SECURMATICA 2004

XV Congreso de Seguridad en Tecnologías de Información y Comunicaciones

20, 21 y 22 de abril de 2004
Hotel Novotel. Campo de las Naciones (Madrid)

www.securmatica.com

Organiza:

REVISTA SIC seguridad en informática y comunicaciones

{Programa}

SECURMATICA 2004

XV Congreso de Seguridad en Tecnologías de Información y Comunicaciones

COPATROCINADORES:

ORGANIZA:

Desde 1992 SIC **Seguridad en Informática y Comunicaciones** es la revista española especializada en seguridad de los sistemas de información. Perteneciente a Ediciones CODA, este publicación organiza SECURMÁTICA, el acontecimiento especializado por excelencia de este pujante ramo de las TIC en nuestro país.

SECURMÁTICA SE RESERVA EL DERECHO A MODIFICAR EL CONTENIDO O LOS PONENTES DE ESTE PROGRAMA SI LAS CIRCUNSTANCIAS ASÍ LO REQUIEREN

PRIMER MÓDULO || 20 de abril de 2004

08:45h. Entrega de documentación
09:15h. Inauguración oficial

10:00h. Ponencia: **La certificación de sistemas de gestión de la seguridad de la información: aclaraciones y previsiones**
Ponente: **José Antonio Mañas**, Catedrático de Ingeniería Telemática. ETSI Telecomunicación de la Universidad Politécnica de Madrid
10:40h. **Coloquio**

10:45h. Ponencia: **La certificación en España de productos de seguridad TIC**
Ponente: **Jaime Gotor**, Subdirector General Adjunto del Centro Criptológico Nacional. Centro Nacional de Inteligencia, CNI.
11:20h. **Coloquio**
11:25h. Pausa-café

11:55h. Ponencia: **El ajuste de los ciclos de la calidad, la auditoría y la seguridad**
Ponente: **Carlos Escudero**, Director del Centro de Calidad, Auditoría y Seguridad. Subdirección General de Informática. Tesorería General de la Seguridad Social, TGSS.
12:30h. **Coloquio**

12:35h. Ponencia: **El gobierno de la seguridad en el contexto de una externalización de la función informática: el caso del Banco Guipuzcoano**
Ponente: **Ángel Morán**, Responsable de Seguridad Lógica del Banco Guipuzcoano
13:10h. **Coloquio**

13:15h. Mesa redonda: **Interrelaciones del departamento de seguridad informática con las Direcciones de proyectos TIC**
Intervienen:
Jaime de Pereda, Responsable de Seguridad y Comunicaciones. Sistemas de Información. Grupo Auna.
José Luis Arribas, Responsable de Seguridad de la Información (Business Information Security Officer, BISO). Banca de Consumo para España y Portugal. Citibank.
Juan Carlos Yustas, Seguridad Lógica Corporativa. Repsol-YPF.
14:30h. **Coloquio**
14:35h. Almuerzo

16:35h. Ponencia: **Seguridad en los Juegos Olímpicos de Atenas 2004**
Ponentes: **Teresa Núñez**, Responsable de Consultoría de Seguridad de Negocio en Atos Origin, y **Josep Micolau**, Responsable de Desarrollo de Negocio del Área de Seguridad de Computer Associates
17:15h. **Coloquio**

17:20h. Ponencia: **Conexión remota segura a los sistemas de información de Radio Televisión de Andalucía, RTVA**
Ponentes: **Pedro Montero**, Director del Sistema de Información de RTVA, y **Miguel Hormigo**, Director de la Delegación Sur de Soluciones Globales Internet
18:00h. **Coloquio**
18:05h. Pausa-café

18:20h. Ponencia: **US Transportation Security Agency: un proyecto de seguridad a gran escala**
Ponente: **Ángel Luis López,** Director de Servicios de Infraestructura de Unisys España y Portugal
19:05h. **Coloquio**

19:10h. Fin de la primera jornada

LA CERTIFICACIÓN DE SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: ACLARACIONES Y PREVISIONES

Sinopsis: no se puede ser tan inconsciente como para no prevenir los incidentes y desastres que nos pueden afectar. Pero tampoco se puede ser tan optimista como para creerse uno que, gracias a las contramedidas implantadas, nada malo va a sucederle. En temas de seguridad, sea escalando la cara norte del Eiger o defendiendo nuestra empresa, hay que estar preparado para lo que suceda en cualquier momento. Estar preparado significa prepararse y también tener los músculos listos para reaccionar con eficacia y presteza a lo que se nos venga encima. Eso es un sistema de gestión de la seguridad (SGSI): antes, durante y después.
Los profesores se pasan la vida evaluando estudiantes y, en base a determinar cuánto saben, emitir un juicio sobre su capacidad para desempeñar adecuadamente una cierta tarea o profesión. Un certificado de un SGSI no está tan preocupado en medir lo que sabe la empresa como en calibrar su tono muscular para desempeñar su cometido pese a las sorpresas que depara la vida real. Y esto da mucha fianza a los que trabajan con o bajo dicho SGSI.
Así dicho queda bonito y deseable; pero surgen mil preguntas: ¿se puede calibrar?, ¿qué criterios existen?, ¿quién los evalúa o certifica?, ¿quién evalúa al evaluador?, ¿quién habilita al certificador?, ¿qué credibilidad aporta una certificación? Y, la guinda, ¿cuánta más confianza merecen las empresas certificadas?

Ponente: José Antonio Mañas. Ingeniero de Telecomunicación, Doctor en informática y Catedrático de Ingeniería de Sistemas Telemáticos en la E.T.S.I. Telecomunicación de la Universidad Politécnica de Madrid, Mañas está especializado en redes de comunicaciones (Internet en particular) y seguridad (criptografía y protocolos seguros para comunicaciones y medios de pago). Participó en la creación del servicio de banca por Internet de BCH y Bankinter, en la definición de la arquitectura de sistemas para los Juegos Olímpicos de Salt Lake City, y el análisis de seguridad del canal Internet de Loterías del Estado. Es Miembro del SC27 (seguridad) de ISO y editor de la norma internacional 18014 (fechado electrónico), y ha publicado el libro «Mundo IP. Introducción a los secretos de Internet y las redes de datos».

LA CERTIFICACIÓN EN ESPAÑA DE PRODUCTOS DE SEGURIDAD TIC

Sinopsis: para determinar con rigor el grado de seguridad de productos y sistemas de las Tecnologías de la Información y Comunicaciones (TIC), se requiere realizar diversas actividades de evaluación, certificación, valoración y acreditación. Se da la circunstancia de que estos términos son utilizados en diferentes ámbitos y muchas veces con diferentes significados, lo que puede crear alguna confusión sobre su alcance.
El objetivo de la ponencia es hacer una descripción de la situación de la certificación de productos de seguridad TIC en España y de las actividades asociadas.

Ponente: Jaime Gotor es subdirector general adjunto del Centro Criptológico Nacional del Centro Nacional de Inteligencia, CNI. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid (UPM) e Ingeniero de Armamento y Material con la especialidad de Telecomunicaciones y Electrónica, es también Especialista Criptólogo y Diplomado en Telecomunicación Militar.

EL AJUSTE DE LOS CICLOS DE LA CALIDAD, LA AUDITORÍA Y LA SEGURIDAD

Sinopsis: la Subdirección General de Informática (SGI) de la Tesorería General de la Seguridad Social decidió en la última reestructuración aglutinar las funciones de calidad, auditoría y seguridad. Bajo un enfoque práctico, se realizará un breve repaso sobre la evolución de la seguridad en la organización y cómo queda afectada por este cambio de planteamiento. Se revisará cómo han influido los procesos de calidad y auditoría sobre la visión de la seguridad y qué iniciativas ha desencadenado este cambio de perspectiva.

Ponente: Carlos Escudero, director del Centro de Calidad, Auditoría y Seguridad de la Subdirección General de Informática (SGI) de la Tesorería General de la Seguridad Social. Es licenciado en Ciencias Físicas y postgrado en informática por la Universidad de Zaragoza y master DISTIC por el INAP y la UPM. 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.

EL GOBIERNO DE LA SEGURIDAD EN EL CONTEXTO DE UNA EXTERNALIZACIÓN DE LA FUNCIÓN INFORMÁTICA: EL CASO DEL BANCO GUIPUZCOANO

Sinopsis: el origen del contrato de *outsourcing* de Banco Guipuzcoano con IBM en materia de Seguridad Lógica es el habitual en toda relación de *outsourcing*: centrarnos en nuestros procesos clave dejando la operativa de aquellos otros en manos de especialistas. Pero la externalización de una función no significa desentenderse de ella sino prestarle una atención diferente, más centrada en la gestión y menos en la operativa, que es lo que realmente se externaliza. Externalizar una función –y máxime cuando se trata de una función tan crítica como la seguridad de la información– no supone delegar por completo ese trabajo; simplemente cambia la manera de afrontarlo. De gestionar la función, es decir de los procesos operativos y administrativos, se encargará el proveedor de servicios; de la gestión global, incluyendo aquí el control, y de los procesos de toma de decisiones debe seguir encargándose el cliente, y además debe hacerlo con una actitud decididamente proactiva. Esto ha de realizarse con arreglo a un esquema formal y con ayuda de ciertos mecanismos facilitadores.

Ponente: Ángel Morán es desde septiembre de 2002 responsable de Seguridad Lógica de Banco Guipuzcoano, teniendo a su cargo toda la política de Seguridad de la Información de la entidad. En el propio Banco Guipuzcoano ha desempeñado con anterioridad los cargos de responsable del área de I+D del departamento de eBusiness y fue director general del portal no financiero del Banco ESPIGÓN.COM. Con anterioridad fue Director del Servicio de Información de la consultoría tecnológica Socintec –Corporación IBV– y socio fundador de la consultora I+G Telemática.

MESA REDONDA

INTERRELACIONES DEL DEPARTAMENTO DE SEGURIDAD INFORMÁTICA CON LAS DIRECCIONES DE PROYECTOS TIC

Propósito: de una buena política corporativa de seguridad de la información debe desprenderse la necesidad de implantar un proceso que permita intervenir a los profesionales de la seguridad TIC de una entidad en los ciclos de diseño, despliegue, mantenimiento y revisión de las aplicaciones y los servicios soportados por el sistema de información tecnológico. La existencia de dicho proceso es uno de los factores de buen gobierno que mejor definen la cultura de seguridad de una empresa y el alineamiento de la misma con su negocio o actividad.

Participantes:

Jaime de Pereda, responsable de Seguridad y Comunicaciones de Sistemas de Información de Grupo Auna. Ingeniero Superior de Telecomunicación, comenzó su carrera profesional en el Grupo Universitario de Tarjeta Inteligente, de donde pasó a Telefónica Investigación y Desarrollo. Desde hace más de tres años trabaja en Amena en aspectos relacionados con la seguridad de la información.

José Luis Arribas, responsable de Seguridad de la Información de Citibank España. Curso estudios de Maestría e Ingeniería Técnica Industrial, iniciando su carrera profesional en 1965; en 1970 empieza sus estudios Informáticos y desde 1973 desarrolla su carrera en el entorno bancario nacional e internacional. Desde 1984 trabaja en Citibank participando o dirigiendo proyectos pioneros en España como Banca Electrónica (1984); Metodologías de Desarrollo y Quality Assurance Software (1989), Control Interno Informático (1991), Planes de Continuidad de Negocio (1993) y desde 1995 es el BISO *(Business Information Security Offcier)* para España y Portugal. Es auditor de sistemas de información, Cisa, desde 1996.

Juan Carlos Yustas forma parte del Grupo de Seguridad Lógica Corporativa de Repsol YPF. Inicia sus trabajos en el campo de los Sistemas de Información en la Universidad Complutense, dentro de la informática estadística. Posteriormente se especializa en la técnica de sistemas y comunicaciones del *host* de IBM en la empresa Campsa. A continuación, se le responsabiliza de la creación y desarrollo del Centro de Información y Ofimática. Participa en la consolidación de los Sistemas de Información del Grupo Repsol y comienza a colaborar en los temas de la Seguridad, siendo el responsable de puesta en producción de las nuevas tecnologías colaborando en todos los proyectos de las diversas líneas de negocio, ya en la nueva Repsol YPF. Adicionalmente, en los últimos tres años, pone en marcha y consolida el grupo de Control de Virus y Vulnerabilidades. Complementa su formación en el área de Seguridad en los ámbitos de auditoría de Cisa, el control de seguridad y las auditorías de ISO 17799.

SEGURIDAD EN LOS JUEGOS OLÍMPICOS DE ATENAS 2004

Sinopsis: el grado de expectación asociado a la celebración de unos Juegos Olímpicos le convierte en un evento singular de gran visibilidad, es por tanto el escaparate idóneo donde queda amplificado cualquier éxito o fracaso. Esta circunstancia tiene implicaciones inmediatas en el ámbito de seguridad, tanto física como lógica, por tanto es necesario disponer una Política de Seguridad global que contemple todas las medidas de seguridad, tanto preventivas como de autenticación y control de acceso.

La experiencia acumulada durante más de quince años de la división de Major Events de Atos Origin en la provisión de Sistemas de Información para la organización de eventos deportivos ha derivado en la certeza de que para conseguir el nivel de seguridad efectiva necesario se debe establecer la Infraestructura de Gestión de Seguridad (Security Information Management-SIM) que permita la integración y correlación de las distintas tecnologías y herramientas desplegadas.

La presente conferencia explicará en detalle las motivaciones de tal convencimiento y la estrategia y logros conseguidos en la implementación de eTrust Security Command Center de Computer Associates como Portal de Gestión de Seguridad en Atenas 2004.

Ponentes:

Mª Teresa Núñez es responsable de Consultoría de Seguridad de Negocio en Atos Origin. Ingeniero Superior de Telecomunicaciones por la UPM, desde su incorporación al ámbito de la consultoría en 1990, ha participado en proyectos de Definición e Implantación de Planes y Proyectos de Seguridad de la Información en diversas empresas del sector financiero, telecomunicaciones, editorial, ocio, instituciones públicas y sanitarias, teniendo en cuenta aspectos organizativos, tecnológicos, de adecuación a la legislación vigente y de continuidad del servicio. Es ponente habitual en diversas conferencias y seminarios sobre TI y colabora con publicaciones especializadas. Asimismo, colabora habitualmente en programas de Master de Universidades y Escuelas de Negocio impartiendo los módulos de seguridad. Participa activamente como miembro de ISO/IEC JTC1: CTN 71 /SC27 Information Technology Security Techniques (WG3) Security Evaluation Criteria, y en la Comisión de Seguridad de Sedisi.

Josep Micolau es Licenciado en Matemáticas por la Universidad de Barcelona y CISSP (Certified Information Systems Security Profesional). Su principal función como responsable de Desarrollo de Negocio del Área de Seguridad de Computer Associates es la promoción de las soluciones de seguridad de CA para cubrir todo el ciclo del análisis de las necesidades de los clientes en este ámbito, diseñando y proporcionando la solución más adecuada para cada organización.

Otro de los aspectos importantes de su actividad es la divulgación del amplio catálogo de soluciones tecnológicas de seguridad entre los integradores y *partners* de Computer Associates.

CONEXIÓN REMOTA SEGURA A LOS SISTEMAS DE INFORMACIÓN DE RADIO TELEVISIÓN DE ANDALUCÍA, RTVA

Sinopsis: la necesidad de movilidad y seguridad en los sistemas de información y en las personas que los usan, llevó a los responsables de RTVA a solicitar a Soluciones Globales Internet la integración de una solución global y flexible para permitir un acceso robusto y seguro a sus sistemas de información, independientemente de la ubicación física desde la que se acceda. El nuevo sistema de acceso remoto seguro proporciona nuevas capacidades de acceso a los sistemas de información de RTVA sin perjudicar ni comprometer los actuales métodos de acceso. Adicionalmente, se han tenido en cuenta dos aspectos fundamentales: proporcionar los métodos más robustos de seguridad, por lo que se utilizan *tokens* hardware personalizados, y la integración en una red corporativa que se comparte con el resto de dependencias públicas de la Junta de Andalucía.

Ponentes:

Pedro Montero, director del Sistema de Información de Radio Televisión de Andalucía (RTVA). Licenciado Ciencias Físicas por la Universidad de Granada en 1979. En 1982 se incorpora al departamento de Informática de la Caja de Ahorros de Ronda (hoy Unicaja). En 1986 pasa a Entel (hoy Indra), como analista o jefe de proyecto. Desde 1989 realiza su actividad en la Radio Televisión de Andalucía, donde comenzó en el Departamento de Planificación como jefe de Desarrollo; en 1998 pasa a técnico de Organización durante algo más de un año. Desde 1999 asume las funciones de director del Sistema de Información, puesto desde el que dirige un equipo de 20 técnicos que administran y desarrollan los sistemas de información ligados a la gestión y comunicación del grupo RTVA. Desde aquí se atienden las necesidades de 1.200 usuarios dispersos en los 10 centros de Andalucía y Madrid.

Miguel Hormigo, director de la Delegación Regional Sur de Soluciones Globales Internet. Es Ingeniero Superior de Informática, rama de Inteligencia Artificial por la Universidad de Granada y Auditor Cisa. En febrero de 1992 inicia su carrera profesional en Telefónica Sistemas como jefe de sala del Centro de Control (CECO) de la Exposición Universal de Sevilla'92. Dentro de Telefónica ocupa diferentes puestos como responsable de proyectos. Dentro de Telefónica Sistemas alcanzó en enero 2000 el cargo de coordinador del subárea de Comercio Electrónico en la Delegación Sur hasta septiembre de 2000 cuando asumió su actual puesto de director de la Delegación Regional Sur de Soluciones Globales Internet S.A.

US TRANSPORTATION SECURITY AGENCY: UN PROYECTO DE SEGURIDAD A GRAN ESCALA

Sinopsis: en respuesta a los atentados del 11 de septiembre, el gobierno de EEUU crea la TSA (Transportation Security Agency), cuyo cometido es supervisar la seguridad de los sistemas de transporte aéreo. La TSA contrató en 2002 a Unisys para el desarrollo y construcción de una infraestructura de seguridad en todos los aeropuertos comerciales del país. Actualmente, Unisys coordina un equipo formado por 3.500 de sus empleados y personal de otras 31 empresas, con objeto de proporcionar una infraestructura global de seguridad. El proyecto incluye también servicios de gestión, integración de sistemas y una red a la que podrán conectarse asistentes digitales personales (PDA´s) y radios móviles, así como redes locales o externas y diversos centros de operaciones. En la ponencia se hará un repaso a uno de los proyectos de seguridad más ambiciosos de todos los tiempos.

Ponente: Ángel Luis López, director de Servicios de Infraestructura de Unisys España y Portugal. Desde su cargo como director de la división Global Infraestructure Services (GIS), López es responsable de todos los servicios de consultoría, soporte, gestión y ventas relativos a infraestructuras, así como de la relación directa con los clientes. López pasó a formar parte de Unisys España en 1998, donde desempeñó diferentes cargos, como el de *account manager* del Sector Financiero, o el de director comercial, hasta su cargo actual en Unisys, que ocupa desde 2002. Anteriormente, trabajó en CDI como director gerente y, posteriormente, en SDI y Siemens Redes Corporativas como responsable de Ventas, donde permaneció hasta su incorporación a Unisys España en 1998.

■ SEGUNDO MÓDULO || 21 de abril de 2004

09:15h.	Entrega de documentación
09:30h.	Ponencia: **Proyecto ACCEDE: mejorando la seguridad, facilitando el acceso** Ponente: **Ramón Montes**, Coordinador de Seguridad Informática de Endesa, y **Víctor Mojarrieta**, Director de Seguridad para el Sur de Europa de BMC Software
10:10h.	**Coloquio**
10:15h.	Ponencia: **Apertura y control de arquitecturas tradicionales a nuevos servicios** Ponente: **Julio San José**, Responsable de seguridad host de Bankinter
10:50h.	**Coloquio**
10:55h.	Pausa-café
11:25h.	Ponencia: **Elementos clave de la seguridad en el proyecto CONECTA-PATRIMONIO** Ponentes: **Daniel Avedillo**, Subdirector General de Compras en la Dirección General del Patrimonio del Estado del Ministerio de Hacienda, y **Eduardo Martín Calleja**, Director de Operaciones para la Administración Pública de Steria
12:00h.	**Coloquio**
12:05h.	Ponencia: **Gas Natural: acceso único** **Ponentes: José Luis Checa**, Jefe de Arquitectura de Sistemas y Software de Base. Dirección de Nuevos Sistemas, Tecnología y Comunicaciones. Gas Natural Informática, y **José María Sánchez**, Director de Proyectos y Servicios de SIA
12:40h.	**Coloquio**
12:45h.	Mesa redonda: **Errores y fallos en la concepción y gestión de la seguridad** Intervienen: **Miguel Ángel de Cara**, Jefe de Proyectos. Área de Seguridad de Davinci; **Ramón Ynat**, Director de Consultoría de ESA *Security*; **Luis Rodríguez**, Director Técnico de Innova; **José Manuel Garayoa**, responsable de Desarrollo de Negocio de Iron Mountain Off-Site Data Protection España**; Jesús Rodríguez**, Director General de Realsec**; Carolina de Oro**, Jefe de Producto y Coordinadora del Grupo de Seguridad de Siemens; **Xabier Mitxelena**, Director Gerente de S21sec; **Carlos Moliner**, Responsable de Consultoría de Gestión de Seguridad de Telindus
14:00h.	**Coloquio**
14:15h.	Almuerzo
16:15h.	Ponencia: **Junta de Comunidades de Castilla La Mancha: 'securización' de los tráficos en la capa perimetral** Ponentes: **Pedro Jesús Rodríguez González**, Jefe de Servicio de Internet. Consejería de Ciencia y Tecnología. Junta de Comunidades de Castilla La Mancha, y **Alberto Torralba**, Technical Account Manager de Trend Micro
16:50h.	**Coloquio**
16:55h.	Ponencia: **Orden Hospitalaria de San Juan de Dios: tres tecnologías de seguridad en una, al servicio de la salud** Ponentes: **Josefina Vidal**, Directora de Informática. Orden Hospitalaria de San Juan de Dios, y **Joaquín Reixa**, Director General de Symantec Ibérica
17:30h.	**Coloquio**
17:35h.	Pausa-café
17:55h.	Mesa redonda: **La redefinición del papel de las herramientas en las arquitecturas de protección modernas** Intervienen: **Camilo Vaquero**, Director de Estrategia y Desarrollo de Negocio de Aladdin; **Javier Carreras**, Responsable de Desarrollo de Negocio de Crossbeam Systems; **Manuel Arrevola**, Director de Internet Security Systems Ibérica; **Federico de la Mora**, Responsable para España de RSA Security; **Alberto Arbizu**, Responsable para Iberia de Secure Computing; **Javier López-Tello**, Director General de Sentryware; **Vesku Turtia**, Consejero Delegado de Stonesoft**; Jacobo Crespo**, Responsable para Iberia de Sybari Software
19:15h.	**Coloquio**
19:20h.	Fin de la segunda jornada
20:30h.	**Cena de la XV Edición de Securmática y entrega de Premios SIC**

■ || PROYECTO ACCEDE: MEJORANDO LA SEGURIDAD, FACILITANDO EL ACCESO

Sinopsis: alcanzar el equilibrio entre las necesidades de nuestros usuarios finales y las políticas corporativas de seguridad, entre la inversión necesaria y la contribución esperada del proyecto: esto es lo que, en definitiva, trata de mostrarse en la ponencia sobre el proyecto Accede, centrado en que el usuario final acceda con facilidad y seguridad máxima a las aplicaciones que, según roles y reglas de negocio, necesite para realizar su trabajo. Para llevarlo adelante, Endesa ha elegido la experiencia y el enfoque de la solución Irene, del integrador SIA, que descansa a su vez sobre la familia de productos Control-SA de BMC Software.

Ponentes:

Ramón Montes ha cursado estudios de Ingeniería Superior en la Universidad Politécnica de Barcelona. En 1974 ingresó en la Escuela de Aprendices de Fecsa, y en 1976 pasó a la Dirección de Sistemas de Información de esta empresa, en la que prestó sus servicios como Operador de Sistemas y como responsable de Explotación. En 1998 y hasta enero de 2000, dirigió el proyecto de Adaptación al Año 2000 de la infraestructura tecnológica de Endesa. Posteriormente, y ya en esta compañía, fue responsable de la creación de la función de Seguridad Informática con el cargo de coordinador de Seguridad Informática, que ocupa en la actualidad. En el año 2001, diseñó el Plan Director de Seguridad Informática 2002-2005 de Endesa, actualmente en fase de desarrollo e implantación.

Víctor Mojarrieta es director para la región sur de Europa del área de seguridad de BMC Software. Se unió a la plantilla de BMC Software en 1996, en calidad de director de Marketing y Canales para Iberia. Con anterioridad trabajó en Digital Equipment Corporation. Mojarrieta es licenciado en CC. Matemáticas por la Universidad Autónoma de Madrid y posee un MBA por el Instituto de Empresa de Madrid.

■ || APERTURA Y CONTROL DE ARQUITECTURAS TRADICIONALES A NUEVOS SERVICIOS

Sinopsis: los grandes ordenadores centrales (*mainframes*), llevan con nosotros varias décadas, forman parte de nuestras infraestructuras 'criticas' y casi siempre almacenan el 'corazón' de nuestros negocios. Para muchos son algo obsoleto y misterioso que debería ser sustituido, ¿debe ser asi? Su apertura a nuevos servicios no debe ser realizada de cualquier forma, ¿a que problemas debemos enfrentarnos?, ¿está la tecnología preparada? ¿Y las personas? En otras palabras, no es un camino fácil, pero es realizable.

Además y dada la actual tendencia de las grandes empresas a la 'externalización' de los servicios de explotación y técnica de sistemas en los mainframes, se nos abren múltiples nuevos frentes para aquellos encargados de 'vigilar' la seguridad. Las preguntas son muchas, pero las principales debieran ser: ¿cómo verificar si se mantienen los niveles de seguridad adecuados?, ¿se están cumpliendo las normas establecidas?

Ponente: Julio San José. Actualmente es el responsable de Seguridad Host en el área de Seguridad Informática de Bankinter. Desde su incorporación en 1997, ha desempeñado varios puestos: responsable de Seguridad de Aplicaciones y Responsable Técnico de Seguridad Informática. Es CISM. Antes de su incorporación a Bankinter, trabajó como oficial de Seguridad Visa/MasterCard en Sistema 4B, responsabilizándose de la gestión de claves criptográficas, custodia y vigilancia electrónica de dispositivos criptográficos. Durante esta etapa colaboró en el diseño de módulos de seguridad para los terminales de pago electrónico. Es coordinador de subgrupo 2 (Criptografía) del Subcomité de Seguridad de las TI (CTN 71 / SC27), habiendo colaborado en la redacción de varias normativas, tanto nacionales como internacionales. Así mismo es co-autor del libro «Seguridad de las tecnologías de la información. La construcción de la confianza para una sociedad conectada», editado por Aenor.

ELEMENTOS CLAVE DE LA SEGURIDAD EN EL PROYECTO CONECTA-PATRIMONIO

Sinopsis: el Ministerio de Hacienda ha desarrollado proyectos importantes basados en técnicas informáticas. Es el caso de la Agencia Tributaria. La compra electrónica se ha hecho un 'hueco' en nuestros hábitos. La AGE impulsa la transformación de los procesos administrativos para dar paso a la e-Administración. La Dirección General de Patrimonio dispone de un servicio de compras Centralizadas de Bienes y Servicios que opera desde 1968. Están suscritas más de 2.000 instituciones. Actúa con alrededor de 350 empresas que, presentan en conjunto, unos 70.000 artículos, agrupados en 15 catálogos como los de mobiliario de oficina, vehículos, ordenadores, material sanitario, fotocopiadoras, software, servicios profesionales, etc.
El proyecto CONECTA-Patrimonio, pasa de un sistema basado en la informática tradicional sustentado en la evidencia documental en papel, a un nuevo sistema que se apoya en Internet, sin mermar en modo alguno la confianza de los actores y las garantías jurídicas en todas las fases del proceso y al mismo tiempo ganando en rapidez y flexibilidad. Son de destacar en el contexto, el uso de certificados digitales para la firma electrónica avanzada y reconocida, la base de datos de licitadores que recoge los atributos (capacidad de representación) de sus poderes, el sobre seguro que permite el envío de documentación 'emulando' el sobre lacrado que se abre en acto público en un momento determinado, la firma colegiada de la mesa de contratación, el depósito de originales electrónicos, y la seguridad física adicional mediante el establecimiento del entorno Extranet y del Internet, sólo acoplados mediante mensajes de intercambio.

Ponentes:

Daniel J. Avedillo, subdirector general de Compras en la Dirección General del Patrimonio del Estado del Ministerio de Hacienda. Licenciado en Matemáticas, pertenece al Cuerpo Superior de Administradores Civiles del Estado y al Cuerpo Superior de Sistemas y Tecnologías de la Información, dispone del Master en Gestión de la Administración Pública en el Instituto Nacional de Administración Pública y del Master en Sistemas y Tecnologías de la Información del Consejo Superior de Informática. A lo largo de su trayectoria en la Administración Pública, ha desempeñado diferentes puestos en los Ministerios de Educación y Ciencia, Cultura y Economía y Hacienda. Ha desarrollado, así mismo, una intensa actividad como ponente y profesor en cursos, seminarios, conferencias, etc., en temas relacionados con la Administración Pública y las Tecnologías de la Información.

Eduardo Martín Calleja, director de operaciones para la Administración Pública de Steria. Licenciado en Matemáticas, ha ocupado distintos puestos de responsabilidad en Steria y en particular ha trabajado varios años como Consultor de Seguridad experto en infraestructuras de certificación y firma electrónica (PKI), y en políticas y planes de seguridad.

GAS NATURAL: ACCESO ÚNICO

Sinopsis: el objetivo es dar visibilidad de la aproximación planteada por Gas Natural a la problemática del acceso único a las aplicaciones de uso global en el Grupo Gas Natural. En los pasados años, la diversificación de actividades y funciones en toda gran compañía y más aún, si cabe, en el sector *Utilities*, el cual se ha sometido a un proceso de liberalización y desregulación del mercado, ha generado la proliferación de entornos de aplicación que pretenden dar cobertura a las diferentes funciones de negocio y las de soporte del mismo. Desde el planteamiento de aplicación de negocio monolítica con el soporte de unos pocos aplicativos satélites que gestionan los entornos de soporte al negocio, se ha pasado a un entorno de aplicaciones disperso en base a las diferentes actividades y productos ofrecidos, sobre entornos totalmente heterogéneos que aportan funciones de CRM, ERM, facturación, portales, etc. Dicha diversificación de sistemas, en conjunción con el concepto de aplicativo orientado al Portal del Empleado, permite concebir un entorno de validación única de acceso, el cual va a permitir la interacción del usuario con los diferentes entornos y entre dichos entornos entre sí. La anterior estrategia se basará en la existencia de un punto único de acceso, el cual va a permitir canalizar la totalidad de necesidades de los empleados en todos los ámbitos de relación con la compañía.

Ponentes:

José Luis Checa, jefe de Arquitectura de Sistemas y Software de Base de Gas Natural. Ingeniero Técnico Industrial por la UPC, cuenta con 18 años de experiencia en el sector informático en diversas áreas, once de ellos en Digital Equipment Corporation. Ha sido responsable de proyectos de diseño e implementación de infraestructuras para Gas Natural, tan significativos como el despliegue de la 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 infraestrucuras SAP, Siebel, Gestión Documental, Output Management, EAI, Portales y Datawarehouse, y el Plan Director de Seguridad y entorno de acceso con *logon* único (SSO).

José María Sánchez, director del Área de Proyectos y Servicios del Grupo SIA. Licenciado en la Escuela Técnica Superior de Ingenieros de Telecomunicación (ETSI) por la Universidad Politécnica de Madrid, con anterioridad a su actual puesto, desempeñó el cargo de responsable técnico del Área e-Security del Grupo SIA durante un periodo de cuatro años, liderando la creación y desarrollo de la misma y ejecutando proyectos de reconocido prestigio a escala nacional e internacional. Anteriormente, su trayectoria profesional se desarrolló en Dinsa como gerente de proyectos.

MESA REDONDA

ERRORES Y FALLOS EN LA CONCEPCIÓN Y GESTIÓN DE LA SEGURIDAD

Propósito: no es desdeñable la experiencia adquirida en estos años por las compañías que ofrecen servicios especializados en seguridad de la información y seguridad TIC. Y aunque tradicionalmente se dice en los ámbitos de mercado que "El cliente siempre tiene la razón", es evidente que no siempre ha de ser así. Se trata, por tanto, de aprovechar esa experiencia del ramo de oferta para intentar conocer si se detectan en el ramo comprador –y no necesariamente por motivos de limitaciones presupuestarias–, errores y fallos de concepción en el planeamiento y la gestión de los riesgos de seguridad TIC.

Participantes:

Miguel Ángel de Cara es responsable de Proyectos en la unidad de negocio de e-security en daVinci. Ingeniero en Informática por la UPC, ha desarrollado su carrera profesional en diversas áreas de las nuevas tecnologías dentro de daVinci y Grupo ADD, haciendo especial énfasis en proyectos de seguridad de la información. Actualmente trabaja en la implantación de distintos proyectos como planes de seguridad, auditorías, consultorías e implantaciones de soluciones de seguridad haciendo especial énfasis en el estándar ISO 17799.

Ramón Ynat es director de Consultoría de ESA *Security*. Auditor CISA y director de Proyectos, es asimismo coordinador por parte de su compañía del Proyecto denominado "I Programa Sectorial de Seguridad de Servicios de la Sociedad de la Información", impulsado por Anei (Asociación Nacional de Empresas de Internet) y Aenor para verificar si las empresas candidatas a la obtención de la Certificación UNE 71502 correspondiente a la Norma Internacional ISO/IEC 17799 cumplen con lo dispuesto en dicha Norma. Igualmente, es miembro de Aenor CTN 178 Ciudades Digitales. Con anterioridad, Ynat ha sido director de Sistemas en 1 a 1 Marketing Relacional y responsable de Informática en Cadmo Conocimiento.

Luis Rodríguez Berzosa, director técnico de Innova Information Systems. Es Licenciado en Físicas y Matemáticas por la Universidad Complutense de Madrid. Ha desempeñado su actividad profesional como consultor técnico y de seguridad TIC en empresas como DyM, Platinum, Ideal Objects, Teknoland o Nakua Technologies.

... MESA REDONDA

José Manuel Garayoa, responsable de Desarrollo de Negocio de Iron Mountain Off-Site Data Protection España. Licenciado en Ciencias Empresariales por la Universidad Complutense de Madrid, ha desarrollado su carrera en el ámbito Comercial, desempeñando distintas funciones de responsabilidad sobre las ventas de diversas empresas multinacionales de servicios. Desde el año 2001, es responsable de la generación y desarrollo de nuevo negocio de Iron Mountain Off-Site Data Protection, división de Iron Mountain especializada en gestión y custodia *off-site* de Cintotecas.

Jesús Rodríguez Cabrero, director general y socio fundador de Realsec. Cuenta con una dilatada experiencia en el sector informático y de la seguridad. En su trayectoria profesional ha desempeñado diversos cargos en Bull, G.I.S.A., T.PI. y Macro-4 España. En 1993 fundó la empresa Quark Software & Services –pionera en el ámbito de auditorías y análisis de vulnerabilidades–, que se fusionó en 1999 con el Grupo Netfinger.

Carolina de Oro, jefe de producto y coordinadora de la unidad de negocio de Seguridad de Siemens. Realizó sus estudios de Ingeniería Superior de Telecomunicación en la Universidad Politécnica de Madrid y formación de postgrado en Administración de Empresas por la Universidad de Alcalá de Henares. Instructora habitual de diversos cursos relacionados con la seguridad lógica, posee amplia experiencia en proyectos de alto valor añadido en el campo TI: gestión de la seguridad de la información, PKI, directorios. Ha participado como ponente en las jornadas Red Iris y ha escrito artículos para publicaciones como Global Communications y SIC.

Xabier Mitxelena, director gerente de S21Sec y consejero delegado y socio fundador del Grupo S21Sec Gestión, S.A. Ingeniero industrial de Organización por la Universidad de Navarra, Mitxelena es asimismo MBA por la Universidad de Deusto. Ha trabajado con anterioridad en Sayma Consultores, Bull España y ATE Informática.

Carlos Moliner, responsable de Consultoría de Gestión de Seguridad de Telindus desde el año 2000. Es Ingeniero Superior de Informática por la Universidad Antonio de Nebrija de Madrid. Cuenta con una amplia experiencia en la consultoría, diseño y desarrollo de infraestructuras complejas de seguridad y gestión en grandes organizaciones. Anteriormente desarrolló su actividad como responsable de Sistemas y Seguridad en la Universidad Antonio de Nebrija, compaginándola con actividades docentes en el mismo centro.

JUNTA DE COMUNIDADES DE CASTILLA LA MANCHA: 'SECURIZACIÓN' DE LOS TRÁFICOS EN LA CAPA PERIMETRAL

Sinopsis: la Junta de Comunidades de Castilla La Mancha está abordando un programa de implantación de políticas de seguridad TIC en todos los frentes: certificación y firma electrónica, infraestructuras PKI/PMI, adaptación a la LOPD... En la ponencia se tratará específicamente la iniciativa centrada en la infraestructura de protección perimetral antivirus, anti-*spam* y de control de contenidos desplegada, basada en la tecnología de Trend Micro. Dicha solución incluye protección de los protocolos smtp, http y ftp, y en el filtrado web se utiliza Icap.

Ponentes:

Pedro Jesús Rodríguez González, Jefe de Servicio de Internet en la Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla La Mancha. Es funcionario desde 1992 del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Junta de Comunidades de Castilla-La Mancha, donde presta sus servicios como Jefe de Servicio de Internet de la Consejería de Ciencia y Tecnología desde septiembre de 2000. Licenciado en Derecho por la Universidad de Castilla-La Mancha, donde también ha realizado cursos de especialización en Seguridad en Tecnologías de Información y Comunicaciones y especialización en Redes y Servicios de Comunicaciones.

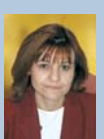
Alberto Torralba. Ingeniero Técnico de Telecomunicaciones por la Universidad Politecnica de Valladolid. Tiene más de cinco años de experiencia como administrador de seguridad y comunicaciones en empresas como NEO y Future Space, entre otras. En Future Space también trabajó con el Grupo de Seguridad de Telefónica Investigación y Desarrollo. Actualmente, y en tanto que Technical Account Manager de Trend Micro, realiza labores de diseño e implantación de soluciones de seguridad de contenidos sobre múltiples plataformas y entornos.

ORDEN HOSPITALARIA DE SAN JUAN DE DIOS: TRES TECNOLOGÍAS DE SEGURIDAD EN UNA, AL SERVICIO DE LA SALUD

Sinopsis: la Orden Hospitalaria San Juan de Dios necesitaba dotarse de una comunicación robusta y segura entre los once centros que componen su red de centros hospitalarios. Dispersos geográficamente, los once centros cuentan con redes de diferentes tamaños, entre 10 y 200 nodos. Dada la singularidad de la información tratada (en ocasiones de carácter sensible y con datos personales de nivel alto) así como el necesario pero delicado tránsito de la misma entre las distintas ubicaciones, los aspectos relativos a la confidencialidad cobraron gran relevancia. Cada centro conectaba por VPN con la central, y necesitaba prioritariamente asegurar en el *gateway* este tráfico de información crítica. Se ha optado por la tecnología proporcionada por Symantec, concretamente Symantec Gateway Security con funcionalidades antivirus, cortafuegos y de red privada virtual.

Ponentes:

Josefina Vidal es directora del Área de Informática de la Orden Hospitalaria de San Juan de Dios de Castilla. Diplomada por la Universidad Complutense de Madrid, ha realizado numerosos cursos de formación en sistemas informáticos y de gestión y cuenta con 14 años de experiencia en Servicios de Informática, desarrollando tareas en diferentes ámbitos de Sistemas de Gestión Sanitaria (análisis y desarrollo de sistemas de información). Desde el año 2000 es Responsable de Tecnologías de la Información de los 14 Centros de la Orden entre Hospitales Generales, Hospitales Psiquiátricos, Centros de Acción Social, Albergue y Servicios Centrales. Actualmente dentro de sus responsabilidades se encuentra el liderazgo en el desarrollo e implantación del Proyecto de los Sistemas de Seguridad Informática de la Orden Hospitalaria San Juan de Dios de Castilla.



Joaquín Reixa, director general de Symantec Ibérica. Ingeniero de Telecomunicaciones y Master Business Administration; se incorporó a Symantec en 2000 para dirigir el establecimiento de la compañía en España. Anteriormente trabajó para Lotus Development, donde fue responsable de la dirección comercial en España; asimismo, desempeñó varias funciones en Fisher Rosemount, donde empezó como ingeniero del servicio de soporte técnico, más tarde pasó a ser especialista de proyectos de control de sistemas, acabando como responsable de proyectos de ventas y distribución. Reixa también trabajó para Foxboro Control como director del departamento de sistemas.

MESA REDONDA

LA REDEFINICIÓN DEL PAPEL DE LAS HERRAMIENTAS EN LAS ARQUITECTURAS DE PROTECCIÓN MODERNAS

Propósito: muchos usuarios consideran que las herramientas tecnológicas de seguridad (defensa frente a código malicioso, cortafuegos, IDS, IPS, control de contenidos, anti-*spam*...) son parches inevitables en su sistema de información. Para mayor confusión, estas herramientas, que inicialmente nacieron con propósitos muy específicos, tienden a fundirse para proporcionar un servicio de seguridad más global. Este hecho se observa hoy de forma notoria en las políticas de adquisiciones y en las políticas de oferta de los grandes fabricantes especializados. ¿A dónde nos lleva esta tendencia? ¿Es un camino correcto para ofrecer mejores productos/servicios al usuario profesional?

... MESA REDONDA

Participantes:

Camilo Vaquero es Ingeniero en Informática por la Universidad Politécnica de Madrid. Comenzó su carrera profesional en el Ministerio de Educación y Ciencia en 1989 como analista de sistemas. Continuó su trayectoria en Unisys como consultor de redes de área local y extensa, interconexión de sistemas heterogéneos y Project Management. En 1995 se incorporó a Fast Ibérica como product manager de Sistemas de Protección de Software. En 2000 nace Aladdin España donde Vaquero define el canal de distribución y promociona los productos de la gama e-Business. Actualmente ocupa el puesto de director de Estrategia y Desarrollo de Negocio en la citada organización.

Javier Carreras es responsable de desarrollo de negocio de Crossbeam Systems para España, Portugal y Latinoamérica. Con anterioridad ha desarrollado su labor profesional en compañías como Netscape, donde fue director regional para España, Portugal y Latino América, iPlanet con el mismo cargo; en AOL fue vicepresidente para Iberoamérica; conjuntamente con Afina lanzó la compañía Redsec.net, primera empresa española dedicada en exclusiva a MSSP (servicios gestionados de seguridad).

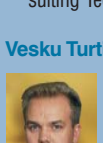
Manuel Arrevola, director de Internet Securirty Systems Ibérica. Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid, Arrevola inició su carrera profesional en Fundesco, como administrador de sistemas Unix. Desde 1995 hasta abril de 2000 llevó a cabo su labor profesional en BMC Software, desempeñando diferentes funciones. También ha trabajado en Professional Training, como instructor, y en Compuware, como consultor de preventa.

Federico de la Mora es responsable de RSA Security España y Portugal. Ha trabajado con tecnologías de seguridad de información durante más de una década. Inició su carrera en uno de los bancos más grandes de Latinoamérica, ahora propiedad de Citibank, liderando la introducción de políticas y soluciones de seguridad en sistemas abiertos. También ocupó puestos de responsabilidad de preventa y de desarrollo de negocio en Verizon y en Novell. De la Mora tiene publicados varios artículos referentes a políticas de seguridad, *scanners* y cortafuegos.

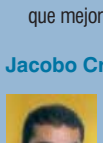
Alberto Arbizu, director para Iberia de Secure Computing. Licenciado en Ciencias Empresariales por la UNED y MBA por el Instituto de Empresa, con anterioridad a su actual cargo en la multinacional norteamericana ha ocupado puestos de responsabilidad en diversas organizaciones: director comercial de OKI Systems Ibérica, director de canal Iberia de Enterasys Networks y director para Iberia de BlueCoat Systems.

Javier López-Tello, director general de Sentryware. Licenciado en CCEE y MBA por ESEUNE es socio fundador de la compañía. Tiene más de 16 años de experiencia en el Sector de TI, desempeñando puestos de responsabilidad en las areas de marketing y ventas. Durante los últimos años ha trabajado en Tecnologías de Seguridad lanzando al mercado productos punteros en la protección perimetral. Perteneció al equipo de alta dirección del Grupo ADD, donde dirigió el negocio y expansión de ADD Distribuciones, mayorista de valor añadido especializado en soluciones *e-business* y seguridad, y daVinci Consulting Tecnológico, integrador especializado en las mismas áreas.

Vesku Turtia es el consejero delegado de Stonesoft Ibérica desde la apertura, en el año 2000, de la filial en España de esta compañía finlandesa. Hasta su incorporación fue director comercial en diferentes empresas, entre las que destacan Kemira Ibérica, Renco SA y Kymmene Ltd., ubicada en Singapur. Turtia ha convertido a Stonesoft en uno de los principales y más reconocidos proveedores de soluciones de seguridad de nuestro país y ha situado a su solución cortafuegos y VPN StoneGate entre las que mejor aceptación está teniendo en el mercado dentro de su categoría.



Jacobo Crespo, director general para Iberia de Sybari Software. Master Profesional en Ingeniería Informática y Comunicaciones, impartido por el Centro de Estudios Profesionales San Pablo CEU y la Facultad de Informática de la UPM, y Master en Dirección de Marketing y Gestión comercial en la Escuela Superior de Gestión Comercial y Marketing ESIC. Inició su carrera profesional en 1995 en Depeltronic (España). Posteriormente trabajó en la firma británica Devon Computers, en ESRI-España Geosistemas y en Askin.



■ TERCER MÓDULO || 22 de abril de 2004

09:15h. Entrega de documentación

09:30h. Ponencia: **Iberdrola-IBM: proyecto de detección de intrusiones a nivel corporativo**
Ponentes: **Fernando Javier Díez Gutiérrez**, Responsable de Seguridad de Sistemas Distribuidos. Departamento de Seguridad de la Información y las Comunicaciones de Iberdrola, y **Moisés Navarro**, Responsable de la práctica de seguridad para el Sur de Europa. IBM.

10:10h. **Coloquio**

10:15h. Ponencia: **Telefónica Móviles España: seguridad proactiva en el puesto de trabajo**
Ponentes: **Enrique Sánchez Hilara**, Director de División de Explotación y Seguridad de Sistemas de Telefónica Móviles España, y **Carlos Jiménez**, Presidente de Secuware

10:55h. **Coloquio**

11:00h. Pausa-café

11:30h. Ponencia: **La seguridad informática en el Plan Estratégico de Sistemas 2004-2006 de Correos**
Ponentes: **Rubén Muñoz**, Director de Tecnología y Sistemas de Correos, y **Jesús Mayor**, Jefe del Área de Seguridad Informática de Correos

12:10h. **Coloquio**

12:15h. Ponencia: **La plataforma tecnológica de la Agencia Notarial de Certificación, ANCERT**
Ponentes: **Marek Szymanski**, Director General de la Agencia Notarial de Certificación, ANCERT, y **Luis Jara**, e-Security Manager de gedas iberia

12:55h. **Coloquio**

13:00h. Ponencia: **Renovación de la infraestructura tecnológica de Ceres-FNMT, un proyecto emblemático de integración en un entorno multitecnología**
Ponentes: **Francisco Jerez**, Jefe de Servicio del Área Técnica de Ceres-FNMT, y **Ascensio Chazarra**, Gestor de Proyectos de Certificación y Firma Electrónica. Indra.

13:40h. **Coloquio**

13:45h. Almuerzo

15:45h. Sesión: **Estafas (suplantación –*phishing*-, engaños y manipulaciones) y chantajes a organizaciones**
Ponentes: **María Nieves Gamoneda**, Inspector Jefe de la Brigada de Investigación Tecnológica. UDEV Central. Comisaría General de la Policía Judicial. Cuerpo Nacional de Policía, y **Juan Salom**, Jefe del Grupo de Delitos Telemáticos de la Unidad Central Operativa de Policía Judicial de la Guardia Civil.

16:25h. **Coloquio**

16:30h. Ponencia: **Requisitos y mecanismos de seguridad en la red corporativa de Microsoft**
Ponentes: **Carlos Lacuna**, Director de IT para España y Portugal de Microsoft, y **Jesús Rodríguez**, Ingeniero de Sistemas. Área de Soluciones Tecnológicas e Infraestructura. División de Grandes Cuentas y Partners de Microsoft.

17:10h. **Coloquio**

17:15h. Pausa-café

17:35h. Ponencia: **Buenas Prácticas de Seguridad en redes de almacenamiento**
Ponente: **Antonio Requejo**, Director de la División de Seguridad de Germinus, y **Javier Zamorano**, Director de la División de Infraestructuras de Red de Germinus

18:15h. **Coloquio**

18:20h. Ponencia: **Seguridad inalámbrica: nuevas tecnologías, ¿viejos retos?**
Ponente: **Miguel Ángel Monjas,** Área de User Security y SSO. Departamento de Ingeniería de Sistemas. Ericsson España

19:00h. **Coloquio**

19:05h. Fin de la tercera jornada

Clausura de Securmática 2004

IBERDROLA-IBM: PROYECTO DE DETECCIÓN DE INTRUSIONES A NIVEL CORPORATIVO

Sinopsis: la presentación cubre la descripción de un proyecto altamente relevante dentro de la estrategia de Seguridad Corporativa de Iberdrola, como parte de una iniciativa orientada a establecer una Gestión de Riesgos de Seguridad a nivel corporativo. De manera adicional a la descripción de cómo fue concebido el proyecto (objetivos, fases, etc.) –comprobándose la bondad de seguir un proceso estructurado para cualquier despliegue de seguridad–, también se contemplará dentro de la presentación cuáles fueron los resultados y conclusiones principales (aspectos organizativos, técnicos y de gestión, y arquitectura tecnológica según casuísticas), así como las lecciones aprendidas tras la ejecución de la iniciativa.

Ponentes:

Fernando Javier Díez Gutiérrez, responsable de Seguridad de Sistemas Distribuidos en el departamento de Seguridad de la Información y las Comunicaciones de Iberdrola desde el año 2002. Es Diplomado en Informática por la Universidad Politécnica de Madrid (1987). Inició su vida laboral en 1987 y 1988 en C.E.N.E.I. y la Comunidad de Madrid en la Unidad de Formación e Investigación, desarrollando programas de aprendizaje. Desde 1989 hasta 1996 trabajó en UITESA (Unión Iberoamericana de Tecnología Eléctrica) como técnico de Redes y Sistemas. Desde 1997 hasta 2001 trabajó como system manager en el área de Sistemas de Información de Iberdrola Ingeniería y Consultoría, siendo responsable de las unidades de Arquitectura Tecnológica, Internet y Sistemas Centrales.

Moisés Navarro, responsable de la Práctica de Seguridad para el Sur de Europa de IBM. Licenciado en Informática por la UPM, Navarro dispone de más de ocho años de experiencia en el área de seguridad de la información, desde la que ha participado y dirigido proyectos globales y corporativos de seguridad para organizaciones de múltiples sectores industriales. Durante 2001 y 2002 fue responsable de los Servicios de Consultoría de Seguridad de IBM Global Services.

TELEFÓNICA MÓVILES ESPAÑA: SEGURIDAD PROACTIVA EN EL PUESTO DE TRABAJO

Sinopsis: La protección de los recursos corporativos y la información es una misión difícil, ya que minimizar correctamente los riesgos a los que están expuestos los sistemas de información en explotación pasa forzosamente por controlar la forma en que están siendo accedidos desde los puestos de trabajo. Es en los puestos, donde los usuarios se pueden convertir voluntaria o involuntariamente en el punto de fallo del sistema. Telefónica Móviles España (TME) ha pensado en la protección corporativa del puesto de trabajo desde un enfoque proactivo que le lleve a controlar sus sistemas. El proyecto de referencia permite identificar al usuario antes del arranque del sistema, asegurando la confidencialidad de la información y autorizando la ejecución de aplicaciones adecuadas a cada usuario, de modo que la plataforma corporativa de TME cumpla estrictamente con el plan de seguridad definido desde Telefónica.

En la presentación, se aportará además una visión sobre los riesgos que el proyecto de TME es capaz de minimizar, tomándolo como caso de estudio de la robustez de SSF de Secuware, hasta la fecha el único sistema de protección corporativa basado en «perímetro de usuario» del mercado.

Ponentes:

Enrique Sánchez Hilara, director de división de Explotación y Seguridad de Sistemas de Telefónica Móviles España desde el año 2001. Ingeniero de Telecomunicación y Master MBA por el Instituto de Empresa y profesor del Master de Telecomunicaciones en la materia de Sistemas Informáticos en la Universidad de Deusto, ha trabajado en Commodore, Idea, Amstrad, System-4, Grupo Z y Hobby-Press. En Telefónica Móviles España comenzó a prestar sus servicios hace once años, y antes de ocupar su actual cargo, fue durante cinco años director de Explotación y Seguridad.

Carlos Jiménez Suárez, presidente de Secuware. Es 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 el año 1990 fundó Anyware Seguridad Informática y tras la petición de colaboración por el Ministerio de Defensa Español creó la empresa Secuware. Principal promotor del desarrollo continuo I+D+i dentro de la compañía, ha conseguido que Secuware se convierta en una empresa puntera en Europa en el desarrollo de soluciones de seguridad informática para el entorno PC.

LA SEGURIDAD INFORMÁTICA EN EL PLAN ESTRATÉGICO DE SISTEMAS 2004-2006 DE CORREOS

Sinopsis: para situar a la audiencia en la realidad de Correos, se hablará de los nuevos retos de negocio que afronta la organización y se ofrecerá una visión general de las diversas acciones emprendidas en el seno de la empresa: Plan Estratégico 2003-2006, Plan Estratégico de Sistemas 2003-2006 y Plan Director de Seguridad. Abundando en las cuestiones de seguridad, se describirá la experiencia vivida en Correos: diagnóstico de la seguridad, resultados obtenidos y lecciones aprendidas.

Ponentes:

Rubén Muñoz, responsable de la Dirección 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 Correos. Ingeniero Superior Industrial y Master 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 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 labores de consultoría de sistemas informáticos.

Jesús Mayor, Licenciado en Farmacia, posee una experiencia profesional de 7 años en Sistemas Informáticos y Comunicaciones. Su trayectoria profesional siempre ha estado ligada a las tecnologías de Internet y a la Seguridad. Actualmente es el responsable del Área de Seguridad Informática en Correos, estando a cargo de la coordinación y organización de las actividades de seguridad de la organización. Anteriormente, desempeñó el puesto de responsable de Sistemas-Internet. Antes de su incorporación a Correos, Mayor Sendra trabajó en Red Digital Forográfica e Infase Comunicaciones.

LA PLATAFORMA TECNOLÓGICA DE LA AGENCIA NOTARIAL DE CERTIFICACIÓN, ANCERT

Sinopsis: la Agencia Notarial de Certificación (ANCERT), empresa del Consejo General del Notariado dedicada en exclusiva a prestar servicios de certificación y a desarrollar avanzadas soluciones telemáticas basadas en la utilización de la firma digital, ha implantado su infraestructura de PKI de la mano de la empresa gedas iberia utilizando la solución de productos Keon de RSA Security. La adopción de RSA Security como proveedor tecnológico, ha permitido no sólo mejorar la operativa y añadir servicios a la infraestructura PKI del notariado, sino que además hace posible que la Agencia participe en iniciativas que harán de la seguridad una actividad presente en todos los aspectos de la administración, la industria, el comercio y, por supuesto, en la mejora de la profesión notarial. La plataforma de gestión de certificados digitales Keon, junto con el servicio de *Time Stamping* (sello de tiempo) que ofrece ANCERT, hace que sea una de las autoridades de certificación europeas más avanzadas.

Ponentes:

Marek Szymanski es Ingeniero de Telecomunicaciones con una amplia experiencia de más de 15 años en el sector de las tecnologías de la información adquirida en compañías como Telefónica, I+D, BBVA y diferentes empresas del Grupo de Deutsche Bank. Desde el año 2002 es director general de la Agencia Notarial de Certificación, ANCERT, empresa del Consejo General del Notariado.

Luis Jara cursó estudios en la Facultad de Ciencias Económicas y Empresariales de Barcelona y es diplomado PDD por el IESE. Dispone de 20 años de experiencia en el sector y ejerció cargos de responsabilidad en Asicom y el grupo ADD hasta su incorporación en 2001 a gedas iberia, donde actualmente ejerce como *manager* de las áreas de e-Security, Client Services y Contact Center.

RENOVACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE CERES-FNMT, UN PROYECTO EMBLEMÁTICO DE INTEGRACIÓN EN UN ENTORNO MULTITECNOLOGÍA

Sinopsis: la FNMT-RCM, a través del departamento Ceres, es el primer Prestador de Servicios de Certificación en España y un ejemplo seguido internacionalmente, con cerca de 500.000 certificados activos actualmente, que hasta la fecha han realizado decenas de millones de transacciones seguras de todo tipo. En este escenario la FNMT-RCM, con Indra como socio tecnológico, ha abordado la renovación del sistema de certificación, consiguiendo extender el uso de esta tecnología en el ámbito público e introducirla en el ámbito privado, permitiendo a las empresas aprovechar algunas de las ventajas de las que ya venían disfrutando las diferentes Administraciones Públicas usuarias de los servicios de la FNMT. En el transcurso de la ponencia se revisará el proceso seguido para desplegar la nueva plataforma (basada en tecnología KeyOne de Safelayer) que da servicio al sistema Ceres (antes basado en tecnología Entrust) de forma totalmente transparente a los usuarios finales, manteniendo los procesos actuales de gestión del ciclo de vida de los certificados (emisión, renovación y revocación) y la interoperabilidad con otros servicios basados en la utilización del certificado. También se tratarán otros aspectos, como la incorporación de nuevos perfiles de certificado y de nuevos procedimientos (suspensión de un certificado activo,etc.) en cumplimiento del marco legal actual.

Ponentes:

Francisco Jerez. Actualmente desempeña su labor profesional como jefe de servicio del Área Técnica de Ceres, departamento de la Fábrica Nacional de Moneda y Timbre, y previamente como jefe de servicio del Área de Relaciones externas. Anteriormente a esta etapa, su labor se ha centrado en la coordinación de equipos de desarrollo para aplicaciones de gestión y producción dentro de la misma empresa.

Ascensio Chazarra. 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. Desde esta posición ha dirigido algunos de los mas importante proyectos de certificación en nuestro país.

ESTAFAS (SUPLANTACIÓN –*PHISHING*–, ENGAÑOS Y MANIPULACIONES) Y CHANTAJES A ORGANIZACIONES

Sinopsis: el engaño, como uno de los elementos principales de la estafa, ha mejorado con la entrada de las nuevas tecnologías. Las herramientas de los estafadores, que les ofrece la informática e Internet, han hallado una nueva modalidad muy lucrativa, el *"phishing"*; mediante el envío masivo de correos electrónicos en nombre de empresas y entidades de renombre, incita a sus víctimas a acceder a direcciones y enlaces que simulan las páginas oficiales de estas instituciones. El incauto, en "pro de la seguridad", introduce sus datos sensibles (claves y contraseñas, etc.), que permiten al receptor de la información (estafador) el uso de sus cuentas (*email*, bancarias...). Este nuevo *modus operandi* ha obligado a los cuerpos policiales implicados en la investigación a mejorar y ampliar sus conocimientos sobre el complejo ámbito de las estafas. En la presentación, se tratará de mostrar cómo se evitan y detectan los ataques *"phishing"*.

Ponente: María Nieves Gamoneda es Inspector Jefe del Cuerpo Nacional de Policía, adscrita a la Brigada de Investigación Tecnológica (BIT) de la Comisaría General de Policía Judicial desde el año 2000, en la que actualmente es Jefe de Grupo Operativo del Grupo de Fraudes en Internet. Ingreso en 1982 como Inspector del Cuerpo Nacional de Policía. Ha estado destinada siempre en labores operativas en la Jefatura Superior del País Vasco, Cataluña y Madrid, y está especializada en distintas áreas de Policía Científica.

Sinopsis: los "delitos informáticos" que, por su nivel de incidencia, causan mayor inseguridad en la red son, sin duda, los fraudes. Los contenidos engañosos o las manipulaciones informáticas que buscan inducir error en la víctima, generándole un perjuicio patrimonial, están a la orden del día. Por ello, la Guardia Civil, su Grupo de Delitos Telemáticos, conforme ha ido creciendo, ha adaptado su plantilla para dedicar un esfuerzo específico a este tipo delictivo, constituyendo el "Equipo de Fraudes en la Red". La experiencia atesorada por éste en sus numerosas actuaciones ha permitido conocer el *modus operandi* y los perfiles delictivos de la amplia casuística de los fraudes. Desde las estafas en el comercio electrónico, tanto entre comercios y consumidores o viceversa (B2C), como entre consumidores (C2C), hasta el fraude bancario en su moderna acepción del "*phishing*", pasando por los timos de la red, que siguen engañando a ingenuos cibernautas.

Ponente: Juan Salom, Comandante de la Guardia Civil con destino actual en la Unidad Central Operativa de Policía Judicial de la Guardia Civil. Su trayectoria profesional la inició en la Lucha Antiterrorista en el Servicio de Información de Guipúzcoa donde permaneció nueve años. Tras un breve paréntesis en el Servicio Fiscal, en la investigación del blanqueo de capitales, en mayo de 2000 desembarcó en su actual destino, para dirigir el Grupo de Delitos Telemáticos de la Guardia Civil. Cuenta con numerosos cursos de especialización en el campo de las TIC, así como cursos profesionales en el campo de la investigación policial. En su haber figuran la dirección de importantes operaciones contra la delincuencia informática realizadas en España, y la participación en numerosos eventos relacionados con la seguridad y la sociedad de la información.

REQUISITOS Y MECANISMOS DE SEGURIDAD EN LA RED CORPORATIVA DE MICROSOFT

Sinopsis: la ponencia girará en torno a cómo Microsoft gestiona internamente la seguridad TIC. Se describirán los siguientes temas:

- Microsoft y su entorno. ¿Cuál es la situación actual de Microsoft?, y datos sobre su infraestructura.
- La estrategia de seguridad en sí, Informática de Confianza –*Trustworthy Computing*.
- La seguridad en sistemas internos.
- La gestión de la seguridad en los servicios de acceso remoto (*SmartCards* for RAS), red *wireless*, exchange y outlook.
- Modelo de respuesta a incidentes.

Ponentes:

Carlos Lacuna, director de IT para España y Portugal de Microsoft. Comenzó su actividad profesional en Microsoft en 1989. Ha desempeñado sus funciones en los departamentos de Soporte Técnico, Finanzas y Administración, y en los últimos doce años dentro del departamento de IT como director de IT para España y Portugal. Entre otras, sus responsabilidades son: la gestión y el mantenimiento de la red de datos y telecomunicaciones, la gestión del departamento de *helpdesk*, la gestión y el mantenimiento del CPD, y las compras de equipos informáticos y el mantenimiento de los mismos.

Jesús Rodríguez, ingeniero de sistemas en el área de Soluciones Tecnológicas e Infraestructura de la División de Grandes Cuentas y Partners de Microsoft España, en la que lleva trabajando desde hace nueve años en diferentes cometidos: cuatro años como PSS/*Services Support Engineer* (soportando Grandes Cuentas en tecnologías de Infraestructura, Gestión y Mensajería), y cuatro años como *senior operations analyst* en Microsoft ITG (Information Technology Group), siendo responsable de la operación e implementación de tecnología en los CPDs de Microsoft en España y Portugal. Hace un año cambió su papel profesional al área de Ingeniería de Sistemas Preventa en la División de Grandes Cuentas y Partners, responsable del apoyo técnico a la fuerza de ventas en las áreas tecnológicas de Infraestructura, Gestión, Mensajería y Almacenamiento.

BUENAS PRÁCTICAS DE SEGURIDAD EN REDES DE ALMACENAMIENTO

Sinopsis: frente al esquema clásico de almacenamiento directamente conectado al servidor, las innegables ventajas que ofrecen las distintas técnicas de consolidación de almacenamiento y por extensión las redes de almacenamiento, han supuesto un importante cambio en la gestión del almacenamiento y su seguridad.

Iniciativas de la industria, como la definición del Shared Storage Model por parte de la SNIA no hacen sino confirmar la necesidad y el interés de definir un modelo de seguridad en todos los niveles, que extienda el control que de forma generalizada se establece en la capa más cercana a la aplicación final.

En esta ponencia se presentarán un conjunto de buenas prácticas especializadas que, combinadas con las que de forma general resultan de aplicación universal, mitigan los riesgos derivados de la implantación de una red de almacenamiento para alimentar la explotación de datos por parte de los sistemas corporativos.

Ponentes:

Antonio Requejo es director de la División de Servicios Profesionales de Seguridad de Germinus. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid, lleva 8 años trabajando en el área de la seguridad lógica. Cuenta con diversas certificaciones independientes, entre las que destaca la de Gestor Certificado de Proyectos de Seguridad (CISM), por la Information Systems Audit & Control Association.

Javier Zamorano es director de la División de Infraestructuras de Germinus. Zamorano es Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid y ha desarrollado su carrera profesional en empresas como SGI Soluciones Globales Internet y Germinus XXI. Cuenta con diversas certificaciones relacionadas con el campo de las soluciones de almacenamiento de fabricantes como StorageTek, Veritas o Sun Microsystems.

SEGURIDAD INALÁMBRICA: NUEVAS TECNOLOGÍAS, ¿VIEJOS RETOS?

Sinopsis: en esta ponencia se examinará la evolución de los mecanismos de seguridad que se han ido introduciendo en WLAN (y su estándar más popular, el 802.11b), partiendo del fallido WEP, hasta el último estándar aparecido, el 802.11i, pasando por WPA, 8021X, EAP y sus n variedades, y considerando también tecnologías que no son "nativas" de WLAN, como las VPN. Para ello se presentarán sus características y diversas comparativas que permitan evaluar su idoneidad, dependiendo de las necesidades de la entidad que desee implantar WLAN...; todo ello teniendo en cuenta que, a pesar del título de la ponencia, no existe una disciplina llamada "seguridad inalámbrica" (o *wireless*), sino que la solución a los nuevos problemas ha de estar integrada con el resto de medidas de seguridad. Y también que la evaluación de los productos o tecnologías más idóneos, no puede hacerse aisladamente, teniendo siempre en cuenta que la centralización y uniformización de soluciones de seguridad redunda en un ahorro de coste.

Ponente: Miguel Ángel Monjas. Ingeniero de Telecomunicación por la UPM. Actualmente desarrolla su labor profesional en el departamento de Ingeniería de Sistemas del centro de I+D de Ericsson España en Madrid, dentro del área de User Security and SSO en donde, desde hace más de dos años, trabaja en aspectos relacionados con la autenticación de usuario y la identidad digital. El centro de I+D de Ericsson España está especializado en bases de datos de usuario de telefonía móvil. Comenzó su carrera profesional en Goya Servicios Telemáticos.

SECURMATICA 2004

AFORO LIMITADO

Fechas y lugar

SECURMÁTICA 2004 tendrá lugar los días 20, 21 y 22 de abril de 2004 en el hotel NOVOTEL*. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2004 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 Premios SIC (21 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 91 401 06 26 / +34 91 309 04 99
- Por fax: +34 91 401 09 90
- 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
  Lombía, 3 - Bajo derecha
  28009 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 para los congresistas que deseen alojarse en el hotel Novotel con motivo de su asistencia a Securmática. Este particular deberá ser comunicado a la entidad organizadora con la debida antelación, ya que el número de habitaciones es limitado.
- 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 2004

Nombre y apellidos _____

Nombre y apellidos _____

Nombre y apellidos _____

Empresa _____ C.I.F. _____

Cargo _____

Dirección _____ Población _____

Código Postal _____ Teléfono _____ Fax _____

Persona de contacto, Departamento y teléfono para facturación _____

_____

❑ MÓDULO 1 DÍA 20 ❑ MÓDULO 2 DÍA 21 ❑ MÓDULO 3 DÍA 22 ❑ Deseo inscribirme a SECURMATICA 2004

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/. de Lombía, 3. Bajo derecha. 28009 Madrid.

Información e inscripciones:

REVISTA SIC seguridad en informática y comunicaciones

Ediciones CODA / Revista SIC
Lombía, 3 - Bajo derecha · 28009 Madrid (España)
Tel: 91 401 06 26 / 91 309 04 99 · Fax: 91 401 09 90
Correo-e: info@securmatica.com / info@codasic.com
Sitio: **www.securmatica.com**