestructura de clave pública que dota al nuevo DNI electrónico de los elementos necesarios para cumplir adecuadamente los objetivos anteriores.

Ponentes:

< **José Luis Díez Aguado** es Jefe de Unidad de Análisis y Programación de la Subdirección General de Gestión y RRHH de la Dirección General de la Policía, y director tecnológico del Documento Nacional de Identidad Electrónico. Díez Aguado, Comisario del Cuerpo Nacional de Policía, ingresó en el Cuerpo General de Policía en 1972, y de 1979 hasta 2005 estuvo destinado en el Área de Informática de la DGP. Experto en TIC, es Técnico de Sistemas (1983 y 1987, varios periodos) por la Escuela de Siemens (München), y posee el Master en Organización Empresarial de Sistemas de Inormación por Cenei/Ernst & Young. En 1992 obtuvo el título de Dirección de Informática y Sistemas de Información de Siemens-Nixdorf/SSI. Igualmente, ha realizado el II Curso Superior de Dirección de Seguridad de la Información (año 2000) de Belt Ibérica y el Instituto Universitario de Administración de Empresas (IADE) de la Universidad Autónoma de Madrid, y el primer curso de Seguridad de las Tecnologías de la Información (I curso Infosec) del Centro Superior de Información de la Defensa (marzo de 2001).

< **Ascensio Chazarra Navarro** es Gestor de proyectos de Certificación y Firma Electrónica en Indra. Ingeniero Superior de Telecomunicación por la Universidad Politécnica de Madrid, ha desarrollado su carrera profesional en Indra, donde actualmente desempeña el cargo de gestor de proyectos de Certificación y Firma Electrónica. Ha sido responsable técnico del despliegue de la infraestructura de clave pública del DNI electrónico y ha participado, entre otros, en los proyectos Titán de Caja Madrid, PKI del Banco de España, migración de la PKI de FNMT-Ceres y las elecciones mediante votación electrónica al Consejo Asesor de la Guardia Civil.

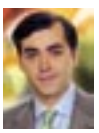
ALTERNATIVAS DE IDENTIDAD CORPORATIVAS: DNI ELECTRÓNICO Y LA TARJETA CORPORATIVA DE IBERDROLA

Sinopsis:

La protección de la plataforma informática de Iberdrola con la implementación de soluciones de seguridad robustas en cada uno de sus PCs, permite a esta organización protegerse de fugas o deterioros de la información. Durante la conferencia se presentará cómo la tecnología española utilizada por Iberdrola, en conjunción con su Tarjeta de Identificación Corporativa, permite proteger la confidencialidad e integridad de su información, así como impedir el acceso de aquellas personas no autorizadas.

Ponentes:

< **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, incorporándose 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.



< **Carlos Jiménez Suárez** es presidente de Secuware. Ingeniero Superior de Telecomunicación por la Universidad Politécnica de Madrid, desde 1989 ha sido el único ingeniero que ha simultaneado cinco de las seis especialidades. En 1988, un año antes de terminar la carrera, realizó el primer antivirus contra el virus Viernes 13. En 1990 fundó Anyware Seguridad Informática y tras la petición de colaboración por el Ministerio de Defensa Español creó la empresa Secuware. Incansable promotor del desarrollo continuo I+D+i dentro de la compañía, ha conseguido que su empresa se convierta en una compañía europea puntera en el desarrollo de soluciones de seguridad informática. Desde finales de los años ochenta lleva desarrollando soluciones de seguridad multinivel para proteger al PC frente a diversas amenazas.

TECNOLOGÍA Y VULNERABILIDADES: ¿UN DIVORCIO POSIBLE?

Sinopsis:

La tecnología evoluciona vertiginosamente y nuestras vidas y empresas lo hacen con ella. Para ello los sistemas se hacen más y más complejos, y el número y el impacto de las vulnerabilidades aumenta, poniendo en serio peligro dicha evolución. ¿Existe alguna salida? ¿Es posible acabar con las vulnerabilidades? Iniciativas como Trusted Computing se anuncian como la Tierra Prometida, pero ¿son realmente una solución? ¿Acabarán con el problema? ¿Cuál es el precio a pagar? ¿Existen otras alternativas? En esta ponencia se intentará dar respuesta a éstas y otras preguntas, y dar una visión de cómo luchar contra las vulnerabilidades de hoy y empezar a preparar a nuestras empresas para el escenario de mañana.

Ponente:

< **Jess García Jiménez** es Experto en Seguridad e Instructor del Instituto SANS. Ingeniero de Telecomunicaciones por la ETSIT de Madrid, es un especialista en seguridad que ejerce como consultor independiente para empresas, entidades financieras, de comunicaciones, espaciales y gubernamentales de Europa, Latino-América, Canadá y Estados Unidos. García es asimismo Instructor Certificado del Instituto SANS en diversas especialidades, dentro de cuyo marco participa y promueve proyectos de formación, investigación, certificación, desarrollo de contenidos, etc. Ponente y autor habitual en conferencias y publicaciones internacionales, lidera numerosos proyectos de investigación básica en el campo de la seguridad de las TIC.

IDENTIDAD FEDERADA: UNA NUEVA RUTA HACIA LA CONFIANZA

Sinopsis:

Los viejos problemas de autenticación y autorización no admiten una solución sencilla en grandes entornos, salvo centralizando. Pero donde la centralización es imposible o indeseable, los roles se reparten y crecen el número de autenticadores y autorizadores (o mejor los llamamos controladores de acceso). Los protocolos de federación permiten la cooperación entre quien conoce los detalles del aspirante y quien los necesita para conceder, denegar o ajustar condiciones de acceso. La federación es una bendición para redes homogéneas, como puede ser una intranet corporativa, habilitando el clásico SSO; son atractivas en extranets o incluso para la administración electrónica; pero crean una cierta inquietud en entornos abiertos como Internet, pues las cuestiones de seguridad y privacidad se plantean con fuerza y excepticismo. Aunque no hay mucho concepto nuevo, sí hay mucho detalle técnico, mucho protocolo y, frecuentemente, reaparece el fantasma de las PKI. ¿Es más de lo mismo? o ¿hemos encontrado la solución a la distribución de la confianza?

Ponente:

< **José Antonio Mañas Argemí** es Catedrático de Ingeniería de Sistemas Telemáticos en la E.T.S.I. Telecomunicación de la Universidad Politécnica de Madrid. Ingeniero de Telecomunicación y Doctor en Informática, está especializado en redes de comunicaciones (Internet en particular) y seguridad (criptografía y protocolos seguros para comunicaciones y medios de pago). Mañas participó en la creación del servicio de banca por Internet de BCH y Bankinter, en la definición de la arquitectura de sistemas para los JJOO de Salt Lake City, y en el análisis de seguridad del canal Internet de Loterías del Estado. Miembro del SC27 (seguridad) de ISO y editor de la norma internacional 18014 (fechado electrónico), ha participado igualmente en el desarrollo de la metodología para el análisis y la gestión de riesgos Magerit y en el de la herramienta de apoyo Pilar.

SECURMATICA, a escena

Panorámica de SECURMÁTICA 2005

Premios SIC 2006

En coincidencia con la celebración de la XVII edición de Securmática, tendrá lugar el acto de entrega de los III 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 segunda edición de los premios SIC

LA HORA DEL REENCUENTRO Y LOS RECONOCIMIENTOS

Cena de celebración

SECURMATICA 2006

XVII Congreso español de Seguridad de la Información

AFORO LIMITADO

Fechas y lugar

SECURMÁTICA 2006 tendrá lugar los días 25, 26 y 27 de abril de 2006 en el hotel NOVOTEL*. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2006 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 III Premios SIC (26 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 2006

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 25 ❑ MÓDULO 2 DÍA 26 ❑ MÓDULO 3 DÍA 27 ❑ Deseo inscribirme a SECURMATICA 2006

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**