SECURMATICA

2011
12.13.14|abril

XXII Congreso español de Seguridad de la Información

SEGURIDAD: ¿FIARSE O CONFIAR?

PROGRAMA

ES HORA DE COMPARTIR EXPERIENCIAS >>> Y AVANZAR

Securmática 2011, XXII edición del Congreso español de Seguridad de la Información organizado por la revista SIC, tendrá lugar los días 12, 13 y 14 de abril en su tradicional sede del Campo de las Naciones de Madrid.

La gestión de riesgos –en concreto los de seguridad, y especialmente los de seguridad de la información–, que en última instancia es una componente de la gestión de los negocios y actividades, se enfrenta hoy con requisitos más precisos de cumplimiento legal, y con un entorno tecnológico complejo que ha propiciado que las filtraciones de datos, los ataques contra la disponibilidad de servicios, la deslealtad de empleados, proveedores y terceros, y el fraude sean noticia diaria.

Ante este panorama, Securmática presenta un programa en el que se van a analizar razonablemente las nuevas circunstancias de naturaleza legal (Código Penal) que al respecto del uso de sistemas tecnológicos de tratamiento de información afectan a apoderados y administradores empresariales y a directivos (incluidos los que cumplen la función de CIO, CSO, CISO, CLO...) y terceros.

También se realizará un análisis del alcance de algunos aspectos cuya inclusión pudiera contemplarse en la modificación de la Directiva de protección de datos personales, al tiempo que se debatirá sobre un asunto capital: "El control del uso de privilegios sobre la información por los usuarios autorizados", que está en la raíz de muchos de los acontecimientos divulgados y no divulgados de fugas de información.

También el Congreso será escenario de aportaciones en varios frentes: gestión tecnológica del riesgo, profundidad de la función de seguridad, gestión integrada, y proyectos concretos de naturaleza tecnológica: cumplimiento de políticas, operación, seguridad gestionada, servicio de desarrollo seguro en "la nube", movilidad y control de acceso a la red corporativa, reputación...

El XXII Congreso también incluye en su programa conferencias sobre dos iniciativas de interés notable: la tarjeta de ciudadano de Portugal (no olvidemos al respecto que España ha sido un país pionero con el DNI-e, y siempre enriquece contrastar lo aquí proyectado en otros países) y el proyecto STORK para la aceptación transfronteriza de identidades electrónicas europeas.

Finalmente, este año se han reservado dos espacios para tratar sendas tipologías de proyectos clave en el ámbito de la seguridad de la información: uno por su implicación directa, el Esquema Nacional de Seguridad –acerca del cual se presentarán dos experiencias de plan de adecuación–, y otro porque sigue siendo la asignatura pendiente de muchas organizaciones, y porque tiene repercusiones decisivas en seguridad: la gestión de usuarios e identidades, un campo en constante evolución del que se presentarán tres experiencias.

Copatrocinadores:

accenture – Alto rendimiento. Hecho realidad.
bluelive
BULL
ECIJA – Derecho y Tecnología
ERNST & YOUNG – Quality In Everything We Do
gmv – Innovating Solutions
GRUPO GESFOR
hp
IBM
indra
Nextel S.A. – Ingeniería y Consultoría
pwc
Telefónica

Organiza:

SIC 20 ANIVERSARIO
Revista seguridad en informática y comunicaciones

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

PRIMER MÓDULO, 12 de abril

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

Moderador: **Arturo Ribagorda Garnacho**, Catedrático de la Universidad Carlos III de Madrid.

10:00h. Conferencia de apertura: "**Puntos clave en la reforma de la Directiva sobre protección de datos personales**".
Ponente: **Rafael García Gozalo**, Vocal Asesor-Jefe del Área Internacional de la Agencia Española de Protección de Datos.
10.30h. Coloquio.
10:45h. Ponencia: "**El Código Penal y los delitos relacionados con el uso de sistemas de información tecnológicos**".
Ponente: **Paloma Llaneza González**. Abogado y CISA. Socio de Razona Legaltech y Presidenta de AEDEL, Asociación Española de Evidencias Electrónicas.
11:20h. Coloquio.
11:25h. Pausa-café.

Moderador: **José de la Peña Muñoz**, Director de la revista SIC.

11:55h. **Debate: "Las responsabilidades de persona jurídica en el Código Penal. Delitos por '*culpa in vigilando*'"**.
Participantes:
- **Ignacio Alamillo i Domingo**. Abogado y CISA. Director General de Astrea La Infopista Jurídica. Abogado y CISA.
- **Francisco Javier García Carmona**, Director de Seguridad de la Información y las Comunicaciones de Iberdrola.
- **Miguel Ángel Rego Fernández**, Director de Seguridad y Riesgos Corporativos de ONO.
- **Carlos Alberto Sáiz Peña**. Abogado y CDPP. Socio Director del Área GRC-Governance, Risk & Compliance de Ecija.

Moderador: **Luis Fernández Delgado**, Editor de la revista SIC.

13:25h. Ponencia: **"Evite que su funcion de seguridad quede borrosa. Profundidad, exposicion y foco"**.
Ponente: **Tomás Roy Catalá**, Director del Área de Calidad, Seguridad y Relaciones con Proveedores del Centro de Telecomunicaciones y Tecnologías de la Información-CTTI de la Generalitat de Cataluña.
14:00h. Coloquio.
14:05h. Almuerzo.

Espacio monográfico:
LA GESTIÓN DE IDENTIDADES. PROYECTOS.

Moderador: **Jorge Dávila Muro**, Director del Laboratorio de Criptografía LSIIS – Facultad de Informática de la UPM.

16:00h. Ponencia: "**Gestión de Identidades y Accesos en Telefónica España: Sistemas de Información Corporativos y de Negocio**".
Ponentes:
- **Víctor Manuel Ruiz Gómez**, Responsable de Seguridad de Sistemas en Telefónica España.
- **Juan José Míguez Iglesias**, Director del Área de Riesgos Tecnológicos de PwC.

16:35h. Coloquio.
16:40h. Ponencia: **"EJIE: la gestión de identidades en un entorno dinámico"**.
Ponentes:
- **Iñaki Astorkia Martín**, Jefe de Proyectos, Departamento de Proyectos y Soporte a Usuarios. EJIE.
- **José Ramón Sierra Elechiguerra**, Gestor de Proyectos. Departamento de Technology Consulting. HP.

17:15h. Coloquio.
17:20h. Pausa-café.
17:35h. Ponencia: **"SSO y gestión de identidades en Rioja Salud. Requisitos y estrategias para una implantación rápida y efectiva".**
Ponentes:
- **Tomás Gómez Pérez**, Subdirector de Infraestructuras, Soporte a Usuarios y Seguridad de la Información en Rioja Salud.
- **Vicente Gozalbo Moragrega**, Responsable de Ventas de Productos de Seguridad Tivoli en IBM España.

18:10h. Coloquio.
18:15h. Fin de la primera jornada.

PUNTOS CLAVE EN LA REFORMA DE LA DIRECTIVA SOBRE PROTECCIÓN DE DATOS PERSONALES

Sinopsis. El proceso de revisión de la Directiva de Protección de Datos comenzó en 2009 y entrará en su fase final cuando en el verano de este año la Comisión presente su propuesta de nuevo instrumento legislativo. Durante los dos años transcurridos hasta ahora, documentos de la propia Comisión, del Consejo, de las Autoridades de Protección de Datos o de expertos han identificado las materias en las que el actual marco legal debe ser modificado. Algunas de estas cuestiones son de carácter general, como ocurre con el tipo de acto que se va a adoptar, teniendo siempre presente que se busca una mayor armonización de los derechos nacionales, o con la regulación global de todos los temas en un mismo entorno, incluidos los relativos al antiguo "Tercer Pilar". En otros casos, se busca renovar y perfeccionar los mecanismos existentes, como sucede en relación con los criterios de determinación de la ley aplicable, con los procedimientos de transferencias internacionales de datos o con las capacidades de actuación de las agencias de protección de datos. En otros, por fin, se busca introducir en el ámbito normativo nuevos conceptos o instrumentos, como la generalización de la notificación de los incidentes de seguridad o la inclusión del llamado derecho al olvido y de la garantía de la portabilidad de los datos.

Ponente:
Rafael García Gozalo es Vocal Asesor-jefe del Área Internacional de la Agencia Española de Protección de Datos, donde ingresó en junio de 2008. Anteriormente, y entre 2005 y 2008, trabajó para el Ministerio del Interior como Director Adjunto de la Oficina de Refugio y Asilo, donde fue responsable de Relaciones Internacionales del organismo. Previamente, entre 1990 y 1995, fue Consejero Senior de la Secretaría General de Consumo y para el Ministerio de Sanidad y Consumo. Funcionario de carrera desde 1987, cuenta con licenciaturas de Psicología y Ciencias Políticas.

EL CÓDIGO PENAL Y LOS DELITOS RELACIONADOS CON EL USO DE SISTEMAS DE INFORMACIÓN TECNOLÓGICOS

Sinopsis. La reforma operada en el Código Penal y que entró en vigor el pasado 23 de diciembre de 2010 nos ha traído modificaciones significativas no solo en los delitos conocidos como "tecnológicos", sino también en la cadena 'culpabilística' clásica, al incorporar la responsabilidad de las empresas tanto directa como derivada de la falta de control de sus trabajadores. Esta última es la que, sin duda, representa un mayor riesgo y un mayor reto: no hay jurisprudencia previa que nos ayude a medir la "culpa in vigilando" que el CP define como "debido control" de las empresas sobre sus empleados, lo que supondrá una nueva manera de mirar el control interno y las labores de auditoría. Entre los delitos relacionados con el uso de las TIC se han producido importantes novedades y adiciones (como los ataques DoS) que han de ser tenidos también en cuenta en el contexto de un endurecimiento de conductas delictivas en el entorno de la legislación sobre datos personales con vistas a futuras posibles modificaciones de la UE en la materia.

Ponente:
Paloma Llaneza González, socio de Razona Legaltech, es abogado, CISA y experta en seguridad. Editora de diversos estándares de seguridad (IEC/ISO 27004:2009, ESI TS on Registered E-Mail, y CEN CWA on Data Protection Good Practices), preside en la actualidad AEDEL (Asociacion Española de Evidencias Electrónicas). Como coordinadora del Grupo Ad-Hoc del SC27 de AENOR sobre evidencias electrónicas, participa en el desarrollo de dos normas nacionales, la 71505 sobre el sistema de gestión de evidencias, y la 71506 sobre análisis forense. Actualmente está participando como

experta en seguridad en diversos grupos internacionales sobre "Interoperability issues on REM", "e-signatures and e-documents Long Term Preservation", y "EU Commission Mandate on RFID".

EVITE QUE SU FUNCIÓN DE SEGURIDAD QUEDE BORROSA. PROFUNDIDAD, EXPOSICIÓN Y FOCO

Sinopsis. Las organizaciones están atravesando una coyuntura de cambios que hacen que sus realidades organizadas y sólidas de antaño aparezcan ahora como inestables y proclives a la transformación. Después de una década de grandes desafíos y expediciones ambiciosas con recursos y porteadores a disposición, las empresas mantienen los objetivos, pero en condiciones más anaeróbicas. Los Directivos y Gestores recitan el mantra de Más, por Menos y Mejor, para evitar caer en la tentación de lo superfluo y retornar a lo esencial. Hay que preguntarse "¿Qué pasaría si dejáramos de hacer…?" Y obtendremos dos beneficios claros. Primero, dejaremos de evitar coincidir con el Director General o Financiero en el ascensor y segundo, redescubriremos que la esencia de nuestra responsabilidad es retornar valor a través de desplegar nuestra función con profundidad, exposición y foco adecuados. Una función debe ser única en la organización, con alcance global, viabilidad y escalabilidad. Una función no es un servicio o un proyecto. Los mismos directivos que en el pasado fueron óptimos gestores de la abundancia pueden aparecer borrosos, con ansias de expansión intrusiva o de resistencia ridícula a tales envites o liados en discusiones organizativas estériles y artificiales. Foco, profundidad y exposición. Más por Menos y Mejor. No suena nada mal. Evolución o –¿por qué no?– Revolución de la Seguridad. Una experiencia apoyada en el desarrollo de competencias técnicas, directivas, de comunicación y liderazgo.

Ponente:

Tomás Roy Catalá es Director del Área de Calidad, Seguridad y Relaciones con Proveedores en el Centro de Telecomunicaciones y Tecnologías de la Información (CTTI) de la Generalitat de Cataluña. Desde 2004 dirige un equipo en el área de la Calidad y la seguridad destacando la gestión de los servicios externalizados. Desde 2006 lidera la gestión de la calidad y la seguridad en proyectos y aplicaciones, y desde septiembre de 2007 ha integrado en sus funciones la Dirección del Área de Relación con Proveedores. Ingeniero Superior en Telecomunicaciones, Ingeniero Superior en Electrónica y Licenciado en Ciencias de la Educación, Roy Catalá ha desarrollado su carrera profesional en Italia, en la *joint venture* Fiat GM Powertrain, en la que fue Responsable de Seguridad de la Información y Privacidad de Datos. Máster Ejecutivo en Administración Pública por ESADE, complementa su formación en el área de seguridad en los ámbitos de auditoría –CISA–, gestion de seguridad –CISSP–, gestión de servicios –ITIL–, mejora continua –6sigma–, y seguridad de sistemas operativos y redes.

DEBATE

LAS RESPONSABILIDADES DE LA PERSONA JURÍDICA EN EL CÓDIGO PENAL. DELITOS POR "CULPA IN VIGILANDO"

Proposición. El nuevo Código Penal español establece que las empresas pueden delinquir en varios frentes, ya sea por actos llevados a cabo por sus administradores o apoderados, o por los de un empleado que haya podido perpetrar la fechoría al no haber ejercido la empresa el debido control, lo que se entiende por "*culpa in vigilando*". En líneas generales, puede afirmarse que en la posibilidad de comisión de muchos delitos por "*culpa in vigilando*" están directamente concernidas las funciones de control de riesgos de seguridad de la información y del sistema de información tecnológico. En el debate se tratará de analizar el impacto en las empresas del Código Penal vigente en esta materia, particularmente en la exigencia por la alta dirección a las funciones de control, de gestión de riesgos y a ejecutivos como los CSO y los CISO de que mantengan de un modo efectivo a la entidad a salvo de conductas penadas.

Intervienen:

Ignacio Alamillo i Domingo es Director General de Astrea La Infopista Jurídica, y asimismo Responsable de Innovación de Logalty e Investigador en el GRISC (Centro de Gobierno del Riesgo). Abogado y CISA, cuenta con una dilatada experiencia en materias como la firma electrónica y la administración electrónica. Con anterioridad Alamillo ha sido Consultor Senior de Seguridad en el CTTI de la Generalitat de Cataluña, Responsable de Análisis e Investigación en la Agencia Catalana de Certificación, y Gerente de Consultoría y Asuntos Legales en la Agencia de Certificación Electrónica.

Miguel Ángel Rego Fernández es Director de Seguridad y Riesgos Corporativos de ONO. Hasta su incorporación a este operador de telecomunicaciones en 2008, y desde 2003, ocupó el cargo de Responsable de Seguridad TIC en la Inspección General CIS del Ministerio de Defensa. Rego es Oficial de la Escala Superior del Cuerpo de Intendencia de la Armada, Diplomado en Estudios Avanzados en Ingeniería Informática (Universidad Pontificia de Salamanca), Especialista en Seguridad Corporativa y Protección del Patrimonio (Universidad Europea de Madrid), Máster en Auditoría de Sistemas, Analista de Sistemas Rama de Gestión (Escuela de Informática de La Armada) y Especialista en Criptología (CCN-Centro Criptológico Nacional). Actualmente es Director Académico del Máster en Dirección y Gestión de Seguridad organizado por Asimelec y la UPM. Posee las siguientes certificaciones: ISO/IEC 2000 Foundation, ITIL Service Manager, Foundation Certificate in IT Service Management, CISM y CISA.

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

Carlos Alberto Sáiz Peña es Socio Director del Área GRC-Governance, Risk & Compliance de Ecija. Cofundador y vicepresidente de la Asociación para el Fomento de la Seguridad de la Información-ISMS Forum Spain, subdirector del Data Privacy Institute-DPI, CDPP y co-director del Foro de Protección de Datos de FIDE, Fundación para el desarrollo de Derecho y Empresa. Sáiz Peña tiene 12 años de experiencia en el asesoramiento a clientes en proyectos de Derecho TIC, Seguridad de la Información y Cumplimiento Normativo. Es profesor del Instituto de Empresa en diversos Programas Avanzados, del Curso especialista de Análisis de Riesgos de ISMS Forum, del Máster de Auditoría, Seguridad y Privacidad de la UAM y del Máster de Seguridad de UPM (ETSIT)-Asimelec.

GESTIÓN DE IDENTIDADES Y ACCESO EN TELEFÓNICA ESPAÑA: SISTEMAS DE INFORMACIÓN CORPORATIVOS Y DE NEGOCIO

Sinopsis. El estado del arte en materia de Gestión de Identidades y Accesos ha madurado ostensiblemente en los últimos años. Tanto los fabricantes e implantadores como los clientes han avanzado en el mutuo entendimiento de las ventajas de abordar este tipo de proyectos en el ámbito de la identidad digital, el aprovisionamiento, el control de accesos y la gestión de roles. Este es el caso de Telefónica España, que ha abordado uno de los mayores proyectos de Gestión de Identidades y Accesos a nivel internacional, en los ámbitos de Sistemas de Información y Sistemas de Red tanto para la línea de negocio fija como móvil. Telefónica España aborda la implantación de una solución única basada en un modelo de autogestión y automatización que mejore el servicio al usuario con el claro objetivo de obtener beneficios a corto plazo y una importante reducción de costes asociada al retorno de la inversión.

Ponentes:

Víctor Manuel Ruíz Gómez es Responsable de Seguridad de Sistemas en Telefónica España. Ingeniero Informático por la Universidad Politécnica de Madrid desde 1995, CISA, Auditor BS25999 y Auditor AP + , lleva en Telefónica Móviles desde 1996. Ha pasado por las áreas de Comunicaciones, Gestión de Sistemas y Redes, y desde 2003 en Seguridad de Sistemas. Dentro de Seguridad, ha sido responsable del grupo de *Hacking* Ético y gestión de Vulnerabilidades y Amenazas desde 2003 hasta 2006, pasando posteriormente a ser el Responsable de la Continuidad de Negocio de Telefónica Móviles España. En esta etapa se realizó el proyecto FENIX consiguiendo el plan de continuidad de negocio en TME. Posteriormente, en junio de 2008 asumió la responsabilidad de la Seguridad en todos los Sistemas de TE (BSS y OSS).

Juan José Míguez Iglesias es Director del Área de Riesgos Tecnológicos de PwC. Ingeniero de Telecomunicación en la especialidad de Telemática y certificado como CISA, CISM y CGEIT por ISACA, y Lead Auditor ISO 27001 y Lead Auditor BS25999-2 por BSI, a lo largo de su trayectoria profesional de más de 15 años en el mundo de la consultoría de seguridad y auditoría informática ha realizado multitud de trabajos entre los que cabe destacar Planes Directores de Seguridad, Planes de Continuidad de Negocio, Análisis de Riesgos, implantación de Gestión de Identidades o Auditorías técnicas informáticas en grandes compañías de diversos sectores a nivel nacional e internacional.

EJIE: LA GESTIÓN DE IDENTIDADES EN UN ENTORNO DINÁMICO

Sinopsis. La gestión de identidad continua siendo una de las principales preocupaciones en materia de seguridad, eficiencia y cumplimiento normativo de las empresas. Ejie ha implantado paulatinamente esta gestión y está preparado para afrontar próximos retos, como el "cloud computing" o el acceso a los sistemas mediante múltiples dispositivos móviles. La ponencia descubre las principales fases que ha tenido que afrontar el proyecto, los cambios organizativos y el grado de preparación para futuras metas.

Ponentes:

Iñaki Astorkia Martín es Responsable de Proyectos Software y Consultoría dentro del Área de Sistemas de Ejie. Licenciado en Informática por la Universidad de Deusto, Iñaki Astorkia cuenta con 22 años de experiencia laboral en el Área de Sistemas de la Sociedad Informática del Gobierno Vasco EJIE realizando proyectos de infraestructuras y tecnológicos de muy distintas materias como seguridad, virtualización, plataformas de integración, software, *hosting*, etc.

José Ramón Sierra Elechiguerra es Director de Proyectos Senior en el departamento de Technology Consulting de Hewlett-Packard. Cuenta con 30 años de experiencia laboral en el ámbito de las Tecnologías de la Información. Ha participado en el diseño, implantación y en la gestión de proyectos complejos de IT, relacionados con la automatización, gestión industrial y la seguridad, tanto en el sector privado, como en la administración pública. Licenciado en Ciencias Físicas por la Universidad del País Vasco.

SSO Y GESTIÓN DE IDENTIDADES EN RIOJA SALUD. REQUISITOS Y ESTRATEGIAS PARA UNA IMPLANTACIÓN RÁPIDA Y EFECTIVA

Sinopsis. La administración pública en general y la del sistema sanitario en particular presentan una problemática muy especial a la hora de abordar un proyecto de Gestión de identidades y accesos y *Single sign on*. Sin duda, la mayor complejidad se halla en los proyectos de gestión de identidades (definición y gestión de roles, aprovisionamiento automatizado, identidad única...), en los que se requiere una importante colaboración de la organización, que a menudo no es sencilla. Abordar un proyecto de *single sign on*, sin embargo, es una tarea considerablemente más sencilla: es un proyecto mucho más "tecnológico", tiene mucha mayor visibilidad por parte de la organización, es bien percibido por la misma y es de rápido despliegue. En definitiva, es un claro "quick win". IBM y Rioja Salud hemos comenzado juntos esta andadura y queremos compartir nuestra visión sobre lo que se debe y lo que no se debe hacer en la implantación de un proyecto de este tipo en una organización sanitaria pública.

Ponentes:

Tomás Gómez Pérez es Subdirector de Infraestructuras, Soporte a Usuarios y Seguridad de la Información en Rioja Salud. Licenciado en Ciencias Físicas por la Universidad de Valladolid, ha trabajado en el ámbito de las TIC desde 1992. Primero en telecomunicaciones, y poco a poco orientando sus preferencias y su carrera hacia el mundo de las redes IP. Se incorpora al proyecto de Rioja Salud en 2006 como director de una muy ambiciosa iniciativa. Desde entonces ha ido asumiendo diferentes responsabilidades a medida que la organización ha ido madurando, sobre todo en materia de seguridad. Hoy, aparte de la Subdirección de Infraestructuras TIC, es Responsable del área de Sistemas, Soporte a usuarios y Seguridad de la Información. Posee un Máster en seguridad y habitualmente representa al organismo cuando se trata sobre cualquier aspecto relacionado con seguridad.

Vicente Gozalbo Moragrega es Responsable de ventas de productos de Seguridad Tivoli en IBM España, donde ha desempeñado su trabajo en distintas posiciones desde 2007, partiendo como Gerente de Desarrollo de Negocio de Servicios Gestionados de Seguridad. Gozalbo posee una experiencia en el sector de la seguridad TI de más de 11 años, habiendo desarrollado su carrera en compañías como RSA Security (responsable para España y Portugal) o Selesta (como Gerente de preventa de la unidad de negocio de Seguridad), y anteriormente en Bull, BMC Software e IBM Global Services. Por su experiencia, tiene un profundo conocimiento en áreas como las de gestión de identidades y SSO, gestión de accesos a la web, sistemas de autenticación robusta, protección de seguridad perimetral, forénsica, correlación y gestión de eventos de seguridad y herramientas de análisis de cumplimiento normativo.

SEGUNDO MÓDULO, 13 de abril

09:00h. Entrega de documentación.

Moderador: **Antonio Ramos García**, Presidente del Capítulo de Madrid de ISACA.

09:30h. Ponencia: "**Servicio integrado de auditorías de cumplimiento de políticas en el CTTI: enfoque y plataforma tecnológica**".
Ponentes:
- **Josep Mangas de Arriba**, Responsable de la Unidad de Seguridad Tecnológica. CTTI. Generalitat de Cataluña.
- **Rafael Ortega García**, Socio de Advisory. Ernst & Young.

10:05h. Coloquio.

10:10h. Ponencia: "**Seguridad 360º: implantación de un modelo integral**".
Ponentes:
- **Guillermo Llorente Ballesteros**, Director de Seguridad de Mapfre.
- **Daniel Largacha Lamela**, Subdirector del Centro de Control General y Análisis Forense de Mapfre.

10:45h. Coloquio.

10:50h. Pausa-café.

Moderador: **Carlos Manuel Fernández Sánchez**, Jefe de Certificaciones TIC. Dirección de Desarrollo de AENOR.

11:20h. Ponencia: "**STORK: la aceptación transfronteriza de identidades electrónicas europeas**".
Ponentes:
- **Miguel Álvarez Rodríguez**, Jefe del Área de Cooperación en Tecnologías de la Información en la Dirección General para el Impulso de la Administración Electrónica del Ministerio de Política Territorial y Administración Pública. MPTyAP.
- **John Heppe**, Jefe de Proyecto. Sistemas de Seguridad de INDRA.

11:55h. Coloquio.

12:00h. Ponencia: "**Arsys: enfoque y gestión operativa de riesgos de seguridad en servicios**".
Ponente: **Sven Olof Sandstrom Herrera**, Director General de Operaciones y Seguridad de Arsys Internet.

12:35h. Coloquio.

12:40h. Ponencia: "**Guardia Civil: seguridad gestionada desde dos SOC**".
Ponentes:
- **Pedro Morcillo Rueda**, Jefe del Área de Redes y Seguridad. Servicio de Telecomunicaciones de la Guardia Civil.
- **Juan Miguel Velasco López-Urda**, Gerente de Ingeniería y Preventa Consultiva de Seguridad de la Unidad de Grandes Clientes de Telefónica España.

13:15h. Coloquio.

13.20h. Ponencia: "**Endesa: servicio de desarrollo de código seguro desde la nube**".
Ponentes:
- **Justo López Parra**, Responsable de Seguridad Informática de Endesa.
- **Abel González Lanzarote**, Director de Desarrollo de Negocio de Ecija.

13:55h. Coloquio.

14:00h. Almuerzo.

Moderador: **Javier Areitio Bertolín**, Catedrático de la Universidad de Deusto.

16:00h. Ponencia: **"Grupo Banco Popular: movilidad y control de acceso a la red".**
Ponentes:
- **Francisco Javier Pastor Portillo**, Responsable de Arquitectura de Comunicaciones del Grupo Banco Popular.
- **Rodrigo Blanco Rincón**, Director de la Oficina de Proyectos de Bull España.

16:35h. Coloquio.

16:40h. Ponencia: **"Sara Lee: gestionando la presencia en la Red y los riesgos asociados".**
Ponentes:
- **Denis Ontiveros Merlo**, Vicepresidente Global de Seguridad de la Información de Sara Lee Corporation.
- **Daniel Solís Agea**, Director de Operaciones de blueliv.

17:15h. Coloquio.

17:20h. Pausa-café.

17:35h. Ponencia: **"El camino adecuado hacia una seguridad IT efectiva: el caso de élogos**".
Ponentes:
- **Xavier Netto Camero**, Director de Explotación y Arquitectura Tecnológica. Área de Tecnología de élogos.
- **Joaquín Crespo Pérez**, Responsable de Producción. Subdirección de Seguridad del Grupo Gesfor.

18:10h. Coloquio.

18:15h. Fin de la segunda sesión.

19:30h. **Cena de la Seguridad y entrega de los VIII Premios SIC.**

SERVICIO INTEGRADO DE AUDITORÍAS DE CUMPLIMIENTO DE POLÍTICAS EN EL CTTI: ENFOQUE Y PLATAFORMA TECNOLÓGICA

Sinopsis. Durante estos últimos años, la gestión de la seguridad ha estado enfocada en la gestación de un marco normativo que respaldase su función. Es hora de ir un paso más allá. Hace falta auditar este marco normativo y, de esa manera, dar respuesta a dos nuevos requerimientos de la gestión TIC, en los cuales la seguridad es un elemento de valor, la auditoría (desde la visión *"assurance"*) y el gobierno de las TIC (*"governance"*). Respondiendo a esta necesidad, se implanta en la Generalitat la herramienta Babel, que permite la industrialización de las auditorías de cumplimiento normativo, con una flexibilidad y amplitud que aportan una elevada eficiencia en dicho proceso. La herramienta no solo permite la auditoría del marco normativo, sino que como este está referenciado al marco de seguridad estándar, permite asimismo el conocimiento del cumplimiento referenciado a cada estándar o ley, y con vistas multidimensionales de clientes, servicios, normativa y proveedor. Además, permite dotar de más valor a la función de auditoría, ya que su flexibilidad da una oportunidad a que otras funciones TIC puedan ser auditadas, respondiendo así a una necesidad cada vez mayor de las herramientas de seguridad: salir del nicho de la seguridad y responder a necesidades transversales.

Ponentes:

Josep Mangas de Arriba es Responsable de la Unidad de Seguridad Tecnológica dentro del Área de Calidad, Seguridad y Relación con Proveedores del Centro de Telecomunicaciones y Tecnologías de la Información (CTTI) de la Generalitat de Cataluña. Entre sus principales funciones, destaca la gestión de la Oficina de Seguridad Corporativa de la Generalitat de Cataluña y, junto al resto de la Unidad, la prescripción de tecnologías de Seguridad. Anteriormente ha trabajado en T-Mobile International (Londres, UK) y en la consultora DMR (Everis), en Barcelona.

Rafael Ortega García es Socio de Advisory de Ernst & Young. Con anterioridad ha ocupado diversos cargos en firmas como Infosafe, Unisys, Deloitte y Azertia Consulting. Posee una larga experiencia en el sector de la protección TIC y de la información, ámbitos en los que ha dirigido y participado en numerosos proyectos, centrados en la planificación estratégica de sistemas de información, planes estratégicos de seguridad, PKI, desarrollo y soporte a planes de contingencia TIC, planes de continuidad de negocio, diagnósticos de seguridad, análisis de riesgos y creación de cuadros de mando.

SEGURIDAD 360º: IMPLANTACIÓN DE UN MODELO INTEGRAL

Sinopsis. La conferencia versará sobre la definición e implantación de una estrategia de seguridad basada en el concepto de 'integralidad', que posibilite el establecimiento de medidas multifacéticas permitiendo una protección eficaz y adecuada de los activos. Este enfoque engloba tanto aspectos que han sido tratados históricamente desde diferentes ámbitos de seguridad, como actividades de estrategia (definición y planificación) y operativas (implementación y control), enfocándolos y aplicándolos de forma unitaria. Se abordará cómo la adopción de una estrategia basada en esta 'integralidad' permite no solo la aplicación de sinergias, sino además una mayor eficiencia gracias a la identificación de nuevas oportunidades que aporten mayor valor directo a las unidades de negocio. Todo ello ayudando al grupo empresarial Mapfre en el cumplimiento de su compromiso con la seguridad, con el fin de garantizar la integridad y disponibilidad de sus activos, así como la confidencialidad de la información de sus clientes, accionistas, empleados y colaboradores.

Ponentes:

Guillermo Llorente Ballesteros es Director Corporativo de Seguridad en Mapfre. Teniente Coronel de Infantería, es Diplomado de Estado Mayor y Estado Mayor Conjunto en excedencia. Tras numerosos destinos operativos al mando de unidades y con amplia experiencia en misiones internacionales, llega al mundo de la seguridad ocupando durante seis años el puesto de jefe de la Unidad de Contrainteligencia y Seguridad Interior del Ejército de Tierra. Se incorpora a Mapfre en 2006, siendo actualmente Director Corporativo de Seguridad con responsabilidades en el ámbito lógico, así como en el físico o de las instalaciones, englobando en sus competencias materias tales como la continuidad de negocio, la gerencia de riesgos y la gestión del cumplimiento de la LOPD.

Daniel Largacha Lamela es Coordinador del Centro de Control General (CCG) de Mapfre. Ingeniero Superior en Informática por la Universidad Politécnica de Madrid, cuenta con 9 años de experiencia en Seguridad, trabajando en consultoría (Deloitte y Azertia), telco (Telefónica) y seguros (Mapfre), habiendo desempeñado funciones como Responsable de Seguridad de TI, y Jefe de Proyectos (Continuidad de Negocio, Análisis de Riesgos, Planes Directores de Seguridad, Bastionado de Servidores, Test de Intrusión). Largacha cuenta con las certificaciones y títulos siguientes: Director de Seguridad por el Ministerio del Interior, CCNA (Cisco Certified Network Associate), CISA (Certified Information Security Auditor), y CHFI (Computer Hacking Forensic Investigator). Asimismo es profesor titular del Máster en Gerencia de Riesgos de la Fundación Mapfre. En su función actual coordina el Centro de Control General (CCG), área de la Dirección de Seguridad en el que se concentran las áreas operativas de los dominios de Seguridad de la Información y Seguridad Física.

LA GESTIÓN TECNOLÓGICA DEL RIESGO: UN NUEVO HORIZONTE

Sinopsis. GTR, un nuevo vocablo. Difiere en mucho a Gestión del Riesgo Tecnológico. De la misma forma que Prevención del Fraude Tecnológico difiere en mucho a Prevención Tecnológica del Fraude. La gestión del riesgo tecnológico, igual que la prevención de fraude tecnológico, se esfuerza mucho en caracterizar el riesgo y el fraude separando el que es tecnológico del que no lo es. GTR, este nuevo vocablo encierra un cambio en la filosofía con la que acercarnos, desde los departamentos de Seguridad de la Información, a los problemas de fraude, riesgo, control interno y auditoría. Nace una nueva disciplina, donde los conocimientos aprendidos en seguridad son el mejor punto de arranque. Esta nueva disciplina requiere que incorporemos a nuestro currículo formación en minería de datos, estadística, búsqueda de patrones de comportamiento y, en general, que nos transformemos en expertos en las tecnologías que sirven para gestionar el fraude, el riesgo, el control interno y los procesos de auditoría. No son tan distintas a las "nuestras" y parece que podría ser una evolución natural de "nuestros" años de experiencia.

Ponente:

Santiago Moral Rubio es Director de Seguridad de la Información del Grupo BBVA. Con más de una década de experiencia en seguridad y protección de la información, este Ingeniero Técnico Informático, poseedor de las certificaciones CISA y CISM, 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, para pasar posteriormente a ocupar la Dirección de Seguridad Lógica Corporativa del Grupo BBVA hasta su nombramiento en 2009 como CISO.

ARSYS: ENFOQUE Y GESTIÓN OPERATIVA DE RIESGOS DE SEGURIDAD EN SERVICIOS

Sinopsis. Llevamos años escuchando que una parte relevante del desarrollo de la Sociedad de la Información descansa sobre la evolución del uso de Internet por parte de la sociedad, entendida en un sentido amplio: administraciones públicas, empresas privadas, ciudadanos, etc. Igualmente, siempre se habla de las amenazas que existen en el uso de Internet, las herramientas para reducir el riesgo asociado a estas amenazas, la colaboración entre las organizaciones involucradas en la seguridad, etc. Sin embargo, bajar al mundo real de la gestión de los riesgos de seguridad, en un entorno en el que se puede pasar del aburrimiento al pánico en cuestión de segundos, requiere mucho más que productos, servicios profesionales y buenas intenciones. Dentro de este marco, la gestión de la seguridad requiere de una combinación de personas, herramientas, metodología, mucha masa gris y cierta osadía que constituya, en su conjunto, una organización bien engrasada y capaz de adoptar decisiones ejecutivas de forma rápida y eficaz.

Ponente:

Sven Olof Sandstrom Herrera es Director General de Operaciones de Arsys Internet. Ingeniero Técnico de Telecomunicaciones, es, asimismo, Presidente de la Comisión de Seguridad Integral de Ametic. Cuenta con las certificaciones CISA y CISM, y es Auditor Jefe acreditado ISO 27001.

GUARDIA CIVIL: SEGURIDAD GESTIONADA DESDE DOS SOC

Sinopsis. En la presentación se abordará el reto de la protección de los sistemas de información y plataformas críticas de comunicaciones e Internet de la Guardia Civil, y cómo poder conseguir el equilibrio entre el despliegue completo de un Centro de Operaciones de Seguridad interno con las máximas garantías de confidencialidad, seguridad y eficiencia, y a la vez combinarlo con la federación con el Centro de Operaciones de Seguridad de Telefónica, de forma que se aprovechen las escalas, experiencia, plataformas y tamaño de Telefónica GG.CC. y sus clientes. Al tiempo se expondrá cómo fue el proceso de diseño del SOC de GC con el equipo de Arquitecturas e Ingeniería de Seguridad de Telefónica y el equipo de Sistemas y Comunicaciones de la Guardia Civil.

Ponentes:

Pedro Morcillo Rueda es actualmente Jefe del Área de Redes y Seguridad del Servicio de Telecomunicaciones de la Guardia Civil. Comandante de Transmisiones de la Escala Superior de Oficiales del ET, Ingeniero Superior de Telecomunicaciones (Universidad Carlos III de Madrid) y Postgrado de Especialidad en Sistemas de Telecomunicaciones para la Defensa, dispone de un extenso currículo de formación en el ámbito de la Ingeniería, la Guerra Electrónica, la Protección Electrónica y en el ámbito global de los Sistemas de Telecomunicaciones y Transmisiones del Ejército. Ha realizado misiones en el extranjero relacionadas con sus especialidades (Bosnia-Herzegovina, Macedonia y La Antártida) y ha sido repetidamente condecorado.

Juan Miguel Velasco López-Urda es actualmente Gerente de Ingeniería y Preventa de Seguridad de la Unidad de Grandes Clientes de Telefónica España. Anteriormente ejerció en Telefónica Empresas como Subdirector de Arquitecturas y Servicios de Seguridad de la Línea de *Outsourcing*, Subdirector de Arquitecturas y Planificación de Infraestructuras, y antes como Subdirector de Ingeniería de Proyectos y Servicios de Protección de la Información de la UN Hosting y ASP, así como CTO y COO y Director de Consultoría de la Agencia de Certificación Electrónica (ACE), sociedad filial de Telefónica DataCorp. Profesor titular de Máster de Dirección y Gestión de Seguridad de la Información, es asimismo miembro de la Cátedra de Riesgos de Empresa y del Comité de dirección de ISMS Forum Spain. Cursó sus estudios de Informática Superior en la Universidad Politécnica de Madrid y entre otros es Máster Executive de Gestión Empresarial por Insead-Euroforum.

ENDESA: SERVICIO DE DESARROLLO DE CÓDIGO SEGURO DESDE "LA NUBE"

Sinopsis. Se expondrá la experiencia práctica de Endesa en el uso de este innovador servicio que funciona de forma descentralizada en la nube. Con él pueden auditar simultáneamente múltiples códigos fuente a través de un *Framework Web-Based*. Sus desarrolladores conocen al mismo tiempo que programan el software, cómo corregir los posibles códigos vulnerables, proponiendo soluciones efectivas para generar aplicativos seguros antes de que estos pasen a explotación. Igualmente, le sirve para verificar que sus aplicaciones desarrolladas por terceros son seguras. De esta manera, Endesa controla la seguridad de sus aplicativos desde el desarrollo de los mismos, donde radica la raíz de la inmensa mayoría de los problemas de seguridad en Internet.

Ponentes:

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

Abel González Lanzarote es Director de Desarrollo de Negocio de Ecija. Con anterioridad, durante más de seis años, fue socio-fundador y Director de Desarrollo de Negocio de ESA *Security,* empresa especializada en seguridad de la información. Antes de cofundar ESA *Security,* era el responsable de Desarrollo Corporativo en la compañía de seguridad informática Cyberguardian. Asimismo, fue durante varios años Director de Desarrollo de Negocio y Regulatorio para España y Portugal de la multinacional norteamericana de telecomunicaciones Viatel. Licenciado en Derecho por la Universidad de Salamanca, cuenta con un LLM, Máster en Derecho y Nuevas Tecnologías, por el King's College de la Universidad de Londres. Es CISA, CISM y CGEIT por ISACA. Es, igualmente, miembro de la Junta Directiva y presidente de la Comisión de Seguridad de ANEI (Asociación Nacional de Empresas de Internet).

GRUPO BANCO POPULAR: MOVILIDAD Y CONTROL DE ACCESO A LA RED

Sinopsis. Banco Popular ha puesto en marcha un proyecto de seguridad y comunicaciones para realizar un control de acceso a la red que reconcilie seguridad y movilidad de sus usuarios. El objetivo es proteger la red de la organización de accesos no autorizados examinando el "endpoint", que abarca dispositivos tales como PCs de sobremesa, portátiles y *netbooks*, e incluso sofisticados dispositivos móviles. A través de una combinación de tecnologías de seguridad, la solución de NAC incorpora tanto autorización como autenticación, control de acceso en base a roles y políticas de seguridad, con el fin de proporcionar un control lo más robusto posible sin dejar de ser flexible para el negocio. La solución, además de contemplar el acceso de invitados y facilitar la continuidad de negocio, cumple con todos los requisitos internos y regulatorios de la organización; es flexible, escalable y reduce costes al centralizar la gestión de accesos de red en una única plataforma.

Ponentes:

Francisco Javier Pastor Postillo es Responsable de Arquitectura de Comunicaciones del Grupo Banco Popular. Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid, especializado en el área de Telemática, cuenta con diferentes títulos y diplomas en el ámbito de las Telecomunicaciones y es integrante del foro de comunicaciones de Gran Banca Española. Tiene más de 13 años de experiencia en entornos de comunicaciones mixtos: datos (LAN y WAN), voz y seguridad en las comunicaciones. Pastor ha desarrollado gran parte de su carrera profesional dentro del Grupo Banco Popular desempeñando diferentes puestos y funciones y desde hace 5 años como responsable del Departamento de Arquitectura de Comunicaciones del Grupo Banco Popular, liderando un equipo de trabajo que desarrolla proyectos de Comunicaciones (datos, voz y multimedia) y de la Seguridad del entorno de Red.

Rodrigo Blanco Rincón es Director de la Oficina de Proyectos en Bull España. Ingeniero Superior de Telecomunicaciones por la Universidad Politécnica de Madrid, y Máster en Gestión y Dirección de la Seguridad de la Información, por la Universidad Pontificia de Salamanca y Asimelec –hoy Ametic–, está certificado como CISA por ISACA y PMP por el Project Management Institute. Es ponente habitual en los foros y conferencias de la industria de seguridad.

SARA LEE: GESTIONANDO LA PRESENCIA EN LA RED Y LOS RIESGOS ASOCIADOS

Sinopsis. La gestión de la información de las organizaciones es crucial ya que contiene datos de negocio, estrategias, datos personales y un largo etcétera. Aunque existen medidas que ayudan a controlar la información que pueda salir de nuestra organización, como soluciones DLP o DRM, estas deben ser complementadas con otro tipo de metodologías y herramientas que permitan determinar la efectividad y eficiencia de los controles establecidos. Del mismo modo, debe conocerse la presencia de información en Internet en diferentes ámbitos: buscadores, bases de datos semi-privadas, redes sociales, redes P2P, etc. Asimismo, para el CISO, así como para otros miembros de la dirección, es estratégico conocer cuál es el grado de presencia, qué se dice de su compañía y de sus productos o cuál es el uso de las marcas, o incluso activos presentes en la red de la compañía.

En esta ponencia se describirá la estrategia de Sara Lee Corporation para afrontar estos retos, considerando los principales aspectos a tener en cuenta, como la organización, la privacidad de los datos y las personas, las normativas de comunicación y uso de la marca, así como el correcto cumplimiento de la política de seguridad y poder complementar las contramedidas tecnológicas existentes.

Ponentes:

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

Daniel Solís Agea es socio fundador y CEO de blueliv. Actualmente dirige la estrategia de la compañía y su expansión internacional. Ingeniero en Telecomunicaciones, Solís ha trabajado en las Naciones Unidas en Nueva York, y ha desarrollado parte de su carrera profesional como Director en KPMG gestionando la línea de servicios de *Information Protection and Business Resilience*. Con más de trece años de experiencia, ha participado en diferentes proyectos de seguridad desarrollando estrategias corporativas en materia de protección de la información, como planes directores, expansiones internacionales de planes directores y estratégicos de seguridad, SGSIs, etc. Asimismo, Solís ha creado, formado y colaborado en equipos de consultores en seguridad de la información y de *hacking* ético en varias empresas del sector, como S21sec, de la cual fue cofundador y miembro del equipo inicial. Es ISO 27001 Lead Auditor acreditado por IRCA, miembro activo de AEDEL y creador de la distribución forense AD-QUIERE.

EL CAMINO ADECUADO PARA UNA SEGURIDAD EFECTIVA: EL CASO DE ÉLOGOS

Sinopsis. élogos es una empresa puntera en el sector de la formación en *e-learning*, en el que las tecnologías de la información van tomando cada vez más importancia en el núcleo de su negocio, y que comienza a tomar medidas concretas en Seguridad TIC de forma dinámica y adaptada a sus necesidades. La definición de una hoja de ruta basada en el conocimiento de la compañía y del establecimiento de objetivos alcanzables es de vital importancia para conseguir la adopción de un modelo que proporcione buenos resultados. En este contexto, partir de la definición del nivel de madurez de la compañía en lo que a Seguridad TIC se refiere, y en función del resultado obtenido, planificar las acciones a realizar a corto, medio y largo plazo, en todos los aspectos (organizativos, técnicos y procedimentales), y con una priorización y planificación adecuadas, garantiza la relación óptima entre beneficio obtenido y esfuerzo invertido, y por tanto, el grado de efectividad del plan en su conjunto.

Ponentes:

Xavier Netto Camero es Director de Explotación y Arquitectura TIC en élogos. Ingeniero Informático por la Universidad Autónoma de Barcelona, Máster en Aplicaciones Cliente-Servidor por la Universidad Politécnica de Cataluña y Máster en Gestión y Dirección de Empresas por el Instituto Catalán de Tecnología, cuenta con más de 20 años de experiencia en el sector de las TIC por lo que prácticamente ha ocupado todos los roles posibles iniciándose desde la pura operación de los servicios, desarrollo de aplicaciones hasta puestos de dirección de proyectos, dirección comercial de productos y dirección estratégica de diferentes áreas TIC.

Joaquín Crespo Pérez es Gerente de Producción en la Subdirección de Seguridad TIC de Grupo Gesfor. Ingeniero Técnico de Telecomunicación con especialidad en Telemática por la Universidad de Alcalá de Henares, cuenta con 10 años de experiencia en el sector de la Seguridad IT. Comenzó su carrera profesional en el año 2000 en SGI (Soluciones Globales Internet), como Ingeniero de Proyectos del Área de Seguridad Lógica. Posteriormente, se incorporó a Germinus XXI, (desde 2006 dentro del Grupo Gesfor) como Jefe de Proyectos e Ingeniero Senior de la División de Seguridad e Infraestructuras de Redes Corporativas. Desde 2008 realiza la coordinación de todas las tareas de producción del área.

TERCER MÓDULO, 14 de abril

09:15h. Entrega de documentación.

Moderador: **José Carrillo Verdún**, Facultad de Informática de la Universidad Politécnica de Madrid.

09:30h. Ponencia: "**La tarjeta de ciudadano de Portugal**".
Ponentes:
- **Gonçalo Caseiro**, Miembro de la Oficina de la Agencia para la Reforma de Servicios Públicos AMA, de Portugal.
- **Pedro Pombo Rodrigues**, Senior Manager. Responsable del Área de Seguridad de Accenture Portugal.

10:05h. Coloquio.

10:10h. Ponencia: "**STORK: la aceptación transfronteriza de identidades electrónicas europeas**".
Ponentes:
- **Miguel Álvarez Rodríguez**, Jefe del Área de Cooperación en Tecnologías de la Información en la Dirección General para el Impulso de la Administración Electrónica del Ministerio de Política Territorial y Administración Pública. MPTyAP.
- **John Heppe**, Jefe de Proyecto. Sistemas de Seguridad de INDRA.

10:45h. Coloquio.

Espacio monográfico:
ESQUEMA NACIONAL DE SEGURIDAD

Moderador: **Julián Inza Aldaz**, Presidente de Grupo Interactiva.

10:50h. Ponencia: "**Creación del Plan de Adecuación al Esquema Nacional de Seguridad y al Esquema Nacional de Interoperabilidad de la Diputación de Castellón".**
Ponentes:
- **Antonio Sáez Sanz**, Jefe del Servicio de Informática de la Diputación de Castellón.
- **Javier Megias Terol**, Director Regional de Levante. GMV Soluciones Globales Internet.

11:25h. Coloquio.

11:30h. Pausa-café.

12:00h. Ponencia: **"Plan de adecuación al Esquema Nacional de Seguridad y al Manual de Seguridad PLATEA"**.
Ponentes:
- **José Ángel Rodríguez**, Responsable de Sistemas Informáticos del Gobierno Vasco.
- **Juantxu Mateos Gil**, Director de Innovación y Desarrollo de Negocio de Nextel.

12:35h. Coloquio.

Moderador: **Luis Fernández Delgado**, Editor de la revista SIC.

12:40h. **Debate:** "**El control del uso de privilegios sobre la información por los usuarios autorizados**".
Participantes:
- **Javier Candau Romero**, Subdirector General Adjunto del Centro Criptológico Nacional, CCN. Supervisor del CCN-CERT.
- **Manuel Carpio Cámara**, Director de Seguridad de la Información y Prevención del Fraude. Telefónica.
- **Juan Cobo Páez**, Jefe del Departamento de Seguridad de la Información de Ferrovial.
- **Jorge Dávila Muro**, Director del Laboratorio de Criptografía LSIIS – Facultad de Informática de la UPM.
- **Javier del Riego Fernández**, Responsable de Seguridad ICT de Vodafone España.

14:00h. Fin del debate.

14:10h. Clausura y fin de la tercera sesión.

14:15h. Almuerzo.

LA TARJETA DE CIUDADANO DE PORTUGAL

Sinopsis. La Tarjeta de Ciudadano Portugués es un documento de ciudadanía. Como documento físico permite a su portador su identificación personal segura. Como documento tecnológico facilita la identificación de una persona a la hora de tratar con servicios informáticos y autenticar documentos electrónicos. La tarjeta de ciudadano es un proyecto que contribuye a la modernización de la Administración Pública y a su dinamismo. Un aspecto destacado de la misma es que mediante un único documento combina todas las claves indispensables para facilitar la relación rápida y eficaz del ciudadano con una amplia variedad de servicios públicos. Asimismo, promueve el desarrollo de transacciones electrónicas proporcionando a los usuarios la tranquilidad de una autenticación fuerte y una firma electrónica cualificada. En esta presentación nos centraremos en los antecedentes, los objetivos, los componentes y el conjunto del proyecto del Programa de Tarjeta de Ciudadano de Portugal.

Ponentes:

Gonçalo Caseiro es Miembro de la Oficina de la Agencia para la Reforma de los Servicios Públicos (AMA) de Portugal. Posgraduado en Inteligencia de Negocio y Gestión del Conocimiento por el Instituto de Estadística y Gestión de la Información de la Universidad de Lisboa –con especialización en "Arquitectura en Nuevos Paradigmas y Redes, Ciencia Informática y Seguridad TI", en la Escuela Nacional Superior de Telecomunicaciones de París–, es asimismo graduado en Ingeniería Informática por el Instituto Superior Técnico de la Universidad de Lisboa. Dispone de la Certificación de Gestión de Proyectos por la Asociación Portuguesa de Gestión de Proyectos. En su experiencia profesional ha sido Director de Accenture, en el área de Administración Pública, donde llevó a cabo numerosos proyectos en los ámbitos de TIC, Estrategia y Gobierno. Desde diciembre de 2009 es Miembro de la Oficina de la Agencia para la Reforma de los Servicios Públicos.

Pedro Pombo Rodrigues es Senior Manager en Accenture Technology Consulting y Responsable de la Práctica de Seguridad para Portugal, España, África e Israel. Cuenta con una década de experiencia en consultoría en infraestructuras y seguridad de varios sectores. Acreditado por $(ISC)^2$ como ISSC, Rodrigues formó parte del equipo de Accenture en el programa de la Tarjeta del Ciudadano Portugués, y contribuyó al diseño de las especificaciones funcionales y técnicas para la tarjeta inteligente del ciudadano (tanto los componentes físicos, como el chip y los lectores), estaciones de despliegue biométrico, el sistema nacional AFIS y la PKI nacional, así como los sistemas de gestión del ciclo de vida de las tarjetas. Asimismo ha realizado tareas de consultoría en asuntos de infraestructura y seguridad vinculados a las tendencias europeas relativas al eID.

STORK: LA ACEPTACIÓN TRANSFRONTERIZA DE IDENTIDADES ELECTRÓNICAS EUROPEAS

Sinopsis. El proyecto STORK (Secure idenTity acrOss boRders linKed) ha establecido una plataforma de interoperabilidad y reconocimiento mutuo transfronterizo de las identidades electrónicas existentes en Europa, la cual permitirá a los ciudadanos acceder e identificarse en servicios de administración electrónica de otros países europeos a través del uso de sus DNIe o identidades electrónicas nacionales. En el consorcio STORK participan 32 organizaciones de 14 países europeos, cuyas credenciales serán aceptadas en estos mismos países. En un principio, estos servicios se definieron a través de 6 pilotos de eGobierno que ya están operativos. A partir de finales de este 2011 otros proveedores de servicios se podrán conectar a la plataforma. Así permitirán a sus usuarios acceder a los servicios simplemente presentando su Identificación Electrónica nacional; la presencia física no será necesaria.

Ponentes:

Miguel Álvarez Rodríguez es Jefe de Área de Cooperación en TI de la Subdirección General de Gestión y RRHH de la Dirección para el Impulso a la Administración Electrónica en el Ministerio de Política Territorial y Administración Pública. Después de terminar la carrera como Ingeniero Superior de Telecomunicación, hizo un MBA por IEDE (Madrid). Es experto nacional en los grupos de trabajo de la Comisión Europea para la interoperabilidad de las firmas y la identidad electrónica, así como Jefe de Proyecto del servicio de validación de certificados y firmas electrónicas @firma. En STORK es líder del paquete de trabajo que diseña e implementa las especificaciones comunes de dicho proyecto europeo.

John Heppe es Jefe de Proyecto de Sistemas de Seguridad de Indra. Licenciado en Informática Empresarial en Holanda, estos últimos 10 años ha desarrollado su carrera profesional en Indra, donde actualmente desempeña el cargo de Jefe de Proyecto de STORK, habiendo sido el responsable técnico del diseño e implantación de las especificaciones comunes del proyecto.

EL ESQUEMA NACIONAL DE INTEROPERABILIDAD DE LA DIPUTACIÓN DE CASTELLÓN

Sinopsis. La Diputación de Castellón entendió que los esquemas nacional de seguridad (ENS) e interoperabilidad (ENI) representaban dos estupendas oportunidades que podían ser utilizados como elementos tractores para alinear con la estrategia de la Diputación los esfuerzos realizados en los campos de seguridad, interoperabilidad y administración electrónica. En este contexto, GMV ha desarrollado un proyecto para crear un Plan de Adecuación, soportado en herramientas que faciliten su seguimiento e implantación, y cuyo fin es explotar las múltiples sinergias y elementos comunes entre ambos esquemas con el fin de realizar una aproximación lo más eficiente y adaptada a la realidad administrativa posible.

Ponentes:

Antonio Sáez Sanz es Jefe del Servicio de informática de la Diputación de Castellón. Ingeniero superior por la Universidad Politécnica de Madrid y Máster en Direccion de Sistemas y Tecnologías de la Información y las Comunicaciones para la Administración Local por el INAP, tiene 24 años de experiencia en el sector TIC, fundamentalmente en el área de gobierno. Ha trabajado en marketing del sector público en IBM durante 11 años y en la Diputación Provincial de Castellón en el puesto actual hasta estos momentos.

Javier Megias Terol es Director Regional de la multinacional española GMV para la zona de Levante. Ingeniero Informático, ha complementado su formación con las titulaciones CIT y ADIT por la Universidad de Cambridge y AMP (Advanced Management Program) por IE Business School. Tiene más de 15 años de experiencia en las áreas de estrategia, innovación y dirección de grandes proyectos, y ha ocupado distintas posiciones en algunas de las compañías más relevantes del sector. En su faceta de comunicador, es coautor de dos libros, colabora con múltiples medios como escritor y conferenciante, imparte periódicamente clases en programas máster de diversas Universidades y es autor de un *blog* sobre estrategia e innovación. Asimismo, actúa como asesor y evaluador de proyectos de I + D + i para la Comisión Europea, forma parte del Comité para la Gestión de la I + D de Aenor y del Comité Europeo de Normalización en Gestión de la Innovación, concretamente como experto en las áreas de Gestión de la Creatividad y Colaboración.

PLAN DE ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD Y AL MANUAL DE SEGURIDAD PLATEA

Sinopsis. La Dirección de Informática y Telecomunicaciones del Gobierno Vasco ha creado PLATEA (Plataforma Tecnológica para la E-Administración) para establecer la construcción de un conjunto de módulos y sistemas comunes que constituyan una plataforma tecnológica de base para ofrecer los servicios de Administración Electrónica. Para garantizar esta seguridad, el Gobierno Vasco ha desarrollado un Manual de Seguridad para PLATEA, en la que establece una serie de directrices de seguridad adicionales, con la intención de convertir los servicios del Gobierno Vasco en un referente de confianza en los servicios públicos electrónicos a nivel nacional. Para la acometida del proyecto, el Departamento de Informática y Telecomunicaciones del Gobierno Vasco contó con Nextel S.A., que, como gran conocedora de las exigencias normativas aplicables y dada su acreditada experiencia en el ámbito de la seguridad, se hizo acreedora de la confianza necesaria para abordar tan importante proyecto.

Ponentes:

José Ángel Rodríguez González es Responsable de Sistemas Informáticos de la Dirección General de Informática y Telecomunicaciones del Gobierno Vasco. Con labores de asesoría, planificación estratégica, estandarización y coordinación de recursos en dicho ámbito, Rodríguez es ingeniero en Informática por la UPV/EHU. Anteriormente desempeñaba tareas similares como Jefe de Proyectos de Sistemas de Información en la extinta Dirección de Organización y Sistemas de dicha Administración Pública y fue Jefe del Área Informática del Instituto Vasco de Estadística. Ha sido CISA y desempeñado actividades relacionadas con la seguridad.

Juantxu Mateos Gil es Director de Innovación y Desarrollo de Negocio de Nextel S.A. Experto en la promoción de proyectos de centros de operaciones de seguridad, gestión de identidades e implantación de normativas internacionales de seguridad, su dilatada experiencia en la compañía –de la cual es socio fundador– le convierte en una fuerza impulsora clave para el desarrollo de nuevos focos de negocio y apertura de mercados con tecnologías orientadas al futuro.

DEBATE

EL CONTROL DEL USO DE PRIVILEGIOS SOBRE LA INFORMACIÓN POR LOS USUARIOS AUTORIZADOS

Proposición. Asuntos como el de WikiLeaks han reavivado la polémica en torno al control del uso que dan a la información de valor aquellas personas que por su posición en una entidad tienen acceso a ella –o posibilidades de tener acceso– con el fin de paliar el riesgo de filtraciones y robos que pudieran afectar a negocios y que también pudieran comprometer el buen nombre de la la organización y de sus gestores por incumplimiento de leyes y/o compromisos con terceros. En general, las fugas y sustracciones de información perpetradas por personal desleal, suelen realizarse hoy en el sistema de información y usando en parte del proceso herramientas de TIC. En el debate se tratará de fijar qué posibilidades hay de trazar con arreglo a la ley las actividades de empleados y colaboradores, qué permite hoy la tecnología para ayudar a gestionar tal riesgo y facilitar evidencia de los hechos y quién o quiénes deben participar en el control.

Intervienen:

Javier Candau Romero es Subdirector General Adjunto del Centro Criptológico Nacional, Supervisor del CCN-CERT. Teniente Coronel de Artillería, Ingeniero Industrial con especialidad en Electrónica y Automática, y especialista criptólogo, dispone de diversas certificaciones de especialización en seguridad de las TIC (ISS, SANS, CRAMM, Curso de Auditoría del INAP, etc.). Los principales cometidos de su actividad son la formación del personal especialista en seguridad de la Administración, el desarrollo de normativa del CCN (elaboración de políticas, directrices y guías de seguridad de las TIC para la Administración Pública-Series CCN-STIC), desarrollo de la herramienta de análisis de riesgos PILAR, la supervisión de acreditación de sistemas y la realización de auditorías de seguridad. Tiene más de 15 años de experiencia en todas estas actividades. Es, además, supervisor de la Capacidad de Respuesta ante Incidentes gubernamental (CC_CERT. www.ccn-cert.cni.es).

Jorge Dávila Muro es Profesor Titular de la Facultad de Informática de la Universidad Politécnica de Madrid (UPM) y desarrolla sus actividades académicas en el ámbito de la Criptología, la Seguridad Informática y en el diseño de nuevos sistemas avanzados para la sociedad de la información. Desde 1993, el profesor Dávila dirige el Laboratorio de Criptología de la UPM en el que, además de desarrollar sus investigaciones, se dedica a la formación y capacitación de nuevos profesionales de la seguridad informática. El profesor Dávila es, desde su inicio y en concepto de experto, miembro de la representación española en el 7º Programa Marco de la UE, en el programa de Seguridad. Igualmente es Responsable de Desarrollo de Negocio e Innovación de CriptoTec.

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

Juan Cobo Páez es Jefe del Departamento de Seguridad de la Información y Continuidad de Negocio de Ferrovial. Ingeniero Técnico Informático por la Universidad Politécnica de Madrid y PDD por IESE. Dispone de las certificaciones CISA, CISM y CRISC de ISACA. Tiene más de 18 años de experiencia en el sector de las Tecnologías de la Información, en los que ha trabajado en compañías tales como Indra, Iecisa o Telefónica, y gran experiencia en la definición, despliegue y evolución de marcos, modelos y procesos de organización y control de la función de TI. En 2005 se incorporó a Ferrovial.

Javier del Riego Fernández es Responsable de Seguridad ICT de Vodafone en España. Licenciado en Informática por la Universidad Politécnica de Madrid y Máster en Administración de Empresas por la EOI, a principios de 1994 se incorpora a Caja Madrid como auditor informático dentro de la unidad de Auditoría, en la que se responsabiliza de la ejecución y seguimiento de auditorías técnicas, tanto de la matriz como de las empresas de la corporación; a finales de 1997 da el salto a Seguridad Lógica en la operadora móvil Vodafone en España, por aquel entonces Airtel Móvil, donde, desde finales de 1998, asume la responsabilidad de la gestión del equipo, abarcando actualmente la seguridad de la información de todos los procesos tecnológicos del Grupo Vodafone en España.

> SECURMATICA, a escena

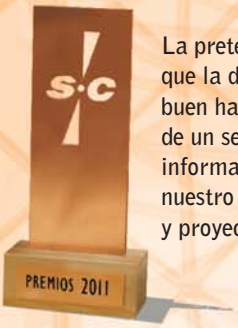
Panorámica de SECURMÁTICA 2010

> Premios SIC 2011

REVISTA S!C PREMIOS 2011

En coincidencia con su 20 aniversario y con la celebración de la XXII edición de Securmática, tendrá lugar el acto de entrega de los VIII 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 séptima edición de los premios SIC

LA HORA DEL REENCUENTRO Y LOS RECONOCIMIENTOS

> Cena de la Seguridad

SECURMATICA 2011

12.13.14|abril

XXII Congreso español de Seguridad de la Información

AFORO LIMITADO

> Fechas y lugar

SECURMÁTICA 2011 tendrá lugar los días 12, 13 y 14 de abril de 2011 en el hotel NOVOTEL*. Campo de las Naciones de Madrid.

> Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2011 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 la Seguridad y entrega de los VIII Premios SIC (13 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 € + 18% IVA	760 € + 18% IVA
2 Módulos	961 € + 18% IVA	1.105 € + 18% IVA
3 Módulos	1.141 € + 18% IVA	1.313 € + 18% 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.
– Inscripción solo al tercer módulo (día 14 de abril): 15% dto.

> Proceso de solicitud de inscripción

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

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

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

- Abono de 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, a:

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

El justificante de dicha transferencia o "escaneo" deberá ser remitido a Ediciones CODA vía fax, vía correo postal o por correo electrónico (info@securmatica.com).

- Las inscripciones solo se considerarán formalizadas una vez satisfecho el importe de las mismas antes de la celebración del Congreso.
- Las cancelaciones de inscripción solo 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 2011

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 12 ❑ MÓDULO 2 DÍA 13 ❑ MÓDULO 3 DÍA 14 ❑ Deseo inscribirme a SECURMATICA 2011

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:

SiC 20 ANIVERSARIO

Revista 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**