SECURMATICA 2008

XIX Congreso español de Seguridad de la Información

22.23.24/abril

PROGRAMA

Securmática 2008, XIX edición del Congreso español de Seguridad de la Información, organizado por la revista SIC, tendrá lugar los días 22, 23 y 24 de abril del presente en su tradicional sede del Campo de las Naciones de Madrid.

Las actividades de seguridad de la información y de protección de los sistemas tecnológicos utilizados para su tratamiento en las organizaciones y como base de servicios a ciudadanos y clientes, cuyo veloz desarrollo a lomos de las TIC –en parte provocado por la obligación de respetar el derecho a la protección de los datos personales y el derecho a la intimidad, y en parte por la evidente obligación de minimizar la posibilidad de comisión de actos ilícitos y su impacto, o las consecuencias de incidentes de otra naturaleza que pudieran poner en peligro la continuidad–, no ha permitido todavía a muchas organizaciones metabolizar sus alcances y formalizar sus ubicaciones en el organigrama.

Sin embargo, los años de práctica no pasan en balde, y los responsables de la gestión de riesgos de seguridad de la información han ido aprendiendo que su actividad, trascendiendo el factor de cumplimiento, debe encauzarse hacia la aportación de valor para los negocios. Ahí está el futuro. Y de ahí que Securmática 2008 confronte en su lema, precisamente el valor para el negocio con la idea de seguridad útil. (Nada puede haber más negativo para el negocio que una seguridad inútil).

El XIX congreso, por tanto, aborda con esta idea, las diferentes facetas de la práctica de seguridad, a través de un programa en el que toman parte expertos de reconocido prestigio de entidades privadas y públicas, que aportarán sus experiencias en la formación y concienciación, la búsqueda de métodos más eficientes para analizar los riesgos, la lucha contra el fraude, la prestación de servicios desde la red, la aplicación de diversas tecnologías a la protección, el ajuste de la seguridad con los procesos de negocio, los enfoques corporativos de protección de la información en movilidad, el análisis y prospectiva de las amenazas y las fuentes de vulnerabilidades...

ES HORA DE COMPARTIR EXPERIENCIAS >>> Y AVANZAR

A ello se suma la organización de dos debates, uno dedicado al peso que tiene la seguridad en el departamento de sistemas de información, y otro centrado en el impacto de la oferta creciente de servicios de externalización de la protección TIC en el papel, atribuciones y organización de la función de seguridad en las empresas. Finalmente, se tratará un asunto de notable interés: el efecto en las entidades que tiene el tratamiento que de la seguridad se hace en el reglamento de desarrollo de la LOPD.

Copatrocinadores:

accenture High performance. Delivered. · Deloitte. · dominion · Ernst & Young Quality In Everything We Do · gmv · Grupo Gesfor · hp invent · IBM · Indra · KPMG · PricewaterhouseCoopers · SIEMENS · Telefónica

Organiza:

Revista SIC seguridad en informática y comunicaciones

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

PRIMER MÓDULO 22 de abril

08:45h. Entrega de documentación.
09:15h. Inauguración.
Moderador: **Arturo Ribagorda Garnacho**, Catedrático de Ciencias de la Computación e Inteligencia Artificial. Universidad Carlos III de Madrid.
10:00h. Ponencia: **La seguridad en el ciclo de vida de los documentos electrónicos.**
Ponente: **Manuel Carpio Cámara**, Director de Seguridad de la Información y Prevención del Fraude de Telefónica.
10:40h. Coloquio.
10:45h. **Ponencia**: **Formación y concienciación de seguridad en el Grupo Santander.**
Ponente: **José Antonio Castro González**, Director de Seguridad Corporativa del Grupo Santander.
11:25h. Coloquio.
11:30h. Pausa-café.
12:00h. **Ponencia**: **Alternativas viables para analizar los riesgos de seguridad en tiempos de mercado: la teoría de juegos.**
Ponente: **Santiago Moral Rubio**, Director de Seguridad Lógica Corporativa del Grupo BBVA.
12:40h. Coloquio.
12:45h. **Ponencia**: **Qué lugar debe ocupar la seguridad TIC en la estrategia global del CIO.**
Ponente: **José Luis Checa López**, Director Gerente del Centro de Telecomunicaciones y Tecnologías de la Información (CTTI) de la Generalitat de Cataluña.
13:25h. Coloquio.
13:30h. **Ponencia**: **Los procesos de la seguridad.**
Ponentes:
• **Francisco Javier García Carmona**, Director de Seguridad de la Información y las Comunicaciones. Iberdrola.
• **Rafael Ortega García**, Socio Director de TSRS de Ernst & Young.
14:10h. Coloquio.
14:15h. Almuerzo.
Moderador: **Jorge Dávila Muro**, Profesor Titular de la Facultad de Informática y Director del Laboratorio de Criptología LSIIS de la Universidad Politécnica de Madrid.
16:15h. **Ponencia**: **Endesa: transformación de la seguridad en un contrato de *outsourcing*.**
Ponentes:
• **Justo López Parra**, Responsable de Seguridad Informática. Endesa.
• **María José Caballero Molina**, Security Account Manager para Endesa. IBM.
16:55h. Coloquio.
17:00h. **Ponencia**: **Sara Lee: afrontando los retos de seguridad en una organización multinacional.**
• **Denis Ontiveros Merlo**, VP Global Information Security. Sara Lee Corporation.
• **Daniel Solís Agea**, Director IT Advisory. KPMG.
17:40h. Coloquio.
17:45h. Pausa-café.
18:00h. **Ponencia**: **Universidad del País Vasco: gestión integrada de la seguridad lógica y la seguridad física.**
Ponentes:
• **Javier Estefanía Cundín**, Director de Informática de Gestión. Universidad del País Vasco. UPV.
• **Víctor Llorente Gómez**, Director de la Línea de Seguridad de Sistemas de Información. Dominion.
18:40h. Coloquio.
19:45h. Fin de la primera jornada.

LA SEGURIDAD EN EL CICLO DE VIDA DE LOS DOCUMENTOS ELECTRÓNICOS

Sinopsis

La puesta en práctica de una política de clasificación de la información plantea interesantes retos a las organizaciones verdaderamente comprometidas con tal iniciativa. En este caso, deberán tenerse en cuenta los servicios de seguridad requeridos: confidencialidad, integridad, disponibilidad... aplicados a cada uno de los distintos formatos que una determinada información puede adoptar a lo largo de su vida útil. Durante la conferencia nos centraremos en el caso particular del servicio de confidencialidad aplicado a los documentos de gestión del negocio en formato electrónico mediante el uso de herramientas de gestión de derechos digitales. Presentaremos el caso práctico de despliegue en una organización compleja de ámbito internacional y advertiremos al responsable de seguridad sobre algunas de las previsibles dificultades que habrá de sortear cuando dé este paso obligado en el ejercicio de su función.

Ponente

• **Manuel Carpio Cámara** es Director de Seguridad de la Información y Prevención del Fraude de Telefónica y miembro del Comité Corporativo de Seguridad de esta compañía. Ingeniero Superior de Telecomunicaciones por la UPM, Programador de Sistemas por la Escuela Superior de Informática, PDD IESE (Universidad de Navarra), y certificado CISA y CISM por ISACA, Carpio ha sido representante español en el ESRAB por designación de la Comisión Europea y es profesor en el Máster de Auditoría y Seguridad de ALI y la Universidad Politécnica de Madrid, y en el Máster de Gestión y Dirección de Seguridad de la Información de Asimelec y la Universidad Pontificia de Salamanca.

FORMACIÓN Y CONCIENCIACIÓN DE SEGURIDAD EN EL GRUPO SANTANDER

Sinopsis

Sin duda alguna nos encontramos ante uno de los ampliamente considerados como aspectos menores de la seguridad, la formación; un concepto generalista que se suele asociar equivocadamente al conocimiento específico de algunas materias relativas a seguridad por parte del usuario final de los sistemas de información. También no es menos cierto que ante grandes males tendemos a aportar enormes soluciones, olvidándonos de una de las principales habilidades que debe poseer el responsable de seguridad, la gestión de problemas complejos, y de las herramientas y posibilidades que las organizaciones ponen a nuestra disposición. En esta ponencia, que realmente es la exposición de un caso práctico, se mostrará cómo ha abordado el Grupo Santander la formación y concienciación de la seguridad de la información, las acciones y programas concretos para dar una adecuada cobertura a este aspecto.

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 (20 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.

ALTERNATIVAS VIABLES PARA ANALIZAR LOS RIESGOS DE SEGURIDAD EN TIEMPOS DE MERCADO: LA TEORÍA DE JUEGOS

Sinopsis

Como continuación del Método Casandra, presentado en Securmática 2007, se describe en esta ocasión con mayor grado de detalle uno de sus componentes, que es el Análisis de Riesgos basado en la Teoría de Juegos. Este modelo de Análisis de Riesgos lleva utilizándose varios años en BBVA con muy buenos resultados. Está fundamentado en el análisis de situaciones de riesgo donde existe un componente de intencionalidad. El análisis de la relación existente entre esta intencionalidad y la corporación que sufre el evento se realiza siguiendo la Teoría de Juegos. Se expondrán en la conferencia un par de ejemplos concretos utilizando este análisis. La Teoría de Juegos está permitiendo tomar decisiones muy rápidas y con gran precisión en materia de gestión de riesgos y está facilitando su comunicación hacia la Dirección. Un entorno muy cambiante exige modelos de toma de decisiones muy ágiles.

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.

QUÉ LUGAR DEBE OCUPAR LA SEGURIDAD TIC EN LA ESTRATEGIA GLOBAL DEL CIO

Sinopsis

Frente a una de las grandes preguntas del mundo de la seguridad, el ponente intentará aportar la visión estratégica de la seguridad para alguien que accede a la posición de CIO de una gran organización, y además CEO de una empresa pública, después de haber ocupado la posición de CISO en otra gran organización. Claramente, la experiencia pasada condicionará la visión de la seguridad aplicada a la gestión TIC, pero aparecen posibles preguntas, tales como: ¿llega a estar condicionada la agenda del CIO realmente por la experiencia pasada?, o bien, ¿los grandes temas de la gestión TIC anteponen criterios de operatividad, costes y en definitiva, orientación a negocio y resultados frente a la seguridad?, y, finalmente, ¿son las estrategias organizativas y de negocio las que deben contemplar la seguridad como un factor que afecta al éxito de las mismas?

Ponente

• **José Luis Checa López** es Director Gerente del Centro de Telecomunicaciones y Tecnologías de la Información, CTTI, de la Generalitat de Cataluña. Ingeniero Técnico Industrial por la 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). Posteriormente ocupó el cargo de Responsable de Seguridad de la Información del Grupo Gas Natural.

LOS PROCESOS DE LA SEGURIDAD

Sinopsis

Hablamos de la Información, Seguridad de la Información, de la Información de Seguridad, de Gestión de Riesgos; como se puede observar, parece una secuencia ciertamente lógica en el ámbito de nuestra actuación y responsabilidad, pero dentro de esta lógica podemos llevar a cabo todas nuestras actividades de manera muy particular; es decir, a nuestro criterio y estilo y, seguramente, con un nivel de esfuerzos y éxitos aceptable. Pero hablando de secuencia, como sinónimo de progreso, ¿por qué no ponernos en consonancia con el estilo y maneras de hacer de nuestras organizaciones? La respuesta es simple: Gestión por Procesos. Ésta nos facilitará el alineamiento e integración de los procesos de la Seguridad, o mejor dicho, de la gestión del riesgo, en los procesos de Negocio: ésta es la clave.

Ponentes

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

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

ENDESA: TRANSFORMACIÓN DE LA SEGURIDAD EN UN CONTRATO DE *OUTSOURCING*

Sinopsis

El proyecto de transformación de la seguridad en el contrato de *outsourcing* entre Endesa e IBM Global Technology Services es fruto de la unión del requerimiento de Endesa Servicios de parametrizar la seguridad de los servidores que dan servicio al negocio de Endesa, de acuerdo a la política de seguridad de Endesa y de la experiencia de IBM GTS en adaptar e implantar las políticas de seguridad de sus clientes de *outsourcing* al nivel tecnológico de sus servidores. Es una historia de compromiso y aportación mutua en la que cada parte es responsable de un aspecto de la seguridad y se mejoran mutuamente con la interrelación, algo que se concreta en el acuerdo de un Documento de Políticas de Seguridad (GSD331 o ISec son los estándares de IBM GTS) y de un proyecto de transformación de Políticas de Seguridad con objetivos de seguridad y gestión de impacto y riesgos. Pero es sobre todo una apuesta por parte de Endesa Servicios a favor de la seguridad, patrocinada por la alta dirección, gestionada por Seguridad Informática de Endesa Servicios y desplegada a los responsables funcionales de los aplicativos de negocio de Endesa.

Ponentes

• **Justo López Parra** es Responsable de Seguridad Informática de Endesa desde septiembre de 2006. Empezó a trabajar en seguridad dentro del Grupo Telefonica como responsable de Seguridad Informática en Terra Networks, incorporándose a Endesa en 2001, desde donde ha venido ocupando distintos cargos en las areas de Innovación y Seguridad Informática. López Parra es Ingeniero Informático por la Universidad de Castilla La Mancha y cuenta con la certificación CISM.

• **María José Caballero Molina** es Security Account Manager para Endesa del área Strategic Outsourcing de IBM Global Technology Services. Ha realizado su carrera profesional en diferentes áreas de Gestión de Servicios IT, teniendo relación desde hace una década con el área de Seguridad Informática, habiendo sido últimamente Security Account Manager para otras grandes organizaciones de *outsourcing* de IBM Global Technology Services. Caballero Molina ha obtenido la certificación profesional de seguridad "GIAC" de SANS Institute y es licenciada en Ciencias Físicas por la Universidad de Cantabria.

SARA LEE: LOS RETOS DE LA SEGURIDAD PARA UNA ORGANIZACIÓN MULTINACIONAL

Sinopsis

Los retos que deben afrontar las organizaciones para mantener la seguridad de su información se ven, en el caso de las multinacionales, incrementados por numerosos factores, como las diferencias culturales y legislativas o la distancia entre los centros operativos y los centros de decisión, que deben tenerse en cuenta para lograr el éxito. En esta ponencia se describirá la estrategia de Sara Lee Internacional para afrontar estos retos, considerando los principales aspectos a tener en cuenta, como la organización, los estándares y normativas internas y la monitorización de la situación de sus negocios y localizaciones geográficas en Americas, EMEA y APAC.

Ponentes

• **Denis Ontiveros Merlo** es VP Global Information Security de Sara Lee Corporation. Con más de una década de experiencia en el mundo de la seguridad de la información, Ontiveros ha liderado múltiples proyectos de envergadura. Inició su andadura profesional en seguridad y más concretamente en auditoría informática en 1999 dentro de KPMG, donde fundó la práctica Barcelona de Information Risk Management de KPMG y donde ejerció de gerente durante varios años. En 2004 se incorporó a la multinacional Sara Lee como responsable de Seguridad de la Información para EMEA, APAC y Latinoamérica. En junio del 2007 asumió la responsabilidad como VP Global Information Security, añadiendo a su responsabilidad la región de las Américas. Diplomado en Ciencias Empresariales por la Universidad del País Vasco y con especialidad en Informática aplicada a la empresa por la Fachhochschule de Wirtschaft de Berlín, es Master en E-Business por la UPC y certificado CISA y CISM.

• **Daniel Solís Agea** es Director de KPMG. En la actualidad dirige la línea de servicios de Seguridad, Privacidad y Continuidad (SPC) en el área de IT Advisory. Con más de diez años de experiencia en el sector de la seguridad de la información y las telecomunicaciones, es Ingeniero en Telecomunicaciones, ha participado en diferentes proyectos de seguridad desarrollando estrategias corporativas en materia de protección de la información, como planes directores, expansiones internacionales de planes directores y estratégicos de seguridad, Sistemas de Gestión de 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.

UNIVERSIDAD DEL PAÍS VASCO: GESTIÓN INTEGRADA DE LA SEGURIDAD LÓGICA Y LA SEGURIDAD FÍSICA

Sinopsis

En la actualidad existe una creciente necesidad por parte de las organizaciones que cuentan con una elevada complejidad tecnológica de optimizar de manera integrada sus procesos internos y externos de autenticación de accesos tanto físicos como lógicos, con el fin de lograr una reducción de sus costes de administración y un control unificado e integrado de su seguridad. Teniendo en cuenta este contexto, la Universidad Pública del País Vasco / Euskal Herriko Unibertsitatea (UPV / EHU), es una de las entidades que ha decidido abordar, de la mano de Dominion, un ambicioso e innovador proyecto que le garantice una gestión centralizada e integrada de su seguridad de accesos físicos y lógicos.

Ponentes

• **Javier Estefanía Cundín** es Director del Centro de Informática de Gestión de la Universidad del País Vasco / Euskal Herriko Unibertsitatea (UPV / EHU). Licenciado en Informática por la Universidad de Deusto, se incorporó en 1984 a la plantilla del Centro de Cálculo de la Universidad del País Vasco. Ha sido responsable del área de Seguridad, Sistemas y Comunicaciones de la Universidad del País Vasco, y actualmente, y desde 2003, es el Director del Centro de Informática de Gestión.

• **Víctor Llorente Gómez** es, desde 2003, Gerente de la línea de Seguridad de Sistemas de Información de Dominion. Licenciado en Informática por la Universidad de Deusto, es máster de Ingeniería del Software y Seguridad de Sistemas por la Universidad de Deusto–Eside, y cuenta con las certificaciones Clarify, CISA y Certificación SGSI. Con anterioridad ha trabajado en Ibermática y en DMR Consulting –actual Everis– en esta última en numerosos proyectos de seguridad técnica y consultoría (Lortad-Lopd, Planes de Continuidad de Negocio, Planes Directores de Seguridad, Análisis y Gestión de Riesgos y Diagnósticos de Seguridad), así como Gerente del Área de Seguridad Lógica de DMR Consulting.

SEGUNDO MÓDULO 23 de abril

09:15h. Entrega de documentación.
Moderador: **José Manuel Vidal Formoso**, Presidente de la Asociación de Auditores de Sistemas (ASIA) y del Capítulo de Madrid de ISACA.

09:30h. **Ponencia**: **Implantación del modelo de segregación de funciones a través de SAP GRC (Governance, Risk & Compliance)**
Ponentes:
- **Ignacio Vázquez Suárez**, Director del Departamento de IT de Grupo Río Narcea Gold Mines.
- **Luis Carro Martínez**, Socio de Enterprise Risk Services-ERS. Deloitte.

10:10h. Coloquio.

10:15h. **Ponencia**: **La seguridad en la banca del futuro**.
Ponente: **Miguel Ángel Navarrete Porta**, Director del Departamento de Seguridad Informática de Caja Madrid.

10:55h. Coloquio.

11:00h. Pausa-café.
Moderador: **Carlos Manuel Fernández Sánchez**, Gerente de TI. Director de Desarrollo Estratégico y Corporativo de AENOR.

11:30h. **Ponencia**: **El Plan Estratégico de Seguridad**.
Ponente: **Jesús Milán Lobo**, Director del Departamento de Seguridad Informática de Bankinter.

12:10h. Coloquio.

12:15h. **Ponencia**: **Diseño del Centro de Operaciones de Seguridad del Ministerio de Defensa.**
Ponentes:
- **Miguel Ángel Rego Fernández**, Área de Seguridad – Inspección General CIS. Ministerio de Defensa.
- **David Fernández-Granado**, Gerente del Área de Seguridad Operacional de Hewlett Packard. Consulting & Integration.

12:55h. Coloquio.

13:00h. **Debate**: **El peso de la seguridad TIC en el Departamento de Sistemas de Información.**
Moderador: **José de la Peña Muñoz**, Director de la revista SIC.
Intervienen:
- **Rubén Muñoz Fernández**, Director de Tecnología y Sistemas de Correos.
- **Joaquín Reyes Vallejo**, Director de Sistemas de Información de Cepsa.
- **Santiago Segarra Tormo**, Director del Departamento de Informática Tributaria de la Agencia Estatal de Administración Tributaria.

14:00h. Almuerzo.
Moderador: **Javier Areitio Bertolín**, Catedrático de la Facultad de Ingeniería. ESIDE. Director del Grupo de Investigación Redes y Sistemas.Universidad de Deusto.

16:00h. **Ponencia**: **Nuevos servicios de Red: Anti-*phishing* de segunda generación y Anti-caballos de Troya. El ejemplo del Banco Sabadell.**
Ponentes:
- **Xavier Serrano Cossío**, Responsable de Seguridad Tecnológica. Banco Sabadell.
- **Juan Miguel Velasco López-Urda**, Director Asociado de Servicios y Soluciones de Seguridad. Servicios desde la RED. UN. Grandes Clientes. Telefónica España.

16:40h. Coloquio.

16:45h. **Ponencia**: **Desarrollo conjunto de nuevos servicios de seguridad y certificación electrónica.**
Ponentes:
- **Javier Montes Antona**, Jefe de Servicio de Colaboraciones Externas de CERES. (FNMT)
- **Miguel Ángel Corpa Ortiz**, Senior Manager Responsable de Servicios de certificación y firma electrónica de Accenture.

17:25h. Coloquio.

17:30h. Pausa-café.

17:55h. **Ponencia**: **Comunidad de Madrid: problemática y arquitectura de seguridad de Educamadrid.**
Ponentes:
- **Felipe Retortillo Franco**, Jefe de la Sección de Desarrollo de Nuevas Tecnologías. Dirección General de Infraestructuras y Servicios. Consejería de Educación. Comunidad de Madrid.
- **Antonio Requejo Novella**, Gerente de Desarrollo de Negocio de Seguridad. Grupo Gesfor.

18:35h. Coloquio.

18:40h. Fin de la segunda jornada.

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

IMPLANTACIÓN DEL MODELO DE SEGREGACIÓN DE FUNCIONES A TRAVÉS DE SAP GRC (GOVERNANCE, RISK & COMPLIANCE)

Sinopsis

El control de acceso y la gestión de las autorizaciones a los recursos por parte de los usuarios es una de las áreas principales de riesgo a tratar en un proceso de puesta en funcionamiento de un entorno de control eficaz y eficiente en el ámbito de los sistemas de información. Todas las compañías tienen o están en fase de definir y poner en marcha un entorno de control adecuado a su entorno económico, de mercado, operacional, etc. La carencia estructural de herramientas y la gestión manual de la gestión de los usuarios y sus autorizaciones suele llevar a una asignación excesiva de privilegios de los usuarios y por tanto, a incompatibilidades e incumplimiento en la segregación de funciones, incremento de esfuerzos y coste.

Ponentes

• **Ignacio Váquez Suárez** es Director del Departamento de IT de Grupo Río Narcea Gold Mines. Nacido en Oviedo en 1975, cursó estudios de Ingeniería Técnica Informática de Sistemas en la Universidad de Oviedo, donde también tuvo sus primeras experiencias laborales. Tras unos años como *freelance* trabajando para varias empresas asturianas, es fichado por el Grupo Río Narcea en 2001, coincidiendo con la fuerte expansión de la empresa, asumiendo la dirección del Departamento de IT. En estos últimos seis años ha liderado los planes de IT del Grupo Río Narcea en España, Portugal, Canadá y Mauritania, incluyendo la alineación de los sistemas de IT con SOX-404.

• **Luis Carro Martínez** es Socio de la división de Enterprise Risk Services (ERS) de Deloitte. Su experiencia principal en la firma, desde su ingreso en 1990, consiste en la realización de proyectos de seguridad y consultoría tecnológica. Es responsable del área de seguridad. Licenciado en Informática por la Universidad Politécnica de Madrid, está en posesión del título CISM de la ISACA y del certificado en BS7799. Ha trabajado durante dos años en Deloitte en Estados Unidos hasta agosto de 2005, siendo socio responsable de los proyectos de auditoría de sistemas de información y seguridad de varias compañías SEC. Asimismo, ha trabajado en proyectos de Sarbanes Oxley en Estados Unidos y en la adaptación de los controles a las legislaciones vigentes.

LA SEGURIDAD EN LA BANCA DEL FUTURO

Sinopsis

Como el futuro es incierto, para hablar de él con alguna garantía hay que preguntar a un viajero del tiempo y, al menos yo, no conozco a ninguno. También puedes declararte visionario, lo que no es mi caso, y a lo mejor así consigues que alguien crea alguna de las cosas que digas. En esta ponencia, se pretende simplemente imaginar con los pies en el suelo y asumir un riesgo razonable de error en lo expuesto, a lo que sí estoy acostumbrado. No obstante, entiéndase que pretenda contener la exposición en ese límite de "razonabilidad" del riesgo y para ello pinte algunos márgenes. Futuro significará el 2011 (más o menos). Banca querrá decir Caja Madrid (aunque me temo que no voy a poder cumplirlo). Seguridad tendrá un vocabulario de gestión y no tecnológico. La ponencia trata de lo que, en opinión del conferenciante, es uno de los retos de la seguridad de la información del futuro: continuar siendo capaces de gestionar riesgos eficazmente, conociendo cuáles son los actores, las vulnerabilidades y las soluciones razonables para aplicar en un "ecosistema" agresivo, en el que usuarios, clientes y proveedores accederán desde cualquier lugar, a cualquier hora, por cualquier canal, a través de cualquier servicio, precisando conocer o alterar cualquier dato.

Ponente

• **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.

EL PLAN ESTRATÉGICO DE SEGURIDAD

Sinopsis

Hasta la fecha, la mayoría de organizaciones disponían de Planes Directores de Seguridad como herramienta de ayuda a la planificación en el medio y largo plazo, generalmente relativas a la implementación de buenas prácticas –véase ISO 27002, ISF, COBIT, etc.–, así como a la adecuación a la regulación vigente que le fuera de aplicación. Ahora bien, según la entidad va adquiriendo madurez y el nivel de implementación de controles técnicos y organizativos alcanza niveles razonables que nos permiten levantar la vista del día a día, nos empiezan a sonar en la cabeza conceptos como Sistemas de Gestión, certificación, la seguridad como servicio, alineamiento con el negocio, calidad, etc., es el momento de ir un paso más allá en el planteamiento. Un paso más allá que no persigue otro fin que garantizar que la visión, la misión, así como los procesos y tareas que desde el Departamento de Seguridad se realizan se encuentren alineadas con la estrategia de la entidad, en sus principios, sus valores y sus objetivos, así como disponer de una herramienta eficaz para la toma de decisión, la gestión del cambio y como elemento cohesionador de grupo. Si además para ello se utilizan técnicas y modelos de gestión estratégica ampliamente reconocidos, divulgados y aplicados con éxito en el ámbito de las áreas de negocio, lo que se tendrá no sólo será algo que te aporte valor como gestor y responsable de un área, sino que también agregará valor a tu entidad desde un punto de vista global.

Ponente

• **Jesús Milán Lobo** es Director de Seguridad Informática en Bankinter. Ingeniero en Informática con especialidad en Gestión por el ICAI-ICADE, dispone del certificado CISM (Certified Information Security Manager) de ISACA. Certificado Lead Auditor, es miembro del Subcomité Nacional de Seguridad de las TI (CTN 71 / SC27) y miembro del WG1, habiendo colaborado en la redacción de varias normativas, tanto nacionales como internacionales. Actualmente representa al SC27 en las reuniones Internacionales ISO y colabora en la redacción, entre otras, de la norma 27004 "Information Security Management Measurement". Milán Lobo es, además, miembro de la Comisión de Seguridad de ASIA, del Comité de Seguridad Informática y de la Comisión de Seguridad, Prevención y Fraude del Centro de Cooperación Interbancaria y de la Junta Directiva del ISMS Forum Spain.

DISEÑO DEL CENTRO DE OPERACIONES DE SEGURIDAD DEL MINISTERIO DE DEFENSA

Sinopsis

Durante estos últimos años, el escenario de amenazas ha evolucionado de forma que se ha pasado de incidentes de seguridad originados por individuos aislados o grupos poco organizados a ataques, que con motivaciones políticas o delictivas, provienen de fuentes altamente capacitadas y estructuradas. Esta nueva realidad, unida al incremento en la sofisticación de las técnicas utilizadas, ha llevado a las organizaciones a constituir centros de operaciones de seguridad (COS). En ellos, la especialización y el empleo de metodologías específicas permiten una adecuada gestión de los servicios de seguridad, aportando la capacidad de prevenir, contener y reaccionar ante los incidentes, minimizando sus impactos en los activos. El Ministerio de Defensa se encuentra inmerso en la constitución de un COS y compartirá en esta conferencia los retos más significativos abordados durante la fase de definición y diseño.

Ponentes

• **Miguel Ángel Rego Fernández** es Comandante de la Armada. Desde 2003 está destinado en el Área de Seguridad de la Inspección General CIS del Ministerio de Defensa, dirigiendo, entre otros, el proyecto de definición del Centro de Operaciones de Seguridad y el desarrollo normativo de seguridad de la información. Desde 2004 a 2006 fue Director del proyecto de Identidad Digital de Defensa. Es Director académico y profesor del Master en Dirección y Gestión de Seguridad de la Información de la Universidad Pontificia de Salamanca (Campus de Madrid) y profesor de la Cátedra D. Juan de Borbón de la Universidad Complutense de Madrid. Cuenta con postgrados y certificaciones profesionales en seguridad y en gestión de servicios TI.

• **David Fernández-Granado** es Gerente del área de Seguridad Operacional de Hewlett-Packard dentro de la Práctica de Seguridad de Consulting & Integration. Ingeniero Industrial del ICAI y certificado ITIL Service Manager, trabaja para HP desde 2001 y tiene amplia experiencia no sólo en proyectos de seguridad de la información, sino también en implantación de procesos de IT, así como en Planes de Continuidad de Negocio. Sus funciones principales son la gestión del portafolio de soluciones de seguridad operacional y el desarrollo del negocio de las mismas.

NUEVOS SERVICIOS DE RED: ANTI-*PHISHING* DE SEGUNDA GENERACIÓN Y ANTI-CABALLOS DE TROYA. EL EJEMPLO DE BANCO SABADELL

Sinopsis

Tras más de cuatro años de implantación y desarrollo de los servicios de seguridad desde la RED, la nueva generación de servicios evoluciona el concepto tradicional de Anti-*spyware*, Anti-caballos de Troya, y la nueva versión del servicio Anti-*phishing* con la gestión proactiva y predictiva del fraude en tiempo real a través del monitor de transacciones. Se realizará un análisis de la incidencia del *phishing* y el *spam* en 2007 y, posteriormente, Banco Sabadell, uno de los usuarios pioneros del servicio, contará su experiencia en la materia.

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, Telecomunicaciones y Administración de Sistemas, habiendo desarrollado la mayor parte de su carrera profesional en el sector financiero. Serrano Cossío ha dirigido, desde su incorporación en 2002 al Banco Sabadell, la ejecución del Plan Director de Seguridad Tecnológica 2004-2006 y ha liderado la realización del Plan Director de Seguridad Tecnológica 2007-2009.

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

DEBATE

EL PESO DE LA SEGURIDAD TIC EN EL DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN

La instauración de la función específica de seguridad en los departamentos de sistemas de información de entidades, es en sí una prueba del peso que los DSI confieren a esta práctica en el contexto de lo que hoy se entiende por buen gobierno TI, al tiempo que se convierte en un reflejo más de su estrategia. En el debate, se tratará de pulsar la opinión profesional de los directivos participantes acerca del presente y futuro de la función, sus relaciones con otras áreas de sistemas y con otras áreas de la organización, la mayor o menor atención presupuestaria que la protección TIC demanda hoy y demandará en un futuro previsible, el estado del arte de las herramientas tecnológicas orientadas a la seguridad en orden a su uso y la alternativa de la externalización.

Intervienen:

• **Rubén Muñoz Fernández** es Director de Tecnología y Sistemas de Correos, estando a cargo del desarrollo y modernización de los sistemas de información y la gestión de la infraestructura técnica y de telecomunicaciones de que dispone esta entidad. Ingeniero Superior Industrial y Máster en Administración de Empresas, posee una experiencia profesional de más de 17 años en TI. Anteriormente ha trabajado en Banco Santander Central Hispano como director de la unidad de e-business para empresas, comercio-e y servicios dirigidos a las administraciones autonómicas, así como en diversos proyectos internacionales; en BBVA, en la función de Director Técnico del banco en línea uno-e y de otras iniciativas de *e-business*, medios de pago electrónicos y servicios multibancarios; en Banesto (en la dirección de proyectos informáticos de las diferentes áreas de negocio de la entidad y liderando la implantación de las nuevas tecnologías), y en Accenture y Compaq en misiones de consultoría de sistemas informáticos.

• **Joaquín Reyes Vallejo** es Director de Sistemas de Información del Grupo Cepsa desde el año 2003. Con anterioridad, fue responsable del área de Tecnologías de la Información de la Red de Estaciones de Servicio, y también de la dirección del Departamento de Informática Técnica e Investigación Operativa desde 1985. Inició su carrera profesional en 1976 como Ingeniero de Seguridad de Centrales Nucleares en Empresarios Agrupados. Es licenciado en Ciencias Físicas, Ciencias Económicas y Diplomado en Ingeniería Nuclear.

• **Santiago Segarra Tormo** es Director del Departamento de Informática Tributaria de la Agencia Estatal de Administración Tributaria, A.E.A.T., desde 1997. Ingeniero Industrial por la Universidad Politécnica de Valencia, Auditor de Cuentas y Funcionario de carrera perteneciente al Cuerpo Superior de Inspectores de Hacienda del Estado, su carrera profesional se ha desarrollado realizando funciones de inspección en Valencia y Madrid. Ha sido Subdirector General de Aplicaciones del Departamento de Informática de la A.E.A.T. y Jefe de Unidad Regional de Inspección en la Delegación Especial de Madrid.

DESARROLLO CONJUNTO DE NUEVOS SERVICIOS DE SEGURIDAD Y CERTIFICACIÓN ELECTRÓNICA

Sinopsis

La conferencia se centrará en el análisis de los desarrollos realizados conjuntamente con la Fábrica Nacional de Moneda y Timbre, FNMT, en el marco de los nuevos servicios de seguridad y certificación electrónica que está demandando el mercado: PKI para firma en móviles (antecedentes, objetivos, marco global, características de la solución desarrollada, aspectos relevantes del proyecto...), plataforma de factura electrónica (barreras identificadas, descripción de la solución desarrollada, aspectos a considerar y modelo de colaboración establecido...), PKI del funcionario y otros proyectos.

Ponentes

• **Javier Montes Antona** es Jefe de Servicio de Colaboraciones Externas de CERES, siendo responsable del área comercial, soporte técnico a Administraciones y empresas, así como de los servicios de atención al usuario de CERES y del DNIe. Ingeniero Técnico Industrial por la Universidad Politécnica de Madrid, su carrera profesional comenzó hace 34 años en el Parque de Atracciones de Madrid, pasando posteriormente a Alcatel, donde estuvo durante 9 años colaborando en la fabricación de centrales telefónicas. Durante los 24 últimos años ha estado ligado a la Fábrica Nacional de Moneda y Timbre, donde ha adquirido una visión amplia al haber formado parte de múltiples departamentos como Mantenimiento, Compras, Ingeniería de tarjetas, Investigación y Desarrollo, y finalmente durante los últimos años en CERES. Ha escrito diferentes artículos sobre criptografía, ha participado en diferentes grupos de trabajo multi-empresariales, y ha realizado numerosas ponencias sobre certificación y firma electrónica en múltiples foros.

• **Miguel Ángel Corpa Ortiz** es *Senior Manager* responsable de los servicios de certificación y firma electrónica en Accenture y Director del Centro de servicios de factura electrónica. Licenciado en Ciencias Físicas por la Universidad Complutense de Madrid, tiene la certificación CPIM (Certified in Production and Inventory Management) otorgada por APICS (American Production and Inventory Control Society). Se incorporó a Accenture en 1990 y ha gestionado a lo largo de su carrera proyectos complejos en grandes entidades, tanto públicas como privadas. Entre otras responsabilidades ha liderado durante los últimos 11 años la relación con la Fábrica Nacional de Moneda y Timbre donde ha participado desde las fases iniciales de definición de CERES, así como en la definición, diseño, implementación, puesta en marcha, comercialización y explotación de sus servicios, que han ido incrementándose a lo largo de los últimos años. Ha sido ponente en numerosos congresos y foros especializados en servicios de certificación y firma electrónica y su aplicación en la mejora de los procesos de negocio.

COMUNIDAD DE MADRID: PROBLEMÁTICA Y ARQUITECTURA DE SEGURIDAD DE EDUCAMADRID

Sinopsis

Con el advenimiento del paradigma Web 2.0, las redes sociales y los portales colaborativos, el profesional de la seguridad TIC se ha encontrado con entornos que promueven valores contrarios a los que tradicionalmente ha manejado para las aplicaciones web en entornos bancarios, industriales o de operadoras. Aunque el planteamiento sigue siendo el mismo, lograr la implantación eficiente de los niveles de seguridad requeridos (o reducción de los niveles de riesgo asumidos), las particularidades que presentan en cuanto a tipo de datos, perfil de usuario e impacto, conforman un escenario novedoso y atractivo para nuestro sector. Tomando como hilo conductor el caso de éxito del Portal Educativo Educamadrid, que da servicio a centenares de miles de usuarios, se expondrá la casuística de este tipo de portales, los retos y particularidades desde el punto de vista de la seguridad de datos y sistemas, las alternativas con que contamos hoy en día para atender estos requerimientos, así como la extrapolación a otros entornos Web 2.0.

Ponentes

• **Felipe Retortillo Franco** es Jefe de la sección de Desarrollo de Nuevas Tecnologías, en la Dirección General de Infraestructuras y Servicios de la Consejería de Educación de la Comunidad de Madrid. Doctor en Psicología de la Educación, ha venido desarrollando su actividad profesional en este ámbito desde hace dos décadas. En 2000, con las transferencias educativas a la Comunidad de Madrid, comenzó a responsabilizarse de la Sección de Desarrollo de Nuevas Tecnologías en la Consejería de Educación. Desde aquí participó en el diseño, desarrollo e implantación de la plataforma Educamadrid. Actualmente afronta los nuevos retos de la integración de este escenario de uso de las tecnologías en los cambios metodológicos y estrategias didácticas de los docentes y en los estilos de aprendizaje de los alumnos.

• **Antonio Requejo Novella** es Gerente de Soluciones Tecnológicas de la Dirección de Desarrollo de Negocio de Grupo Gesfor. Ingeniero de Telecomunicaciones por la UPM y Executive MBA por la Escuela de Negocios IESE, cuenta con varias certificaciones de la ISACA (CISA y CISM). Su trayectoria profesional en el sector de la Seguridad TIC comenzó hace más de 10 años en SGI, pasando posteriormente a Germinus como responsable del equipo de Seguridad. Con la integración de Germinus dentro de Grupo Gesfor, entra a formar parte de la Subdirección de Seguridad de la Dirección de Soporte Tecnológico y Outsourcing.

TERCER MÓDULO 24 de abril

09:15h.	Entrega de Documentación. **Moderador**: **Marcos Gómez Hidalgo**, Subdirector de e-Confianza de INTECO, Instituto Nacional de Tecnologías de la Comunicación.
09:30h.	**Ponencia**: **Banco de España: Plataforma Corporativa de Firma Electrónica e Infraestructura de Certificación asociada**. **Ponentes**: • **Miguel Angel Peña Piñon**. División de Gestión Interna y Seguridad. Departamento de Sistemas de Información. Banco de España. • **Juan Carlos de Miguel Pérez-Herce**, Jefe de Proyectos Sistemas de Seguridad. Indra.
10:10h.	Coloquio.
10:15h.	**Ponencia**: **Plan Estratégico de Prevención del Fraude Electrónico del Grupo BBVA.** **Ponentes**: • **Luis Sáiz Jimeno**, Responsable de Prevención de Delitos Tecnológicos. Grupo BBVA. • **Juan José Míguez Iglesias**, Senior Manager del Área de Seguridad de la Información. PricewaterhouseCoopers.
10:55h.	Coloquio.
11:00h.	Pausa-café. **Moderadora**: **Paloma Llaneza González**, Abogada Socia de Llaneza A+A. Abogados Asociados.
11:30h.	**Ponencia**: **Certificados electrónicos en movilidad.** **Ponente**: **Juan Carlos Yustas Romo**, Responsable de Ingeniería de Seguridad de la Información. Repsol YPF.
12:10h.	Coloquio.
12:15h.	**Ponencia**: **La seguridad en el reglamento de desarrollo de la LOPD**. **Ponente**: **Artemi Rallo Lombarte**, Director de la Agencia Española de Protección de Datos.
12:55h.	Coloquio.
13:00h.	**Debate**: **El impacto de la externalización de la protección TIC en el papel, atribuciones y organización de la función de seguridad en las empresas.** **Moderador**: **Luis Fernández Delgado**, Editor de la revista SIC. **Intervienen**: • **Juan Crespo Sánchez**, Responsable del Centro de Seguridad Lógica. Cuerpo Nacional de Policía. DGP y GC. • **Carlos Escudero Rivas**, Director de Calidad, Auditoría y Seguridad de la Gerencia de Informática de la Seguridad Social. • **Casimiro Juanes Calvo**, Responsable de Seguridad IT. Grupo Ericsson. • **Pedro Pablo López Bernal**, Gerente de Infraestructura de Seguridad, Auditoría y Normalización de Rural Servicios Informáticos. Grupo Caja Rural. • **Tomás Roy Catalá**, Director de Calidad, Seguridad y Relación con Proveedores del Centro de Telecomunicaciones y Tecnologías de la Información (CTTI) de la Generalitat de Cataluña.
14:00h.	Almuerzo. **Moderador**: **José Carrillo Verdún**, Profesor del Departamento LSIS. Facultad de Informática de la Universidad Politécnica de Madrid.
16:00h.	**Ponencia**: **"UCI: *logon* biométrico a aplicaciones mediante un sistema de SSO"**. **Ponentes**: • **José Antonio Borreguero**, Director de Informática de UCI-Unión de Créditos Inmobiliarios. • **Benjamín Crespo Ramos**, Jefe de Producto de Gestión de Identidades. Siemens Enterprise Communications.
16:40h.	Coloquio.
16:45h.	**Ponencia**: **SGSI en la plataforma de pago de la Junta de Andalucía**. **Ponentes**: • **Manuel Narbona Sarria**, Jefe de Gabinete de Sistemas. Servicio de Producción. Dirección General de Sistemas de Información Económico-Financiera. Consejería de Economía y Hacienda. Junta de Andalucía. • **Rafael Castillo García**, Responsable de Consultoría y Gestión de la Seguridad. Delegación Regional Sur. GMV Soluciones Globales Internet.
17:25h.	Coloquio.
17:30h.	Pausa-café.
17:55h.	**Ponencia**: **Ataque y defensa. Perfiles del mañana.** **Ponente**: **Jorge Dávila Muro**, Consultor independiente. Director del Laboratorio de Criptografía LSIIS – Facultad de Informática. Universidad Politécnica de Madrid. UPM.
18:30h.	**Clausura de Securmática 2008.**

BANCO DE ESPAÑA: PLATAFORMA CORPORATIVA DE FIRMA ELECTRÓNICA E INFRAESTRUCTURA DE CERTIFICACIÓN ASOCIADA

Sinopsis

El Banco de España constituyó una Infraestructura de Clave Pública corporativa para que el personal que trabaja en sus instalaciones pueda disponer de certificados electrónicos para el control de acceso a sistemas informáticos, así como para la firma y cifrado electrónico de información. Dicha plataforma también permite validar de modo centralizado los certificados emitidos por Prestadores de Servicios de Certificación, necesidad derivada del intercambio de información electrónica con entidades externas. Una vez cumplido este objetivo, abordó la integración de los servicios de PKI en las aplicaciones corporativas. Con este propósito llevó a cabo la implantación de una arquitectura orientada a servicios ("web services") basada en tecnología de Safelayer. El trabajo ha sido ejecutado por la Unidad de Seguridad Informática del Departamento de Sistemas de Información y Procesos de la entidad, con la colaboración de Indra.

Ponentes

• **Miguel Ángel Peña Piñón** es desde el año 2003 miembro de la Unidad de Seguridad Informática del Departamento de Sistemas de Información y Procesos del Banco de España. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid e Ingeniero Técnico de Telecomunicación por la Universidad de Alcalá, entre sus principales funciones está la gestión y coordinación de proyectos de seguridad TI que realiza el Banco en materia de certificación electrónica, así como la supervisión y explotación de determinadas infraestructuras y sistemas de seguridad ya existentes (PKI, plataforma de firma, sistema de emisión de tarjetas de identificación, etc.). Con anterioridad fue miembro del área de atención a clientes del Departamento CERES de la FNMT-RCM, realizando tareas de consultoría y soporte para los organismos usuarios. Ha participado en proyectos internacionales en materia de firma electrónica.

• **Juan Carlos de Miguel Pérez-Herce** es Gestor de Proyectos en el departamento de Sistemas de Seguridad de Indra. Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid, CISA y CISM por la ISACA, ha desarrollado toda su carrera profesional en Indra y participado en proyectos de muy diversa índole, principalmente dentro del área de seguridad lógica (certificación y firma electrónica, gestión de identidades, consultoría, etc.), para diversos sectores tanto en el ámbito nacional como internacional –administraciones públicas, procesos electorales, sector financiero y seguros...–. En la actualidad complementa sus funciones de desarrollo de negocio con el soporte a operaciones y gestión de proyectos.

PLAN ESTRATÉGICO DE PREVENCIÓN DEL FRAUDE ELECTRÓNICO DEL GRUPO BBVA

Sinopsis

Una vez finalizada la implantación de los proyectos derivados del Plan Director de Seguridad Lógica en las Entidades del Grupo a nivel internacional, el Área de Seguridad Lógica Corporativa se plantea abordar un ambicioso proyecto que surge de un modelo de trabajo forjado en el seno del Área y con el que ha cosechado muy buenos resultados en el pasado. Dado que el fraude está en constante evolución, profesionalización y globalización y tiene cada vez más impacto en las organizaciones, hay que combatirlo de la misma forma, con un planteamiento estructurado y global, tal como se explicará en la ponencia. Este es un trabajo en el que se demuestra que los perfiles técnicos de seguridad combinados con el conocimiento de los procesos de negocio pueden generar un gran valor a las organizaciones, no sólo en términos intangibles y de protección de los activos, sino incluso en términos económicos representando un balance positivo en la cuenta de resultados: reduciendo la cifra del fraude.

Ponentes

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

• **Juan José Míguez Iglesias** es Senior Manager dentro de la Solución de Seguridad de la Información de PricewaterhouseCoopers. Es Ingeniero de Telecomunicación en la especialidad de Telemática y certificado como CISA, CISM y Lead Auditor del ISO 27001. A lo largo de su trayectoria profesional de 11 años en el mundo de la consultoría de seguridad y auditoría informática, ha realizado multitud de trabajos entre los que cabe destacar Planes Directores de Seguridad, Planes de Continuidad de Negocio, Análisis de Riesgos, Auditorías informáticas en grandes compañías del sector financiero y telecomunicaciones e incluso a nivel internacional.

CERTIFICACIÓN ELECTRÓNICA EN MOVILIDAD

Sinopsis

La conferencia versará sobre los nuevos mecanismos de autenticación de usuarios que están valorando las empresas, en concreto la posibilidad de uso de la certificación electrónica en vez de código y contraseña, todo ello particularmente aplicado a los dispositivos móviles –teléfonos, PDA...– que utilizan los ejecutivos. Se repasarán las acciones que hay que revisar en este contexto: certificación de estos dispositivos, posibilidades de gestión, modos de trabajo y limitaciones -en función del estado del arte de la tecnología para poder dar servicio al negocio-, y se enumerarán los retos principales que hay que superar para conseguir una protección óptima, que pueda permitir desde la consulta de correo electrónico a la firma de transacciones corporativas.

Ponente

• **Juan Carlos Yustas Romo** es Responsable de Ingeniería de Seguridad de la Información de Repsol YPF. Licenciado en Ciencias Químicas, posee las certificaciones CISA y CISM por ISACA, y es Lead Auditor de la BS-7799-2 por BSI. Tiene experiencia en áreas de Técnica de Sistemas para grandes sistemas, sistemas medios, microinformática y comunicaciones. Yustas Romo colabora en el desarrollo de normativas, políticas y gestión de áreas de Seguridad Lógica de la información y posee más de 10 años de experiencia en la realización de proyectos de seguridad en ámbitos como la autenticación, el control de accesos, el cifrado de información y la utilización de autoridades de certificación electrónica.

LA SEGURIDAD EN EL REGLAMENTO DE DESARROLLO DE LA LOPD

Ponente

• **Artemi Rallo Lombarte** es Director de la Agencia Española de Protección de Datos. Catedrático de Derecho Constitucional y Director del Departamento de Derecho Público (1993-1998) de la Universidad Jaume I de Castellón, ha llevado a cabo una intensa actividad investigadora en el Instituto Internacional de Derechos Humanos de Estrasburgo, en el Departamento de Teoría del Estado de la Universidad La Sapienza (Roma) y en el Centro de Recherche de Droit Constitutionnel de la Universidad Paris I-Panthèon-Sorbonne. De 2004 a 2008 ocupó el cargo de Director General del Centro de Estudios Jurídicos del Ministerio de Justicia. Rallo Lombarte es autor de numerosas monografías, libros colectivos y artículos científicos en revistas especializadas nacionales e internacionales.

UCI: LOGON BIOMÉTRICO A APLICACIONES MEDIANTE UN SISTEMA DE SSO

Sinopsis

Unión de Créditos Inmobiliarios (UCI) es una multinacional puntera en financiación inmobiliaria que pertenece al Grupo Santander y a BNP Paribas, con más de 1.000 empleados en 79 agencias de España, Portugal y Grecia. En este entorno distribuido, UCI se planteó "securizar" el acceso a los sistemas y aplicaciones que sus empleados utilizan en el trabajo diario, evitando vulnerabilidades como la suplantación de identidad y facilitando al mismo tiempo el proceso de *logon*. Con esta motivación, Siemens Enterprise Communications ha integrado en UCI un sistema de SSO basado en huella digital que permite el acceso a partir de una sola autenticación inicial a la red Windows, aplicaciones a través de Terminal Server, *mainframe* AS400 y aplicaciones web. Dicha integración se ha llevado a cabo en un tiempo de marca, evitando la modificación de las aplicaciones existentes.

Ponentes

• **José Antonio Borreguero** es Director de Informática del Grupo UCI. Ingeniero Informático por la Universidad de Extremadura, ha realizado la mayor parte de su carrera profesional dentro del Grupo UCI, desempeñando varios cargos de dirección en el área de Tecnología y Desarrollo. En 1999 fue nombrado Director de Informática del Grupo UCI, y desde el año 2003 simultanea este cargo con el de Director General de Tramitación Externa, una de las empresas del Grupo. También es miembro fundador y Vicepresidente de Pléyades, Grupo de usuarios de Plex y 2E.

• **Benjamín Crespo Ramos** es Responsable de Producto dentro del área de preventa de Gestión de Identidad de Siemens Enterprise Communications. Ingeniero Técnico de Telecomunicación por la Universidad de Valladolid y Máster en Dirección y Gestión de Seguridad de la Información por la Universidad Pontificia de Salamanca, trabaja en Siemens desde 2000, inicialmente como ingeniero de soporte en redes de transmisión de datos y posteriormente en el ámbito de las soluciones de gestión de identidad, SSO, *smart cards*, PKI y biometría. Actualmente es Responsable de Producto dentro del área de preventa de Gestión de Identidad de Siemens Enterprise Communications.

SGSI EN LA PLATAFORMA DE PAGO DE LA JUNTA DE ANDALUCÍA

Sinopsis

Las organizaciones necesitan alcanzar cierto grado de madurez para aceptar de buen grado las iniciativas tendentes a la planificación, organización y control de los Servicios TI. De no ser así, dichas iniciativas están abocadas al fracaso. Sin embargo, dichos fracasos también forman parte del proceso de madurez. La historia de los éxitos y fracasos en la gestión TI puede ayudar a comprender por qué estamos donde estamos, y en este sentido la seguridad de la información no es una excepción. La primera iniciativa en torno a la seguridad consistió en una foto fija sobre el estado de nuestros sistemas. Ahora entendemos que la seguridad de la información requiere un sistema de gestión, en realidad el mismo que el resto de los procesos.

Ponentes

• **Manuel Narbona Sarria** es Jefe del Gabinete de Sistemas del Servicio de Producción de la Dirección General de Sistemas de Información Económico-Financiera de la Consejería de Economía y Hacienda de la Junta de Andalucía. Licenciado en Física por la Universidad de Sevilla y Máster en Dirección de Sistemas y Tecnologías de la Información y las Comunicaciones por la Universidad Politécnica de Madrid, trabaja en la administración andaluza desde el año 1987 en el área de las TI. Desde 2001 se interesa por la Gestión TI y en 2002 se incorporó al Servicio de Producción con el objetivo de apoyar la producción de Servicios TI de la Consejería desde la perspectiva de la Gestión TI. Ha presentado diversas comunicaciones relacionadas con la Gestión TI en congresos y revistas especializadas.

• **Rafael Castillo García** es el Responsable del Área de Consultoría y Gestión de la Seguridad de la Delegación Regional Sur de GMV desde el año 2001. Ingeniero en Informática por la Universidad de Málaga, es CISA, CISSP y CISM. Dentro de las líneas de Planificación y Auditoría de la Seguridad, ha colaborado en la definición e implantación de varios SGSI en otras organizaciones, así como en GMV Soluciones Globales Internet. Participa activamente como colaborador en medios escritos, diversas tribunas de opinión y otros foros de seguridad lógica.

ATAQUE Y DEFENSA. PERFILES DEL FUTURO

Sinopsis

Siempre es difícil hablar del mañana porque nadie, afortunadamente, tiene el poder de conocer el futuro; sin embargo, el mundo que conocemos es bastante "clásico" y las relaciones de causa y efecto se mantienen. Así pues, podemos imaginar que el futuro a medio plazo ya está insinuado en la realidad actual y en nuestro pasado inmediato. Con la llegada de cada nuevo año, los chamanes de la IT se ponen a elucubrar sobre lo que va a pasar y algunos hablan de una inmediata hecatombe que definitivamente hará cuajar la seguridad de la información, al estilo del Patriot Act y el 11-S. En esta ponencia intentaremos ver con un poco de calma y mesura cuáles pueden ser los ataques a los que nos vamos a enfrentar en los próximos años, y cuáles las defensas que poner en marcha para mitigarlos o incluso rechazarlos. El futuro físico microscópico es algo profundamente insondable, pero los errores humanos, que no sus aciertos, son bastante más previsibles, y los Sistemas de Información son exultantemente humanos.

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

EL IMPACTO DE LA EXTERNALIZACIÓN DE LA PROTECCIÓN TIC EN EL PAPEL, ATRIBUCIONES Y ORGANIZACIÓN DE LA FUNCIÓN DE SEGURIDAD EN LAS EMPRESAS

La oferta de servicios de seguridad TIC está llegando a una fase de madurez en la que la externalización (en sus distintos grados, modalidades y duración) empieza a ocupar un papel significativo en las estrategias corporativas. Y es un hecho que la de la protección es un caso muy particular de externalización, que afecta notoriamente al modelo de organización de la función interna de seguridad, y que además de tener implicaciones relevantes con el cumplimiento de leyes (LOPD y Reglamento, LAECSE, LMISI, LSSI…) y normas sectoriales, es especialmente sensible al incumplimiento de expectativas de eficiencia y calidad. En el debate se pondrá sobre la mesa el presente y el futuro de los profesionales de TIC especializados en seguridad en función, precisamente, del previsible crecimiento de la externalización en los próximos años, y se pulsará la opinión de los participantes sobre si esta previsible tendencia redundará en una mejor calidad de la seguridad en empresas y entidades públicas.

Intervienen:

• **Juan Crespo Sánchez** es Responsable del Centro de Seguridad Lógica y Gestor de PKI del Cuerpo Nacional de Policía. Inspector Jefe del Cuerpo Nacional de Policía, está destinado en Informática desde el año 1986. Crespo Sánchez es Diplomado en Seguridad de la Información por el Instituto Nacional de Administración Pública (INAP/MAP), diplomado en Seguridad de las Tecnologías de la Información y las Comunicaciones por el Centro Criptológico Nacional (CCN/CNI), y dispone del título de Máster en Dirección y Gestión de la Seguridad de la Información de Asimelec y la Universidad Pontificia de Salamanca.

• **Carlos Escudero Rivas** es director del Centro de Calidad, Auditoría y Seguridad de la Gerencia de Informática de la Seguridad Social de la Tesorería General de la Seguridad Social. Es licenciado en Ciencias Físicas y postgrado en informática por la Universidad de Zaragoza y Máster DISTIC por el INAP y la Universidad Politécnica de Madrid. Ha desarrollado su carrera profesional en el ámbito TIC de la Administración Pública. Encuadrado en la estructura de la SGI, ha trabajado en distintos departamentos, incorporándose a su último cargo desde la dirección de Producción y Sistemas.

• **Casimiro Juanes Calvo** es Responsable de Seguridad IT del grupo Ericsson. Ha sido nombrado para dicho puesto en enero de 2008, trasladando su residencia a Estocolmo, Suecia, sede central de la compañía. Ingeniero Técnico Superior de Telecomunicaciones por la Universidad Politécnica de Madrid, Juanes Calvo ha estado ligado toda su carrera profesional, más de diez años, a Ericsson, habiendo ocupado diversos puestos, principalmente en el área de IT y de seguridad, siendo anteriormente el Responsable de Seguridad para la Market Unit Iberia (España y Portugal). Colaborador de SIC y ponente en Securmática, cuenta con la certificación CISSP, y la concentración de gestión de seguridad ISSMP, siendo colaborador de ISC^2 en la preparación de los exámenes.

• **Pedro Pablo López Bernal** es el Gerente de Infraestructura de Seguridad, Auditoría y Normalización de Rural Servicios Informáticos, empresa que presta los servicios de outsourcing global, desde 1986, a las cajas rurales y empresas participadas que forman el Grupo Caja Rural, en total más de 73 entidades financieras y seguros. Técnico Informático con Máster en Auditoría Informática desde 1991, certificado CISA y cursando Máster en Seguridad Global en la Universidad Europea y Belt Ibérica, ha trabajado en los últimos 23 años en los Servicios Informáticos de Empresas tales como Entel, Citibank, Banco Santander y RSI, en las que ha desarrollado diversos puestos y funciones relacionadas con las TIC (Auditoría, Seguridad, Calidad, Procesos, Sistemas y Fraude). Además participa en diversos comités, foros y grupos de trabajo relacionados con Riesgos Laborales, Seguridad y Calidad, internos y externos, y forma parte del Grupo de Seguridad y de la Comisión de Seguridad, Prevención y Fraude de CCI, en representación de la UNACC.

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

> SECURMATICA, a escena

Panorámica de SECURMÁTICA 2007

> Premios SIC 2008

En coincidencia con la celebración de la XIX edición de Securmática, tendrá lugar el acto de entrega de los V 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 cuarta edición de los premios SIC

LA HORA DEL REENCUENTRO Y LOS RECONOCIMIENTOS

> Cena de celebración

SECURMATICA 2008

XIX Congreso español de Seguridad de la Información

AFORO LIMITADO

> Fechas y lugar

SECURMÁTICA 2008 tendrá lugar los días 22, 23 y 24 de abril de 2008 en el hotel NOVOTEL*. Campo de las Naciones de Madrid.

> Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2008 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 V Premios SIC (23 de abril)
- Diploma de asistencia

> Cuota de inscripción

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

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

Descuentos:

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

> Proceso de solicitud de inscripción

- Por fax: +34 91 577 70 47
- Por correo electrónico: info@securmatica.com
- Por sitio web: **www.securmatica.com**

- Por correo convencional: envíe el Boletín adjunto o fotocopia del mismo a:

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

- 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 2008

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 22 ❑ MÓDULO 2 DÍA 23 ❑ MÓDULO 3 DÍA 24 ❑ Deseo inscribirme a SECURMATICA 2008 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**