SECURMÁTICA

2016
26.27.28 abril

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

CISOs:

¿Qué le está pasando a la ciberseguridad?

www.securmatica.com

PROGRAMA

Tendrá lugar en Madrid los días 26, 27 y 28 de abril

Securmática 2016: ¿qué le está pasando a la ciberseguridad?

Las actividades asociadas con la ciberseguridad crecen en todos los sectores a mayor velocidad que la estabilización de requisitorias de control y cumplimiento legal, aunque a menor ritmo que la galopante tranformación digital en red que va conquistando día a día todos los espacios.

Este hecho ha generado desajustes (de calidad y cantidad) en el mercado de especialistas, ha dejado en evidencia la vergonzosa falta de estrategia de los gestores de aquellas compañías proveedoras de servicios que hoy pretenden sumarse atropelladamente a la "moda" de la ciberseguridad, ha provocado la insatisfacción de muchas organizaciones usuarias que optaron por una externalización ateniéndose solo al precio (lo que acarrea una degradación de la calidad de servicio), está fomentando la aparición de emprendedores ajenos a la gestión de riesgos y desconocedores de la oferta tecnológica ya existente, y ha propiciado una confusión entre las posibilidades que ofrece la seguridad técnica de calidad para garantizar los derechos de las personas y los límites que han de fijarse para no violar la privacidad sin por ello desatender la protección.

Las organizaciones de estados y los gobiernos han ido tomando estos años decisiones trascendentales que empiezan a anudarse en forma de legislación, ya en vigor o a punto de publicarse (Reglamento General de Protección de Datos y directiva NIS), y en forma de normativas sectoriales y/o específicas. Especial mención merece el todavía por ejecutar desarrollo de la Ley de Seguridad Privada española para reglamentar la actividad de la seguridad informática.

Y en este marco, las entidades privadas y las administraciones públicas, ya por requisitos de mercado y actividad, ya por requisitos de cumplimiento, han tenido que ir formalizando estructuras orientadas a la gestión de los riesgos de ciberseguridad, teniendo presente que el futuro inmediato, y a efectos globales, se va a definir por la obligatoriedad de notificar ataques sufridos y exposición y pérdida de información (datos personales o no), hecho que será uno de los grandes catalizadores del cambio.

El programa que tiene usted en sus manos pretende arrojar luz sobre lo que está pasando en el campo de la ciberseguridad, incluyendo lo que muchas entidades están haciendo para proteger su patrimonio y los datos personales que tratan, y para colaborar en la defensa de los intereses de la sociedad.

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 actividad.

Copatrocinadores

Aiuken Solutions · Blueliv. · BT · Deloitte. · EY Building a better working world

gmv Innovating Solutions · IBM · KPMG · pwc · S2 Grupo · S21sec Committed to cybersecurity

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

PRIMER MÓDULO, 26 DE ABRIL

08:45h. Entrega de documentación
09:15h. Ceremonia de apertura
10:00h. **Conferencia de inauguración**
10:20h. Ponencia introductoria:
Ley de Seguridad Nacional y Ciberseguridad.
Ponente: **Joaquín Castellón Moreno**, Director Operativo. Departamento de Seguridad Nacional. Gabinete de la Presidencia del Gobierno.
10:35h. Ponencia: **La interpretación del Ministerio Público de los Delitos contra los datos y sistemas informáticos y los delitos de acceso ilegal a sistemas e interceptación de datos.**
Ponente: **Elvira Tejada de la Fuente**, Fiscal de Sala. Coordinadora en materia de lucha contra la criminalidad informática.
11:05h. Coloquio
11:10h. Pausa-café
11:40h. Ponencia: **El CISO de los Operadores Críticos en el modelo PIC.**
Ponente: **Fernando J. Sánchez Gómez**, Director del Centro Nacional para la Protección de las Infraestructuras Críticas, CNPIC. Secretaría de Estado de Seguridad.
12:10h. Coloquio
Moderador: **Francisco Javier García Carmona**, Experto en Ciberseguridad.
12:15h. Ponencia: **Información de fuente público-privada: el registro nacional de ciberataques.**
Ponente: **Javier Candau Romero**, Jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional, CCN.
12:45h. Coloquio
12:50h. Ponencia: **Ley de Seguridad Privada: bases para un reglamento de actividades de seguridad informática.**
Ponente: **Esteban Gándara Trueba**. Comisario Jefe de la Unidad Central de Seguridad Privada. Policía Nacional. Secretaría de Estado de Seguridad. Ministerio del Interior.
13:20h. Coloquio
13:25h. Ponencia: **CERTSI: sectorización, verticalización y alineamiento de servicios en base a requisitos regulatorios.**
Ponentes:
Miguel Rego Fernández, Director General de INCIBE, Instituto Nacional de Ciberseguridad.
Alberto Hernández Moreno, Director de Operaciones de INCIBE, Instituto Nacional de Ciberseguridad.
13:55h. Coloquio
14:00h. Almuerzo
Moderador: **Jorge Dávila Muro**, Profesor Titular. Director del Laboratorio de Criptografía LSIIS. Facultad de Informática-UPM.
16:00h. Ponencia: **Formas de colaboración efectiva con el Centro de Cibercrimen Europeo y las empresas de ciberseguridad.**
Ponentes:
José Durán Martín. J-CAT Liaison Officer (Spain) European Cybercrime Centre.
José Alemán Hernández. S21sec Service Marketing Manager. Law Enforcement and Defense Line of Business Manager.
16:30h. Coloquio.
16:35h. Ponencia: **Seguridad como palanca del negocio digital.**
Ponentes:
Luis Varela Negreira, Responsable del Equipo de eCrime y Security Analytics. Equipo de Ciberseguridad. Caixabank.
Ramón Vicens Lillo, Vicepresidente de Threat Intelligence. Blueliv.
17:05h. Coloquio
17:10h. Fin de la primera jornada

Conferencia de inauguración

Ley de Seguridad Nacional y Ciberseguridad

Sinopsis: La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, contempla la ciberseguridad como uno de los ámbitos de especial interés de la Seguridad Nacional, por resultar básico para preservar los derechos y las libertades y el bienestar de los ciudadanos, así como para garantizar el suministro de los servicios y recursos esenciales. La Ley establece la obligación de las Administraciones Públicas de establecer mecanismos de coordinación e intercambio de información, de forma especial respecto de los sistemas de vigilancia y alerta ante posibles riesgos y amenazas. Además, se regula la colaboración privada, de modo que las entidades privadas, cuando las circunstancias lo aconsejen y, en todo caso, cuando operen servicios esenciales e infraestructuras críticas, colaboren con las Administraciones Públicas. El Gobierno desarrollará reglamentariamente esta colaboración. Respecto de la gestión de crisis, el Sistema de Seguridad Nacional que dirige el Presidente del Gobierno asistido por el Consejo de Seguridad Nacional, deberá contar con los órganos de coordinación y enlaces necesarios con todas las Administraciones del Estado a los efectos de la detección, valoración y respuesta frente a las ciberamenazas. Se contempla la posibilidad de que la contingencia pueda derivar en una situación de interés para la Seguridad Nacional debido a la gravedad, dimensión, urgencia y transversalidad de las medidas precisadas para su resolución. En este caso es preciso reforzar y sincronizar de manera óptima la cooperación de las autoridades competentes bajo la dirección del Sistema de Seguridad Nacional.

Ponente:
Joaquín Castellón Moreno se incorporó al Departamento de Seguridad Nacional de la Presidencia del Gobierno en el momento de su creación, en el verano de 2012, donde ocupa el puesto de Director Operativo. Durante este tiempo ha coordinado la Comisión Técnica que elaboró la Estrategia de Seguridad Nacional 2013 y los trabajos de elaboración de la Estrategia de Ciberseguridad Nacional, de la Estrategia de Seguridad Marítima Nacional y de la Estrategia de Seguridad Energética Nacional. Es, además, vocal del Consejo Nacional de Ciberseguridad y del Consejo Nacional de Seguridad Marítima. Igualmente, ha participado en la elaboración de la Ley de Seguridad Nacional. Es Oficial del Cuerpo General de la Armada y ha ocupado numerosos destinos a bordo de unidades de La Flota, el Estado Mayor de la Armada, el Ministerio de Defensa y el Instituto Español de Estudios Estratégicos.

La interpretación del Ministerio Público de los delitos contra los datos y sistemas informáticos y los delitos de acceso ilegal a sistemas e interceptación de datos

Sinopsis: La evolución constante de las TIC, junto a grandes ventajas, genera también grandes riesgos al facilitar a los delincuentes una mayor capacidad para atentar contra los derechos y libertades de los ciudadanos y el interés general. Por ello, los Estados y la Comunidad Internacional trabajan para ofrecer soluciones legales adaptando a dicho fin el ordenamiento jurídico a las necesidades que plantea la actuación frente a estas nuevas manifestaciones criminales. A este propósito obedece la Directiva 2013/40/UE sobre ataques a los sistemas de información cuyo objeto es avanzar en la definición uniforme, en los Estados Miembros, de conductas delictivas y sus respectivas sanciones como medio para potenciar y reforzar la persecución y sanción penal de estos comportamientos en el territorio de la Unión. De acuerdo con ese planteamiento el legislador español, con ocasión de la reforma del Código Penal por LO 1/2015, acaba de implementar en nuestro ordenamiento dicha Directiva europea lo que ha determinado la modificación de algunas figuras delictivas como el acceso ilegal a sistemas o los daños informáticos y también la tipificación de otras nuevas como la interceptación ilegal o el abuso de dispositivos.

Ponente:

Elvira Tejada de la Fuente es Fiscal de Sala Coordinadora en materia de lucha contra la 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 Corresponsalía Nacional para Eurojust en materia de terrorismo.

El CISO de los Operadores Críticos en el modelo PIC

Sinopsis: El nuevo Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC) adoptado en febrero de 2016, recoge las medidas a implantar en cada nivel de activación del mismo por los diferentes agentes participantes. Al igual que el Plan de Prevención y Protección Antiterrorista, este plan está clasificado.

El PNPIC supone la culminación del Sistema de Protección de Infraestructuras Críticas emanado de la Ley 8/2011, PIC, y la implantación de todas las herramientas de planificación previstas en dicha norma. Así mismo significa, como principal novedad, la puesta en marcha de medidas operativas concretas sobre dos presupuestos fundamentales: 1) La inclusión de la figura del operador crítico como partícipe del sistema de seguridad nacional, y 2) La inclusión de medidas de ciberseguridad, dando contenido al concepto de *seguridad integral*.

En el actual marco de actuación, que sigue la estela iniciada por la Ley 8/2011, el CISO, o el responsable TI de las organizaciones identificadas como operadores críticos, tiene reservado un rol de la mayor importancia en el desarrollo del Sistema PIC, que se abordará en la ponencia.

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.

Moderador:

Francisco Javier García Carmona es un destacado experto en Ciberseguridad. Maestro Industrial e Ingeniero de Telecomunicaciones. Dispone de un Máster en Administración y Dirección de empresas, ha realizado el Curso Superior de Dirección de Seguridad de ICAI y es Director de Seguridad homologado por el Ministerio del Interior. Tiene una larga experiencia profesional en empresas y por cuenta propia en áreas como automatismos, investigación aplicada, telecomunicaciones, desarrollo de software de protección y gestión de riesgos de seguridad de la información. Durante años ocupó el cargo de Director de Seguridad de la Información y las Comunicaciones en Iberdrola.

Información de fuente público-privada: el registro nacional de ciberataques

Sinopsis: El reto del Centro Criptológico Nacional (CCN) para 2016 es alcanzar una visión global de los incidentes de ciberseguridad sufridos por las Administraciones Públicas, los sistemas clasificados y las empresas de interés estratégico para el país. El RD 951/2015, de modificación del RD 3/2010, que regula el ENS, obliga a las AAPP a notificar los incidentes que tengan un impacto significativo y permite al CCN-CERT realizar investigaciones con más profundidad. Para cumplimentar este mandato, durante 2015 se pusieron en marcha dos grandes proyectos con los que el CCN pretende favorecer la gestión de ciberincidentes, la coordinación y la comunicación entre todas las organizaciones. Se trata de LUCIA y REYES basados, respectivamente, en herramientas de código abierto como RT-IR y MISP. En este 2016 se espera conectar ambos sistemas y, de este modo, obtener una visión conjunta, tanto desde el punto de vista del atacante, como de la víctima. Estamos pues, ante un proyecto estratégico para la ciberseguridad nacional, cuyo éxito dependerá de las organizaciones usuarias y de la confianza y reciprocidad que se genere. De conseguirlo, habremos sentado entre todos las bases para una defensa activa y eficiente del ciberespacio español.

Ponente:

Javier Candau Romero es Jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional. Teniente Coronel de Artillería e 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, Cursos CCN-STIC, 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), el desarrollo de la herramienta de análisis de riesgos PILAR, la supervisión de acreditación de sistemas y la realización de auditorías de seguridad, así como todas las acciones derivadas del Esquema Nacional de Seguridad (ENS). Tiene más de 16 años de experiencia en todas estas actividades y también es Responsable de la Capacidad de Respuesta ante Incidentes gubernamental (CCN-CERT).

Ley de Seguridad Privada: bases para un reglamento de actividades de seguridad informática

Sinopsis: La Ley de Seguridad Privada reconoce a la seguridad informática como una actividad compatible con las definidas en el ámbito de la Seguridad Privada; pero no la define ni especifica qué actividades deben entenderse como de seguridad informática y qué personas físicas y jurídicas pueden llevarlas a cabo, ni cómo ni dónde. Para tales fines, en la mencionada Ley se prevé un desarrollo reglamentario. En la conferencia, el Comisario Jefe de la Unidad Central de Seguridad Privada expondrá los puntos de interés que el Ministerio del Interior, que es el competente para llevar a cabo el proyecto, considera que deberían contemplarse a la hora de regular la actividad de la ciberseguridad.

Ponente:

Esteban Gándara Trueba es Comisario del Cuerpo Nacional de Policía y Jefe de la Unidad Central de Seguridad Privada. Licenciado en Derecho (UCM), Licenciado en Ciencias Policiales (Universidad de Salamanca), Diplomado en Criminología (Universidad de Barcelona), Diplomado en Investigación Privada (Universidad de Barcelona), Diplomado en Dirección y Gestión de la Seguridad (Universidad Francisco de Vitoria) y Diplomado en Dirección y Planificación Estratégica (Centro de Altos Estudios Policiales), Gándara Trueba tiene una larga trayectoria en el Cuerpo Nacional de Policía en donde ha ejercido el mando de diversas Unidades Policiales de Investigación, ha sido Jefe del Servicio de Apoyo Técnico en la Comisaría General de Policía Judicial, Jefe de la Brigada de Policial Judicial de Zaragoza, Jefe de las Comisarías de Policía de Fuenlabrada y Tetuán (Madrid) y Vocal del Consejo asesor de la Policía. Es autor de varios libros, articulista en revistas especializadas, conferenciante en cursos de especialización y actualización de la Policía Nacional, Guardia Civil, Policías Locales, Policías Extranjeras, Seguridad privada, Carrera Judicial y Fiscal, Secretarios Judiciales, Periodistas y Universidades. Participa, además, en diversos grupos de trabajo, nacionales y extranjeros, relativos a aspectos metodológicos, preparación de legislación internacional y nacional y proyectos de trabajo en materias policiales.

CERTSI: sectorización, verticalización y alineamiento de servicios en base a requisitos regulatorios

Sinopsis: El nuevo Plan Nacional de Infraestructuras Críticas, así como la próxima aprobación de la Directiva NIS, hacen necesario trabajar en la potenciación de las capacidades actuales del CERT de Seguridad e Industria (CERTSI). La evolución de las capacidades de detección y la especialización y sectorización en la prestación de servicios públicos son requisitos obligatorios para garantizar una respuesta adecuada al previsible incremento del número y tipo de amenazas. En los dos últimos años, el número de incidentes de ciberseguridad que el CERTSI ha gestionado se ha duplicado, tendencia que se prevé continúe para este año y el futuro más próximo, lo que viene a reforzar aún más la necesidad de dicha potenciación y especialización de capacidades. Recogiendo esta necesidad, el CERTSI ya dispone de un Plan ambicioso para la obtención de estas capacidades.

Ponentes:

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 las 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. 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 en esta firma.

Alberto Hernández Moreno, Director de Operaciones de INCIBE desde febrero de 2014; es Ingeniero Superior de Telecomunicaciones por la Escuela Técnica Superior de Ingenieros en Telecomunicaciones de la Universidad Politécnica de Madrid. Alberto Hernández cuenta con una dilatada trayectoria profesional de más diecisiete años en el ámbito de la ciberseguridad y la ciberdefensa, habiendo trabajado en empresas destacadas del sector como INDRA e ISDEFE. A su formación académica se añaden certificaciones especializadas en el ámbito de la ciberseguridad y las Tecnologías de la Información y las Comunicaciones, como CISA, CISSP, CSFI-DCOE y Director de Seguridad por el Ministerio del Interior entre otras, así como formación en capacidades directivas en diferentes escuelas de negocio. Previa incorporación a INCIBE y como Jefe de Área de Ciberdefensa en Isdefe, Alberto Hernández formó parte del equipo responsable del diseño y puesta en marcha del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

Moderador:

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

Formas de colaboración efectiva con el Centro de Cibercrimen Europeo y las empresas de ciberseguridad

Sinopsis: Esta contribución estará a cargo de S21sec, única empresa de origen español y con gran proyección internacional, que tiene un acuerdo de colaboración con el Centro del Cibercrimen Europeo en materia de ciberseguridad, de y un representante de la Guardia Civil en el EC3, el Centro del Cibercrimen Europeo con sede en Europol, en La Haya. Se aportarán detalles de cómo articular la colaboración entre el Centro del Cibercrimen Europeo y las empresas de Ciberseguridad, al tiempo que se responderá a cuestiones tales como: ¿qué pueden aportar las empresas a Europol? ¿Qué es importante a la hora de establecer una colaboración efectiva? Se expondrá un reciente caso de éxito basado en dicha colaboración.

Ponentes:

José Durán Martín es Comandante de la Guardia Civil, Institución a la que representa en el Grupo de Acción Conjunta contra la Ciberdelincuencia (J-CAT) de Europol. Cuenta con más de diecisiete años de experiencia profesional, desarrollada siempre en los ámbitos de la investigación policial, análisis de inteligencia, y en el campo de la colaboración policial internacional. Ha realizado distintos cursos de carácter profesional, como el Curso Superior de Información, Curso de Liderazgo de Equipos Conjuntos de investigación, Curso de Inteligencia Prospectiva contra el Crimen Organizado, etc. Además, es Máster en Seguridad, Máster en Estudios sobre Terrorismo y Máster en Seguridad Informática.

José Alemán Hernández es experto en ciberseguridad, y cuenta con más de quince años de experiencia en el sector. Actualmente es responsable de la línea de negocio dirigida a las Fuerzas del Orden y Defensa, tanto para España como para Europa, y Service Marketing Manager en S21sec, además es el enlace entre S21sec y el Centro del Cibercrimen Europeo. Fue Subdirector del Centro Nacional de Excelencia en Ciberseguridad, proyecto puesto en marcha por la Dirección General de Home Affairs de la Comisión Europea en 2009 para dotar a los países miembros de ayudas para la creación de Centros Nacionales de Excelencia en Ciberseguridad, con el objetivo de formar la red europea de centros dedicados a la formación y desarrollo tecnológico para la lucha coordinada contra el fenómeno creciente de la cibercriminalidad. En los últimos años ha sido profesor del Máster en Ciberseguridad de Next International Business School y del Máster de Seguridad de la Información de la Universidad de Deusto.

Seguridad como palanca del negocio digital

Sinopsis: En el ámbito financiero, las compañías europeas están afrontando el reto ante nuevas ciberamenazas que rodean las tecnologías del mundo digital, concretamente los entornos móviles. La ponencia explicará cómo Caixabank ha adaptado sus ciclos de desarrollo y de requisitos de seguridad para tratar estas nuevas amenazas manteniendo y preservando sus necesidades de negocio.

En este proceso de adaptación, el equipo de seguridad la información de Caixabank y Blueliv han colaborado en el proceso de identificación de vulnerabilidades en aplicaciones, colaboración con los proveedores y desarrolladores en la mitigación de las mismas, y como producto del análisis continuado de aplicaciones, se ha elaborado un conjunto de guías de buenas prácticas para el desarrollo seguro de aplicaciones móviles en el sector financiero con aplicación en el negocio digital.

Gracias a este proceso se han fortalecido los procesos de 'securización' en aplicaciones móviles, pudiendo dar respuesta a las necesidades del nuevo negocio de forma segura.

Ponentes:

Lucas Varela Negreira, Responsable del equipo de eCrime y Security Analytics. Equipo de Ciberseguridad de Caixabank, además de Arquitecto de Ciberseguridad dentro del equipo de seguridad de información de la Entidad. Su trabajo incluye la aplicación de inteligencia para la detección temprana de amenazas, el estudio de la eficiencia dentro de los procesos de Incident Response y el estudio sobre el *malware* bancario. Todo ello aplicando la metodología de la industrialización, "lessons learned" y estableciendo ciclos de mejora continuos.

Ramón Vicens Lillo, Vicepresidente de Threat Intelligence. Blueliv. Cuenta con más de una década de experiencia en ciberseguridad. Como VP de Threat Intelligence de Blueliv, Ramón Vicens dirige diversas investigaciones en profundidad sobre inteligencia de amenazas y fraude. Antes de incorporarse a Blueliv trabajó en compañías internacionales como BDO y One eSecurity. Es experto en *honeypots/nets*, gestión de incidencias, forenses, análisis de *malware*, ingeniería inversa y en tendencias de ciberataques. Es ingeniero de telecomunicaciones y posee un máster en seguridad, así como diversas certificaciones en seguridad.

SEGUNDO MÓDULO, 27 DE ABRIL

09:00h. Entrega de documentación
Moderador: **Paloma Llaneza González**, Socio Director en Razona LegalTech.

09:30h. Ponencia: **Bankia, fraude tecnológico en canales digitales: realidad vs regulación.**
Ponentes: **Vicente Moscardó Gil**, Director de Seguridad Informática de Bankia.
Israel Hernández Ortiz, Socio. Riesgos Tecnológicos. PwC.

10:00h. Coloquio

10:05h. Ponencia: **Aquae Security: Estrategia corporativa de uso seguro de servicios Cloud.**
Ponentes: **Eduardo Di Monte**, Security & Business Continuity Director. Aquae Security.
Juan Miguel Velasco López-Urda, CEO. Aiuken Solutions.

10:35h. Coloquio

10:40h. Ponencia: **Kill chain: a la búsqueda y captura del enemigo.**
Ponentes: **Carles Solé Pascual**, Director de Seguridad de la Información. Caixabank.
Vicente de la Morena Baena, Responsable Comercial de Grandes Empresas. Unidad de Seguridad de IBM.

11:10h. Coloquio

11:15h. Pausa-café
Moderador: **Román Ramírez Giménez**, fundador y miembro del equipo de Dirección de Rooted CON.

11:45h. Ponencia: **Banco Sabadell: estrategia de seguridad en el ciclo de vida de desarrollo de aplicaciones.**
Ponentes: **Santiago Minguito Santos**, Director Seguridad de la Información, Regulación y Prevención de Fraude. Banco Sabadell.
Xavier Gracia Lacalle, Director de CyberSOC. Deloitte.

12:15h. Coloquio

12:20h. Ponencia: **Banco Santander: Cyber Security Management Model.**
Ponentes: **Idoia Mateo Murillo**, Chief Operational Risk Officer Global de Produban (Banco Santander).
Julio San José Sánchez, Socio en la aplicación de la práctica de gestión de riesgos tecnológicos al sector financiero. EY.

12:50h. Coloquio

12:55h. Ponencia: **La transformación digital de la lucha contra el fraude: estrategias de ataque a la rentabilidad de las acciones de la delincuencia organizada.**
Ponente: **Santiago Moral Rubio**, Global Head Cybersecurity & Digital Trust. Grupo BBVA y Doctor en Análisis y Gestión de Riesgos de Ciberseguridad por la Universidad Rey Juan Carlos.

13:25h. Coloquio

13:35h. Almuerzo
Moderador: **Carlos Manuel Fernández Sánchez**, Gerente de TICs. Evaluación de la Conformidad. Dirección Comercial de Certificación. AENOR.

16:15h. Ponencia: **Retos e Iniciativas de Seguridad en la Dirección General de Tráfico.**
Ponentes: **Jesús Cuadrado García de la Calera**, Jefe de Explotación, Soporte y Servicios en la Gerencia de Informática de la Dirección General de Tráfico.
José Francisco Pereiro, Director de Servicios de Seguridad de BT Iberia.

16:45h. Coloquio

16:50h. Ponencia: **Endesa: Plan estratégico de capacitación de personas Human Firewall**
Ponentes: **Montserrat Bajo Martínez**, Responsable de Concienciación y Formación de Seguridad de la Información de ENDESA.
Andrés Núñez Barjola, Director de la Delegación de Madrid de S2 Grupo.

17:20h. Coloquio

17:25h. Fin de la segunda sesión

19:30h. **Cena de la Ciberseguridad y entrega de los XIII Premios SIC**

Moderador:

Paloma Llaneza González es Socio Director en Razona LegalTech, CISA desde el año 2005, y cuenta más de veinticinco años de experiencia en nuevas tecnologías, Internet, comunicaciones digitales y seguridad TI, tanto en los aspectos legales como regulatorios y de políticas, en España, la UE y Estados Unidos. Además, es árbitro de la Corte de Arbitraje del Colegio de Abogados de Madrid, de AEADE y de la Cámara de Comercio de Madrid en temas TI. Desde diciembre de 2013, es Presidenta de la Sección de Derecho TIC del Ilustre Colegio de Abogados de Madrid. Es miembro, coordinando el grupo de Aspectos Legales, del Centro de Movilidad del ISMS Fórum. Es editora de normas y estándares internacionales, como la ISO/IEC 27004 de métricas de seguridad, las de ETSI sobre correo electrónico certificado (REM) así como las normas europeas (EN) del esquema de acreditación y certificación de CABs y Prestadores de Servicios de Confianza (TSP) del nuevo Reglamento eIDAS, así como la norma europea (EN) que fija sus políticas y requerimientos.

Bankia, fraude tecnológico en canales digitales: realidad vs regulación

Sinopsis: El gobierno del fraude digital es la verdadera piedra angular que trasmitirá más confianza a todos los jugadores del comercio digital, incluyendo tanto a *retailers*, agencias de viaje, cadenas hoteleras, telcos y entidades financieras, entre otras muchísimas. En este sentido, el regulador europeo de las entidades financieras (SSM) ha desarrollado, en el contexto de SecuRe Pay, un esquema de control novedoso y muy detallado que pretende tanto directa como indirectamente cambiar las reglas del juego en el momento de pago del bien o servicio. Este esquema propone obligaciones de las que se desprenden oportunidades y frenos para el comercio digital. Propone homogeneizar los momentos de pago, formar e informar al usuario y gobernar el fraude tecnológico con el objetivo de incrementar su nivel de confianza minimizando el fraude por Internet. Bankia y PwC, en este contexto, explicarán su visión crítica sobre la realidad que viven y las regulaciones que están por llegar.

Ponentes:

Vicente Moscardó Gil es Director de Seguridad Informática de Bankia, ocupando la posición de CISO en la Dirección Corporativa de Estrategia e Innovación Tecnológica. Ingeniero Superior de Caminos, Canales y Puertos por la Universidad Politécnica de Valencia (1985). Profesor de 1997 a 2008 del Máster en Ingeniería del Software, del Departamento de Sistemas Informáticos y Computación, de la Universidad Politécnica de Valencia. Responsable de Seguridad de la Información y Ciberseguridad en Bankia, siendo los principales cometidos de su actividad, la definición y establecimiento de las Políticas y Normativas de Seguridad de la Información, el análisis y gestión de los Riesgos de Seguridad de la Información, la Monitorización, Vigilancia y Respuesta a las Amenazas e Impactos de Seguridad, la Vigilancia y Control del Fraude Tecnológico, la Administración de Permisos y Accesos a los Sistemas de Información, el Sistema de Gestión de la Continuidad de Negocio de la entidad, el establecimiento de los Disaster Recovery Plan, el despliegue de Sistemas de Vigilancia y Defensa y las Revisiones Técnicas de Sistemas y Aplicaciones, como actividades más señaladas.

Israel Hernández Ortiz es Socio de PwC en el área de Riesgos Tecnológicos. Anteriormente trabajó en Telefónica Ingeniería de Seguridad y EY. Es Ingeniero Superior en Informática por la Universidad Alfonso X "El Sabio" y posee varios posgrados como el Máster en Auditoría Informática por la Universidad Politécnica de Madrid y un E-MBA por ESADE, varias certificaciones como CSX, CISA, CISM, CGEIT por ISACA y CISSP por (ISC)², además de la acreditación de Director de Seguridad (TIP) homologada por el Ministerio del Interior. Cuenta con experiencia en múltiples sectores como el Asegurador, Sector Público, Telco y especialmente el sector Banca. En este último ha liderado la línea de relación con el Supervisor/Regulador para iniciativas con impacto en Riesgos Tecnológicos en materia de Riesgos, Ciber, fraude tecnológico, IT-Resilience, Auditoría. Es el Director homologado por ISACA HQ como responsable del capítulo de ISACA Madrid para la iniciativa de formación en Ciberseguridad.

Aquae Security: Estrategia corporativa de uso seguro de servicios Cloud

Sinopsis: En la conferencia se describirán las nuevas tendencias y oportunidades que el Cloud brinda para la mejora de los procesos de negocio y el abaratamiento de los servicios TI de las grandes organizaciones, y como Aquae Security permite en su organización global adoptar las oportunidades de la Nube de forma segura, desplegando tecnologías avanzadas de cifrado, monitorización y Cloud Application Security Control (CASB). Todo ello de forma centralizada y con apoyo de servicios de seguridad gestionada global

Ponentes:

Eduardo Di Monte es ingeniero en Telecomunicaciones y MBA del EuroMBA. Cuenta con doce años de experiencia laboral en el sector de la seguridad de la información y continuidad de negocio. Colaborador habitual del Business Continuity Institute de UK. Actualmente es Director de Seguridad y Continuidad de Negocio de Aquae Security para España y Chile.

Juan Miguel Velasco López-Urda es actualmente CEO y Fundador de AIUKEN SOLUTIONS multinacional española especializada en seguridad internet y servicios Cloud que opera en 7 países, además es consejero de varias compañías de Seguridad Internet y Consultor Estratégico para Grandes Corporaciones en Cloud IT y Seguridad. Con más de 20 años de experiencia en Comunicaciones, Tecnologías de Información y Seguridad, ha desempeñado distintos cargos directivos en Grandes Compañías, líderes en sus sectores, como Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Clientes de Telefónica España. Anteriormente ejerció en Telefónica Empresas como Subdirector de Arquitecturas y Servicios de Seguridad de la Línea de Outsourcing, Subdirector de Arquitecturas y Planificación de Infraestructuras y DataCenters, en Telefonica Data España, y antes como Subdirector de Ingeniería de Proyectos y Servicios de Protección de la Información de la UN Hosting y ASP de Telefonica TTD, así como CTO, COO y Director de Consultoría de la Agencia de Certificación Electrónica (ACE), y responsable de Desarrollo y Despliegue de Servicios Internet en Telefonica DataCorp en Europa y LATAM, y distintos cargos de responsable de despliegue de servicios y redes en Telefónica Servicios de Información y Alcatel Sistemas de Información. Cursó estudios de Informático Superior (UPM), dispone de varios Másteres y es profesor del Máster en Dirección y Gestión de Seguridad de la Información de la ESIT (UPM).

Kill chain: a la búsqueda y captura del enemigo

Sinopsis: En el contexto actual de ciberamenazas, cada vez más sofisticadas y orientadas a provocar impactos económicos y reputacionales no asumibles por el negocio, ni los controles de seguridad "per se" ni los modelos de análisis y respuesta a incidentes tradicionales van a resultar suficientes para contenerlas. Por no hablar de neutralizarlas. Sólo con un conocimiento avanzado del enemigo y el uso real de la ciberinteligencia –demasiadas veces confundida con la mera acumulación de fuentes de información– nos permitirá defender a capa y espada nuestras empresas. Y tratándose de una guerra sin tregua, ¿por qué no aplicar en el entorno digital técnicas consolidadas de estrategia militar? Esta pretende ser una aproximación humilde al modelo de "kill chain" aplicado a la defensa de nuestros activos digitales.

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.

Vicente de la Morena Baena es Responsable Comercial de Grandes Empresas en la Unidad de Seguridad de IBM. 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. Ha sido responsable comercial de la compañía ISS, actualmente integrada en la Unidad de Seguridad de IBM.

Moderador:

Román Ramírez Giménez es cofundador y miembro del equipo de dirección del congreso de seguridad técnica Rooted CON, actividad que compagina con sus actuales responsabilidades como responsable de Seguridad en Arquitecturas, Sistemas y Servicios en la Dirección Corporativa de Seguridad de la Información de Ferrovial. Tiene una carrera profesional de más de quince años en tecnología y seguridad de la información, a lo largo de los cuales ha desarrollado funciones en empresas tan diversas como eEye Digital Security o PwC, pasando por una etapa como emprendedor con su compañía Chase The Sun.

Banco Sabadell: estrategia de seguridad en el ciclo de vida de desarrollo de aplicaciones

Sinopsis: En la conferencia se expondrá el escenario actual de desarrollo de aplicaciones que está afrontando Banco Sabadell, y cómo integra la seguridad en todo el proceso. La creación de una metodología adaptada a los procesos de negocio y desarrollo, así como el uso de servicios especializados de seguridad, incluyendo formación, tecnologías de revisión de código fuente, y asesoramiento continuo, permiten asegurar el éxito y la buena acogida por parte del equipo de desarrollo, así como establecer eficiencias y ahorro de costes en el proceso.

Ponentes:

Santiago Minguito Santos es Director Seguridad de la Información, Regulación y Prevención de Fraude de Banco Sabadell. Tiene más de diecinueve años de experiencia profesional en Seguridad de la Información y gestión de Riesgos Tecnológicos. Desde su incorporación a Banco Sabadell en mayo de 2007, ha gestionado la estrategia de Seguridad de la Información en el Grupo, así como proyectos estratégicos relacionados, entre otros asuntos, con firma electrónica, gestión del fraude, ciberseguridad o identidades y accesos. Actualmente está liderando en Londres el ámbito de Seguridad de la Información, Regulación y Prevención de Fraude, dentro del proyecto de migración del Banco Británico TSB, adquirido por Banco Sabadell en 2015.

Xavier Gracia Lacalle es Director de 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 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).

Banco Santander: Cyber Security Management Model

Sinopsis: Disponer de un modelo que organice las actividades para la gestión del riesgo, tecnológico o general, es fundamental: Los modelos permiten el tratamiento de los riesgos y deben incorporar o ser complementados con un mecanismo de medida de la evolución de los niveles de riesgo. Adicionalmente a la medida del nivel de riesgo de la organización y el análisis, es necesario evaluar lo adecuado del modelo que se usa para gestionarlo. Esta adecuación debe realizarse en una doble vertiente: por su contenido y por su madurez. Por último la evaluación del modelo de gestión del riesgo por un tercero habilita su mejora. Banco Santander ha desarrollado un modelo de valoración de las prácticas de ciberseguridad denominado Cyber Security Management Model. El objeto del proyecto es la evaluación de la madurez de la implantación en el Grupo Santander del marco de gestión de ciber-riesgos

Ponentes:

Idoia Mateo Murillo es, desde enero de 2016, Chief Operational Risk Officer Global de Produban, compañía de Gestión de IT e Infraestructuras del grupo Santander, llevando Riesgo Operacional, Ciberseguridad, Third Party Risk management y IT Assurance & Compliance, centralizando todas las funciones de gestión y control del Riesgo tecnológico y operacional dentro de Produban en todos los países. La función principal de esta unidad es liderar el desarrollo estratégico y ejecución de la estrategia global del riesgo operacional y ser responsable de establecer un marco de riesgos para ayudar en la identificación, evaluación y gestión de riesgos, así como el análisis de la información de riesgos proporcionada por los países para crear un perfil de riesgos de Produban.

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 veinticinco 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. 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 transformación digital de la lucha contra el fraude: estrategias de ataque a la rentabilidad de las acciones de la delincuencia organizada

Sinopsis: En todas las industrias formales se hacen análisis de rentabilidad de las inversiones. Se invierte un capital y se asume cierto riesgo en pos de unas ganancias esperadas. En la caso de la Delincuencia Organizada es exactamente igual. Invierten un capital y esperan por ello un beneficio. En el caso de la Delincuencia Organizada los riesgos que asumen no son sólo de pérdida del capital invertido sino de acabar en la cárcel. Para desincentivar la actividad de la Delincuencia Organizada hay que trabajar en estos tres ejes: reducir el flujo del capital de retorno, aumentar los costes de ejecución y aumentar la sensación de poder ser detenido. Algunas de las herramientas que se están empezando a utilizar con éxito en este campo son las matemáticas del comportamiento y la analítica de redes complejas. Con estas y otras herramientas científicas se están generando los siguientes avances en Ciberseguridad.

Ponente:

Santiago Moral Rubio es Doctor en Análisis y Gestión de Riesgos de Ciberseguridad por la Universidad Rey Juan Carlos, Ingeniero Técnico en Informática por la Universidad Politécnica de Madrid, Máster de Postgrado en Tecnologías y Sistemas de la Información por la Universidad Rey Juan Carlos y Máster de Postgrado en Ingeniería de la Decisión por la misma universidad. Cuenta con las certificaciones CISA, CISM, CGEIT y CRIS de la ISACA. Comenzó a mediados de los 80 a trabajar sobre entornos Unix, Oracle e Informix fundando su propia compañía "Open Systems Administration Group". En el año 2000 comenzó a trabajar en el Banco Uno-e (del Grupo BBVA) como Director de Seguridad de la Información. En 2001 pasó al BBVA como Director del Departamento de Seguridad Lógica, con responsabilidad global dentro del Grupo BBVA. En la actualidad es el Global Head of Cibersecurity & Digital Trust. Ha publicado recientemente en Estados Unidos el libro "Intentional Risk Management Through Complex Networks Analysis" con la editorial Springer.

Moderador:

Carlos Manuel Fernández Sánchez, Gerente de TICs en Evaluación de la Conformidad de la Dirección Comercial de Certificación de AENOR. Y antes fue Gerente de Desarrollo de Certificaciones TIC en la Dirección de Desarrollo de AENOR. Asimismo, es Profesor Coordinador de la asignatura Control y Auditoría de los Sistemas de Información en la Universidad Pontificia de Salamanca. Previamente también fue Profesor Coordinador del Máster ADTIC de la Universidad de Alcalá y Director de Relaciones Institucionales de BSA en España, además de haber trabajado para Microsoft y Citibank. Ingeniero en Informática por la Universidad Politécnica de Madrid, cuenta con las certificaciones CISA y CISM.

Retos e Iniciativas de Seguridad en la Dirección General de Tráfico

Sinopsis: La DGT, en su misión de mejora continua de los servicios prestados a los ciudadanos, sigue apostando por la digitalización de sus procesos como mecanismo para mejorar la cercanía y comunicación con los conductores así como agilizar los trámites que estos tienen que realizar. Sin embargo, esta trasformación debe hacerse con todas las garantías de seguridad y al mismo tiempo incorporar la innovación en seguridad como elemento clave de éxito. En la ponencia, la DGT compartirá junto con BT su visión y estrategia en el campo de la seguridad, tratando temas como la seguridad gestionada, el proyecto "@clave" y la protección de las aplicaciones con tecnologías como Datapower de IBM.

Ponentes:

Jesús Cuadrado García de la Calera, Jefe de Explotación, Soporte y Servicios en la Gerencia de Informática de la Dirección General de Tráfico. Con casi 20 años de experiencia, ingresa en 2008 en la DGT como desarrollador de la Gerencia de Informática. Ha impulsado y participado en relevantes proyectos para los ciudadanos, como la implantación de la renovación telemática del permiso de conducir o la integración del registro de conductores con el resto de Estados Miembros de la Unión Europea. Su actual puesto –desde 2012– está más relacionado con infraestructuras y más cercano a la estrategia del organismo, permitiéndole tener una visión completa de la actividad de los diferentes departamentos de la DGT y del resto de organismos y departamentos ministeriales de la AGE con los que colabora habitualmente la DGT.

Jose Francisco Pereiro ocupa el cargo de Director de Servicios de Seguridad de BT Iberia y tiene más de quince años de experiencia en el área de Seguridad de la Información. Ha trabajado en proyectos nacionales e internacionales en diversos campos como la protección de sistemas de control de empresas energéticas o seguridad de medios de pago de entidades financieras. Dispone de varias de las principales certificaciones de seguridad como CISA, CISM, CISSP, CSSA y QSA entre otras.

Endesa: Plan estratégico de capacitación de personas Human Firewall

Sinopsis: De sobra es conocido que la mejora de la seguridad no depende "sólo" de la implantación de medidas técnicas de seguridad o la definición de procedimientos; es fundamental la implicación de las personas. Sin obviar la necesidad de seguir reforzando los pilares de la tecnología y los procesos, se debe fortalecer el, hasta ahora, débil pilar de las personas, en busca de una posición de equilibro y solidez que permita incrementar el nivel de madurez en seguridad de una organización. Para conseguirlo, hay que atacar el problema desde el origen, convirtiendo al empleado en parte de la defensa: "human firewall". protectIT es un plan estratégico de capacitación que tiene como objetivo conseguir que las personas sean capaces de realizar una gestión adecuada de los riesgos que les afectan por medio de acciones continuadas de concienciación, formación y prueba en entornos de simulación. Disponemos en nuestra organización de un ejército dormido, ¿a qué esperamos para activarlo?

Ponentes:

Montserrat Bajo Martínez, Responsable de Concienciación y Formación de Seguridad de la Información de Endesa. Con amplio recorrido en la implantación de modelos de privacidad y protección de datos así como en la definición e implantación de modelos de Análisis de Riegos y SGSI en Endesa. Anteriormente ha liderado proyectos de Continuidad de Negocio e implantación y cumplimiento de la normativa de Infraestructuras Críticas en Endesa. Ingeniera en Informática de Gestión (Universidad Pontificia de Salamanca), es CISA y Director de Seguridad por el Ministerio del Interior. Previamente ha desarrollado actividades profesionales en los sectores de telecomunicaciones y farmacéutico.

Andrés Núñez Barjola, Director de la Delegación de Madrid de S2 Grupo. Desde 2008 en la compañía, es Ingeniero Superior en Informática por la UAM, Máster en Dirección y Gestión de la Seguridad de la Información por la UPSAM, CISA por ISACA e ISO 27001 Lead Auditor por Applus. En su bagaje profesional acumula gran experiencia en el ámbito del desarrollo de negocio, la dirección y coordinación de proyectos (SGSI, ENS, ISO 27001) y es experto en comunicación, siendo participante habitual en charlas y jornadas técnicas y de divulgación y concienciación. Con anterioridad ha trabajado en Siemens, Endecar y Soluziona.

TERCER MÓDULO, 28 DE ABRIL

09:30h.	Entrega de documentación
	Moderador: **Miguel García-Menéndez**, Responsable de Gobierno Corporativo y Estrategia. Centro de Ciberseguridad Industrial. CCI.
10:00h.	Ponencia: **Ciberseguros: la última línea de defensa... ¿o la primera?**
	Ponente: **Adolfo Hernández Lorente**, Subdirector y cofundador de THIBER, the cybersecurity think tank.
10:30h.	Coloquio
10:35h.	Ponencia: **Vodafone: The Last Mile. Cómo implementar una estrategia global de ciberseguridad.**
	Ponentes: **Javier Sevillano Izquierdo**, Chief Security Technology Officer. Vodafone.
	Roberto López Navarro, Jefe de la División de Servicios gestionados. GMV Secure e-Solutions.
11:05h.	Coloquio
11:10h.	Ponencia: **Los ciberterrosecretos de la Deep Web.**
	Ponentes: **María Carmen Aguilar Carneros**, Responsable de Concienciación, Auditoría y Cumplimiento. Departamento de Seguridad de la Información. Dirección de Seguridad y Compras. Ferrovial.
	Juan Antonio Calles. Cyber Security Senior Manager. KPMG España.
11:40h.	Coloquio
11:45h.	Pausa-café
	Moderador: **Luis Guillermo Fernández Delgado**, Editor de Revista SIC.
12:15h.	Ponencia: **BP: adaptación a los retos digitales para generar valor.**
	Ponente: **Denis Ontiveros Merlo**, CISO responsable de aplicaciones de negocio e Infraestructura global de TI. BP.
12:45h.	Coloquio
12:55h.	Ponencia: **El reto del CISO ante las notificaciones de incidentes de ciberseguridad: datos personales y presuntos delitos.**
	Ponente: **Manuel Carpio Cámara**, Director de Seguridad de la Información y Prevención del Fraude. Telefónica.
13:25h.	Coloquio
13:45h.	Almuerzo, fin de la tercera jornada y fin de Securmática 2016

Moderador:

Miguel García-Menéndez, Responsable de Gobierno Corporativo y Estrategia del Centro de Ciberseguridad Industrial (CCI), es un veterano del sector tecnológico con más de dos décadas de trayectoria profesional. Se incorporó al Centro de Ciberseguridad Industrial (CCI) a finales de 2014, en calidad de Vicepresidente, con la misión de acercar el mensaje "ciber" a los directivos del sector industrial. Tras iniciar su carrera en el mundo de la industria, ha sido CIO, consultor, auditor, divulgador y, más recientemente, observador y analista de la realidad del mercado (en 2011 co-funda el "think tank" español, iTTi, que hoy preside). Ha estado o está ligado a los órganos de gobierno de diversas organizaciones profesionales del sector: AEMES, ATI, ISACA. Dispone de las certificaciones CGEIT, CISM, CISA, CRISC.

Ciberseguros: La última línea de defensa... ¿o la primera?

Sinopsis: *Cyberrisk policies*, *cyberinsurance coverage*, *privacy protection*, *network liability*, *security & privacy liability*, *media liability*, ciberpólizas o pólizas de ciberriesgo. Sus coberturas son tan heterogéneas como la falta de consenso en cuanto a su definición. Servicios pre-siniestro vs servicios reactivos, paneles de servicios preaprobados vs paneles abiertos, exclusiones, definiciones, ámbitos de aplicación, temporalidad, etc. El seguro ha sido tradicionalmente un método de compensación y transferencia de riesgo, no de mitigación. Por extensión, las ciberpólizas son a menudo conceptuadas como la última línea de defensa. Sin embargo cuando se afrontan como una medida directriz, se convierten en la primera pieza de una estrategia proactiva de gestión de ciber-riesgos. Ahora más que nunca se hace necesaria una colaboración continua entre los departamentos de siniestros de las aseguradoras la industria de seguridad y los departamentos TIC de las compañías aseguradas. Se presentarán las principales conclusiones del informe "Ciberseguros. La transferencia del ciber-riesgo en España".

Ponente:

Adolfo Hernández Lorente, es Subdirector y cofundador de THIBER the cybersecurity think tank. Ingeniero informático por la Universidad Autónoma de Madrid con más de diez años de experiencia profesional en la gestión de riesgos tecnológicos y ciberseguridad, es ponente habitual en diversos postgrados y másteres, así como autor de múltiples publicaciones relacionadas con la ciberseguridad, la ciberdefensa y el derecho de las nuevas tecnologías. Compagina su actividad profesional como asesor de ciberseguridad en Telefónica/Eleven Paths con la involucración como subdirector y cofundador de THIBER, el primer think tank de referencia de la comunidad hispanohablante en materia de seguridad y defensa del ciberespacio.

Vodafone: The Last Mile. Cómo implementar una estrategia global de ciberseguridad

Sinopsis: La gestión de la seguridad es un problema global, que no es racional circunscribir a fronteras políticas ni organizativas. Esta realidad se vive día a día en organizaciones de carácter multinacional, donde la estrategia de seguridad pasa por la coordinación de capacidades y recursos distribuidos a lo largo y an-

cho de la organización. Sin embargo, esta estrategia no está exenta de retos que es necesario gestionar para alcanzar los niveles de eficacia y eficiencia exigidos. Los ponentes revisarán el caso de Vodafone como un manifiesto ejemplo de organización multinacional con una potente y marcada estrategia global de seguridad que se apoya fuertemente en capacidades locales.

Ponentes:

Javier Sevillano Izquierdo es Responsable de Seguridad Tecnológica en Vodafone España. Dispone de veintisiete años de experiencia en TI, diecinueve 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 Bankia, Caja Madrid, Sistema 4B, Seinca y McDonnell Douglas.

Roberto López Navarro es Jefe de la División de Servicios gestionados de GMV Secure e-Solutions. Ingeniero Superior de Telecomunicaciones por la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid, y MBA por ESADE Business School. Certificado CISA (Certified Information System Auditor) y CISM (Certified Information Security Manager) por ISACA (Information Systems Audit and Control Association).Certificado CISSP (Certified Information Systems Security Professional) por (ISC)^2 (International Information Systems Security Certifications Consortium). Roberto López ha desarrollado toda su carrera profesional en GMV, ocupando diferentes responsabilidades, siempre asociadas al ámbito de la Ciberseguridad.

Los ciberterrosecretos de la Deep Web

Sinopsis: En la conferencia se llevará a efecto una introducción a la *Deep Web*, y en concreto a los *Black Markets*, foros y demás canales utilizados por ciberdelincuentes para intercambiar contenidos y vender activos fraudulentos. Por otro lado, se analizarán algunos lugares donde los terroristas realizan contacto y captación e intercambian contenidos.

Ponentes:

María Carmen Aguilar Carneros es Responsable de Concienciación, Auditoría y Compliance en el Departamento de Seguridad de la Información, perteneciente a la Dirección de Seguridad y Compras de Ferrovial. Su carrera en el campo de la seguridad de la información se inició en el año 2007 liderando diversas iniciativas y proyectos vinculados al gobierno, privacidad, riesgos, cumplimiento, auditoría y concienciación en materia de seguridad de la información. Es Ingeniero Informático e Ingeniero Técnico en Informática de Gestión por la Universidad Carlos III de Madrid. Cuenta con las certificaciones CISA, CISM por ISACA, CDPP por Data Privacy Institute, Lean IT e ITIL Foundation por ITSMF y Lead Auditor ISO 27001 por IRCA.

Juan Antonio Calles es Cyber Security Senior Manager en KPMG España. Fue socio fundador y director de la compañía especializada de ciberseguridad Zink Security, perteneciente actualmente a KPMG. Doctor en Informática. Ingeniero Técnico en Informática de Sistemas, Postgrado en TI y Sistemas Informáticos y en Ingeniería de Sistemas de Decisión. Certified Hacking Forensic Investigator (CHFI v8) por Ec-Council, CISA por la Isaca, ITIL v3 por EXIN, Dlink Certified, FCSI y FTSAI. Igualmente, es miembro de la Asociación Nacional de Ciberseguridad y Pericia Tecnológica (ANCITE). Es ponente habitual en diversos foros y congresos de seguridad, entre los que se encuentran No cON Name, RootedCon, HomeSec y SID, y coorganizador de las Jornadas X1RedMasSegura.

Moderador:

Luis Fernández Delgado. Licenciado en Ciencias de la Información, rama de Periodismo, por la Universidad Complutense de Madrid/CEU San Pablo. Desde 1992 edita la revista española SIC, propiedad de Ediciones Coda. Igualmente, codirige el equipo de Organización de Securmática, el Congreso global de Ciberseguridad, Seguridad de la Información y Privacidad, Espacio TiSEC y Respuestas SIC. Fernández Delgado ha participado como ponente en numerosos cursos, congresos y seminarios nacionales e internacionales sobre seguridad TIC; es profesor colaborador del Máster de Ciberseguridad de la Universidad Carlos III de Madrid y del de Auditoría y Seguridad de la Información de UPM. Igualmente, es asesor en materia de ciberseguridad, seguridad de la información, auditoría, control, y de la industria y el mercado de seguridad TIC. Actualmente es miembro, entre otras, del capítulo de Madrid de ISACA, del ISMS Forum y de CriptoRed.

BP: adaptación a los retos digitales para generar valor

Sinopsis: Las nuevas tendencias en la gestión de TI, requieren la adaptación de toda organización y en consecuencia una revisión continua de su gestión de la ciberseguridad. Su alineación continua con las necesidades del negocio y las expectativas de seguridad imponen un enfoque dinámico para afrontar el cambio y, en ocasiones, la ruptura con métodos tradicionales. Durante la ponencia, se expondrá el viaje que BP ha seguido para afrontar los retos tecnológicos partiendo de los retos externos a los internos para adaptar los procesos de seguridad a los nuevos modelos operativos de TI de forma sostenible.
La conferencia dará ocasión de conocer como BP incorpora la ciberseguridad y la gestión del riesgo en las principales iniciativas de transformación con el fin de generar de valor de forma segura.

Ponente:

Denis Ontiveros Merlo es CISO responsable de aplicaciones de negocio y del área de Infraestructura global de TI de BP. Con más de 18 años de experiencia en el mundo de la seguridad Informatica, Denis Ontiveros inició su trayectoria en el mundo de la Auditoría Informatica en 1999, siendo el miembro fundador del departamento de la Gestión de Riesgos Informáticos (IRM) de KPMG Barcelona alcanzando el nivel de gerente. En 2004 se incorporó como CISO a Sara Lee Corporatión para sus operaciones de EMEA, asumiendo el rol de VP Global CISO en 2007. Durante este tiempo lideró múltiples proyectos corporativos, entre ellos la implementación de Binding Corporate Rules, Servicios de gestión de identidades y programas holísticos de seguridad en el área del cumplimiento corporativo. En 2013 se incorporó al Departamento de Ciberseguridad y Riesgos de BP como CISO Responsable de Aplicaciones de Negocio, incorporando el 2016 el área de Infraestructura global de TI. Denis es diplomado en Empresariales e Informatica por la Universidad del País Vasco y el Fachhochschule de Económicas de Berlín. Dispone de un Máster en comercio electrónico y numerosas certificaciones: CISA, CISM y CIPP/E.

El reto del CISO ante las notificaciones de incidentes: datos personales y presuntos delitos

Sinopsis: Los marcos regulatorios de la UE en lo que respecta al tratamiento de datos personales (RGPD) y el que por el momento se deduce de la futura directiva NIS, van a consagrar, cada uno en su universo competencial, la notificación de incidentes. Los que sucedan y se detecten deberán ser considerados como presuntos delitos si se ajustan a lo tipificado en la legislación penal; y, además, pueden llevar aparejada la exposición, pérdida o sustracción de datos de carácter personal. Esta doble circunstancia va a tener consecuencias relevantes en la delimitación de funciones y competencias del CISO y su relación con el CIO, el DPO y con otras figuras clave en la organización.

Ponente:

Manuel Carpio Cámara es Director de Seguridad de la Información y Prevención del Fraude de Telefónica. Ingeniero Superior de Telecomunicación (ETSIT UPM), PDD (PDD (IESE Universidad Navarra) y CISA y CISM. Co-fundador del Grupo de Trabajo de Seguridad, que agrupa a los responsables de seguridad de 15 empresas del IBEX, fue miembro del ESRAB (European Security Research Advisory Board) por designación de la Comisión Europea. Carpio es Profesor asociado en el Máster de Seguridad Informática de la UPM, representa a Telefónica en el grupo de referencia eComms de ENISA, y es miembro del Comité directivo de ETIS (www.etis.org) y de la junta directiva de CONTINUAM. En 2004 recibió un premio profesional otorgado por SIC. Se incorporó a Telefónica Sistemas en 1988 como ingeniero de desarrollo en proyectos de seguridad de las comunicaciones. En 1992 fundó el área de seguridad telemática para grandes clientes de Telefónica. En 1998 pasó a ocupar la Gerencia de Seguridad de la Información de Telefónica de España. Desde 2001 hasta hoy es Director de Seguridad de la Información y Prevención del Fraude en Telefónica, S.A y miembro del Comité Corporativo de Seguridad de Telefónica.

// Securmática 2016

Securmática 2015 tuvo el honor de contar con la participación en el acto inaugural de **Francisco Martínez Vázquez**, Secretario de Estado de Seguridad y Presidente de la Comisión Nacional para la Protección de las Infraestructuras Críticas.

Más de 7.300 expertos han pasado por Securmática, un congreso que con sus 26 ediciones ya celebradas es el foro de intercambio de experiencias en ciberseguridad por excelencia.

// Premios SIC 2016 y Cena de la Ciberseguridad

En coincidencia con la XXVII edición de Securmática, tendrá lugar el acto de entrega de los XIII 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 duodécima edición de los Premios SIC.

Fechas y lugar de celebración

SECURMÁTICA 2016 tendrá lugar los días 26, 27 y 28 de abril de 2016 en el hotel NOVOTEL. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2016 recibirán las carpetas de congresistas con el programa oficial y toda la documentación –papel y pendrive– referente a las ponencias.
- Almuerzos y cafés.
- Cena de la Seguridad y entrega de los XIII Premios SIC (27 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 28 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 26 ☐ Módulo 2 Día 27 ☐ Módulo 3 Día 28 ☐ Deseo inscribirme a SECURMÁTICA 2016
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**