SECURMATICA 2013

XXIV Congreso español de Seguridad de la Información

23.24.25 | abril

Ciberseguridad: y ahora, ¿de qué va esto?

estrategias
sectorización
compartición

www.securmatica.com

Organiza:

Revista SIC

PROGRAMA

Tendrá lugar los días 23, 24 y 25 de abril en su tradicional sede del Campo de las Naciones de Madrid

Securmática 2013: Ciberseguridad: y ahora, ¿de qué va esto?

El Congreso de Seguridad de la Información, en su 24 edición, pretende aportar luz sobre dos puntos esenciales. El primero tiene por objetivo atisbar cómo se están organizando en España los frentes público y privado de la gestión de la seguridad en el ciberespacio: lucha contra la criminalidad, freno al ciberespionaje industrial y la sustracción de otras informaciones de valor, configuración de los Planes Estratégicos Sectoriales para Infraestructuras Críticas, desarrollo de las capacidades de la ciberdefensa militar y estado del arte del difícil equilibrio entre la privacidad y la seguridad en la posible nueva legislación de la UE.

El segundo punto, por su parte, se sustancia en la presentación de iniciativas y proyectos cuya finalidad es la lucha contra el fraude, la seguridad de la información y la continuidad de actividades y negocio, ya sea por imperativo legal, ya por responsabilidad social o cumplimiento de requisitos/recomendaciones sectoriales admitidas por los mercados. El objeto de este segundo apartado es ofrecer una idea de lo que en realidad se está haciendo.

Junto a lo dicho, Securmática 2013 acercará a los congresistas algunos proyectos de innovación en seguridad tecnológica emprendidos por el sector privado, será cauce para la presentación de acciones orientadas a la mejora de la confianza y la ciberseguridad que pudieran derivarse de la Agenda Digital, y será el escenario de dos reveladoras conferencias, tituladas, respectivamente, "Ataques, más allá de la imaginación de los CISOs" y "¿Se puede restaurar la confianza en la certificación digital?". Ambas serán impartidas por dos polémicos conferenciantes, que aúnan profundos conocimientos y crudeza en sus exposiciones.

Organiza

Revista SIC

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.

Copatrocinadores

arsys es cloud · bluelive · Ernst & Young Quality In Everything We Do · gmv Innovating Solutions · hp · IBM · indra · Nextel S.A. Ingeniería y Consultoría · pwc · Telefónica

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

PRIMER MÓDULO, 23 DE ABRIL

08:45h. Entrega de Documentación.

09:15h. Inauguración oficial.
Moderador: **José de la Peña Muñoz**, Director de Revista SIC.

10:00h. Conferencia de Apertura: **Estrategia Nacional de Seguridad y ciberseguridad.**
Ponente: **Joaquín Castellón Moreno**, Director Operativo del Departamento de Seguridad Nacional - Gabinete de la Presidencia del Gobierno.

10:30h. Coloquio.

10:40h. Ponencia: **Guerra al ciberespionaje industrial: hacia un modelo de colaboración Institucional entre el CCN-CERT y las empresas privadas estratégicas.**
Ponente: **Javier Candau Romero**, Jefe del Área de Ciberseguridad del Centro Criptológico Nacional.

11:10h. Coloquio.

11.20h. Pausa-café.
Moderador: **Arturo Ribagorda**, Catedrático de la Universidad Carlos III de Madrid.

12:00h. Ponencia: **Agenda Digital para España: programas para la mejora de la confianza y la ciberseguridad.**
Ponente: **Antonio Alcolea Muñoz**, Vocal Asesor en la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Ministerio de Industria, Energía y Turismo.

12:30h. Coloquio.

12:40h. Ponencia: **La innovación colaborativa en la era del conocimiento.**
Ponente: **Santiago Moral Rubio**, Director de Riesgo IT, Fraude y Seguridad. Grupo BBVA.

13:10h. Coloquio.

13:20h. Ponencia: **CNPIC: Planes Estratégicos Sectoriales (PES).**
Ponente: **José Ignacio Carabias Corpa**, Jefe del Servicio de Seguridad Física del CNPIC, Centro Nacional para la Protección de las Infraestructuras Críticas. Secretaría de Estado de Seguridad. Ministerio del Interior.

13:50h. Coloquio.

14:00h. Almuerzo.
Moderador: **Javier Areitio Bertolín**, Catedrático de la Universidad de Deusto.

16:15h. Ponencia: **EiTB (Radio Televisión Pública Vasca): "¿Y si nos ponen una bomba?"**
Ponentes:
Iñaki Regidor Mendiolea, Director de Vanguardia de EiTB.
Ricardo Acebedo Lejardi, Responsable de Marketing de Nextel, S.A.

16:45h. Coloquio.

16:55h. Ponencia: **Administración del Principado de Asturias: modernizando el Servicio de Seguridad TIC dentro del marco establecido por el Esquema Nacional de Seguridad.**
Ponentes:
Javier Rojo Fernández, Jefe del Servicio de Seguridad de la DGTIC. Consejería de Economía y Empleo. Principado de Asturias.
Francisco Javier Diéguez Barriocanal, Gerente Zona Norte. Unidad de Ciberseguridad. Indra.

17:25h. Coloquio.

17:35h. Fin de la primera sesión.

Estrategia Nacional de Seguridad y ciberseguridad

Sinopsis: Mediante la publicación en el BOE (23 de julio de 2012) del Real Decreto 1119/2012, de 20 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, se reestructuró la Presidencia del Gobierno. Una de estas modificaciones comportó la creación del Departamento de Seguridad Nacional (DSN), que es el órgano permanente de asesoramiento y apoyo técnico en materia de Seguridad Nacional a la Presidencia del Gobierno. Su Director Operativo tiene el nivel orgánico de Subdirector General.
Entre las siete funciones atribuidas al DSN pueden mencionarse dos de especial significancia en el contexto de la ponencia: la primera, contribuir a la elaboración, implantación y revisión de las estrategias, así como la coordinación y el seguimiento de las directivas y la integración de los planes que en materia de seguridad nacional se desarrollen; y la segunda, contribuir a la elaboración de propuestas normativas, estudios e informes sobre Seguridad Nacional y la divulgación de la información que resulte de interés en esa materia, sin perjuicio de las funciones que correspondan a otros órganos.

Ponente:
Joaquín Castellón Moreno. Capitán de Fragata. Desde el pasado 1 de febrero de 2013 es el Director Operativo del Departamento de Seguridad Nacional de la Presidencia del Gobierno. Diplomado en Altos Estudios Internacionales por la Sociedad de Estudios Internacionales de Madrid (SEI), tiene el Diploma de Estudios Universitarios Avanzados en Derecho Internacional Público, y ha realizado el III Curso de Estado Mayor de las Fuerzas Armadas. Durante los empleos de Alférez de Navío (1988-1992) y Teniente de Navío (1992-2000) desempeñó numerosos destinos en buques, entre los que merece destacar la fragata "Baleares" y el portaviones "Príncipe de Asturias". Posteriormente fue destinado al Centro de Adiestramiento y Evaluación Operativa para el Combate de la Flota (CEVACO). Castellón Moreno ha estado destinado en los siguientes empleos: Estado Mayor de la Armada (entre los años 2001 y 2003); Célula Permanente de la Fuerza Marítima Europea con sede en Toulon (Francia) (entre los años 2003 y 2005); Estado Mayor de la Armada (2005-2006); Instituto Español de Estudios Estratégicos (2007-2011); Segundo Jefe de la División de Planes de la "Operación Atalanta" en el Operational Headquarter de Northwood (Reino Unido) (2009 -2010); Dirección General de Política de Defensa (2011-2012); en agosto de 2012 fue nombrado Jefe de la Oficina de Asuntos Estratégicos del Departamento de Seguridad Nacional de la Presidencia del Gobierno.

Guerra al ciberespionaje industrial: hacia un modelo de colaboración institucional entre el CCN-CERT y las empresas privadas estratégicas

Sinopsis: Desde el año 2008 se ha ido poniendo de manifiesto que los objetivos de los atacantes se están moviendo cada vez más hacia el robo de información sensible de grandes corporaciones y organismos gubernamentales. De ahí el avance del ciberespionaje, cuyo origen hay que buscarlo tanto en las empresas como en los propios Estados, y cuya naturaleza puede ser política o económica, pero siempre con un mismo motivo: obtener una ventaja sobre otras personas, instituciones o países. Ante esta situación es necesario articular un modelo dinámico de intercambio seguro y ágil de información técnica que permita, tanto a las Administraciones Públicas como a las empresas que manejan propiedad intelectual nacional, una defensa más activa basada en el mejor conocimiento posible de la amenaza. Esta situación es nueva porque el reconocimiento de un ataque por parte de una empresa u organismo público ya será un paso importante para poder articular este nuevo modelo de relación. Por ello este proceso necesita un punto neutro de confianza que proteja de manera adecuada la información proporcionada por las empresas y Administraciones, y que convenientemente 'sanitizada' pueda ser compartida por otras empresas del sector. Este modelo de colaboración pasa, además, por el despliegue de las herramientas necesarias que permitan la mayor agilidad posible en el intercambio de patrones de ataque y el apoyo necesario en la respuesta al mismo.

Ponente:
Javier Candau Romero es el Jefe del Área de Ciberseguridad 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 (CCN-CERT. www.ccn-cert.cni.es).

Agenda Digital para España: programas para la mejora de la confianza y la ciberseguridad

Sinopsis: Uno de los objetivos de la Agenda Digital para España es el establecimiento de un clima de confianza en el ámbito digital como factor imprescindible para conseguir una implantación efectiva de las TIC en empresas y Administraciones, y un uso más intensivo de las mismas por la ciudadanía. Para ello, la Agenda plantea tres líneas de actuación principales en el ámbito de la confianza: impulsar el mercado de los servicios de confianza, reforzar las capacidades actuales para promover la confianza digital, e impulsar la excelencia de las organizaciones en materia de confianza digital. El objetivo de la ponencia es presentar los planes específicos que en materia de ciberseguridad y servicios de confianza desarrollarán la Agenda Digital para España, así como el nuevo contexto regulatorio europeo y nacional que acompañarán a estas iniciativas.

Ponente:
Antonio Alcolea Muñoz es Vocal Asesor de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo. Entre sus competencias destacan el desarrollo estratégico de políticas públicas para la ciberseguridad y la confianza digital, especialmente en materias normativas y supervisoras. Es Ingeniero Superior de Telecomunicación por la Universidad Politécnica de Madrid, Postgrado en Dirección de Tecnologías y Sistemas de Información por el Instituto de Empresa y Master en Gestión Pública Directiva por el Instituto Nacional de Administraciones Públicas.

La innovación colaborativa en la era del conocimiento

Sinopsis: Bajo la idea de que quien tiene la mejor estrategia de adaptación al cambio es quien maximiza su capacidad de éxito, para establecer la estrategia de Innovación Colaborativa hay que determinar y desarrollar tres aspectos. El primero es fijar cuáles son los ámbitos en los que te interesa innovar. Serán aquellos en los que pequeñas mejoras respecto del entorno generen grandes diferencias. El segundo es definir e incorporar a los actores necesarios en el ecosistema. Empresas colaboradoras, competencia, Universidades, Centros de Investigación, Polos Tecnológicos... El tercero es marcar el tamaño del ecosistema donde se va a rentabilizar la innovación. Pueden ir desde un pequeño grupo de compañías que gestionen la Propiedad Intelectual hasta la creación de *Open Communities* donde se comparta globalmente el resultado de la innovación y pueda volverse incluso uno de sus mecanismos.

Ponente:
Santiago Moral Rubio es actualmente 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 CISO.

CNPIC: Planes Estratégicos Sectoriales (PES)

Sinopsis: Para garantizar la protección de las infraestructuras críticas frente aquellas *amenazas de carácter físico y lógico* que puedan ponerlas en situación de grave riesgo se hace necesario, en desarrollo de la Ley 8/2011, la ejecución de una serie de planes de actuación a diferente nivel.
En la cúspide de esta "pirámide" se encuentran los Planes Estratégicos Sectoriales que, como instrumentos de estudio y planificación, permitirán identificar cuáles son los *servicios esenciales* proporcionados a la sociedad, el funcionamiento general de estos, las vulnerabilidades del sistema, riesgos a los que se enfrenta el sector, consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento.
A su vez, se podrá *identificar la tipología de infraestructuras de carácter crítico, que deberán de ser protegidas*, sobre las que se asientan esta serie de servicios, así como los operadores estratégicos propietarios y/o gestores de las mismas. La coordinación de estos operadores, *tanto en el ámbito de la seguridad física como en el de la seguridad cibernética corresponderá al Ministerio del Interior*, a través del CNPIC, como órgano competente legalmente para ello.
Los PES serán elaborados bajo la coordinación del CNPIC, con la participación de los ministerios competentes y de los operadores principales en cada uno de los sectores. *Los primeros de ellos están siendo ya acometidos* por sendos grupos de trabajo ad hoc, esperándose su aprobación tras el verano de 2013.

Ponente:
José Ignacio Carabias Corpa es Jefe del Servicio de Seguridad Física del **Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)**, adscrito al Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad del Ministerio del Interior. Licenciado en Ciencias Políticas por la Universidad Complutense de Madrid –especializado en Administración Pública–, miembro de la Escala Ejecutiva del Cuerpo Nacional de Policía, y Máster en Dirección y Gestión de la Seguridad por la Universidad Carlos III de Getafe (Madrid), Carabias ha formado parte del equipo encargado de la elaboración y diseño de la Ley y Real Decreto sobre Protección de Infraestructuras Críticas. En este ámbito de las PIC actualmente se encarga del desarrollo de los Planes Estratégicos Sectoriales, del contacto directo con los operadores críticos, para el estudio y análisis de sus infraestructuras estratégicas. Ha sido moderador y ponente en diferentes conferencias y jornadas, tanto nacionales como internacionales, en el marco de la seguridad y protección de las infraestructuras críticas.

EiTB (Radio Televisión Pública Vasca): "¿Y si nos ponen una bomba?"

Sinopsis: El 31 de diciembre de 2008, ETA hizo explosionar una furgoneta bomba en el edificio que alberga, entre otras, a la sede central del grupo de comunicación EiTB (Radio Televisión Pública Vasca). En la ponencia se relatará lo que pasó ese día, cómo se pusieron en marcha los mecanismos de contingencia, cómo respondieron los diversos equipos implicados en las labores de recuperación del negocio, y se compartirán las conclusiones obtenidas de todo ello que, por supuesto, en muchos casos no son meramente técnicas.
Asimismo, se recalcará la necesidad de tener en cuenta en los procedimientos de contingencia, factores humanos imprescindibles y casi siempre obviados, a la hora de plasmar planes y actuaciones. Y estará presente a lo largo de la exposición, las ventajas que tiene el uso de ciertos servicios en la nube para la correcta gestión de los planes de contingencia.

Ponentes:
Iñaki Regidor Mendiolea es Director de Vanguardia de EiTB (Radio Televisión Pública Vasca). Ingeniero en informática por la Universidad de Deusto, comenzó su andadura profesional en 1986 en los ámbitos de la consultoría en ambientes *mainframe* para empresas del sector industrial vasco y para el sector público. Tras una etapa de responsable de informática de una empresa siderometalúrgica vizcaína, donde fundamentalmente se centró en la integración de aplicaciones empresariales, en septiembre de 1999 se hace cargo de la Dirección de Vanguardia del Grupo de Comunicación EuskalerratiTelebista. Entre sus labores destacan las de desarrollo, soporte y apoyo tecnológico al mantenimiento y desarrollo de procesos de negocio dentro del Grupo EiTB, tanto mediante plataformas C/S como mediante la Intranet y la de soporte a la web, estando integrado en la dirección de dicho medio.

Ricardo Acebedo Lejardi es Responsable de Marketing de Nextel, S.A. Licenciado en Ciencias Económicas y Empresariales por la Universidad del País Vasco (UPV/EHU) y especializado en Marketing (Máster en Marketing en el año 2000) ha desarrollado su labor profesional principalmente como Responsable de Marketing y *Account Manager* en Nextel S.A. Ingeniería y Consultoría, compañía a la que se incorporó en enero de 1999. Actualmente colabora también como profesor asociado en el Departamento de Comunicación Audiovisual y Publicidad de la Universidad del País Vasco (UPV/EHU).

Administración del Principado de Asturias: modernizando el Servicio de Seguridad TIC dentro del marco establecido por el Esquema Nacional de Seguridad

Sinopsis: Proporcionar servicios de Seguridad TIC a una Organización de la envergadura de la Administración del Principado de Asturias, formada por Consejerías y Organismos de características variadas, condicionada por la actual realidad presupuestaria de las Administraciones Públicas españolas y por las regulaciones que afectan al sector público, es una labor que requiere una dirección firme y dinámica, una gestión rigurosa de la proporcionalidad en los costes, la selección de socios tecnológicos solventes y una estrecha colaboración entre la Administración y dichos socios.
En la ponencia se pretende guiar a la audiencia por el camino que ha seguido la seguridad TIC en la Administración del Principado desde 2008 hasta el presente. Se proporcionará una descripción general de la situación de partida, de las razones que llevaron a cambiar el planteamiento, las decisiones que se tomaron, cómo se materializaron a finales de 2010 y cómo han ido evolucionando desde entonces tomando como brújula los requisitos del Esquema Nacional de Seguridad. Por último, se dejarán entrever las líneas maestras que se considera deberían contribuir a seguir modernizando el servicio.

Ponentes:
Javier Rojo Fernández es Jefe del Servicio de Seguridad de la DGTIC (Consejería de Economía y Empleo del Principado de Asturias). Informático (Universidad de Oviedo) y Máster en Informática Empresarial, tiene concimientos profundos en el terrero profesional y de investigadora en sistemas dinámicos caóticos y entornos AS-400. Es docente de programación en lenguajes de 4ª Generación y miembro del equipo de investigación EDS en la Universidad de León y Funcionario de la Administración, donde ha ejercido como Director de Proyectos en el Área de Sistemas Educativos, Director del Centro de Gestión de Servicios Informáticos (CGSI) del Principado de Asturias y actualmente Jefe del Servicio de Seguridad. También es Miembro del Grupo de trabajo de Seguridad del Comité Sectorial de Administración Electrónica y miembro del Comité de Seguridad de la Información de las Administraciones Públicas.

Francisco Javier Diéguez Barriocanal es Gerente en el Departamento de Ciberseguridad de Indra. Licenciado en Informática por la Universidad de Deusto, PMP por el PMI, y CISA-CISM-CRISC por ISACA, ha desarrollado su carrera profesional en Norsistemas, Soluziona y actualmente en Indra. Cuenta con 10 años de experiencia en seguridad de la información y es responsable de *delivery* de proyectos de ciberseguridad para Indra en el Norte de España. Ha dirigido proyectos de consultoría de seguridad, auditoría de sistemas, "securización" de infraestructuras TI, *hacking* ético, planes de continuidad, sistemas de gestión de seguridad de la información y oficinas técnicas de seguridad, entre otros.

SEGUNDO MÓDULO, 24 DE ABRIL

09:00h. Entrega de documentación.
Moderador: **José Carrillo Verdún**, Facultad de Informática de la Universidad Politécnica de Madrid.

09:30h. Ponencia: **El proceso de ciclo de vida de desarrollo seguro (PCVDS) en Bankia.**
Ponentes:
Javier Sevillano Izquierdo, Responsable de Seguridad Tecnológica. Bankia.
Vicente de la Morena Baena, Responsable Comercial de Grandes Empresas de IBM Security Systems.

10:00h. Coloquio.

10:10h. Ponencia: **Bankinter: Detección temprana de incendios digitales y ciberriesgos en Internet.**
Ponentes:
Julio San José Sánchez, Gerente de Riesgos Tecnológicos de Bankinter.
Daniel Solís Agea, CEO de blueliv.

10:40h. Coloquio.

10:50h. Pausa-Café.
Moderador: **Luis Fernández Delgado**, Editor de Revista SIC.

11:30h. Ponencia: **Dirección General de la Policía: ciberseguridad, un enfoque integral de ciclo completo.**
Ponentes:
Francisco Jara González, Jefe del Servicio de Seguridad TIC de la Dirección General de la Policía.
Jesús Milán Lobo, Responsable de Servicios de Seguridad y Riesgos Tecnológicos para Empresas. Telefónica España.

12:00h. Coloquio.

12:10h. Ponencia: **Grupo BBVA: innovación en Sistemas de Detección y Prevención de fraude bancario.**
Ponentes:
Juan Francisco Losa Muñoz, Responsable de Ingeniería y Productos del área de Innovación en Riesgo, Fraude y Seguridad IT de Grupo BBVA.
Juan Jesús León Cobos, Director de Productos y Nuevos Desarrollos. GMV.

12:40h. Coloquio.

12:50h. Ponencia: **"Compliance" en tiempo real.**
Ponentes:
Idoia Mateo Murillo, Directora de Riesgos Tecnológicos Global de Produbán. Grupo Santander.
Nekane Arjona Suquía, Gerente Global de Audit & Compliance de Produbán. Grupo Santander.

13:20h. Coloquio.

13:30h. Ponencia: **Hacia una colaboración eficiente entre los CISOs y la 'ciberpolicía judicial' en la investigación de la Criminalidad Informática.**
Ponente: **Elvira Tejada de la Fuente**, Fiscal de Sala contra la Criminalidad Informática. Fiscalía General del Estado.

14:00h. Coloquio.

14:10h. Almuerzo.
Moderador: **Jorge Dávila Muro**, Director del Laboratorio de Criptografía LSIIS-Facultad de Informática de la Universidad Politécnica de Madrid.

16:10h. Ponencia: **Novagalicia Banco: Análisis de Seguridad en Aplicaciones.**
Ponentes:
Carlos Pérez Saldaña, Gestor de Proyectos de Seguridad en el Departamento de Seguridad TI de Novagalicia Banco.
Jaume Ayerbe Font, Responsable de HP Enterprise Security Products en Iberia.

16:40h. Coloquio.

16:50h. Ponencia: **Dixi Media y su expansión corporativa. La seguridad de su entorno *cloud* como premisa.**
Ponentes:
Carlos Bote, Director de Sistemas de Dixi Media.
Olof Sandstrom Herrera, Director de Operaciones de Arsys Internet

17:20h. Coloquio.

17:30h. Fin de la segunda sesión.

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

El proceso de ciclo de vida de desarrollo seguro (PCVDS) en Bankia

Sinopsis:
PCVDS (Proceso de ciclo de vida de desarrollo seguro).
¿Por qué?
• Una parte importante de los incidentes de seguridad producidos en las compañías es debida a la explotación malintencionada de defectos de seguridad en los aplicativos.
¿Para qué?
• Evitar, detectar y/o mitigar incidentes de seguridad.
• Relación coste vulnerabilidad – proceso de desarrollo
• Confianza: mostrar a la Dirección y a los Auditores que se trabaja con un método seguro, normalizado y estándar.

Ponentes:
Javier Sevillano Izquierdo es Responsable de Seguridad Tecnológica en Bankia. Dispone de 26 años de experiencia en Tecnologías de la Información, 18 de ellos relacionados directamente con la Seguridad Informática. Informático, ISO 27001 Lead Auditor por la British Standard Institution y vocal del Subcomité 27 de ISO (Seguridad en Tecnologías de la Información). Anteriormente desarrolló su carrera profesional en Caja Madrid, Sistema 4B, Seinca y McDonnell Douglas.

Vicente de la Morena Baena es Responsable Comercial de Grandes Empresas de IBM Security Systems. Cuenta con 17 años de experiencia en el sector TI, los últimos 15 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.

Bankinter: detección temprana de incendios digitales y ciber-riesgos en Internet

Sinopsis:
Bankinter, una de las entidades más pioneras en tecnología de nuestro país, ha seguido reforzando en los últimos años su línea estratégica de trabajo mediante la ciberinteligencia y mitigación de posibles riesgos en Internet. En esta ponencia, se mostrará cómo mediante la plataforma Optos, la recolección de información en el *deep*internet, *underground*, web 2.0, repositorios documentales, etc., se puede realizar detección temprana de incendios digitales y una seguridad colaborativa, que posibilita y facilita cumplir los objetivos de negocio de la entidad.
Todo ello impulsado desde el área de Riesgos Tecnológicos, que gestiona un ecosistema de especialistas en fraude, riesgos y reputación. De esta manera se facilitan métricas para medir los riesgos y tomar medidas mitigadoras gracias a una gestión proactiva de los riesgos en Internet.

Ponentes:
Julio San José Sánchez es Gerente de Riesgos Tecnológicos de Bankinter. Con una trayectoria de más de veintidós años en seguridad de la información, desde su incorporación al banco en 1997 ha desempeñado varios puestos, desde Responsable de Seguridad de Aplicaciones hasta Responsable Técnico de Seguridad Informática. Es Director de Seguridad Privada, CISM / CRISC por ISACA y BS 7799, BS 25999 por BSI. Miembro del Subcomité de Seguridad de las TI (CTN 71/SC27) –habiendo colaborado en la redacción de varias normativas, tanto nacionales como internacionales– y representante del SC27 en el *Grupo Especial de Análisis de Riesgos GET 13*. Vocal del CTN 71/SC7/WG25, *IT Service and Operations Management, ITIL,* San José es también miembro del Grupo de Expertos de la Cátedra Gestión de Riesgo del Instituto de Empresa y profesor del Máster en Dirección y Gestión de la Seguridad de la Información de la UPM. Así mismo es coautor del libro *"Seguridad de las tecnologías de la información. La construcción de la confianza para una sociedad conectada"*, editado por AENOR.

Daniel Solís Agea es CEO de blueliv. Ingeniero en Telecomunicaciones y socio fundador de la compañía, 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 catorce 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.

Dirección General de la Policía: ciberseguridad, un enfoque integral de ciclo completo

Sinopsis:
Los tiempos han cambiado. Vivimos en un mundo global, hipercontectado a la red donde la realidad que nos ha tocado vivir en términos de Seguridad y Gestión de Riesgos es totalmente diferente y lo que nos viene, de manera natural, a la cabeza son las palabras de Sir Walter Scott "Mira hacia atrás y ríete de los peligros pasados". Las reglas del juego han cambiado, el campo de batalla también y disponer de información sobre los jugadores, sus motivaciones e intereses, así como los medios y vectores de ataque que se dispone y sus marcos de aplicación es crítico para poder tener criterio y así tener capacidad de actuar. Todo ello conforma la ciberinteligencia, el tener "ojos y oídos" en la red y la capacidad de contextualizar la información obtenida al objeto de ponerla en valor integrándola con los sistemas de ciberseguridad y protección, especialmente cuando eres una Infraestructura Crítica.

Ponentes:
Francisco José Jara González es Responsable de Seguridad TIC de la Dirección General de la Policía. Inspector del Cuerpo Nacional de la Policía, pertenece al Cuerpo desde 1999.

Jesús Milán Lobo es Responsable de los Servicios de Seguridad y Riesgos Tecnológicos para Empresas de Telefónica España. Ingeniero en Informática con especialidad en Gestión por el ICAI-ICADE. Certificado CISM, Lead Auditor ISO27001 -BS25999 y CSSK (Certified of Cloud Security Knowledge) emitido por la CSA. Miembro del Subcomité Nacional de Seguridad de las TI (CTN 71 / SC27) y miembro WG1 y colaborador en la redacción de normas internacionales. Miembro de la Junta Directiva de ISMS Forum Spain y Vicepresidente del Cloud Computing Alliance (CSA) - Capítulo Español.

Grupo BBVA: innovación en Sistemas de Detección y Prevención de Fraude Bancario

Sinopsis:
Las herramientas que apoyan a los analistas que detectan fraude tradicionalmente están ligadas a las tecnologías y algoritmos originales de los fabricantes, los cuales no tienen razones para adoptar tecnologías disruptivas que pudieran mejorar sus resultados y reducir los costes de operación, en un perfecto ejemplo del clásico libro "Innovator's Dilemma" de Christensen. En el transcurso de los dos últimos años, GMV y BBVA, a través de su Centro de Investigación para la Gestión Tecnológica del Riesgo, vienen trabajando conjuntamente en el desarrollo de nuevas tecnologías disruptivas de Inteligencia Artificial para la detección del fraude, basadas en los denominados "Sistemas In-

munitarios Artificiales", que hacen posible el entrenamiento "on-line" y proporcionan con cada alerta información de apoyo a los analistas que las clásicas Redes Neuronales no proporcionan. Sin embargo, un reto aún mayor es la incorporación de estas nuevas tecnologías de manera sinérgica con las tradicionales que operan en la entidad.
Una aproximación innovadora, desde el punto de vista de las entidades financieras, es el diseño de una arquitectura que admita la incorporación de múltiples algoritmos de detección y saque partido de la complementariedad entre tecnologías diferentes con el objetivo, a largo plazo, de posibilitar la incorporación de mejores algoritmos de una forma continua, ordenada y lo que es más importante, bajo el control de la entidad financiera.

Ponentes:
Juan Francisco Losa Muñoz es Responsable de Ingeniería y Productos del área de Innovación en Riesgo, Fraude y Seguridad IT de BBVA. Ingeniero en Informática por ICAI y Executive MBA por el Instituto de Empresa, Losa cuenta además con las certificaciones CISA, CISM y CISSP. Ha desempeñado distintos puestos de responsabilidad en consultoría y empresas del sector financiero, siempre ligados a la seguridad.

Juan Jesus León Cobos es Director de Productos y Nuevos Desarrollos de GMV. Ingeniero Aeronáutico por la UPM, PDD por el IESE y CISM, León 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 EEUU. 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.

"Compliance" en tiempo real

Sinopsis:
Actualmente las organizaciones están sometidas a un entorno que cambia muy rápido, al cual se le exige cada día mayor nivel de control. Alcanzar los niveles de control y testeos de tales entornos en base a muestra, no es suficiente para mejorar de manera dinámica, y una verdadera gestión del riesgo requiere de los responsables de los entornos que sean capaces por sí de valorar su nivel de control de manera exhaustiva. Sin duda las herramientas para la automatización en este contexto son indispensables donde incluso los responsables de los citados entornos puedan evaluarse en tiempo real en un periodo razonable. Esta es la única manera de que los controles lleguen a formar parte de los procesos tecnológicos y la gestión del riesgo añada el valor que los clientes nos demandan.

Ponentes:
Idoia Mateo Murillo es Directora Global de Riesgos Tecnológicos de Produban. Grupo Santander. Tiene 18 años de trayectoria profesional en el mundo de la Seguridad y los Riesgos Tecnológicos, los 7 últimos como Responsable Global de Riesgos Tecnológicos en Produban, la empresa de gestión de infraestructuras del Grupo Santander, con reporte de todos los responsables de Riesgos Tecnológicos y Seguridad de todos los países del Grupo, más de 200 personas (Brasil, México, EE.UU., Reino Unido, Alemania, Portugal y España). Dentro de su ámbito de actuación están las áreas de Auditoría y Cumplimiento, Seguridad, Gestión de la Contigencia Tecnológica y Riesgos Tecnológicos. La función principal de Produban es realizar una gestión unificada y estandarizada de la Producción de las entidades Financieras del Grupo Santander, así como la creación de una Infraestructura de Grupo con criterios de eficiencia, calidad de servicio y disminución del riesgo Operacional. Sus funciones principales son definir la estrategia de Seguridad y Riesgos Tecnológicos en Produban, acometiendo la definición de proyectos de minimización de Riesgos Tecnológicos, y asegurar su implantación en todos los países, a la vez que asegurar la satisfacción de los clientes del Grupo Santander con los servicios de Seguridad y Riesgos Tecnológicos proporcionados desde Produban.

Nekane Arjona Suquía es Gerente Global de Auditoría y Cumplimiento de Produban. Grupo Santander. Durante los últimos 8 años ha estado contribuyendo activamente a la definición y puesta en marcha de marcos de control de riesgos tecnológicos y seguridad eficaces y eficientes, integrando los mismos en los procesos de la organización, para fomentar la consecución de mitigación de riesgos, optimización de los costes y aumentar el valor añadido. Entre sus especialidades se encuentra: IT Governance, IT Risk Management, Cumplimiento de TI (auditoría de TI y coordinación de auditorías y automatización de controles), Normas de trabajo: SOX-IT, ITIL, lean IT, ISO 27000 serie, CobiT. Asimismo, cuenta con más de 6 años de experiencia en el ámbito internacional, multicultural y multilingüe (más de 12 países).

Hacia una colaboración eficiente entre los CISOs y la 'ciberpolicía judicial' en la investigación de la Criminalidad Informática

Sinopsis:
La criminalidad informática es un fenómeno complejo, en constante evolución y capaz de afectar gravemente a bienes jurídicos muy diversos como la intimidad y libertad personal, el honor, la integridad moral, la indemnidad sexual de menores, el patrimonio, el orden económico-social o la seguridad colectiva.
Actuar eficazmente ante este fenómeno exige un planteamiento multidisciplinar y la colaboración y *suma de esfuerzos* de investigadores, responsables de seguridad informática de entidades públicas o privadas y operadores jurídicos. En este marco, el Ministerio Fiscal, defensor de la legalidad, regido por criterios de imparcialidad y unidad de actuación interna y encargado constitucionalmente del ejercicio de acciones penales en defensa de los ciudadanos y del interés general se configura como el actor idóneo para coordinar, facilitar y canalizar hacia los Tribunales de Justicia, con plena sujeción a la normativa vigente, las investigaciones policiales y las denuncias y reclamaciones de particulares, colectivos o instituciones víctimas de estas criminales conductas.

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. 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 Fiscal General del Estado en materia de Delincuencia Informática entre diciembre del 2007 a noviembre de 2008.

Novagalicia Banco: análisis de seguridad en aplicaciones

Sinopsis:
Las aplicaciones son el motor de los negocios, y lamentablemente el principal vector de ataque de los cibercriminales. Por ello, la dirección de NovaGalicia Banco –entidad resultante de la fusión de las cajas gallegas– tuvo muy clara la necesidad de implantar una oficina de seguridad de las aplicaciones en un tiempo mínimo. A tal efecto se eligió un servicio gestionado con escalabilidad y que permitiera la personalización de los análisis para reflejar las particularidades de los *frameworks* usados en el banco y conjugar las ventajas de un servicio gestionado, con toda la personalización de un despliegue tradicional.
Para NovaGalicia Banco la seguridad en su banca electrónica es un aspecto estratégico de su actividad y, por lo tanto, el análisis de código en aplicaciones se convierte en un pilar fundamental de la lucha contra el fraude bancario.

Ponentes:
Carlos Pérez Saldaña es Gestor de Proyectos de Seguridad en el Departamento de Seguridad TI de Novagalicia Banco. Ingeniero Superior en Informática por la Universidad Pontificia Comillas (ICAI), actualmente lleva 4 años es su cargo. Anteriormente desempeñó el puesto de Consultor de Seguridad durante 5 años en Business Integration del Grupo British Telecom.

Jaume Ayerbe Font es Responsable de HP Enterprise Security Products en la región de Iberia. Ingeniero Electrónico, posee un MBA por el IESE Universidad de Navarra y está certificado como CRISC por ISACA, entre otras acreditaciones profesionales. En sus más de 8 años en HP, ha desarrollado distintas responsabilidades dentro de la división de soluciones de gestión de IT para grandes organizaciones. Anteriormente desarrollo su carrera en NetIQ y Microsoft.

Dixi Media y su expansión corporativa. La seguridad de su entorno *cloud* como premisa

Sinopsis:
En la ponencia de Dixi Media y Arsys se compartirá con los asistentes a Securmática 2013 los planes de expansión del grupo mediatico y la rotunda apuesta por el entorno *cloud* como base de su entorno TI, haciendo especial énfasis en las capacidades que en el ámbito de seguridad un proveedor de servicios de nube debe garantizar para poder hacer frente a los innumerables retos que en dicho ámbito se plantean todos los días y sobre los que sin el adecuado compañero de viaje le sería muy difícil desarrollar su actividad.

Ponentes:
Carlos Bote es Director de Sistemas de Dixi Media. Con más de 15 años de experiencia en entornos IT en grupos de medios, como Grupo Prisa y Unidad Editorial, ha trabajado también previamente en el sector financiero. Bote se caracteriza por ser un "evangelista" en entornos tecnológicos y especialista en entornos *Open Source*. Tiene asimismo experiencia contrastable en temas de seguridad de la información y está certificado en la 27001 sobre SGSI.

Olof Sandstrom Herrera es Director de Operaciones de Arsys Internet. Ingeniero Técnico de Telecomunicación por la Universidad de Las Palmas de Gran Canaria, es CISA y CISM, Auditor Jefe ISO 27001, vicepresidente de la Comisión de Seguridad de AMETIC, miembro del consejo técnico asesor de CESICAT, miembro del consejo técnico asesor del capítulo español de Cloud Security Alliance, además de coordinador del grupo de trabajo 4 del Subcomité 27 de Aenor.

TERCER MÓDULO, 25 DE ABRIL

09:00h. Entrega de documentación.
Moderador: **Antonio Ramos García**, Presidente del Capítulo de Madrid de ISACA.

09:30h. Ponencia: **La seguridad como piedra angular de la internacionalización de las empresas: Telefónica Global Solutions.**
Ponentes:
Cristina Gómez Sánchez, Responsable de Seguridad de Sistemas de Telefónica Global Solutions.
Juan José Míguez Iglesias, Socio de Riesgos Tecnológicos de PwC.

10:00h. Coloquio.

10:10h. Ponencia: **Beneficios de la integración de la metodología de riesgos empresariales en una Oficina Técnica de Seguridad de la Información.**
Ponentes:
Jordi Trapero Puig, CISO del Grupo SEAT. IT Security, Risk & Compliance.
José Luis Rojo de Luque, Senior Manager en IT Advisory. Ernst & Young.

10:40h. Coloquio.
Moderador: **José de la Peña Muñoz**, Director de Revista SIC.

10:50h. Ponencia: **Puntos de fricción en la negociación de contenidos de la nueva Directiva de privacidad y el Reglamento.**
Ponente:
José Luis Piñar Mañas, Catedrático de Derecho Administrativo y Vicerrector de Relaciones Internacionales de la Universidad CEU - San Pablo de Madrid. Abogado. Titular de la Cátedra Google sobre Privacidad, Sociedad e Innovación.

11:20h. Coloquio.

11:30h. Pausa-café.

12:00h. Ponencia: **MCCD-Mando Conjunto de Ciberdefensa: prioridades en el desarrollo de las capacidades de la ciberdefensa militar.**
Ponentes:
Francisco Zea Pasquín, Capitán de Navío. Jefe de Seguridad de la Información de los Sistemas CIS del Estado Mayor de la Defensa. Ministerio de Defensa.

12:30h. Coloquio.
Moderador: **Luis Fernández Delgado**, Editor de Revista SIC.

12:40h. Ponencia: **Ataques: más allá de la imaginación de los CISOs.**
Ponente:
Chema Alonso, Consultor de Seguridad en Informática 64.

13:10h. Coloquio.

13:20h. Ponencia: **¿Se puede restaurar la confianza en la certificación electrónica?**
Ponente:
Jorge Dávila Muro, Criptólogo, Profesor Titular de la Facultad de Informática de la UPM y Director de I+D+i de EnCifra.

13:50h. Coloquio.

14:00h. Almuerzo, fin de la tercera sesión y fin de Securmática 2013.

La seguridad como piedra angular de la internacionalización de las empresas: Telefónica Global Solutions

Sinopsis:
En el marco actual de crisis económica en España, cada vez son más las organizaciones que exportan sus productos y servicios al exterior: tanto en el caso de las multinacionales españolas, que ya venían realizándolo con anterioridad y ven crecer la rentabilidad de sus inversiones en el extranjero con resultados, en algunos casos, mejores que en el mercado local, como otras que recurren a la internacionalización como recurso para maximizar las oportunidades de negocio. En este escenario internacional, de nuevas oportunidades, también aparecen nuevos retos asociados a las diferentes legislaciones, culturas, idiomas y horarios, dificultándose la coordinación de los diferentes equipos distribuidos, que incrementan los riesgos relativos a la Seguridad de la Información.
Se pretende dar una visión de cómo Telefónica Global Solutions, con el apoyo de PwC, ha logrado convertir la necesidad de mitigar dichos riesgos en una oportunidad para aportar valor al negocio en su dimensión internacional. Partiendo de un modelo de seguridad corporativo, pasando por la utilización de infraestructuras comunes de seguridad, hasta llegar a la protección de la información crítica del negocio, todo está enfocado, desde su concepción, a potenciar el desarrollo del negocio a nivel internacional.

Ponentes:
Cristina Gómez Sánchez es Responsable de Seguridad de Sistemas de Telefónica Global Solutions. Ingeniera Informática por la Universidad Rey Juan Carlos, cuenta con más de 10 años de experiencia en el ámbito de Seguridad de la Información. Desde hace casi tres años colabora con Telefónica Global Solutions en la responsabilidad de la seguridad global de plataformas multinacionales analizando, definiendo y ejecutando la implantación de novedosas soluciones de seguridad con el objetivo de garantizar unos niveles de protección global de la compañía y permitiendo cubrir todos los aspectos necesarios dictados por la Corporación. Gómez cuenta con innumerables cursos de especialización en el ámbito de Seguridad de la Información y tiene una relevante experiencia en proyectos internacionales en multinacionales españolas, lo que le hace conocedora de las óptimas soluciones tecnológicas en seguridad para una compañía global como es Telefónica Global Solutions.

Juan José Míguez Iglesias es Socio del Área de Riesgos Tecnológicos de PwC. Cuenta con más de 15 años de experiencia en el ámbito de Seguridad de la Información. Ingeniero de Telecomunicación en la especialidad de Telemática por la Universidad de Vigo, es Lead Auditor ISO 27001 y 22301 por BSI, CGEIT, CISA y CISM por ISACA. Ha liderado múltiples proyectos, desde Planes Directores de Seguridad y Planes de Continuidad de Negocio, hasta Soluciones de Gestión de Identidades y Accesos y revisiones de Seguridad técnicas. Durante su trayectoria ha tenido la oportunidad de coordinar numerosos proyectos en el ámbito internacional, contando con una dilatada experiencia en la definición del marco estratégico de Seguridad en la internacionalización de las compañías

Beneficios de la integración de la metodología de riesgos empresariales en una Oficina Técnica de Seguridad de la Información

Sinopsis:
Nadie pone en duda la importancia y el valor añadido que aporta durante el proceso de toma de decisiones integrar los riesgos de Seguridad de la Información dentro del universo de riesgos empresarial que afectan a una organización. Sin embargo, también son bien conocidos los retos que presenta este proceso: por un lado, conseguir hacer partícipe a toda la organización para disponer de una visión global y completa; y por otro, transformar los procesos empleados en el ámbito de la gestión de la Seguridad de la Información con el fin de adecuarlos, técnica y organizativamente, a los criterios establecidos por la metodología de gestión de riesgos empresarial.
Grupo SEAT, con la colaboración de Ernst&Young, ha conseguido hacer frente a esta situación mediante el despliegue de un modelo de oficina técnica de seguridad TIC basado en procesos que alimentan, impulsan, monitorizan y actualizan de manera continua el sistema de gestión de riesgos corporativo.

Ponentes:
Jordi Trapero Puig es CISO del Grupo SEAT. IT Security, Risk & Compliance. Ingeniero de Telecomunicaciones por la UPC de Barcelona, tiene más de 5 años de experiencia en el campo de la Seguridad de la Información y gestión de riesgos IT. En este ámbito ha desarrollado toda su carrera profesional, principalmente dentro del Grupo SEAT, ocupando las funciones de Information Security Officer, IT Risk Officer y Chief Information Security Officer, cargo que ostenta actualmente. Entre sus principales proyectos implantados destaca el despliegue de una metodología de gestión de riesgos en el ámbito de IT, así como su integración en los procesos y metodologías de gestión de la seguridad de la información. En la actualidad, dirige y coordina el Programa de Seguridad TI dentro del Grupo SEAT y es miembro del *Information Security Steering Commitee* del Grupo Volkswagen.

José Luis Rojo de Luque es Senior Manager en IT Advisory en Ernst & Young. Tiene más de 9 años de experiencia liderando múltiples proyectos y servicios relacionados con la Gestión de Riesgos IT y Gestión y Estrategia de la Seguridad de la Información. Ha colaborado con varias de las principales compañías de nuestro país en la planificación y gestión de la seguridad de la información, así como en el despliegue de metodologías de análisis y gestión de riesgos, tanto de IT como de seguridad. De entre toda su experiencia destaca su amplia colaboración con las compañías del Grupo Volkswagen, y concretamente con Grupo SEAT, en el que lidera los servicios de seguridad que proporciona Ernst & Young.

Puntos de fricción en la negociación de contenidos de la nueva Directiva de Privacidad y el Reglamento

Sinopsis:
La Comisión Europea está decidida a aprobar un nuevo Reglamento Europeo de Protección de Datos. En enero de 2012 presentó el proyecto, que en estos momentos está siendo analizado por el Parlamento Europeo. Se trata de la más importante reforma del marco normativo europeo sobre protección de datos desde que se aprobó la Directiva 95/46/CE, que será derogada. Las novedades que introduce son de enorme importancia y las negociaciones para sacar adelante el proyecto están siendo muy intensas. Aspectos como la aplicación extraterritorial del propio reglamento (aplicación a tratamientos de datos llevados a cabo fuera de la Unión Europea), la regulación del consentimiento (que pasaría a ser explícito), el régimen llamado "*one stop shop*" en cuanto a la competencia de la Autoridad nacional de control, que pasaría a ser la del domicilio del ente matriz en el caso de multinacionales, o la regulación del derecho al olvido, son algunos de los que están planteando más serias discrepancias. Por otra parte, se considera muy positiva la incorporación de los principios de *privacy by design* o *privacy by default*, la referencia a las *Binding Corporate Rules* y el régimen de transferencias internacionales o la inclusión del principio de *accountability* o de responsabilidad. Una muy importante novedad es la previsión obligatoria de la figura del *Data Protection Officer* en ciertos casos y la supresión con carácter general de la obligación de inscripción de los ficheros.

Ponente:
José Luis Piñar Mañas es Catedrático de Derecho Administrativo y Vicerrector de Relaciones Internacionales de la Universidad CEU-San Pablo de Madrid, Titular de la Cátedra Google sobre Privacidad, Sociedad e Innovación, Doctor en Derecho por la Universidad Complutense de Madrid, Abogado y consultor internacional en materia de protección de datos y *Adjunct Professor of Law de la Georgetown University* (2005-2007). Ha sido Director de la Agencia Española de Protección de Datos, Vicepresidente del Grupo Europeo de Autoridades de Protección de Datos y Presidente-Fundador de la Red Ibe-

roamericana de Protección de Datos. Está en posesión de Cruz de Honor de San Raimundo de Peñafort (2012). Ha sido Decano de las Facultades de Derecho de las Universidades de Castilla-La Mancha y CEU-San Pablo de Madrid. Ha sido miembro de la Junta Directiva de la Asociación Española de Profesores de Derecho Administrativo y lo es de la Comisión Jurídica del Consejo General de la Abogacía Española y del Consejo Asesor de la Asociación Española de Fundaciones. Presidente de la Sección 6ª y Vicepresidente del Jurado de la Publicidad de Autocontrol, Investigador Principal del Proyecto de Investigación "Protección de Datos, transparencia, seguridad y mercado", del Ministerio de Ciencia e Innovación (2010-2012) y del Proyecto "Aplicación Extraterritorial de la normas y reforma de la Directiva sobre protección de Datos, del Ministerio de Economía y Competitividad (2013-2015)". Profesor invitado de numerosas Universidades. Es autor de numerosas publicaciones sobre Derecho público, desarrollo sostenible, derecho de protección de datos, transparencia y acceso a la información, fundaciones, contratos públicos y derecho comunitario.

MCCD-Mando Conjunto de Ciberdefensa: prioridades en el desarrollo de las capacidades de la ciberdefensa militar

Sinopsis:

Tras la aprobación en febrero de 2013 de la Orden Ministerial de creación del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD), en el Estado Mayor de la Defensa (EMAD) se está trabajando intensamente en su desarrollo y puesta en funcionamiento. Este Mando, asumirá y potenciará todas las capacidades de ciberdefensa que actualmente posee el EMAD y desarrollará todas aquellas necesarias que permitan proteger adecuadamente ante ciberataques, tanto a los sistemas de las Fuerzas Armadas (FAS) como aquellos otros que se le encomienden y puedan afectar a la Defensa Nacional.

Las FAS disponen actualmente de una serie de capacidades de ciberdefensa con un alto nivel de desarrollo, como son por ejemplo aquellas relacionadas el Adiestramiento y Formación, en el que destaca los Ejercicios de Ciberdefensa de las FAS, en los que personal del Ministerio de Defensa relacionado con la seguridad de las TIC, es adiestrado en técnicas de seguridad y defensa. Además, a estas capacidades hay que sumar aquellas de carácter preventivo, detectivo y reactivo que serán proporcionadas por el CERT-FAS, actualmente operando con una capacidad inicial. El desarrollo de todas estas capacidades estará alineado con la Estrategia Española de Ciberseguridad, potenciándose la colaboración entre diferentes entidades para conseguir el objetivo común que es la seguridad nacional en el ciberespacio.

Ponente:

Francisco Zea Pasquín, Capitán de Navío. Actualmente es Jefe de Seguridad de la Información de los Sistemas CIS del Estado Mayor de la Defensa (Ministerio de Defensa). Nació en Ferrol en 1959. Cursó sus estudios en la Escuela Naval Militar de Marín y desde el 16 de Julio de 2011 ostenta el empleo de Capitán de Navío de la Armada Española. Posee la Especialidad de Analista de Sistemas Integrados y es Diplomado de Estado Mayor de las Fuerzas Armadas. En el ámbito de los Sistemas de Información y Telecomunicaciones, entre los años 1997 y 1999 ha sido el Jefe del Programa de Mando y Control de las Fragatas clase Baleares; desde julio del 2004 a julio de 2007 ha trabajado en la Agencia OTAN de Consulta, Mando y Control "NC3A" en Bruselas (Bélgica) como Jefe del Programa Naval "MCCIS" (Sistema de Mando y Control Marítimo), y entre los años 2008 y 2011 fue nombrado Jefe del equipo de desarrollo e implementación del programa OTAN "Sistema de Alerta Marítima" (MSA) en el Cuartel General de la OTAN en Norfolk (Estados Unidos de América).

Ataques: más allá de la imaginación de los CISOs

Sinopsis:

Una FOCA, dos FOCAs, tres FOCAs. Como siempre hay nuevas formas de atacar tu sistema, ya sea por medio de metadatos, nuevos fallos en la web o el protocolo IPv6. Todos viviendo contigo y de los que debes preocuparte cuanto antes. Durante los últimos años me he levantado todos los días pensando en cómo romper la seguridad de los sistemas informáticos, de cómo aprovechar los fallos para organizar un ataque, y a desarrollar herramientas que demostraran lo fácil que es. En esta sesión podrás verlo en real.

Ponente:

Chema Alonso, Consultor de Seguridad. Informática 64. Conocido como el Maligno, es quizá uno de los referentes de seguridad informática y *hacking* a nivel mundial. Ingeniero Informático de Sistemas por la Universidad Politécnica de Madrid –donde ha sido nombrado Embajador Honorífico por su excelente carrera profesional– e Ingeniero Informático y Máster en Sistemas de Información por la Universidad Rey Juan Carlos (URJC). Ha sido premiado como *Most Valuable Professional* en *Enterprise Security* por Microsoft durante 8 años. En la URJC ha realizado su Doctorado en Informática, dedicado a técnicas de auditoría de seguridad web.

Alonso es Miembro fundador de Informática 64, donde trabaja como consultor e investigador de Seguridad desde hace 14 años. De su trabajo en esta compañía, han salido herramientas populares de la seguridad informática como FOCA, MetaShield Protector o la reciente Forensic FOCA, y las publicaciones de técnicas *hacking* como Time-BasedBlind SQL Injection, (Blind) LDAP Injection o Connection String Parameter Pollution.

Recorre el mundo participando en conferencias de seguridad de renombre, como Defcon, BlackHat, ShmooCON, HackCON, SEC-T, DeepSEC, RootedCON, NoConName, Ekoparty, Yahoo! Security Week, Digital CrimeConsortium, FIRST, ToorCON, etc., en las que ha pronunciado más de 100 conferencias.

¿Se puede restaurar la confianza en la certificación electrónica?

Sinopsis:

La confianza es una característica esencial de la experiencia existencial humana y en parte lo es porque a menudo queda defraudada. La dimensión digital de nuestras sociedades adolece de las mismas necesidades de confianza pero han sido muchos los ejemplos que más bien favorecen a su antónimo, la **Desconfianza Digital**. En esta ponencia se verá cuál es esa necesidad, cómo se ha depositado en resistencias algorítmicas abstractas y cómo la realidad ha sido capaz de ponerla en jaque más de una vez. Veremos qué es lo que ha fallado y veremos a qué factores puede atribuirse. Veremos si son los algoritmos criptográficos los que han defraudado muestra necesaria confianza, o si han sido sus implementaciones (instalaciones, productos) o procedimientos (Autoridades de Certificación) los que han invocado al desastre. Y veremos también si hay que echarle la culpa al usuario y, si hay que hacerlo, en qué sentido, ya que vamos mal si después de todo hubiera que arremeter contra los clientes y razón de ser de todo este tinglado.

En esta conferencia se tratará, igualmente, si hay nuevos escenarios (M2M) en los que los viejos paradigmas PKI si puedan llegar a tener éxito por el mero hecho de haber eliminado el factor humano (*smartgrids*) y, si es posible, intentaremos asomarnos a lo nuevo que pueda estar por venir en criptología o en sus aplicaciones prácticas. Son muchas las preguntas pendientes, ¿Habrá un futuro sin Autoridades de Certificación? ¿Y si la criptograía de clave pública RSA se hunde? ¿Hay soluciones efectivas ante la ingeniería social en general y en las Infraestructuras Críticas en particular? ¿Qué efectos tendría la alteración/falsificación de sellos de tiempo? ¿Es realmente segura la criptografía si se hace en máquinas virtuales? Con la limitación del tiempo disponible, intentaremos revisar someramente qué es esto de la Confianza Digital y si hay razones para seguir confiando en ella.

Ponente:

Jorge Dávila Muro es Criptólogo, Profesor Titular de la Facultad de Informática de la Universidad Politécnica de Madrid y Director de I+D+i de Encifra, compañía dedicada a la seguridad informática y al 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, además de colaborador habitual de SIC en la sección "En construcción", 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.

Securmática 2013

Cerca de 7.000 expertos han pasado por Securmática, un congreso que con sus 23 ediciones ya celebradas, es el foro de intercambio de experiencias en ciberseguridad por excelencia.

Premios SIC 2013 y Cena de la Seguridad

En coincidencia con la XXIV edición de Securmática, tendrá lugar el acto de entrega de los X 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 ciberseguridad, la seguridad de la información y la privacidad en nuestro país– cuyo estado de madurez y proyección ha alcanzado un punto crítico.

Los galardonados de la novena edición de los Premios SIC.

AFORO LIMITADO

Fechas y lugar de celebración

SECURMÁTICA 2013 tendrá lugar los días 23, 24 y 25 de abril de 2013 en el hotel NOVOTEL. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2013 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 X Premios SIC (24 de abril).
- Diploma de asistencia.

Cuota de inscripción

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

Cuota	Hasta el 31 de marzo	Después del 31 de marzo
1 Módulo	450 € + 21% IVA	550 € + 21% IVA
2 Módulos	750 € + 21% IVA	900 € + 21% IVA
3 Módulos	900 € + 21% IVA	1.100 € + 21% 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 25 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.
BANKIA
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 23 ☐ Módulo 2 Día 24 ☐ Módulo 3 Día 25 ☐ Deseo inscribirme a SECURMÁTICA 2013

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

Revista SIC

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**