SECURMATICA

XXIII Congreso español de Seguridad de la Información

2012
24.25.26
abril

Seguridad, inteligencia y reputación

PROGRAMA

ES HORA DE COMPARTIR EXPERIENCIAS Y AVANZAR

Securmática 2012 tendrá lugar los días 24, 25 y 26 de abril en su tradicional sede del Campo de las Naciones de Madrid.

El ritmo de transformación imperante y el avance de los medios tecnológicos que lo realimentan están contribuyendo a forzar una renovada visión de la gestión de los riesgos en los negocios en la que la presión del cumplimiento (a escala doméstica y global), la búsqueda de la eficiencia, la rendición de cuentas de cotizadas a los inversores y el cuidado de la buena reputación se convierten en las reglas del juego en el camino trazado con el uso de "inteligencia" para fijar y alcanzar objetivos.

Una función bien asentada de protección de la información tratada principalmente en sistemas tecnológicos –en sus dos vertientes más significadas: la mitigación del fraude y la ciberseguridad– debe estar en disposición de alimentar el sistema de inteligencia de una corporación y ayudar a la toma de decisiones fundamentadas.

Para obtener ventajas en una orientación hacia la inteligencia hay que integrar todos los procesos de seguridad y, una vez conseguido, fundirlos con los de negocio y actividad, de tal suerte que evolucionen al unísono.

Y es en este contexto en el que se celebra la XXIII edición de Securmática, en cuyo marco se van a tratar asuntos de especial relevancia profesional: propuesta de marco único normativo de protección de datos en la UE, normalización de las evidencias digitales, la red de fiscales especializados en la persecución de la criminalidad informática, las ciberarmas, la lucha contra las APTs, los SIEM de nueva generación…

Al tiempo, se presentarán proyectos de seguridad y relacionados de gran calado, como en el caso de algunos alusivos a la implantación de GRC, de inteligencia y seguridad, de sistemas corporativos de seguridad con base en fuentes abiertas, de gestión de calidad de datos, de uso de la nube por parte de una entidad financiera multinacional para colaboración y productividad, de gestión de CERTs, de implantación y uso de DRM y de despliegue de servicios de MSSP.

Igualmente, se presentará un plan de ciberseguridad de Infraestructuras Críticas realizado por un operador de IC en España, la prueba de ciberseguridad en el sector financiero británico: 2011 UK FSA Market Wide Exercise, y se celebrará un debate titulado: "¿Aporta la titulación de Director de Seguridad Privada los conocimientos necesarios para gestionar la ciberseguridad de Infraestructuras Críticas?"

Copatrocinadores

accenture – Alto rendimiento. Hecho realidad.
arsys.es
bluelive
Ernst & Young – Quality In Everything We Do
gmv – Innovating Solutions
hp
IBM
indra
logica – be brilliant together
Nextel S.A. – Ingeniería y Consultoría
pwc
S21sec
Telefónica

Organiza

SiC – Revista seguridad en informática y comunicaciones

SIC Seguridad en Informática y Comunicaciones es desde 1992 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.

Securmática se reserva el derecho a modificar el contenido o los ponentes de este programa si las circunstancias así lo requieren.

PRIMER MÓDULO, 24 DE ABRIL

08:45h. Entrega de Documentación.
09:15h. Inauguración oficial.
Moderador: **Arturo Ribagorda Garnacho**, Catedrático de la Universidad Carlos III de Madrid.
10:10h. Conferencia de apertura:
El nuevo Marco Europeo de Protección de Datos.
Ponente: **José Luis Rodríguez Álvarez**, Director de la Agencia Española de Protección de Datos.
10.45h. Coloquio.
10:50h. Ponencia: **La red de Fiscales de Criminalidad Informática: investigación y persecución de las conductas delictivas.**
Ponente: **Elvira Tejada de la Fuente**, Fiscal de Sala. Fiscal Jefe de Criminalidad Informática. Fiscalía General del Estado.
11:25h. Coloquio.
11:30h. Pausa-café.
Moderador: **José Antonio Mañas**, Catedrático de la Universidad Politécnica de Madrid.
12:00h. Ponencia: **Normalizando las evidencias o de cómo los juristas y los técnicos se hablan entre sí.**
Ponente: **Paloma Llaneza González**. Abogado y CISA. Socio de Razona Legaltech y Presidenta de AEDEL, Asociación Española de Evidencias Electrónicas.
12:35h. Coloquio.
12:40h. Ponencia: **Los ingredientes del agujero perfecto: SGSI por compromiso + desconocimiento de lo que las TIC aportan al control de riesgos.**
Ponente: **Román Ramírez Giménez**, Presidente y Cofundador de RootedCon.
13:15h. Coloquio.
13:20h. Ponencia: **Plan de ciberseguridad en las Infraestructuras Críticas de Gas Natural Fenosa.**
Ponentes:
Andreu Bravo Sánchez, Responsable de la Seguridad en los Sistemas de la Información de Gas Natural Fenosa.
Manel Álvarez González, Gerente. Estrategia y Desarrollo de Negocio Sector Industria. S21sec.
13:55h. Coloquio.
14:00h. Almuerzo.
Moderador: **Jorge Dávila Muro**, Director del Laboratorio de Criptografía LSIIS - Facultad de Informática de Universidad Politécnica de Madrid.
16:00h. Ponencia: **Repsol: Seguridad e inteligencia desde los inicios.**
Ponentes:
Javier Velasco Vidal, Director de Ingeniería de Seguridad y Análisis Forense de Repsol.
Vicente de la Morena Baena, Responsable de Ventas de Seguridad de Infraestructura para el Sur de Europa de IBM.
16:35h. Coloquio.
16:40h. Ponencia: **Produban: seguridad + *open source*: ¿funciona?**
Ponentes:
Daniel Concepción López, Head of Global Systems de Produban (Santander).
Iñaki Murcia García, Director de la Zona Centro de Nextel, S.A.
17:15h. Coloquio.
17:20h. Pausa-café.
17:35h. Ponencia: **Endesa: implantación de SAP GRC.**
Ponentes:
Joaquín Álvarez Pérez, Subdirector de Seguridad de la Información de Endesa.
Javier Fernández Bonache, Manager de Accenture.
18:10h. Coloquio.
18:15h. Fin de la primera jornada.

EL NUEVO MARCO EUROPEO DE PROTECCIÓN DE DATOS

Sinopsis. La revisión del marco europeo de protección de datos ha iniciado su última fase con la presentación por la Comisión de dos propuestas normativas: un Reglamento General de Protección de Datos y una Directiva aplicable a las actividades del ámbito policial y judicial.
El Reglamento, la pieza central del nuevo modelo contribuirá a dotar de mayor homogeneidad al sistema por cuanto se trata de una norma que se aplica directamente en todos los Estados Miembros. Con ello se reducirán notablemente las divergencias resultantes de las trasposiciones nacionales de la directiva del año 1995.
El Reglamento refuerza los principios y derechos básicos que han caracterizado la protección de datos en Europa. Al mismo tiempo, introduce una serie de elementos nuevos que han marcado el debate sobre la renovación de los mecanismos de protección durante los últimos años.
Entre estos elementos son especialmente reseñables los que persiguen incrementar el compromiso de las entidades que tratan datos personales con la protección de los derechos de los individuos: el análisis de impacto sobre protección de datos, la privacidad en el diseño, la privacidad por defecto o los esquemas de certificación. En esta misma línea se pueden incluir las previsiones sobre notificaciones de incidentes de seguridad. En contrapartida, el proyecto de Reglamento contempla la supresión del requisito general de notificación.
Otras dos novedades importantes son el reforzamiento de los poderes y de los mecanismos de cooperación entre las autoridades de protección de datos, lo cual incluye la atribución con carácter general de capacidad sancionadora en el marco de un nuevo régimen sancionador armonizado.

Ponente:

José Luis Rodríguez Álvarez es desde el 17 de junio de 2011 Director de la Agencia Española de Protección de Datos. Su anterior cargo (desde febrero de 2009) fue el de director del Gabinete del Ministro de Justicia. Su trayectoria es amplia: de 2002 a 2004 fue director gerente de la Fundación Democracia y Derecho Local; en abril de 2004 fue nombrado director del Gabinete del Secretario de Estado de Relaciones con las Cortes, y desde abril de 2008 hasta febrero de 2009 desempeñó el cargo de director general de Coordinación Jurídica en el Ministerio de la Presidencia. Rodríguez Álvarez es Licenciado en Derecho y Profesor de Derecho Constitucional en la Facultad de Derecho de la Universidad Complutense de Madrid. Ha realizado estudios de postgrado en la Facultad de Derecho de la Universidad de Heidelberg (Alemania) y ha sido investigador en el Max-Planck-Institut de Derecho Público y Derecho Internacional durante tres años.

LA RED DE FISCALES DE CRIMINALIDAD INFORMÁTICA: INVESTIGACIÓN Y PERSECUCIÓN DE LAS CONDUCTAS DELICTIVAS

Sinopsis. El proceso de especialización del Ministerio Público español ha determinado la reciente articulación de esta red de Fiscales que, coordinada a nivel nacional por un Fiscal de la primera categoría, se integra por los Delegados de esta especialidad designados en todas las Fiscalías provinciales, y pretende potenciar la eficacia del Ministerio Fiscal ante este fenómeno criminal. La actuación en red de los Fiscales especialistas y su preparación específica en esta materia hacen de esta iniciativa un instrumento altamente eficaz para la fijación y mantenimiento de criterios uniformes en la interpretación y aplicación de las normas jurídicas, la coordinación en las investigaciones que trascienden el ámbito provincial y el establecimiento de relaciones fluidas y constantes con las fuerzas y cuerpos de seguridad y los restantes organismos con responsabilidad en este ámbito, sin olvidar su extraordinaria importancia para facilitar la cooperación con las autoridades judiciales de otros Estados.

Ponente:

Elvira Tejada de la Fuente es Fiscal de Sala Coordinadora en materia de Criminalidad Informática, puesto para el que fue nombrada el 1 de abril de 2011 y del que tomó posesión el 12 de julio de ese año. En el ejercicio de esta responsabilidad ha participado activamente en la elaboración de la Instrucción 2/2011 de la Fiscalía General del Estado (octubre) y en la puesta en funcionamiento de la red de Fiscales especialistas, cuya dirección asume actualmente. Tejada de la Fuente ingresó en el Ministerio Fiscal en 1981, Institución en la que hasta su actual responsabilidad ha desempeñado las siguientes funciones: Fiscal de la Audiencia Provincial de Guipúzcoa, Fiscal del Tribunal Superior de Justicia de Madrid (destino en el que desempeñó, entre otras funciones, la coordinación de la actividad de la Fiscalía ante los Juzgados de la Plaza de Castilla), asesora del Centro de Estudios Jurídicos en materia de Formación de Fiscales y de Unidades de Policía Judicial (1996-1999) y Fiscal Jefe de la Secretaría Técnica de la Fiscalía General del Estado, con categoría de Fiscal de Sala, desde julio de 2004 a julio de 2011. En el ejercicio de esta actividad, asumió las funciones propias de la Delegación del FGE en materia de Delincuencia Informática entre diciembre de 2007 y noviembre de 2008.

NORMALIZANDO LAS EVIDENCIAS O DE CÓMO LOS JURISTAS Y LOS TÉCNICOS SE HABLAN ENTRE SÍ

Sinopsis. Los diálogos interprofesionales no son sencillos. Sin un profundo respeto por el conocimiento de cada parte y un mapeo de elementos y requerimientos, este diálogo está llamado a fracasar. Si el objetivo de sentar a la mesa a técnicos y a juristas desprejuiciados se realiza, estamos más cerca de establecer generalizaciones multijurisdicción y de conseguir su traslación, como requerimientos de usuario, al mundo técnico. Así se ha venido trabajando en la producción de normas que, partiendo de un modelo en tres fases, con tres parejas de atributos y completamente agnóstico en cuanto a la legislación aplicable, pretenden facilitar a la incompleta y cambiante legislación española de un marco estandarizado de generación, almacenamiento, transmisión y recuperación segura de información para dotarla de valor evidencial basándose en los estándares de la familia 27000, así como de una metodología de análisis forense que permita la adquisición, análisis y presentación de estas evidencias como prueba confiable e inalterada con el fin de que las haga prosperables en juicio o en otros entornos legales de resolución de disputas.

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 Desarrollo de las 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".

LOS INGREDIENTES DEL AGUJERO PERFECTO: SGSI POR COMPROMISO + DESCONOCIMIENTO DE LO QUE LAS TIC APORTAN AL CONTROL DE RIESGOS

Sinopsis. Los actuales mecanismos de gobernanza de seguridad en las distintas organizaciones adolecen de problemas diversos desde su concepción. Los enfoques más pragmáticos, orientados al mero cumplimiento, y las limitaciones en presupuestos y personal, llevan a tomar decisiones con cierto nivel de riesgo e, incluso, a la negociación forzosa de la adecuación a los requisitos de seguridad dentro de estas organizaciones. Esta situación es especialmente grave en organizaciones con responsabilidad sobre infraestructuras críticas o donde sus servicios pueden comportar riesgos para el usuario y ciudadano. El propósito de esta conferencia es exponer dónde se asumen riesgos excesivos o cómo las organizaciones realizan valoraciones suavizadas para poder manejar los controles a implantar y dónde los atacantes juegan con la ineficacia de estos enfoques.

Ponente:

Román Ramírez Giménez es Presidente y Cofundador del Congreso de Seguridad Técnica Rooted CON, actividad que compagina con sus actuales responsabilidades en Ferrovial como Arquitecto de Seguridad. Tiene una carrera profesional de más de quince años en tecnología y seguridad de la información, a lo largo de los cuales ha desarrollado funciones en empresas tan diversas como eEye Digital Security o PricewaterhouseCoopers, pasando por una etapa como emprendedor con su compañía Chase The Sun.

PLAN DE CIBERSEGURIDAD DE LAS INFRAESTRUCTURAS CRÍTICAS DE GAS NATURAL FENOSA

Sinopsis. En la actualidad las redes de los sistemas que controlan las Infraestructuras Críticas están interconectadas con redes de gestión, redes de usuarios o incluso Internet, y el riesgo de que se materialice un incidente en estas infraestructuras es cada vez mayor. Así, el legislativo aprobó hace un tiempo la Ley de Protección de Infraestructuras Críticas. Consciente de ello, Gas Natural Fenosa ha realizado un análisis de ciberseguridad de sus sistemas industriales de control de la distribución de gas y electricidad en España como base para su adecuación a la nueva Ley PIC. Mediante esta ponencia, se presentarán los pasos seguidos por Gas Natural Fenosa para la protección de los sistemas SCADA, así como del resto de sistemas de control, de las redes inteligentes *(Smart Grid)* y de nuevas tecnologías diseñadas para cubrir las necesidades incipientes del sector energético. Todo ello, necesario para asegurar el despliegue homogéneo de un plan de seguridad integral adecuado a la Ley PIC y a las futuras necesidades de demanda energética.

Ponentes:

Andreu Bravo Sánchez es Responsable de la Seguridad en los Sistemas de la Información de Gas Natural Fenosa. Con más de 20 años de experiencia profesional en las diferentes áreas de las TI (desarrollo, sistemas, comunicaciones, arquitectura y seguridad). Dispone del Certificado CISSP por (ISC)^2, CISM por ISACA e ISO-27001 Lead Auditor por BSI y es miembro del grupo de expertos de seguridad SGIS del SGCG encargado del desarrollo de estándares europeos para el M/490 sobre *smart grids*. Ha participado en la definición, gestión e implantación de los proyectos de seguridad de la información de la compañía. Entre ellos: gestión de identidades, definición de políticas de seguridad, clasificación de activos, análisis de riesgos, diseño de la seguridad perimetral, gestión operativa de la seguridad, certificación digital y firma electrónica, análisis de vulnerabilidades, delitos informáticos y fraude electrónico, DLP, etc. Asimismo, ha intervenido en el proceso estratégico de integración de los sistemas de la información del Grupo Gas Natural y de Unión Fenosa.

Manel Álvarez González es Responsable de la Estrategia y Desarrollo de Negocio para el Sector Industria, como Gerente de la división en S21sec, compañía reconocida dedicada al 100% a la seguridad. Antes de desarrollar estas funciones, se incorporó a S21sec como Responsable de los Servicios de Preventa. Álvarez ha desarrollado su carrera profesional en el sector IT en multinacionales como GE Capital ITS –como director de desarrollo de negocio de Enterprise Computing–, Computer Associates –como Customer Relationship Manager– y en la AEAT –como responsable de explotación y sistemas del centro regional de Cataluña–.

REPSOL: SEGURIDAD E INTELIGENCIA DESDE LOS INICIOS

Sinopsis. "Secure by Design" es el eslogan que resume la estrategia de IBM en materia de Seguridad. Desde el pasado 1 de enero de 2012, IBM ha dado un paso importante al poner en marcha su nueva división de Seguridad "IBM Security Systems" dentro del Software Group. Un buen exponente de dicha filosofía la encontramos en Repsol, compañía que desde hace años está en constante evolución en aspectos de seguridad en el Sector de la Energía, tanto en España como a nivel internacional. En el ámbito de las infraestructuras, Repsol está dotando a sus sistemas de seguridad de una capa de inteligencia que permita optimizar los procesos y encontrar sinergias entre las diferentes tecnologías implementadas.

Ponentes:

Javier Velasco Vidal es Responsable de Ingeniería de Seguridad y Análisis Forense en Repsol. Cuenta con 25 años de experiencia en el mundo de las TIs, 20 de ellos en Repsol, en el entorno de las telecomunicaciones y de la seguridad de la información durante los últimos 3 años.

Vicente de la Morena Baena es Responsable de Seguridad en las Infraestructuras en IBM Security para el sur de Europa. Cuenta con 16 años de experiencia en el sector TI, los últimos 14 en IBM en diferentes responsabilidades comerciales en el ámbito de la tecnología. Desde finales de 2010 es responsable comercial de la compañía ISS, actualmente integrada en la División Security Systems de IBM.

PRODUBAN: SEGURIDAD + *OPEN SOURCE*: ¿FUNCIONA?

Sinopsis. Produban y Nextel comparten en esta ponencia la experiencia y lecciones aprendidas en el desarrollo de un Sistema de Prevención de Intrusión basado en código abierto para su uso en entornos financieros. Después de muchos años de debate, la pregunta de si el código abierto está listo para su implantación en infraestructuras corporativas para la gran empresa sigue abierto. ¿Es viable y oportuno emplear código abierto para crear sistemas de seguridad? ¿Es seguro? ¿Es económicamente ventajoso afrontar un proyecto *open source* de seguridad que no es "Out of the box"? ¿Un IPS basado en código abierto está a la altura de las soluciones tradicionales de mercado? ¿Las ampliaciones y adaptaciones al software deben volver a la comunidad para que todos puedan aprovecharlas sin mantener partes "secretas"? ¿Tienen algo que ver el *open source* y la responsabilidad social corporativa? Y, por supuesto, ¿funciona?

Ponentes:

Daniel Concepción Pérez es Director de Sistemas Globales de Produban. Con más de 10 años de experiencia en el mundo IT se incorporó en el año 2003 a Grupo Banesto y en el año 2006 a Produban. Actualmente es Director de Sistemas Globales de Produban, donde coordina las iniciativas para la innovación tecnológica y el soporte a los proyectos de transformación.

Iñaki Murcia García es Director Regional de Nextel, S.A. Licenciado en Informática y CISA, lleva más de 25 años vinculado al mundo de las TIC. Inició su carrera en 1985 en La Casera donde llegó a desempeñar la responsabilidad informática. En 1993 y 1995 fundó las compañías PurpleSystem y PurpleInet vinculadas al mundo telemático e Internet. En 1998 pasó a ser consultor estratégico de Seguridad para Centrisa desarrollando grandes proyectos para la gran banca en Latinoamérica. Después de su etapa como gerente de Seguridad Informática en Dinsa fue nombrado Director Regional de Nextel, S.A., puesto que desempeña desde 2004. Ha colaborado en algunos de los mayores proyectos de infraestructuras de seguridad en España.

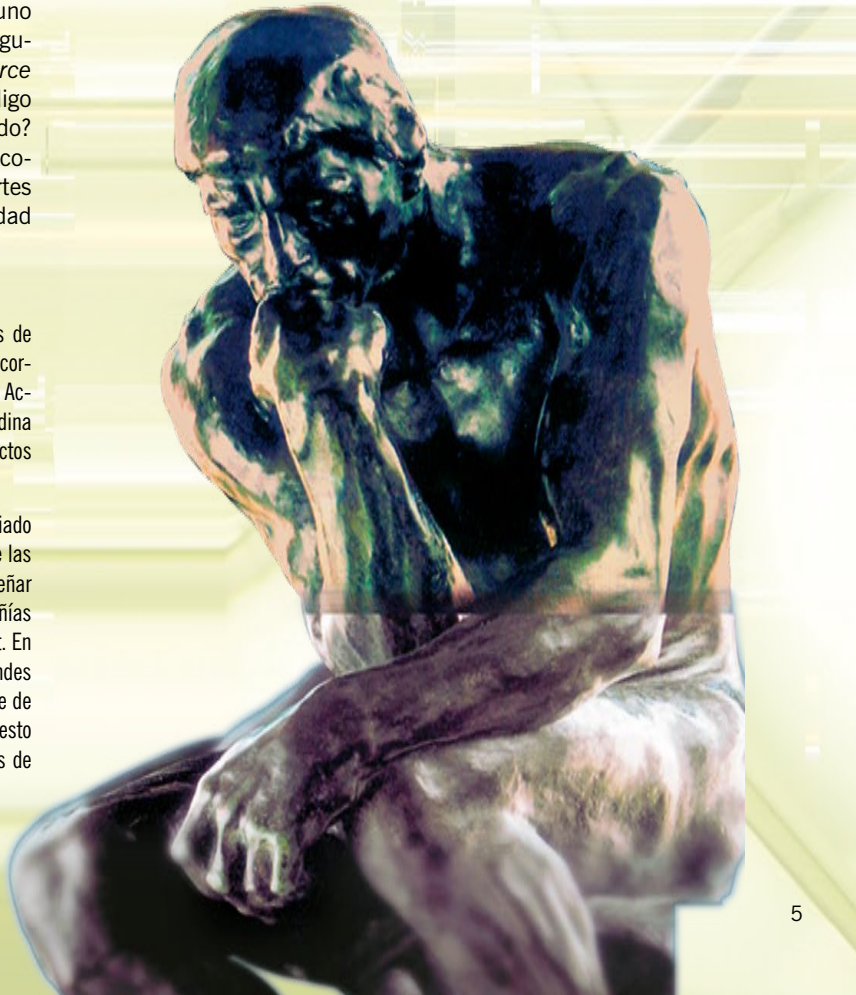
ENDESA: IMPLANTACIÓN DE SAP GRC

Sinopsis. La conferencia versará sobre la definición e implementación de un modelo de Segregación de Funciones y Gestión de Super Usuarios, soportado por la solución de Control de Accesos de SAP de la *suite* de GRC (SAP GRC Access Control), que ha permitido a Endesa mejorar los controles en los accesos a los sistemas de información, reduciendo el riesgo de fraude financiero y controlando el acceso a la información sensible de la empresa. Este enfoque hace posible controlar los accesos a los diferentes sistemas, limitando los usuarios con amplios permisos e introduciendo un nuevo modelo de gobierno para garantizar que las acciones en los sistemas, definidas como críticas sean realizadas únicamente por las personas autorizadas, en un ambiente controlado y totalmente auditable.

Ponentes:

Joaquín Álvarez Pérez es Subdirector de Seguridad de la Información del grupo Endesa. Inició su carrera profesional en el mundo de los sistemas de información, donde ha trabajado como Ingeniero de Desarrollo de Sistemas y como responsable del Centro de Información. A lo largo de los últimos años ha centrado su actividad en el área de organización de la compañía, donde ha dirigido diseños de procesos de negocio, análisis organizativos, normativa estratégica y ha desarrollado la función de seguridad de la información junto con sus procesos de gobierno. Posee una Licenciatura en Derecho, es Máster en Consultoría Estratégica de las Organizaciones y Diplomado en Seguridad Corporativa y Protección del Patrimonio.

Javier Fernández Bonache es Gerente del área de Tecnología SAP de Accenture. Ingeniero Superior de Telecomunicaciones por la Universidad Politécnica de Cataluña y está también diplomado en Ciencias Empresariales por la Universitat Oberta de Catalunya. Con más de 11 años de experiencia en Implantaciones de Soluciones SAP y el desarrollo de soluciones de seguridad de acceso a la información, en los últimos años, ha centrado su carrera en el Diseño e Implementación de SAP GRC Access Control para el control de accesos a sistemas, el control de la Segregación de Funciones, la integración con los sistemas de aprovisionamiento de usuarios, y el control de Super Usuarios.



SEGUNDO MÓDULO, 25 DE ABRIL

09:15h. Entrega de documentación.
Moderador: **Antonio Ramos García**, Presidente del Capítulo de Madrid de ISACA.

09:45h. Ponencia: **Cerrando el círculo de la seguridad: La Oficina de Calidad de Datos de Banco Popular.**
Ponentes:
Alberto Romero Orencio, Director de la Oficina de Calidad de Datos del Banco Popular.
Juan Manuel Matalobos Veiga, Director, Advisory Services FSO. Ernst & Young.

10:20h. Coloquio.

10:25h. Ponencia: **Bankinter: Lucha contra las Amenazas Avanzadas y Persistentes (APTs) mediante inteligencia en la red.**
Ponentes: **Jesús Milán Lobo**, Director de Riesgos Tecnológicos y Seguridad de la Información de Bankinter.
Daniel Solís Agea, Director General de blueliv.

11:00h. Coloquio.

11:05h. Pausa-café.

Moderador: **Miguel Bañón Puente**, Director de Epoche & Espri.

11:35h. Ponencia: **Prueba de ciberseguridad en el sector financiero: "2011 UK FSA Market Wide Exercise".**
Ponente: **Daniel Barriuso Rojo**, Director Global de Seguridad de la Información (CISO) y Riesgo Tecnológico de Credit Suisse.

12:10h. Coloquio.

12:15h. Ponencia: **Grupo BBVA y Google: disociación de la información en la nube.**
Ponente: **Santiago Moral Rubio**, Director de Riesgo IT, Fraude y Seguridad de Grupo BBVA.

12:55h. Coloquio.

13:00h. Ponencia: **Bankia: la seguridad al servicio de la inteligencia corporativa.**
Ponentes: **Javier Rodríguez Llorente**, Director de Seguridad de la Información de Bankia.
Isabel María Gómez González, Responsable de Políticas y Normativas de Seguridad de la Información de Bankia.

13:40h. Coloquio.

13:45h. Almuerzo.

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

16:00h. Ponencia: **Andalucía CERT: Gestión de incidentes de seguridad en la Junta de Andalucía.**
Ponentes:
Juan Antonio Muñoz Risueño, Responsable del Centro de Seguridad TIC de la Junta de Andalucía.
Godofredo Fernández Requena, Consultor Senior de Telefónica.

16:35h. Coloquio.

16:40h. Ponencia: **Seguridad y *cloud*: ¿Cuál es el problema?**
Ponentes:
Eloy Acosta Toscano, Subdirector de Tecnología de RTVE Medios Interactivos.
Olof Sandstrom Herrera, Director General de Operaciones y Seguridad de Arsys Internet.

17:15h. Coloquio.

17:20h. Pausa-café.

17:35h. Ponencia: **Evolución de la arquitectura de Seguridad de la Comunidad de Madrid: de la protección de sistemas a la provisión de servicios seguros.**
Ponentes:
Carlos Gamallo Chicano, Jefe de Área de Comunicaciones de la Dirección de Producción e Infraestructuras de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid.
Alfonso Franco Gómez, Gerente de Preventa de la Práctica de Seguridad TIC de Logica Iberia.

18:10h. Coloquio.

18:15h. Fin de la segunda sesión.

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

CERRANDO EL CÍRCULO DE LA SEGURIDAD: LA OFICINA DE CALIDAD DE DATOS DE BANCO POPULAR

Sinopsis. Cuando pensamos en los objetivos de seguridad de la información, con frecuencia pensamos inmediatamente en la C de confidencialidad y en la D de disponibilidad... y dejamos en un segundo término la I de integridad. Históricamente la integridad de la información ha quedado encuadrada en un vacío entre las áreas usuarias, que se consideran protegidas por el servicio que proporciona la tecnología y las áreas de tecnología, que consideran responsabilidad del usuario toda la información que procesan sus sistemas. Esto no significa que no existan medidas para controlar la integridad de la información, sino que estas medidas no se implantan según una estrategia definida con una visión global de las necesidades, sino cubriendo objetivos particulares y puntuales. La experiencia demuestra que las incidencias producidas o favorecidas por un bajo nivel de calidad de la información pueden tener sobre las organizaciones un impacto financiero, legal y reputacional igual o superior al de cualquier otro tipo de incidente de seguridad, y por ello la integridad de la información debe dejar de considerarse un objetivo menor de la seguridad, y figurar como una más de la prioridades principales de las organizaciones. Según los estándares, la integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio. Para lograr un nivel adecuado de calidad de la información es inevitable normalizar y mejorar los procesos de captación, mantenimiento y actualización de la información, así como emplear sistemas de almacenamiento y procesamiento adecuadamente controlados.

Ponentes:

Alberto Romero Orencio es Director de la Oficina de Calidad de la Información de Banco Popular. Desde su incorporación al Banco en 1974, ha asumido distintas funciones en las áreas de Valores, Auditoría Interna y Sistemas y Métodos. Antes de asumir la dirección de la Oficina de Calidad fue Director de Tecnología de Bancopopular-e y director de diversos proyectos tecnológicos en el Área Comercial.

Juan Manuel Matalobos Veiga es Director de Advisory en Ernst & Young, en el área de riesgos y auditoría tecnológica (IT Risk & Assurance) para el sector financiero. Entre otras funciones es el responsable en España de los servicios de gestión y calidad de datos. A lo largo de su carrera ha dirigido y participado en numerosos proyectos relacionados con la gestión del riesgo tecnológico, como planes directores de seguridad, revisiones de seguridad o auditorías tecnológicas.

BANKINTER: LUCHA CONTRA LAS AMENAZAS AVANZADAS Y PERSISTENTES (APTs) MEDIANTE INTELIGENCIA EN LA RED

Sinopsis. Bankinter es una referencia en la seguridad de la información, tanto en el desarrollo de nuevas tecnologías como en el avance en la lucha contra el fraude y otras amenazas en el cibermundo. Siguiendo esta premisa de la innovación, el Banco ha adquirido la tecnología inteligente de blueliv: OPTOS, para complementar los mecanismos existentes en la Entidad, en la lucha contra las Amenazas Persistentes Avanzadas (APT). Es decir, el objetivo ha sido colaborar en ser parte de los ojos y los oídos del banco en Internet, aportando inteligencia en el proceso. A lo largo de la ponencia, se irán desgranando vías para la implementación de la estrategia Bankinter de protección frente a APT's, considerando entre otros aspectos: la búsqueda y control de información a través de buscadores, redes sociales, redes p2p, foros, etc., detección de potenciales fraudes (*carding*, robo de datos, *phishing* etc.), así como movimientos de bandas criminales y, por supuesto, el *malware*.

Ponentes:

Jesús Milán Lobo es Director de Riesgos Tecnológicos y Seguridad de la Información en Bankinter. Ingeniero en Informática con especialidad en Gestión por el ICAI-ICADE, cuenta con la certificación CISM y es Lead Auditor ISO27001 - BS25999. Es miembro del Subcomité Nacional de Seguridad de las TI (CTN 71/SC27) y miembro WG1, y colaborador en la redacción de normas internacionales. Igualmente, es miembro de la Junta Directiva de ISMS Forum Spain; de la Comisión de Seguridad del Capítulo de Madrid de ISACA; y del Comité de Seguridad Informática y de la Comisión de Seguridad, Prevención y Fraude del Centro de Cooperación Interbancaria.

Daniel Solís Agea es Socio fundador y Director General de blueliv. 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 por ejemplo S21sec, de la cual fue miembro del equipo inicial. Es ISO 27001 Lead Auditor acreditado por IRCA, miembro activo de AEDEL y creador de la distribución forense AD-QUIERE.

PRUEBA DE CIBERSEGURIDAD EN EL SECTOR FINANCIERO: "2011 UK FSA MARKET WIDE EXERCISE"

Sinopsis. En noviembre de 2011, a instancias de la 'Financial Services Authority' (FSA), más de 3.500 profesionales de 87 entidades financieras participaron en un simulacro de ciberataque en Reino Unido. El objetivo del ejercicio era mejorar la coordinación entre las distintas entidades, y probar la capacidad de resistencia, respuesta y recuperación ante ciberataques. La ponencia aborda aspectos claves del ejercicio tales como: Planificación y preparación del evento; Ejecución y coordinación del simulacro de ataque, y Resultados y lecciones aprendidas.

Ponente:

Daniel Barriuso Rojo es Director Global de Seguridad de la Información (CISO) y Riesgo Tecnológico de Credit Suisse. Su responsabilidad incluye la gestión del riesgo tecnológico y la seguridad de la información a través de todas las áreas de negocio y países del grupo. Con una amplia experiencia en Seguridad y TIC, la prioridad de Barriuso está centrada en los aspectos estratégicos de la seguridad, tales como gobierno, gestión del riesgo, delito electrónico y ciberinteligencia. Desde 2002, imparte clases como profesor en el Máster de Seguridad y Auditoría de la Universidad Politécnica de Madrid. En la actualidad reside en Londres, donde recientemente ha diseñado y dirigido la primera prueba de ciberseguridad en el sector financiero para la 'Financial Services Authority' (FSA) de Reino Unido.

GRUPO BBVA Y GOOGLE: DISOCIACIÓN DE INFORMACIÓN EN LA NUBE

Sinopsis. Una historia que comienza muy apegada a la tierra, como una evolución tecnológica de los sistemas de correo, como un movimiento de externalización con claros tintes crematísticos. Una Dirección Técnica, que en su oficio de encontrar las mejores opciones para el Grupo, explora lo que puede aportar el SaaS en cuanto a herramientas colaborativas para grandes corporaciones. Y expone al resto de unidades de TI la idea de que Gmail puede ser una alternativa realista. Hasta la fecha, y según la Metodología Casandra, Gmail es el sistema de información que mejor valoración técnica ha tenido desde el punto de vista del riesgo de confidencialidad, integridad, disponibilidad y auditabilidad. Por sus patentes, su seguridad estadística y su ausencia de incidentes conocidos. Finalmente la decisión no ha sido económica, ni técnica ni estratégica. La transformación cultural de los empleados es uno de los cambios imprescindibles que deben dar todas las entidades que aspiren a ser parte de la sociedad del conocimiento.

Ponente:

Santiago Moral Rubio es desde 2011 Director de Riesgo IT, Fraude y Seguridad 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 Director de Seguridad de la Información del Grupo BBVA.

BANKIA: LA SEGURIDAD AL SERVICIO DE LA INTELIGENCIA CORPORATIVA

Sinopsis. En la conferencia se expondrá la experiencia de Bankia en la implantación de ATHINA, su herramienta de Inteligencia Corporativa. De dónde surge la necesidad, cuáles son los objetivos que se establecieron para el proyecto, la selección y el desarrollo de la herramienta, fuentes de la que se nutre, productos obtenidos y destinatarios de los mismos, serán algunos de los aspectos que se tratarán en el transcurso de la misma, para terminar con un esbozo del plan de desarrollo de la función de Inteligencia Corporativa en el Grupo Bankia.

Ponentes:

Javier Rodríguez Llorente es actualmente Director del Departamento de Seguridad Informática del Grupo Bankia. Ingeniero de Telecomunicación por la UPM, anteriormente ha trabajado como Jefe de Sistemas en Caja de Ávila durante 16 años, llevando la gestión de todas las plataformas tecnológicas de la Entidad, la red de comunicaciones y todo lo referente a la seguridad, tanto de servidores como perimetral, incluida la gestión de usuarios. Ha sido profesor de la Facultad de Ciencias y Artes de La Universidad Católica, impartiendo y elaborando programas de asignaturas de Redes de Computadores, así como ponente de diversos máster y seminarios. Sus inicios profesionales están ligados también al sector financiero en el Departamento de Informática de Citibank, desempeñando funciones en el desarrollo de aplicaciones de medios de pago.

Isabel Mª Gómez González es actualmente Responsable de Políticas y Normativas de Seguridad de la Información del grupo Bankia. Su carrera profesional ha transcurrido siempre en el mundo de la seguridad, habiendo desempeñado cargos de relevancia en este campo en consultoras como KPMG o Indra, y para grandes organizaciones, como el Grupo Santander, AENA, etc. Es una profesional con más de 15 años de experiencia en el desarrollo de estrategias de gobierno de la seguridad, inteligencia, gestión de riesgos, y optimización y obtención de beneficios de los procesos de seguridad, así como en la adaptación de las organizaciones a los nuevos retos.

ANDALUCÍACERT: GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA JUNTA DE ANDALUCÍA

Sinopsis. En esta ponencia se describirá el panorama actual de gestión de incidentes de seguridad en la Junta de Andalucía y cómo el Centro de Seguridad TIC de Andalucía, AndalucíaCERT, contribuye a la consecución de los objetivos definidos por esta administración pública respecto a la Gestión de la Seguridad de la Información. Asimismo, se presentará la arquitectura de sistemas, servicios y procesos sobre los que se apoyan los servicios ofrecidos por AndalucíaCERT, así como los modelos de interrelación con otros centros similares. Se concluirá con la presentación de algunos indicadores que arroja el servicio después de varios años de prestación y sus principales vías de actuación y evolución.

Ponentes:

Juan Antonio Muñoz Risueño es Ingeniero de Telecomunicación por la Universidad de Sevilla. Durante los últimos diez años ha desarrollado su labor profesional en el ámbito de las redes de comunicaciones y la gestión de la seguridad de la información. Actualmente es el Responsable del Centro de Seguridad TIC de Andalucía (AndalucíaCERT) en la Sociedad Andaluza para el Desarrollo de la Sociedad de la Información, empresa dependiente de la Consejería de Economía, Innovación y Ciencia de la Junta de Andalucía.

Godofredo Fernández Requena es Ingeniero de Telecomunicación y Licenciado en Investigación y Técnicas de Mercado por la Universidad de Sevilla. Especializado en Ingeniería Telemática ha desarrollado su labor profesional como Jefe de Proyecto en las áreas de Redes Privadas y Seguridad de diferentes empresas del Grupo Telefónica, participando desde el año 1997 en importantes proyectos desarrollados tanto en el ámbito público como en el privado. Actualmente es Consultor Senior en la Dirección de Infraestructuras de Telefónica Grandes Clientes y profesor asociado en el Departamento de Ingeniería Telemática de la Escuela Superior de Ingeniería de la Universidad de Sevilla.

SEGURIDAD Y *CLOUD*: ¿CUÁL ES EL PROBLEMA?

Sinopsis. RTVE Medios Interactivos (rtve.es) tiene hospedadas varias de sus plataformas (por ejemplo Águila Roja, mundo virtual de Cuéntame, o la retransmisión en directo de los resultados de las elecciones) en *cloud* desde hace más de un año. Esta solución le ha facilitado a RTVE Medios Interactivos el poder abstraerse de las tareas relacionadas con la gestión de la infraestructura y de la seguridad de sus plataformas, delegando una parte significativa de esta gestión en el equipo de Arsys. Así, la solución desplegada incorpora las funcionalidades y servicios de protección necesarios para dotar a los distintos entornos de producción, de unos niveles de seguridad (en sus tres vertientes de confidencialidad, integridad y disponibilidad) adecuados a los exigentes requerimientos que RTVE Medios Interactivos establece para sus sistemas. Es importante tener en cuenta que se trata de entornos muy dinámicos, en los que las necesidades de recursos varían en cuestión de minutos, requiriendo de una interacción constante entre los equipos técnicos. Y evidentemente la seguridad tiene que estar alineada con la demanda de recursos. Un caso muy significativo fue la retransmisión en directo de los resultados de las últimas elecciones generales, en la que (además de las necesidades evidentes de seguridad) se comenzó con 3 frontales y se llegó a tener hasta 10 frontales en producción para absorber los picos de carga en un periodo de apenas dos horas, adecuando en caliente las necesidades, tanto de recursos como de seguridad.

Ponentes:

Eloy Acosta Toscano es Subdirector de Tecnología en RTVE Medios Interactivos desde enero de 2010. Ha estado involucrado desde 1999 en la gestión y desarrollo de TI en organizaciones de Medios de comunicación y Telcos. Su desembarco profesional fue en IPSistemas como Ingeniero de sistemas para a continuación ser Responsable de Sistemas de Producción en PRISACOM (medios digitales: elpais.com, as.com, los40.com, etc). Igualmente, también ha desempeñado labores profesionales de TI en DBA y FON Wireless Ltd., y ha sido Responsable de sistemas en Lainformación.com y Subdirector de sistemas en RTVE.es

Sven Olof Sandstrom Herrera es Director General de Operaciones y Seguridad 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 ISO27001.

EVOLUCIÓN DE LA ARQUITECTURA DE SEGURIDAD DE LA COMUNIDAD DE MADRID: DE LA PROTECCIÓN DE SISTEMAS A LA PROVISIÓN DE SERVICIOS SEGUROS

Sinopsis. La ponencia presentará la evolución de la arquitectura de Seguridad de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid desde sus comienzos, en los que se instalaron los primeros cortafuegos para proteger determinados sistemas, las distintas modificaciones realizadas en la arquitectura para aumentar la capacidad de la misma y dotarla de mayores funcionalidades, a la situación actual en la que, distintos factores, (fomento de administración electrónica, reducción de costes, virtualización, centralización y consolidación de competencias) han motivado la realización de cambios en el modelo de seguridad, adaptando la arquitectura hacia un nuevo modelo orientado a la provisión de servicios seguros.

Ponentes:

Carlos Gamallo Chicano es Jefe de Área de Comunicaciones de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid. Ingeniero Industrial por la UC3M y Máster en Redes y Sistemas por el ETSIT, comenzó su carrera en Lucent Technologies; posteriormente trabajó en el departamento de operaciones en Nortel Networks durante tres años. En 2003 cofundó una empresa de integración de sistemas y en 2008 se incorporó a la Agencia de Informática y Comunicaciones de la Comunidad de Madrid como Consultor de Sistemas de Información. Desde abril de 2009 ocupa en ICM el puesto de Jefe de Área de Comunicaciones.

Alfonso Franco Gómez es Gerente de Preventa de la Práctica de Seguridad TIC de Logica Iberia. Franco Gómez estudió Ingeniería Informática en la Universidad Politécnica de Madrid, cuenta con quince años de experiencia en el campo de la Seguridad TIC y, desde el año 2001, con un conocimiento exhaustivo de la oferta tecnológica del sector, lidera la labor de preventa de la Práctica de Seguridad TIC de Logica Iberia, realizando igualmente dirección de proyectos estratégicos y participando en la selección de las apuestas tecnológicas de la compañía.

TERCER MÓDULO, 26 DE ABRIL

09:15h. Entrega de documentación.
Moderador: **José Carrillo Verdún**, Facultad de Informática de la Universidad Politécnica de Madrid.

09:30h. Ponencia:
ISBAN: DRM en el Servicio de Publicaciones con Arkano.
Ponentes:
Fernando Zamácola Martínez, Local Information Security Officer,
Riesgo Tecnológico y Operacional. ISBAN (Santander).
Juan Jesús León Cobos, Director de Productos de GMV.

10:05h. Coloquio.

10:10h. Ponencia:
Desarrollo seguro de sistemas y servicios en Ferrovial.
Ponentes:
Juan Cobo Páez, Jefe del Departamento de Seguridad de la Información de Ferrovial.
Jaume Ayerbe Font, Director de Ventas de HP Enterprise Security Products. HP.

10:45h. Coloquio.

10:50h. Pausa-café.
Moderador: **Carlos Manuel Fernández Sánchez**, Jefe de Certificaciones TIC. Dirección de Desarrollo de AENOR.

11:20h. Ponencia:
Simulador Avanzado para la Ciberdefensa.
Ponentes:
Juan Manuel Estévez Tapiador, Profesor Visitante. Universidad Carlos III de Madrid.
Jorge López Hernández-Ardieta, Ingeniero Senior. Unidad de Ciberseguridad de Indra.

11:55h. Coloquio.

12:00h. Ponencia:
Diseño y despliegue del MSSP global de Telefónica: globalización, agilidad y cercanía al cliente para la Seguridad del futuro.
Ponentes:
José Luis Gilpérez López, Director Security Product Development & Innovation. Telefónica Digital.
Jesús Romero Bartolomé, Director de Riesgos Tecnológicos de PwC.

12:35h. Coloquio.
Moderador: **José de la Peña Muñoz**, Director de la revista SIC.

12:40h. **DEBATE:**
¿Aporta la titulación de Director de Seguridad Privada los conocimientos necesarios para gestionar la ciberseguridad de Infraestructuras Críticas?
Participantes:
Miguel Ángel Abad Arranz, Jefe del Servicio de Seguridad Lógica del Centro Nacional de Protección de Infraestructuras Críticas - CNPIC.
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 y Director del CESICAT.
Francisco Javier García Carmona, Director de Seguridad de la Información y de las Comunicaciones de Iberdrola.
Antonio Ramos García, Presidente del Capítulo de Madrid de ISACA.
Gianluca D'Antonio, Presidente de ISMS Forum Spain.
Carlos Bachmaier Johanning, Cumplimiento Normativo de Seguridad de la Información de Sistemas Técnicos de Loterías (STL), Grupo SELAE.

14:00h. Fin del debate.

14:05h. Clausura y fin de la tercera sesión.

14:10h. Almuerzo.

ISBAN: DRM EN EL SERVICIO DE PUBLICACIONES CON ARKANO

Sinopsis. ¿Es posible hacer compatibles, por un lado, la necesidad de acceso a la documentación de productos de los miles de desarrolladores que trabajan para ISBAN en todo el mundo, y por otro los estrictos requisitos de control de acceso a esta documentación tan sensible? La implantación de Arkano en el servicio de publicaciones de ISBAN consigue compatibilizar la seguridad con la usabilidad, de manera que cada persona tiene acceso fácil e inmediato a la información que necesita para su trabajo a través de la Intranet, mientras que simultáneamente este acceso queda auditado y además se previene que dicha información pueda ser extraída (copiada o impresa). Todo ello utilizando cifrado de extremo a extremo, basado en la identidad del usuario, sobre un universo preexistente de decenas de miles de documentos.

Ponentes:

Fernando Zamácola Martínez es Responsable de la Seguridad de la Información en ISBAN. Estudió Ingeniería Técnica de Telecomunicaciones en la Universidad de Alcalá de Henares, y desarrolló su carrera profesional como Técnico de Sistemas MVS en ENTEL y como Consultor Senior en Accenture. En el año 2000 pasa a formar parte del Grupo Sabadell como Director de Explotación en Activo Bank y tres años después se independiza, fundando Zagull Gestión Informática. Finalmente, en 2010 pasa a formar parte del Grupo Santander.

Juan Jesús León Cobos es Director de Productos y Nuevos Desarrollos en GMV. Ingeniero Aeronáutico por la UPM, PDD por el IESE y CISM, inició su carrera profesional en GMV en 1988 en el sector espacial, y continuó posteriormente en el grupo Indra, gestionando proyectos en el sector de Defensa en España y EE.UU. En el año 1997 se incorporó al grupo El Corte Inglés, donde llegó a ser Jefe del Área de Desarrollo para sus Centros Comerciales. En el año 2000 se incorporó al grupo BBVA donde contribuyó como Director de Desarrollo a la puesta en producción del banco Uno-e. En Junio de 2001 regresó a GMV.

DESARROLLO SEGURO DE SISTEMAS Y SERVICIOS EN FERROVIAL

Sinopsis. En Ferrovial la gestión de la seguridad en el Ciclo de Desarrollo de Productos y Servicios contempla la inclusión de medidas de control con las que mitigar los riesgos asociados a la definición, diseño, desarrollo y/o despliegue de nuevos productos/servicios TI dentro de la organización. Teniendo en cuenta las necesidades y requisitos en materia de Seguridad de la Información que pueda requerir un determinado nuevo producto/servicio, y mediante la revisión de sus niveles de implantación durante el proceso del ciclo de vida, se puede conseguir una optimización notable de la Gestión del Riesgo y del esfuerzo económico necesario a la hora de subsanar ulteriores carencias de seguridad. Dentro de este proceso continuo de aseguramiento y calidad, Ferrovial ha escogido la solución de HP Fortify como servicio para apoyar sus validaciones y revisiones de adecuación a los requisitos planteados.

Ponentes:

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.

Jaume Ayerbe Font es Ingeniero Electrónico, MBA por el IESE Universidad de Navarra y está certificado CRISC por ISACA entre otras acreditaciones profesionales. Actualmente lidera el equipo de HP Enterprise Security Products en la región de Iberia. En los más de 8 años que lleva trabajando en HP, ha desarrollado distintas responsabilidades dentro de la división de soluciones de gestión de IT para grandes organizaciones. Anteriormente desarrolló su carrera con cargos de responsabilidad en NetIQ y Microsoft.

SIMULADOR AVANZADO PARA LA CIBERDEFENSA

Sinopsis. En un contexto en el que los ciberataques crecen en número y sofisticación, urge no solo que los sistemas de información incorporen los mecanismos de seguridad adecuados, sino también que los operadores de dichos sistemas sepan hacer frente y reaccionar de manera eficaz y rápida ante los incidentes de seguridad que puedan producirse. Para ello, es necesario una formación especializada y un entrenamiento continuo que dote a dichos operadores de las habilidades y conocimientos que se requieren en materia de ciberdefensa. Los actuales entornos y herramientas de entrenamiento en ciberdefensa tienen ciertas carencias que impiden una adecuada formación continua, dinámica, y que incorpore de forma flexible nuevos escenarios y técnicas conforme avanza el estado del arte en la materia. El Simulador Avanzado para la Ciberdefensa Organizada (SACO) es un proyecto de innovación industrial liderado por Indra y financiado por el Ministerio de Economía y Competitividad que busca desarrollar una solución avanzada para el entrenamiento en técnicas de ataque y defensa en el ciberespacio. El simulador permitirá la construcción de ejercicios de ciberdefensa de forma sencilla, flexible y contemplando una gran variedad de escenarios. Asimismo, se adaptará al nivel del alumno, dotándole de interactividad con un entorno en el cual tanto los ataques como las medidas defensivas se desplegarán sobre sistemas reales. De esta forma, el alumno podrá observar el comportamiento e impacto de los ataques y contramedidas desplegados, estudiar su eficacia en tiempo real, y llevar a cabo análisis forenses que complementen su formación. La dinámica de los ejercicios garantizará el aprendizaje no solo observacional sino también por descubrimiento al ser el alumno un agente activo consciente de las consecuencias de sus acciones, con capacidad para la toma de decisiones propias y pudiendo analizar diferentes alternativas durante el transcurso del ejercicio.

Ponentes:

Juan Manuel Estévez Tapiador es Ingeniero en Informática (2000) y Doctor en Informática (2004) por la Universidad de Granada. En la actualidad es Profesor Visitante en el Laboratorio de Seguridad de la Universidad Carlos III de Madrid. Previamente trabajó como investigador en la Universidad de York (UK) y en el IBM Thomas J. Watson Research Center (NY, USA). Su actividad académica se centra en diversos aspectos de la seguridad de la información y la criptografía aplicada. Actualmente sus principales áreas de trabajo comprenden la ciberdefensa y el modelado de ataques; la seguridad y privacidad en redes de sensores y dispositivos de identificación por radiofrecuencia (RFID); los sistemas de prevención de fugas de datos (DLP); y la seguridad en teléfonos inteligentes.

Jorge López Hernández-Ardieta es Ingeniero Informático (2003), Diplomado de Estudios Avanzados (2005) por la Universidad Autónoma de Madrid, y Doctor en Ciencia y Tecnología Informática por la Universidad Carlos III de Madrid (2011) (UC3M). Actualmente es Ingeniero Senior en la Unidad de Ciberseguridad de Indra Sistemas, y Profesor Asociado y miembro del Laboratorio de Seguridad de la UC3M. Participa en diversas iniciativas de estandarización y desarrollo normativo en el campo de la seguridad, siendo miembro de la Agencia de Defensa Europea (EDA-IAP4), ISO/IEC JTC 1/SC 27, CEN/TC 224, IEEE, IETF y AENOR. Sus áreas de investigación principales son la ciberdefensa orientada a la protección de redes y sistemas críticos, las metodologías de evaluación de seguridad (Common Criteria, FIPS), el desarrollo de software seguro, el modelado y categorización de ataques, y el no repudio.

DISEÑO Y DESPLIEGUE DEL MSSP GLOBAL DE TELEFÓNICA: GLOBALIZACIÓN, AGILIDAD Y CERCANÍA AL CLIENTE PARA LA SEGURIDAD DEL FUTURO

Sinopsis. Dentro de su posición de liderazgo en el mercado digital, la oferta global de seguridad en general y los servicios de seguridad gestionada en particular, constituyen una de las líneas estratégicas de Telefónica Digital. En la ponencia se describirán la estrategia y planteamientos seguidos por Telefónica Digital con apoyo de PwC, para la industrialización y despliegue de los SOCs (Security Operation Centers) que le constituyen como MSSP (Managed Security Service

Provider) Global, la estandarización de los servicios prestados, el aumento de su flexibilidad, su acercamiento al cliente y la agilización del *time-to-market* asociado a su comercialización en todos los países en los que Telefónica está presente. Además, en la ponencia también se describirán las iniciativas de innovación que Telefónica Digital está impulsando en materia de seguridad, tanto orientadas a empresas como a particulares.

Ponentes:

José Luis Gilpérez López es Director de Security Product Development & Innovation de Telefónica Digital. Ingeniero Industrial por la UPM, certificado CISA por ISACA y OCSA/OCSE/OCSM por AlienVault, trabaja en Telefónica desde 1988, compañía en la que ha ocupado diferentes responsabilidades relacionadas con la seguridad de la red y de sus servicios. Desde 2010 es el responsable del desarrollo de las plataformas y servicios globales de seguridad de Telefónica, y en particular, de la puesta en marcha de la estrategia global de los SOCs y de los diferentes servicios gestionados que presta local y globalmente. Con anterioridad, fue el responsable del desarrollo e implantación de los procesos de gestión de la seguridad en las áreas de operación de la compañía, y del plan de seguridad operativa para toda la red de Telefónica de España y sus áreas de servicio.

Jesús Romero Bartolomé es Director de Riesgos Tecnológicos en PwC. Ingeniero Superior de Telecomunicación y MBA, ha desempeñado con anterioridad funciones de responsabilidad en Indra, Bull y el Grupo Altran. A lo largo de esta trayectoria ha participado en el desarrollo de algunas de las iniciativas de Seguridad más emblemáticas del mercado español. Es Certified Information Security Manager (CISM) y miembro del Consejo Profesional Asesor del área TIC de la Universidad Europea de Madrid. A lo largo de su carrera profesional ha sido miembro del Subcomité Nacional de Seguridad de las TI (CTN 71/SC27) de AENOR y Vicepresidente de la Plataforma española de Seguridad y Confianza, coordinada por AETIC (ahora AMETIC).

DEBATE

¿APORTA LA TITULACIÓN DE DIRECTOR DE SEGURIDAD PRIVADA LOS CONOCIMIENTOS NECESARIOS PARA GESTIONAR LA CIBERSEGURIDAD DE INFRAESTRUCTURAS CRÍTICAS?

Proposición. La legislación vigente sobre protección de infraestructuras críticas (PIC) y el protagonismo creciente de la ciberseguridad han avivado la polémica de la pertinencia o no de disponer de una función de seguridad integrada o unificada en las organizaciones, cuyo gobierno requiere, en buena lid, profesionales y equipos con conocimientos en muchos frentes de la protección y el control, especialmente en seguridad de la información y seguridad TIC. Se tratar de debatir acerca de si el título de Director de Seguridad Privada, que reconoce el Ministerio del Interior, dota hoy a quien lo obtiene de conocimientos adecuados para la PIC y, por extensión, para gestionar los procesos de seguridad de cualquier organización.

Participantes:

Miguel Ángel Abad Arranz es Jefe de la Sección de Seguridad Lógica del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Oficial de la Guardia Civil (Escala Facultativa Superior) e Ingeniero Informático por la Universidad de Comillas ICAI-ICADE, posee el título de Máster de Investigación en Inteligencia Artificial por la Universidad Politécnica de Madrid. Hasta su ingreso en la Guardia Civil, trabajó desde el año 1999 en distintas compañías del sector tecnológico, desempeñando distintas funciones técnicas en proyectos dirigidos a operadores de telefonía móvil principalmente. Ha desarrollado sus funciones en los últimos años en el campo de la seguridad de infraestructuras e instalaciones de carácter estratégico (ámbito lógico). Colabora habitualmente en la impartición de diferentes cursos y másteres relacionados con defensa y seguridad organizados por la UNED, e igualmente participa frecuentemente en conferencias y jornadas, tanto nacionales como internacionales, en el marco de la seguridad y protección de las infraestructuras críticas.

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 de Privacidad de Datos. 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.

Francisco Javier García Carmona es Director de Seguridad de la Información y las Comunicaciones de Iberdrola. Maestro Industrial e Ingeniero de Telecomunicaciones, dispone de un Máster en Administración y Dirección de empresas, ha realizado el Curso Superior de Dirección de Seguridad de ICAI y es Director de Seguridad reconocido por el Ministerio del Interior. Tiene una larga experiencia profesional en empresas y por cuenta propia en áreas como automatismos, investigación aplicada, telecomunicaciones, desarrollo de software de protección y gestión de riesgos de seguridad de la información. García Carmona es miembro de Aenor en el Subcomité 27, profesor en el Máster de Asimelec-UPM y ponente en jornadas nacionales e internacionales de seguridad.

Antonio Ramos García es Presidente del Capítulo de Madrid de ISACA. Ramos compatibiliza este reto profesional con la codirección de la firma n+1 Intelligence & Research, y con las responsabilidades como Jefe de Proyecto de la Agrupación Empresarial Innovadora para la Seguridad de las Redes y los Sistemas de Información, así como las de Líder del Grupo de Trabajo 2 del capítulo español de la Cloud Security Alliance.

Gianluca D'Antonio tiene como misión principal desde 2005 promover, desarrollar e impulsar la Política de Seguridad de la Información del Grupo FCC en su calidad de Director de Seguridad de la Información y Gestión del Riesgo de dicho Grupo. Es Cofundador y Presidente de la Asociación Española para el Fomento de la Seguridad de la información ISMS Forum Spain, Miembro del Grupo Permanente de Expertos PSG de la Agencia Europea de Seguridad de las Redes y de la Información ENISA (European Network and Information Security Agency). Licenciado en Derecho, D'Antonio, desde el comienzo de su vida profesional, ha trabajado en proyectos de seguridad de la información. Posee las certificaciones CISM, CISA, CGEIT, L.A. ISO27001 y CCSK.

Carlos Bachmaier Johanning es responsable de Cumplimiento Normativo/ Seguridad de la Información en STL/Grupo Loterías y Apuestas del Estado. Ingeniero Aeronáutico por la UPM, es Profesor Titular de Universidad (excedente) y Diplomado en el Programa de Dirección en Responsabilidad Corporativa por el Instituto de Empresa (primera convocatoria). Su actividad profesional actual se desarrolla en STL y LAE (Grupo Loterías y Apuestas del Estado) en diversas áreas relacionadas con la seguridad, entre ellas como "Data Privacy Officer". Fue socio fundador de GMV y SGI Soluciones Globales Internet. Bachmaier es Auditor Jefe SGSI, miembro de ISACA –mantiene activas su certificaciones CGEIT, CRISC, CISA y CISM–, representante de LAE en el SC27 (Seguridad de la Información) y SC7/GT25 (Gobierno TIC) de AENOR (ISO) y en el Comité de Seguridad y gestión de Riesgos de la Asociación Mundial de Loterías y en el Grupo de Trabajo de Seguridad y Gestión de Riesgos de la Asociación Europea de Loterías, en los que ocupa el cargo de Vicepresidente.

Premios SIC 2012

En coincidencia con la XXIII edición de Securmática, tendrá lugar el acto de entrega de los IX 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 de la octava edición de los Premios SIC

LA HORA DEL REENCUENTRO Y LOS RECONOCIMIENTOS

Cena de la Seguridad

AFORO LIMITADO

SECURMATICA 2012
XXIII Congreso español de Seguridad de la Información
24.25.26 abril

Fechas y lugar de celebración

SECURMÁTICA 2012 tendrá lugar los días 24, 25 y 26 de abril de 2012 en el hotel NOVOTEL. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2012 recibirán las carpetas de congresistas 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 IX Premios SIC (25 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 26 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: enviando 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 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% de gastos administrativos.

Boletín de inscripción

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 24 ☐ Módulo 2 Día 25 ☐ Módulo 3 Día 26 ☐ Deseo inscribirme a SECURMÁTICA 2012
Firma:

Forma de pago: ☐ Talón ☐ Transferencia

Los datos personales que se solicitan, cuya finalidad es la formalización y seguimiento de su 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
Revista seguridad en informática y comunicaciones

EDICIONES CODA / REVISTA SIC
Goya, 39. 28001 Madrid (España)
Tel.: +34 91 575 83 24 / 25 Fax: +34 91 577 70 47
Correo-e: info@securmatica.com / info@codasic.com
Sitio: **www.securmatica.com**