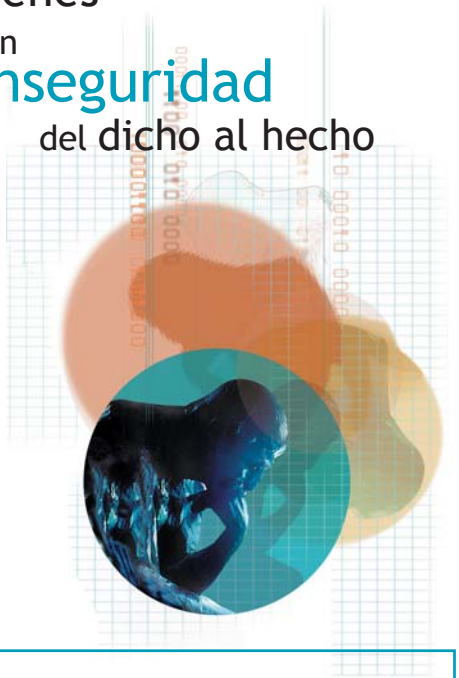
SECURMATICA 2003

para
quienes
entienden
de **inseguridad**
del dicho al hecho



COPATROCINADORES:

bmcsoftware — Assuring Business Availability™
Computer Associates
Deloitte & Touche
Ernst & Young — Quality In Everything We Do
IBM
Indra
NOKIA — Connecting People
SAFELAYER
SGI — Soluciones Globales Internet
steria
symantec.
Telefónica Data

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, 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 23 de abril de 2003

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

10:00h. **Conferencia de apertura:** Nuevos horizontes en la protección de datos personales
Ponente: **José Luis Piñar Mañas,** Director de la Agencia de Protección de Datos
10:30h. Coloquio

10:40h. **Ponencia:** El Plan Director de Seguridad de la Información y Comunicaciones
Ponente: **Javier García Carmona,** Director de Seguridad de la Información y Comunicaciones de Iberdrola
11:15h. Coloquio
11:20h. Pausa-café

11:50h. **Ponencia:** El cuadro de mando de seguridad de la información
Ponente: **Juan Carlos Gómez Castillo,** Gerente de Seguridad de la Información. Dirección de Seguridad de la Información y Prevención de Fraude. Telefónica S.A.
12:25h. Coloquio

12:30h. **Ponencia:** Plan de contingencia: replicar y organizar
Ponente: **Celso Álvarez Movilla,** Responsable de Seguridad entorno Host y Autoservicio de La Caixa
13:05h. Coloquio

13:10h. **Mesa redonda:** Cómo se entiende hoy la protección de la información en las organizaciones.
La visión de los responsables de seguridad
Intervienen:
– **Miguel A. Guzmán,** Responsable de Seguridad de Fremap Mutua de Accidentes de Trabajo
– **Antonio Martín,** Jefe de Seguridad Informática de Renfe
– **José Antonio Castro,** Director de Seguridad Informática de Santander Central Hispano
14:25h. Coloquio
14:30h. Almuerzo

16:30h. **Ponencia:** Políticas, planes y normativas de seguridad: ¿de qué estamos hablando?
Ponente: **Rafael Ortega,** Director de Enterprise Risk Services de Deloitte & Touche
17:05h. Coloquio

17:10h. **Ponencia:** Cómo justificar hoy las inversiones en seguridad informática ante la alta dirección
Ponentes: – **Jesús Merino,** Socio Responsable del área de Technology & Security Risk Services de Ernst & Young
– **Daevid A. Lane,** Socio del área de Technology & Security Risk Services de Ernst & Young
17:45h. Coloquio
17:50h. Pausa-café

18:10h. **Ponencia:** Estructura organizativa global de seguridad de la información. Deutsche Bank.
Ponente: **Miguel Ángel Hervella,** Director de Riesgos de Información de Deutsche Bank SAE
18:45h. Coloquio

18:50h. **Ponencia:** El papel de los administradores de seguridad en la organización de la seguridad de una empresa
Ponente: **Jaime de Pereda,** Planificación y Arquitectura de Sistemas y Seguridad. Sistemas de Información. Amena
19:25h. Coloquio
19:30h. Fin de la primera jornada

NUEVOS HORIZONTES EN LA PROTECCIÓN DE DATOS PERSONALES

Sinopsis: la protección de datos de carácter personal es una cuestión clave dentro del marco del respeto a los derechos fundamentales y del desarrollo de las nuevas tecnologías, así como de la evolución de iniciativas empresariales del más variado tipo. Ello hace imprescindible impulsar el correcto conocimiento de la legislación sobre protección de datos al objeto de garantizar su aplicación y cumplimiento. Se trata de establecer, generalizar y normalizar la que podríamos llamar cultura de la protección de los datos personales, que hoy se percibe como algo distante y gravoso. Para ello la Agencia de Protección de Datos pondrá en marcha cuantas iniciativas sean necesarias para incrementar la seguridad jurídica en el sector y facilitar el conocimiento de la legislación vigente.

Ponente: **José Luis Piñar Mañas** es director de la Agencia de Protección de Datos. Doctor en Derecho por la Universidad Complutense de Madrid y Abogado del Ilustre Colegio de Abogados de Madrid (en la actualidad no ejerciente), ha sido Profesor Titular de Derecho Administrativo de la Universidad Complutense de Madrid, Catedrático excedente de Derecho Administrativo de la Universidad de Castilla-La Mancha, Catedrático excedente en la Universidad San Pablo CEU de Madrid, y Decano de las Facultades de Derecho de estas Universidades. En la actualidad es Presidente de la Junta de Garantías Electorales del Consejo Superior de Deportes, Consejero asesor del Centro de Fundaciones, miembro del Secretariado Permanente de la UIBA y Vocal de la Comisión General de Codificación.

EL PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES

Sinopsis: el plan director de seguridad de la información ha de identificar y evaluar los niveles de riesgos y controles existentes dentro de la Organización, definiendo la estrategia de seguridad sobre la Información y estableciendo una serie de mejoras y proyectos a acometer, con el objeto de alinear el nivel de riesgo global asociado de los Activos de Información. Pero a la hora de poder confeccionar el Plan Director de Seguridad se ha de crear un continente y desarrollar un contenido sin dejar aparcado ninguno de los tres pilares fundamentales sobre los que éste se ha soportar.

Ponente: **Francisco Javier García Carmona**. Director del departamento de Seguridad de la Información y Comunicaciones de Iberdrola desde 2001, año en el que se incorporó a esta compañía. García Carmona inició su actividad en 1982 en el sector de las Telecomunicaciones pasando a dirigir este departamento en diversas empresas del sector, incorporándose al mundo de la Seguridad en el año 96, simultaneando la Dirección de Operaciones con funciones técnicas.

EL CUADRO DE MANDO DE SEGURIDAD DE LA INFORMACIÓN

Sinopsis: una actividad no puede gestionarse si no puede ser medida. El cuadro de mando de seguridad de la información, más que un conjunto de métricas de seguridad, es una herramienta de control de gestión que traduce la estrategia en un conjunto de objetivos de seguridad relacionados entre sí, medidos a través de indicadores y ligados a unas iniciativas. El cuadro de mando traslada la visión de los responsables de seguridad en objetivos medibles, permitiendo priorizar los planes de acción y ayudando en la toma de decisiones. En la ponencia se tratarán todos los componentes de un cuadro de mando de seguridad de la información, la necesidad y utilidad del mismo, el enfoque y los factores de éxito para su creación en una gran empresa. Es un elemento fundamental para contestar a la simple y temida pregunta de su presidente: «¿y…cómo vamos en seguridad?».

Ponente: **Juan Carlos Gómez Castillo**. Ingeniero Superior de Telecomunicación por la UPM, CISA y miembro de ISACA. Actualmente es Gerente de Seguridad de la Información en Telefónica S.A. Previamente ha sido Responsable de Seguridad en Sistemas de Información de Telefónica Data España, British Telecom España (incluido ISP) y Servicom, y ha trabajado también como consultor y jefe de proyectos de seguridad en Telefónica Sistemas y TPTI.

PLAN DE CONTINGENCIA: REPLICAR Y ORGANIZAR

Sinopsis: el desarrollo de un Plan de Contingencia Informático que permita la continuidad del negocio, es una labor con un elevado porcentaje de componente técnico, pero para asegurar su éxito deberemos atender a temas organizativos y de arquitectura de aplicaciones:

- ¿Hemos diseñado y tenemos actualizado el circuito de escaladas?
- ¿Tenemos documentados los criterios para decidir si se conmuta al centro secundario?
- ¿Tenemos documentados y actualizados los procedimientos técnicos que se han de activar en la conmutación al centro secundario?
- ¿Saben los empleados cómo deben trabajar si el CPD no está disponible?
- ¿Podrán seguir operando nuestros clientes mientras el CPD no está disponible?
- ¿Están nuestros puestos de trabajo y terminales preparados para trabajar sin conexión?
- ¿Tenemos datos para procesar las transacciones no recuperadas en la conmutación?

Ponente: **Celso Álvarez Movilla**. Licenciado en Matemáticas, se ha dedicado profesionalmente a la Informática desde principios de los 80, trabajando casi en exclusiva para entidades financieras. Ha sido responsable de aplicaciones de Medios de Pago, Internet y ahora desarrolla su labor como responsable de Seguridad entorno Host y Autoservicio de La Caixa.

MESA REDONDA

CÓMO SE ENTIENDE HOY LA PROTECCIÓN DE LA INFORMACIÓN EN LAS ORGANIZACIONES. LA VISIÓN DE LOS RESPONSABLES DE SEGURIDAD.

Propósito: en esta mesa redonda, tres expertos en la disciplina de la seguridad informática darán su opinión profesional acerca de los cambios que ha experimentado en los últimos años la concepción empresarial de la función específica de la seguridad de la información hasta llegar a su papel actual, cada vez más ligado a la gestión de riesgos en los sistemas de información tecnológicos.

Se abordarán, entre otros, los siguientes puntos de interés: dependencia jerárquica de la función, visión actual de la seguridad en el departamento de sistemas de información y en otros departamentos de la entidad, forma en la que los gestores de una entidad entienden los riesgos de seguridad TIC, dedicación de recursos internos, formación, e impacto del cumplimiento de la LOPD, del Reglamento de medidas de seguridad, y de otras leyes y normas.

Participantes:

– **Miguel A. Guzmán**. Responsable de Seguridad de Fremap desde enero de 2001. Ha desarrollado su carrera profesional en esta compañía en la que ha prestado servicio como Jefe de Explotación (1982-1995), Jefe de Gestión del Entorno Distribuido (1995-1996) y Jefe de Integración de Sistemas (1996-2000). En dichas funciones siempre ha tenido contacto directo con distintos proyectos vinculados con la seguridad de la información.

...MESA REDONDA

– **Antonio Martín Moreno**. Responsable de Seguridad Informática de Renfe desde 1996. Martín Moreno ingresó en esta compañía en 1962, con Maestría Industrial, pasando al campo de la Informática en el año 1973 como Operador. Ha participado en distintas conferencias sobre seguridad e impartido cursos en la Escuela de Informática Francisco de Vitoria y el Colegio de Ingenieros de Madrid.

– **José Antonio Castro González** es Director de Seguridad Informática de Santander Central Hispano. Ha desarrollado la práctica totalidad de su carrera profesional en tecnologías de la información (16 años) en esta institución financiera, primero como consultor del área internacional y luego como responsable de diferentes áreas técnicas. Cuenta con 10 años de experiencia en el mundo de la seguridad de la información.

POLÍTICAS, PLANES Y NORMATIVAS DE SEGURIDAD: ¿DE QUÉ ESTAMOS HABLANDO?

Sinopsis: llegados al punto en el que la visión de la seguridad se comienza a entender como un proceso de mejora permanente y no como un estado en el tiempo, según lo demuestran las tendencias más recientes, y en particular el tan últimamente nombrado ISO/IEC 17799, queremos compartir nuestra visión de lo que entendemos como los pilares básicos de la gestión de la seguridad: la **planificación estratégica** que la *dirige*, las **políticas y normativas** para *soportarla* y los **procesos operativos** para *llevarla a cabo*. Todo ello bajo el prisma de la "calidad total", elemento fundamental para lograr certificar la "calidad de la seguridad".

Ponente: **Rafael Ortega**. Director responsable de Seguridad y PKI del Área de Enterprise Risk Services en Deloitte & Touche España, S.L. Ortega ha dirigido y participado en numerosos proyectos de seguridad de los Sistemas de Información, de planificación estratégica de sistemas de información, en proyectos relacionados con PKI, Planes Estratégicos de Seguridad, Desarrollo y Soporte a Planes de Contingencia, Diagnósticos de Seguridad y Análisis de Riesgos.

CÓMO JUSTIFICAR HOY LAS INVERSIONES EN SEGURIDAD INFORMÁTICA ANTE LA ALTA DIRECCIÓN

Sinopsis: se ha producido un cambio cultural claro en lo que a la seguridad informática se refiere, promovido inicialmente por los efectos potenciales del año 2000, seguido por la legislación sobre datos personales y por último por las consecuencias del 11-S. Jamás ha existido tanta amenaza para la empresa como consecuencia de una seguridad informática débil y fácilmente vulnerable. Hoy, más que nunca, el público y los mercados exigen que las organizaciones tengan una seguridad informática robusta y, en consecuencia, ésta se ha convertido en un activo cada vez más claro en los negocios. En la ponencia se intentará analizar cómo la Dirección puede convertir la seguridad informática en un valor estratégico.

Ponentes:

– **Jesús Merino Fernández**. Socio de Ernst & Young, responsable del área Technology and Security Risk Services (TSRS). Merino es Licenciado en Ciencias Económicas y Empresariales por la Universidad Complutense de Madrid, Censor Jurado de Cuentas y auditor CISA. Cuenta con 25 años de experiencia en la actividad de auditoría, 20 de los cuales dedicados a la revisión de sistemas de seguridad y auditoría informática.

– **Daevid A. Lane**. Socio del departamento de Technology and Security Risk Services de Ernst & Young. Lane es Licenciado en Ciencias Físicas, miembro del Institute of Chartered Accountants in England and Wales, auditor CISA y asociado a la ISACA. Tiene más de 15 años de experiencia en la actividad de auditoría informática en Inglaterra y España. Sus responsabilidades actuales abarcan las siguientes líneas de negocio de seguridad: servicios de intrusiones por Internet, firma digital (PKI, VPN, proyectos Identrus) y la elaboración de planes de continuidad de negocio con un gran énfasis en el sector de banca.

ESTRUCTURA ORGANIZATIVA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN. DEUTSCHE BANK

Sinopsis: para las organizaciones multinacionales, independientemente de su tamaño, la gestión de la seguridad de la información ha sufrido grandes cambios en los últimos años. Se ha pasado de un conjunto de islas interconectadas a redes globales en las que intervienen múltiples operadores y colaboradores. Las aplicaciones son ahora desarrolladas, instaladas y mantenidas por equipos humanos ubicados en diferentes países. Los usuarios han incrementado su conocimiento técnico, siendo exigentes en cuanto a prestaciones y funcionalidad, pero más reacios en cuanto a control. La tecnología avanza en diferentes caminos, incrementando día a día la complejidad de las soluciones. Habida cuenta de lo dicho, ¿cómo se debe de gestionar la información para evitar amenazas?

En este escenario, es necesario instrumentar un sistema organizativo de seguridad de la información que permita mantener unos niveles de riesgo bajos en la operativa diaria. La alternativa entre centralización y descentralización, las normas de obligado cumplimiento frente a permisividad, la injerencia frente a la autonomía, el uso de metodologías comunes o específicas, las necesidades legales y las diferencias organizativas de cada país, configuran una ecuación de difícil resolución.

Ponente: **Miguel Ángel Hervella**. Director de Riesgos de Información de Deutsche Bank para España desde el año 2000. Hervella es Ingeniero Superior de Telecomunicaciones por la UPC. Su trayectoria profesional le aporta experiencia laboral en multinacionales, pymes y como profesional liberal. Hasta el año 1996 ejerció como Jefe de Sistemas en Rank Xerox Española en las áreas de redes e impresión electrónica. Inició después una etapa en consultoría informática asociada a la gestión del cambio en la organizaciones. Posteriormente, y como consultor, se especializó en seguridad informática, desarrollando planes de seguridad informática para diversas entidades.

EL PAPEL DE LOS ADMINISTRADORES DE SEGURIDAD EN LA ORGANIZACIÓN DE LA SEGURIDAD DE UNA EMPRESA

Sinopsis: la administración de seguridad requiere personal con un nivel de conocimiento y sensibilización diferente al de otros administradores por lo que es una función que se puede concentrar en un grupo especializado. Conviene detallar qué tareas debe realizar y cómo se relaciona con otros grupos de la empresa, ya que su ámbito de actuación está a caballo entre la operación de sistemas y la atención al usuario interno. Las diferentes alternativas sobre cómo establecer un grupo de administración de seguridad varían desde que sus componentes sean personal de la empresa hasta que sea un servicio que se subcontrate enteramente a otras compañías.

Ponente: **Jaime de Pereda Huelves**. Presta sus servicios en Planificación y Arquitectura de Sistemas y Seguridad, en el área de Sistemas de Información de Amena. Ingeniero Superior de Telecomunicación, De Pereda comenzó su carrera profesional en el Grupo Universitario de Tarjeta Inteligente, de la UPM, 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.

SEGUNDO MÓDULO 24 de abril de 2003

09:15h. Entrega de documentación
09:30h. **Ponencia:** El beneficio de una gestión de usuarios efectiva. La experiencia de EDS con eTrust Admin
Ponentes:
– **Carmen García González,** Gerente de Seguridad de EDS para el Sur de Europa
– **Josep Micolau,** CISSP. Responsable de Desarrollo de Negocio del Área de Seguridad de Computer Associates
10:10h. Coloquio
10:15h. **Ponencia:** La correlación inteligente de eventos
Ponente: **Pedro Castillo,** Director Técnico de Seguridad Informática de Bankinter
10:50h. Coloquio
10:55h. Pausa-café
11:25h. **Ponencia:** Un modelo de empresa digital segura: eOficina Telefónica Data
Ponentes:
– **Ángel Barrio,** Subdirector Oficina eBA (eBusiness + Banda Ancha) del Área de Coordinación y Apoyo al Desarrollo. Telefónica Data.
– **Juan Miguel Velasco,** Subdirector de Ingeniería de Proyectos y Servicios de Protección de la Información. Telefónica Data España.
12:00h. Coloquio
12:05h. **Ponencia:** El Plan Director de Seguridad Lógica en el Ciclo de Vida de los Sistemas de Información
Ponente: **Carlos Capmany**, Responsable corporativo del Plan Director de Seguridad Lógica. Seguridad Lógica Corporativa. BBVA.
12:40h. Coloquio
12:45h. **Mesa redonda:** Seguridad TIC: hacia una integración más especializada
Intervienen:
– **Miguel Ángel de Cara,** Responsable del Área de Seguridad. Barcelona. Davinci
– **Luis Jara,** Responsable de eSecurity de Gedas Iberia
– **Jorge Hurtado,** Director de Desarrollo de Negocio del Área de Seguridad de Germinus
– **Manuel Urbán,** Director de Tecnología de GFT Iberia Solutions
– **Jesús Rodríguez,** Director General de Realsec
– **Facundo Rojo,** Director de Consultoría del Dpto. de Administración de las Aplicaciones y Seguridad de Selesta
– **Fernando Vega,** Director de Consultoría de Grupo SIA
– **Pedro Merino,** Director de Consultoría de Redes y Seguridad de Telindus
14:00h. Coloquio
14:15h. Almuerzo
16:15h. **Ponencia:** Gestión centralizada de usuarios en CCM: un proyecto posible
Ponentes:
– **Faustino Villarrubia,** Jefe de Seguridad y Control de Proceso de Datos Caja Castilla La Mancha
– **Víctor Mojarrieta,** Director de Soluciones de Seguridad. Región Sur de Europa. BMC Software
16:50h. Coloquio
16:55h. **Ponencia:** Aena: implantación del sistema de seguridad en centros de control y torres
Ponentes:
– **Narciso Pérez Llera,** Responsable de Proyectos de Automatización. División de Automatización de Navegación Aérea de Aena
– **José Gros,** Director para España de Nokia Internet Communications
17:30h. Coloquio
17:35h. Pausa-café
17:55h. **Mesa redonda:** Sistemas integrados de seguridad multifunción y multifabricante: ¿para qué y por qué?
Intervienen:
– **Pedro Galatas,** Director de Desarrollo de Negocio de Afina
– **Camilo Vaquero,** Director de Estrategia y Desarrollo de Negocio de Aladdin
– **José Manuel Cea,** Director de Check Point Software Technologies España
– **Manuel Arrevola,** Director de Internet Security Systems
– **Carlos Jiménez,** Presidente de Secuware
– **Vesku Turtia,** Consejero Delegado de Stonesoft España
– **Xabier Mitxelena,** Director Gerente de S21sec
– **Mario Velarde,** Director General de Trend Micro
19:15h. Coloquio
19:30h. Fin de la segunda jornada
20:30h. **Cena de la XIV edición de Securmática**

EL BENEFICIO DE UNA GESTIÓN DE USUARIOS EFECTIVA. LA EXPERIENCIA DE EDS CON eTRUST ADMIN.

Sinopsis: la administración efectiva de usuarios es un requisito que hay que abordar cuando la magnitud, distribución geográfica y disparidad de entornos hacen evidente el gran coste y la falta de procedimientos efectivos. La concepción actual del negocio, con gran movilidad de usuarios y cambios organizativos frecuentes ponen de nuevo en evidencia la necesidad de buscar soluciones en este área. EDS presentará la experiencia en la implementación de eTrust Admin como plataforma de administración centralizada de usuarios, en cuyo ámbito de actuación administra a más de 2.700 empleados propios, distribuidos en centros de trabajo de Barcelona, Madrid, Oviedo, Valencia, Valladolid y Zaragoza. En el curso de la ponencia, se detallarán las necesidades identificadas que motivaron a EDS a adoptar esta solución, el procedimiento de implementación y los beneficios que se derivan de la utilización de esta solución de administración centralizada de Computer Associates.

Ponentes:

– **Carmen García González**. Gerente de Seguridad de EDS para el sur de Europa. Licenciada en Ciencias Matemáticas por la Universidad de Zaragoza, inició su carrera profesional en EDS (1982) como ingeniero de software en grandes sistemas, pasando por soporte técnico a ventas y llegando en 1989 a encabezar el área de seguridad para España y Portugal. Durante estos años ha desempeñado también funciones de consultoría y auditoría, llegando al momento actual en el que además de responsable de Seguridad para el sur de Europa, es responsable de coordinación de proyectos corporativos de seguridad para Europa, Medio Este y África.

– **Josep Micolau**. Licenciado en Matemáticas por la Universidad de Barcelona y CISSP, sus principales funciones como Responsable de Desarrollo de Negocio del Área de Seguridad de Computer Associates se centran en la promoción de las soluciones de seguridad de esta compañía 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, y la divulgación del catálogo de soluciones tecnológicas de seguridad entre los integradores y socios de Computer Associates.

LA CORRELACIÓN INTELIGENTE DE EVENTOS

Sinopsis: orientar los trabajos de revisión de los eventos de seguridad en una mediana o gran empresa puede ser una labor inabordable, dados los altísimos volúmenes de información que generan sistemas, aplicaciones y elementos propios de la seguridad (cortafuegos, IDS, antivirus, etc.). Estos eventos crecen en volumen y formato a medida que disponemos de más elementos que controlan la seguridad de la empresa. ¿Cómo sacar conclusiones que nos permitan conocer el estado de la seguridad de la compañía? La correlación de eventos proporciona un marco sobre el que trabajar y llegar a dar solución al problema, pero, ¿cómo generar las reglas de correlación sobre la estructura de nuestra compañía? Y lo más importante, ¿cómo conseguir que nuestro sistema de correlación de eventos no trabaje únicamente con reglas fijas y predefinidas sino que en su lugar «entienda» qué eventos u operaciones son normales y cuáles no? Añadir «inteligencia» al proceso es el reto al que nos enfrentamos y del que se hablará en la ponencia.

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

UN MODELO DE EMPRESA DIGITAL SEGURA: eOFICINA TELEFÓNICA DATA

Sinopsis: eOficina es un proyecto piloto en Telefónica Data dentro de la iniciativa empresa 2004, que pretende demostrar y poner en práctica las nuevas capacidades de los servicios eBA sobre banda ancha, y desplegar una serie de aplicaciones de valor añadido como multivideo conferencia, aplicaciones en red vía Citrix (Office, correo, etc.), autenticación segura robusta con capacidades de itinerancia *(roaming)* y ubicuidad de los empleados/usuarios, permitiendo el acceso a todas las aplicaciones y servicios de la empresa desde cualquier localización, sea Internet , Extranet o Intranet. eOficina integra los servicios DataOficina y correo colaborativo (Lotus-Exchange) de Telefónica Data, mediante la aplicación de la solución de SSO basada en *tokens* USB permitiendo el *logon* único en aplicaciones web y en aplicaciones no web, lo que facilita una gestión centralizada de las aplicaciones así como de la seguridad.

Ponentes:

– **Ángel Barrio**. Subdirector de Coordinación y Apoyo al Desarrollo de la Oficina eBA, de Telefónica Data España desde agosto de 2001. La oficina eBA es la unidad encargada de coordinar la estrategia y desarrollos de e-Business y Banda Ancha para grandes empresas y administraciones públicas en el Grupo Telefónica. Ingeniero de Telecomunicación por la UPC y Diplomado en Ciencias Empresariales por la UNED, Barrio se incorporó a Telefónica Data en 1988, y desde entonces ha desempeñado diversas responsabilidades nacionales e internacionales. Con anterioridad trabajó durante 7 años en Telefónica I+D.

– **Juan Miguel Velasco López-Urda**. Subdirector de Ingeniería de Proyectos y Servicios de Protección de la Información de Telefónica Data España. Anteriormente fue director técnico y de consultoría de la Agencia de Certificación Electrónica (ACE), sociedad filial de Telefónica Data. Hasta a su incorporación a ACE, Velasco –que cursó sus estudios de informática en la UPM– ejerció como responsable de la Alianza entre Telefónica Data y VeriSign y como gestor de Proyectos en Telefónica DataCorp. Asimismo, ha venido desarrollando su carrera profesional dentro del Grupo Telefónica, desempeñando diversos puestos en TSAI y Telefónica Data España.

EL PLAN DIRECTOR DE SEGURIDAD LÓGICA EN EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN

Sinopsis: dentro del marco del Plan Director de Seguridad Lógica se han definido una serie de proyectos e iniciativas encaminadas a supervisar el estado de la seguridad en el ciclo de vida productivo de los sistemas de información, desde que se realiza el análisis de viabilidad de un servicio hasta que se implanta en explotación. Dentro de este ciclo se describen las iniciativas adoptadas en las fases de Análisis de Viabilidad, Análisis Funcional y Orgánico, Generación de Código, Pruebas Unitarias, Pruebas Integradas, Infraestructuras de Soporte e Implantación.

Ponente: **Carlos Capmany**, Responsable corporativo del Plan Director de Seguridad Lógica. Seguridad Lógica Corporativa. BBVA.

Ingeniero Superior de Telecomunicación por la UPM, posee las certificaciones CISA y CISSP. Antes de ocupar su función actual, desde 1997 ha trabajado en seguridad lógica como consultor en Telefónica Sistemas y TPTI, Jefe de Implantación y Gestión de Seguridad de SI en Telefónica de España, Responsable Técnico de Seguridad de SI en uno-e y Responsable de Gestión de Riesgos de Seguridad de SI en BBVA Europa.

MESA REDONDA

SEGURIDAD TIC: HACIA UNA INTEGRACIÓN MÁS ESPECIALIZADA

Propósito: en la misma medida en que los usuarios han ido emprendiendo iniciativas de implantación de seguridad técnica en sus sistemas de información, ha ido creciendo un pujante ramo de compañías especializadas –exclusivamente o no– en la integración de tecnologías de seguridad y en el diseño y adaptación de soluciones corporativas.

Las preguntas principales a las que los miembros de la mesa redonda habrán de contestar son las siguientes: ¿Se necesitan integradores especializados? ¿Existe alguna receta para distinguir a los integradores con experiencia y vocación de permanencia en el mercado de protección de la información de aquellos otros que sólo ven en él una moda pasajera o una oportunidad para paliar la recesión que atraviesa el sector de tecnologías de la información?

Participantes:

– **Miguel Ángel de Cara**. Ingeniero en Informática por la UPC, es responsable de proyectos en el Area de Seguridad y Calidad de Servicio de Davinci. Cuenta con una amplia experiencia en la implantación y desarrollo de proyectos relacionados con normativa y estandar ISO 17799, auditorías, consultorías e emplantación de soluciones de seguridad.

– **Luis Jara Díaz-Aguado**. Responsable de la unidad de negocio e-Security de gedas iberia. Cursó estudios en la Facultad de Ciencias Económicas y Empresariales de Barcelona. Ha trabajado en ASICOM y en el Grupo ADD, desde donde introdujo en España marcas punteras como Check Point, e-Safe, Internet Security Systems, Baltimore, Valicert. En 2001 se incorporó a gedas iberia para desarrollar la línea de negocio de seguridad telemática.

– **Jorge Hurtado**. Director de Desarrollo de Negocio del Área de Seguridad de Germinus. Ingeniero de Telecomunicaciones por la UPM, ha dedicado su carrera profesional a la seguridad informática. Ha trabajado en Quark Software & Services como consultor de seguridad informática, y en Grupo GMV donde ejerció como Director del Área de Seguridad de SGI.

– **Manuel Urbán**. Director de Tecnología de GFT Iberia. Posee más de 20 años de experiencia en el área de Tecnología y Sistemas de Información. Ingeniero Industrial por la UPC con formación complementaria en TI, Urbán ha desarrollado sus funciones en empresas como Seat, Banco Atlántico, Banco Comercial Transatlántico y Deutsche Bank.

– **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.P.I. 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.

– **Facundo Rojo**. Director de la Unidad de Negocio de Seguridad Informática de Selesta desde 1999. Ingeniero T. Químico y Licenciado en Informática por la UPC y auditor CISA, Rojo ha sido Director de Soporte de IS en Nestlé España, Responsable de los proyectos de Diseño e Implantación de Tecnología y Seguridad Informatica en los JJOO de Barcelona y Director del CPD Olímpico. En 1993 inició su colaboración con Selesta.

...MESA REDONDA

– **Fernando Vega**. Director de Consultoría del Grupo SIA desde 2001. Ingeniero Superior de Telecomunicación por la UPM, Vega posee las certificaciones CISA y CISSP. Tras su paso por Andersen Consulting, la mayor parte de su carrera profesional ha estado vinculada al mundo de la seguridad informática, principalmente en el Grupo Telefónica como consultor, jefe de proyectos y Gerente de Seguridad en SI en Telefónica de España.

– **Pedro Merino.** Director del Departamento de Consultoría de redes y seguridad y miembro del Consejo de Dirección de Telindus, S.A. Ingeniero Superior de Telecomunicación por la Universidad Politécnica de Madrid y Executive M.B.A por el Instituto de Empresa, cuenta con una amplia experiencia en el ámbito del diseño y consultoría de redes de comunicaciones e infraestructuras de seguridad complejas.

GESTIÓN CENTRALIZADA DE USUARIOS EN CCM: UN PROYECTO POSIBLE

Sinopsis: la ponencia pretende mostrar, a través de la experiencia de Caja Castilla La Mancha, que la gestión de identidades es un proyecto viable, que genera beneficios indudables para las organizaciones y donde el secreto del éxito estriba en una suma de componentes tanto de gestión como tecnológicos, que están al alcance de todos. Se expondrán los retos de negocio, organizativos o tecnológicos que CCM ha sabido superar, cómo se ha llevado a cabo el proyecto –asentado tecnológicamente en la solución Control-SA de BMC Software– para, finalmente, hacer balance de los beneficios obtenidos y describir los pasos a dar en el inmediato futuro.

Ponentes:

– **Faustino Villarrubia**. Jefe de Seguridad y Control de Proceso de Datos de Caja Castilla La Mancha. Licenciado e Ingeniero en Informática por la Universidad Politécnica de Madrid, Villarrubia es auditor CISA y Decano del Colegio de Ingenieros en Informática de Castilla La Mancha.

– **Víctor Mojarrieta**. 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.

AENA: IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD EN CENTROS DE CONTROL Y TORRES

Sinopsis: la presentacion ofrecerá una idea clara de la protección implementada por Aena para la 'securización' de los sistemas de control de tránsito aéreo (sistema SACTA) que utiliza Navegación Aérea a nivel nacional, con actuaciones en todos los centros de control y torres de aeropuerto de España, implantándose políticas de seguridad y seguridad perimetral en cada una de las cerca de noventa ubicaciones. Se tratarán de explicar en la ponencia los aspectos más importantes de este gran proyecto compuesto por cuatro fases, se hará un recorrido por los diferentes aspectos del mismo y se centrará la parte técnica de la presentacion en la seguridad de las comunicaciones, defensa perimetral, el entorno *multicast* de la organización así como las VPN´s.

Ponentes:

– **Narciso Pérez Llera**. Responsable de Proyectos de Automatización de la División de Automatización de Navegación Aérea de Aena desde 1999. En 1991 inició sus trabajos en la Dirección General de Aviación Civil como técnico aeronáutico en el proyecto SACTA dentro del subsistema de Comunicaciones de Datos y Supervisión de Sistemas Informáticos ATC (Control de Tráfico Aéreo). Posteriormente desempeñó el puesto de analista de sistemas dentro del mismo proyecto. De 1992 a 1998 pasó a integrarse en Aena como Responsable de Proyectos de Comunicaciones, participando en el desarrollo de REDÁN (Red Corporativa de Datos de Navegación Aérea).

– **José Gros**. Director para España y Portugal de Nokia Internet Communications. De 1991 a 1996, Gros ocupó el cargo de director comercial de Attachmate España, editor de software especializado en productos de conectividad pc-mainframe IBM. Posteriormente trabajó en New Technology and Co., mayorista de productos de conectividad y seguridad, del que fue cofundador. Desde 2000 ocupa la dirección general de Nokia Internet Communications para el mercado ibérico, filial para la seguridad de Nokia.

MESA REDONDA

SISTEMAS INTEGRADOS DE SEGURIDAD MULTIFUNCIÓN Y MULTIFABRICANTE: ¿PARA QUÉ Y POR QUÉ?

Propósito: desde su nacimiento, la oferta comercial de herramientas tecnológicas de seguridad ha estado marcada primordialmente por el desarrollo de productos con fines de protección frente a amenazas específicas: accesos no autorizados, códigos maliciosos, intrusiones...; sin embargo, las necesidades que tienen los usuarios de una seguridad más avanzada, interoperable y completa está propiciando el desarrollo de soluciones software+hardware integradas multifabricante, que cubren o pueden cubrir varios servicios y objetivos de seguridad (cortafuegos, túneles, defensa frente a códigos maliciosos, IDS...). ¿Cuál es la razón de ser de este comportamiento de la oferta? ¿Podrá decidir en algún momento el usuario corporativo la marca de los productos integrados? ¿Qué puede hacer el usuario y el integrador ante cambios bruscos de política de alianzas entre fabricantes?

Participantes:

– **Pedro Galatas**. Director de Estrategia de Negocio de Afina. Graduado en Economía por la Universidad de Notre Dame EEUU 1989 y PDD IESE en 1996, Galatas fue fundador de Afina Sistemas en 1990, empresa en la que ha desempeñado los cargos de director comercial, director de marketing y actualmente director de Estrategia de Negocio. Asimismo, ha sido fundador de las oficinas de Afina en Portugal, EEUU, México, Venezuela y Colombia.

– **Camilo Vaquero**. Director de Estrategia y Desarrollo de Negocio de Aladdin. 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. Posteriormente trabajó en Unisys y en Fast Ibérica como responsable de sistemas de protección de software. Tras la fusión de Fast Ibérica con PC Hardware a finales de 2000 se creó Aladdin España, donde actualmente ocupa el cargo de director de Estrategia y Desarrollo de Negocio.

...MESA REDONDA

– **José Manuel Cea**. Director General de la unidad Iberia de Check Point Software Technologies. Licenciado en Informática, tiene un Master en Diseño de Sistemas y ha cursado sus estudios en EEUU. Antes de su incorporación a Check Point, fue director de Tecnología y Desarrollo de Negocio en Bea Systems Ibérica y responsable de Desarrollo de Negocio para grandes sistemas en Sun. Anteriormente había desempeñado distintos puestos de responsabilidad en AT&T, Cray Research y Airtel.

– **Manuel Arrevola**. Director de Internet Security Systems. 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.

– **Carlos Jiménez Suárez**. Presidente de Secuware. Ingeniero Superior de Telecomunicaciones por la UPM de Madrid, fundó en 1990 la compañía Anyware, y un año más tarde Anyware Seguridad Informática. Durante 1998, vende Anyware a Network Associates y continúa su trayectoria dentro de la multinacional, hasta finales de 1999, como director de Seguridad para el Sur de Europa. Posteriormente, funda Secuware, empresa 100% española que ofrece soluciones a problemas de seguridad y de estabilidad de PCs que funcionan bajo Windows. Durante sus dos primeros años de existencia centró su actividad en el desarrollo de productos de seguridad para el Ministerio de Defensa español, y en el año 2000, inicia su acercamiento a la comunidad empresarial.

– **Vesku Turtia**. Consejero Delegado de Stonesoft para España y Portugal. Antes de su nombramiento, ocupó el puesto de director general de la compañía. Hasta su incorporación a Stonesoft, Turtia fue director de ventas en diferentes empresas, entre las que destacan Kemira Ibérica, Renco SA y finalmente Kymmene Ltd. en Singapur. Desde la apertura de la filial de Stonesoft en España, se ha encargado de desarrollar la comercialización de la solución cortafuegos y VPN de alta disponibilidad StoneGate.

– **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.

– **Mario Velarde**. Director General de la filial española de Trend Micro desde 2001. Master en Dirección de Empresas, PDG por el IESE y licenciado en Ciencias Físicas (Cálculo Automático), comenzó su andadura profesional en Control Data Corp. Posteriormente desarrolló diversas funciones en compañías integradoras de sistemas y, después, fue durante cinco años Director de la filial en España de Software Products International. Finalmente, antes de su incorporación a Trend Micro, ocupó el cargo de director de Expansión Internacional en el fabricante de antivirus español Panda Software.

TERCER MÓDULO 25 de abril de 2003

09:15h. Entrega de documentación
09:30h. **Ponencia:** Proyecto de diseño e implantación de la PKI de la Junta de Andalucía
Ponentes:
– **Antonio Ramos,** Jefe de Coordinación Informática de la Junta de Andalucía
– **Carlos García Perales,** Gerente de e-Security de Steria Ibérica
10:05h. Coloquio
10:10h. **Ponencia:** El Proyecto Titán de Caja Madrid: identificador único multifunción soportado en tarjeta inteligente de última generación.
Ponentes:
– **Miguel Ángel Navarrete,** Director de Seguridad Informática. Planificación e Innovación Tecnológica. Caja Madrid
– **Javier Sevillano.** Responsable de Equipo de Sistemas Distribuidos e Inet. Departamento de Seguridad Informática. Caja Madrid.
10:45h. Coloquio
10:50h. **Ponencia:** Izenpe, prestador de servicios de certificación para las administraciones públicas vascas. Primeros pasos.
Ponentes:
– **Luis María Guinea,** Director Gerente de Izenpe
– **Manuel Torres,** Director de Servicios Profesionales de Safelayer Secure Communications
11:25h. Coloquio
11:30h. Pausa-café
12:00h. **Ponencia:** Las Tecnologías de Certificación como habilitadoras del voto electrónico. Análisis de las elecciones al Consejo Asesor de la DGGC, primera experiencia europea de carácter oficial.
Ponentes:
– **Arturo Prieto Bozec,** Gabinete Técnico. Dirección General de la Guardia Civil.
– **Juan Carlos Batanero,** Director de la Unidad de Arquitecturas Avanzadas y Seguridad de Indra.
12:35h. Coloquio
12:40h. **Ponencia:** Comunicaciones seguras vía satélite: una iniciativa europea
Ponentes:
– **Nasser Zaidi,** Ingeniero de Sistemas. Astrium.
– **Enrique Crespo Antolín,** Consultor de Seguridad de Soluciones Globales Internet
13:15h. Coloquio
13:20h. **Ponencia:** Situación de la futura ley de firma electrónica y otros desarrollos legales
Ponente: **Leopoldo González-Echenique,** Director General para el Desarrollo de la Sociedad de la Información. Mª de Ciencia y Tecnología.
13:55h. Coloquio
14:00h. Almuerzo
16:00h. **Ponencia:** Grupo Recoletos: la seguridad en las nuevas comunicaciones y su repercusión en costes
Ponentes:
– **Juan José Garrido,** Jefe de Proyectos de Seguridad de Grupo Recoletos
– **Joaquín Reixa,** Director General de Symantec
16:35h. Coloquio
16:40h. **Ponencia:** El Plan de Seguridad Crédito y Caución 2003 y un caso de ejemplo: firma electrónica
Ponentes:
– **José Manuel González de Heredia,** Director de Tecnología de Crédito y Caución
– **Moisés Navarro,** Consultor de Seguridad IT. IBM Global Services
17:15h. Coloquio
17:20h. Pausa-café
17:45h. **Mesa redonda:** Aportaciones de la universidad española a la industria de seguridad y a la seguridad de las TIC de uso en organizaciones
Intervienen:
– Universidad Carlos III de Madrid: **Arturo Ribagorda,** Catedrático de Ciencias de la Computación e Inteligencia Artificial y Director del Departamento de Informática
– Universidad de Deusto: **Javier Areitio,** Catedrático y Director del Grupo de Investigación de Redes y Sistemas
– Universidad de Málaga: **Javier López,** Profesor titular y Responsable del Grupo de Seguridad
– Universidad Politécnica de Barcelona: **Manel Medina,** Catedrático de Aplicaciones Telemáticas y Director de esCert/UPC
– Universidad Politécnica de Madrid: **José Antonio Mañas,** Catedrático de Ingeniería Telemática. ETSI Telecomunicación.
– Universidad Politécnica de Madrid: **Jorge Dávila,** Profesor Titular y Director del Laboratorio de Criptografía. LSIIS. Facultad de Informática.
19:15h. Coloquio
19:25h. Fin de la tercera jornada

Clausura de Securmática 2003

PROYECTO DE DISEÑO E IMPLANTACIÓN DE LA PKI DE LA JUNTA DE ANDALUCÍA

Sinopsis: la implantación efectiva de la firma electrónica en los sistemas de tramitación electrónica, precisa de la creación de una estructura técnica, organizativa y jurídica, capaz de soportar el conjunto de servicios requeridos, tales como son el Prestador de Servicios de Certificación, los sistemas de registro y validación, los sistemas de *TimeStamping* y las plataformas de registro de evidencias electrónicas y recibos.

En el transcurso de la ponencia se revisa el proceso seguido para diseñar y construir la arquitectura de PKI de la Junta de Andalucía, elemento habilitante del Sistema de Tramitación Electrónica, identificándose la necesidad de cada elemento constituyente y describiéndose las funciones que cubre dentro del sistema, tanto desde el punto de vista técnico como organizativo y jurídico.

Ponentes:

– **Antonio Ramos Olivares.** Jefe de Coordinación Informática de la Junta de Andalucía. Es el responsable del diseño y realización de los proyectos horizontales, destinados a cubrir las necesidades informáticas comunes al conjunto de las Consejerías y Organismos de la Junta de Andalucía. Con esta misión se ha encargado de la definición, estructuración y coordinación de los proyectos destinados al diseño e implantación de los "elementos habilitantes" necesarios para la implantación del futuro Sistema Integrado de Tramitación Electrónica.

– **Carlos García Perales.** Gerente de e-Security de Steria Ibérica, desde 1996 ha sido responsable de la oferta de seguridad, participando en la coordinación de los proyectos de consultoría de seguridad, auditoría de seguridad e implantación de soluciones de certificación y firma electrónica, realizados tanto para corporaciones privadas como para instituciones públicas.

EL PROYECTO TITÁN DE CAJA MADRID: IDENTIFICADOR ÚNICO MULTIFUNCIÓN SOPORTADO EN TARJETA INTELIGENTE DE ÚLTIMA GENERACIÓN

Sinopsis: el objetivo de la ponencia es dar a conocer los factores principales del ciclo de vida de construcción de un identificador único multifunción soportado en tarjeta inteligente, poniendo el foco en dos aspectos: por un lado, explicar los motivos que dan origen al proyecto, el objetivo, los requisitos y expectativas de los intervinientes, cómo se afrontó, cuál es la situación actual,... en definitiva el relativo a la gestión; y, por otro lado, dar a conocer cómo está hecho, es decir la infraestructura construida, la tarjeta, los certificados, software, hardware,... sin olvidar la logística necesaria para obtener como producto la tarjeta multifunción, con capacidades financieras, de control de acceso físico y lógico a los sistemas de información, tanto de forma remota como en entornos locales.

Ponentes:

– **Miguel Ángel Navarrete**. Director de Seguridad Informática de Caja Madrid. Ha trabajado como informático desde hace 20 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 un buen número de áreas de las TI como Técnica de Sistemas, Gestión Presupuestaria, de Recursos y Proyectos, Metodología, Arquitectura y más recientemente Desarrollo de Software, donde ha dirigido los equipos y proyectos de infraestructura de oficinas y autoservicio, del centro de informática personal y de soluciones internet. Actualmente se enmarca en el Área de Planificación e Innovación Tecnológica, donde se ubica el Departamento de Seguridad Informática del Grupo Caja Madrid.

– **Javier Sevillano**. Técnico Superior en Informática Empresarial por Cibernos. Ha desarrollado su trayectoria profesional en diversas empresas: McDonnell Douglas, Servicios Informáticos de las Cajas de Ahorro y Sistema 4B. Se incorporó a la plantilla de Caja Madrid en el año 2000 y desde el año 2001 es responsable de Equipo de Sistemas Distribuidos e Internet del Departamento de Seguridad Informática de Caja Madrid.

IZENPE, PRESTADOR DE SERVICIOS DE CERTIFICACIÓN PARA LAS ADMINISTRACIONES PÚBLICAS VASCAS. PRIMEROS PASOS

Sinopsis: Izenpe arranca desde el respeto a la autonomía que en materia de modernización administrativa, y más concretamente en el desarrollo de la administración electrónica corresponde a las instituciones implicadas en esta iniciativa.

Con este proyecto de certificación digital, las administraciones vascas pretenden potenciar el uso de internet y el desarrollo de servicios de valor añadido en la sociedad vasca, especialmente en la relación administración-ciudadano y viceversa.

Izenpe se constituye como una iniciativa global de las administraciones publicas vascas, con objetivos de coordinación, en primer lugar, entre el ámbito autonómico y foral (que constituyen el accionariado de la sociedad) y posteriormente con el mundo municipal de la comunidad autónoma del País Vasco.

Para el cumplimiento de estos objetivos, Izenpe ha contado con la participación de diferentes empresas, entre las que cabe destacar EJIE, Euskaltel y Safelayer. Esta última ha aportado además de su tecnología, su experiencia en la implantación de servicios de certificación electrónica.

Ponentes:

– **Luís María Guinea**. Director Gerente de Izenpe, la Entidad de Certificación para las Administraciones Públicas Vascas. Guinea ha trabajado en diversos departamentos del Gobierno Vasco (Educación, Justicia, Dirección de Organización y Sistemas) y en la Sociedad Informática del Gobierno Vasco (EJIE), donde fue primero responsable del área de soporte técnico y despues director general, hasta su incorporación a Izenpe.

– **Manuel Torres**. Director de los Servicios Profesionales de Safelayer Secure Communications, actividad que viene desarrollando desde su incorporación a la firma y donde se encarga de la coordinación y ejecución de proyectos de PKI. Torres, cuenta con una amplia experiencia en el sector tanto a nivel nacional como internacional habiendo participado en numerosos proyectos entre los que destacan Theseus, Tecodis, ACE, eFirma, eDNI, eEpoch e Izenpe. Previamente ocupó diferentes cargos de responsabilidad en Baltimore Technologies, Fujitsu ICL y Penta3.

LAS TECNOLOGÍAS DE CERTIFICACIÓN COMO HABILITADORAS DEL VOTO ELECTRÓNICO. ANÁLISIS DE LAS ELECCIONES AL CONSEJO ASESOR DE LA DGGC, PRIMERA EXPERIENCIA EUROPEA DE CARÁCTER OFICIAL

Sinopsis: el voto electrónico es ya una realidad como parte de los nuevos canales de negocio y tramitación administrativa que han sido habilitados por las Tecnologías de Certificación. En esta ponencia Indra, tras un breve repaso a la aplicación de las Tecnologías de la Información en el ámbito electoral que se ha venido realizando en las últimas décadas, expondrá el avance trascendental que supone la introducción de la certificación en los procesos electorales electrónicos. Como análisis de caso práctico, la Dirección General de la Guardia Civil presentará el proyecto de elecciones a su Consejo Asesor de Personal del Cuerpo, primera votación electrónica europea de carácter oficial, realizado por Indra con tarjetas y certificados de Ceres-FNMT.

Ponentes:

– **Arturo Prieto Bozec.** Gabinete Técnico del Director General de la Guardia Civil. Comandante de la Guardia Civil. Prieto Bozec es Director Técnico del plan de implantación de firma electrónica y voto electrónico en la Guardia Civil.

– **Juan Carlos Batanero.** Ingeniero Superior de Telecomunicación por la Universidad Politécnica de Madrid. Ha desarrollado su carrera profesional en Indra, donde ha desempeñado diversos puestos de responsabilidad en áreas relacionadas con comunicaciones, seguridad y arquitecturas internet. Actualmente desempeña el cargo de Director de la Unidad de Arquitecturas Avanzadas y Seguridad de la compañía.

COMUNICACIONES SEGURAS VÍA SATÉLITE: UNA INICIATIVA EUROPEA

Sinopsis: en la ponencia se hará un énfasis especial en resaltar los desafíos a los que se enfrentan en la actualidad los sistemas de satélite con contenido IP. Entre ellos destacan la transición, coexistencia de IPv4 a IPv6, la seguridad, el comportamiento específico del medio satélite, problemas y puntos abiertos referentes a *multicast*. Se presentará WEST como un esfuerzo europeo de proporcionar un banco de prueba que arroje resultados de valor y realistas sobre los aspectos más críticos en lo referente a los puntos anteriores. Se presentarán también las líneas futuras de actividad.

Ponentes:

– **Nasser Zaidi**. Ingeniero en Sistemas de Comunicaciones y Redes de Astrium. Cuenta con una carrera profesional de 15 años de experiencia en los campos de investigación aplicada en la industria Aeroespacial. Ha trabajado, entre otros, en los proyectos Stentor, de tipo EPS, Sistema Euridis, Inmarsat SDM, Servicio de Navegación Geoestacionaria, Egnos y Artes 3.

– **Enrique Crespo**. Consultor de Seguridad de Soluciones Globales Internet. Licenciado en Matemáticas, acredita una experiencia profesional en Proyectos de Seguridad Bancaria, del Programa Marco Europeo, Agencia Espacial Europea, Proyectos I+D+I del MCYT y diversos proyectos centrados en la seguridad y administración digital. Es miembro del SC27, Grupo de Trabajo de Criptografía.

SITUACIÓN DE LA FUTURA LEY DE FIRMA ELECTRÓNICA Y OTROS DESARROLLOS LEGALES

Ponente: Leopoldo González-Echenique. Director General para el Desarrollo de la Sociedad de la Información de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología. Licenciado en Derecho y en Ciencias Económicas por ICADE, González-Echenique pertenece al Cuerpo de Abogados del Estado. Ha estado destinado en los Servicios de la Abogacía del Estado en Barcelona y en los Ministerios de Interior y de Economía y Hacienda, y ha sido Subdirector de los Servicios Jurídicos de la Comisión Nacional del Mercado de Valores y Director del Gabinete Técnico del Subsecretario de Economía.

GRUPO RECOLETOS: LA SEGURIDAD EN LAS NUEVAS COMUNICACIONES Y SU REPERCUSIÓN EN COSTES

Sinopsis: el proyecto objeto de presentación surgió de la necesidad de dar una mayor calidad de servicio en el ámbito de las comunicaciones del Grupo Recoletos, contando con todas las delegaciones de que dispone, así como con los diferentes centros de impresión.

El principal motivo para abordar la iniciativa fue el ahorro de costes derivado de la sustitución de las líneas que se venían utilizando por las nuevas líneas con tecnología ADSL. Dicho ahorro era suficiente para financiar todo el equipamiento necesario para instalar la nueva infraestructura.

Además de contar con esta nueva forma de conectividad, también se empezó a disponer de una nueva infraestructura de seguridad. La tecnología basada en el estándar IPSec, sirve de apoyo para crear una red WAN sobre Internet.

Ponentes:

– **Juan José Garrido**. Jefe de Proyectos de Seguridad del Grupo Recoletos. Licenciado en Administración y Dirección de Empresas (Esp. Dirección empresarial) e Ingeniero Técnico de Telecomunicación (Esp. Equipos Electrónicos), Garrido tiene 5 años de experiencia en el área de Ingeniería de Sistemas de Recoletos Grupo de Comunicación. En la actualidad centra su atención en el área de seguridad TIC.

– **Joaquín Reixa**. Director General de Symantec Ibérica. Ingeniero de Telecomunicaciones y Master Business Administration, se incorporó a Symantec en septiembre de 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. Reixa también trabajó para Foxboro Control como director del departamento de sistemas.

EL PLAN DE SEGURIDAD CRÉDITO Y CAUCIÓN 2003 Y UN CASO DE EJEMPLO: FIRMA ELECTRÓNICA

Sinopsis: la ponencia cubrirá los contenidos del Plan de Seguridad de Crédito y Caución (marco normativo; seguridad activos de negocio; infraestructura Tivoli para la gestión de identidades; gestión de accesos y gestión del riesgo; formación-divulgación-concienciación), analizando cómo se abordó dicha planificación en aras de alinear la estrategia de seguridad con la estrategia de negocio de Crédito y Caución. Se describirá el Proyecto de Firma Electrónica de Crédito y Caución como ejemplo de este alineamiento, cubriendo aspectos de negocio y aspectos técnicos asociados al proyecto.

Ponentes:

– **José Manuel González de Heredia**. Director de Tecnología de Crédito y Caución. Dispone de una experiencia de más de 26 años en el sector de las Tecnologías de la Información. Comenzó su carrera profesional como Técnico de Sistemas, cubriendo posteriormente responsabilidades en áreas comerciales como Técnico de Ventas y Marketing Manager.

– **Moisés Navarro Marín**. Consultor de Seguridad IT de IBM. Licenciado en Informática por la UPM, Navarro dispone de más de 7 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 ha sido Responsable de los Servicios de Consultoría de Seguridad de IBM Global Services. Actualmente, Navarro presta sus servicios como experto de IBM para el área de Negocios e Infraestructuras Resilientes.

MESA REDONDA

APORTACIONES DE LA UNIVERSIDAD ESPAÑOLA A LA INDUSTRIA Y A LA SEGURIDAD DE LAS TIC DE USO EN ORGANIZACIONES

Propósito: ¿En qué ha contribuido y está contribuyendo la Universidad al desarrollo de la seguridad de la información en España? ¿Existen líneas de colaboración entre la Universidad española y otros actores del sector de seguridad de la información: usuarios, consultores, integradores y fabricantes? ¿Estimulan las autoridades públicas la transferencia de conocimientos de la Universidad hacia la empresa? ¿Está preparada la Universidad española para colaborar activamente con el mercado de seguridad de la información? ¿Se adaptan los conocimientos de la disciplina de la seguridad de la información que se imparten en la Universidad española a los diversos perfiles profesionales que demandan empresas y organismos?

Participantes:

– **Arturo Ribagorda Garnacho.** Ingeniero de Telecomunicación y Doctor en Informática por la Universidad Politécnica de Madrid. Es Catedrático de Universidad en la Universidad Carlos III de Madrid y director de su Departamento de Informática. Su actividad académica se centra en la Seguridad de las T. I. Es Presidente del Comité Organizador de Securmática desde el primer congreso celebrado en 1990, y especialista de la sección bibliográfica de la revista Seguridad en Informática y Comunicaciones (SIC).

– **Javier Areitio.** Catedrático de la Universidad de Deusto (Facultad de Ingeniería, Area de Telecomunicaciones) y Doctor en Ciencias Físicas. Forma parte de CORDIS (Community Research and Development Information Service) European Commission, Directorate General XIII-D.2. Es Tutor de la AECI (Agencia Española de Cooperación Internacional). Ha sido Coordinador Técnico del Proyecto COMMETT "Information and Computer Security" ICS/EU y dirige el Laboratorio SIC de Evaluación de Productos de Seguridad/Criptografía. Es también miembro de la ISOC y Coordinador del Equipo de Mejora del Area de Telecomunicaciones para la implantación en la Facultad de Ingeniería de la Universidad de Deusto de un Sistema de Calidad Total según el Modelo de la EFQM (European Foundation for Quality Management).

– **Javier López Muñoz**. Doctor Ingeniero en Informática del Departamento de Lenguajes y Ciencias de la Computación de la Universidad de Málaga. Desarrolla su actividad docente como Profesor Titular en la E.T.S. de Ingeniería Informática, y su labor investigadora dentro del grupo GISUM, donde coordina el subgrupo de Seguridad. Su actividad investigadora está centrada en el área de Seguridad en Redes de Comunicaciones y en Comercio Electrónico, habiendo realizando parte de esa labor de investigación en varios centros universitarios de E.E.U.U. especializados en la materia. Es responsable técnico de varios proyectos de investigación relacionados con los aspectos prácticos de Seguridad de las TIC, entre los que destaca el proyecto internacional «Global PKI» del Telecommunications Advancement Organization de Japón. Asimismo, es Director Tecnico del Proyecto IST «CASENET» del V Programa Marco de la UE.

– **Manel Medina** es Doctor en Ingeniería de Telecomunicación por la UPC, Catedrático de Aplicaciones Telemáticas en la UPC, Director del servicio es-CERT-UPC, Presidente de InetSecur, Asesor de Safelayer y Director de Tecnología de SeMarket (grupo dedicado al desarrollo, integración y comercialización de productos de soporte a PSC y firma-e, y al desarrollo e integración de aplicaciones en el uso de firma-e). Medina es uno de los expertos españoles más destacados en materia de TTP´s, tanto en el desarrollo de proyectos de I+D como en el terreno del asesoramiento a organizaciones públicas y de normalización. Ha editado, entre otros, el informe "*EESSI (European Electronic Signature Standardization Initiative) technical report*" y es miembro del taller homónimo patrocinado por el CEN.

– **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 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).

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

SECURMATICA 2003

Fechas y lugar

SECURMÁTICA 2003 tendrá lugar los días 23, 24 y 25 de abril de 2003 en el hotel NOVOTEL*. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2003 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 (24 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

- **AFORO LIMITADO**
- * 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.
- 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 2003

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 23 ❑ MÓDULO 2 DÍA 24 ❑ MÓDULO 3 DÍA 25 ❑ Deseo inscribirme a SECURMATICA 2003

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**