SECURMÁTICA

25 años

XXV Congreso español de Seguridad de la Información

22.23.24 abril | 2014

Protección del negocio: todo se complica

PROGRAMA

Organiza:

Revista SIC

www.securmatica.com

SECURMÁTICA 25 años

Tendrá lugar los días 22, 23 y 24 de abril en su tradicional sede del Campo de las Naciones de Madrid

Securmática 2014. Protección del negocio: todo se complica

La seguridad de la información y la ciberseguridad se encuentran hoy en una etapa de formalización normativa, organizativa y operativa en los estados. Y España no es una excepción, como lo demuestra la existencia de la ECSN2013 y la constitución del Consejo Nacional de Ciberseguridad.

Estos que vivimos son tiempos históricos, en los que prepondera la necesidad de establecer los límites competenciales de los organismos más directamente involucrados y de marcar espacios para la colaboración entre las administraciones públicas, el sector privado y la ciudadanía, guardando un equilibro entre la seguridad y otros derechos ajustado a la ley.

Securmática cumple este año un cuarto de siglo de vida. Y su forma de celebrarlo es presentando este programa, que intenta ser una fotografía del estado de las cosas y de su proyección a futuro.

Y en esa línea, encuentran cabida en sus dos días y medio de celebración asuntos tales como los trabajos de desarrollo de la ECSN, el plan para la protección del Patrimonio Tecnológico español, el calendario de materialización de los Planes Estratégicos Sectoriales en el campo de las Infraestructuras Críticas, las novedades regulatorias en la gestión de incidentes de ciberseguridad, los ciberjercicios orientados a la seguridad, la propuesta de un sistema de indicadores de ciberresiliencia o la articulación del uso legal de herramientas TIC en la investigación de conductas ilícitas. A estas aportaciones, que realizarán expertos autorizados de los organismos públicos directamente implicados en la gestión global de la ciberseguridad nacional, se unirán otras realizadas por especialistas de primer nivel del sector privado, que abordarán asuntos alusivos a la gestión inteligente de riesgos (sector financiero, petróleo…), la continuidad de negocio, el tratamiento unificado de amenazas físicas y lógicas, la transformación de la banca al espacio digital, el avance en la creación de pólizas de seguros ante ciberriesgos, o las implicaciones en la gestión de la privacidad y la ciberseguridad del Reglamento General de Protección de Datos de la UE respaldado por el Parlamento Europeo y hoy en fase de aprobación por los Estados Miembros.

Securmática 2014 también será el escenario de presentación de proyectos de ciberseguridad y continuidad llevados a cabo por usuarios públicos y privados de diversos sectores, algunos de ellos fundamentados en servicios de cibersoc externos.

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

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

PRIMER MÓDULO, 22 DE ABRIL

08:45h. Entrega de Documentación

09:15h. Ceremonia de apertura

10:00h. **Conferencia inaugural**

Ponente: **Félix Sanz Roldán**, Secretario de Estado Director del CNI y Presidente del Consejo Nacional de Ciberseguridad**.**

Moderador: **Miguel A. Amutio Gómez,** Subdirector Adjunto. Subdirección General de Programas, Estudios e Impulso de la Administración Electrónica. D. G. de Modernización Administrativa, Procedimientos e Impulso de la Administración-e. Mº de Hacienda y Administraciones Públicas.

10:20h. Ponencia: **Estrategia de Ciberseguridad Nacional: un punto de partida.**

Ponente: **Joaquín Castellón Moreno**, Director Operativo del Departamento de Seguridad Nacional.

10:50h. Coloquio

10:55h. Ponencia: **Acciones programadas para la protección del Patrimonio Tecnológico español.**

Ponente: **Javier Candau Romero**, Jefe del Área de Ciberseguridad del Centro Criptológico Nacional.

11:25h. Coloquio

11:30h. Pausa-café

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

12:00h. Ponencia: **Calendario de materialización de los Planes Estratégicos Sectoriales.**

Ponente: **Fernando Sánchez Gómez**, Director de CNPIC, Centro Nacional para la Protección de Infraestructuras Críticas. Secretaría de Estado de Seguridad. Ministerio del Interior.

12:30h. Coloquio

12:35h. Ponencia: **Novedades regulatorias para la gestión de incidentes de 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.

13:05h. Coloquio

13:10h. Ponencia: **Ejercicios de ciberdefensa en las Fuerzas Armadas.**

Ponente: **Enrique Cubeiro Cabello**, Jefe de Operaciones del Mando Conjunto de Ciberdefensa (MCCD). Ministerio de Defensa.

13:40h. Coloquio

13:45h. Ponencia: **Modelo de indicadores de ciberresiliencia.**

Ponente: **Miguel Rego Fernández**, Director General de INTECO.

14:15h. Coloquio

14:20h. Almuerzo

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

16:20h. Ponencia: **Ciberseguridad industrial: despliegue de nuevas capacidades del CSIRT-CV.**

Ponentes:

Carmen Serrano Durbá. Jefa de Servicio de Seguridad de la Información de la Generalitat Valenciana.

José Rosell Tejada. Socio-Director de S2 Grupo.

16:50h. Coloquio

17:00h. Ponencia: **Ministerio de Industria, Energía y Turismo: Servicio de Seguridad Gestionada.**

Ponentes:

Miguel Ángel Rodríguez Ramos, Jefe del Área de Sistemas y Seguridad. Ministerio de Industria.

Alfonso Martín Palma, Responsable del CyberSecurity Operations Center (i-CSOC) de Indra.

17:30h. Coloquio

17:40h. Fin de la primera jornada

Conferencia inaugural

Félix Sanz Roldán, Secretario de Estado Director del CNI y Presidente del Consejo Nacional de Ciberseguridad.

Estrategia de Ciberseguridad Nacional: un punto de partida

Sinopsis: El ciberespacio es un campo de oportunidades y un ámbito imprescindible para el desarrollo de todo nuestro potencial económico y social; pero al mismo tiempo, constatamos la existencia de múltiples riesgos y amenazas. Sin embargo, España no se había dotado de un documento estratégico que perfilara los elementos necesarios para proteger nuestro ciberespacio.

La Estrategia de Ciberseguridad Nacional es el marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada, y en la participación de la ciudadanía

El Consejo Nacional de Ciberseguridad dará apoyo al Consejo de Seguridad Nacional prestando asistencia a la dirección y coordinación de la Política de Seguridad Nacional en materia de Ciberseguridad.

El Consejo cuenta ya con un plan de trabajo que permitirá avanzar en la consecución de los objetivos fijados en la Estrategia de Ciberseguridad Nacional.

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.

Acciones programadas para la protección del Patrimonio Tecnológico español

Sinopsis: En los últimos años hemos confirmado una especial virulencia en ataques del tipo amenazas persistentes avanzadas realizados principalmente por estados u organizaciones adscritas a éstos. Durante 2013 las campañas OCTUBRE ROJO, GRUPO APT 1, ICEFOG y NETTRAVELER confirmaron el creciente interés en el patrimonio tecnológico e información comercial sensible de empresas, impactando principalmente en los sectores energético (industria nuclear pero atacando a empresas de otros sectores), aeroespacial, defensa, telecomunicaciones y naval, entre otros, además de los ataques correspondientes en la información sensible / clasificada de las Administraciones Públicas.

En el marco de la Estrategia de Ciberseguridad Nacional, en cumplimiento de su objetivo II y de las líneas de acción correspondientes (1.4 y 5.1 principalmente) y según el mandato establecido en la ley 11/2002 (Función 4.b) de protección de los intereses económicos nacionales, se está trabajando en una serie de medidas que se integrarán en el correspondiente Plan Nacional de Ciberseguridad, que mejoren las actividades de detección, alerta y respuesta por parte de AAPP y empresas a este tipo de ataque. Esta actividad se considera crítica para la es-

tabilidad de nuestras empresas y la libre competencia de las mismas. Es necesario recibir del sector privado ideas y propuestas para realizar de una manera más eficiente el intercambio de información necesario para atajar esta amenaza, optimizando y asimilando lecciones aprendidas de empresas y AAPP que la hayan sufrido.

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.

Novedades regulatorias para la gestión de incidentes de ciberseguridad

Sinopsis: La gestión de incidentes de ciberseguridad basada en esquemas voluntarios tiene grandes ventajas para los distintos actores implicados. No obstante, la creciente complejidad e impacto de las amenazas aconseja buscar modelos regulatorios que permitan reforzar los esquemas disponibles y aumentar su eficacia. Por un lado, la Propuesta de Directiva de Seguridad de la Información y las Redes afronta este reto para sectores especialmente sensibles para la economía. Por otro, la nueva disposición adicional novena de la Ley de Servicios de la Sociedad de la Información, introducida en el proyecto de Ley General de Telecomunicaciones, actualmente en tramitación parlamentaria, propone nuevas obligaciones a los prestadores de servicios de la sociedad de la información y a los CERTs para la gestión de incidentes de ciberseguridad, introduciendo un modelo novedoso basado en códigos de conducta.
El objetivo de la ponencia es presentar el nuevo contexto regulatorio para la gestión de incidentes de ciberseguridad profundizando en su alcance, aspectos críticos de éxito, así como en el conjunto de obligaciones para todos los actores implicados.

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. Es responsable de la regulación y el desarrollo estratégico de políticas públicas para el desarrollo de la economía digital, la ciberseguridad y la confianza digital en el mercado digital interior. Antonio Alcolea 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.

Calendario de materialización de los Planes Estratégicos Sectoriales

Sinopsis: Actualmente, y después de varios meses de intenso trabajo y de una labor de coordinación sin precedentes en la corta historia del CNPIC, nos encontramos en la recta final de la elaboración de los Planes Estratégicos Sectoriales (PES) de la Electricidad, el Gas, el Petróleo, el Sistema Nuclear y el Sistema Económico y Financiero. La aprobación de dichos Planes, prevista en la Ley 8/2011, supondrá el espaldarazo definitivo a la norma PIC y la materialización de parte de las directrices marcadas por la Estrategia Española de Seguridad, aprobada en junio de 2013.

Ponente:
Fernando Sánchez Gómez, Director del CNPIC, Centro Nacional para la Protección de Infraestructuras Críticas, dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior. Es Teniente Coronel de la Guardia Civil (Carrera Superior Militar). Diplomado de Estado Mayor. Previamente a su cargo actual desarrolló sus funciones durante varios años en el campo de la seguridad de infraestructuras e instalaciones de carácter estratégico en la Dirección General de la Guardia Civil, Dirección Adjunta Operativa (Estado Mayor). Ha realizado varios cursos oficiales de la Guardia Civil, entre otros el Superior de Especialista en Información y el de Especialista en Policía Judicial. Posee diferentes condecoraciones nacionales. Habla tres idiomas: inglés, francés e italiano. Está en posesión de diversos Máster y Cursos Superiores y tiene reconocido el título de Director de Seguridad. Es coautor del libro *"Marco Legal y de Gestión de la Protección de las Infraestructuras Críticas en España"*. Asimismo, es autor de diferentes publicaciones y artículos relacionados con el campo de su dominio. Colabora asiduamente en diferentes cursos y máster relacionados con defensa y seguridad, organizados por diversas universidades (UNED, Camilo Jose Cela, Carlos III, etc.). En su cargo actual ejerce como coordinador en la elaboración y desarrollo de la normativa española sobre protección de infraestructuras críticas (Ley 8/2011, Real Decreto 704/2011 y sus planes derivados). Es el Punto de Contacto del Estado Español con la Unión Europea en materia de protección de infraestructuras críticas.

Ejercicios de ciberdefensa en las Fuerzas Armadas

Sinopsis: Se expondrán los principales ejercicios orientados a la Ciberdefensa militar pura en el panorama internacional en los que participan nuestras Fuerzas Armadas (Cyber Storm, Locked Shield, Cyber Coallition, Cyber Europe), así como otros ejercicios que incluyen escenarios e incidentes de ciberdefensa (CMX, FCEX), con especial atención a los de carácter nacional y, muy especialmente, al Ejercicio de Ciberdefensa de las FAS, que organiza anualmente el Mando Conjunto de Ciberdefensa. En este último, se analizan los objetivos, participantes, evolución histórica, arquitectura, plataformas, desarrollo, resultados, lecciones aprendidas y retos futuros. Por último, se aportarán algunas reflexiones sobre cómo potenciar la formación y la concienciación, enfocadas al usuario medio, mediante el apoyo de herramientas de simulación.

Ponente:
Enrique Cubeiro Cabello, Capitán de Navío. Jefe de Operaciones del Mando Conjunto de Ciberdefensa (MCCD). Ministerio de Defensa. Ingresó en la Armada en el año 1981 y fue promovido a su empleo actual en julio de 2013. A lo largo de su carrera, ha ejercicio el mando de los buques "Bergantín", "Serviola" y "Patiño" y ha participado en numerosas operaciones, entre las que destacan la operación Sharp Guard para el embargo a la antigua Yugoslavia, Active Endeavour de la OTAN para prevenir el movimiento de terroristas y de armas de destrucción masiva en el Mediterráneo, y, más recientemente, la Operación Atalanta de la Unión Europea para la lucha contra la piratería en el Océano Índico. Durante su mando del buque Patiño en esta última operación, se produjo el apresamiento de los primeros piratas juzgados y condenados en España por el delito de piratería. Es Especialista en Comunicaciones y Diplomado en Estado Mayor de las Fuerzas Armadas. Fue Premio Defensa 2002 en la modalidad de trabajos de investigación desarrollados por concurrentes a cursos de altos estudios militares por su monografía "Sistemas de mando y Control, una visión histórico-prospectiva". Actualmente preside el Grupo de Trabajo de Implantación de la Ciberdefensa en el Ámbito Marítimo, que deriva de la Estrategia de Seguridad Marítima Nacional.

Modelo de indicadores de ciberresiliencia

Sinopsis: Las TIC propician el desarrollo económico de la sociedad de manera integrada dentro de las empresas. Pero esta integración y desarrollo están sujetos a riesgos y amenazas cibernéticas, que deben afrontarse de manera coordinada para dar respuestas eficaces que garanticen la seguridad en el ciberespacio. La Ciberresiliencia, como capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes, es el instrumento necesario para afrontar este reto, y en su configuración se hace necesaria la definición y establecimiento de

un modelo de indicadores dirigido a medir la capacidad de las organizaciones ante distintos ataques, amenazas o incidentes que puedan sufrir. En la actualidad no existe un modelo de medición estándar reconocido orientado a la evaluación de la ciberseguridad y la ciberresiliencia en las organizaciones. El objetivo es estudiar y proponer la creación de un modelo proporcionando unas pautas generales que permitan medir la capacidad de resistencia de las organizaciones frente a ataques, su nivel de preparación, de respuesta a incidentes reales y posibles amenazas, y su capacidad para mantener la continuidad de su negocio y recuperarse de posibles impactos. Dicho modelo se basa en varias capas que recogen la Gobernanza de la Ciberseguridad y la Ciberresiliencia, una propuesta de modelo de indicadores, hasta llegar a un esquema de madurez del modelo que permita su mejora, mantenimiento y su comparación en el tiempo o con otras organizaciones que lo apliquen.

Ponente:

Miguel Rego Fernández, Director General de INTECO. 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 la práctica de seguridad de esta firma- hasta su incorporación a INTECO como director general.

Ciberseguridad industrial: despliegue de nuevas capacidades del CSIRT-CV

Sinopsis: Con el paso de los años las competencias de los Centros de Operaciones de Seguridad han ido evolucionando, orientándose a diferentes ámbitos de la seguridad y ampliando su catálogo de servicios para abarcar la mayor parte de la problemática tecnológica existente. Dentro de estas nuevas competencias ha surgido la necesidad de incluir las relacionadas con los sistemas de control industrial que, entre otras instalaciones, garantizan el correcto funcionamiento de muchas infraestructuras críticas, estén o no incluidas en los catálogos nacionales. El aumento de la exposición de este tipo de redes de control al exterior, unida a la criticidad que en muchos casos presentan los entornos controlados por estos sistemas, ha motivado que los atacantes tengan en su punto de mira este tipo de redes. En este sentido es necesario que los Centros de Respuesta ante Incidentes adecúen sus capacidades a las necesidades de la sociedad en cada momento. Es el momento de complementar las capacidades más tradicionales de nuestros Centros de Operaciones de Seguridad con conocimientos y habilidades requeridas para enfrentarse a escenarios desconocidos hasta la fecha. El CSIRT-CV es el Centro de Respuesta ante Incidentes de Ciberseguridad de la Generalitat Valenciana y trabaja de forma continua para adecuar su Catálogo de Servicios a las necesidades que detecta.

Ponentes:

Carmen Serrano Durbá es Jefa del Servicio de Seguridad de la Dirección General de TI en la Conselleria de Hacienda y Administración Pública de la Generalitat Valenciana. Licenciada en Informática por la Universidad Politécnica de Valencia y funcionaria de carrera de la Generalitat Valenciana adscrita al cuerpo Administración Especial, es Superior técnico de ingeniería informática. Tras ocupar diversos puestos en la Conselleria de Obras Públicas, Urbanismo y Transportes, ocupó durante 14 años la jefatura del Servicio de Informática de la Conselleria de Medio Ambiente desarrollando diversos proyectos de seguridad. Actualmente es Jefa del Servicio de Seguridad de la Dirección General de TI en la Conselleria de Hacienda y Administración Pública y también Responsable de Seguridad de la Generalitat, representante de la Comunidad Valenciana en el Grupo de Trabajo de Seguridad del Comité Sectorial de Administración Electrónica del Mº de Hacienda y Administraciones Públicas y miembro del Comité de Seguridad de la Información de las Administraciones Públicas. Dirige la estrategia de seguridad de la Dirección General de TI y del Centro de Seguridad TIC de la Comunitat Valenciana (CSIRT-CV).

José Rosell Tejada es Socio Director de S2 Grupo. Consultor especializado en Seguridad, en Explotación de sistemas críticos y en Sistemas de Gestión por procesos basados en distintos referenciales como la ISO 27001, ISO 9000, ISO 28000, ISO 20000, ISO 14001, etc., en su carrera profesional ha ocupado entre otros el puesto de Director de TIC de Unión Naval de Levante (Valencia, Madrid y Barcelona) y ha sido Director de Explotación de Tissat, consultora tecnológica de la Generalitat Valenciana donde fue, entre otros cargos, Director Gerente del Centro telemático de la Generalitat Valenciana, Director de Explotación Tecnológica de los Centros de Emergencias de Valencia y Murcia y Responsable de explotación de la plataforma tecnológica de la tarjeta sanitaria de Valencia.

Ministerio de Industria, Energía y Turismo: Servicio de Seguridad Gestionada

Sinopsis: El Ministerio de Industria, Energía y Turismo afronta los nuevos retos en seguridad y el cambio en el panorama de amenazas en el marco de la Estrategia de Ciberseguridad Nacional, lanzando un proyecto para mejorar la prevención, detección y recuperación ante incidentes. Para ello se ha apoyado, además de en personal propio, en los servicios de seguridad gestionada prestados por Indra con la colaboración de Symantec. Indra y Symantec han establecido un modelo de servicio que combina el soporte de la tecnología de monitorización de comportamiento de *malware* y amenazas más avanzado del mercado de Symantec, que se basa en la inteligencia capturada a través de su red global, con el *expertise* en ciberseguridad de los especialistas del i-CSOC de Indra. Para ello al equipo 24x7 de monitorización de Symantec se le añade una capa local, también 24x7, que aporta el conocimiento de la infraestructura del cliente, el idioma y la posibilidad de desplazarse físicamente para la contención y remediación de incidentes. En esta conferencia se pondrán en valor los aspectos más destacados de este modelo en el que cada una de las partes, aportando su *expertise* reconocido, han conseguido alcanzar una solución óptima.

Ponentes:

Miguel Ángel Rodríguez Ramos, Jefe del Área de Sistemas y Seguridad. Ministerio de Industria. Es Ingeniero en Informática por la Universidad Politécnica de Madrid y Máster en Gestión Pública de Tecnologías de la Información y las Comunicaciones por el Instituto Nacional de Administración Pública. Dirige proyectos relacionados con el desarrollo de la Política de Seguridad de la Información del Ministerio, el plan de adecuación al Esquema Nacional de Seguridad, las infraestructuras de TI del Datacenter y las arquitecturas tecnológicas de operación de los sistemas de información de Administración Electrónica.

Alfonso Martín Palma, Responsable del CyberSecurity Operations Center (i-CSOC) de Indra. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid, CISA, CISM, CRISC y CGEIT por la ISACA, Alfonso Martín es experto implantador y auditor ISO 27000 por Aenor. Ha desarrollado su carrera profesional en GFI, Thales, Magari, Azertia y actualmente en Indra. Cuenta con 20 años de experiencia en seguridad de la información, habiendo dirigido proyectos y servicios de seguridad gestionada, certificación y acreditación de sistemas, gestión de identidades y acceso, consultoría de seguridad, 'securización' de infraestructuras TI, PKI, sistemas de gestión de seguridad de la información y oficinas técnicas de seguridad.

SEGUNDO MÓDULO, 23 DE ABRIL

09:00h. Entrega de documentación
Moderador: **Jess García**, Instructor Jefe para EMEA de SANS Institute.

09:30h. Ponencia: **Bankia: SIEM de cuarta generación.**
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: **Servicios Gestionados: socorriendo al "CISO-orquesta".**
Ponentes:
Carles Solé Pascual, Director de Seguridad Informática de CaixaBank.
Karen Gaines Cordero, Ejecutiva de Ventas de ESS HP Enterprise Security Services Iberia.

10:40h. Coloquio

10:50h. Ponencia: **Seguridad y Riesgos Tecnológicos: dos palabras y un destino.**
Ponente: **Julio San José Sánchez**, Gerente de Riesgos Tecnológicos de Bankinter.

11:20h. Coloquio

11:30h. Pausa-café
Moderador: **Román Ramírez Giménez**, Cofundador de Rooted CON.

12:10h. Ponencia: **La ciberseguridad como catalizador de la transformación de la banca clásica en banca digital.**
Ponente: **Santiago Moral Rubio**, Director de Riesgo IT, Fraude y Seguridad. Grupo BBVA.

12:40h. Coloquio

12:50h. Ponencia: **¿Qué daños derivados de ciberataques deberían cubrir las pólizas de seguros orientadas al mercado empresarial?**
Ponentes:
José Ramón Monleón Martínez, Gerente de Seguridad de la Información Corporativa de Orange.
Alfredo Zorzo Losada, Responsable de Seguros de Orange en España.

13:20h. Coloquio

13:30h. Ponencia: **Ciberseguridad: enfoque y evolución. El caso de BP.**
Ponente: **Daniel Barriuso Rojo**, CISO y Responsable de Seguridad Digital. BP.

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.

16:30h. Ponencia: **El compromiso de la Alta Dirección. Ejercicio práctico de Gestión de Crisis en Mapfre.**
Ponentes:
Lionel Güitta Abellán, Subdirector. Subdirección de Continuidad de Negocio. Subdirección General de Seguridad y Medio Ambiente de Mapfre.
Juan José Míguez Iglesias, Socio. Departamento de Riesgos Tecnológicos de PwC.

17:00h. Coloquio

17:10h. Ponencia: **Telefonica Global: llegué, vi y vencí, estrategia de ciberinteligencia para la protección proactiva ante nuevas amenazas.**
Ponentes:
Pedro Pablo Pérez García, Responsable de Ciberseguridad. Telefónica Global.
Daniel Solís Agea, CEO de blueliv.

17:40h. Coloquio

17:50h. Ponencia: **Grabación de Pruebas de Continuidad de Negocio: Planificación, Realismo y Concienciación.**
Ponentes:
Marcos Guasp, Gerente de Riesgos y Continuidad en el ámbito de Ciberseguridad y Riesgo Tecnológico de Repsol.
Joaquín Castillón Colomina, Senior Manager del área de Advisory Services de EY.

18:20h. Coloquio

18:30h. Fin de la segunda sesión

19:30h. **Cena de la seguridad y entrega de los XI Premios SIC**

Bankia: SIEM de cuarta generación

Sinopsis: La conferencia mostrará la evolución de la infraestructura SIEM en Bankia, desde la prehistoria (los recolectores de *logs*) hasta la era espacial (*time stamping*, inteligencia de red, APTs, fraude…). Ciberseguridad, *Advanced Persistent Threats*, Ciberfraude... son algunos de los grandes retos que las organizaciones tienen en la actualidad. En la ponencia se analizará cómo la nueva generación de SIEM y *Security Intelligence* ayudan al reto de proteger el negocio.

Ponentes:
Javier Sevillano Izquierdo es Responsable de Seguridad Tecnológica en Bankia. Dispone de 27 años de experiencia en TI, 19 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 18 años de experiencia en el sector TI, los últimos 16 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.

Servicios gestionados: socorriendo al "CISO-orquesta"

Sinopsis: Los delitos cibernéticos representan una gran amenaza para cualquier organización, especialmente para bancos o instituciones financieras como CaixaBank, en los que se gestiona una importante cantidad de información confidencial relativa a empresas y particulares. Esta entidad financiera ha confiado en HP Enterprise Services para la prestación de servicios gestionados de seguridad, así como el proceso de adaptación y evaluación del cuerpo normativo de seguridad para todas las empresas del Grupo. En servicios gestionados, CaixaBank y HP Enterprise Services han construido un modelo de ventana única que permite canalizar las consultas y las peticiones del toda la entidad hacia el departamento de Seguridad Informática, añadiendo una capa de *expertise*, tanto en materia de seguridad como en los propios circuitos de la compañía, para proporcionar un servicio ágil y de valor ante una demanda cada vez más exigente.

Ponentes:
Carles Solé Pascual, Director de Seguridad Informática de CaixaBank desde el año 2009. Bajo la responsabilidad del mismo está el gobierno de la seguridad de la información, la protección de la información y la ciberseguridad. Es ingeniero superior de informática por la UPC y executive MBA por el IESE. También es Director del Instituto Español de Ciberseguridad (SCSI) del ISMS Forum Spain, y forma parte de la Junta Directiva de ISACA Barcelona, del Security Board of Advisors de IBM y del Comité de certificación de Applus.

Karen Gaines Cordero, Ejecutiva de Ventas de EES HP Enterprise Security Services Iberia. Se unió a HP en junio de 2013. Tiene quince años de experiencia en TIC, dedicados principalmente a la seguridad TIC y al *cloud computing*. Karen 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* llamado NComputing, desarrollando planes de negocio con alianzas como Citrix y Microsoft. Anteriormente, Karen fue Country Manager para Iberia de Websense. Con anterioridad, realizó funciones de ventas y gestión de marketing en RSA Security y Telefónica Internacional.

Seguridad y Riesgos Tecnológicos: dos palabras y un destino

Sinopsis: En estos veinticinco últimos años hemos pasado de la protección del acceso a nuestros ordenadores o centros de cálculo, allá por finales de los 80, hasta la protección integral de nuestros negocios frente a los ciberriesgos del siglo XXI. De haberse realizado esta evolución, habríamos pasado de la protección de nuestras infraestructuras a la protección real de nuestras organizaciones, la información que en ellas se genera y de la que dependen como su principal activo. Entonces ¿por qué nos empeñamos en proteger la infraestructura?, ¿frente a qué? y lo que es peor, ¿frente a quién? ¿No sería mejor centrarnos en la protección de la información del negocio de nuestras organizaciones? Siempre pedimos el apoyo y la comprensión de la alta dirección pero cuando nos preguntan, normalmente

les respondemos con ¿un cacharrito (*firewall,* ids, ips, antivirus...) más? Al igual que las especies, donde la adaptación supone la subsistencia, la función de gestión de Riesgos Tecnológicos nos asegura una correcta protección de nuestros negocios y sus activos frente a los ciberriesgos del XXI, porque los Riesgos Tecnológicos no son cosa de *hackers*...

Ponente:
Julio San José Sánchez es Gerente de Riesgos Tecnológicos de Bankinter. Con una trayectoria de más de veinticinco 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, 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. Asimismo es coautor del libro *"Seguridad de las tecnologías de la información. La construcción de la confianza para una sociedad conectada"*, editado por Aenor.

La Ciberseguridad como catalizador de la transformación de la banca clásica en banca digital

Sinopsis: La Seguridad de la Información y la Gestión del Riesgo Tecnológico han dejado de ser, sólo, elementos habilitadores de la digitalización de los negocios para convertirse en catalizadores de la transformación de los mismos. Los mecanismos que se utilizan para saber que un consumidor o un cliente es quien dice ser, dónde puede alojarse la información del negocio, bajo qué características y quién puede acceder a ésta, permite hacer la auténtica transformación de los negocios clásicos al negocio digital.
Identificar los patrones de comportamiento de los consumidores, identificar el patrón de usos de los negocios y explotar desde el punto de vista del Riesgo Tecnológico, a través de mecanismos de Big Data, toda esta información permite, no sólo un análisis de Riesgos mucho más fino, sino que nos puede mostrar nuevas oportunidades de negocio.

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.

¿Qué daños derivados de ciberataques deberían cubrir las pólizas de seguros orientadas al mercado empresarial?

Sinopsis: En esta conferencia se llevará a cabo, en una primera fase, un repaso del catálogo de preocupaciones actuales y a futuro de los Gerentes de Riesgos Tecnológicos y, en concreto, de los de Seguridad de la Información en orden a las tecnologías en uso, al incremento del volumen de información y en lo que toca a la modalidad de servicios, incluidos los asociados con la Nube, y a la cuantificación de riesgos, para en una segunda fase informar de qué ofrece hoy el seguro cíber y qué palancas utiliza el sector asegurador para cotizar. Al tiempo, se tratará de aportar ideas para la relación entre la dirección de seguridad de la información y la de seguros, y se llevará a efecto una comparación entre la situación de oferta seguradora.

Ponentes:
José Ramón Monleón Martínez, Gerente de Seguridad de la Información Corporativa de Orange España. Ingeniero Superior de Telecomunicación, en su actual cargo, asume la responsabilidad de Seguridad de la Información a nivel local y la de coordinador de Seguridad Global en el Grupo Orange desde 2006. Tiene diez años de experiencia en Sistemas de Información, en especial en los sistemas de medios de pago.

Alfredo Zorzo Losada, Responsable de Seguros de Orange España. Máster en Dirección Económico Financiera (CEF), Mediador de Seguros Titulado grupo "A" (Udima), Experto en Gerencia de Riesgos y Seguros (Mapfre), con formación en distintos ámbitos de la gerencia de riesgos y seguros y con una experiencia profesional de más de veinte años, en su actual cargo asume la responsabilidad de la gerencia de los riesgos asegurables a nivel local y de la interlocución y aplicación de la filosofía y los procesos estratégicos corporativos del Grupo Orange en esta materia. Desde 2011 es miembro de la Junta Directiva de AGERS (Asociación Española de Gerencia de Riesgos y Seguros), en la que actualmente ostenta el cargo de Vicepresidente y participa en diferentes Comisiones y Grupos de Trabajo, siendo el actual Director del Curso sobre Gestión de Riesgos Tecnológicos que la asociación viene impartiendo desde 2012.

Ciberseguridad: enfoque y evolución. El caso de BP

Sinopsis: La gestión de la ciberseguridad en un mundo cambiante y complejo requiere una aproximación que permita una comunicación clara con el negocio, alinear los esfuerzos de las distintas áreas y un enfoque dinámico. Durante la ponencia, Barriuso expondrá el modelo que ha seguido BP, centrado en tres elementos principales: tres barreras sobre las que estructurar las defensas frente a ciberataques; tres principios para conducir el diseño de controles prácticos y precisos; y tres estrategias para mantener contramedidas ágiles, adaptables y sostenibles que permitan afrontar el reto de la ciberseguridad. Igualmente, la conferencia dará ocasión de conocer algunas de las iniciativas internacionales de ciberseguridad que se están desarrollando en el sector Energético, de las que BP forma parte.

Ponente:
Daniel Barriuso Rojo es CISO y Responsable de Seguridad Digital de BP. Basado en Londres, Barriuso es responsable de la ciberseguridad a través de todas las áreas de negocio y países del grupo, incluyendo estrategia, gobierno, arquitectura, formación, operaciones y respuesta ante incidentes. Antes de su incorporación a BP, Barriuso ha ocupado distintos cargos en el sector financiero y ha coordinado numerosas iniciativas sectoriales en el mundo de la ciberseguridad tales como 'WakingShark' o 'Market Wide Exercise'. Desde 2002, Barriuso imparte clases como profesor en el Máster de Seguridad y Auditoría de la Universidad Politécnica de Madrid.

El compromiso de la Alta Dirección. Ejercicio práctico de Gestión de Crisis en Mapfre

Sinopsis: Un Plan de Continuidad de Negocio puede considerarse completo cuando se hayan realizado pruebas de recuperación de la actividad y los resultados obtenidos se consideren satisfactorios y adecuados a los requerimientos del negocio. Plantear un ejercicio de Gestión de Crisis a la Alta Dirección supone un desafío cuyo resultado debe servir de impulso a la función de continuidad de negocio. Es una oportunidad que no se debe desaprovechar. Se presenta a los asistentes la forma en que la Subdirección General de Seguridad y Medio Ambiente de Mapfre, con el apoyo de PwC, ha realizado un ejercicio de gestión de crisis con el Comité de Crisis y Continuidad de Negocio Corporativo de Mapfre, diseñando un escenario realista, apoyado con contenidos multimedia, para conseguir que los miembros del Comité "entren en situación" desde el primer momento, se planteen las diferentes problemáticas a resolver y adopten las decisiones necesarias, eficientes y adecuadas para el control de la situación.

Ponentes:
Lionel Güitta Abellán es Subdirector de Continuidad de Negocio y Contingencia Informática en la Subdirección General de Seguridad y Medio Ambiente de Mapfre. Licenciado en Informática por la Universidad Politécnica de Madrid, Lead Implementer ISO 22301 por PECB, es asimismo Director de Seguridad Privada. Ha desarrollado la práctica totalidad de su carrera profesional en los ámbitos de las tecnologías de la información, seguridad de la información y continuidad de negocio en el Grupo Mapfre. Acumula una experiencia de más de 15 años en el diseño, desarrollo, implantación y realización de pruebas de planes de continuidad de negocio y contingencia informática, en el sector de seguros y en el sector bancario, tanto en España como a nivel internacional.

Juan José Míguez Iglesias es Socio del Área de Riesgos Tecnológicos de PwC. Cuenta con más de 16 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 Director

de Seguridad Privada acreditado por el Ministerio del Interior, 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, proyectos de prevención del fraude y revisiones de seguridad técnicas. Durante su trayectoria ha tenido la oportunidad de participar en numerosos simulacros de gestión de crisis y pruebas de recuperación de desastres.

Telefónica global: llegué, vi y vencí: estrategia de ciberinteligencia para la protección proactiva ante nuevas amenazas

Sinopsis: Telefónica Global, como pieza fundamental en la lucha contra el fraude y la protección de sus clientes Small Business y Gran Cuenta, está utilizando la solución *cloud* de ciberinteligencia Blueliv, que recolecta información fuera del perímetro de las empresas. En esta ponencia se mostrará el proyecto que han desarrollado conjuntamente blueliv y Telefónica para la recolección de información, tratamiento de la misma a través de tecnologías *Big Data* (grandes cantidades de información y diferentes tipos y estructuras de datos) y Business Security Intelligence (BSI) con el objetivo de obtener, de forma anticipada, información relativa a ciberriesgos y ciberamenazas para realizar una defensa inteligente y preventiva de los clientes de Telefónica.

Ponentes:

Pedro Pablo Pérez García es Responsable de Ciberseguridad de Telefónica Global. Ingeniero Superior y MBA por IESE, cuenta con las certificaciones CISSP, CISA, ITIL Service Manager e ISO2001 Lead Auditor. Actualmente desarrolla su carrera profesional como responsable de "CyberSecurity" en Telefónica a nivel global, siendo adicionalmente miembro del consejo de blueliv. Amplio conocedor de los distintos productos de seguridad del mercado, tanto de protección como de ataque, posee una experiencia de 20 años en seguridad informática.

Daniel Solís Agea es CEO y fundador de la compañía de ciberseguridad Blueliv. Visionario, lleva más de 20 años dedicados al desarrollo de una tecnología más segura con el objetivo de garantizar la continuidad de los negocios y la protección de los usuarios. Ingeniero en Telecomunicaciones, antes de crear Blueliv, ocupó puestos de responsabilidad en el área de ciberseguridad en las Naciones Unidas en Nueva York así como en KPMG y S21sec. Especialista reconocido a nivel internacional por sus contribuciones, tecnologías desarrolladas y experiencia en proyectos globales, Solís está certificado como ISO 27001 Lead Auditor acreditado por IRCA y es miembro activo de Aedel y creador de la distribución forense Ad-quiere.

Grabación de Pruebas de Continuidad de Negocio: Planificación, Realismo y Concienciación

Sinopsis: Repsol dispone de una ambiciosa estrategia en el ámbito de la continuidad de negocio, la cual le permite ser uno de los ejemplos a seguir en su sector a nivel mundial, como se desprende del análisis de la *International Association of Oil & Gas Producers* (OGP). Su Sistema de Gestión de Continuidad de Negocio de TI, certificado en ISO 22301, ha alcanzado un nivel de madurez que impulsa la mejora continua y la excelencia de su gestión. Para ello, la organización tiene un programa de despliegue de distintas iniciativas, entre las que destaca la búsqueda de elementos innovadores de mejora en la gestión de la continuidad de negocio. Es ahí donde se ha encontrado un elemento que aporta un valor añadido en el ámbito de la implicación y concienciación de toda la organización, desde la Alta Dirección, pasando por el personal involucrado en el sistema de gestión, hasta todas las partes interesadas receptoras de los servicios definidos en el alcance del sistema.

Ponentes:

Marcos Guasp, Gerente de Riesgos y Continuidad en el ámbito de Ciberseguridad y Riesgo Tecnológico de Repsol. Es Licenciado en Marina Civil y Piloto de la Marina Mercante. Tiene ocho años de experiencia en asuntos de Seguridad y Continuidad de Negocio, y es el Responsable en su compañía del Plan de Continuidad de TI a nivel internacional e integrante del Proyecto de Despliegue del Plan de Continuidad de Sedes a escala mundial. Es LA ISO22301, ISO 31000, ITIL, BCI y posgrado como Director Experto Profesional de Seguridad Integral.

Joaquín Castillón Colomina, Senior Manager Advisory Services de EY. Licenciado en Administración y Dirección de Empresas, Posgrado en Informática y Máster en seguridad TIC, dispone de más de quince años de experiencia en la actividad de asesoramiento en materia de sistemas de información, incluyendo Gestión de riesgos corporativos, tecnológicos y operacionales, Gestión de seguridad de la información, Estrategia de TI y Seguridad, Gobierno y Cumplimiento de TI, Privacidad de la Información y Gestión de Oficinas de Proyecto de Seguridad. Tiene también experiencia en proyectos internacionales de gran envergadura. Dispone de la certificaciones CGEIT, CISA, ITIL, ISO 22301 LA, ISO 27001 LA, OPST y SAP GRC (Risk Management, Process Control y Fraud Management).

TERCER MÓDULO, 24 DE ABRIL

09:00h.	Entrega de documentación
	Moderador: **Carlos Manuel Fernández Sánchez**, Gerente de TICs. Dirección Comercial de Certificación de Aenor.
09:30h.	Ponencia: **Grupo BBVA: despliegue de la 'securización' de cajeros de la red internacional.**
	Ponentes:
	Carlos Villaverde Clavero, Responsable de Sistemas de Prevención de Fraude. Departamento de Riesgo IT, Fraude y Seguridad. Grupo BBVA.
	Juan Jesús León Cobos, Director de Productos y Nuevos Desarrollos de GMV.
10:00h.	Coloquio
10:10h.	Ponencia: **Estrategia de Seguridad y SOC de Mutua Universal.**
	Ponentes:
	Josep María Ezcurra Tort, Director del Área de Servicios Informáticos de Mutua Universal.
	José Francisco Pereiro Seco, Director de Servicios de Seguridad de BT España.
10:40h.	Coloquio
10:50h.	Ponencia: **Security Tracking Lab: hacia una estrategia de protección ante amenazas físicas y lógicas.**
	Ponentes:
	Idoia Mateo Murillo. Directora Global de Riesgos Tecnológicos y Seguridad de Produbán. Grupo Santander.
	Carlos Moreno Durán, Director de Inteligencia y Análisis. Área Corporativa de Seguridad. Grupo Santander.
11:20h.	Coloquio
11:30h.	Pausa-café
	Moderador: **Ignacio Alamillo Domingo**, Director de Astrea, la Infopista Jurídica.
12:10h.	Ponencia: **La notificación de incidentes en la nueva normativa europea sobre protección de datos personales y su relación con las iniciativas regulatorias de la ciberseguridad.**
	Ponente: **Ricard Martínez Martínez**, Presidente de APEP (Asociación Profesional Española de Privacidad).
12:40h.	Coloquio
12:50h.	Ponencia: **¿Son legales en España todas las funcionalidades de los sistemas de seguridad TIC de mercado que se implantan en la organizaciones?**
	Ponente: **Paloma Llaneza González**, Abogada y Socia Directora de Razona Legaltech.
13:20h.	Coloquio
	Moderador: **José de la Peña Muñoz**, Director de Revista SIC.
13:30h.	Conferencia de clausura: **La articulación del uso legal de herramientas TIC para la investigación de conductas ilícitas en el marco de la colaboración entre Fuerzas y Cuerpos de Seguridad y CERTs.**
	Ponente: **Elvira Tejada de la Fuente**, Fiscal de Sala Coordinadora en Materia de Criminalidad Informática. Fiscalía General del Estado.
14:00h.	Coloquio
14:10h.	Almuerzo, fin de la tercera jornada y fin de Securmática 2014.

Grupo BBVA: despliegue de la 'securización' de cajeros de la red internacional

Sinopsis:
El despliegue de una solución de *end-point-security* en una red de cajeros automáticos presenta de por sí importantes desafíos. Cuando, como sucede en BBVA, resulta necesario gestionar la seguridad de más de 20.000 cajeros desplegados en distintos países de forma coordinada, el reto es enorme. La conocida expresión "piensa globalmente y actúa localmente" plantea cuestiones interesantes: ¿Cómo pueden adaptarse las políticas de seguridad a distintos países con distintas amenazas? ¿Cómo se pueden tener en cuenta las diversas necesidades regulatorias? ¿Cuál es la manera más adecuada de centralizar alarmas e informes? El despliegue de un producto específico para la seguridad en redes de autoservicio financiero permite dar solución a situaciones tan delicadas y tan dispares como la importancia crucial de la disponibilidad, las limitaciones derivadas de la antigüedad de los parques instalados, la finalización del soporte de Windows XP o la necesidad de establecer controles compensatorios del factor humano.

Ponentes:
Carlos Villaverde Clavero, Responsable de Sistemas de Prevención de Fraude. Departamento de Riesgo IT, Fraude y Seguridad. Grupo BBVA. Ingeniero Superior Industrial por la Universidad Politécnica de Cataluña. Máster en Seguridad en Tecnologías de la Información por la Salle/Universidad Ramón Llull, cuenta con las certificaciones CISSP, PMP y CCNA. Inició su carrera profesional en HP, donde desempeñó varios puestos: Responsable de Cuentas, Responsable de Proyectos de Cumplimiento Normativo, Líder del Servicio de Gestión de Identidades en Ingeniería de Producción, Account Security Officer y Transition and Transformation Manager para Banca. Ha trabajado en el Banco de España como miembro del equipo de Seguridad IT, centrado en proyectos del Sistema Europeo de Bancos Centrales en las áreas de PKI, Plataformas de Operaciones de Mercados y Gestión de Valores. Actualmente es el Responsable de los equipos de Sistemas de Prevención de Fraude y Dirección Técnica de Proyectos de IT Risk Fraud & Security en Grupo BBVA.

Juan Jesús León Cobos, Director de Productos y Nuevos Desarrollos de GMV. Ingeniero Aeronáutico por la UPM, PDD por el IESE y CISM, Juan Jesús 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 EE.UU. En el año 1997 se incorporó al grupo El Corte Inglés, donde llegó a ser Jefe del Área de Desarrollo para sus Centros Comerciales. En el año 2000 se incorporó al grupo BBVA donde contribuyó como Director de Desarrollo a la puesta en producción del banco Uno-e. En junio de 2001 regresó a GMV.

Estrategia de Seguridad y SOC de Mutua Universal

Sinopsis:
Mutua Universal, una de las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social (MATEPPSS) más relevantes a nivel estatal, está en proceso de implantación de una nueva estrategia de seguridad de la información con el objetivo de abordar los nuevos retos que aparecen en el horizonte. En la conferencia se expondrán los antecedentes y motivaciones que han llevado a la definición de esta estrategia y los criterios directores de la misma. Para ello, Mutua Universal se apoya en BT como integrador y proveedor de servicios gestionados de seguridad desde su CySOC, así como en fabricantes de tecnologías líderes como Cisco. Para finalizar, la entidad colaboradora expondrá los componentes tecnológicos y detalles de la solución diseñada para su cliente Mutua Universal.

Ponentes:
Josep María Ezcurra Tort ocupa el cargo de Director de Servicios Informáticos de Mutua Universal dentro de la Dirección de Tecnología y Sistemas de Información, y tiene cerca de 18 años de experiencia en servicios TIC y seguridad informática, tanto desde la visión de la provisión de servicios y proyectos, como desde la visión del cliente final y receptor de dichos servicios. Tras 12 años vinculado a la empresa T-Systems llevando a cabo funciones de gestión de áreas de ingeniería y de servicios TIC, en la actualidad lleva 5 años vinculado a la empresa Mutua Universal.

José Francisco Pereiro 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 como las conferencias. Dispone de varias de las principales certificaciones de seguridad como CISA, CISM, CISSP, CSSA entre otras.

Security Tracking Lab: hacia una estrategia de protección ante amenazas físicas y lógicas

Sinopsis:
Proporcionar estrategias adecuadas a la anticipación debe ser uno de los ejes vehiculares de las definiciones de los programas de seguridad, por lo que es vital dotarse de soluciones integrales y Analisis de Riesgos Dinámicos a la hora de diseñar la capa de protección. Para ello disponemos nuestro foco en el desarrollo e implementación de estrategias que complementen las medidas de seguridad actualmente definidas con la aplicación de tendencias innovadoras de vigilancia tecnológica en internet, inteligencia y Analisis para la mitigación y anticipación de riesgos operacionales en el sector financiero. Líneas de actuación, de máximo nivel, que no solo nos aseguren una protección frente a las amenazas tradicionales físicas, sino también frente aquellas que afectan a la seguridad lógica y ante una eventualidad, permitan y garanticen una adecuada gestión de los ciberincidentes, reduciendo los tiempos de exposición. Este diseño pretende fortalecer un entorno colaborativo entre las diferentes áreas que participan en la toma de decisiones con un fin evidente: garantizar los procesos de negocio.

Ponentes:
Idoia Mateo Murillo, Directora Global de Riesgos Tecnológicos y Seguridad de Produban. Grupo Santander. Lleva 19 años de trayectoria profesional en el mundo de la seguridad y los riesgos tecnologicos. Los ocho últimos en su actual cargo en Produban, la empresa de gestión de infraestructuras del Grupo Santander, con reporte de todos los responsables de Riesgos Tecnologicos 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 Audit & Compliance, Seguridad, Gestión de la Contingencia 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 Tecnologicos 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.

Carlos Moreno Durán, Director de Inteligencia & Análisis del Área Corporativa de Seguridad del Grupo Santander. Licenciado Superior, Diplomado en Ciencias Policiales y Director de Seguridad. Su carrera profesional se ha desarrollado dentro los Servicios de Información e Inmigración del Cuerpo Nacional de Policía, tanto en el ámbito nacional como internacional, habiendo residido y desplazado a Francia, México, Mauritania y Pakistán. En el Grupo Santander centra su tarea en Brand Protection, Infraestructuras Críticas, Análisis y Evaluación del Riesgo Seguridad, Seguridad para Expatriados e Innovación en Seguridad. Forma parte del Comité Técnico en materia de Ciberseguridad de la Fundación ESYS. Entre los diversos cursos y foros a los que

asistió, tiene el Máster de Director Internacional de la Seguridad, Second Mid Level – FRONTEX, y ha realizado diferentes cursos especializados en materia de Inteligencia (Comisaría General de Información-Madrid, Universidad Iberoamericana-México). Ha participado como ponente en diferentes foros y reuniones nacionales e internacionales relacionados con la materia, siendo profesor de varios máster y cursos especializados (Universidad de Comillas-ICADE, Universidad Europea de Madrid).

La notificación de incidentes en la nueva normativa europea sobre protección de datos personales y su relación con las iniciativas regulatorias de la ciberseguirdad

Sinopsis:
La regulación europea sobre protección de datos personales se halla actualmente en una situación de permanente transición. La modificación del llamado Paquete Telecom introdujo innovaciones significativas en materia de seguridad, y especialmente en lo relativo a la notificación de quiebras o incidentes de seguridad. Se trata de una obligación de contenido complejo, sometida a distintas posibilidades de interpretación y susceptible de generar serios problemas de relación con reguladores y usuarios. La Propuesta de Reglamento General de Protección de Datos propone una extensión o generalización de esta obligación y cuando ésta apenas alcanza a su primer trámite ante el Parlamento Europeo, se agiliza la tramitación de la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión. Este complejo entramado obliga a determinar con precisión el concepto de incidente de seguridad, los modelos de gestión de los mismos, los sujetos obligados y las consecuencias.

Ponente:
Ricard Martínez Martínez, Data Protection Officer en la Universitat de València y Presidente de la Asociación Profesional Española de Privacidad. Anteriormente ha sido responsable del Área de Estudios de la Agencia Española de Protección de Datos. Doctor en Derecho por la Universitat de València, ha dedicado su investigación al estudio del derecho fundamental a la protección de datos y a distintas cuestiones relacionadas con las repercusiones de las tecnologías de la información y las comunicaciones en la vida privada. Es autor de monografías dedicadas a esta materia ("Tecnologías de la Información, Policía y Constitución", "Una aproximación crítica a la autodeterminación informativa") y ha participado como autor o coordinador en distintos comentarios al Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, y coordinador de las monografías "Derecho y redes sociales" y "Derecho y *Cloud Computing*". Colabora con distintas Universidades como docente en estudios de grado (Universitat Oberta de Catalunya UOC) o de posgrado (Universitat de València, Universidad Carlos III, UOC, Universidad de Murcia y Universidad Politécnica de Valencia).

¿Son legales en España todas las funcionalidades de los sistemas de seguridad TIC de mercado que se implantan en organizaciones?

Sinopsis:
Las posibilidades que nos brindan los sistemas de monitorización de la seguridad fueron pensadas por un técnico, dios de su universo, en donde las únicas reglas aplicables eran las del código orientadas a cumplir, con mayor o menor eficiencia, con la función de securizar un sistema. Si se contemplan normas externas al mejor funcionamiento técnico de la herramienta, éstas suelen estar pegadas a una realidad social y legal ajena a nuestro sistema de valores. Cuando las herramientas y sus funcionalidades chocan con personas y organizaciones en entornos legales continentales europeos, el escenario se complica. Por eso, es esencial que, a la capa de aplicaciones y personas que los usan, se le dé el barniz del análisis legal.

Ponente:
Paloma Llaneza González, Abogada y Socia Directora de Razona Legaltech. Dispone de la certificación CISA de ISACA y es experta en seguridad de la información. Editora de diversos estándares de seguridad (IEC/ISO 27004:2009, ESI TS on Registered E-Mail, y CEN CWA on Data Protection Good Practices), preside AEDEL (Asociacion Española de Desarrollo de las Evidencias Electrónicas). Como coordinadora del Grupo Ad-Hoc del SC27 de AENOR sobre evidencias electrónicas, ha participado en el desarrollo de dos normas nacionales, la 71505 sobre el sistema de gestión de evidencias, y la 71506 sobre análisis forense. Actualmente está participando como experta en seguridad en diversos grupos internacionales, en concreto, en el Mandato de la Comisión UE 460 sobre racionalización de los estándares de firma electrónica, siendo editora de, entre otros, las normas europeas EN 319 403 "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers" y EN 319 401 "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

CONFERENCIA DE CLAUSURA

La articulación del uso legal de herramientas TIC para la investigación de conductas ilícitas en el marco de la colaboración entre Fuerzas y Cuerpos de Seguridad y CERTs

Sinopsis:
Como bien señala la Estrategia Nacional de Ciberseguridad, los conocimientos y experiencias adquiridos en el ámbito de la ciberseguridad pueden y deben ser aprovechados para articular instrumentos legales aptos para hacer frente al uso irregular y/o con fines delictivos de las nuevas tecnologías, así como para definir tipos penales adecuados para la prevención y represión de estas manifestaciones criminales. A su vez, la potencialidad de las TICs como herramientas de investigación criminal aporta un valor añadido a la actuación frente a la ciberdelincuencia, pero la incorporación al proceso judicial de los resultados obtenidos exige que el uso de dichas herramientas respete los derechos fundamentales de las personas y las garantías propias del Estado de Derecho. La colaboración de los CERTs y de los operadores de ciberseguridad del sector privado con las Fuerzas y Cuerpos de Seguridad y con las autoridades judiciales y el Ministerio Fiscal constituyen un factor esencial para el logro de estos objetivos y, en definitiva, para la efectiva persecución y sanción de los ciberdelitos.

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

Más de 7.000 expertos han pasado por Securmática, un congreso que con sus 24 ediciones ya celebradas, es el foro de intercambio de experiencias en ciberseguridad por excelencia.

•• Premios SIC 2014 y Cena de la Seguridad

En coincidencia con la XXV edición de Securmática, tendrá lugar el acto de entrega de los XI 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 décima edición de los Premios SIC.

Fechas y lugar de celebración

SECURMÁTICA 2014 tendrá lugar los días 22, 23 y 24 de abril de 2014 en el hotel NOVOTEL. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2014 recibirán las carpetas de congresista con el programa oficial y toda la documentación –papel y CD-ROM– referente a las ponencias.
- Almuerzos y cafés.
- Cena de la Seguridad y entrega de los XI Premios SIC (23 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 24 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 22 ☐ Módulo 2 Día 23 ☐ Módulo 3 Día 24 ☐ Deseo inscribirme a SECURMÁTICA 2014 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**