SECURMÁTICA

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

25.26.27 abril 2017

La ciberseguridad aterriza en la alta dirección

PROGRAMA

Tendrá lugar en Madrid los días 25, 26 y 27 de abril

Securmática 2017: la ciberseguridad llega al gobierno corporativo

Los miembros de los órganos de gobierno y equipos de dirección de empresas avanzadas y los gestores públicos y gobernantes de estados modernos, empiezan a ubicar la ciberseguridad como uno de los pilares del cambio en el que sus organizaciones están inmersas para operar en la sociedad hipertecnificada en construcción, en la que una mala gestión del riesgo puede provocar que se emprendan procesos de transformación errados, propiciar situaciones de exposición a incumplimientos legales concatenados o poner en riesgo la continuidad de actividades por no haber valorado en su justo término el grado de resistencia del negocio a los ciberataques.

La ciberseguridad es, por la vía de los hechos, un recientísimo ingrediente del buen gobierno; y como tal debe ser tratado en todas sus manifestaciones: gestión, tecnología, regulación, procesos, organización, resultados, automatización, valor de marca, diferenciación, ventaja competitiva, reducción de costes, previsión… Por la rapidez propia de estos tiempos, resulta complicado encontrar profesionales y equipos humanos que sepan fundir negocios y TIC en una sola entidad. Pero una cosa es cierta: esos profesionales y equipos deben incorporar entre sus habilidades las de ciberseguridad. De no ser así, los órganos de gobierno de las corporaciones que los empleen estarán enfocando incorrectamente los procesos de transformación de los que dependen sus compañías. Y eso tiene un precio en el mercado.

El programa del XXVIII congreso global Securmática está configurado con el fin de brindar una visión actualizada de cómo se está transformando la ciberseguridad y, a su vez, de cómo se está incorporando a los procesos de transformación sectoriales y empresariales. Por ello, su lectura permitirá encontrar diversos sabores, a través de una cuidada selección de proyectos y conferencias: complejidad organizativa, modernización de sistemas corporativos de ciberseguridad, servicios gestionados con base en la inteligencia, la detección de anomalías, la 'securización' de sistemas de control industrial, la transferencia de ciberriesgos al sector asegurador, la automatización de la respuesta a incidentes, el análisis del contexto, la gestión de identidades, iniciativas de gestión global de riesgos de seguridad, el reto de la adaptación al RGPD y la futura transposición de la Directiva NIS al ordenamiento jurídico español.

■ 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 · AON Empower Results® · aruba a Hewlett Packard Enterprise company · Blueliv. · Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING · Deloitte. · EY Building a better working world · gmv INNOVATING SOLUTIONS · Hewlett Packard Enterprise · IBM · KPMG · Nextel S.A. Ingeniería y Consultoría · MONITOR PLUS A PLUS IT SOLUTION · pwc · S2 GRUPO

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

PRIMER MÓDULO, 25 DE ABRIL

08:45h. Entrega de documentación

09:15h. Ceremonia de apertura

10:00h. **Conferencia de inauguración**

Ponente: **Mar España Martí**, Directora de la Agencia Española de Protección de Datos.

10:20h. Ponencia: **La ciberseguridad en la transformación digital para Telefónica**

Ponente: **Chema Alonso**, Chief Data Officer (CDO) y Responsable de la Unidad de Seguridad Global de Telefónica.

10:50h. Coloquio

11:55h. **Pausa-café**

11:30h. Ponencia: **por confirmar**

Ponente: **por confirmar**

12:00h. Coloquio

12:05h. Ponencia: **CISO VS CISO**

Ponentes:

Santiago Moral Rubio, Global CISO de BBVA Group.

Pedro Ignacio Pastor Rivas, Head of Engineering Risk & Corporate Assurance Spain. Grupo BBVA.

12:35h. Coloquio

12:40h. Ponencia: **Grupo Inversis Banco: Protección inteligente en tiempo real ante amenazas a sistemas web transaccionales**

Ponentes:

Manuel Fernández, Director de Seguridad de la Información y Entorno Corporativo de Grupo Inversis Banco.

Juan Miguel Velasco, CEO de Aiuken Solutions.

13:10h. Coloquio

13:15h. Ponencia: **SAREB: Cuando la seguridad no es una opción**

Ponentes:

Gabriel Enrique Moliné Sosa, Gerente de Seguridad de la Información. SAREB.

Daniel López Rojo, Security Sales Executive para España y Portugal. HP Enterprise Services.

13:45h. Coloquio

13:50h. **Almuerzo**

15:50h. **Debate**: **Transposición de la Directiva NIS: el escenario para una nueva configuración de la Estructura Nacional de Ciberseguridad**

Participantes:

Ángel León Alcalde, Vocal Asesor en la Subdirección General de Servicios de Sociedad de la Información de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital del Mº de Energía, Turismo y Agenda Digital.

Luis Jiménez, Subdirector General del Centro Criptológico Nacional, CCN.

Fernando Sánchez, Director del Centro Nacional para la Protección de Infratestructuras Críticas, CNPIC.

Joaquín Castellón, Director Operativo del Departamento de Seguridad Nacional. Gabinete de la Presidencia del Gobierno.

Carlos Gómez López de Medina, Comandante Jefe del Mando Conjunto de Ciberdefensa.

17:00h. Fin del primer módulo

Conferencia de inauguración

Mar España Martí, Directora de la Agencia Española de Protección de Datos (AEPD). Licenciada en Derecho por la Universidad Pontificia de Comillas, Máster en Protección Internacional en Derechos Humanos por la Universidad de Alcalá y experta en gestión de entidades sin ánimo de lucro por la Fundación Luis Vives. Es funcionaria de carrera del Cuerpo Superior de Administradores Civiles del Estado en la especialidad jurídica desde 1989.En cuanto a su actividad académica, ha sido profesora del Máster de Protección Internacional de Derechos Humanos de la Universidad de Alcalá, profesora del Máster de Acción Política del Colegio de Abogados y la Universidad Rey Juan Carlos y profesora colaboradora de Derecho Administrativo en ICADE.

La ciberseguridad en la transformación digital para Telefónica

Sinopsis: En la conferencia se hablará de cuál es la visión de Telefónica respecto a la ciberseguridad como parte fundamental del negocio y la transformación interna de la compañía, así como la visión personal del ponente de cómo afrontar esta tarea en el futuro cercano.

Ponente:

Chema Alonso, es Chief Data Officer en Telefónica y miembro del Comité Ejecutivo de la compañía. Su misión allí es ocuparse de las unidades de negocio de CiberSeguridad (ElevenPaths) y BigData (LUCA), además de la transformación digital interna por medio de la 4ª Plataforma.

CISO VS. CISO

Sinopsis: Un grupo bancario multinacional debe respetar e integrar en su cultura las legislaciones y particularidades de los mercados en los que opera, sin por ello perder su identidad y estilo como entidad. La gestión de la ciberseguridad no escapa a esta circunstancia. En la conferencia, un CISO global y un CISO local expondrán las lecciones aprendidas en dos escenarios: el modelo organizativo en ciberseguridad y la gestión de multireguladores. Al tiempo explicarán las interrelaciones y la dinámica entre la estrategia global de ciberseguridad y la responsabilidad local.

Ponentes:

Santiago Moral Rubio es Global CISO de BBVA Group. 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 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, y posteriormente fue nombrado Director de IT Risk, Fraud & Security.

Pedro Ignacio Pastor Rivas es Head of Engineering Risk & Corporate Assurance Spain de Grupo BBVA. Ingeniero Civil Industrial por la Universidad de La Frontera (Chile) con el Máster Executive MBA por el IE, cuenta con diversas certificaciones incluida CISM. Pastor Rivas fue con anterioridad a su actual posición Head of ITRisk, Fraud & Security de BBVA en Chile y CISO de Banco Security. Tiene además una fructífera trayectoria profesional en los ámbitos de innovación, procesos y ciberseguridad.

SAREB: Cuando la seguridad no es una opción

Sinopsis: En julio de 2012 el Gobierno de España aprobó la creación de Sareb. Su nacimiento era una de las condiciones establecidas en el Memorándum de Entendimiento (MoU) firmado con los socios europeos para que las cajas con excesiva exposición al negocio inmobiliario pudieran recibir ayudas públicas. Sareb tiene la misión de liquidar antes de 2027 todos los activos financieros e inmobiliarios recibidos de estas entidades y su actividad es piedra angular para el saneamiento del sistema bancario español y la reactivación del mercado inmobiliario. En la conferencia, Sareb, en colaboración con HPE, explicará cómo ha afrontado el reto de dotar de la ciberseguridad necesaria a una sociedad con participación pública que recibió una cartera de activos valorados en más 50.000 millones de euros y que posee toda su infraestructura en la nube, al tiempo que planteará la forma de encarar diferentes desafíos: salvaguardar la reputación y el cumplimiento normativo, priorizar las amenazas y necesidades, cómo gestionar correctamente los recursos y, sobre todo, cómo poder dar un servicio fiable y escalable de ciberseguridad, alineando las necesidades del negocio con una correcta gestión de los riesgos que necesita evolucionar y madurar permanentemente.

Ponentes:

Gabriel Enrique Moliné Sosa es CISO/Gerente de Seguridad de la Información de SAREB. Dispone de varias especialidades: Gestión de Proyectos y servicios de Seguridad de la Información, gestión de centros de CiberSeguridad, Sistemas de Firma y Certificados Electrónicos, Privacidad, Recuperación ante Desastres, despliegue de Soluciones de

DEBATE

Transposición de la Directiva NIS: el escenario para una nueva configuración de la Estructura Nacional de Ciberseguridad

Propuesta: La estructura de la Ciberseguridad Nacional española se ha ido creando estos años en base a normas de distinto alcance, de diferente rango y que se han publicado y han ido entrando en vigor en momentos diferentes. Pero la Ley de Seguridad Nacional, en conjunción con la directiva NIS (que deberá transponerse a nuestra legislación a más tardar en 2018) y una posible revisión de la Estrategia Nacional de Ciberseguridad, abren la posibilidad de ajustar nuestra actual estructura. Los trabajos de preparación de un documento de consenso entre todos los actores involucrados para transponer la directiva NIS están liderados por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

Participantes:

Ángel León Alcalde es Vocal Asesor en la Subdirección General de Servicios de Sociedad de la Información de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital del Ministerio de Energía, Turismo y Agenda Digital. Ingeniero de Telecomunicación por la UPM (1990), tras un breve paso por Telefónica I+D se incorpora a la Dirección General de Telecomunicaciones como funcionario del Cuerpo de Ingenieros Superiores de Radiodifusión y Televisión (1992). Desde entonces desarrolla su carrera profesional en diferentes áreas de la Administración. En 2006 comienza a participar en actividades legislativas en el ámbito de la Unión Europea, con motivo del primer Reglamento comunitario sobre roaming internacional, y con posterioridad participa en la negociación de la revisión del marco regulador de las telecomunicaciones de 2009, en el Reglamento de 2015 sobre Roaming e Internet Abierta, y finalmente en la elaboración de la Directiva NIS. León Alcalde forma parte del grupo de trabajo encargado de la transposición de la Directiva, en el que también participan el DSN, el Ministerio del Interior y el CCN.

Luis Jiménez es Subdirector del Centro Criptológico Nacional, Especialista criptólogo y Máster en Dirección de Sistemas y TIC por el Instituto Nacional de Administración Pública y la Universidad Politécnica de Madrid, dispone de diversas certificaciones de especialización en seguridad de las TIC y es representante nacional en los Comités de seguridad de la información y ciberseguridad del Consejo de la Unión Europea y de la OTAN. Entre los principales cometidos de su actual puesto de trabajo se encuentran el impulso y desarrollo del Esquema Nacional de Seguridad, el impulso y desarrollo de la Capacidad de Respuesta ante Incidentes de Seguridad, la mejora de las capacidades de Evaluación y Certificación de la Seguridad de las TIC, y la elaboración de políticas, directrices y guías de seguridad TIC para la administración pública.

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.

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. Cuenta con más de 26 años de experiencia en el campo de la seguridad. Previamente a su cargo actual desarrolló durante varios años sus funciones en el Estado Mayor de la D.G. 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. 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. 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.

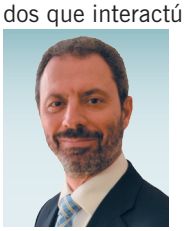
Carlos Gómez López de Medina es Comandante Jefe del Mando Conjunto de Ciberdefensa. Perteneciente a la 33ª Promoción de la Academia General del Aire, Gómez es desde el 3 de julio de 2013 comisionado al Estado Mayor de la Defensa y designado Comandante Jefe del Mando Conjunto de Ciberdefensa. En mayo de 2009 es designado Jefe del Grupo Central de Mando y Control (GRUCEMAC) en la Base Aérea de Torrejón, jefatura que desempeña desde julio de 2009 hasta julio de 2011. En dicho año asciende a General de Brigada y se le destina al Mando del Apoyo Logístico del E.A., donde ocupa el puesto de Subdirector de Gestión de Programas en la Dirección de Sistemas de Armas. Diplomado de Estado Mayor del Aire, ha realizado los cursos de Mandos de Unidades Paracaidistas y Transmisiones y Guerra Electrónica del E.A., así como otros cursos de especialización en telecomunicaciones, logística y relaciones internacionales.

Seguridad tecnológicas, soluciones basadas en servicios SaaS, y continuidad de negocio... Ha desarrollado su actividad profesional en los ámbitos públicos y privados, tanto en Europa como en América. Posee las certificaciones: Certificate on Cybercrime and Electronic Evidence. Comisión Europea del programa JPEN, System/Cryptographic Security Engineer, NCipher, y SEI Certificate in Incident Response Process.

Daniel López Rojo es Security Sales Executive para España y Portugal en HP Enterprise Services, siendo integrante del área de ventas de seguridad de la compañía desde el año 2011.Ingeniero Superior en Organización Industrial por la Universidad de Valladolid e Ingeniero Técnico en Diseño industrial por la Universidad Politécnica de Valencia, López Rojo además ha realizado el Máster Universitario en Seguridad de Tecnologías de la Información y de las Comunicaciones, Seguridad TIC por la Universidad Europea de Madrid. Posee también el ITIL Foundation Certificate in IT Service Management (ITILF).

Grupo Inversis Banco: Protección inteligente en tiempo real ante amenazas a sistemas web transaccionales

Sinopsis: El servicio Delphos Aiuken proporciona información de fraude en tiempo real para sistemas bancarios y venta online, sin necesidad de instalar ningún servidor y combinando la ciberinteligencia de los Centros de Inteligencia de los SOCs de Aiuken para proporcionar la información de fraude en tiempo real. El cliente, en este caso Grupo Inversis Banco, dispone de información en tiempo real de nivel de infectación y seguridad de los clientes y empleados que interactúan con sus aplicaciones y servicios de internet.



Ponentes:

Manuel Fernández es Director de Seguridad de la Información y Entorno Corporativo de Grupo Inversis Banco, entidad en la que lleva trabajando desde hace dieciséis años, y en la que en su actual posición se responsabiliza de las funciones de Seguridad de la Información, Seguridad y Continuidad de Negocio, ocupando con anterioridad la dirección del área de Infraestructuras y Explotación de la entidad. Fernández, Ingeniero de Telecomunicaciones, CISM y posee la certificación ITIL, fue en otras etapas profesionales, Responsable de Comunicaciones y Servicios de Información en Merrill Lynch para España y Portugal durante cuatro años y responsable de Comunicaciones y Redes en FG Valores y Bolsa durante un año.

Juan Miguel Velasco López-Urda es actualmente CEO y Fundador de Aiuken Solutions, multinacional española especializada en Ciberseguridad 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, TI 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 Data Centers, en Telefónica Data España, y antes como Subdirector de Ingeniería de Proyectos y Servicios de Protección de la Información de la UN Hosting y ASP de Telefónica 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 Telefónica DataCorp en Europa y LATAM. Cursó sus estudios de Informática Superior en la UPM y, entre otros, es Máster Executive de Gestión Empresarial por INSEAD-EUROFORUM, miembro de la Cátedra de Riesgos del Instituto de Empresa y profesor del Máster en Dirección y Gestión de Seguridad de la Información de la Escuela Superior de Ingenieros de Telecomunicaciones de la Universidad Politécnica de Madrid. Es Miembro del Consejo Asesor del iSMS Forum Spain, y Presidente de la Comisión de Confianza y Seguridad de Eurocloud Spain.

SEGUNDO MÓDULO, 26 DE ABRIL

09:00h.	Entrega de documentación
09:30h.	Ponencia: **Gestión de la Seguridad de la Información en los Servicios de Salud de las Islas Baleares** Ponentes: **Miguel Ángel Benito Tovar**, Responsable del área de Seguridad del Servicio de Salud de las Islas Baleares. **Manuel Giralt Herrero**, Socio del área de Risk en España. Advisory Services. EY.
10:00h.	Coloquio
10:05h.	Ponencia: **La MISP (Malware Information Sharing Platform) en el sector Banca** Ponentes: **James Gill**, Global CSIRT Manager. Banco Sabadell. **Xavier Gracia Lacalle**, Socio de Deloitte. Cyber Risk Services.
10:35h.	Coloquio
10:40h.	**Pausa-café**
11:15h.	Ponencia: **ABANCA: prevención holística del Fraude** Ponentes: **Fátima Cereijo Conde**, Gerente de la Oficina de Prevención de Fraude y Pérdidas de Abanca. **Jorge Domingo Samayoa**, Fundador y CEO de Plus Technologies.
11:45h.	Coloquio
11:50h.	Ponencia: **Grupo BBVA: Behavior analytics en la lucha contra el fraude** Ponentes: **Sergio Iglesias Pérez**, Responsable de Cybersecurity Analytics de Grupo BBVA. **Pablo González Lafuente**, Responsable del Equipo de Data Scientist de GMV.
12:20h.	Coloquio
12:25h.	Ponencia: **Grupo Iberdrola: Modelo de gobierno de la ciberseguridad e implantación de un programa de Ciberseguros global** Ponentes: **Rosa Kariger**, CISO de Grupo Iberdrola. **Cristina San Sebastián**, Gerente de Riesgos y Seguros. Grupo Iberdrola. **Carmen Segovia**, Responsable Nacional de Ciberriesgos. Aon Risk Solutions.
12:55h.	Coloquio
13:00h.	Ponencia: **Aquae Security: Un paso por delante de los ciberataques dirigidos** Ponentes: **Eduardo di Monte**, Director de Seguridad y Continuidad de Negocio de Aquae Security para España y Chile. **Daniel Solís**, CEO y fundador de Blueliv.
13:30h.	**Almuerzo**
15:30h.	Ponencia: **Protección de los Sistemas de Control de EDP** Ponentes: **Arturo Eloy Díaz Rodríguez**, Responsable de Seguridad Lógica de EDP. **Óscar Navarro**, Director de Ciberseguridad Industrial de S2 Grupo.
16:00h.	Coloquio
16:05h.	Ponencia: **Ciberseguridad en sistemas de control: nuevas propuestas tecnológicas** Ponente: **Alberto Hernández Moreno**, Director General de INCIBE.
16:35h.	Coloquio
16:40h.	Fin del segundo módulo
19:30h.	**Cena de la Ciberseguridad y entrega de los XIV Premios SIC**

Gestión de la Seguridad de la Información en los Servicios de Salud de las Islas Baleares

Sinopsis: El principal objetivo de este proyecto es proporcionar a los Servicios de Salud de las Islas Baleares un servicio de seguridad de la información gestionado que garantice un nivel de seguridad adecuado para cubrir las necesidades de la Organización y cumplir con las exigencias normativas y regulatorias de protección de la información. Entre los servicios ofrecidos se incluye formación y concienciación continuada en seguridad de la información, desarrollo y mantenimiento de la Política de Seguridad y Marco Normativo, realización de auditorías de seguridad, asesoramiento en seguridad en todos los proyectos TIC, monitorización de la seguridad, gestión de vulnerabilidades, protección ante incidentes o eventos indeseados y soporte continuado en la adecuación de sus diferentes entornos tecnológicos a un nivel de seguridad adecuado. Todo ello cubriendo los tres pilares fundamentales: procesos, tecnologías y personas.

Ponentes:

Miguel Ángel Benito Tovar es Responsable del área de Seguridad del Servicio de Salud de las Islas Baleares. Durante los últimos diez años ha desarrollado su carrera profesional en el ámbito de la seguridad de la información y el cumplimiento normativo, gestionando todo tipo de proyectos tanto de índole técnico como consultivo y normativo. Actualmente forma parte de la Red de Responsables de Seguridad de la Información de Organismos y Centros Sanitarios a nivel estatal y ha sido ponente en diferentes congresos dentro del sector. Miguel Ángel cuenta con amplios conocimientos legales y normativos especialmente en materia de protección de datos, Esquema Nacional de Seguridad, Esquema Nacional de Interoperabilidad, firma electrónica, contratación pública y administración electrónica. Es titulado en Ingeniería Técnica en Informática de Gestión por la Universidad Pontificia de Salamanca y graduado en Ingeniería Informática por la Universidad Europea de Madrid. Además, posee un Máster en Auditoría y Seguridad Informática por la Universidad Politécnica de Madrid y un Máster Universitario en Administración Sanitaria por la UNED. También dispone de las certificaciones CISM y CISA por ISACA y SGSI por AENOR.

Manuel Giralt Herrero es Socio del área de Risk en España en Advisory Services de EY. Cuenta con más de 19 años de experiencia en Gestión del Riesgo, Control Interno, SAP GRC (AC, PC, RM and AMS) –marco en el que lidera el desarrollo y la definición de metodologías para la implantación de estas herramientas en el mercado español e internacional, principalmente Europa, Middle East, India y Japón–, Ciberseguridad y Cumplimiento. Ha dirigido proyectos de Planes de Continuidad de Negocio, Directores de seguridad, auditoría de seguridad informática, gestión de seguridad y auditoría y asesoramiento sobre protección de datos. Es Licenciado en Económicas y Administración de Empresas por las universidades de Zaragoza y Estocolmo (Suecia), MBA en ESADE Business School (Barcelona), Global e-Management Master de ESADE Business School y dispone de la certificación CISA de ISACA. Giralt es miembro de la Asociación Española de Consultoría (AEC), del Information Systems Audit and Control Association (ISACA), EuroPriSe Member Committee in Europe, IAPP European Member (International Association of Privacy Professionals), SACHO KAI Spanish Chapter y Member of EY Spain representing Japanese subsidiaries in Spain. Es profesor de cursos y másteres relacionados con estas disciplinas.

La MISP (Malware Information Sharing Platform) en el sector Banca

Sinopsis: La Red MISP de Deloitte –Malware Information Sharing Platform– es una comunidad de clientes de Banca de Deloitte, feeds de inteligencia público, CERTS y base de datos de conocimiento gestionada en una plataforma Web. MISP es una plataforma interactiva que envía una notificación al Banco Sabadell cada vez que algo nuevo se comparte, proporciona automatización para una fácil integración con herramientas de defensa cibernética. Los expertos en malware del Banco Sabadell encuentran en la red MISP de Deloitte muestras de malware reales y confirmadas de manera online, asi como una amplia variedad de información técnica sobre malware, lo que ayuda a obtener protección semi-instantánea para el Banco. La clave de su éxito es compartir entre la comunidad MISP la parte técnica de la información de malware y no compartir la información sobre el contexto del ataque. Hoy en día, la red MISP de Deloitte ya ha conectado a las principales empresas del sector bancario español (entre las que destaca el Banco Sabadell). Igualmente, Deloitte tiene un plan estratégico para desplegar su red a través de las empresas más importantes del Sector Bancario europeo.

Ponentes:

James Gill es el Director del equipo de Advanced Cyber Defence del Banco Sabadell. En este rol, es el responsable de los equipos de Gestión de Incidentes y Ciberinteligencia. Tiene más de quince años de experiencia en seguridad, en diversidad de posiciones, en su mayoría en una de las entidades financieras más importantes del mundo, ocupando puestos de responsabilidad a nivel regional y global. Tiene un posgrado en Auditoría Técnica y Análisis forense, además de diversas certificaciones de Seguridad.

Xavier Gracia Lacalle es Socio de Cyber Risk Services 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 y ciberseguridad de Deloitte. Las industrias en las que está especializado son: FSI (Banca), Energía 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 TIC, en la Business Engineering School, de La Salle (URL).

ABANCA: Prevención holística del fraude

Sinopsis: Hoy en día la prevención integral del fraude es clave en una banca centrada en el cliente, esto presupone que las instituciones financieras cuenten con controles preventivos tanto en las operaciones financieras como las operaciones administrativas en tiempo real. Esta ponencia dará a conocer los desafíos y logros del caso de uso de ABANCA en la prevención integral del fraude, y cómo dicha estrategia se ha convertido en un valor agregado tanto para la gestión de riesgo interno como la experiencia con los clientes. Además compartiremos cuáles son los elementos clave en el manejo de una estrategia integral en la prevención de fraude así como los beneficios en el corto y largo plazo.

Ponentes:

Fátima Cereijo Conde es Gerente en la Oficina de Prevención de Pérdidas y Fraude de Abanca. Ingeniera Superior Industrial, en la especialidad de Organización Industrial, experta universitaria en Gestión y Planificación Empresarial, Postgrado en Auditoría de Calidad, Certificada PMP, y especialista en Delitos Financieros, tiene 10 años de experiencia en el sector financiero, donde ha desempeñado distintos roles y responsabilidades, desde las áreas de Organización, Eficiencia y Procesos a la gestión BPO de los proveedores de servicios externalizados, donde recibió el premio a la Eficiencia y Eficacia operativa en 2010 por Call Center. Fue seleccionada para participar en el Programa Executiva de la Xunta de Galicia en 2012 y para el Programa Executive impartido por AIESIDE en ese mismo año. Desde hace 1 año y medio, es la responsable de la oficina de Gestión de Pérdidas y Fraude, representando a Abanca en la Comisión de AAECF y en distintos foros especialistas del sector.

Jorge Domingo Samayoa es Fundador y CEO de Plus Technologies. Considerado uno de los pioneros en Latinoamérica en el desarrollo de sistemas de monitorización y prevención en tiempo real, con más de 30 años de experiencia en la industria de tecnología de información ha llevado a Plus TI y Monitor Plus, su marca líder, a tener uno de los mayores reconocimientos en la industria financiera latinoamericana en prevención de fraude

bancario y prevención de lavado de activos, con presencia en los cinco continentes y más de 300 instituciones financieras. Jorge es Ingeniero civil, cuenta con un MBA y es conferencista internacional.

Aquae Security: Un paso por delante de los ciberataques dirigidos

Sinopsis: Los atacantes cada vez son más eficientes y las empresas son más atacadas. Para ello, los ciberdelincuentes con claros objetivos dirigidos o *targeted*, en contra de las compañías, preparan ataques con mucha información obtenida de fuentes públicas y combinando ingeniería social. Por ello, los atacantes estudian la superficie de ataque o de amenazas a fin de buscar el eslabón más débil y estudian a la víctima y los activos tecnológicos potencialmente vulnerables. Con dicha premisa en mente, Aquae Security ha decidido contar con Blueliv para simular ciberataques en las diferentes cadenas de ataque o "killchain", contra sus activos tecnológicos y empleados. De la misma forma que actuaría un ciberdelincuente con una clara intención dirigida, Aquae Security verifica la robustez de sus medidas de seguridad, así como el nivel de concienciación y de reacción de los usuarios y equipos implicados.

Ponentes:
Eduardo di Monte es Director de Seguridad y Continuidad de Negocio de Aquae Security para España y Chile. Ingeniero en Telecomunicaciones y MBA del EuroMBA, cuenta con trece 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.

Daniel Solís es CEO de Blueliv. Ingeniero en Telecomunicaciones y socio fundador de la compañía, ha trabajado en las Naciones Unidas en Nueva York, y ha desarrollado parte de su carrera profesional como Director en KPMG gestionando la línea de servicios de Information Protection and Business Resilience. Con más de diecisiete años de experiencia, ha participado en diferentes proyectos de seguridad desarrollando estrategias corporativas en materia de protección de la información, como planes directores, expansiones internacionales de planes directores y estratégicos de seguridad, SGSIs, etc. Asimismo, Solís ha creado, formado y colaborado en equipos de consultores en seguridad de la información y de *hacking* ético en varias empresas del sector, como por ejemplo S21sec, de la cual fue miembro del equipo inicial. Es ISO 27001 Lead Auditor acreditado por IRCA, miembro activo de AEDEL y creador de la distribución forense Ad-quiere.

Grupo BBVA: Behavior analytics en la lucha contra el fraude

Sinopsis: La existencia de caballos de Troya de nueva generación hace que las técnicas utilizadas hasta la fecha sean poco efectivas, pues no son capaces de adaptarse y generalizar ante nuevos casos. Por este motivo, es frecuente que fallen ante cambios en el patrón del troyano o con la aparición de nuevas amenazas. Para solucionar esto, es necesario crear huellas digitales avanzadas "behaviour analytics", para la detección de estos nuevos patrones dentro de la operativa bancaria. Esta nueva huella se basa en algoritmos de modelado de las sesiones de los clientes y la búsqueda de similitudes con las huellas dejadas por el troyano en anteriores sesiones fraudulentas a través de sistemas de Machine Learning supervisado. Uno de los principales retos es el trabajo con conjuntos de datos extremadamente no balanceados, con decenas de miles de casos negativos por cada positivo. BBVA y GMV han colaborado mano a mano para buscar la solución tecnológica que ponga freno a los nuevos troyanos. BBVA ha aportado los conjuntos de datos etiquetados y GMV la parte tecnológica.

Ponentes:
Sergio Iglesias Pérez es Responsable de Cybersecurity Analytics del grupo BBVA. Cuenta con más de 15 años de experiencia en el sector. Ingeniero superior de Telecomunicaciones por la Universidad del País Vasco, desde sus inicios ha estado involucrado en el mundo de la seguridad informática, formando parte de empresas como DaVinci Consulting Tecnológico, Gedas e Indra. En la actualidad su trabajo se centra principalmente en la detección de amenazas complejas utilizando tecnologías de Machine Learning y Big Data.

Pablo González Lafuente es Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid y Máster Big Data and Bussines Analytics por la Universidad de Alcalá de Henares de Madrid. González Lafuente es un apasionado de la tecnología que lleva dedicándose al mundo del software más de 10 años. Actualmente lidera el equipo de Data Scientist en GMV, centrado en la investigación y trabajando en tecnologías Big Data y algoritmos de Machine Learning.

Grupo Iberdrola: Modelo de gobierno de la ciberseguridad e implantación de un programa de Ciberseguros global

Sinopsis: El Consejo de Administración de Iberdrola establece, a través de la Política de Riesgos de Ciberseguridad, un marco global para el control y gestión de los riesgos de ciberseguridad aplicable a todas las sociedades del Grupo. Por medio del Comité de Ciberseguridad, en el que están representados todos los negocios y funciones corporativas, se despliega un modelo de gestión integral para todo el Grupo, basado en el análisis y gestión de los riesgos y en la aplicación de medidas técnicas y organizativas para una adecuada protección y resiliencia de los activos en función de su criticidad. Desde Gerencia de Riesgos y Seguros, dentro de este modelo de gestión integral, se aporta la mitigación del riesgo vía transferencia al mercado asegurador a través de un Programa Internacional que recoge las necesidades específicas de Iberdrola en materia de protección de Ciberriesgos.

Ponentes:
Rosa Kariger es responsable de la Dirección de Ciberseguridad del Grupo Iberdrola, desde la que se gobiernan y supervisan, a nivel global, las iniciativas para asegurar que la ciberinfraestructura del Grupo está adecuadamente protegida, así como el cumplimiento de la normativa vigente en materia de ciberseguridad y privacidad en todo los países en los que el opera Iberdrola. Ingeniero Industrial por la Universidad Politécnica de Madrid, ha participado en el Programa Escuela de Dirección del IESE y en el Global Leadership Program de IMD y acumula más de 20 años de experiencia en el sector eléctrico.

Cristina San Sebastián es responsable de la dirección de Gerencia de Riesgos y Seguros en Iberdrola, departamento que colabora con las distintas áreas de negocio del Grupo en la identificación, análisis y gestión del riesgo operacional, centralizando el diseño, implementación y gestión de los programas de seguros más adecuados al perfil de riesgo del Grupo Iberdrola en cada momento. Licenciada en Derecho por la Universidad de Deusto, se incorporó a Iberdrola en 1993, dentro del área de Servicios Jurídicos, pasando en 1994 a formar parte de la dirección de Gerencia de Riesgos y Seguros, la cual dirige desde 2005. Cristina es vicepresidente de IGREA (Iniciativa de Gerentes de Riesgo Españoles Asociados), asociación de la que Iberdrola es miembro fundador, entre otras compañías del IBEX.

Carmen Segovia, Directora y Responsable Nacional de Ciber Riesgos en AON España, con más de 10 años de experiencia analizando y asegurando los riesgos vinculados a Líneas Financieras y Profesionales, así como desarrollando nuevas coberturas y estrategias dirigidas a asegurar los Riesgos Cibernéticos. Ha participado en la colocación, negociación y desarrollo, tanto en mercado nacional como internacional, del Seguro de Ciber Riesgos de algunas de las principales corporaciones españolas de Infraestructura Crítica, Sector Bancario, Industrial y Retail.

Protección de los Sistemas de Control de EDP

Sinopsis: Las Infraestructuras Críticas son objeto de ciberataques cada vez más sofisticados. Existe una inmadurez general de soluciones capaces de proteger aspectos puntuales de ciberseguridad de los sistemas de control industrial, y aún más crítico, del proceso de monitorización y supervisión de ciberseguridad sobre los sistemas de control industrial. El objetivo de la presentación es mostrar cómo la solución es capaz de trabajar con protocolos industriales analizando también el *payload* de los paquetes para identificar el fin de un determinado comando a nivel de la red industrial. El sistema posee un diseño mínimamente invasivo y no posee capacidad de bloquear acciones de los operadores del entorno industrial a proteger o interferir en el tráfico en las redes. Su concepción es la de un sistema de alertas y su ejecución garantiza que, en ningún caso, se va a introducir tráfico proveniente del exterior en la red de control. La base del sistema está en la identificación de aquellas situaciones que pueden suponer un riesgo para la infraestructura de control y en su rápida detección, partiendo del conocimiento preciso de la forma en que se explotan este tipo de sistemas.

Ponentes:

Arturo Eloy Díaz Rodríguez es Responsable de Seguridad Lógica en EDP. Ingeniero Técnico de Sistemas, ha sido responsable de las Infraestructuras de EDP Energía en España hasta el año 2015 en el que pasó a desarrollar sus labores profesionales como responsable de Seguridad Lógica. Cuenta con amplia experiencia tanto en las tecnologías de TI como de OT. Díaz ha sido igualmente responsable de proyectos de migración de sistemas corporativos multigeografía a entornos virtuales.

Óscar Navarro es Director de Ciberseguridad Industrial de S2 Grupo. Ingeniero Industrial, durante gran parte de su carrera ha trabajado en el sector eléctrico y en diversas empresas en el ámbito de la ingeniería y construcción de infraestructuras públicas, tanto en redacción de proyectos como en ejecución de obras. Actualmente es el Director de Ciberseguridad Industrial de S2 Grupo, teniendo una amplia experiencia en evaluación de ciberseguridad de sistemas SCADA y en diseño, despliegue y operación de sistemas de monitorización en infraestructuras industriales. Es ponente habitual en cursos y conferencias en la materia y en sesiones de concienciación específicas para colectivos relacionados con el diseño, mantenimiento y operación de sistemas de control.

Ciberseguridad en sistemas de control: nuevas propuestas tecnológicas

Sinopsis: Todos conocemos la gran importancia de la Ciberseguridad de nuestros entornos TI, pero no ocurre lo mismo cuando hablamos de los entornos OT. Estos entornos se basan, como todos sabemos, en Sistemas de Control que son en definitiva los pilares que sustentan los servicios esenciales de los que todos disfrutamos: luz, agua, transporte y comunicaciones, etc. Son ya conocidos numerosos incidentes que han afectado a los entornos OT y cuyas consecuencias han afectado incluso al activo más valioso de todos: las personas. Es necesario por tanto abordar la Ciberseguridad en OT con nuevas estrategias y tecnologías y en coordinación con todos los actores clave: los fabricantes, los laboratorios industriales y la propia industria entre otros. Tecnologías innovadoras asociadas a la detección de sistemas de control expuestos en Internet, detección activa de vulnerabilidades en entornos controlados y detección pasiva de malware en la red de control, son ejemplos de iniciativas tecnológicas puestas en marcha desde INCIBE en colaboración con el resto de agentes del sector.

Ponente:

Alberto Hernández Moreno es Director General de INCIBE. Ingeniero Superior de Telecomunicaciones por la Escuela Técnica Superior de Ingenieros de Telecomunicaciones de la Universidad Politécnica de Madrid y Director de Seguridad por el Ministerio del Interior, ha sido Director de Operaciones de INCIBE desde el año 2014 hasta su nombramiento como DG en octubre 2016. En dicho periodo ha sido responsable de la puesta en marcha de los servicios, tecnologías y actividades de apoyo a la industria, la I+D+i y el talento lanzados desde INCIBE y ha venido participando, como experto internacional, en misiones de la Organización de Estados Americanos (OEA) para el desarrollo de las estrategias nacionales de ciberseguridad en varios países Latinoamericanos. Previa incorporación a INCIBE, y como Jefe de Área de Ciberdefensa de ISDEFE, formó parte del equipo responsable del diseño y puesta en marcha del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

TERCER MÓDULO, 27 DE ABRIL

09:15h. Entrega de documentación

09:30h. Ponencia: **Applus+: Definición de un marco de evaluación de la seguridad para elementos interconectados**

Ponentes:

Juan Francisco Ruiz Gualda, Responsable del Servicio de Common Criteria de Applus.

Juan Carlos Pascual, Consultor Senior de Capgemini.

10:00h. Coloquio

10:05h. Ponencia: **IRP: Orquestación y automatización de la respuesta a incidentes en Telefónica Business Solutions**

Ponentes:

Leonardo Amor, Head of Security. Telefónica Business Solutions.

Juan Carlos de Miguel, Associate Partner. IBM Security.

10:35h. Coloquio

10:40h. **Pausa-café**

11:15h. Ponencia: **Asegurando el negocio frente a las ciberamenazas y protegiendo a la alta dirección**

Ponentes:

Silvia Villanueva, CISO Transversal para la Región de EMEA-LATAM de AXA.

Javier Urtiaga, Socio responsable de Ciberseguridad de PwC España.

11:45h. Coloquio

11:50h. Ponencia: **Despliegue internacional de la estrategia de ciberseguridad de AXA Global Direct**

Ponentes:

Gorka Díaz Orbe, CISO Internacional de AXA Global Direct.

Sergio Gómez Rodríguez, Manager de Ciberseguridad en IT Advisory de KPMG.

12:20h. Coloquio

12:25h. Ponencia: **Proyecto Norbide 2017: evolución de la gestión de identidades en el Servicio Vasco de Salud-Osakidetza**

Ponentes:

Pedro Totorikaguena Arana, Jefe de Servicio de la Subdirección de Informática y Sistemas de Información de Osakidetza-Servicio Vasco de Salud.

Álvaro Fernández Peña, Consultor Senior de gestión de Identidades y Accesos del departamento de Ingeniería de Nextel, S.A.

12:55h. Coloquio

13:00h. Ponencia: **Ministerio de Justicia. El contexto, la clave para un acceso seguro a la red**

Ponentes:

César Hernando Ceña, Jefe de Sección Comunicaciones. Subdirección General de Nuevas Tecnologías de la Justicia. Secretaría General de la Administración de Justicia. Ministerio de Justicia.

Carlos Gómez Gallego, Security and Innovation Office de Aruba CTO.

13:30h. Coloquio

13:35h. **Almuerzo, fin del tercer módulo y fin de Securmática 2017**

Applus+: Definición de un marco de Evaluación de Seguridad para elementos interconectados

Sinopsis: A pesar del consenso entre los distintos analistas que apuntan a una explosión en el número de dispositivos interconectados (IoT), y que parece que nos llevará a cifras de 50.000 millones de dispositivos en el año 2020, los últimos ataques sobre estas tecnologías hacen pensar que estamos lejos de una situación ideal. En la ponencia se describirá tanto la necesidad de una evaluación de este tipo, como el esquema de evaluación de Seguridad que Capgemini ha definido para Applus+, uno de los líderes mundiales en ensayos y certificación, y que complementa su esquema de evaluación de Seguridad. Se hablará también de cómo es posible aplicar este esquema de evaluación en una amplia gama de productos y sectores, validando la seguridad de un producto interconectado.

Ponentes:

José Francisco Ruiz Gualda es Responsable del Servicio Common Criteria en Applus. Ingeniero informático por la universidad de Granada, tiene más de 10 años de experiencia en el sector de la seguridad TIC, principalmente en la evaluación de productos IT en metodologías reconocidas internacionalmente como Common Criteria, Global Platform y FIPS 140-2. Actualmente dirige el servicio de Common Criteria y lidera las iniciativas de ciberseguridad en el laboratorio Applus+. Es "chairman" de uno de los sub-grupos de trabajo dentro del grupo ISCI-WG1 de Eurosmart para el desarrollo de la metodología Common Criteria en la evaluación de tarjetas inteligentes y también es miembro activo del grupo temático ERNCIP "IACS Cybersecurity certification". Ha dado charlas en diversos congresos internacionales (ICCC – Conferencia Internacional de Common Criteria o ICMC – Conferencia Internacional de módulos criptográficos) como experto en certificaciones de seguridad.

Juan Carlos Pascual es Consultor Senior en Capgemini y en la actualidad lidera la iniciativa Application Centric Security de Capgemini. Titulado en Informática, CISA y PIC (Deusto Business School), cuenta con más de 20 años de experiencia en Seguridad informática, y experiencia en empresas como IpsCA o Sogeti en puestos de gerencia y técnicos relacionados con la gestión de seguridad y vulnerabilidades, incluyendo la gestión y coordinación de equipos de hacking ético y análisis de vulnerabilidades en aplicaciones. En su desempeño actual trabaja en proyectos nacionales e internacionales relacionados con la incorporación de la seguridad en el diseño y la verificación y validación de la seguridad.

IRP: Orquestación y automatización de la respuesta a incidentes en Telefónica Business Solutions

Sinopsis: Telefónica Business Solutions (TBS) es la empresa del Grupo Telefónica que ofrece de forma global los negocios de multinacionales, mayorista e itinerancia en más de 170 países, así como servicios IT y convergentes a empresas multinacionales fuera del *footprint*, apoyándose para ello en su extensa red internacional y en acuerdos locales con terceros operadores e integradores. En la ponencia se presentará la estrategia interna que se plantea TBS para la gestión de la respuesta a incidentes de seguridad desde una doble perspectiva: en primer lugar, estableciendo una taxonomía y clasificación de los incidentes mediante un lenguaje flexible y común a toda la organización a nivel mundial, que no esté sujeto a la subjetividad, y que posteriormente sirva como base para estandarizar el proceso de gestión de incidentes de forma horizontal entre todas las áreas implicadas. Esto además permitirá conocer la situación de cómo está la organización y tener unos KPI's respecto al proceso global. En segundo lugar, utilizando una plataforma tecnológica IRP para la orquestación y automatización de la respuesta sobre la que implementar el modelo definido, y que además proporcione flujos ad-hoc según el tipo de incidente, integre inteligencia sobre ciberamenazas de fuentes externas, mejore la eficiencia e industrialización del proceso de gestión y respuesta mediante la integración con las infraestructuras de TBS y la recopilación semiautomática y almacenamiento de información y evidencias, y guíe el proceso de reporte de brechas de seguridad teniendo en cuenta la legislación local de cada país.

Ponentes:

Leonardo Amor es Head of Security en Telefónica Business Solutions (TBS). Licenciado en Derecho por la universidad Francisco de Vitoria, CISA y CISM por Isaca, es asimismo el representante del Grupo Telefónica en las asociaciones internacionales FIRST, TERENA y APWG, además de colaborador habitual de eventos y medios especializados. Su carrera profesional ha estado vinculada a Telefónica en la que comenzó hace más de 15 años, y donde ha asumido diversas responsabilidades en materia de ciberseguridad para varias empresas del Grupo, tanto como responsable de seguridad TIC a nivel interno, como realizando funciones más comerciales y de desarrollo de negocio relacionadas con la construcción, comercialización y explotación del portafolio de servicios de ciberseguridad hacia terceros.

Juan Carlos de Miguel es Associate Partner en IBM Security, compañía a la que se incorporó a principios de 2016. Ingeniero Superior de Telecomunicación por la UPM, MBA por el IE, CISA y CISM por ISACA, ha desempeñado con anterioridad funciones de responsabilidad en PwC y en Indra en las áreas de desarrollo de negocio, soporte a operaciones y coordinación de proyectos complejos. Es asimismo ponente y colaborador habitual en revistas y medios especializados en la materia, y miembro del capítulo de Madrid de ISACA. A lo largo de su trayectoria ha participado en varias iniciativas de seguridad de relevancia del mercado español, en los ámbitos del diseño y transformación de centros de Seguridad y SOCs/CSIRTs, consultoría estratégica y gobierno en materia de ciberseguridad, externalización, evolución y optimización de servicios y oficinas de seguridad, planes estratégicos, gestión del riesgo y cumplimiento, auditorías técnicas (third-party assurance), seguridad perimetral y gestión de vulnerabilidades y ciberamenazas, etc.

Asegurando el negocio frente a las ciberamenazas y protegiendo a la alta dirección

Sinopsis: El programa de cibertransformación permite dar respuesta a toda la responsabilidad que pueda tener la alta dirección en materia de ciberseguridad. Un programa razonablemente ambicioso, bien estructurado y medible permitirá a la organización culminar con éxito este proceso tan relevante para todos, teniendo en cuenta los distintos enfoques y puntos clave. Durante la ponencia se tratarán los retos existentes y las soluciones que permiten desarrollar este programa de forma satisfactoria en un entorno internacional, incluyendo tanto enfoques estratégicos como tácticos y operativos.

Ponentes:

Silvia Villanueva es CISO Transversal para la Región de EMEA-LATAM en AXA desde hace más de 3 años. Previamente a su incorporación trabajó más de 15 años en algunas de las principales empresas internacionales de auditoría y consultoría, siempre dentro del área de la seguridad. Durante este tiempo dirigió y ejecutó proyectos de ámbito nacional e internacional para numerosas empresas 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.

Javier Urtiaga es Socio responsable de Ciberseguridad en PwC España. Ingeniero de Telecomunicaciones por la Universidad Politécnica de Cataluña y Executive MBA por el Instituto de Empresa, cuenta con más de 20 años de experiencia en ciberseguridad en diversos sectores y ha centrado su carrera profesional en el desarrollo de este ámbito ayudando a las principales compañías del país a afrontar sus retos y a protegerse de las ciberamenazas.

Dirige y coordina proyectos que incluyen la estrategia en ciberseguridad, el modelado de amenazas, las arquitecturas de seguridad, Ciberinteligencia, planes de transformación digital, Servicios de RedTeam.

Despliegue internacional de la estrategia de ciberseguridad en AXA Global Direct

Sinopsis: Tras la realización de análisis en cada una de sus entidades locales, la alta dirección de AXA Global Direct toma la decisión de impulsar iniciativas globales de seguridad que permitan elevar su nivel de madurez, con un enfoque eficiente de gestión de riesgos y consumo de su presupuesto. El contexto cultural y el modelo operativo de cada entidad serán factores determinantes para el éxito de la implantación del Plan Estratégico.

Ponentes:
Gorka Díaz Orbe es CISO Internacional de AXA Global Direct. Experto en la gestión internacional de estrategias de seguridad en el sector financiero. Orientado en el establecimiento de capacidades de seguridad sostenibles e integradas en el negocio en entornos tecnológicos complejos y heterogéneos; ejerciendo liderazgo global para impulsar la seguridad de la información y el cambio cultural organizativo.

Sergio Gómez Rodríguez es Manager de Ciberseguridad en IT Advisory de KPMG. Experto en consultoría de Riesgos Tecnológicos y Seguridad de la Información a nivel nacional e internacional. Gestión y ejecución de 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, gestión y análisis de riesgos, definición de funciones y estructuras organizativas, certificación de sistemas de gestión, auditorías TI, control interno, SOX y planes de continuidad de negocio. Cuenta con las certificaciones profesionales CISA, CISM, ISO 27001 e ISO 22301.

Proyecto Norbide 2017: evolución de la gestión de identidades en el Servicio Vasco de Salud-Osakidetza

Sinopsis: El proyecto de Gestión de Identidad (Norbide) del Servicio Vasco de Salud, (Osakidetza), vive en continua evolución, ya que al ser transversal a toda la organización debe evolucionar en paralelo al resto de cambios organizativos y tecnológicos. El producto (Oracle Identity Manager) en el que se sustenta el servicio también ha evolucionado habiendo migrado recientemente a la última versión.
Respecto a las necesidades funcionales, se aportan constantes mejoras operativas, entre las que destacan: la inclusión en el sistema de todo el personal externo, la publicación del servicio en Internet, la autenticación y autorización centralizada de aplicaciones a través del Oracle Access Manager, y el diseño de un catálogo corporativo de roles.

Ponentes:
Pedro Totorikaguena Arana es Jefe de Servicio de la Subdirección de Informática y Sistemas de Información de Osakidetza-Servicio Vasco de Salud. Con anterioridad ha sido durante 5 años responsable informático del Hospital Txagorritxu en Vitoria-Gasteiz, y en el área corporativa cuenta con 15 años como responsable del área de Producción y otros 4 años como responsable del área Planificación y Estrategia. Ingeniero Informático por la Universidad de Deusto, Totorikaguena cuenta con más de 30 años de experiencia en el sector TI. Ha diseñado, implementado y gestionado el proyecto de Gestión de Identidades y el Control de Acceso en Osakidetza, además de múltiples proyectos en el área de Infraestructuras y Comunicaciones.

Álvaro Fernández Peña es Consultor Senior de Gestión de Identidades y Accesos del departamento de Ingeniería de Nextel S.A. Ingeniero de Telecomunicaciones por la Universidad de Deusto, cuenta con 9 años de experiencia en el sector TI, 7 de los cuales ha estado dedicado al campo de la Gestión de Identidades y el Control de Acceso. Ha diseñado, implementado y gestionado proyectos IAM en entornos universitarios, transportes y sanidad, participando en las distintas fases de su evolución. También cuenta con experiencia en proyectos de VDI y como administrador de sistemas de Internet para operadoras de comunicaciones.

Ministerio de Justicia. El contexto, la clave para un acceso seguro a la red

Sinopsis: Durante el año 2015 la Subdirección General de Nuevas Tecnologías de la Justicia acometió la puesta en marcha de un servicio de navegación con tecnología WIFI. En primer lugar se analizó la situación de partida y se fijó un escenario objetivo teniendo en cuenta la posible evolución de la demanda del servicio. Se tomaron como criterios principales la seguridad, sencillez de provisión y flexibilidad de la solución, y en base a ello se realizó un piloto previo para analizar algunas de las principales alternativas de mercado. Se adoptó la solución de Aruba desplegando infraestructura de movilidad, combinada con la solución ClearPass de autenticación. A la vista de las posibilidades de la solución, se decidió hacer de ClearPass el punto central de autenticación en otros accesos a la red, como la red cableada (802.1x + Portal Cautivo) o el acceso celular por APN privado, realizando además integraciones con productos existentes (MDM, gestión de direccionamiento) que aportaban mayor detalle en la definición de políticas de acceso seguro y de reporting.

Ponentes:
César Hernando Ceña es Jefe de Sección Comunicaciones. Subdirección General de Nuevas Tecnologías de la Justicia. Secretaría General de la Administración de Justicia. Ministerio de Justicia. Ingeniero de Telecomunicación por la Universidad de Valladolid (2003) y funcionario de la Administración General del Estado (2010), en 2002 se incorpora a la operadora de cable Retecal, en Valladolid, para luego pasar a Vodafone en 2004 en Madrid y al Servicio de Red Corporativa de la Junta de Castilla y León en 2005, lugar en el que permanece hasta 2010, realizando tareas de administración y diseño de redes Ethernet/IP e integración de equipamiento de diversos fabricantes. En 2010 se incorpora al Área de Comunicaciones de la Subdirección de Nuevas Tecnologías de la Justicia (Ministerio de Justicia), donde asume responsabilidades de las redes LAN de las sedes, de la red IP y la SAN de los Centros de Datos y la puesta en marcha de diversos servicios.

Carlos Gómez Gallego es Licenciado en Ingeniería Eléctrica por la Universidad de Queensland (Australia). Cuenta con más de 18 años de experiencia en el campo de la Seguridad y la Tecnología Inalámbrica. Actualmente, trabaja en la oficina del CTO en HPE Aruba. Fue Co-fundador y CEO de Amigopod, un proveedor líder de software empresarial de Acceso de Invitado (guest-access). Como pionera en soluciones de BYOD, Amigopod fue adquirida por Aruba Networks en diciembre de 2010. Como parte del equipo de Aruba, Carlos Gómez fue Director Senior de Gestión de Productos, donde impulsó con éxito la estrategia de productos y tecnología de la compañía, sus nuevas adquisiciones, así como el lanzamiento y la gestión del exitoso grupo de productos ClearPass. Gómez nació en Madrid y actualmente reside en San Francisco, California.

Securmática 2016 tuvo el honor de contar con la participación en el acto inaugural de **Carlos Gómez López de Medina**, General de División y Comandante Jefe del Mando Conjunto de Ciberdefensa del Mº de Defensa.

Más de 7.300 expertos han pasado por Securmática, un congreso que con sus 27 ediciones ya celebradas es el foro de intercambio de experiencias en ciberseguridad por excelencia.

// Premios SIC 2017 y Cena de la Ciberseguridad

En coincidencia con la XXVIII edición de Securmática, tendrá lugar el acto de entrega de los XIV 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 decimotercera edición de los Premios SIC.

Fechas y lugar de celebración

SECURMÁTICA 2017 tendrá lugar los días 25, 26 y 27 de abril de 2017 en el hotel NOVOTEL. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en SECURMÁTICA 2017 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 XIV Premios SIC (26 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 25 ☐ Módulo 2 Día 26 ☐ Módulo 3 Día 27 ☐ Deseo inscribirme a SECURMÁTICA 2017

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**