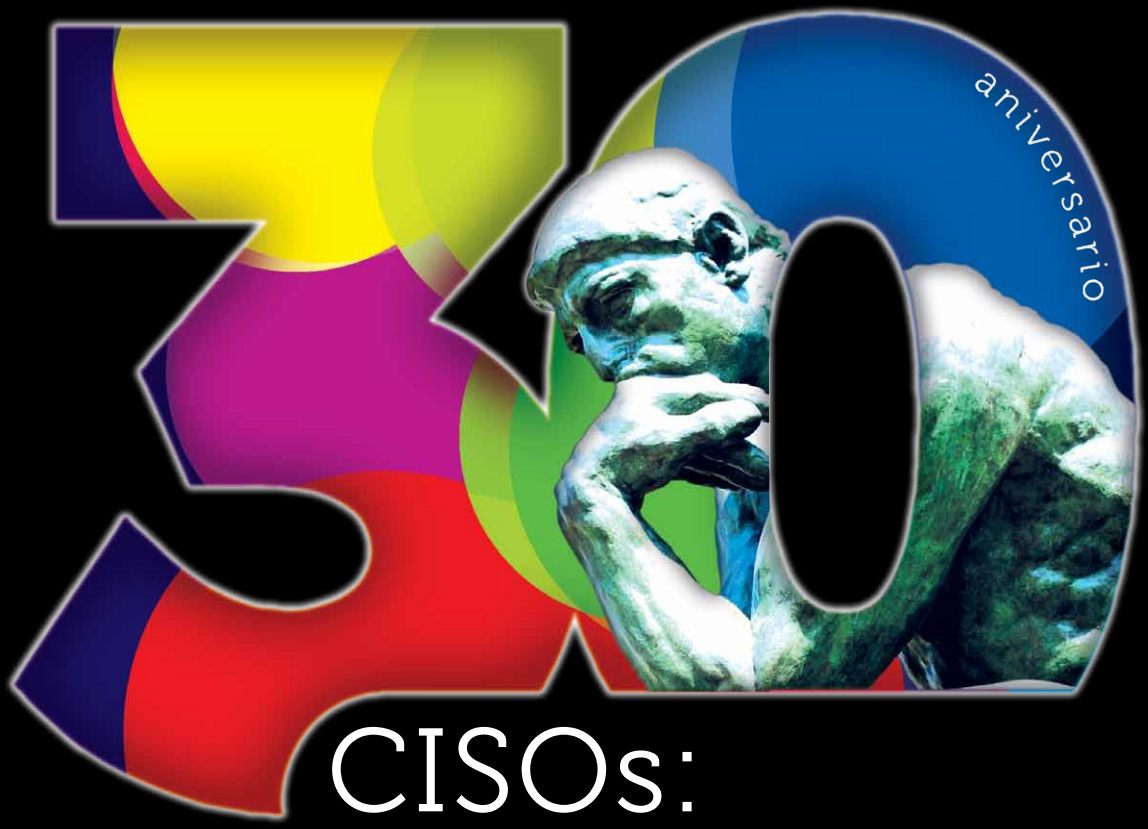
SECURMÁTICA

XXX Congreso Global de Ciberseguridad,
Seguridad de la Información y Privacidad

23.24.25
ABRIL 2019



CISOs:

lo que sí se está haciendo

PROGRAMA

www.securmatica.com

Seguridad digital: lo que sí se está haciendo

Securmática cumple 30 años, un periodo largo que partió de la antaño denominada seguridad informática, bautizada luego como gestión de riesgos de seguridad de la información y convertida hoy en ciberseguridad y/o seguridad digital.

En el principio, y al ritmo del desarrollo de los escenarios TIC, no siempre hubo legislación desarrollada sobre privacidad, ni sobre infraestructuras críticas, servicios esenciales y proveedores de servicios digitales, ni entidades como la AEPD, el CCN, el CNPIC, el Consejo Nacional de Ciberseguridad, el DSN, INTECO (transformado a posteriori en INCIBE), el MCCD, ni obligaciones de notificar, ni sanciones.

Pero siempre hubo responsables de seguridad informática (los CISOs del presente), algunos –los menos en los orígenes– a tiempo completo. Y fue a ellos, en tanto que expertos en esta disciplina, y a la incipiente industria especializada, a quienes se dirigió el Congreso.

Este ideario no ha cambiado en tres décadas; antes bien, se ha intensificado –no sin esfuerzo–, como se puede observar en este programa de 2019, en el que se brinda una selección representativa, intersectorial y avanzada de la moderna gestión de ciberseguridad.

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

accenture security · Aiuken Cybersecurity · AON Empower Results® · Blueliv. · Capgemini · cipher a PROSEGUR company · Eleven Paths Telefónica Cyber Security Unit · Entelgy Innotec Security · EY Building a better working world · gmv Innovating Solutions · IBM · KPMG · Micro Focus · MNEMO · pwc · S2 Grupo · S21sec

PRIMER MÓDULO, 23 DE ABRIL

08:45h. Entrega de documentación
09:15h. Ceremonia de apertura
10:00h. **Conferencia de Inauguración**
Ponente: **Julia Olmo**, Embajadora en Misión Especial para las Amenazas Híbridas y la Ciberseguridad. Mº DE ASUNTOS EXTERIORES, UE Y COOPERACIÓN
10:20h. Ponencia: **SECURMÁTICA 30 aniversario: En compañía de CISOs**
Ponentes: **Manuel Carpio**, Cybersecurity Senior Advisor. INERCO
Santiago Moral, CEO de BLUEVOYANT Spain
10:50h. Coloquio
10:55h. Pausa-café
11:30h. Ponencia: **El nuevo Cyber Security Center global de GRUPO SANTANDER en Madrid: anticipando el mañana, hoy**
Ponente: **Daniel Barriuso**, CISO Global. GRUPO SANTANDER
12:00h. Coloquio
12:05h. Ponencia: **Poli bueno, poli malo**
Ponentes: **Alejandro Javier Figueroa**, Head of Corporate Security & Engineering Risk de BBVA España
Martín Suárez, TISO-Technology Information Security Officer en BBVA España
12:35h. Coloquio
12:40h. Ponencia: **AXA INM: Transformando la gestión de la seguridad sobre entornos diversos y complejos**
Ponentes: **Silvia Villanueva**, CISO del Grupo AXA
Francisco Escobar, Manager de Ciberseguridad. MNEMO
13:10h. Coloquio
13:15h. Ponencia: **La Seguridad en 2020: Hacia un mundo hiperconectado**
Ponentes: **Hugo de los Santos**, Director de Productos y Servicios para el segmento Empresas de TELEFÓNICA
Pedro Pablo Pérez, CEO de ELEVENPATHS y VP de Seguridad Global de TELEFÓNICA
13:45h. Coloquio
13:50h. Almuerzo
15:50h. Ponencia: **MÁSMÓVIL: Gestión de la ciberseguridad en un entorno de integración continua de compañías**
Ponentes: **Daniel Martinez**, CISO. Grupo MÁSMÓVIL
Joaquín Castillón, Director Advisory Services. EY
16:20h. Coloquio
16:25h. Ponencia: **GRUPO EUSKALTEL: Transformación digital, Operaciones de Seguridad y Protección del cliente final**
Ponentes: **Idoia Uriarte**, CISO de EUSKALTEL
Jorge Hurtado, Vicepresidente del área de servicios gestionados en S21sec
16:55h. Coloquio
17:00h. Fin del primer módulo

CONFERENCIA DE INAUGURACIÓN

Julia Olmo
Embajadora en Misión Especial para las Amenazas Híbridas y la Ciberseguridad
Dirección General de Política Exterior y de Seguridad
Mº DE ASUNTOS EXTERIORES, UNION EUROPEA Y COOPERACIÓN

"SECURMÁTICA 30 aniversario: en compañía de CISOs"

Sinopsis. "La conferencia, pronunciada por dos excepcionales ingenieros y expertos en ciberseguridad, CISOs durante muchos años de dos compañías multinacionales de origen español de sectores muy regulados, BBVA y Telefónica, brindará a la audiencia un refrescante paseo histórico por la función y las figuras de la dirección de seguridad de la información y de seguridad TIC en nuestro país, enmarcando sus vivencias profesionales y los avatares de este sector, actividad y práctica en un relato orientado a descubrir qué cabe esperar tras estos treinta años de historia".

Ponentes:

Manuel Carpio es actualmente Cybersecurity Senior Advisor en INERCO. Ingeniero Superior de Telecomunicación (ETSIT UPM), PDD (IESE Universidad de Navarra), CISA, CISM y co-fundador del Grupo de Trabajo de Seguridad-GTS, fue miembro del ESRAB (European Security Research Advisory Board) por designación de la Comisión Europea. Carpio 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 2016 fue Director de Seguridad de la Información y Prevención del Fraude en Telefónica, S.A y miembro del Comité Corporativo de Seguridad de Telefónica. En 2004 recibió un galardón profesional otorgado por SIC.

Santiago Moral es CEO de BlueVoyant Spain desde su fundación en marzo de 2018. CISO del Grupo BBVA de 2001 a 2018. 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 1997 lanza en ATOS el Departamento de Ciberseguridad. En el año 2000 comenzó a trabajar en el Banco Uno-e (del Grupo BBVA) como Director de Seguridad de la Información. Doctor en 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 ISACA. Fundador del Instituto DCNC Sciences de la URJC (Data, Networks & Cybersecurity Sciences). Presidente del capítulo Español de la Asociación Internacional Hispanic IT Executive Council (HITEC). Fue galardonado en 2005 y 2012 con sendos premios SIC.

"El nuevo Cyber Security Center global de GRUPO SANTANDER en Madrid: anticipando el mañana, hoy"

Sinopsis. "Los cimientos de la ciberresiliencia requieren un enfoque estratégico centrado en las personas, los procesos y la tecnología. Es esencial contar con una base sólida de capacidades internas para construir servicios estratégicos y disponer de instalaciones modernas que permitan tener la agilidad y un entorno colaborativo. El nuevo "Cyber Security Center" global de Santander, con sede en Madrid, proporciona servicios de protección, detección y respuesta las 24 horas del día, los siete días de la semana, en todas las regiones en las que está presente el Grupo. El centro dispone de las últimas tecnologías para proteger tanto a empleados y clientes, como a los sistemas y datos de la entidad. Las instalaciones están diseñadas para albergar a más de 300 profesionales con una amplia experiencia profesional y capacidades diversas en ciberseguridad. El nuevo centro actúa como núcleo central desde el que impulsar la colaboración a nivel mundial, coordinar la respuesta ante amenazas y ayudar a anticipar las necesidades futuras".

Ponente:

Daniel Barriuso es CISO Global de Grupo Santander. Cuenta con una de las trayectorias más prestigiosas a nivel internacional en el desempeño de la función. Con anterioridad ha desempeñado el cargo de CISO en BP y Credit Suisse, además de ser Presidente del Grupo de Seguridad IBSIG, donde ayudó a coordinar, en asociación con el Banco de Inglaterra y la FSA, el ciberejercicio Waking Shark. Asimismo, Barriuso, es Profesor en la Universidad Politécnica de Madrid, donde imparte clases e investiga en las áreas de gobierno y seguridad de TI, y ha sido en repetidas ocasiones ponente en Securmática.

"Poli bueno, poli malo"

Sinopsis. "En la era de la transformación digital, las empresas están sometidas a asumir ciertos riesgos bajo un fuerte marco regulatorio. La inmediatez de las operaciones, la digitalización, uso masivo de nubes, terceros que actúan como nosotros, y un mundo cada vez más competitivo, son características de contexto del medio que han dejado obsoletas las estrategias de seguridad tradicionales centralizadas. Para poder superar estas dificultades, hay que instaurar estrategias de colaboración en las que prime el trabajo en equipo y en cuyo marco, el negocio, la seguridad y la tecnología vayan siempre de la mano, sin miedo pero con respeto y responsabilidad".

Ponentes:

Alejandro Javier Figueroa es Head of Corporate Security & Engineering Risk de BBVA España. Ingeniero en Informática, Contador Auditor por la Universidad de Chile, Máster en Dirección de Tecnologías de Información del IE Business School y certificado CISA y CISM, Figueroa cuenta con más de 15 años de experiencia en el sector financiero y de consultoría con foco en materias de gestión del riesgo tecnológico, ciberseguridad, prevención de fraude, continuidad de negocios, riesgo operacional y auditoría. Considera vital para el futuro de la banca transformar el rol de los CISOs hacia un habilitador de los negocios de las entidades, aprovechando las bondades que brindan las nuevas tecnologías. En la actualidad vive su primera experiencia internacional en el grupo BBVA, como CISO de la unidad de negocios de España. Anteriormente fue Director de Auditoría de Ciberseguridad y Riesgo Operacional en Itaú Corpbanca y CISO de BBVA Chile.

Martín Suárez es TISO –Technology Information Security Officer– en BBVA España. Ingeniero en Informática, máster en Seguridad Informática con más de 15 años de experiencia en seguridad, Suárez comenzó su andadura en el desarrollo de sistemas basados en criptografía. Durante su carrera profesional se fue especializando en banca y diseñando y construyendo sistemas de seguridad con una visión muy centrada en el cliente. Con anterioridad a BBVA, ha trabajado en compañías como Bankia, GFI y Redsys. Es un firme creyente en la idoneidad de las Arquitecturas Seguras para acompañar al negocio en su carrera, garantizando la seguridad desde el origen y llegando a acuerdos en todo el ciclo de una idea.

"AXA INM: Transformando la gestión de la seguridad sobre entornos diversos y complejos"

Sinopsis. "Actualmente, el Grupo AXA se encuentra entre los principales proveedores de protección financiera del mundo, presente en 57 países y con más de 163.000 empleados comprometidos en atender a más de 101 millones de clientes. El área de seguridad, que incluye Information Security, Operation Resilience y Physical Security de AXA International New Markets (INM), como parte de AXA tiene como misión garantizar que AXA es **#safe**, **#secure** y **#resilient**, supervisando y dando soporte y apoyo a 32 entidades en crecimiento del Grupo en todo el mundo donde la diversidad social, política, económica y cultural impactan directamente en el grado de madurez en la gestión de la seguridad. Adaptar, transformar e industrializar la gestión de los servicios de seguridad en entornos complejos, diversos y multiculturales ha sido, es y seguirá siendo un reto para AXA INM, cuyo camino sigue recorriendo y mejorando".

Ponentes:

Silvia Villanueva es actualmente CISO de AXA INM. Con anterioridad fue CISO Transversal para la Región de EMEA-LATAM en AXA. Y previamente a su incorporación a esta compañía trabajó más de 15 años en algunas de las principales empresas internacionales de auditoría y consultoría, siempre dentro del área de la ciberseguridad. Durante este tiempo dirigió y ejecutó proyectos de ámbito nacional e internacional para numerosas compañías de diversos sectores. Villanueva es Ingeniera en Informática por la Universidad Alfonso X El Sabio y cuenta con las certificaciones CEH, CISM, CISSP, CISA, CSSA, CSSLP y GISCP.

Francisco Escobar es Manager de Ciberseguridad en Mnemo. Licenciado en Ciencias Gerenciales y Administrativas, con especialización en sistemas de información y EMBA en la European Business School of Madrid, ITIL Expert e ISO Lead Auditor, Escobar dispone de varias certificaciones en herramientas de ITSM. Tiene más de 15 años de experiencia en el área de TI, durante los cuales ha liderado diferentes proyectos, programas, servicios y planes directores en clientes relevantes como: BBVA, London City Hall, Accenture, NATO, FCC, Endesa, Gobierno de España, Mutua Madrileña, AvantCard y recientemente en AXA INM. Colaborador en la Escuela Europea de Negocios de España para el asesoramiento en proyectos de maestría en EMBA.

"La Seguridad en 2020: hacia un mundo hiperconectado"

Sinopsis. "En la conferencia se llevará a cabo, desde la perspectiva de un operador de Red, una exposición de la seguridad requerida para el mundo interconectado, se explicará la evolución de las redes X25/ATM → MPLS/Internet → SDN/NFV, Redes Hibridas y el futuro 5G, la desaparición del perímetro y el futuro digital de la interconexión masiva, así como la necesidad de la seguridad en el dato. En el contexto se explicarán algunos casos de éxito (clientes y tecnologías) en los que se deja apuntada la ciberseguridad embebida en la Red/Cloud, lo que va a cambiar de forma drástica el panorama de la prestación de servicio".

Ponentes:

Hugo de los Santos es el Director de Productos & Servicios para el segmento Empresas en Telefónica con responsabilidad global. Desde su creación en 2011 y hasta hace escasamente tres años, ha sido el director de aceleración de negocios de Wayra (la aceleradora de start-ups de Telefónica), en cuya fundación participó activamente. Antes de unirse a este proyecto, desempeñó diferentes puestos de responsabilidad en áreas de Negocio, Marketing y Ventas dentro del Grupo Telefónica. Con casi 20 años de experiencia internacional en el mundo de las TIC, De los Santos cuenta con un sólido historial académico, es Ingeniero de Telecomunicaciones, posee un postgrado de PDD (programa de desarrollo ejecutivo) de la escuela de negocios del IESE otorgado por la Universidad de Navarra y cuenta además con el programa "Entrepreneurship Network Program" de la Universidad de Stanford.

Pedro Pablo Pérez es VP de Seguridad de Telefónica y CEO de ElevenPaths, su unidad de Ciberseguridad. Trabaja en el sector de la seguridad TI desde hace más de 15 años. Licenciado en Informática y Global MBA por IESE, posee numerosas certificaciones en seguridad, como CISA, CISM, ITIL Service Manager o ISO 27001 Lead Auditor. Ha participado en la implantación de centros de operaciones de seguridad global en España, Latinoamérica y EEUU. Además, ha sido el responsable de la definición del nuevo portafolio de ciberseguridad de ElevenPaths y lidera la propuesta de innovación en ciberseguridad para clientes internos y externos de Telefónica.

"MÁSMÓVIL: Gestión de la ciberseguridad en un entorno de integración continua de compañías"

Sinopsis. "Grupo MásMóvil ha experimentado en los últimos años el crecimiento más importante en su sector, donde la adquisición e integración de varios operadores ha sido uno de los elementos destacables de dicho proceso. Estas circunstancias han requerido (y requieren) de un gran esfuerzo de gestión y transformación en los procesos de la organización. La Ciberseguridad no es un proceso más en este entorno. Al aumento de la notoriedad la organización y la integración de TI ya operativos, debemos unir el aumento de la concienciación en ciberseguridad por parte del management y los consejos de administración y el incremento de amenazas e incidencias de seguridad en todos los sectores. Por ello, Grupo MásMóvil está embarcado en un proceso de transformación de la gestión de la ciberseguridad que le permita apoyar su ambiciosa estrategia empresarial de una manera eficiente e innovadora".

Ponentes:

Daniel Martínez es CISO del Grupo MásMóvil, las marcas del grupo son MásMóvil, Yoigo, PepePhone, Llamayá y Lebara. Anteriormente trabajó en Indra/Minsait como Head of Infrastructure Security. Experto en Seguridad en Redes y Sistemas TIC con casi 20 años de experiencia en el Sector. MCT de Microsoft e ingeniero certificado en ForeScout, FireEye, StormShield, Stonesoft, Aruba, Array, Bradford, Allot, Clearswitf y otras tecnologías. Ha diseñado arquitecturas de Operadores de Wifi y Wimax, en distintos países y ha diseñado comunicaciones satélite seguras para el ministerio de Defensa y la OTAN. Ha participado en numerosas iniciativas, proyectos y comunidades Open Source. Colaborador y ponente en diversos Másteres y Conferencias de Comunicaciones y Seguridad.

Joaquín Castillón es Director del área de Advisory Services de EY, con más de 20 años de experiencia en el asesoramiento 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 experiencia en proyectos internacionales de gran envergadura. Licenciado en Administración y Dirección de Empresas, Executive MBA por el Instituto de Empresa, Posgrado en Informática y Máster en Seguridad TIC; es certificado CGEIT, CISA, ITIL, ISO 22301 LA, ISO 27001 LA, OPST y SAP GRC (Risk Management, Process Control y Fraud Management).

"GRUPO EUSKALTEL: Transformación digital, Operaciones de Seguridad y Protección del cliente final"

Sinopsis. "La transformación digital que está llevando a cabo el Grupo Euskaltel obliga a que términos aparentemente contradictorios tengan que ponerse de acuerdo, no solo para proteger las operaciones internas, sino también para aportar un valor diferencial al negocio. En la ponencia se describirá la puesta en marcha del Centro Integrado de Operaciones de Seguridad del Grupo Euskaltel, en un enfoque orientado a la minimización del riesgo corporativo, centrado y guiado por Inteligencia y cómo desde las operaciones de seguridad puede soportarse la creación de nuevos productos y servicios y dar una capa de protección frente a ciberamenazas al cliente final, tanto en la operación de soluciones específicas de ciberseguridad como en la protección de soluciones específicas de productos generalistas".

Ponentes:

Idoia Uriarte es CISO del Grupo Euskaltel, que incluye las marcas R, Telecable, RACCtel y Euskaltel. En la actualidad es la responsable del área de Ciberseguridad, encargándose de la gestión de la seguridad de la información, la seguridad física y la continuidad del negocio. Todo ello tanto para los sistemas de información (que dan soporte a los procesos del grupo) como para la red (que da soporte a los servicios prestados a los clientes) y demás activos, alineando la seguridad digital con los objetivos del negocio y la estrategia del Grupo Euskaltel. Ingeniera de Telecomunicaciones por la UPV, Máster en Gestión de Innovación por la Deusto Business Schoool/Cambridge Judge Business School y en Administración de Empresas por Eseune, cuenta con 25 años de experiencia en el sector de las Telecomunicaciones, en áreas de Ingeniería, Operación y Mantenimiento, Innovación, Desarrollo de Negocio...

Jorge Hurtado es Vicepresidente del área de servicios gestionados en S21sec. Ingeniero de Telecomunicaciones por la UPM y PIC de la Deusto Business School, es miembro del Comité Ejecutivo de la compañía, liderando el área de Certificación y miembro del Comité Operativo del Centro de Estudios de Movilidad en ISMS Forum. Hurtado ha desarrollado su carrera profesional enfocado en el área de Ciberseguridad, donde ha trabajado desde hace más de 20 años en compañías nacionales y multinacionales como GMV, Germinus, CGI o Capgemini en España, Estados Unidos y Latinoamérica. Entre otras funciones, trabaja como coordinador ejecutivo del servicio DFIR de S21sec para la coordinación Extremo a Extremo de Incidentes de Seguridad.

SEGUNDO MÓDULO, 24 DE ABRIL

09:00h.	Entrega de documentación	
09:30h.	Ponencia:	**CODERE: La apuesta por el SOC virtual**
	Ponentes:	**Luis Miguel Brejano**, CISO de CODERE
		Luis Muñoz, Director Comercial de AIUKEN Cybersecurity
10:00h.	Coloquio	
10:05h.	Ponencia:	**CODERE: Los retos de la ciberseguridad en el sector del juego y cómo trasladarlos a un programa de transferencia de riesgos**
	Ponentes:	**José Luis Sebastián**, Jefe de Compras - Coordinador Corporativo de Seguros. CODERE
		Claudia Gómez, Directora de Líneas Financieras & Aon Cyber Solutions. AON España
10:35h.	Coloquio	
10:40h.	Pausa-café	
11:15h.	Ponencia:	**SUEZ ESPAÑA: Cuando las barbas de tu vecino veas afeitar, pon las tuyas a remojar. El riesgo en proveedores**
	Ponentes:	**Sergi Carmona**, CISO de SUEZ ESPAÑA
		Gerard Cervelló, Director de Operaciones de BLUELIV
11:45h.	Coloquio	
11:50h.	Ponencia:	**AENA: El estado del arte de una Oficina de Seguridad en una Infraestructura Crítica**
	Ponentes:	**Cándido Arregui**, CISO de AENA
		Andrea De Nigris, Information Security Service Manager. CAPGEMINI
12:20h.	Coloquio	
12:25h.	Ponencia:	**RENFE: Las amenazas avanzan. ¿Avanzan los métodos de detección?**
	Ponentes:	**Francisco Lázaro**, CISO y DPO de RENFE
		Isabel Tristán, Directora Comercial de Soluciones de IBM Security
12:55h.	Coloquio	
13:00h.	Ponencia:	**FNMT: Identidad digital basada en Blockchain: las soluciones de la Fábrica Nacional de Moneda y Timbre**
	Ponentes:	**Ángel Laín**, Responsable de Desarrollo de Negocio de la FNMT
		Antonio Requena, Socio. Business Security Solutions. PwC
13:30h.	Coloquio	
13:35h.	Almuerzo	
15:30h.	Ponencia:	**SANTALUCÍA: Automatización con Service Now/ SecOps de la gestión de incidentes y vulnerabilidades. Alineamiento de Seguridad, TI y Negocio**
	Ponentes:	**Francisco Javier Santos**, Director de Seguridad Global (CSO) del Grupo SANTALUCÍA
		Sergio Gómez Rodríguez, Senior Manager de Ciberseguridad en IT Advisory de KPMG
16:00h.	Coloquio	
16:05h.	Ponencia:	**ACCENTURE: Organización y gestión de la ciberseguridad a escala global**
	Ponentes:	**Ignacio Horcajo**, Former CISO team & Director de Infraestructuras en Latam, África, Middle East y Sur de Europa. ACCENTURE
		Floren Molina, Responsable de CiberDefensa y MSS de Iberia. ACCENTURE
16:35h.	Coloquio	
16:40h.	Fin del segundo módulo	
19:30h.	**Cena de la Ciberseguridad y entrega de los XVI Premios SIC**	

"CODERE: La apuesta por el SOC virtual"

Sinopsis. "En el marco de su Plan Director de Seguridad, a comienzos de 2018, Codere abordó la selección y despliegue de un servicio gestionado de ciberseguridad desde un SOC. Tras un minucioso proceso de análisis de la oferta de servicios en España, considerando capacidades, madurez, catálogo de servicios y modelo de servicio, de un amplio abanico de proveedores, se escogió el SOC virtual ofertado por Aiuken. La ponencia describe el proceso de selección, sus resultados, las características fundamentales del VSOC, el estado actual del proyecto y su valoración".

Ponentes:

Luis Miguel Brejano es CISO Corporativo de Codere desde 2017. Anteriormente fue CISO en Altamira Asset Management. Desarrolló su carrera en los departamentos de seguridad de Ono y Vodafone como Jefe de Seguridad Corporativa y Security Specialist, respectivamente. Tiene una dilatada experiencia en entornos de ciberseguridad Telco/Banca y consultoría tecnológica. Es Ingeniero en Informática y MBA por la Universidad Politécnica de Madrid, Auditor CISA y miembro de ISACA.

Luis Muñoz es Director Comercial de Aiuken Cybersecurity. Ejecutivo con más de 30 años de experiencia en ventas y desarrollo de negocio en empresas de tecnología y comunicaciones tales como: IBM, NCR, Tandem, Amdahl, Mnemo o Quantis, Muñoz posee la licenciatura en Ingeniería Geológica por la Universidad Complutense de Madrid.

"CODERE: Los retos de la ciberseguridad en el sector del juego y cómo trasladarlos a un programa de transferencia de riesgos"

Sinopsis. "La conferencia versará en presentar un riesgo diferente y peculiar, el negocio del juego en materia de riesgos tecnológicos y de delitos. Se analizarán las dificultades de implementación a escala multinacional de un programa homogéneo, el valor que aporta el seguro para el grupo Codere más allá del pago de las pérdidas económicas y cuáles son los próximos retos. Todo ello bajo la perspectiva de un diseño de seguro a medida, las complejidades y dificultades que tiene el mercado asegurador para dar encaje a este riesgo y como por el momento vamos lentos en encontrar soluciones combinadas ciber y delitos".

Ponentes:

José Luis Sebastián es Jefe de Compras – Coordinador Corporativo de Seguros de Codere. Ingeniero Industrial (Mecánica y Máquinas) por la Universidad Politécnica de Madrid y Executive MBA por la Universidad Pontifica de Comillas (ICADE-ICAI), entre sus responsabilidades y logros se encuentra el montaje del programa internacional de Seguros de Codere, incluyendo Ciber Riesgos y Crimen. Sebastián es el responsable máximo del departamento de compras de la empresa (no core) y Coordinador corporativo de seguros a nivel mundial (8 países). Actualmente imparte clase como profesor en el Máster de Dirección y Gestión Patrimonial y Facility management de la Universidad Europea en Madrid, y ha impartido también clases en la Universidad Alfonso X El Sabio y en la Universidad de Extremadura.

Claudia Gómez es Directora de la Specialty de Líneas Financieras y Aon Cyber Solutions en Aon España. Cuenta con más de 20 años de experiencia en el sector de la intermediación, fundamentalmente en grandes riesgos industriales, sector financiero y otros riesgos complejos. Desde el año 2012 ha participado activamente en el desarrollo de soluciones aseguradoras y de consultoría de riesgos asegurables relacionados con la ciberseguridad y tecnologías de la información.

"SUEZ España: Cuando las barbas de tu vecino veas afeitar, pon las tuyas a remojar. El riesgo en proveedores"

Sinopsis. "Los proveedores tienen una serie de activos que están directamente o indirectamente relacionados con las compañías contratantes, ya sea por redes de ordenadores, por datos o por personas. Cuando estos proveedores sufren algún tipo de amenaza de seguridad, el riesgo asociado puede tener un fuerte impacto en las organizaciones contratantes. Por ejemplo, esto ocurrió con WannaCry en diferentes partes del mundo. Esta es la razón por la que mediante los modelos matemáticos actuales, la capacidad de ingestión de datos externos y la capacidad de procesamiento de datos, es esencial para disponer de una serie de indicadores que permitan visualizar de forma pragmática la posición de ciberseguridad de proveedores críticos tal como se percibe desde el exterior, de cara a que puedan mejorar su desempeño. Todo ello para ofrecer una visión independiente de la posición de ciberseguridad vista desde fuera del perímetro, a fin de conocer cómo puede impactar en los contratantes.
En esta ponencia, Suez España ha contado con Blueliv para el desarrollo de un sistema de "scoring" de ayuda a la toma de decisiones conforme a la posición de ciberseguridad de sus proveedores para diferentes casos de uso, que serán expuestos durante la conferencia".

Ponentes:

Sergi Carmona es CISO de Suez Spain. Ingeniero Informático con Máster en Cybersecurity Management por la UPC, es especialista en Ciberseguridad de Sistemas de Control Industrial. Los últimos años los ha dedicado de forma intensa a los aspectos de ciberprotección en sistemas de automatización y control industrial, en especial procesos soportados por Infraestructuras Críticas. Es el coordinador de proyectos de innovación en Ciberseguridad con una visión integral en IT, OT e IoT.

Gerard Cervelló es Director de Operaciones de Blueliv. Ingeniero de Telecomunicaciones por la Universidad Politécnica de Cataluña, cuenta con 20 años de experiencia en la industria TIC, con especial foco en criptografía aplicada y ciberseguridad. En su dilatada carrera ha trabajado en varios países, incluyendo Estados Unidos y Emiratos Árabes Unidos, tanto en grandes empresas como Philips, como en *start ups* como iSOCO o Scytl Secure Electronic Voting, donde ocupó diversas posiciones que permitieron a la empresa dominar el mercado del cibervoto. Cervelló es, además, autor de varios artículos en revistas internacionales, coautor de tres patentes y ha asesorado a varios gobiernos sobre cómo implementar elecciones ciberseguras.

"AENA: Estado del arte de una Oficina de Seguridad en una Infraestructura Crítica"

Sinopsis. "Gestionar una oficina de seguridad es en sí mismo un tema complejo pero si además su día a día tiene lugar en un entorno de infraestructura crítica, el hecho se convierte en todo un reto, tanto por los tipos de incidentes y el impacto que tienen los mismos, como por las nuevas regulaciones, la evolución de la tecnología, y la relación con la administración y terceros... Durante la presentación se especificará como se asume el reto desde Capgemini para gestionar la oficina de Seguridad en Aena".

Ponentes:

Cándido Arregui es CISO de Aena. Actualmente es jefe del Departamento de Seguridad TIC (CISO) en Aena SME, S.A. Es doctor en Ingeniería Aeronáutica por la Universidad Politécnica de Madrid, técnico superior de la Edificación por la Universidad Nacional de Educación a Distancia, licenciado en Ciencias Físicas por la Universidad Autónoma de Madrid, CISM por ISACA y Director de Seguridad por el Ministerio del Interior. Con más de 15 años de experiencia en el sector TIC, actualmente forma parte de mesas y grupos de trabajo donde se aborda la seguridad integral en el sector del transporte aéreo.

Andrea De Nigris es Information Security Service Manager en Capgemini. Actualmente gerencia el servicio de la Oficina de Seguridad de Aena SME, S.A. Es licenciado en Ingeniería en Telecomunicaciones por el Politécnico de Turín, Máster en Seguridad de la Información por la Universidad Camilo José Cela e IMF Business School, CISM por ISACA, Auditor Interno de SGSI por Bureau Veritas, Project Manager Profesional por PMI. Con más de 11 años de experiencia en ciberseguridad como analista de seguridad, integrador y preventa de soluciones de ciberseguridad y consultor GRC.

"RENFE: Las amenazas avanzan. ¿Avanzan los métodos de detección?"

Sinopsis. "Es un hecho comúnmente aceptado que el cibercrimen cada vez se sofistica más y pone constantemente a prueba las medidas de seguridad adoptadas por las organizaciones, los procesos y las tecnologías. Por tanto, cada vez es más necesario adoptar una aproximación proactiva en el proceso de detección de amenazas, para así evitar, o al menos minimizar, el posible impacto en el negocio".

Ponentes:

Francisco Lázaro es CISO y DPO de Renfe. Igualmente es Director de Seguridad, Director del Centro de Estudios de Movilidad e Internet de las cosas del ISMS Forum, Presidente del Grupo de Calidad y Seguridad de la Asociación de Usuarios de Telecomunicaciones y Sistemas de Información (AUTELSI) y cuenta con la acreditaciones CDPP (Certified Data Privacy Professional) y CCSP (Certified Cyber Security Professional). Lázaro es experto en Normalización y profesor en diversos cursos y másteres universitarios en Seguridad de la Información.

Isabel Tristán es Directora Comercial de Soluciones de IBM Security. Ha desarrollado su carrera profesional durante más de 10 años en la compañía, ocupando diversas posiciones en las áreas de Continuidad de Negocio, Analytics y, por último, en Seguridad de la Información desde la creación de la unidad de IBM Security en 2012. Actualmente lidera el departamento comercial de estas soluciones, desde donde ayudan a empresas a mejorar su posición de Ciberseguridad y Protección de los activos críticos de las compañías. Es Ingeniera Superior de Telecomunicaciones por la Universidad de Sevilla y MBA por la Universidad Autónoma de Madrid.

"FNMT: Identidad digital basada en Blockchain: Las soluciones de la Fábrica Nacional de Moneda y Timbre"

Sinopsis. "En la ponencia se presentará la plataforma Blockchain que la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM) ha desarrollado con la ayuda de PwC, y que como aplicativo de partida y fundamental evolucionará sus servicios actuales de certificación, dando solución al nuevo paradigma de identidad digital, tanto en el ámbito del sector público, como para el contexto empresarial.

Los nuevos servicios basados en Blockchain permitirán la Gestión de las Identidades tanto de personas físicas como jurídicas, y facilitarán la utilización y verificación de todo tipo de atributos a los que esté sujeta una determinada credencial, permitiendo la gestión selectiva de información y atributos que se podrán compartir con distintos actores. El objetivo último es que sea posible acceder a un conjunto de servicios en los que elegir qué información se comparte con un tercero determinado, con la seguridad para todas las partes de que dicha información es verdadera.

Estas capacidades funcionales serán de gran aplicación, entre otros, en los ámbitos sanitarios, académico, o financiero, para distintas finalidades. El formato flexible de credenciales verificables permitirá la interacción con la privacidad, siguiendo el principio de protección de datos central de minimización de los datos, así como la simplificación de procesos de diligencia debida para cumplimientos regulatorios del tipo KYC o AML".

Ponentes:

Ángel Laín es Jefe de Área de Calidad, Desarrollo de negocio y Cumplimiento normativo de la FNMT. Es Graduado en Ingeniería Telemática e Ingeniero Técnico de Telecomunicaciones, ambos títulos por la Universidad Politécnica de Madrid. Su carrera profesional ha estado ligada al sector tecnológico, trabajando en empresas como IBM, o en los departamentos de FNMT dedicados a tarjetas criptográficas o Ceres. En este último departamento lleva trabajando más de 15 años. Participa en diversos foros relacionados con el uso de las TIC en la Administración, como la Comisión Ministerial de Administración Digital del Ministerio de Hacienda, el grupo de trabajo de firma e identidad del CDTIC o el Comité de Nuevas Tecnologías de la FNMT.

Antonio Requena es Socio de Business Security Solutions en PwC. Ingeniero de Telecomunicaciones y MBA por la EOI, lidera la práctica de servicios de Blockchain de PwC España, dentro de la unidad de negocio BSS (Business Security Solutions): desde la conceptualización de nuevos casos de negocio, transformación de procesos, soporte al lanzamiento de ICOs, e implementación de las soluciones. Además, dentro de BSS, centra su actividad en los sectores de Energía, Gobierno, Tráfico y Transporte, Sanidad y Turismo, donde atesora una amplia experiencia y conocimiento de mercado, en los principales organismos públicos y entidades de referencia a nivel nacional.

"SANTALUCÍA: Automatización con Service Now/SecOps de la gestión de incidentes y vulnerabilidades. Alineamiento de Seguridad, TI y Negocio"

Sinopsis. **"**Los equipos de seguridad actualmente se encuentran saturados de alertas e información relativa a vulnerabilidades de un creciente número de fuentes aisladas de información; Antivirus, herramientas automáticas de detección de vulnerabilidades, análisis estático de código fuente, campañas de pentesting manuales, etc. La priorización de estos incidentes y vulnerabilidades en base al potencial impacto en los procesos de negocio, la certeza de un conocimiento detallado de la interdependencia entre los distintos activos que dan soporte a los mismos, así como la automatización previa de los distintos flujos de trabajo y la delegación automática entre los distintos actores involucrados (internos y externos a la compañía), son las claves para una resolución eficiente".

Ponentes:

Francisco Javier Santos, Director de Seguridad Global (CSO) del Grupo Santalucía. Ingeniero Superior Industrial, cuenta con una solvente y longeva trayectoria profesional. Con anterioridad ocupó el cargo de Director de Ciberseguridad en IT Advisory desde 2014 en KPMG. También, ha trabajado en Atos Origin, Ernst & Young y WISeKey ELA (España y Latinoamérica). Desde 2008 a 2014, fue el CISO de ONO. Posee la Cruz al Mérito Policial con distintivo blanco otorgada por el Ministerio del Interior en 2013 y es Premio SIC 2018. Santos lidera las políticas, directrices y estándares de seguridad en su actual compañía.

Sergio Gómez Rodríguez, Senior Manager de Ciberseguridad en IT Advisory de KPMG. Experto en consultoría de Riesgos Tecnológicos y Seguridad de la Información a nivel nacional e internacional, participa en la gestión y ejecución de un amplio número de iniciativas en el ámbito de la seguridad y protección de sistemas en empresas de primer nivel; definición y despliegue de planes estratégicos de seguridad, análisis y gestión de riesgos, definición de funciones y estructuras organizativas, certificación de sistemas de gestión, auditorias TI, control interno y planes de continuidad de negocio. Cuenta con las certificaciones profesionales CISA, CISM, ISO 27001 e ISO 22301.

"ACCENTURE: Organización y gestión de la ciberseguridad a escala global"

Sinopsis. "La postura de Accenture frente a la seguridad de la información es clave para garantizar no solo la seguridad de su información sino también la de sus clientes. Para ello en 2011 se crea la figura del CISO único global, que establece diferentes áreas de trabajo: Governance, Certificaciones, CDP (programa especifico para cada cliente), Herramientas y software de seguridad, Incidence Management (CIRT único global)… La conferencia estará centrada en la parte del modelo de gobierno, relaciones entre el CISO y las diferentes organizaciones (no solo el CIO) y, sobre todo, en la parte de prevención, concienciación de los empleados y gestión automatizada de incidentes a escala global".

Ponentes:

Ignacio Horcajo es Director de Operaciones de IT para más de 40 países en Europa, Latinoamérica y África y más de 100.000 empleados, al tiempo que es responsable de Information Security para España, Portugal, Israel, países africanos, Turquía y Oriente Medio, implantando todas las acciones a nivel CISO. Horcajo es miembro del equipo de Inclusion & Diversity Accenture Iberia Committee (Age Diversity lead), miembro del Spain Social Responsibility Committee, y miembro del consejo en la Cátedra de Innovación UAM-Accenture.

Floren Molina es Responsable de CiberDefensa y MSS de Iberia. Cuenta con amplia experiencia en el área de la Seguridad IT, desde sus inicios en S21sec como uno de los cofundadores, ha ido trabajando en el área de *pentesting* tradicionalmente, hasta que se hizo cargo del departamento a nivel de España y de su remodelación; más adelante estuvo a cargo del desarrollo de negocio de Auditoría y el área de ACSS. Ha participado en la mayor parte de los procesos de innovación en S21sec, es mentor en la aceleradora BerriUp en San Sebastián y asesor técnico en inversiones en el VC Easo Ventures. Ha participado como ponente internacional en varias conferencias y ha colaborado como asesor externo en varios comités de seguridad de grandes compañías.

TERCER MÓDULO, 25 DE ABRIL

09:15h. Entrega de documentación

09:30h. Ponencia: **MAPFRE: Gestión integral operativa de la (ciber)seguridad**

Ponentes: **Daniel Largacha**, Security Director Head of Global Control Center-CERT. MAPFRE

Cristóbal de Donesteve, Director de Ventas para España de Cipher, a Prosegur company

10:00h. Coloquio

10:05h. Ponencia: **Retos de ciberseguridad en entornos críticos: El segmento de control terreno de GALILEO**

Ponentes: **José Ramón Coz**, GNSS Cyber Internal Auditor (CIA). ESA-AGENCIA ESPACIAL EUROPEA

Juan Antonio Abánades, Head of GCS Segment Security. GMV

10:35h. Coloquio

10:40h. Pausa-café

11:15h. Ponencia: **ACCIONA: La ciberseguridad en el servicio "Motosharing Acciona Mobility"**

Ponentes: **Juan Carlos Sánchez**, Gerente de Ciberseguridad en ACCIONA

Enrique Domínguez, Director Estratégico de ENTELGY INNOTEC Security

11:45h. Coloquio

11:50h. Ponencia: **GENERALITAT VALENCIANA: Integración segura de dispositivos industriales**

Ponentes: **Carmen Serrano**, Jefa de Servicio de Seguridad en la D.G. de TIC de la Conselleria de Hacienda y Modelo Económico, en la GENERALITAT VALENCIANA

Maite Moreno, Jefa de Servicio en el Área de Seguridad y Ciberinteligencia de S2 GRUPO

12:20h. Coloquio

12:25h. Ponencia: **GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL: La seguridad más allá del cumplimiento normativo**

Ponentes: **Santiago Rodríguez**, Director del Centro de Seguridad de la Información de la Gerencia de Informática de la Seguridad Social-GISS

Jorge Sendra, Security Account Executive. MICRO FOCUS

12:55h. Coloquio

13:00h. **Conferencia de clausura:**

El Centro de Operaciones de Ciberseguridad para la Administración General del Estado

Ponentes: **Miguel Ángel Amutio**, Director de la División de Planificación y Coordinación de Ciberseguridad de la Secretaría General de la Administración Digital. MINISTERIO DE POLÍTICA TERRITORIAL Y FUNCIÓN PÚBLICA

Pablo López, Jefe del Área de Normativa y Servicios de Ciberseguridad del Departamento de Ciberseguridad del CCN CENTRO CRIPTOLÓGICO NACIONAL

14:00h. Coloquio

14:05h. Almuerzo

Fin del tercer módulo y fin de Securmática 2019

"MAPFRE: Gestión integral operativa de la (ciber)seguridad"

Sinopsis. "La seguridad en sí no es un fin sino un proceso que se debe adaptar a cada organización. A pesar del gran número de estándares, *frameworks* y modelos de gestión de riesgo, lamentablemente no existen modelos que se puedan ajustar de forma sencilla a la organización (al más puro estilo *one size fits all*) y el principal objetivo de un responsable de seguridad debe ser el de aterrizar un modelo conceptual que se encaje en los pilares de una empresa. En la conferencia vamos a mostrar nuestra visión particular de la parte más activa de nuestro modelo".

Ponentes:

Daniel Largacha, Subdirector del Centro de Control General de Mapfre. Ingeniero en Informática por la Universidad Politécnica de Madrid, con más de 18 años en seguridad, cuenta con varias certificaciones relacionadas con la TI y Seguridad (CISA, CISSP, CHFI, ITIL y 27001 Lead implementer) y el título de Director de Seguridad por el Ministerio del Interior. Empezó su carrera profesional en Telefónica, y ha complementado su carrera con la experiencia que ha ido acumulando tras su paso por la consultora Deloitte. Desde hace 13 años se unió a Mapfre donde dirige actualmente el Centro de Operaciones de Seguridad. Compagina su trabajo con actividades docentes en varios organismos como el IE, y de fomento de la concienciación y conocimiento en seguridad en la asociación ISMS como director del Centro de Ciberseguridad.

Cristóbal de Donesteve, Director de Ventas para España de Cipher, a Prosegur company. Licenciado en Empresariales por la Suffolk University, PDD-Executive IESE Business School por la Universidad de Navarra y Director de Seguridad por el Cuerpo Nacional de Policía-Seguridad Privada, empezó su trayectoria profesional en Coca Cola, y prosiguió su carrera en empresas como Tech Data, Logitech, Tele Atlas y Tom Tom. Desde hace más de 8 años se unió a Prosegur, donde dirige actualmente el equipo de ventas de Cipher, a Prosegur company, como Director Comercial.

"Retos de ciberseguridad en entornos críticos: el segmento de control terreno de GALILEO"

Sinopsis. "GMV fue adjudicatario en 2018 del contrato de la Agencia Espacial Europea para el diseño, evolución, despliegue y mantenimiento del segmento de control terreno de Galileo en su segunda fase de explotación. Como parte del contrato, GMV proporciona un conjunto de servicios de ciberseguridad, incluyendo ingeniería de seguridad, desarrollo seguro, gestión de vulnerabilidades, acreditación e implementación de un programa de auditoría, entre otros. En esta sesión se expondrán los retos a los que se enfrentan los auditores, como el de la planificación, y se esbozarán algunas de las lecciones aprendidas sobre la auditoría de ciberseguridad de los grandes sistemas y programas públicos, con grandes presupuestos en entornos críticos de alta seguridad".

Ponentes:

José Ramón Coz, Auditor Interno Cyber para la Agencia Espacial Europea, ESA. Es Doctor en Economía por la Universidad Complutense de Madrid y Doctor en Ingeniería Informática por la UNED. Además, es Licenciado en Ciencias Físicas, Grado Máster en Economía, Graduado Especialista en Gestión Pública y Máster en Dirección de Tecnologías de la Información por el IDE-CESEM. Posee más de una docena de certificaciones internacionales en Tecnologías de la Información y varios postgrados en Telecomunicaciones. Tiene más de veinte años de experiencia en el campo de la Auditoría y la Ciberseguridad. Es, además, profesor e investigador en varias instituciones, universidades y escuelas de negocio. Ha realizado multitud de publicaciones científicas y de tecnología, es revisor de varias revistas de ciencia y tecnología internacionales, ha publicado artículos en SIC y es miembro de varias comisiones y asociaciones de auditoría y tecnologías de la información.

Juan Antonio Abánades, PMP, CISSP, CISM, ejerce actualmente en GMV como Head of Security en el contrato del Segmento de Control Terreno (GCS) de Galileo. Abánades es Licenciado en Informática por la Universidad Politécnica de Madrid con más de 20 años de experiencia en el campo de la ciberseguridad. Antes de involucrase en Galileo ejerció como Business Partner de la Vertical Internacional y como Jefe de la Sección de Tecnologías de Ciberseguridad de GMV, liderando proyectos de seguridad para grandes clientes en múltiples sectores en España, resto de Europa y Estados Unidos. Posee, además, un Global MBA por el IEB y colabora habitualmente con (ISC)2 en calidad de Subject Matter Expert.

"ACCIONA: la ciberseguridad en el servicio Motosharing ACCIONA Mobility"

Sinopsis. "Motosharing de ACCIONA Mobility es un servicio de alquiler de motos eléctricas de 125 cc que permite desplazar al usuario por su ciudad de manera cómoda y sostenible. Para comenzar a utilizar el servicio, el usuario sólo tiene que descargarse la app, registrarse y localizar la moto más cercana. Asimismo la app funciona como llave para arrancar la moto y abrir el baúl.
Acciona y Entelgy Innotec Security presentan los retos de analizar la seguridad de todos los elementos de la plataforma de motosharing, desde las aplicaciones móviles, hasta la centralita de la moto eléctrica, pasando por las comunicaciones 4G, la geolocalización y los web services que permiten funcionar a la plataforma".

Ponentes:

Juan Carlos Sánchez es Gerente de Ciberseguridad en Acciona. Cursó estudios de Matemáticas en la Universidad Complutense de Madrid. Durante sus 25 años de carrera profesional ha tenido la oportunidad de trabajar en los más diversos ámbitos del mundo de TIC: arquitectura y desarrollo de aplicaciones, ingeniería y calidad del software, arquitectura de sistemas y comunicaciones, pasando por la innovación y la gestión de proyectos. En los últimos diez años se ha centrado en el ámbito de Ciberseguridad, inicialmente en entidades del sector financiero y actualmente en Acciona, una de las principales corporaciones empresariales españolas, líder en la promoción y gestión de infraestructuras (construcción, industrial, agua y servicios) y energías renovables. El reto en Acciona es desarrollar un proyecto integral de Ciberseguridad multi-país y multi-negocio apoyado en las mejores prácticas y plataformas con un enfoque muy práctico y adaptando la gestión del riesgo a la actividad de cada uno de los negocios.

Enrique Domínguez es Director Estratégico de Entelgy Innotec Security. Actualmente dirige el área de Estrategia, enfocada en lograr el éxito y sostenibilidad a largo plazo de la división, impulsando la transformación de Entelgy Innotec Security para enfrentarse a los retos actuales y futuros. Ingeniero en Informática por la Universidad de Zaragoza y MBA por ESADE, Domínguez ha desarrollado su carrera de más de 10 años en el terreno de la consultoría, especializándose en gestión de la ciberseguridad en ámbitos internacionales y continuidad de negocio, liderando proyectos de referencia en importantes entidades en España, Latinoamérica, Turquía o Estados Unidos. Está certificado profesionalmente como CISSP por (ISC)2, CISM y CISA por ISACA, ISO 27001 Lead Auditor por BSI y Profesional Nivel Negro en Ciberseguridad Industrial por el CCI. Ha sido ponente en materia de ciberseguridad en España y LATAM, en universidades y foros como ISACA, ENISE, Legal Management Forum o World Football Summit y publicado artículos en medios especializados en tecnología y ciberseguridad.

"GENERALITAT VALENCIANA: Integración segura de dispositivos industriales"

Sinopsis. "Las administraciones públicas, principalmente dedicadas a la gestión administrativa donde sus redes están orientadas a la conexión de ordenadores, se han visto invadidas por dispositivos industriales que han aprovechado la existencia de estas redes para ser conectados. La demanda creciente de conectividad y acceso desde el exterior a estos dispositivos plantea un nuevo reto para la seguridad. Abordar la problemática que supone por un lado la conexión a la red de dispositivos IoT y la complejidad de los riesgos y amenazas específicos de los dispositivos médicos hace necesario analizar la situación y definir un marco de seguridad industrial. En esta ponencia se mostrará la problemática analizada y el enfoque de solución definido por CSIRT-CV para la integración segura de dispositivos IoT en la red corporativa y la seguridad en dispositivos médicos".

Ponentes:

Carmen Serrano es Jefa del Servicio de Seguridad de la Dirección General de TIC en la Consellería de Hacienda y Modelo Económico de la Generalitat Valenciana. Ingeniera Informática por la Universidad Politécnica de Valencia, es funcionaria de carrera de la Generalitat Valenciana adscrita al cuerpo de Administración Especial Superior Técnico de Ingeniería Informática. Junto a su cargo actual, que ocupa desde 2012, también es Responsable de Seguridad de la Generalitat, y miembro del Comité de Seguridad de la Información de las AA.PP. Dirige el desarrollo de la estrategia de seguridad de la D.G. de TIC y el Centro de Seguridad TIC de la Comunitat Valenciana (CSIRT-CV). Es Premio SIC.

Maite Moreno es Jefa de Servicio en el Área de Seguridad y Ciberinteligencia de S2Grupo. Lleva más de 12 años dedicada a la ciberseguridad y especializándose en dirección, gestión y desarrollo de SOC/CSIRT avanzados, respuesta a incidentes e inteligencia de amenazas. Es Ingeniera de Telecomunicaciones por la UPV con diversas certificaciones en ciberseguridad. Durante los dos últimos años ha participado como docente colaboradora en el Máster en Inteligencia de Seguridad, Ciberdefensa y Protección de Infraestructuras Críticas de la Universidad Politécnica de Valencia y en el Máster en Ciberseguridad de la Universidad de Alicante, tutorizando además TFG/TFM especializados en Ciberseguridad. En S2Grupo además dirige ENIGMA, su escuela de alto rendimiento en formación en ciberseguridad.

"GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL: La seguridad más allá del cumplimiento normativo"

Sinopsis. "En un entorno altamente regulado donde cada vez más prima el servicio al ciudadano y la interoperabilidad, la seguridad se postula como el facilitador que hace posible gestionar el riesgo de forma proactiva y global.
Durante la ponencia, se expondrán los conceptos clave que permiten a la Gerencia Informática de la Seguridad Social, una de las principales instituciones nacionales, balancear y aprovechar sus recursos organizativos, capacidades de innovación tecnológica y factores humanos, para dar respuesta de forma segura a las necesidades de atención a los ciudadanos en un mundo crecientemente digital".

Ponentes:

Santiago Rodríguez es Director del Centro de Seguridad de la Información de la Gerencia de Informática de la Seguridad Social, organismo en el que ingresó por oposición en el año 2000. Desde entonces ha trabajado siempre en seguridad informática, especialmente en asuntos relacionados con los certificados digitales y firma electrónica, así como en todo lo relacionado con el control de acceso, las autorizaciones y la gestión de identidades.

Jorge Sendra es Security Account Executive en Micro Focus. Profesional con más de quince años de experiencia en Seguridad TIC, dispone de las certificaciones CISA, CISM, CRISC y C|CISO. Con anterioridad a su actual puesto ha desempeñado puestos de responsabilidad en empresas relevantes del sector, como son HPE, PwC, Oracle... ayudando a clientes de diferentes sectores en la gestión de los Riesgos Tecnológicos y de Seguridad de la Información. Es Ingeniero en Informática por la Universidad de Alicante.

CONFERENCIA DE CLAUSURA

"El Centro de Operaciones de Ciberseguridad para la Administración General del Estado"

Sinopsis. "El Centro de Operaciones de Ciberseguridad para la Administración General del Estado ha sido creado por Acuerdo de Consejo de Ministros el 15 de febrero de 2019. Consolida el Servicio Compartido de Seguridad Gestionada, declarado como servicio compartido por Acuerdo de la Comisión de Estrategia TIC el 15 de septiembre de 2015. Su finalidad es la prestación de servicios horizontales de ciberseguridad que aumenten la capacidad de vigilancia y detección de amenazas en las operaciones diarias de los sistemas de información y comunicaciones de la Administración General del Estado, así como la mejora de su capacidad de respuesta ante cualquier ataque. En esta ponencia se exponen los aspectos principales de ámbito del servicio, funciones, desarrollo, colaboración y responsabilidades".

Ponentes:

Miguel Ángel Amutio es Director de la División de Planificación y Coordinación de Ciberseguridad de la Secretaría General de Administración Digital, Ministerio de Política Territorial y Función Pública (MPTFP). Estudió en el Colegio La Salle de Deusto y es Licenciado en Informática por la Universidad de Deusto (1988). CISA, CISM, CRISC. Coordinador de la elaboración y desarrollo del Esquema Nacional de Seguridad (Real Decreto 3/2010) y de sus Instrucciones Técnicas de Seguridad; así como del Esquema Nacional de Interoperabilidad (Real Decreto 4/2010), y de sus Normas Técnicas de Interoperabilidad, junto con su documentación complementaria. Miembro de la delegación española en el Programa ISA^2 de la Unión Europea y, anteriormente, de los programas ISA, IDABC e IDA II, así como del Grupo del Plan de Acción de Administración Electrónica y del European Multi-Stakeholder Platform for ICT Standardization de la Comisión Europea.
Amutio también es miembro del Grupo de seguridad y privacidad en la economía digital de la OCDE (WPSPDE) y del Comité gestor del Arreglo de reconocimiento mutuo de los certificados de seguridad de TI (CCRA), además de Presidente del órgano técnico de normalización de AENOR AEN CTN 307 "Gestión de riesgos".

Pablo López es Jefe del Área de Normativa y Servicios de Ciberseguridad del departamento de Ciberseguridad del CCN-Centro Criptológico Nacional. Teniente Coronel, Cuerpo General, del Ejército del Aire. Especialista Criptólogo. Máster en Dirección de Sistemas y Tecnologías de la Información y las Comunicaciones.
Entre los cometidos de su actividad está la formación del personal especialista en seguridad de la Administración, el desarrollo de normativa CCN-STIC, la supervisión de acreditación de sistemas y la realización de auditorías de seguridad. Tiene más de 17 años de experiencia en todas estas actividades.

La XXIX edición de Securmática tuvo el honor de contar en su acto inaugural con **Julián Sánchez Melgar**, Fiscal General del Estado.

Más de 7.850 expertos han pasado por Securmática, un congreso que con sus 29 ediciones ya celebradas es el foro de intercambio de experiencias en ciberseguridad por excelencia.

// Premios SIC 2019 y Cena de la Ciberseguridad

En coincidencia con la XXX edición de Securmática, tendrá lugar el acto de entrega de los XVI 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 decimoquinta edición de los Premios SIC en 2018.

Fechas de celebración SECURMÁTICA 2019

Tendrá lugar los días 23, 24 y 25 de abril de 2019.

Lugar de celebración

La sede para su XXX aniversario es el HOTEL ELBA MADRID ALCALÁ, calle de Alcalá, 476. 28027 Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2019 recibirán las carpetas de congresistas con el programa oficial y la documentación –papel y pendrive– referente a las ponencias.
- Almuerzos y cafés.
- Cena de la Seguridad y entrega de los XVI Premios SIC (24 de abril).
- Diploma de asistencia.

Cuota de inscripción

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

Cuota	Hasta el 31 de marzo	Después del 31 de marzo
1 Módulo	450 € + 21% IVA	550 € + 21% IVA
2 Módulos	750 € + 21% IVA	900 € + 21% IVA
3 Módulos	900 € + 21% IVA	1.100 € + 21% IVA

Descuentos:

- Dos inscripciones de una misma empresa: 10% dto. cada una.
- Tres inscripciones y siguientes: 15% dto. cada una.
- Universidades: 25% dto. cada una.
- Inscripción solo al tercer módulo (día 25 de abril): 15% dto.

Proceso de solicitud de inscripción

- Por web: **www.securmatica.com**
- Por correo electrónico: info@securmatica.com
- Por correo convencional: enviando el boletín adjunto o fotocopia del mismo a:

EDICIONES CODA/REVISTA SIC c/ Goya, 39. 28001 Madrid (España)

- Abono de la cantidad correspondiente mediante transferencia nominativa a favor de **Ediciones CODA, S.L.**, a la siguiente cuenta bancaria: **IBAN: ES45 2038 1861 6160 0033 4847**

BANKIA. Oficina: O'Donnell, 53 - 28009 Madrid (España)

El justificante de dicha transferencia 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.

Acceso al lugar de celebración

NUEVA SEDE

HOTEL ELBA MADRID ALCALÁ
C/ Alcalá, 476. 28027 Madrid

Aparcamientos públicos:

- En el hotel. C/ Alcalá, 476.
- Aparcamiento La Fábrica. C/ Santa Leonor, 50. (a 8 minutos)
- Parking Homely Julián Camarillo I. C/ Albarracín, 27, (a 10 minutos)
- Parking Homely Julián Camarillo II. C/ Julian Camarillo, 17, (a 11 minutos)

Transporte:

- Metro: Línea 5. Suanzes (a 6 minutos) y Ciudad Lineal (a 7 minutos)
- Autobús: Líneas 77, 104. Paradas: Alcalá-Santa Leonor (a 2 minutos) y Alcalá-Alfonso Gómez (a 3 minutos)
- Aeropuerto: Madrid-Barajas (15 minutos en coche)
- Tren: Puerta de Atocha (18 minutos en coche)

Boletín de inscripción

Nombre y apellidos _____

Nombre y apellidos _____

Nombre y apellidos _____

Empresa _____ C.I.F. _____

Cargo _____

Dirección _____ Población _____

Código Postal _____ Teléfono _____ Fax _____

Persona de contacto, Departamento y teléfono para facturación _____

_____

☐ Módulo 1 Día 23 ☐ Módulo 2 Día 24 ☐ Módulo 3 Día 25 ☐ Deseo inscribirme a SECURMÁTICA 2019 Firma:

AFORO LIMITADO

Forma de pago: ☐ Talón ☐ Transferencia

Los datos personales que se solicitan, cuya finalidad es la formalización y seguimiento de su solicitud de inscripción al Congreso serán objeto de tratamiento por Ediciones Coda, S.L. Usted puede ejercitar sus derechos, reconocidos en la legislación vigente española y del resto de la UE sobre Protección de Datos de Carácter Personal (acceso, rectificación, supresión, limitación, oposición y, si aplicara al caso, portabilidad), en el domicilio del responsable del fichero: Ediciones Coda, S.L., C/ de Goya, 39, 2ª planta. 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**