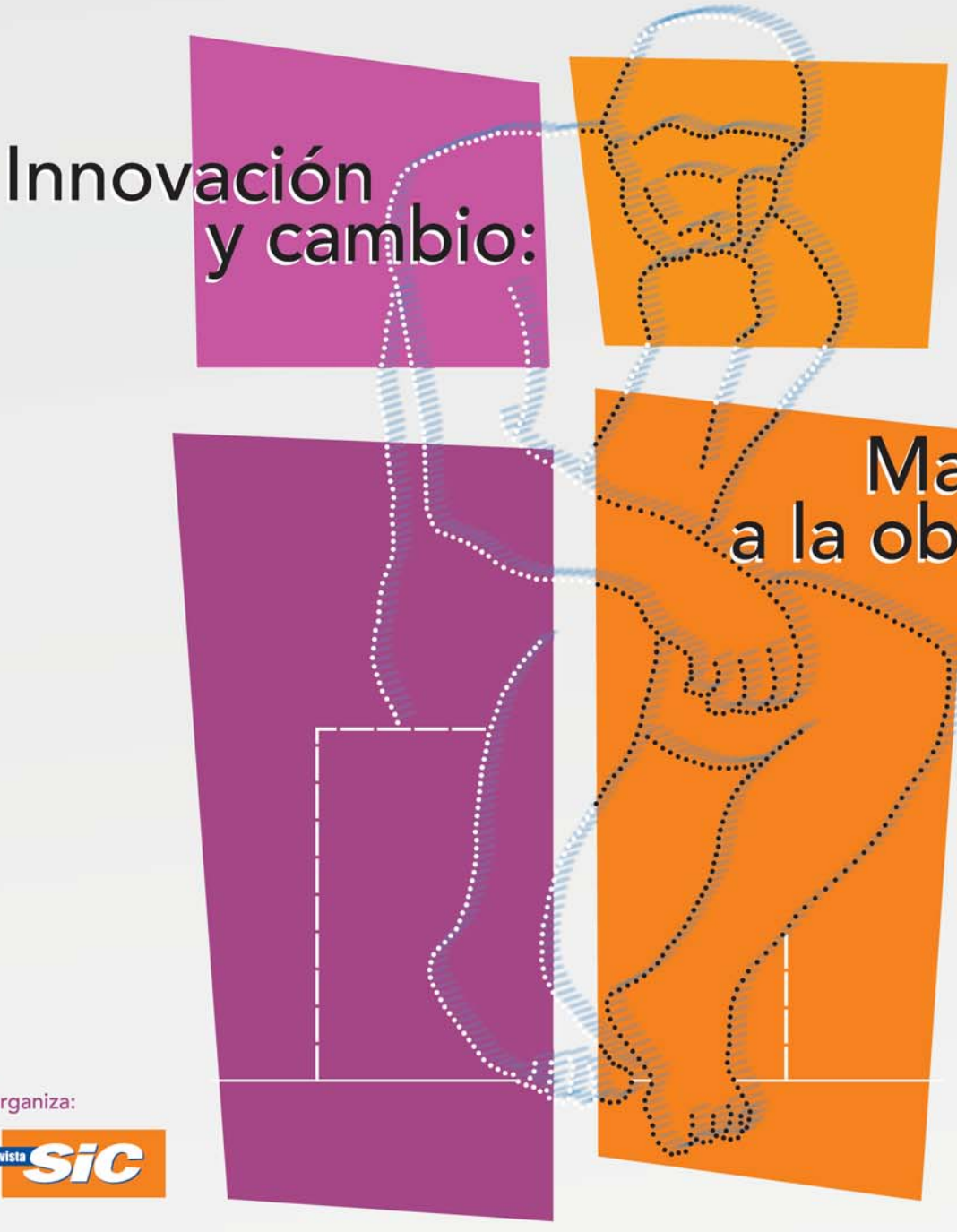
SECURMÁTICA

2015

XXVI Congreso global de ciberseguridad, seguridad de la información y privacidad

21.22.23 | abril



Organiza:

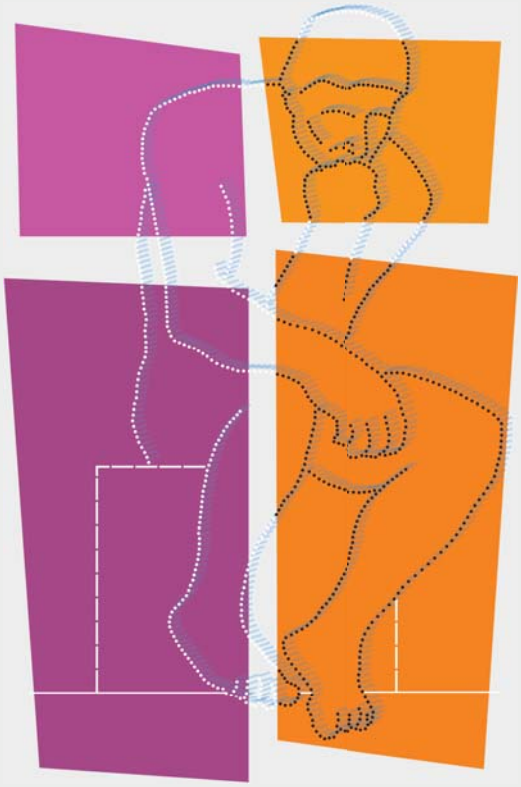
Revista SiC

PROGRAMA

Tendrá lugar los días 21, 22 y 23 de abril en su tradicional sede del Campo de las Naciones de Madrid

Securmática 2015: la ciberseguridad se mueve

No hay industria o actividad conocida que no se esté viendo afectada por la necesidad de gestionar su ciberseguridad. La progresión de la sociedad digital y el avance de las técnicas de ataque en contraposición a las dificultades de estabilizar en tiempos de mercado las de defensa, están provocando una exposición al riesgo multisectorial y global en la que se funden organizaciones supranacionales, estados, empresas y personas en una suerte de plasma legislativo, normativo y regulatorio todavía por construir y en el que se manifiestan diferencias notables dependiendo de en qué áreas del mundo se opere.



Por otra parte, los hechos conocidos demuestran que los objetivos de los atacantes son cada vez más ambiciosos, se manifiesten sus acciones en el terreno de la delincuencia o en los entornos del espionaje (estados, empresas, personas) y de las actividades terroristas.

Sea como fuere, las funciones de seguridad de la información, prevención de fraude y continuidad de negocio están pasando a un primer plano corporativo, porque se imbrican en el conjunto de responsabilidades nucleares de los consejos de administración y de los comités de dirección (máxime si se trata de empresas cotizadas), que han de demostrar ejemplaridad en el buen gobierno de sus sociedades y en el cumplimiento legal, y, por tanto, deberían estar también en disposición de invertir adecuadamente en la gestión de ciberriesgos de seguridad, como una de las piezas esenciales de sus planes de transformación a la economía digital. Y lo mismo reza para las administraciones públicas.

En su XXVI edición el Congreso sigue manteniendo su ideario de mostrar qué se está haciendo en ciberseguridad tanto en las empresas como en las administraciones. Para ello se ha confeccionado un programa para que los congresistas se hagan una idea del estado del arte en la materia, ya en lo que toca a las acciones que se derivan de las iniciativas vinculantes de las estructuras del Estado más directamente concernidas por la Ciberseguridad Nacional (**DSN**, **CCN**, **CNPIC**, **INCIBE**), ya en lo que toca a proyectos relevantes de seguridad TIC y continuidad de las administraciones (**AGE**, **Generalitat de Cataluña**, **Junta de Castilla y León**...), como del sector empresarial (**Abanca**, **Abertis**, **Bankinter**, **Banco Sabadell**, **BBVA**, **Caixabank**, **Ferrovial**, **Premap**, **ING Bank**, **Renfe**, **Sanitas**...).

Securmática 2015, por tanto, es la cita obligada para todos aquellos directivos y expertos en ciberseguridad, del sector privado y del sector público, que pretendan, por una parte estar informados de los avances del sector profesional, y por otra que quieran saber si sus compañías están alineadas con las tendencias en prevención, defensa y respuesta.

Organiza

Revista SIC

Nacida en el año 1992, SIC es la revista española especializada en gestión de seguridad de la información, ciberseguridad y privacidad. Perteneciente a Ediciones CODA, esta publicación organiza SECURMÁTICA, el acontecimiento profesional por excelencia en España de este pujante ramo de las TIC.

Copatrocinadores

Atos · Blueliv. · BT · Deloitte. · EQUIFAX · EY Building a better working world

gmv · hp · indra · Nextel S.A. Ingeniería y Consultoría · pwc · S2 GRUPO

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

PRIMER MÓDULO, 21 DE ABRIL

08:45h.	Entrega de documentación
09:15h.	Ceremonia de apertura
10:00h.	**Conferencia inaugural**
10:30h.	Ponencia: **Consejo Nacional de Ciberseguridad-CNCS: logros y retos.**
	Ponente: **Joaquín Castellón Moreno**, Director Operativo. Departamento de Seguridad Nacional. Presidencia del Gobierno.
11:00h.	Coloquio
11:10h.	Pausa-café
11:40h.	Ponencia: **Servicios de alerta ante ataques a la Ciberseguridad Nacional por robo de información a empresas y organismos.**
	Ponente: **Javier Candau Romero**, Jefe del Área de Ciberseguridad del Centro Criptológico Nacional, CCN. Centro Nacional de Inteligencia, CNI. Ministerio de la Presidencia.
12:10h.	Coloquio
12:20h.	Ponencia: **La gestión de la ciberseguridad en los Planes Estratégicos Sectoriales y en los Planes de Seguridad de operadores críticos ya designados.**
	Ponente: **Fernando Sánchez Gómez**, Director del Centro para la Protección de las Infraestructuras Críticas, CNPIC. Secretaría de Estado de Seguridad. Ministerio del Interior.
12:50h.	Coloquio
13:00h.	Ponencia: **El SOC de la AGE-Administración General del Estado.**
	Ponente: **Miguel Ángel Amutio Gómez**, Subdirector Adjunto en la S.G. de Coordinación de Unidades TIC de la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Hacienda y Administraciones Públicas.
13:30h.	Coloquio
13:40h.	Almuerzo
16:00h.	Ponencia: **APT: detección del compromiso.**
	Ponentes:
	Javier Candau Romero, Jefe del Área de Ciberseguridad del Centro Criptológico Nacional, CCN. Centro Nacional de Inteligencia. CNI.
	Antonio Villalón Huerta, Director de Seguridad de S2 Grupo.
16:30h.	Coloquio
16:40h.	Ponencia: **Gobierno y gestión de la ciberseguridad desde una perspectiva de negocio: la Administración Pública de Cataluña.**
	Ponentes:
	Xavier Gatius Garriga, Director General del CESICAT.
	Jesús Romero Bartolomé, Socio de Riesgos Tecnológicos. PwC.
17:10h.	Coloquio
17:20h.	Ponencia: **Modelo de Servicios Avanzados de Seguridad de la Red de la Junta de Castilla y León.**
	Ponentes:
	Luis Miguel Navas Santos, Jefe de la Sección de Servicios de Internet y Seguridad del Servicio de Red Corporativa de la Consejería de Hacienda. Junta de Comunidades de Castilla y León.
	Óscar Riaño de Antonio, Jefe de Área de Consultoría Zona Norte de GMV.
17:50h.	Coloquio
18:00h.	Fin de la primera jornada

Acto inaugural

Consejo Nacional de Ciberseguridad-CNCS: logros y retos

Sinopsis: En este último año la Ciberseguridad Nacional ha avanzado de manera notoria. La puesta en marcha de los elementos estructurales de la Ciberseguridad Nacional, entre ellos, el Consejo de Ciberseguridad han emprendido una labor sin precedentes en la mejora de la coordinación, la cooperación y la colaboración entre Administraciones Públicas y el sector privado, así como en la eficacia de las actuaciones que hoy se acometen en este ámbito. Entre sus logros, sin duda uno de más relevantes ha sido la elaboración del Plan Nacional de Ciberseguridad, aprobado el 31 de octubre de 2014 por el Consejo de Seguridad Nacional. En este Plan se destaca la asignación de responsabilidades para alcanzar los objetivos fijados por la Estrategia de Ciberseguridad Nacional, asignando cometidos específicos a los órganos y organismos representados en el Consejo de Ciberseguridad Nacional. Su contenido se instrumenta a través de la creación de siete Planes Derivados, que se están elaborando en la actualidad y que supondrán la aplicación práctica de las medidas recogidas en las líneas de acción de la Estrategia. Este es el punto de partida para el desarrollo de actuaciones concretas en un ámbito definido como prioritario para la Seguridad Nacional. Entre estas actuaciones, caben destacar como de especial relevancia la mejora en la coordinación en la gestión ante situaciones de crisis y la construcción de una fuerte "Cultura de ciberseguridad" que cree conciencia en la sociedad actual. En cuanto al primer aspecto se refiere, el apoyo a la gestión ante una situación de crisis de cualquier tipo y, en especial aquellas situaciones que puedan utilizar como medio o fin el ciberespacio y el uso de las tecnologías dada su transversalidad, cuenta con instrumentos para facilitar la coordinación operativa entre los órganos y autoridades competentes: el Consejo, el Comité de Situación y el Centro Nacional de Situación del DSN; pero aún es necesaria la construcción, desarrollo y mejora de los mecanismos y herramientas de apoyo a esta gestión que son proyectos que nos quedan por acometer. En lo concerniente a la cultura de ciberseguridad, es vital concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad, del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información. En este sentido, el Departamento de Seguridad Nacional tiene el fuerte compromiso de crear una permeable Cultura de Ciberseguridad que es, sin duda, la piedra angular para facilitar el éxito del uso seguro del ciberespacio. Las oportunidades para seguir avanzando en el camino emprendido son numerosas. Hoy en día ya contamos con instrumentos para cumplir mejor con las responsabilidades que plantea el gran reto de la ciberseguridad y, sin duda, estamos en el buen camino.

Ponente:

Joaquín Castellón Moreno, Capitán de Fragata. 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 portaaviones "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.

Servicios de alerta ante ataques a la Ciberseguridad Nacional por robo de información a empresas y organismos

Sinopsis: Durante 2014 se han publicado más de 100 informes relacionados con APTs (www.github.cm//kbandia/APTnotes) demostrando la virulencia y complejidad de estos ataques, que necesitan de una aproximación diferente para su detección y erradicación. Por ello es fundamental el intercambio de información utilizable de forma inmediata y automática de estas amenazas en las que se especifiquen las acciones urgentes a realizar para su identificación y eliminación. Por otro lado resulta esencial que por parte de las empresas y organismos receptores la colaboración sea ejemplar, proporcionando información sobre evidencias en la detección, muestras identificadas e impacto recibido para que se pueda valorar el coste para España de este tipo de ataques. Los casos recientes de *Desert Falcons* o *Equation Group*, así como las nuevas funcionalidades identificadas en *Snake / Uroburos* nos hacen ver que el ataque puede venir de cualquier origen, que la complejidad técnica puede superar en su engaño a cualquier defensa y que tenemos que analizar de forma permanente el tráfico de entrada y salida de la organización con herramientas que puedan de forma automática incorporar la información remitida por los organismos responsables de contrainteligencia. Por otro lado se considera fundamental disponer de equipos diseñados y con el conocimiento suficiente para detectar cualquier anomalía en nuestro perfil de tráfico que pueda derivarse en la evidencia de una infección, movimiento lateral dentro de la organización o posible salida de información de valor de la misma. Los Centros de Operaciones de Seguridad y el intercambio de información ya no son una opción deseable y sí una necesidad imperiosa.

Ponente:

Javier Candau Romero es el Jefe del Área de Ciberseguridad del Centro Criptológico Nacional y 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 quince años de experiencia en todas estas actividades.

La gestión de la ciberseguridad en los Planes Estratégicos Sectoriales y en los Planes de Seguridad de operadores críticos ya designados

Sinopsis: En el proceso de implantación del Sistema de Protección de Infraestructuras Críticas, se aprobaron el pasado 30 de junio de 2014 los **Planes Estratégicos Sectoriales** de la Energía (electricidad, gas, petróleo), Industria Nuclear y Sistema Financiero, designándose 37 operadores críticos e identificándose en torno a unas 146 infraestructuras críticas. Los operadores críticos han presentados sus Planes de Seguridad del Operador y una vez aprobados los mismos deberán realizar sus **Planes de Protección de Específicos** por cada una de sus infraestructuras críticas identificadas. Para junio del 2015 se aprobaran los Planes Estratégicos Sectoriales del Transporte (aéreo, ferroviario, marítimo, carretera) y Agua. La **gestión de la ciberseguridad** se está realizando dentro del marco de referencia de las Estrategias de Seguridad y Ciberseguridad Nacionales aprobadas en el 2013, diseñando y promoviendo acciones dirigidas a los operadores de infraestructuras críticas que garanticen el uso seguro de las redes y los sistemas de información mediante el fortalecimiento de las capacidades de prevención, detección y respuesta ante ciberincidentes. En este sentido, para **hacer frente a los diferentes riesgos y amenazas que afectan al ciberespacio** (terrorismo, crimen organizado, espionaje, *hacktivismo*, etc.), se hace necesario el potenciar las capacidades del Estado relativas a la prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación. La **ciberseguridad** es hoy uno de los **principales ejes de acción del Ministerio del Interior**. Por ello, se han fortalecido los mecanismos y estructuras dedicados a este tema: creación del **CERT de Seguridad e Industria**, creación de la **Oficina de Coordinación Cibernética (OCC)** y fortalecimiento de las capacidades humanas y tecnológicas de las **Unidades de las Fuerzas y Cuerpos de Seguridad del Estado dedicadas al ciberterrorismo y a la ciberdelincuencia.**

Ponente:

Fernando J. Sánchez Gómez es Director del Centro Nacional para la Protección de las Infraestructuras Críticas, dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior. Es Teniente Coronel de la Guardia Civil, Diplomado de Estado Mayor. Ha realizado numerosos cursos oficiales de la Guardia Civil y otras instituciones, participando en varias misiones internacionales con la UE y la ONU. Está en posesión de diversos Másteres y Cursos Superiores y tiene reconocido el título de Director de Seguridad. Cuenta con diferentes condecoraciones. Habla cuatro idiomas: inglés, francés, italiano y portugués. Cuenta con más de 25 años de experiencia profesional en el campo de la seguridad. Previamente a su cargo actual desarrolló durante varios años sus funciones en el Estado Mayor de la Dirección General de la Guardia Civil. Más recientemente, ha dirigido el equipo de trabajo encargado de elaborar la normativa española sobre protección de infraestructuras críticas, (Ley 8/2011, Real Decreto 704/2011 y sus planes derivados), y ha formado parte del grupo de redacción del borrador de la Estrategia Nacional de Ciberseguridad, aprobada en diciembre de 2013. De la misma manera, ha participado en representación española en las discusiones en el seno de la Comisión Europea para la redacción de la Directiva 114/2008 sobre protección de las infraestructuras críticas europeas. Forma parte de la Comisión Nacional para la Protección de las Infraestructuras Críticas, es el Punto de Contacto del Estado Español con la UE en materia de protección de infraestructuras críticas y participa habitualmente en diversos grupos de trabajo, nacionales e internacionales, en dicho campo. Es coautor de los libros *"Marco Legal y de Gestión de la Protección de las Infraestructuras Críticas en España"* (2013) y *"Seguridad nacional, amenazas y respuestas"* (2014). Asimismo, es autor de diferentes publicaciones y artículos relacionados con el campo de su dominio. Colabora asiduamente en la impartición de diferentes cursos y másteres relacionados con defensa y seguridad, organizados por universidades e institutos universitarios y participa frecuentemente en conferencias y jornadas, tanto nacionales como internacionales.

El SOC de la AGE-Administración General del Estado

Sinopsis: En el contexto configurado por las medidas CORA relativas a la mejora de la eficiencia de las AA.PP., la consolidación de las comunicaciones del Sector Público Administrativo Estatal, lo previsto en la Estrategia de Ciberseguridad Nacional sobre la seguridad de los sistemas de información y telecomunicaciones que soportan las AA.PP., la plena implantación del Esquema Nacional de Seguridad y la prestación de Servicios Comunes por la DTIC, se contempla la prestación de servicios centralizados de seguridad gestionada materializados en un Centro de Operaciones de Seguridad. Dicho Centro de Operaciones de Seguridad que tiene por finalidad prestar servicio, en principio, a las entidades del citado Sector Público Estatal, constituye una oportunidad para aumentar de forma notable el nivel de seguridad de los sistemas de información y comunicaciones del conjunto, en condiciones de mejor eficacia y eficiencia, a la vez que se reduce el esfuerzo individual de las entidades integradas en el mismo. Por delante hay tareas relativas al diseño de la arquitectura, implantación, configuración, puesta en marcha, gestión y operación de este Centro de Operaciones de Seguridad.

Ponente:

Miguel A. Amutio Gómez es Subdirector Adjunto en la S.G. de Coordinación de Unidades TIC de la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Hacienda y Administraciones Públicas. Licenciado en Informática por la Universidad de Deusto (1988), CISA, CISM y CRISC, es coordinador de la elaboración y desarrollo del Esquema Nacional de Seguridad (Real Decreto 3/2010) y del Esquema Nacional de Interoperabilidad (Real Decreto 4/2010), así como del desarrollo de las Normas Técnicas de Interoperabilidad previstas en la disposición adicional primera del Real Decreto 4/2010, junto con su documentación complementaria. Es miembro de la delegación española en el comité gestor y grupos de trabajo del Programa ISA (desde 2010) y, anteriormente, de los programas IDA II (1999-2004) e IDABC (2005-2009)

de la Unión Europea, y coordinador nacional de la red transeuropea TESTA; así como miembro de *European Multi-Stakeholer Platform for ICT Standardization* de la Comisión Europea. Es miembro del grupo de seguridad y privacidad en la economía digital de la OCDE (WPSPDE), del Comité gestor del Arreglo de reconocimiento mutuo de los certificados de seguridad de TI (CCRA) y Presidente del órgano técnico de normalización de AENOR AEN CTN.

APT: detección del compromiso

Sinopsis: El contenido de la ponencia mostrará un análisis práctico de las aproximaciones y capacidades operativas para la detección de compromisos por parte de amenazas avanzadas persistentes.

Ponentes:

Javier Candau Romero es el Jefe del Área de Ciberseguridad del Centro Criptológico Nacional y 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 quince años de experiencia en todas estas actividades.

Antonio Villalón Huerta, Director de Seguridad de S2 Grupo. Ingeniero en Informática por la Universidad Politécnica de Valencia, es Director de Seguridad por la Universidad de Valencia habilitado por el Ministerio del Interior y auditor CISA. Desde 2003 es Director de Seguridad de S2 Grupo, donde dirige los servicios y proyectos de ciberseguridad con componente técnica. Anteriormente ejerció de consultor de seguridad en otras empresas del sector TIC, además de como profesor en cursos de postgrado de la Universidad Politécnica de Valencia en diferentes ámbitos relacionados con entornos Unix.

Gobierno y gestión de la ciberseguridad desde una perspectiva de negocio: la Administración Pública de Cataluña

Sinopsis: El Centro de Seguridad de la Información de Cataluña (CESICAT) es la entidad designada por el Gobierno de la Generalitat de Cataluña para garantizar una Sociedad de la Información segura para administraciones, instituciones y ciudadanía en Cataluña, con especial atención a la ciberseguridad del propio gobierno de la Generalitat y de sus activos TIC. En la ponencia se presentará la estrategia y orientación del CESICAT en los últimos años, analizando la trayectoria y evolución de su función obtenida por medio de una revisión profunda del diseño y la ejecución de sus principales servicios (SOC, Gobierno de la seguridad, Gestión de la identidad digital, Cumplimiento normativo, etc.) con una clara orientación a negocio. Para ello, a lo largo de la ponencia se estudiará el proceso seguido para la construcción del actual CESICAT como entidad de servicios de Ciberseguridad, incluyendo el establecimiento de sus objetivos estratégicos, la definición de sus procesos de negocio, el despliegue y la puesta en marcha de un Modelo Estándar de Seguridad en los distintos ámbitos departamentales, y la construcción del catálogo de servicios dirigido a la Administración Pública de Cataluña. Por último, la ponencia también recogerá los retos que tiene el CESICAT para el futuro próximo, así como la perspectiva y estrategia utilizadas para afrontarlos.

Ponentes:

Xavier Gatius Garriga es Director General del Centro de Seguridad de la Información de Cataluña (CESICAT). Ingeniero en Informática de Gestión por la Universidad de Girona, Certificado en ITIL v3 Foundations por Exin y PDD por IESE Business School Universidad de Navarra, fue con anterioridad gerente y director de la división de desarrollo de soluciones en la multinacional SII Group Concatel de 2007 a 2013, director técnico del proyecto Clasificados.es en Grupo Godó de 2006 a 2007 y director de sistemas del diario electrónico Vilaweb de 1999 a 2005, entre otros. Asesor externo de estrategia en operaciones y sistemas de información en el consejo de administración de Nadico Industrial Management de 2006 a 2012 y profesor asociado de la Business Engineering School La Salle en la asignatura de Dirección de operaciones del Executive MBA y del posgrado de Marketing digital hasta el 2013. Desde enero de 2014 es miembro del Consejo Asesor de la Agencia de Calidad y Evaluación Sanitaria de la Generalitat de Cataluña.

Jesús Romero Bartolomé. Socio de Riesgos Tecnológicos en PwC, firma a la que se incorporó en 2011. Ingeniero Superior de Telecomunicación, MBA y CISM, 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. Ponente y articulista habitual en materia de Seguridad TIC, Romero es profesor del máster universitario de Seguridad de la Universidad Europea, así como miembro de la Comisión de Seguridad de AMETIC y del capítulo de Madrid de ISACA. Con anterioridad 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 Ametic. En 2012 fue galardonado con el Premio SIC en reconocimiento de su trayectoria profesional.

Modelo de Servicios Avanzados de Seguridad de la Red de la Junta de Castilla y León

Sinopsis: Las administraciones públicas, incluidas las autonómicas, no son ajenas a los Riesgos de Seguridad (o de Ciberseguridad) actuales. También son objetivo de intentos de explotación o afectados por amenazas generales. Y, ya sea por propio convencimiento, como por la existencia de requisitos legales, han trabajado en el despliegue de soluciones de detección, prevención y respuesta, que han de ser lo suficientemente dinámicas como para responder a la complejidad de las amenazas actuales. Pero, ¿qué ocurre cuándo las medidas implantadas no han sido capaces de detectar un compromiso o intento de explotación avanzado? ¿Tiene el equipo de gestión de incidentes suficiente información para desarrollar su trabajo de la forma más adecuada? En el presente proyecto se muestra la aproximación de seguridad implantada en la Junta de Castilla y León, la cual se encuentra centrada tanto en el despliegue de mecanismos de detección de amenazas y correlación de eventos de seguridad, como en la implantación de herramientas de apoyo a la investigación forense para el equipo especializado de gestión de incidentes de seguridad.

Ponentes:

Luis Miguel Navas Santos es Jefe de la Sección de Servicios de Internet y Seguridad del Servicio de Red Corporativa de la Dirección General de Atención al Ciudadano, Calidad y Modernización de la Consejería de Hacienda de la Junta de Castilla y León. Ingeniero de Telecomunicaciones y Graduado en Empresariales por la Universidad de Valladolid y funcionario de carrera de la Junta de Castilla y León adscrito al Cuerpo de Ingenieros Superiores (Telecomunicaciones). En el sector privado desarrolló e integró aplicaciones basadas en mensajería móvil para operadores de telecomunicaciones nacionales e internacionales. Tras su entrada en el sector público dirige servicios críticos de infraestructura de Internet de la Comunidad Autónoma de Castilla y León, así como es responsable de la seguridad perimetral y de red del Servicio de Red Corporativa.

Oscar Riaño de Antonio es Jefe de Área de Consultoría Zona Norte de GMV. Ingeniero Informático por la UVA. Oscar Riaño inicia su carrera profesional en GMV en 2005 pasando en el año 2007 a dirigir el Área de Consultoría de la zona norte de GMV centrándose en la dirección de proyectos relacionados con la implantación y operación de centros de operaciones de seguridad y sistemas de gestión. Miembro de ISACA, posee las certificaciones CISA, CISM y Lead Auditor 25999. A lo largo de su trayectoria en GMV ha adquirido una amplia experiencia en áreas de trabajo relacionadas con la seguridad lógica, auditorías de seguridad, normativas de cumplimiento y gestión de incidentes de seguridad.

SEGUNDO MÓDULO, 22 DE ABRIL

09:00h. Entrega de documentación
09:30h. Ponencia: **Construyendo un programa de prevención de fraude *online* – El punto de vista de Abanca.**
Ponentes:
Roberto Baratta Martínez, Director de Gestión de Prevención de Pérdida, Continuidad de Negocio y Seguridad de Abanca.
David Navarro González, Responsable de Ventas de Trusteer para SPGI en IBM Security.
10:00h. Coloquio
10:10h. Ponencia: **Equifax: marco de gestión y gobierno global de la seguridad de la información.**
Ponentes:
Eduardo García Martínez, CISO. Equifax.
Ofelia Alfonso, Directora de Marketing. Equifax.
10:40h. Coloquio.
10:50h. Ponencia: **La aportación del sector financiero a la homogeneización de las regulaciones en los nuevos negocios digitales.**
Ponentes:
Borja Larrumbide Martínez, Responsable de la Normativa de Seguridad Global y del Departamento de IT Risk Institutional Affairs. Grupo BBVA.
Juan Manuel Matalobos Veiga, Responsable de IT Risk Compliance. Grupo BBVA.
11:20h. Coloquio
11:30h. Pausa-café
12:10h. Ponencia: **Simulación continua de ciberataques.**
Ponentes:
Jordi André Vallverdú, Responsable del Área de Ciberseguridad. Seguridad de la Información. Caixabank.
Julio San José Sanchez, Socio de EY.
12:40h. Coloquio
12:50h. Ponencia: **ING BANK NV España: Proyecto Kangaroo.**
Ponentes:
Miguel Ángel Sánchez Barroso, Information Security Officer / Data Protection Officer. ING BANK NV, Suc. en España.
Alejandro Ramos Fraile, IT Security Manager. ING BANK NV, Sucursal en España.
13:20h. Coloquio
13:30h. Ponencia: **Innovación y seguridad en Bankinter: tarjeta financiera de débito y crédito por software para movilidad. Pagos HCE.**
Ponentes:
Alberto Pérez-Lafuente, Director de Estrategia y Gestión de la Innovación. Bankinter.
Fernando Vega Viejo, Director de Seguridad de la Información. Gneis-Grupo Bankinter.
14:00h. Coloquio
14:10h. Almuerzo
16:15h. Ponencia: **Prevención de amenazas: cómo ser más persistente que una APT.**
Ponentes:
Antonio Cerezo Hormeño. Arquitecto de Seguridad de Sanitas.
Daniel Martínez Ponce, Experto en Seguridad de Red. Dirección de Ciberseguridad. Indra.
16:45h. Coloquio
16:55h. Ponencia: **Gestión integral de la seguridad en tiempo real: la obsolescencia del "divide y vencerás".**
Ponentes:
Narciso Mazas González, Coordinador. Área de Ergonomía y Psicosociología Aplicada Regional Norte de PREMAP Seguridad y Salud.
Agustín Moyano Díaz, Product Manager, Departamento de Consultoría. Nextel, S.A.
17.25h. Coloquio
17:35h. Fin del segundo módulo
19:30h. **Cena de la Ciberseguridad y entrega de los XII Premios SIC**

Construyendo un programa de prevención de fraude *online* - El punto de vista de Abanca

Sinopsis: Los canales *online* se han convertido en un potente componente de las nuevas estrategias de ventas y servicios de las entidades financieras. Al mismo tiempo, pueden introducir significantes riesgos de seguridad, operacionales y de reputación. ¿Cómo los bancos pueden lograr la difícil misión de promover y desarrollar canales personalizados y ágiles, protegiendo tanto al banco como a los clientes frente al fraude? Por otro lado las nuevas regulaciones van poniendo el acento en la protección del consumidor en los canales *online* y cambian las necesidades de las entidades financieras a la hora de desarrollar sus estrategias antifraude manteniendo la usabilidad del canal al tiempo que protegen al cliente y cumplen con las normativas. En esta ponencia se mostrará cómo presentar las iniciativas de seguridad al negocio, involucrar a los responsables del mismo, y alinear la tecnología con los procesos –y no al revés– para prevenir el fraude al mismo tiempo que convertir la prevención del fraude en un habilitador del negocio.

Ponentes:

Roberto Baratta Martínez es Director de Gestión de Prevención de Pérdida, Continuidad de Negocio y Seguridad de Abanca. En dependencia directa de la Dirección General de Control Corporativo y Riesgos está al frente de las competencias de Gestion de Pérdida y Fraude, Seguridad Física, Seguridad TI, Continuidad de Negocio, Depositaria y Gestión de Efectivo. Con más de once años de experiencia en gestión de la seguridad y riesgos de la información en entidades financieras, con anterioridad ha sido Gerente de Seguridad TI y CISO en Novagalicia Banco, y ha desempeñado las funciones de IT Security Officer y Director de Operación de Seguridad en Caixanova. Ha sido profesor en la Universidad de Vigo y la Escuela Gallega de Administraciones Públicas en materias relacionadas con seguridad y riesgos y es ponente habitual en temas de seguridad y tecnología, además de disponer de las más relevantes certificaciones de seguridad.

David Navarro Gonzaléz es Responsable de Ventas de Trusteer para SPGI (España, Portugal, Grecia e Israel) en IBM Security. Con más de 17 años de experiencia en el sector de las TI, ha desarrollado los últimos 6 años en el área de seguridad, siendo desde hace un año el responsable para España, Portugal, Grecia e Israel de Trusteer, compañía dedicada a los servicios de antifraude en el canal *online*, adquirida por IBM y encuadrada desde entonces en la división de seguridad de este fabricante. Con anterioridad, Navarro ha desarrollado su carrera profesional en RSA, la división de seguridad de EMC como Responsable de Ventas en Servicios Financieros en la propia EMC, BMC Software y Alma.

Equifax: marco de gestión y gobierno global de la seguridad de la información

Sinopsis: Equifax ha creado un Marco de Gestión y Gobierno Global de la Seguridad de la Información en una empresa con 5000 empleados presente en 15 países (USA, Latam, Europa y Asia) con grandes diferencias en infraestructuras, legislaciones, cultura y zonas horarias. Su modelo de gobierno y gestión le ha permitido alcanzar un alto nivel de madurez en los procesos de la Seguridad de la Información, y como prueba de ello ha obtenido la certificación ISO-27001 con un alcance muy amplio tanto lógico como físico, para todas las geografías y oficinas, siendo la única empresa del sector de la gestión de *bureaus* de crédito que dispone de esta certificación de seguridad completa en la actualidad. Su ponencia versará sobre la estructura y modelo de gestión y los *"do and dont's"*, mejores prácticas o recomendaciones que pueden servir como guía a otras empresas en una situación similar o para aquellas que están en una situación de crecimiento o de despliegue en el extranjero, etc.

Ponentes:

Eduardo García Martínez. Director Senior de Seguridad de la Información con más de trece años de experiencia en el sector. Máster de Grado en Administración de Empresas y TIC en la Universidad de Alcalá, y Máster en Dirección de Tecnologías de la Información en IDE-CESEM Business School, ha llevado a cabo proyectos internacionales con equipos de trabajo multiculturales en diversas compañías multinacionales como Tata Consultancy Services, Atos, HP o Capgemini hasta recalar en Equifax, donde actualmente ejerce como CISO para España y Portugal. Posee las certificaciones ISACA CISA, CISM, CGEIT y CRISC.

Ofelia Alfonso es Directora de Marketing de Equifax para España y Portugal. Tiene una amplia experiencia en entornos de negocio y TI. Ingeniera Industrial por la Universidad Pontificia de Comillas (ICAI), Executive Master of Business Administration (MBA) de Leadership Development en Harvard Business School, ha desarrollado gran parte de su carrera profesional en la multinacional HP.

La aportación del sector financiero a la homogeneización de las regulaciones en los nuevos negocios digitales

Sinopsis: En el ámbito financiero, las compañías europeas están afrontando el reto de la evolución y la competencia en un mundo digital global. Las necesidades de los nuevos modelos de negocio, en dicho entorno, han de ser cada vez más disruptivas para adaptarse a las expectativas y comportamientos de los clientes, así como para la reducción de los costes, del *time to market* y de la complejidad, a la hora de ofertar los nuevos modelos del negocio digital. Las diferencias regulatorias en países dentro de Europa, así como entre estos y otros, como por ejemplo, Estados Unidos, han producido grandes desniveles competitivos en el mundo digital, lo que ha propiciado la aparición de empresas como Google, Facebook, Amazon o Twitter, muy centradas en el modelo de negocio del Perfilado del Usuario. Estos desniveles, entre empresas ya existentes y las de nueva creación, están suponiendo grandes retos para la Innovación y la Libre Competencia, en un mercado cada día más global, donde el consumidor, por su libertad universal de utilización de cualquier servicio, somete a la empresa y a sí mismo a complicados dilemas en lo referente a los Derechos de Privacidad y de Protección de Datos. BBVA IT Risk Fraud and Security ha creado, recientemente, un nuevo departamento, con el objetivo de transmitir a los distintos reguladores sus inquietudes y recomendaciones, desde el punto de vista de Riesgo Tecnológico, a fin de homogenizar las regulaciones, tanto en el ámbito nacional como en el internacional.

Ponentes:

Borja Larrumbide Martínez es Responsable de la Normativa de Seguridad Global y del Departamento de IT Risk Institutional Affairs. Grupo BBVA. Licenciado en Ciencias Informáticas por la Universidad de Boston, tiene una experiencia de veintiún años en IT, invertidos en diversos sectores de la industria IT. Durante diez años, en Microsoft, responsable del Dpto. de Soporte Premier, Arquitecto y Jefe de Proyecto de Soluciones de Infraestructura y Desarrollo para clientes. Actuó asimismo como Consultor Estratégico para Movistar y el Ministerio de Defensa español. En BBVA fue responsable del diseño, liderando al mismo tiempo los departamentos de Arquitectura de Datos, Servicios y Procesos y del departamento de Soluciones Ágiles, siendo responsable técnico de la transformación IT del área global de Riesgos. Gestionó la Oficina de Proyectos de Holding y en Seguridad ha sido el CISO de los Servicios Centrales y de la Banca Digital y responsable IT de la Seguridad Física, puesto que aún desempeña. Actualmente es responsable de la Normativa de Seguridad Global y del recientemente creado, Dpto. de IT Risk Institutional Affairs.

Juan Manuel Matalobos Veiga es Responsable de IT Risk Compliance en el Grupo BBVA. Previamente a su incorporación, trabajo durante más de 12 años en algunas de las principales empresas internacionales de auditoría y consultoría, siempre dentro del ámbito de la Gestión del Riesgo Tecnológico. Durante este tiempo, dirigió y ejecutó proyectos de ámbito nacional e internacional para numerosas empresas de diversos sectores, con un foco especial en el Sector Financiero. Matalobos es Licenciado en Informática por la Universidad Politécnica de Madrid y dispone de las certificaciones CISA, CISM, CRISC, CISSP y AMBCI.

Simulación continua de ciberataques

Sinopsis: La evolución de las amenazas sobre los activos de las organizaciones es tan rápida que las capacidades defensivas de las organizaciones deben estar permanentemente actualizadas y entrenadas. La protección requiere desde un excelente comportamiento frente a ataques dirigidos hasta un seguimiento impecable de procedimientos de seguridad, pasando por resiliencia ante eventuales indisponibilidades de personal clave dentro del equipo de seguridad. CaixaBank, buscando exceder la excelencia de su función de seguridad, ha elegido el servicio de Simulación Continua de Ciberataques (SCC), proporcionado por EY, que permite ejercitar de una forma continua sus capacidades de defensa con respuestas ante escenarios y amenazas no preavisados, ya que el SCC es en estos momentos el único servicio diseñado para evidenciar, constantemente, aspectos de mejora sobre servicios defensivos muy maduros.

Ponentes:

Jordi André Vallverdú es ingeniero superior en Telecomunicaciones especializado en la Seguridad de la Información con más de 15 años de experiencia en este campo. Es el responsable del área de ciberseguridad dentro del equipo de seguridad de la información de Caixabank. Este equipo se encarga del estudio de técnicas innovadoras aplicables a la seguridad de la información, la monitorización continua de la seguridad en los activos de la entidad y las revisiones técnicas que hacen posible la seguridad de sus clientes. Dentro de este ámbito cabe destacar la creación y gestión del Cyber SOC encargado de aplicar la inteligencia en los controles de seguridad desplegados en sus sistemas para combatir los diferentes vectores de ciberataque.

Julio San José Sánchez es Socio de EY en la aplicación de la práctica de gestión de riesgos tecnológicos al sector financiero. Tiene una trayectoria profesional de más de 25 años dedicado a distintas disciplinas de la seguridad de la información en el negocio y las actividades bancarias. Cuenta con el título de Director de Seguridad Privada, y con las certificaciones CISM/CRISC por ISACA, y BS 7799, BS 25999 por BSI. Miembro del Subcomité de Seguridad de las TI (CTN 71/SC27) –ha 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. Asimismo es coautor del libro *"Seguridad de las tecnologías de la información. La construcción de la confianza para una sociedad conectada"*, editado por Aenor.

ING BANK NV España: Proyecto Kangaroo

Sinopsis: En la conferencia se expondrá el proyecto de definición e implantación del marco de control en los accesos de personal de IT a sistemas críticos de ING BANK NV España mediante el uso de autenticación fuerte y monitorización avanzada.

Ponentes:

Miguel Ángel Sánchez Barroso es Information Security Officer / Data Protection Officer en ING BANK NV, Sucursal en España. Licenciado en Psicología por la Univ. Complutense de Madrid; Máster en Ingeniería de Software por la Univ. Politécnica de Madrid; Auditor Certificado de Sistemas de Información (CISA) y posee las certificaciones de Seguridad CISSP y CRISC. Actualmente es Responsable de Gestión del Riesgo Tecnológico y de Seguridad de la Información de ING Bank en España, donde ha adquirido una importante experiencia en la prevención del fraude online y en la gestión de la seguridad en procesos externalizados en régimen de *outsourcing*. Desde enero de 2014 Miguel Ángel es además Data Protection Officer del banco en España y Portugal.

Alejandro Ramos Fraile es Responsable del departamento de IT Security de ING BANK NV, Sucursal en España, Profesor colaborador en el Máster de Seguridad de la Universidad Europea de Madrid, posee las certificaciones CISSP, CISA, CEH y CHFI. Actualmente es uno de los editores del blog de divulgación de seguridad informática SecurityByDefault.com y autor del libro Hacker Épico.

Innovación y seguridad en Bankinter: tarjeta financiera de débito y crédito por software para movilidad. Pagos HCE

Sinopsis: Esta ponencia abordará el enfoque de Bankinter en lo que toca a la seguridad en las nuevas aplicaciones móviles, y sobre la necesidad creciente de estas de disponer de mecanismos de autoprotección. En concreto la exposición girará en torno a la solución Tarjetas Virtual Móvil de Bankinter para pagos HCE.

Ponentes:

Alberto Pérez-Lafuente es Director de Estrategia y Gestión de Innovación en Bankinter. Ingeniero superior de telecomunicaciones por la Universidad Politécnica de Madrid, cuenta con 15 años de experiencia en comunicaciones móviles, inicialmente en operadores de telefonía móvil y posteriormente en el sector de la tarjeta inteligente con microprocesador. Igualmente dispone de 7 años de experiencia

en innovación aplicada a nuevos *drivers* de negocio. Experto en pagos móviles, convergencia e Internet de las cosas, tiene amplia experiencia en organismos de estandarización de las comunicaciones. Autor de varias patentes y solicitudes de patente.

Fernando Vega Viejo es Director de Seguridad de la Información en GNEIS - Grupo Bankinter desde octubre de 2014. Ha desarrollado toda su carrera profesional desde 1995 en el campo de seguridad de la información, tanto con el rol de consultor y proveedor, como de responsable de Seguridad. Antes de su incorporación al Grupo Bankinter estuvo en PwC, McAfee, Doc on Time, SIA y Grupo Telefónica. Posee las certificaciones de seguridad CISA, CISSP, CISM y Auditor 17799, así como el título de Director de Seguridad homologado por el Ministerio del Interior.

Prevención de amenazas: cómo ser más persistente que una APT

Sinopsis: Las amenazas persistentes avanzadas (APT) se han convertido en la gran preocupación de seguridad para las empresas, y son uno de los peligros más importantes y de más rápido crecimiento que las organizaciones deben afrontar hoy en día. Los vectores de ataque usados por las APT no son diferentes de los empleados en otros tipos de ataque, pero su principal diferencia radica en la perseverancia y recursos de los atacantes, y en que va mutando sus características de manera intencional y continua, haciéndolo muy difícil de detectar con métodos tradicionales. En Sanitas se ha optado por una estrategia de protección más proactiva, donde la protección a nivel del puesto de trabajo se complementa con el análisis en "sandboxing" en la conexión a Internet. De este modo no solamente se bloquea la interacción con el ciberdelincuente, sino también las amenazas cuando intentan actuar sobre los sistemas víctima.

Ponentes:

Antonio Cerezo Hormeño es Arquitecto de Seguridad de Sanitas y responsable del diseño, implantación y gestión de los proyectos de Gestión de Identidades, "Securización" de Infraestructuras (puestos de trabajo, red, accesos remotos, navegación y correo electrónico) y protección contra APTs, entre otros. Tiene más de trece años de experiencia en la compañía.

Daniel Martínez Ponce es Network Security Expert de la unidad de ciberseguridad de Indra. Experto en Seguridad de Redes y de Sistemas TIC con más de 16 años de experiencia en el sector. MCT de Microsoft e ingeniero certificado en ForeScout, FireEye, StormShield, StoneSoft, Aruba, Array, Bradford, Allot, Clearswift y otras tecnologías. Ha diseñado arquitecturas de Operadoras de WiFi y WiMax, en distintos países, y diseñado comunicaciones satélite seguras para el Ministerio de Defensa. Ha participado en numerosas iniciativas, proyectos y comunidades Open Source. Colaborador y ponente en diversos Masters y Conferencias de Comunicaciones y Seguridad.

Gestión integral de la seguridad en tiempo real: la obsolescencia del "divide y vencerás"

Sinopsis: Nextel, S.A. presenta una nueva forma de entender la Seguridad Integral de una empresa u organización, mediante la correlación, integración, coreografía y orquestación de sus sistemas de ciberseguridad, seguridad física y seguridad personal, ya que la fiabilidad de estos sistemas por separado no garantizan la seguridad integral. Para abordar este reto, se han desarrollado novedosas metodologías de gestión de la información, nuevas formas de modelado de patrones de riesgo, nuevas tecnologías de configuración y control remoto de dispositivos, y todo ello basado en una nueva cultura preventiva sustentada en el análisis de tendencias. Para dar soporte a todo esto, nace NextRisk como una plataforma tecnológica que será capaz de concentrar alrededor de la gestión del ciber-riesgo toda la información disponible en la organización, tales como sensores, aplicaciones, bases de datos, sistemas de producción, sistemas de seguridad, etc., para monitorizar, detectar y gestionar situaciones de riesgo, así como para poder ejecutar acciones preventivo-correctoras utilizando todos los elementos de ciberseguridad activa y pasiva disponibles, así como los dispositivos de información existentes (teléfonos, *smartphones*, tabletas, etc.), con la intención de mitigar o minimizar el impacto de una situación de la manera más rápida y efectiva.

Ponentes:

Narciso Mazas González. Coordinador del Área de Ergonomía y Psicosociología Aplicada de la Dirección regional de País Vasco y Navarra de PREMAP Seguridad y Salud. Ingeniero técnico industrial por la Escuela Universitaria de Ingeniería Técnica Industrial de Bilbao, cuenta con una experiencia de 16 años. Técnico Superior de Prevención de Riesgos Laborales y Máster Universitario en Gestión y Coordinación de Seguridad en Obras de Construcción, ha colaborado con la Escuela de Graduados Sociales, la Universidad del País Vasco, Colegio Oficial de Ingenieros Técnicos Industriales en sus cursos Máster y ha participado en diferentes congresos y foros. Cabe resaltar su participación en el proyecto FASyS-Fábrica Absolutamente Segura y Saludable, que busca establecer el modelo de excelencia en la gestión de la seguridad y la salud laboral en la industria de manipulación, mecanizado y montaje, así como una nueva generación de tecnologías y mecanismos de seguridad.

Agustín Moyano Díaz. Product Manager del departamento de Consultoría de Nextel, S.A. Ingeniero Informático con 13 años de experiencia en el sector IT, durante los cuales ha ido evolucionando a través del desarrollo, diseño, gestión y coordinación, hasta llegar a la dirección de proyectos de consultoría e implantación de sistemas de gestión en múltiples ámbitos. En los más de 7 años en Nextel, combina actividades de dirección técnica de proyectos de I+D+i con labores de consultoría y asesoría en soluciones avanzadas de seguridad integral y, además, es *product manager* de varias soluciones y plataformas tecnológicas, desarrolladas a partir de los resultados y las buenas prácticas obtenidas en múltiples proyectos de investigación.

TERCER MÓDULO, 23 DE ABRIL

09:00h.	Entrega de documentación
09:30h.	Ponencia: **Esquema Nacional de Ciberseguridad Industrial.**
	Ponente: **Miguel Rego Fernández**, Director General de INCIBE.
10:00h.	Coloquio
10:10h.	Ponencia: **Ferrovial: despliegue de la seguridad y el control en Data Center Virtuales.**
	Ponentes:
	Javier Rubio Sanz, Responsable de Gobierno de la Seguridad y Continuidad de Negocio. Ferrovial.
	Karen Gaines Cordero, Directora General de HP Security para Iberia.
10:40h.	Coloquio
10:50h.	Ponencia: **Renfe: Sistema de monitorización de APTs.**
	Ponentes:
	Francisco Lázaro Anguis, CISO de Renfe.
	Ramón Vicens Lillo, Vicepresidente de Threat Intelligence. Blueliv.
11:20h.	Coloquio
11:30h.	Pausa-café
12:10h.	Ponencia: **Accesos y cuentas privilegiados: un enfoque como programa corporativo.**
	Ponentes:
	David Carrascosa Bover, Responsable de gestión de identidades y control de accesos BSIS / Grupo Banco Sabadell.
	Javier Zapata Victori, Director Cybersecurity Big Data & Security. Atos Iberia.
12:40h.	Coloquio
12:50h.	Ponencia: **Cyber Security Response Team: equipo de alto rendimiento.**
	Ponentes:
	Carles Solé Pascual, Director de Seguridad de la Información. CaixaBank.
	Xavier Gracia Lacalle, Director CyberSOC Deloitte.
13:20h.	Coloquio
13:30h.	Ponencia: **Abertis: la movilidad como factor crítico para el desarrollo del negocio.**
	Ponentes:
	Manel Leal Sáez, Responsable de Seguridad Tecnológica. Abertis.
	José Francisco Pereiro Seco, Director de Servicios de Seguridad. BT Iberia.
14:00h.	Coloquio
14:10h.	Almuerzo, fin de la tercera jornada y fin de Securmática 2015

Esquema Nacional de Ciberseguridad Industrial

Sinopsis: En los últimos años, la ciberseguridad en los entornos industriales más dependientes de las tecnologías ha tomado una gran relevancia, motivada por el impacto que podría tener un ciberataque a gran escala en estos sistemas y en las infraestructuras a las que dan soporte. Los ciberataques a infraestructuras estratégicas son una realidad a la que nos enfrentamos diariamente y por ello los principales países de nuestro entorno están haciendo un esfuerzo por mejorar sus niveles de ciberseguridad. Desde INCIBE y el CERTSI se está trabajando por un lado en la elaboración de un Esquema Nacional de Ciberseguridad Industrial, que abordará un catálogo completo de guías, procedimientos, normativas de buenas prácticas y estándares de ciberseguridad, y por otro, y mediante la colaboración con la industria, se pondrán en marcha *test beds* de sistemas de control industrial y, finalmente, un modelo de indicadores para medir la ciberresiliencia.

Ponente:
Miguel Rego Fernández, Director General de INCIBE, Instituto Nacional de Ciberseguridad. Oficial de la Escala Superior del Cuerpo de Intendencia de la Armada (Teniente Coronel en excedencia), experto en ingeniería informática, analista de sistemas, especialista en Criptología y especialista en seguridad corporativa, posee la acreditación profesional de Director de Seguridad y diversas certificaciones, como la de CISM y CISA, de ISACA, o las de Service Manager ITIL V3 Experto, IT Service Management according to ISO/IEC 20000 (EXINX-2008), e ITIL Foundation Certificate in IT Service Management (ITSMF, 2006). Ha realizado, además, el Curso INFOSEC del CNI y dispone de dos premios SIC (2008 y 2010). Su experiencia es extensa, iniciándose en el Ministerio de Defensa, en el que además de ser Profesor y Coordinador de la Escuela de Informática de la Armada Española, fue Jefe del Equipo de Apoyo Informático del Cuartel General de la Armada y Jefe de la Unidad de Seguridad de la Inspección General CIS (actual Subdirección General TIC del Ministerio de Defensa). En el ámbito privado, Miguel Rego ha ocupado los cargos de CSO y CRO (Chief Security and Risk Officer) en Cableuropa (ONO) y posteriormente ha sido Director de Riesgos Tecnológicos en Deloitte España, reportando al socio responsable de esta práctica en esta firma.

Ferrovial: despliegue de la seguridad y el control en Data Center Virtuales

Sinopsis: ¿Es posible gestionar riesgos en entornos *cloud*? ¿De qué mecanismos y garantías de seguridad y control disponen los clientes que optan por este tipo de soliciones? Para responder a estas cuestiones se dará visión acerca de una situación real que tuvo lugar en Ferrovial. Se describirá el caso de Amey, una de las principales filiales de Ferrovial en el Reino Unido, y cómo se decidió la externalización de su infraestructura tecnológica, optando por la solución Virtual Private Cloud de HP, socio tecnológico de Ferrovial. En la ponencia se describirá cómo, dados los riesgos de seguridad inherentes a los entornos de nube, se establecieron los necesarios requerimientos, mecanismos y controles de seguridad, así como los procesos de revisión de dichos elementos y cómo fueron cubiertos por los servicios ofrecidos por HP en el contexto de soluciones VPC.

Ponentes:
Javier Rubio Sanz es Responsable de Gobierno de la Seguridad y Continuidad de Negocio desde agosto de 2012 en el Departamento de Seguridad de la Información, perteneciente a la Dirección de Seguridad y Compras de Ferrovial. Ingeniero Informático por la Universidad Pontificia de Salamanca en Madrid, dispone de un Postgrado en Buen Gobierno de las TIC por la Universidad de Deusto y de las certificaciones CISA, CISM, LA y LI 27001 y LA 22301. Su carrera en el campo de la seguridad de la información comenzó en el año 2005 en EY. En 2008 se incorporó a Deloitte, firma en la llegó a ser Gerente Responsable del Sector de Infraestructuras. En ambas firmas ha llevado a cabo diversos trabajos e iniciativas en materia de Seguridad de la Información, Gestión de Riesgos y Auditoría TIC.

Karen Gaines Cordero es Directora General de HP Security para Iberia. Se unió a HP en junio de 2013 como Ejecutiva de Ventas de EES HP Enterprise Security Services Iberia. Tiene quince años de experiencia en TIC, dedicados principalmente a la seguridad TIC y al *cloud computing*. Gaines es Licenciada en Ciencias por la Universidad Internacional de Florida, y tiene un MBA de la Escuela Europea de Negocios. Antes de incorporarse a HP gestionó las ventas para el oeste de Europa para un VDI *start-up* llamada NComputing, desarrollando planes de negocio con alianzas como Citrix y Microsoft. Anteriormente, fue Country Manager para Iberia de Websense, y previamente realizó funciones de ventas y gestión de marketing en RSA Security y Telefónica Internacional.

Renfe: Sistema de monitorización de APTs

Sinopsis: En los últimos cuatro años, el número de ciberamenazas se ha multiplicado de manera exponencial produciéndose además un cambio en su naturaleza. Se ha pasado de amenazas conocidas, puntuales y dispersas, a amenazas de elevada sofisticación, persistentes y con objetivos muy concretos, surgiendo una nueva categoría: las APT. En este contexto, Renfe es consciente de la necesidad de desarrollar un sistema de Monitorización de APTs que permita prevenir, detectar, notificar y reaccionar ante potenciales riesgos para mantener adecuadamente el nivel de seguridad de la plataforma tecnológica que da soporte a la actividad de su negocio. Para ello, se ha llevado a cabo un proyecto de ciberseguridad junto con Blueliv cuyo objetivo es la integración de la plataforma Blueliv con otras soluciones de monitorización interna y externa para la prevención, detección y reacción ante ciberamenazas.
La plataforma Blueliv aborda una gran variedad de ciberamenazas para convertir la información sobre las mismas en inteligencia en tiempo real, predictiva y procesable para compañías como Renfe. En la ponencia se explicará el proceso de integración y monitorización, así como la gestión que está efectuando Renfe junto con Blueliv.

Ponentes:
Francisco Lázaro Anguis es CISO de Renfe Operadora. Ingeniero de Telecomunicaciones, es también vicepresidente de la Asociación Española de Evidencias Electrónicas (AEDEL) y vocal en comités de normalización, tales como SC27 Subcomité de Seguridad de las TI del CTN 196 Protección y Seguridad de los ciudadanos. Adicionalmente es editor de la norma UNE 71505-1 Sistema de Gestión de Evidencias Electrónicas, y autor de diversos artículos y libros, así como asiduo ponente en Jornadas y Másteres sobre TIC y Seguridad de los Sistemas de Información. En 2012 fue acreedor del premio ASLAN a su trayectoria profesional.

Ramón Vicens Lillo es Vicepresidente de Threat Intelligence de Blueliv. Cuenta con más de una década de experiencia en el sector de la ciberseguridad y es responsable de exhaustivas investigaciones sobre Inteligencia en ciberamenazas y fraude *on line* y, de la definición de la plataforma Blueliv. Se encarga también de las colaboraciones con otras compañías y grupos del sector para ofrecer la mejor protección global frente a ciberamenazas. Incorporado a Blueliv a principios de 2010 como *penetration tester* y analista forense senior, con anterioridad trabajó en compañías como BDO y One eSecurity como analista de ciberseguridad. Experto en *honeypots/nets*, gestión de incidentes, análisis forense y de *malware*, ingeniería inversa y en nuevas tendencias de ciberataques, es ingeniero de telecomunicaciones por la Universidad de Cataluña y cuenta con un máster en seguridad de la Universidad Ramon Llull, además de varias certificaciones profesionales.

Accesos y cuentas privilegiados: Un enfoque como programa corporativo

Sinopsis: Los proyectos de implantación de soluciones de gestión de cuentas y accesos privilegiados suelen plantearse desde una óptica muy técnica, resolviendo únicamente la problemática desde un punto de vista de operativa básica. No obstante, un acercamiento integral a la gestión de cuentas y accesos privilegiados puede incrementar de forma exponencial los beneficios de un proyecto técnico, dando respuesta a los retos presentados por los actores que intervienen en los procesos, como auditoría, cumplimiento normativo, seguridad de la información e incluso los propios equipos técnicos que operan las infraestructuras de producción. De acuerdo a las características y madurez de cada organización, el análisis sobre los criterios que definen el desarrollo de este acercamiento permite trazar un programa corporativo que en su despliegue progresivo actúe activamente sobre todos los componentes, no sólo dentro del ámbito de la gestión de cuentas y accesos privilegiados, sino de los procesos de producción y explotación de los sistemas de información.

Ponentes:

David Carrascosa Bover. Desde hace cuatro años ocupa el cargo de responsable de gestión de identidades y control de acceso (IAM) en Banco Sabadell, el cuarto grupo financiero privado de España. Como tal, es el responsable del desarrollo e implementación del programa corporativo de gestión de la identidad. Dentro de este programa se maneja la visión estratégica de este ámbito para Banco Sabadell, así como la definición y ejecución de los proyectos necesarios para obtener los objetivos definidos en el programa. También realiza la supervisión sobre la explotación de los servicios de *on-going* de gestión de identidades. Dentro de sus experiencias anteriores, durante más de 10 años ha realizado tareas como gerente de proyectos de TI y de servicios de TI dentro de empresas proveedoras de servicios. Adicionalmente dispone de experiencia de más de 5 años como consultor, jefe de proyecto y preventa en el ámbito de seguridad de la información. En esta posición, ha tenido la oportunidad de trabajar para grandes empresas en el sector financiero, aseguradoras, *utilities*, servicios y administración pública, etc. Carrascosa es ingeniero en telecomunicaciones y dispone de un máster en administración de empresas. Es CISM por el capítulo de Barcelona de Isaca.

Javier Zapata Victori lidera desde enero de 2015 la unidad de Ciberseguridad dentro de BDS Atos Iberia. Y con anterioridad llevaba tres años como Director de la BU de Seguridad de Bull España. Ingeniero superior en Telecomunicaciones por la UPC, PDD por el IESE, CISSP y Lead Auditor ISO 27001, cuenta con 17 años de experiencia en consultoría y seguridad TI, y ha trabajado para grandes organizaciones en el Sector Financiero, Energía y *Utilities* y Administraciones Públicas. Durante estos años ha desempeñado funciones de Senior Manager dentro del área de Consultoría de Bull, Manager en el área de Technology Services en Capgemini y Consultor de eCommerce en BT UK.

Cyber Security Response Team: equipo de alto rendimiento

Sinopsis: "la Caixa" orienta su actividad en base a un modelo de banca universal fomentado en una estrategia multicanal. Dentro de este modelo, la vigilancia proactiva de las amenazas que pongan en riesgo los activos tecnológicos en los que se sustenta el negocio resulta un elemento clave. En este contexto, Seguridad de la Información establece los reglamentos y procedimientos necesarios para establecer esta vigilancia y garantizar que se implementan los controles necesarios para mitigar estos riesgos. El **Cyber Security Response Team** proporciona el apoyo operativo 24x7x365 necesario al grupo de Ciberseguridad de "la Caixa". Dicho grupo se encarga de implantar, gestionar, monitorizar, evaluar la adecuación y garantizar que los controles de seguridad que protegen la red, los sistemas y las aplicaciones de "la Caixa", conjuntamente con la reacción ante ataques externos o internos, permiten desarrollar el negocio y mantener la excelencia en la protección de la información de "la Caixa", de sus clientes y de las entidades y organizaciones relacionadas.

Ponentes:

Carles Solé Pascual es Director del Departamento de Seguridad de la Información de CaixaBank, liderando los equipos responsables del gobierno de la seguridad de la información, la protección de la información y la ciberseguridad. También es Director del Instituto Español de Ciberseguridad, una iniciativa del ISMS Forum. Es Ingeniero Superior de Informática por la UPC y Executive MBA por el IESE. Actualmente forma parte del Security Board of Advisors de IBM, del Comité Ejecutivo del ISMS y del Comité de Certificación de Applus.

Xavier Gracia Lacalle es Director del CyberSOC de Deloitte. A lo largo de su trayectoria profesional ha liderado diferentes proyectos tecnológicos y actualmente es responsable del desarrollo de negocio en Cataluña, Aragón, Baleares y Andorra, en el ámbito de riesgos tecnológicos en el CyberSOC de Deloitte. Las industrias en las que está especializado son: FSI (Banca), Sector Público y Sanidad. Ingeniero de Telecomunicaciones por la UPC, es diplomado en Alta Dirección de Empresas por el IESE y Máster en Dirección de las TI por la Salle (Universidad Ramon Llull). Igualmente es profesor asociado de dirección estratégica de sistemas de información en el MBA de la UPC y en el Máster en Dirección de TIC, en la Business Engineering School, de La Salle (URL).

Abertis: la movilidad como factor crítico para el desarrollo del negocio

Sinopsis: En la evolución de la estrategia de seguridad de Abertis era necesario acometer el reto de incorporar una solución de EMM (*Enterprise Mobility Management*) para abordar el ciclo de vida de los dispositivos móviles, *securizando* los dispositivos, las aplicaciones y los datos que los mismos contienen (con especial foco en el correo electrónico corporativo y los adjuntos correspondientes), garantizando la seguridad del activo en todas sus vertientes y relacionando la tecnología con todo el ecosistema de TI existente. Para ello Abertis ha confiado en un *partner* tecnológico de contrastada experiencia como BT y en una de las tecnologías líderes del mercado como es la de MobileIron, con el objetivo de incorporar la solución en la organización en tiempo y forma para los diferentes perfiles y roles de la organización.

Ponentes:

Manel Leal Sáez es Responsable de Seguridad Informática de Abertis. Con más de 30 años de experiencia en el ámbito de los sistemas informáticos, los últimos quince ha trabajado en empresas de grupo Abertis llevando el Servicio de Explotación y Seguridad. Desde 2006 ha desarrollado sus funciones en la corporación y los últimos siete centrado en seguridad.

José Francisco Pereiro Seco es Director de Servicios de Seguridad de BT Iberia y tiene más de 15 años de experiencia en el área de Seguridad de la Información. Desde su incorporación a BT como responsable de la práctica de seguridad ha lanzado nuevos productos y soluciones al mercado como el Centro de Operaciones de Ciberseguridad de BT en España que se une a la red Global de 12 SOCs de BT. Es miembro de la Junta Directiva y el Comité Operativo del ISMS Forum y ponente en diversos eventos. Dispone de varias de las principales certificaciones de seguridad como CISA, CISM, CISSP o CSSA, entre otras.

// Securmática 2015

Securmática 2014 tuvo el honor de contar con la participación en el acto inaugural de **Félix Sanz Roldán**, Secretario de Estado Director del CNI y Presidente del Consejo Nacional de Ciberseguridad.

Más de 7.000 expertos han pasado por Securmática, un congreso que con sus 25 ediciones ya celebradas es el foro de intercambio de experiencias en ciberseguridad por excelencia.

// Premios SIC 2015 y Cena de la Seguridad

En coincidencia con la XXVI edición de Securmática, tendrá lugar el acto de entrega de los XII 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 undécima edición de los Premios SIC.

Fechas y lugar de celebración

SECURMÁTICA 2015 tendrá lugar los días 21, 22 y 23 de abril de 2015 en el hotel NOVOTEL. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2015 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 XII Premios SIC (22 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 23 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)
IBAN: ES27 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 21 ☐ Módulo 2 Día 22 ☐ Módulo 3 Día 23 ☐ Deseo inscribirme a SECURMÁTICA 2015

Firma:

AFORO LIMITADO

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**