SECURMATICA

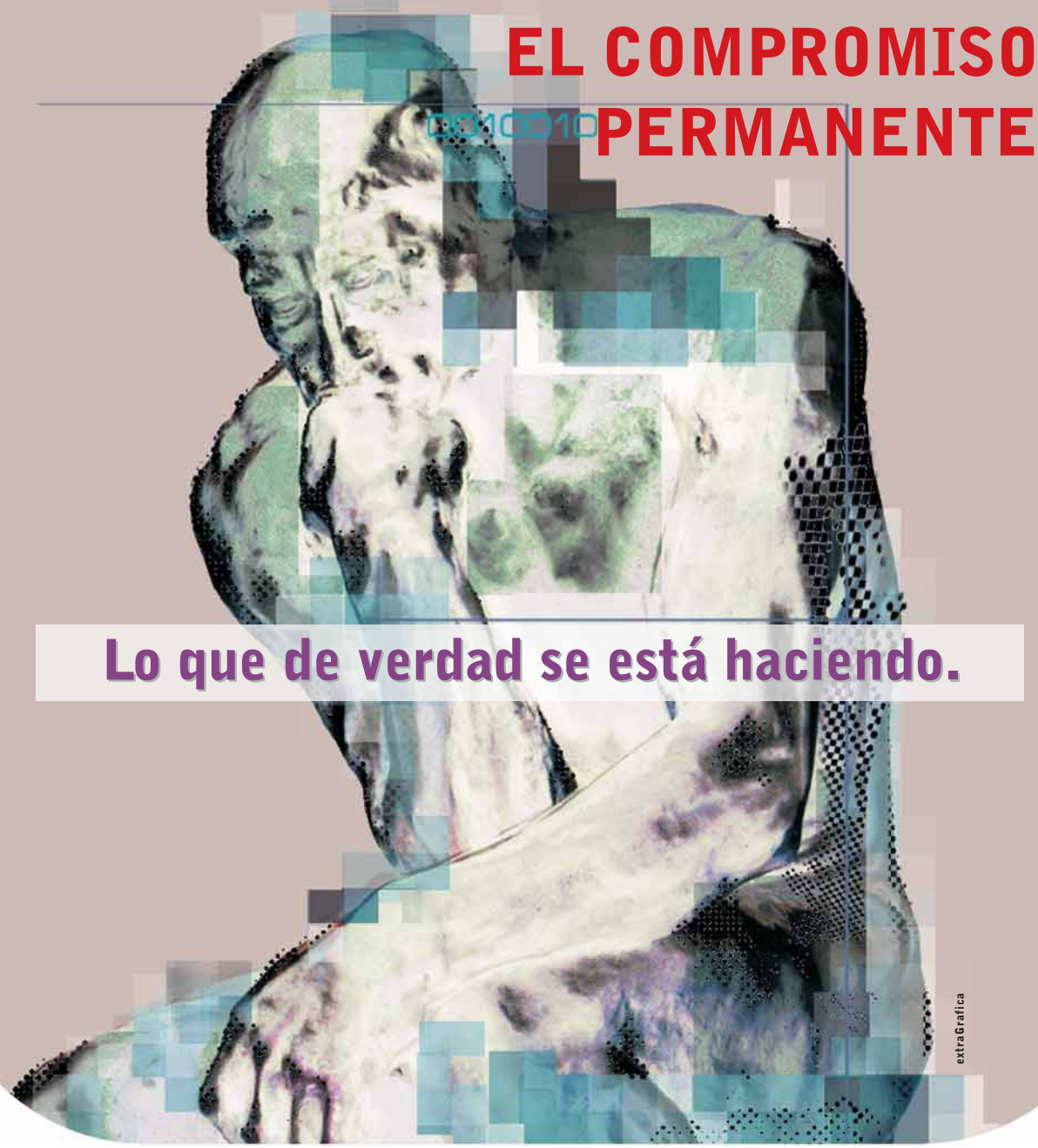
XVI Congreso español de Seguridad de la Información 2005

www.securmatica.com

26, 27 y 28 de abril
Hotel Novotel. Campo de las Naciones (Madrid)

Protección de la información:

EL COMPROMISO PERMANENTE



Lo que de verdad se está haciendo.

extraGrafica

PROGRAMA

Una vez más Securmática se cita con su audiencia natural: los responsables de seguridad de la información, y la industria y los servicios relacionados con la seguridad TIC. La XVI edición del congreso que anualmente organiza la revista SIC, se celebrará los días 26, 27 y 28 de abril en su ya tradicional sede del Campo de las Naciones de Madrid.

ES HORA DE COMPARTIR EXPERIENCIAS Y AVANZAR

En línea con el enfoque que le caracteriza, la Organización del congreso ha conformado un programa que refleja fielmente lo que de verdad se está haciendo en materia de protección, al tiempo que profundiza en debates estratégicos para la profesión, como son las nuevas y más amplias perspectivas que se avecinan para el desempeño de la función, el papel jugado hoy por la tecnología ante los riesgos, la evolución de las amenazas en su propósito de entorpecer el normal desarrollo de la Sociedad de la Información, y, por último, evidenciar algunas de las tendencias tecnológicas venideras más significativas.

Copatrocinadores:

Deloitte. · Ernst & Young Quality In Everything We Do · gedas your IT partner · germinus

IBM · Indra · S2Isec · Secuware

SGI Soluciones Globales Internet · sia · steria · Telefónica

Organiza:

Revista SIC seguridad en informática y comunicaciones

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

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

PRIMER MÓDULO 26 de abril

08:45h. Entrega de documentación
09:15h. Inauguración oficial
10:00h. Conferencia de apertura: **Los retos para el control efectivo del cumplimiento de la legislación sobre protección de datos personales en la sociedad digital.**
Ponente: **Álvaro Canales Gil**, Subdirector General de Inspección de Datos de la Agencia Española de Protección de Datos.
10:30h. Coloquio
10:35h. Ponencia: **MADRE: aplicación de soporte al proceso de cumplimiento del "Reglamento" y la LOPD.**
Ponente: **Juan Carlos Gómez Castillo**, Gerente de Seguridad de la Información. Dirección de Seguridad de la Información y Prevención del Fraude. Telefónica, S.A.
11:15h. Coloquio
11:20h. Pausa-café
11:50h. Ponencia: **Hacia el Buen Gobierno Corporativo en TI: proyecto SOX ITGC en Ericsson.**
Ponente: **Casimiro Juanes**, Responsable de Seguridad Informática de EMEA. Dirección de TI Corporativa de Ericsson.
12:30h. Coloquio
12:35h. Ponencia: **Gestión centralizada de sistemas de seguridad corporativos.**
Ponente: **Santiago Moral Rubio**, Director de Seguridad Lógica Corporativa del Grupo BBVA.
13:15h. Coloquio
13:20h. Mesa redonda: **El papel actual de la tecnología de seguridad TIC en la gestión de riesgos de información.**
Intervienen:
- **José Antonio Castro**, Director de Seguridad Informática de Grupo Santander.
- **Luis Jiménez**, Subdirector General Adjunto del Centro Criptológico Nacional. Centro Nacional de Inteligencia.
- **Miguel Ángel Navarrete**, Director de Seguridad Informática de Caja Madrid.
- **Ana Mª Ramos**, Responsable de Seguridad de Sistemas de BT.

14:30h. Coloquio
14:35h. Almuerzo
16:35h. Ponencia: **La seguridad lógica en las Cajas de Ahorro. Tendencias de mercado y líneas de actuación.**
Ponentes: **Vicente García Llorens**, Director de Innovación Tecnológica y Seguridad Lógica. Caixa Galicia, y **Antonio E. Martínez**, Senior IT Architect. ITS. IBM.
17:15h. Coloquio
17:20h. Ponencia: **La gestión de identidades en Auna.**
Ponente: **Jaime de Pereda Huelves**, Responsable de Seguridad y Comunicaciones de Sistemas de Información de Auna.
18:00h. Coloquio
18:05h. Pausa-café
18:20h. Ponencia: **La importancia de la seguridad en los sistemas de información sanitarios.**
Ponentes: **Jesús García Marcos**, Subdirector de Tecnologías y Sistemas de la Información del Ministerio de Sanidad y Consumo, y **Eduardo Martín Calleja**, Director de Steria Consulting.
19:05h. Coloquio
19:10h. Fin de la primera jornada

LOS RETOS PARA EL CONTROL EFECTIVO DEL CUMPLIMIENTO DE LA LEGISLACIÓN SOBRE PROTECCIÓN DE DATOS PERSONALES EN LA SOCIEDAD DIGITAL

Sinopsis:
La conferencia inaugural versará sobre la necesaria conciliación entre los sistemas de información y comunicaciones, que se encuentran en un proceso de constante evolución, y el derecho fundamental a la protección de datos de carácter personal, que la Constitución Española y la Constitución Europea reconocen a los ciudadanos. Dentro de esta relación, el principio de seguridad en el tratamiento de datos personales, constituye una exigencia normativa sin la cual no resulta posible atender a la garantía del citado derecho. En este entorno, se analizarán las diferentes tecnologías de la información y de las comunicaciones y los riesgos que pueden suponer para los diferentes agentes que las utilizan para administrar la recogida y el tratamiento de datos personales.

Ponente:

< Álvaro Canales Gil es Subdirector General de Inspección de Datos de la Agencia Española de Protección de Datos (AEPD). Licenciado en Derecho y Doctor, tiene una larga experiencia como Interventor de la Administración del Estado (1982) y también en el ámbito docente, como Profesor numerario de la Escuela de Intervención (Ministerio de Defensa), Profesor adjunto de la Facultad de Ciencias Jurídicas de la Administración de la Universidad San Pablo CEU (Madrid) y Profesor asociado de la Facultad de Ciencias Políticas y Sociología de la UCM. Ha publicado numerosas monografías entre 1996 y 2003, y está en posesión de diversos premios, entre los que cabe destacar el Premio III Edición San Raimundo de Peñafort, Universidad San Pablo CEU, por el trabajo titulado "El sector energético del gas natural: un caso especial de regulación de la actividad económica" (1999) y el primer accesit del Premio convocado por la Intervención General de la Administración del Estado con motivo del CXXV Aniversario de su creación (2000). Antes de desempeñar su actual cargo en la AEPD, ha sido Secretario General de este Organismo.

MADRE: APLICACIÓN DE SOPORTE AL PROCESO DE CUMPLIMIENTO DE LA LOPD Y EL "REGLAMENTO"

Sinopsis:
El cumplimiento de la Ley Orgánica de Protección de Datos y el Reglamento de Medidas de Seguridad (RMS) es un proceso continuo en el que deben estar involucradas diferentes áreas de la organización: asesoría jurídica, seguridad de la información, áreas de negocio, sistemas de información, atención al cliente, etc. Este escenario implica que en grandes y medianas organizaciones el proceso sea complejo y deba apoyarse en una herramienta de gestión como MADRE.
MADRE permite la gestión del cumplimiento del RMS y la LOPD de manera más eficaz y eficiente. Se trata de una aplicación web flexible y adaptable a cualquier empresa. Entre otras muchas funcionalidades, facilita el mantenimiento distribuido y sistemático de los documentos de seguridad, integrándose con los sistemas, procesos y procedimientos existentes. En la ponencia se analizará qué es y cómo ha surgido MADRE, los retos que ayuda a resolver y los módulos funcionales que la componen, así como una demostración práctica de la aplicación.

Ponente:

< Juan Carlos Gómez Castillo es Gerente de Seguridad de la Información en Telefónica S.A. Ingeniero Superior de Telecomunicación por la UPM, CISA y CISM por la ISACA y PDD por el IESE Business School, previamente ha desarrollado su carrera profesional como Responsable de Seguridad de Sistemas de Información en Telefónica Data España, British Telecom España y Servicom, trabajando también como consultor y jefe de proyectos de seguridad en Telefónica Sistemas y TPTI.

HACIA EL BUEN GOBIERNO CORPORATIVO EN TI: PROYECTO SOX ITGC EN ERICSSON

Sinopsis:

Es de todos conocido el interés y la necesidad de la instauración de métodos y prácticas de *Buen Gobierno Corporativo* para gestionar y controlar eficazmente la empresa, incluyendo el entorno informático. Esta necesidad se ha convertido en una obligación tras la aprobación de la norma Sarbanes Oxley (SOX) en Estados Unidos. En esta presentación se mostrarán estos temas teniendo como base el proyecto global de adecuación a dicha norma realizado en Ericsson, especialmente el trabajo realizado en el proyecto de Controles en el entorno Informatico (SOX ITGC). Se hará hincapié en las experiencias acumuladas durante el proyecto, dando recomendaciones prácticas a la hora de enfrentarse a uno similar. Asimismo, se intentará dar continuidad a las prácticas llevadas a cabo en este proyecto para obtener un buen gobierno de la Seguridad TIC.

Ponente:

< **Casimiro Juanes** es Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid. Desde el comienzo de su vida profesional ha trabajado en Ericsson en el área de Informática. Juanes ha trabajado con proyectos de seguridad desde entonces hasta 2002, cuando fue nombrado Responsable de Seguridad Informática de Ericsson España. Más tarde, ese mismo año, obtuvo el puesto de Responsable de Seguridad Informática para la región de EMEA en la dirección corporativa de TI, que es su posición actual. Entre sus responsabilidades actualmente se encuentran las de adecuación a la normativa SOX en el entorno TI para su región. Obtuvo el certificado profesional de seguridad CISSP en 2003.

GESTIÓN CENTRALIZADA DE SISTEMAS DE SEGURIDAD CORPORATIVOS

Sinopsis:

A lo largo de la ponencia se desgranarán los aspectos fundamentales a tener en cuenta a la hora de desarrollar un "Sistema Centralizado de Gestión de la Seguridad de la Información" (SCGSI) en una corporación. Los tres ejes fundamentales para determinar el funcionamiento de un SCGSI son: *reducción del riesgo*, *reducción de costes* y *reducción de la complejidad*. El primer aspecto que se debe abordar es la definición explícita de las mejoras, en cuanto a *reducción del riesgo*, que se van a obtener al definir e implantar una Función Corporativa de Seguridad de la Información soportada por un SCGSI. Uno de los aspectos fundamentales a tener en cuenta es analizar la "idoneidad y la forma" en las que se debe separar la "gestión de la seguridad" de la "operación de las tecnologías de seguridad". Dependiendo de cómo se realice "esta separación" podrían provocarse tiempos de recuperación mayores cuando en una incidencia tecnológica en un CPD estén involucradas las propias tecnologías de seguridad. Este tipo de situaciones podrían penalizar la disponibilidad y, por ende, uno de los tres pilares de la seguridad de la información.

El segundo aspecto es analizar los costes asociados a un SCGSI y cómo se consigue el ROI/ROSI. Para una Corporación, la implantación de un SCGSI tiene ventajas económicas que pueden medirse en el corto, medio y largo plazo. Estando éstas asociadas tanto al capital humano, TCO e infraestructura de seguridad, gestión del fraude electrónico, lucro cesante, cumplimiento de la legislación y regulaciones locales de cada país y la concentración de servicios de seguridad prestados al resto de la unidades de TI y a la Corporación en general.

MESA REDONDA

EL PAPEL ACTUAL DE LA TECNOLOGÍA DE SEGURIDAD TIC EN LA GESTIÓN DE RIESGOS DE INFORMACIÓN

Proposición:

Nadie discute hoy la importancia y la necesidad de disponer de buenas herramientas tecnológicas con propósitos de seguridad bien definidos para apoyar una gestión real de los riesgos de información en una organización. Sin embargo, en ocasiones se tiende a descargar sobre ellas el éxito o el fracaso en la propia gestión del riesgo, confiriéndoles un protagonismo desmesurado. En la mesa redonda se debatirá sobre este asunto y sobre otros de gran interés que guardan una relación directa: el papel real de la tecnología en la gestión, los riesgos de su uso, la interoperabilidad de las herramientas de mercado, los límites actuales de la tecnología, la conveniencia y viabilidad de la certificación de seguridad y los puntos negros en donde los desarrolladores todavía no han aportado un enfoque eficaz y eficiente a problemas de seguridad.

Intervienen:

> **José Antonio Castro** es director de Seguridad Informática de Grupo Santander. Ha desarrollado la práctica totalidad de su carrera profesional en tecnologías de la información (17 años) en Santander Central Hispano, primero como consultor del área internacional y luego como responsable de diferentes áreas técnicas. Cuenta con 11 años de experiencia en el mundo de la gestión de riesgos de seguridad de la información en áreas como la continuidad operativa, la seguridad en canales alternativos, las infraestructuras de clave pública y las arquitecturas de seguridad net.

> **Luis Jiménez Muñoz** es Subdirector General Adjunto del Centro Criptológico Nacional y Jefe del Área de Certificación del Organismo de Certificación. Entre 1983 y 1988 hizo la carrera militar en la Academia General Militar de Zaragoza. Entre 1991 y 1992 recibió cursos de especialización en matemáticas y criptología, siendo destinado al Centro Criptológico Nacional (CCN). En dicho organismo ha trabajado como especialista criptólogo entre 1992 y 1998, como especialista en seguridad de las Tecnologías de la Información y las Comunicaciones (TIC entre 1998 y 2002, y como jefe de la unidad de políticas y servicios de seguridad de las TIC entre 2002 y 2004. Desde estos puestos ha participado como representante nacional en diversos grupos de trabajo internacionales, y ha sido profesor en los cursos de especialización de criptología y seguridad de las TI que imparte el CCN para la Administración. Dispone de diversas certificaciones de especialización en seguridad de las TIC, incluida la de CISA de ISACA. Actualmente es el representante nacional en los Comités INFOSEC del Consejo de la Unión Europea y de la OTAN, y entre los principales cometidos de su actual puesto se encuentra el desarrollo del esquema Nacional de Evaluación y Certificación de la Seguridad de las TIC, y la elaboración de políticas, directrices y guías de seguridad TI para la administración pública.

> **Miguel Ángel Navarrete** es director del departamento de Seguridad Informática de Caja Madrid. Ha trabajado como informático desde hace 21 años en diferentes entidades financieras. Desde su primer contacto en Explotación y hasta su llegada al mundo de la seguridad de la información, ha recorrido casi todas las áreas de las TI (Técnica de Sistemas, Gestión Presupuestaria, Recursos y Proyectos, Metodología, Arquitectura y Desarrollo de Software), donde ha dirigido numerosos proyectos. Actualmente se enmarca en Planificación e Innovación Tecnológica de Caja Madrid, donde se ubica el departamento de Seguridad Informática, que dirige desde el año 1999.

> **Ana Ramos Centeno** es Responsable de Seguridad de Sistemas de BT España. Licenciada en Ciencias Matemáticas, entre 1996 y 2000 trabajó en el departamento de seguridad de Ceres de la FNMT, ingresando en ese último año en Seguridad de Sistemas de BT España. Ramos es promocionada a responsable de Seguridad de Sistemas de la operadora desde el pasado año y entre las diversas funciones que lleva a cabo en el departamento se encuentran las de la aplicación de procesos y estándares de seguridad de BT Group en España (basados en la BS7799), la aprobación de cambios y elaboración de requerimientos de seguridad de sistemas, así como dar soporte en materia de seguridad en el lanzamiento de nuevos productos/clientes. Es BS7799 Lead Auditor por el BSI.

Ponente:

< **Santiago Moral Rubio** es director de Seguridad Lógica Corporativa del Grupo BBVA. Con 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.

LA SEGURIDAD LÓGICA EN LAS CAJAS DE AHORRO. TENDENCIAS DE MERCADO Y LÍNEAS DE ACTUACIÓN

Sinopsis:

En los últimos años se ha venido produciendo una evolución en la manera de trabajar la seguridad en las Cajas de Ahorros. La situación actual presenta un escenario donde la seguridad lógica está claramente ligada a los procesos de negocio y a los procesos organizativos. Esto es debido a que la respuesta temprana ante un incidente de seguridad impacta de modo muy positivo en el negocio, y, por tanto, ambas estrategias (negocio y seguridad) deben estar correctamente alineadas.

Dada esta situación, las Cajas de Ahorros, a través de la COAS, y en colaboración con IBM, han abordado un amplio estudio sobre Seguridad Lógica. Partiendo de un análisis del estado de la seguridad en las Cajas participantes, el estudio aborda una cobertura global y profunda de la Seguridad Lógica (amenazas, estado del arte y tendencias), así como el análisis de las tendencias de negocio del sector y su impacto en la Seguridad Lógica, para finalmente definir las líneas de actuación prioritarias en este ámbito dentro de las Cajas de Ahorros. En esta ponencia se presenta dicho proyecto, y las principales conclusiones obtenidas de él.

Ponentes:

< **Vicente García Llorens** es Responsable de las Áreas de Innovación y Seguridad Lógica en la Subdirección de Gestión Interna de Caixa Galicia. MBA por INSEAD e Ingeniero en Informática por la Universidad Politécnica de Madrid, desde septiembre de 2003 trabaja en la Subdirección de Gestión Interna de Caixa Galicia donde es miembro del comité de innovación tecnológica. Asimismo, García Llorens se responsabiliza, entre otras actividades, de los proyectos relacionados con Seguridad. Con anterioridad ha sido consultor con Accenture y Arthur D.Little en Inglaterra, Holanda, y Estados Unidos, donde lideró y participó en numerosos proyectos de estrategia y tecnología para empresas de diversos sectores.

< **Antonio E. Martínez** es Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid, y DEA en Informática por la Universidad Autónoma de Madrid. Trabaja en IBM desde 1982, desarrollando arquitecturas de sistemas distribuidos, entre las que se pueden destacar la del sistema de almacenamiento y visualización de documentos del Archivo General de Indias de Sevilla (1992) y la de la Intranet de presentación de resultados de los Juegos Olímpicos de Sydney (2000). Especialista en seguridad en entornos de proceso distribuido, ha liderado por parte de IBM la elaboración del material necesario para la construcción del Libro Blanco de Seguridad Lógica en las Cajas de Ahorros, y participado activamente en el resto de las fases del proyecto de Estudio sobre Seguridad Lógica para las Cajas de Ahorros. Es también Profesor Asociado en la Escuela Politécnica Superior de la Universidad Autónoma de Madrid, donde compagina la docencia en Telemática con la investigación en esta misma área.

LA GESTIÓN DE IDENTIDADES EN AUNA

Sinopsis: AUNA está poniendo en producción su sistema de gestión de identidades con el objetivo de resolver los siguientes problemas: multitud de sistemas cada uno con su propio repositorio de cuentas de usuario; gran volumen de cuentas a gestionar; desfase entre usuarios-cuentas, y realización manual de los procesos de alta y baja de las cuentas. Para resolver estos problemas se ha elegido una herramienta de gestión de identidades que permitirá alcanzar las siguientes metas: propagación automática de la información de cuentas de usuario entre el sistema de gestión de identidades y las aplicaciones integradas en él; la identificación única e inequívoca de los usuarios en un directorio único; el registro centralizado y estándar a los datos de los usuarios, sus accesos y sus credenciales; la gestión del ciclo de vida de las cuentas de usuarios mediante un *work-flow* automatizado para cargas masivas y/o individuales de cuentas, y la gestión centralizada de política de contraseñas.

Ponente:

< **Jaime de Pereda Huelves** es responsable de Seguridad y Comunicaciones de Sistemas de Información de 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 cinco años trabaja en Auna en aspectos relacio nados con la seguridad de la información.

LA IMPORTANCIA DE LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN SANITARIOS

Sinopsis: El Sistema Nacional de Salud ha quedado configurado por la descentralización administrativa derivada de la transferencia de las competencias de gestión a todas las Comunidades Autónomas, la Ley de financiación Autonómica y la Ley de Cohesión y Calidad. Este nuevo marco legal y administrativo hace que el Ministerio de Sanidad y Consumo tenga actualmente un papel de garante de las prestaciones y de la igualdad de los ciudadanos ante el Sistema de forma que ante necesidades iguales se garanticen prestaciones iguales según el principio de equidad, y además que la prestación del servicio se haga conforme a criterios de calidad.

Existe un proyecto básico de identificación de usuarios y también una plataforma tecnológica de comunicaciones sobre los cuales descansa el resto de aplicaciones y funcionalidades. Sobre esa base, sería posible el intercambio de información clínica.

En la ponencia se tratarán los siguientes puntos: la seguridad como consecuencia del tratamiento y disponibilidad de la información sanitaria, el acceso a la información y el intercambio de información en el esquema de los Servicios Web del Sistema Nacional de Salud, las soluciones globales de seguridad, la metodología de los *audits* de seguridad basados en tests de intrusión, y se llevará a efecto la radiografía de un ataque para determinar qué herramientas y métodos utilizan los atacantes y cómo pueden protegerse los servicios web frente al ataque de intrusos.

Ponentes:

< **Jesús García Marcos** es Subdirector General de Tecnologías de la Información del Ministerio de Sanidad y Consumo desde agosto de 2002. Miembro del Cuerpo Superior de Sistemas y Tecnologías de la Información, ha ocupado con anterioridad diversos cargos de responsabilidad, como, entre otros, el de Subdirector General de Sistemas de Información del Ministerio de la Presidencia, y el de Subdirector General del Centro de Sistemas de Información del Ministerio del Interior.

< **Eduardo Martín Calleja**, es actualmente director de Steria Consulting. Licenciado en matemáticas y consultor experto en seguridad de los sistemas de información, previamente ha ocupado en esta compañía otros puestos de responsabilidad como director de la Línea de Negocio de Seguridad y director de las Operaciones para las Administraciones Públicas.

SEGUNDO MÓDULO 27 de abril

09:15h. Entrega de documentación

09:30h. Ponencia: **Experiencias en la prevención y detección de amenazas mediante servicios de seguridad gestionada en red.**
Ponente: **Juan Miguel Velasco López-Urda**, Subdirector de Arquitectura y Planificación de Infraestructuras HASP. Telefónica Empresas.

10:15h. Coloquio

10:20h. Ponencia: **La seguridad de la información en el Banco de España. Organización y acciones sistemáticas.**
Ponente: **María Esther Vidal**, Responsable de la unidad de Seguridad Informática del Banco de España.

11:05h. Coloquio

11:10h. Pausa-café

11:40h. Ponencia: **La seguridad en el ciclo de vida de los proyectos tecnológicos.**
Ponente: **Daniel Barriuso**, Director de Gestión de Riesgos en los Proyectos. ABN Amro Bank N.V.

12:25h. Coloquio

12:30h. Ponencia: **'Securización' de la plataforma PC del Ministerio del Interior: entornos críticos.**
Ponentes: **Jaime Denis Zambrana**, Subdirector General del Centro de Sistemas de Información del Ministerio del Interior, y **Carlos Jiménez**, Presidente de Secuware.

13:15h. Coloquio

13:20h. Ponencia: **Ministerio de Agricultura, Pesca y Alimentación: infraestructura de movilidad segura.**
Ponentes: **Jesús Gallego Suárez**, Coordinador de Sistemas Informáticos del Ministerio de Agricultura, Pesca y Alimentación (M.A.P.A.), y **Antonio Carlos Díaz Molina**, Responsable del Área de Desarrollo de SGI Soluciones Globales Internet.

14:05h. Coloquio

14:10h. Almuerzo

16:15h. Ponencia: **Banesto: la experiencia de desarrollar un cuadro de mando de seguridad.**
Ponentes: **José Díaz Lifante**, Gerente de Seguridad Lógica de Banesto, y **Alfonso del Castillo**, Director de Integración y Servicios de S21sec.

17:00h. Coloquio

17:05h. Ponencia: **Proyecto TAFU (Tarjeta de Funcionario) en la Gerencia de Informática de la Seguridad Social.**
Ponente: **Francisco Manuel Pérez Fernández**, Jefe del Área de Seguridad. Centro de Calidad, Auditoría y Seguridad de la Gerencia de Informática de la Seguridad Social.

17:50h. Pausa-café

18:05h. Ponencia: **Honeypots y honeynets: I+D+i**
Ponentes: **Javier Urtiaga**, Senior Manager de T&SRS de Ernst & Young, y **César Tascón**, Manager de T&SRS de Ernst & Young.

18:50h. **Coloquio**

18:55h. **Fin de la segunda jornada**

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

EXPERIENCIAS EN LA PREVENCIÓN Y DETECCIÓN DE AMENAZAS MEDIANTE SERVICIOS DE SEGURIDAD GESTIONADA EN RED

Sinopsis:
Telefónica Empresas tiene, entre otros objetivos, proporcionar los elementos de servicio de seguridad gestionada necesarios para conseguir el "tráfico limpio", conexiones, accesos y servidores de Internet con las garantías de seguridad necesarias para el desarrollo de negocios y actividades con confianza para empresas y usuarios. Para ello, dispone de servicios de antivirus, anti-*spam*, cortafuegos gestionado, monitorización y gestión de cortafuegos, IDS y filtrado de contenidos. La prestación de estos servicios desde el SOC ha dado a Telefónica Empresas una posición privilegiada para conocer el comportamiento de las distintas amenazas en función de diversas variables. En la conferencia, se aportarán algunos datos relacionados con patrones e incidencias en el contexto.

Ponente:

< **Juan Miguel Velasco López-Urda** es Subdirector de Arquitecturas y Servicios de Seguridad de la Línea de Outsourcing de Sistemas de Telefónica Empresas. Anteriormente ejerció en Telefónica Data como Subdirector de Ingeniería de Proyectos y Servicios de Protección de la Información de la UN Hosting y ASP y Director Técnico y de Consultoría de la Agencia de Certificación Electrónica (ACE), sociedad filial de Telefónica DataCorp, afiliado internacional de Verisign. Ha cursado estudios de Informática en la Universidad Politécnica de Madrid y, entre otros, es Master Executive de Gestión Empresarial por INSEAD-Euroforum.

LA SEGURIDAD INFORMÁTICA EN EL BANCO DE ESPAÑA. ORGANIZACIÓN Y ACCIONES SISTEMÁTICAS

Sinopsis:
En el Banco de España se ha contemplado siempre la seguridad informática desde una óptica amplia que incluye, no sólo la selección e implantación de medidas técnicas, sino también, y muy especialmente, la definición de un marco organizativo que garantice la puesta en funcionamiento y observancia de los procedimientos y medidas de seguridad. Pieza clave para alcanzar los objetivos de seguridad es conseguir que la asignación de responsabilidades dentro de la organización esté claramente definida, de tal manera que cada cual conozca qué se espera de él en relación con la seguridad. Esta asignación de responsabilidades debe tener en cuenta a todos los actores que intervienen, desde el usuario final, que debe hacer un uso responsable de los sistemas y equipos que se ponen a su disposición, hasta el personal técnico de operación, que asegura que los sistemas funcionan de acuerdo con los requerimientos establecidos, pasando por los mandos intermedios, directores de departamento, desarrolladores y, entre otros, los responsables de seguridad.

Ponente:

< **María Esther Vidal González** es responsable de la Unidad de Seguridad Informática del Banco de España. Ingeniero superior de telecomunicaciones por la Universidad Politécnica de Madrid, en el año 1981 ingresa en el Departamento de Sistemas de Información del Banco de España. Su carrera profesional se ha desarrollado siempre dentro de este Departamento. En el año 1994 pasó a dirigir la Unidad de Seguridad Informática, cuyas funciones comprenden, tanto la responsabilidad técnica de la seguridad de los diferentes entornos, como la definición de las políticas, procedimientos y organización necesarios para una correcta gestión de la seguridad dentro de la Institución. Desde el año 2000 participa, como representante del Banco de España, en el grupo de trabajo de Seguridad Informática del Sistema Europeo de Bancos Centrales.

LA SEGURIDAD EN EL CICLO DE VIDA DE LOS PROYECTOS TECNOLÓGICOS

Sinopsis: La gestión de la seguridad entendida como un proceso dinámico, necesariamente debe ocuparse de los aspectos cambiantes de la organización, y por tanto, de los proyectos tecnológicos. En el actual entorno económico, donde el "*time to market*" y la competitividad de las soluciones tecnológicas son fundamentales, es necesario implementar una seguridad eficiente y flexible que se adapte a las necesidades de negocio. Factores como el perfil de riesgo que asume una entidad, la implementación de una seguridad efectiva en coste, o la fiabilidad de los controles existentes, dependen en gran medida de la correcta integración de la gestión de riesgos en el ciclo de vida de los proyectos tecnológicos.

Ponente:

< **Daniel Barriuso** es Director del Departamento de Gestión de Riesgos en los Proyectos en ABN Amro Bank N.V., donde tiene responsabilidad global sobre la seguridad en los proyectos de desarrollo y nuevas soluciones tecnológicas a través de más de 40 países. Con una experiencia de más de 10 años en Seguridad y TIC, la prioridad de Barriuso está centrada ahora en los aspectos organizativos de la seguridad, tales como el gobierno, la estrategia y la gestión del riesgo. Previamente a su incorporación a ABN Amro, ha sido Director del Departamento de Seguridad de Credit Suisse España. Desde 2002, imparte clases como profesor en el Master de Seguridad y Auditoría de la UPM sobre áreas tales como el gobierno y la gestión de la inversión en seguridad. Es Ingeniero Superior en Informática por la Universidad Carlos III de Madrid y está certificado como Lead Auditor BS7799.

"SECURIZACIÓN" DE LA PLATAFORMA PC DEL MINISTERIO DEL INTERIOR: ENTORNOS CRÍTICOS

Sinopsis: El Ministerio del Interior (MIR) y su personal, en estrecha colaboración con Secuware, está "securizando" la plataforma PC puesta a disposición de los funcionarios que manejan datos altamente confidenciales. Para ello, el MIR ha implantado la herramienta SSF que ayuda a cifrar la información de manera que sea ilegible fuera del entorno MIR. Adicionalmente, dado que los funcionarios también trabajan con información menos confidencial y que no requiere la clasificación de secreta, el departamento de seguridad del MIR, usando la herramienta de referencia y un amplio conocimiento de las políticas de Microsoft, ha creado dos perfiles de usuario, el primero con grandes niveles de seguridad para imposibilitar la extracción de información secreta, y el segundo con un nivel de seguridad funcional para manejar información menos sensible.

Ponentes:

< **Jaime Denis Zambrana** es Subdirector General del Centro de Sistemas de Información del Ministerio del Interior. Físico (UAM), Máster en Administración de Empresas (MBA por el Instituto de Empresa) y Funcionario del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado, Denis Zambrana tiene una larga trayectoria profesional. Ha sido profesor del departamento de Física Aplicada de la UAM, Técnico de Sistemas responsable del Área de Bases de Datos de la Comisión Interministerial de Ciencia y Tecnología (CICYT del Mº de Educación y Ciencia, Jefe del Área Informática del Instituto de la Pequeña y Mediana Empresa Industrial (hoy Dirección General de Política de PYME del Mº de Industria, Turismo y Comercio), Director del Programa de Nuevas Tecnologías de la Información y la Comunicación del Mº de Educación y Cultura, Director de Multimedia del Grupo Santillana de Ediciones, S.A., y Director de Tecnología y Realización de Santillana Formación.

< **Carlos Jiménez Suárez** es presidente de la compañía Secuware. Ingeniero Superior de Telecomunicación por la Universidad Politécnica de Madrid, desde 1989 ha sido el único ingeniero que ha simultaneado cinco de las seis especialidades. En 1988, un año antes de terminar la carrera, realizó el primer antivirus contra el virus Viernes 13. En 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 líder europeo en el desarrollo de soluciones de seguridad informática en el entorno PC. Desde finales de los años 80 lleva desarrollando soluciones de seguridad que protegen el PC frente a las diversas amenazas y a múltiples niveles.

MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACIÓN: INFRAESTRUCTURA DE MOVILIDAD SEGURA

Sinopsis: Ante los problemas y peligros que puede acarrear hoy el uso de redes inalámbricas –acceso no autorizado a los recursos de la red, escuchas de la señal inalámbrica, suplantación, etc.– el Ministerio de Agricultura, Pesca y Alimentación (M.A.P.A.) emprendió el correspondiente proyecto de "securización" de su sistema de gestión de redes inalámbricas. En la solución a las necesidades identificadas en el contexto ha colaborado Soluciones Globales Internet, ayudando a la implantación de su Sistema de Gestión Inalámbrico Emissary Wireless Security en la red inalámbrica del Ministerio.

Ponentes:

< **Jesús Gallego Suárez** es Coordinador de Sistemas Informáticos del Ministerio de Agricultura, Pesca y Alimentación (M.A.P.A.). Licenciado en Ciencias Físicas por la Universidad Complutense de Madrid en 1967, fue profesor de Ciencias hasta 1970, año en el que ingresó en la Junta de Energía Nuclear (Ciemat) hasta 1990, en el Departamento de Informática, realizando diversos cometidos: Técnico en Cálculo Numérico, Jefe de Operación, Explotación e Infraestructuras, Analista, Técnico de Sistemas. En 1990 se trasladó al Mº de Agricultura, Pesca y Alimentación como Jefe de Área Informática, estando en un principio como adjunto a la dirección. En 1996 fue nombrado Jefe de Área de Comunicaciones, Sistemas e Infraestructuras, abordando proyectos como la instalación de una nueva red de voz y datos, cambiando todo el sistema tanto a nivel de sistema operativo, como de bases de datos, y llevando a efecto la instalación de redes inalámbricas en los dos edificios principales del Departamento. La "securización" de estas redes ya se ha realizado con un sistema altamente eficaz. Desde 2003 ocupa el cargo de Coordinador de Sistemas Informáticos del M.A.P.A.

< **Antonio Carlos Díaz Molina** es Responsable del Área de Desarrollo de Soluciones Globales Internet. Ingeniero Superior en Informática por la Universidad Politécnica de Valencia, tiene 12 años de experiencia profesional en equipos de desarrollo especializados para la Administración Pública, tanto en entorno propietario y cliente-servidor, como en entorno web. Durante estos 12 años ha desarrollado su actividad profesional en TAO Grupo Gedas, realizando las funciones de equipo de desarrollo de aplicaciones de gestión para la Administración Local, Provincial y Autonómica y la jefatura de proyecto para adaptación de aplicaciones de gestión para superar el efecto 2000 y la adaptación al Euro, para migración de datawarehouse entre sistemas heterogéneos y para soluciones basadas en desarrollos web. Desde 2003 es Responsable del Área de Desarrollo de Soluciones Globales Internet en la Delegación Sur donde se responsabiliza de la gestión del equipo humano, coordinación y estrategia del Área de Desarrollo, la dirección y ejecución de diversos proyectos centrados en: soluciones en entorno web, aplicación de software libre, soluciones de seguridad en redes inalámbricas, soluciones de correo corporativo, soluciones de movilidad, soluciones de infraestructuras de clave pública y soluciones de provisión de servicios y aplicaciones.

BANESTO: LA EXPERIENCIA DE DESARROLLAR UN CUADRO DE MANDO DE SEGURIDAD

Sinopsis:

El objetivo de la ponencia es, como intenta transmitir su título, compartir con los asistentes la experiencia de Banesto y S21sec en el desarrollo de un cuadro de mando de seguridad. Para ello se analizará cómo surge la necesidad de disponer de un grupo de indicadores que midan la seguridad de la información desde el área de Seguridad Informática de Banesto, cuál fue el proceso de selección de dichos indicadores y, finalmente, cómo se llevaron a la realidad dichos indicadores con la colaboración de S21sec.

Finalmente, y como ejemplo del trabajo realizado, se expondrán algunos ejemplos de los indicadores implantados (con datos ficticios) utilizando el software Bitácora como soporte de la información.

Ponentes:

< **José Díaz Lifante** es Gerente de Seguridad Lógica de Banesto. Ingeniero Industrial y MBA por ESDEN, ha desempeñado su carrera profesional en Explosivos Río Tinto como Jefe de Microinformática en la Refinería de Huelva, en Tecnológica S.A., y en la Agencia Espacial Europea (Holanda), en Ingeniería de componentes electrónicos para la industria espacial. Desde 1990 dirige la Unidad responsable de la seguridad informática en Banesto con el cargo de Gerente de Seguridad Lógica.

< **Alfonso del Castillo Jurado** es Director de Integración y Servicios de S21sec. Ingeniero Técnico en Informática por la UPM (Sistemas) y CISA, es especialista en el análisis y la gestión de la seguridad (test de intrusión, auditorías externas, análisis forenses), en el análisis y gestión de *logs* y en la gestión y análisis de vulnerabilidades. Con anterioridad a su actual ubicación en S21sec trabajó durante 5 años en T&SRS de Ernst & Young.

PROYECTO TAFU (TARJETA DE FUNCIONARIO) EN LA GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL

Sinopsis: La nueva tarjeta de empleado de la Seguridad Social, objeto del proyecto TAFU (Tarjeta de Funcionario) de la GISS, basada en tecnología JavaCard, se concibe como una herramienta para el incremento de la seguridad en el acceso físico y electrónico al puesto de trabajo, aportando un conjunto de servicios de valor añadido con base en la firma electrónica y el certificado digital. En la ponencia se profundizará en la concepción de este proyecto, del que ya se ha realizado un piloto para dos mil usuarios, y que una vez implantado y desplegado afectará a cuarenta mil personas.

Ponente:

< **Francisco Manuel Pérez Fernández** es Jefe del Área de Seguridad en el Centro de Calidad, Auditoría y Seguridad de la Gerencia de Informática de la Seguridad Social, GISS. Licenciado en Ciencias Físicas por la Universidad del País Vasco, Master DisTic en Tecnologias de Información y Comunicaciones por la Universidad Complutense de Madrid y Posgrado de Consultor de Seguridad por la U.O.C., posee una experiencia de 20 años en la Gerencia de Informatica de la Seguridad Social, en donde ha ocupado puestos de responsabilidad en los entornos de Administración de datos, Administración de bases de datos, Infraestructuras y Producción, hasta su actual ubicación como jefe del Área de Seguridad.

HONEYPOTS Y HONEYNETS: I+D+i

Sinopsis: La creciente complejidad y creatividad de los actuales, y cada vez más elaborados, ataques a través de Internet a los que está expuesta cualquier organización, obliga a replantear el escenario en el que se encuentran las empresas con respecto a la seguridad informática. Cada vez más, medidas reactivas como son los análisis de vulnerabilidades, la gestión de *logs* o los detectores de intrusión no son suficientes, y se plantea la necesidad de desarrollar soluciones novedosas y proactivas que ayuden a mejorar el nivel de exposición al riesgo y respuesta frente a un ataque.
En este marco, soluciones *Honeypot* / *Honeynet* de última generación aportan nuevas funcionalidades y posibilidades para desarrollar protecciones frente a los ataques más actuales. El establecimiento de servicios y/o equipos señuelo que atraigan la atención de un potencial atacante, unido a una serie de posibles capacidades a implementar (monitorización, estudio, reacción, identificación inteligente de patrones, *mirror* de servicios, evidencias forenses, etc), permitirán a estas organizaciones ofrecer niveles alternativos de seguridad que complementen y mejoren sus actuales sistemas de protección.

Ponentes:

< **Javier Urtiaga Baonza** es Senior Manager de Technology & Security Risk Services (TSRS) de Ernst & Young. Ingeniero Técnico en Telecomunicaciones por la Universidad Politécnica de Barcelona, actualmente desempeña el puesto de responsable de Productos y Servicios del departamento, coordinando las líneas de servicio de Advanced Security Solutions, SGSI & Corporate Intelligence y Soluciones de Identidad Digital.

< **César Tascón Álvarez** es Gerente de Technology & Security Risk Services (TSRS) de Ernst & Young. Ingeniero Técnico en Informática de Sistemas, es actualmente responsable de la línea de servicio Advanced Security Solutions, que engloba aquellos proyectos en seguridad con una elevada carga tecnológica (*hacking* ético, auditorías técnicas, bastionado de servidores, *forensics*, *HoneyPot*, etc). Actualmente dirige los laboratorios de Madrid y Barcelona de Ernst & Young.

TERCER MÓDULO 28 de abril

09:15h. Entrega de documentación

09:30h. Ponencia: **Oficina de Armonización del Mercado Interior (OAMI): certificación de seguridad BS7799-2/2002**
Ponentes: **Francisco García-Valero**, Jefe del Servicio de Atención a Usuarios y de Seguridad Informática de la OAMI, y **Angel Pujol de Lara**, Gerente de Enterprise Risk Services de Deloitte.

10:10h. Coloquio

10:15h. Ponencia: **Sistema de gestión unificada de usuarios y *login* único de la Autoridad Portuaria de Barcelona.**
Ponentes: **Francesc Xavier Bonada**, Responsable de Sistemas y Atención a Usuarios. Departamento de Sistemas de Información de la Autoridad Portuaria de Barcelona, y **Antonio Rodríguez de la Torre**, Responsable de Gestión de Identidades y Plataformas OS. Servicios Profesionales y e-Security de gedas Iberia.

10:55h. Coloquio

11:00h. Pausa-café

11:30h. Ponencia: **Implantación de la Oficina de Seguridad de los Sistemas de Información y Comunicaciones de la Guardia Civil – Proyecto BUHO.**
Ponentes: **Tomás Villalba de la Luz**, Jefe de la Oficina de Seguridad de los Sistemas de Información y Comunicaciones (OSSIC) de la Guardia Civil, y **Jorge Laredo**, Consultor Senior de Seguridad TI de Indra.

12:10h. Coloquio

12:15h. Mesa redonda: **El futuro de la función de seguridad de la información.**
Participan:
- **Francisco Javier García Carmona**, Director del Departamento de Seguridad de la Información y las Comunicaciones de Iberdrola.
- **Víctor Jiménez**, Responsable de Seguridad y Auditoría de la Información. Departamento de Sistemas de Información. Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda.
- **Tomás Roy Catalá**, Director de Calidad y Seguridad. Generalitat de Catalunya.
- **Javier Valdés**, Director del Departamento de Seguridad Informática de Bankinter.

13:45h. Coloquio

14:00h. Almuerzo

16:00h. Ponencia: **Tendencias en tecnologías de seguridad: ¿vamos por el buen camino?**
Ponente: **Jorge Hurtado**, Director Comercial de Germinus.

16:40h. Coloquio

16:45h. Sesión de clausura: **La progresión del fraude en servicios de la sociedad de la información.**
Intervienen:
- **María Nieves Gamoneda**, Inspector-jefe de la Brigada de Investigación Tecnológica. UDEV Central. Comisaría General de la Policía Judicial. Cuerpo Nacional de Policía.
- **Juan Salom**, Jefe del Grupo de Delitos Telemáticos de la Unidad Central Operativa de la Policía Judicial de la Guardia Civil.

17:45h. Coloquio

18:00h. **Clausura de Securmática 2005**

OFICINA DE ARMONIZACIÓN DEL MERCADO INTERIOR (OAMI): CERTIFICACIÓN DE SEGURIDAD BS7799-2/2002

Sinopsis:
La OAMI, Agencia Europea con sede en Alicante, ha culminado con éxito el proceso de certificación en el estándar de seguridad BS7799-2/2002 para su proceso de registro de Diseños Comunitarios, convirtiéndose en la tercera entidad en España que consigue esta certificación. El proceso de diseño e implantación del Sistema de Gestión de Seguridad de la Información ha contado con la colaboración de Deloitte, consultora homologada por BSI para este tipo de trabajos.
La certificación BS7799-2/2002 consiste en el establecimiento de un marco demostrable de gestión y mejora continua de la seguridad, tanto tecnológica como no tecnológica. Esta seguridad se soporta mediante la implantación de controles (basados en el estándar ISO17799) para mitigar los riesgos relevantes identificados.

Ponentes:

< **Francisco García-Valero** es Jefe del Servicio de Soporte a Usuarios y Seguridad Informática, de la Oficina de Armonización en el Mercado Interior (OAMI), Agencia Europea encargada del registro de las marcas, dibujos y modelos comunitarios (http://oami.eu.int/es/design/default.htm) con sede en Alicante. Licenciado en Informática por la Universidad Politécnica de Madrid, Master in Bussines Administration por IMEA (Beçanson, Francia) y Master en Estudios Jurídicos Europeos del Instituto Europeo de Administración Pública (Luxemburgo), cuenta con quince años de experiencia tanto en el sector privado –Andersen Consulting (Madrid) y Société Générale de Surveillance (Ginebra, Suiza)– como también en la Administración Pública (la Comisión Europea y en la OAMI). Ha trabajado en producción de estadísticas monetarias con fines a la introducción del euro, así como en proyectos tecnológicos ligados a la publicación en Internet e infraestructura de teletrabajo. Actualmente, en la OAMI, es el secretario del Comité Director de TI y bajo su coordinación, la agencia se ha convertido en la primera administración pública europea en obtener la certificación BS7799.

< **Ángel Pujol de Lara** es Gerente de la división de ERS (Enterprise Risk Services) de Deloitte en la oficina de Madrid, a la que pertenece desde que ingresó en la firma en 1994. Ingeniero en Informática de Gestión por la Universidad Politécnica de Valencia, está en posesión de los títulos CISA y CISM y Lead Auditor (Certificado por BSI), es autor de artículos en diversas publicaciones informáticas y ha impartido clases en distintas Universidades. Cuenta con una amplia experiencia en todo tipo de sectores, entre ellos, Financiero, Gran Consumo, *Utilities*, Distribución y Fabricación Industrial y Administraciones Públicas. Posee una amplia experiencia profesional en Auditoría Informática y Gestión de Riesgos Tecnológicos, Implantación de medidas para la Certificación BS7799, Planes Directores de Seguridad y Planes de Recuperación de Negocio.

SISTEMA DE GESTIÓN UNIFICADA DE USUARIOS Y 'LOGIN' ÚNICO DE LA AUTORIDAD PORTUARIA DE BARCELONA

Sinopsis: El propósito de este proyecto en la Autoridad Portuaria de Barcelona es automatizar los procesos que proporcionan a los empleados el acceso a los servicios, gestionar desde un repositorio único (metadirectorio) dicha información, e integrar los distintos sistemas de información que hacen uso de la información e identidad del usuario con el metadirectorio, con objeto de reducir los costes administrativos y la cantidad de información incorrecta generada por errores de tipografía o sencillamente no introducida mediante los procesos manuales.

Ponentes:

< **Francesc Xavier Bonada** es Responsable de Sistemas y Atención a Usuarios dentro del Departamento de Sistemas de Información de la Autoridad Portuaria de Barcelona. Ingeniero Técnico de Telecomunicaciones y Master en Telecomunicaciones de la Empresa por la Universidad Ramón Llull, su experiencia profesional comenzó en 1990 en la multinacional Sony Corporation, para pasar al año siguiente a la Autoridad Portuaria de Barcelona, entidad en la que hasta el momento ha ido desarrollando las siguientes funciones: de 1991 a 1999, Jefe de proyectos de Telecomunicaciones (Departamento de Sistemas de Información); de 1999 a 2000, Jefe del Departamento de Telecomunicaciones, y desde 2001 hasta la actualidad, Responsable de Sistemas y Atención a Usuarios dentro del Departamento de Sistemas de Información.

MESA REDONDA

EL FUTURO DE LA FUNCIÓN DE SEGURIDAD DE LA INFORMACIÓN

Propósito: La seguridad de la información es una disciplina en rápida evolución, cuya práctica demanda perfiles profesionales con conocimientos cada vez más amplios y diversos. El fenómeno creciente del fraude aprovechando debilidades en los sistemas tecnológicos, el cumplimiento legal en materia de datos personales, la obligación de mantener la continuidad operativa ante contingencias, el requisito de proteger la información de negocio o actividad, y de usuarios, clientes, terceros e interesados, son una buena muestra de asuntos que afectan a toda la empresa y, en gran medida, a la función de seguridad de la información, históricamente nacida y ubicada en las áreas de tecnología. En la mesa redonda se debatirá acerca del futuro de dicha función y de los profesionales más directamente implicados: perfil de los expertos, atribuciones, dependencia, nuevos conocimientos, nuevas responsabilidades... En suma, se intentará vislumbrar una respuesta a la siguiente pregunta: ¿qué somos, y en qué nos convertiremos?

Intervienen:

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

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

> **Tomàs Roy Català** es, desde junio de 2004, Director del Área de Calidad y Seguridad en el Centro de Telecomunicaciones y Tecnologías de la Información de la Generalitat de Catalunya. Ingeniero Superior en Telecomuniciones, Ingeniero Superior en Electrónica y Licenciado en Ciencias de la Educación, Roy Catalá ha desarrollado su carrera profesional en Italia, en la *joint venture* Fiat GM Powertrain, en la que fue Responsable de Seguridad de las Informaciones y de Privacidad de Datos. Con anterioridad, en 2001, en tanto Responsable de un centro de investigación, dirigió proyectos de I+D en el ámbito del documento de identidad electrónico italiano. Tiene patentes sobre criptografía y autenticación fuerte. En 2000 fue Responsable del primer Master Italiano en Seguridad de los Sistemas, Informaciones y Aplicaciones. Complementa su formación en el area de Seguridad en los ámbitos de auditoría CISA, la Gestion de Seguridad CISSP, Seguridad de Sistemas Operativos MCSE y Certificaciones Cisco.

> **Javier Valdés Quirós** es director del departamento de Seguridad Informática de Bankinter. Ha desempeñado labores directamente relacionadas con la seguridad lógica desde el año 1981 en que, en Banco Herrero de Oviedo, desarrolló el área de Auditoría Informática. Se incorporó a Bankinter en esta misma función, que posteriormente desembocó en la puesta en marcha de un departamento con un enfoque de seguridad integral, y que, bajo el nombre de "Seguridad Corporativa", pretendía aunar las disciplinas de Seguridad Física y Seguridad Informática. Esta experiencia, interesante en su momento y portadora de valiosa experiencia, fue desechada al cabo de algunos años por no ser la mejor manera de resolver los problemas de seguridad (al menos en la entidad y circunstancias de aquel momento). De 1996 a 1999 dirigió los primeros avances de Bankinter en el desarrollo de opciones de negocio a través de Internet y construcción de la primera versión de web transaccional hasta su nombramiento como director del departamento de Seguridad Informática.

< Antonio Rodríguez de la Torre, Ingeniero Superior en Informática por la Universidad Politécnica de Cataluña, Licenciado en Administración y Dirección de Empresas (ADE) por la Universidad Oberta de Catalunya y CISSP. Con una experiencia de más de diez años en el sector TIC, actualmente es el responsable de la línea de competencia de Gestión de Identidad en gedas Iberia S.A. Anteriormente desarrolló su carrera profesional en el Instituto Catalán de Tecnología, CyberMedia Sistemas S.A., Metrolico, y en el departamento de Ingenieria de Sistemas, Automática e Informática Industria (ESAII) de la UPC.

IMPLANTACIÓN DE LA OFICINA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES DE LA GUARDIA CIVIL – PROYECTO BUHO

Sinopsis:
En esta ponencia la Dirección General de la Guardia Civil expondrá los motivos que le llevaron a constituir una Oficina de Seguridad de los Sistemas de Información y Comunicaciones, los objetivos del Proyecto BUHO de implantación de la Oficina, componente del Plan de Acción resultado del Plan de Sistemas de Información y Comunicaciones, qué ventajas espera obtener y sus particularidades.
La implantación de la Oficina conlleva a su vez la implantación de un Sistema de Gestión de la Seguridad de la Información, un cuadro de mando de seguridad y una herramienta que soporte la gestión de la seguridad.

Ponentes:

< Tomás Villalba de la Luz es Teniente Coronel de la Guardia Civil y Diplomado en Informática Militar. En la actualidad es el Jefe de la Oficina de Seguridad de los Sistemas de Información y Comunicaciones (OSSIC) de la Dirección General de la Guardia Civil.

< Jorge Laredo de la Iglesia es Consultor Senior de Seguridad TI en Indra. Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid (UPM) y Master en Dirección de Sistemas de Información y Comunicaciones por la Universidad Politécnica de Madrid, ocupa el cargo de Consultor Senior de Seguridad TI en Indra desde el año 1999, habiendo participado y dirigido múltiples proyectos en materia de seguridad, adecuación a la legislación de protección de datos, certificación electrónica y planes de contingencia en diferentes empresas y administraciones públicas.

TENDENCIAS EN TECNOLOGÍAS DE SEGURIDAD: ¿VAMOS POR EL BUEN CAMINO?

Sinopsis: Durante los últimos años hemos asistido a la constante aparición de nuevas tecnologías de seguridad. Algunas de ellas verdaderamente innovadoras y otras impulsadas por la constante obligación de la industria de sacar nuevos productos y versiones al mercado. Cortafuegos, IDS, IPS, sistemas de gestión de vulnerabilidades, de alerta temprana, de acceso remoto, autenticación robusta... ¿Estamos avanzando realmente en tecnologías de Seguridad? ¿Hasta qué punto es la tecnología tan importante? Durante la exposición se tratará de analizar la evolución y tendencias futuras de las tecnologías de seguridad y se intentará ver cómo encajan éstas con las necesidades reales que el autor detecta en el mercado español de seguridad, contando para ello con opiniones anónimas de algunos de sus clientes.

Ponente:

< Jorge Hurtado Rojo es Director Comercial de Germinus. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid, su carrera profesional ha girado en torno a la seguridad informática, pasando de ser Consultor de Seguridad en Quark Software and Services a Responsable del Área de Seguridad de SGI (Grupo GMV) en 1998, hasta que en 2001 pasa a Germinus XXI como Director de Desarrollo de Negocio, siendo nombrado en 2004 Director Comercial. A lo largo de su carrera ha participado en numerosos proyectos, desde las primeras implantaciones en nuestro país de sistemas de seguridad perimetral, pasando por la implantación de sistemas de PKI o la redacción de Planes y Políticas de Seguridad.

SESIÓN DE CLAUSURA

LA PROGRESIÓN DEL FRAUDE EN SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

Enfoque: Las TI avanzan sin fronteras para todos, tanto es así que el mundo delincuencial lo sabe y despliega ampliamente su quehacer en los medios telemáticos. En lo que respecta a los Cuerpos y Fuerzas de Seguridad del Estado en el ámbito de los delitos económicos, su trabajo se ha visto desbordado por aquellas formas delictivas dedicadas a capturar datos sensibles y de interés que pueden ser reutilizados en perjuicio de los usuarios y de las entidades e instituciones que operan en Internet.
Estos nuevos delincuentes tienen conocimiento de que la aceleración cotidiana deja de lado comprobaciones y actos de seguridad mínimos, que cualquier usuario de la red podría/debería ejercer, aprovechándose en beneficio propio, ofertando servicios inexistentes y suplantando a los reales. Ante estas circunstancias ¿qué se hace y se podría hacer "desde el otro lado" para evitar tanto perjuicio global en crecimiento continuo?

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. Ingresó 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.

Enfoque: Desde la pasada edición de Securmática en 2004, en la que el Grupo de Delitos Telemáticos de la Guardia Civil trató el por entonces emergente fenómeno del *phishing*, éste se ha disparado. Lo que en 2004 fue novedoso, hoy es habitual por la incidencia tan alta que ha tenido. Su crecimiento ha sido posible por la diversificación de los procesos del *phishing*. Del inicial correo indiscriminado con enlace a página bancaria fraudulenta para obtener datos de usuario de banca electrónica, y la inmediata suplantación de personalidad para ordenar transferencias a bancos en paraísos fiscales, se ha pasado a técnicas más elaboradas de obtención de los datos, buscando mejores coberturas que induzcan al error en el usuario, y a la diversificación de sistemas de recogida de dinero apoyado en redes internacionales de países del Este, destino final del fraude y, presumiblemente, origen de la estrategia del *phishing*. Es también en estos países donde empiezan a sonar con fuerza los *blackmail*, técnicas que al más puro estilo mafioso, intentan conjugar la extorsión y el *hacking*, conscientes de la importancia de los sistemas informáticos en la empresa como soportes de su activo patrimonial más importante, la información.
Paralelo a todo ello, no han faltado los que aprovechando la ingenuidad, ambición o sentimiento de solidaridad han ideado y buscado nuevas fórmulas para "timar" a los ciudadanos. Qué duda cabe que este año se nos ha dibujado un panorama cuanto menos interesante a nivel policial, pero a nivel usuario, ciertamente desalentador.

Ponente:

< Juan Salom es Jefe del Grupo de Delitos Telemáticos de la Unidad Central Operativa de la Policía Judicial de la Guardia Civil. Comandante de la Guardia Civil con destino actual en la Unidad Central Operativa de Policía Judicial de la Guardia Civil, Salom inició su trayectoria profesional 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.

SECURMATICA, a escena

Panorámica de SECURMÁTICA 2004

Premios SIC 2005

En coincidencia con la celebración de la XVI edición de Securmática, tendrá lugar el acto de entrega de los II 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 primera edición de los premios SIC

LA HORA DEL REENCUENTRO Y LOS RECONOCIMIENTOS

Cena de celebración

SECURMATICA

XVI Congreso español de Seguridad de la Información 2005

AFORO LIMITADO

Fechas y lugar

SECURMÁTICA 2005 tendrá lugar los días 26, 27 y 28 de abril de 2005 en el hotel NOVOTEL*. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2005 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 II Premios SIC (27 de abril)
- Diploma de asistencia

Cuota de inscripción

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

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

Descuentos:

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

Proceso de solicitud de inscripción

- Por teléfono: +34 91 575 83 24 / 25
- Por fax: +34 91 577 70 47
- Por correo electrónico: info@securmatica.com
  info@codasic.com
- Por sitio web: **www.securmatica.com**
- Por correo convencional: envíe el Boletín adjunto o fotocopia del mismo a:

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

- Abone la cantidad correspondiente mediante cheque nominativo a favor de **Ediciones CODA, S.L.**, que deberá ser remitido a la dirección de Ediciones CODA, o
- Transferencia bancaria, cuya fotocopia deberá ser remitida vía fax o correo, a nombre de:

  EDICIONES CODA, S.L.
  CAJA DE MADRID
  Oficina: Avda. de Felipe II, 15
  28009 Madrid (España)
  C.C.C.: 2038 1726 67 6000477427

- * Existen descuentos del hotel Novotel para los congresistas que deseen alojarse en el mismo con motivo de su asistencia a Securmática.
- Las inscripciones sólo se considerarán formalizadas una vez satisfecho el importe de las mismas antes de la celebración del Congreso.
- Las cancelaciones de inscripción sólo serán aceptadas hasta 7 días antes de la celebración del Congreso, y deberán comunicarse por escrito a la entidad organizadora. Se devolverá el importe menos un 10% por gastos administrativos.

Boletín de inscripción a Securmática 2005

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 26 ❑ MÓDULO 2 DÍA 27 ❑ MÓDULO 3 DÍA 28 ❑ Deseo inscribirme a SECURMATICA 2005

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**