red seguridad

Revista especializada en Seguridad de la Información

Nº 92 primer trimestre 2021 Época II

everbridge®

Pon la seguridad en buenas manos

Automatiza tu respuesta ante cualquier crisis para proteger tu gente y tu negocio

www.everbridge.es

Ecosistema español de la ciberseguridad

ISO 27701
Gestión sostenible de la privacidad

La protección de los datos personales cobra especial relevancia no sólo por ser una obligación legal, sino porque la vulneración de la privacidad puede traducirse en una merma de confianza que se materialice en un impacto de negocio. Se impone la necesidad de definir un modelo de gestión de la privacidad sostenible.

En GMV nos encantaría ayudarte en la implantación y certificación de un sistema de gestión de la privacidad basado en el estándar 27701:

· Somos la primera empresa en España en obtener la certificación ISO 27701.
· Seguimos una metodología de implantación ágil.
· Ofrecemos flexibilidad en la aplicación de la metodología, optimizando el proceso.

marketing@gmv.com

gmv.com

gmv®
INNOVATING SOLUTIONS

Presentación

Transformación y ciberseguridad

La pandemia del coronavirus ha puesto de manifiesto la necesidad de que las empresas se doten de políticas, planes y medidas que les permitan ser resilientes. La irrupción de la pandemia impactó de forma sobrevenida en la continuidad del negocio, de manera que solo los más preparados y ágiles fueron capaces de reaccionar de manera urgente. El resto, quien más, quien menos, también ha sido capaz de salir adelante adaptándose sobre la marcha a las circunstancias y, sobre todo, realizando una importante inversión (en todos los sentidos) en tecnología. De ahí que, dentro de todo lo malo, la crisis sanitaria ha propiciado también que muchas empresas hayan sido capes de transformarse digitalmente o estén en ese proceso. Han tenido que pasar de la urgencia a un estadio en el que es fundamental establecer una estrategia. Es aquí donde la ciberseguridad ha de calar en todas las decisiones y estar alineada con ese camino hacia un modelo de producción digitalizado.

Las pymes son, en general, las que más apoyo y esfuerzo requerirán para conseguir sus objetivos de digitalización, que deben ir siempre acompañados de las medidas necesarias para proteger la información en la Red. Hemos visto cómo durante la pandemia la actividad de los ciberdelincuentes ha consistido en aprovechar las debilidades del momento, con campañas de *phishing*, *ransomware* o cualquier otro tipo de ataque que les ayudara a pescar en río revuelto. Las empresas pequeñas y medianas, *a priori* con menor capacidad y medios para hacer frente a esta tormenta perfecta, necesitan ahora interiorizar que la ciberseguridad no es una elección, sino una obligación. Para ello, además de aplicar medidas y procesos de protección, han de concienciarse de la importancia proteger sus activos en la Red. Solo así conseguirán llegar a esa senda de la resiliencia y la continuidad del negocio, incluso en situaciones inesperadas de alto impacto.

En la editorial Borrmart, editora de RED SEGURIDAD, lo sabemos. Estamos atravesando proceso de digitalización para ser capaces de continuar informándoles y ofreciendo servicios, no solo a través de las páginas web que hemos lanzado durante la pandemia, sino también con eventos virtuales que acerquen a toda la sociedad la importancia de la ciberseguridad y multitud de herramientas a disposición de nuestros anunciantes. Gracias a nuestro ecosistema digital, ahora podemos llegar a más gente y ofrecer mejor servicio. Queremos de esta manera contribuir a la creación de una cultura de ciberseguridad en las empresas en general, y en las pymes en particular.

A través de este número especial queremos dar muestra de que la ciberseguridad es un asunto de Estado, para el que existen organismos y una auténtica industria que se nutre de multitud de profesionales. Si en la pandemia todos somos parte de la solución, en este asunto igualmente se trata de sumar esfuerzos, desde las empresas más pequeñas hasta las más altas capacidades de nuestro país. El número está dividido en cinco bloques, dedicados a los organismos de ciberseguridad del Estado, los centros de respuesta a incidentes, varios responsables de seguridad de la información, empresas, asociaciones y normativa. De este modo, queremos ofrecer una visión completa de esta actividad no solo a los profesionales sino a toda la sociedad. Todos estos actores conforman el grueso de los recursos españoles, que tendrán que aumentar y evolucionar al ritmo en que lo haga una sociedad cada vez más digital. Las pymes incluidas. ■

sumario

7

corporativo

Yolanda Duro, nueva directora de RED SEGURIDAD

34

respuesta a incidentes

Contención de las ciberamenazas

10

corporativo

Evento "La Alta Dirección, Concienciación & Implicación con la Ciberseguridad"

44

empresas

Entrevista a José Manuel Villanueva

Country Manager para Iberia de Everbridge

12

organismos

La ciberseguridad española

98

asociaciones

Nexo de unión entre profesionales y empresas

22

expertos

Protegiendo las empresas en tiempos de ciberpandemia

110

normativa

La regulación avanza al ritmo de los retos en el ciberespacio

CONSEJO TÉCNICO ASESOR

PRESIDENTE
Guillermo Llorente Ballesteros
Mapfre

VOCALES
Mar España Martí
Agencia Española de Protección de Datos (AEPD)

Pedro Mier
Ametic

Fernando Rodríguez del Estal
Asociación de Empresarios de TIC de Andalucía (ETICOM)

Joaquín González Casal
Asociación de Ingenieros e Ingenieros Técnicos en Informática (ALI)

Vicente Aceituno Canal
Asociación Española para la Seguridad de los Sistemas de Información (ISSA España)

Alfonso Castaño
ASIS España

José Valiente
Centro de Ciberseguridad Indutrial (CCI)

Pedro Pacheco
Unidad Central de Ciberdelincuencia del Cuerpo Nacional de Policía

Juan Sotomayor
Unidad de Delitos Telemáticos (GDT) de la Guardia Civil

Rosa Díaz
Instituto Nacional de Ciberseguridad (INCIBE)

Vanesa Gil
ISACA Capítulo de Madrid

Gianluca D'Antonio
ISMS Forum Spain

Vicente Aguilera Díaz
Open Web Application Security Project (OWASP)

CONSEJEROS INDEPENDIENTES
Tomás Arroyo
Javier Moreno Montón
Javier Pagès
Olof Sandstrom
Juan Carlos Batanero

PRESIDENTE DE HONOR
Alfonso Mur Bohigas

red seguridad

Suscripción anual:
50 euros (España), 110 euros (Europa, zona euro), 150 euros (resto países)
suscripciones@borrmart.es

Depósito Legal: M-46198-2002
ISSN: 1695-3991

STAFF

Borrmart: Presidenta: Ana Borredá. Directora general: Ana Borredá. Adjunto a la Presidencia y a la Dirección General: Antonio Caballero Borredá. Publicidad: Yolanda Duro, Pedro José Pleguezuelos, Paloma Melendo, Fco. Javier Borredá García, Virginia Alcalde y Carmen Dorribo. Directora de Relaciones Institucionales: Mª Victoria Gómez.
Red Seguridad: Directora: Yolanda Duro. Subdirector: Enrique González Herrero. Redactor: Juanjo S. Arenas. Colaboradores: David Marchal, Bernardo Valadés, Leticia Duque Guerrero y Jaime Sáez de la Llave. Maquetación: Macarena Fdez. López. Fotografía: Banco de imágenes GettyImages. Diseño: Escriña Diseño Gráfico. Área digital: Laura Borredá y Natividad Benéitez. Suscripciones: Mª Isabel Melchor y Elena Sarriá. Dirección Financiera: Javier Pascual Bermejo. Redacción, Administración y Publicidad: C/ Don Ramón de la Cruz, 68. 28001 Madrid • Tel.: +34 91 402 96 07
• www.borrmart.es • www.redseguridad.com • red@borrmart.es. Fotomecánica e impresión: Comeco Gráfico S.L.U.

RED SEGURIDAD no se responsabiliza necesariamente de las opiniones o trabajos firmados, no autoriza la reproducción de textos e ilustraciones sin autorización escrita.
Usted manifiesta conocer que los datos personales que facilite pasarán a formar parte de un fichero automatizado titularidad de BORRMART, S.A. y podrán ser objeto de tratamiento, en los términos previstos en la Ley Orgánica 03/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y normativa al respecto. Para el cumplimiento de los derechos de acceso, rectificación y cancelación previstos en dicha ley dirijase a BORRMART, S.A. C/ Don Ramón de la cruz, 68. 28001 Madrid.

OPEN WEEK

SOLUCIONES POSTCOVID

#JUNTOS SOMOS PARTE DE LA SOLUCIÓN

OPEN SECURITY DAY

OPEN CYBERSECURITY DAY

OPEN SAFETY DAY

OPEN FACILITY DAY

OPEN CLEANING DAY

MÁS DE 3.500 PROFESIONALES CONECTADOS
MÁS DE 60 PONENTES DE PRIMER NIVEL

¿TE LO HAS PERDIDO?

Accede a la Webapp y visita la Galería de Productos, los vídeos de las ponencias y mucho más...

ACCEDE A LA WEBAPP

BORRMART EVENTOS Apostamos por los eventos digitales. Por responsabilidad

El Grupo Borrmart apuesta por la digitalización

A comienzos de 2020, el Grupo Borrmart, editor de RED SEGURIDAD, impulsó una importante e innovadora estrategia de digitalización de todo su ecosistema: nueva imagen de sus webs, formatos novedosos de publicidad, analítica, programática y herramientas de marketing digital que tienen como objetivo llegar a más lectores que nunca y ofrecer un mejor servicio. Una transformación de negocio que ha hecho que la revista RED SEGURIDAD registre 240.000 páginas vistas y un incremento de un 50 por ciento más de usuarios durante el pasado año.

A esos buenos datos hay que sumar sus más de 17.000 contactos en sus **servicios de suscripción** por *email*, 60.000 lectores de RED SEGURIDAD Digital en Kiosko Pro por número, 70.000 visitas a su página web, más de 20.000 seguidores en **redes sociales** y más de 15.000 asistentes a los más de 10 eventos digitales que ha organizado en 2020. Todo ello confirma su dominio absoluto.

Todas las **webs** de Borrmart consiguieron sus datos más altos (1 millón de visitas) en sus 10 años de historia y suman varios meses como las webs informativas líderes en todos los sectores en los que operan.

Cada revista ha rediseñado sus páginas y ***newsletters*** con un diseño que apuesta por la imagen y la versatilidad.

Un nuevo proyecto que les permite ofrecer las técnicas más avanzadas y efectivas en comunicación y venta *online*: nuevas herramientas de analítica digital, estrategia SEO, incorporación del AdServer Google Ad Manager, segmentación de audiencias e integración de herramienta de Marketing Automation y CRM social para la gestión y personalización de sus clientes y lectores.

Eventos y marketing digital

Como se acaba de mencionar, el Grupo Borrmart, bajo la marca **Borrmart Eventos**, ha realizado numerosos congresos desde que comenzó la pandemia del coronavirus. Para ello, ha consolidado un nuevo modelo de eventos, en formato digital, con la incorporación e integración de la última tecnología y herramientas digitales.

Por otro lado, cabe destacar la apuesta de Borrmart por el marketing digital con **Visibility**. Una nueva agencia cuyo objetivo es optimizar la presencia de las empresas en el mundo digital.

Visibility adapta las mejores prácticas del mundo digital a las necesidades del negocio de las compañías, a las que ofrece los siguientes servicios: webs y *e-commerce*, posicionamiento web SEO y redes sociales; estrategia de redes sociales; *email* marketing; inteligencia de CRM digital; y planes de medios.

Kiosko Pro

La última innovación de Borrmart es **Kiosko Pro**, una moderna y completa plataforma de *e-commerce* que permitirá a los lectores y *partners* beneficiarse de sus diferentes servicios: revistas y suscripciones; informes, estudios y libros; inscripciones a eventos; y publicidad y marketing.

En definitiva, Kiosko Pro será un espacio exclusivo para suscriptores y una tienda *online* que posibilitará beneficiarse de servicios y las mejores ofertas. ■

Yolanda Duro, nueva directora de RED SEGURIDAD

Ana Borredá, hasta el año pasado directora de RED SEGURIDAD, ha cedido el testigo a Yolanda Duro para sumir las riendas de la revista. Esta profesional se hará cargo de definir la estrategia y objetivos de esta publicación, tanto en su formato en papel, como digital y en la organización de eventos. Borredá deja la dirección para dedicarse de pleno a la presidencia y dirección general del Grupo Borrmart, al que pertenece la cabecera.

Yolanda Duro se incorporó a la editorial Borrmart en 2015 como responsable de Marketing y Publicidad. Poco después trabajó en el impulso del negocio de la editorial en Latinoamérica, pasando a ser responsable de desarrollo de negocio en la región.

La nueva directora de RED SERGURIDAD es licenciada en Derecho y Gestión Empresarial, ha sido socia fundadora de varias empresas a lo largo de su trayectoria, asumiendo la dirección comercial y de marketing, y durante 13 años ejerció como procuradora en los Tribunales.

Equipo de RED SEGURIDAD

Junto a Yolanda Duro se mantiene como subdirector de la publicación Enrique González, responsable de contenidos y redacción de la revista. En la redacción permanece también Juanjo S. Arenas, periodista especializados seguridad, apoyado por otros periodistas de la editorial y colaboradores como David Marchal.

Yolanda Duro.

Arriba: Juan Carlos Batanero y Ana Borredá. Abajo: Enrique González (izquierda) y Juanjo S. Arenas (derecha).

El área comercial está compuesta por Virginia Alcalde, Carmen Dorribo, Paloma Melendo y Javier Borredá. Dorribo se incorporó al proyecto el año pasado, para apoyar en la estrategia de marketing y publicidad de la revista.

El resto del equipo está compuesto por Mariví Gómez Alonso, directora de relaciones Institucionales, así como Laura Borredá, responsable del área digital, y Natividad Benéitez, redactora de dicha área.

Incorporación al CTA

RED SEGURIDAD también tiene el placer de contar con la incorporación de Juan Carlos Batanero a su Consejo Técnico Asesor (CTA), como asesor independiente. Batanero es actualmente consultor en defensa, seguridad y ciberseguridad, tras una trayectoria de cerca de 30 años en Indra en puestos de responsabilidad, como director de unidad de negocio.

Batanero se suma al resto del CTA de la revista, que está presidido por Guillermo Llorente, subdirector general de Seguridad y Medio Ambiente de Mapfre. Este órgano asesor está compuesto además por otros profesionales independientes y por representantes de la AEPD, Policía Nacional, Guardia Civil e Incibe, así como de las asociaciones AMETIC, ETICOM, ALI, ISSA España, ASIS España, CCI, ISACA Madrid, ISMS Forum y OWASP. ■

RED SEGURIDAD convoca los Trofeos de la Seguridad TIC

RED SEGURIDAD retoma este año la convocatoria de sus Trofeos de la Seguridad TIC, con los que reconoce la labor de los profesionales, empresas y organismos dedicados a la ciberseguridad. Tras un parón el año pasado motivado por la irrupción de la pandemia del coronavirus, la revista convoca su 14ª edición este año.

Si bien cada convocatoria de estos galardones premia a los profesionales, proyectos, programas, operaciones o productos destacados el año anterior, en esta ocasión el periodo que aceptará el jurado para las candidaturas comprende los años 2020 y 2019.

El plazo máximo de presentación de candidaturas de los premios finaliza el 30 de julio y el fallo se dará a conocer a finales de este año. Dado que la pandemia no ha finalizado, la modalidad de entrega de los galardones vendrá determinada por las circunstancias de ese momento.

Cómo participar

Los profesionales, empresas y organismos que deseen presentar su candidatura a los Trofeos de la Seguridad TIC tendrán que rellenar en primer lugar el formulario de inscripción que encontrarán en la página web: https://form.jotform.com/borrmart/trofeos-de-la-seguridad-tic-2021

Una vez enviado, los candidatos tendrán hasta el 30 de julio para presentar un memoria personalizada (con una extensión mínima de tres páginas), acompañada de un carta de presentación remitida a la dirección de la revista, al siguiente correo electrónico: trofeos.redseguridad@borrmart.es.

Estos premios cuentan con seis candidaturas abiertas y un trofeo extraordinario que concede el propio Jurado. Las candidaturas son:

- Trofeo al producto/servicio o sistema de seguridad más innovador.
- Trofeo a la empresas SegTIC.
- Trofeo a la institución u organismo público en materia de seguridad TIC.
- Trofeo a la trayectoria profesional pública o privada en seguridad TIC
- Trofeo a la captación, divulgación, concienciación o formación en seguridad TIC.
- Trofeo al centro educativo SegTIC.

El Comité Técnico Asesor de RED SEGURIDAD, compuesto por representantes de las principales asociaciones del sector, varios organismos y profesionales independientes, conforman el Jurado de estos premios. Son ellos quienes deliberan tras recibir todas las candidaturas y formularán el veredicto definitivo.

red seguridad

Consulte las bases completas en:

https://www.borrmart.com/trofeos/trofeos-de-la-seguridad-tic/bases-y-formulario/

Trofeos de la Seguridad TIC

red seguridad

Imagen de los premiados en los últimos Trofeos de la Seguridad TIC, celebrados en la sede de la Bolsa de Madrid en 2019.

Participa en la 14ª edición de los **Trofeos de la Seguridad TIC**

RED SEGURIDAD, revista independiente especializada en seguridad de la información, ha puesto en marcha de nuevo los **Trofeos de la Seguridad TIC**. Estos galardones pretenden reconocer y exaltar los méritos de aquellas personas, fabricantes y entidades públicas y privadas relacionadas con la seguridad TIC.

Para mantener la independencia de este certamen, el Jurado de estos premios está conformado por los representantes del Consejo Técnico Asesor de la publicación, que son los representantes de las principales asociaciones del sector, varios organismos y profesionales independientes del mundo de la ciberseguridad.

El año pasado tomamos la decisión de interrumpir los Trofeos debido a la situación sobrevenida por la pandemia del COVID-19, pero en esta convocatoria se podrán presentar candidaturas relativas a 2019 y 2020. Las modalidades a las que podrán optar las candidaturas son:

MODALIDADES DE LOS "TROFEOS DE LA SEGURIDAD TIC"

T1.- TROFEO AL PRODUCTO/SERVICIO O SISTEMA DE SEGURIDAD MÁS INNOVADOR.

T2.- TROFEO A LA EMPRESA SegTIC.

T3.- TROFEO A LA INSTITUCIÓN U ORGANISMO PÚBLICO EN MATERIA DE SEGURIDAD TIC.

T4.- TROFEO A LA TRAYECTORIA PROFESIONAL PÚBLICA O PRIVADA EN SEGURIDAD TIC.

T5.- TROFEO A LA CAPACITACIÓN, DIVULGACIÓN, CONCIENCIACIÓN O FORMACIÓN EN SEGURIDAD TIC.

T6.- TROFEO AL CENTRO EDUCATIVO SegTIC.

Para conocer las normas que deben seguir las candidaturas que opten a los Trofeos, así como los formularios para presentarlas, consulte la página web: www.borrmart.com/trofeos/trofeos-de-la-seguridad-tic/bases-y-formulario/

El plazo máximo de presentación de candidaturas finaliza el próximo 30 de julio, si bien la organización se reserva el derecho a posibles modificaciones, que anunciará debidamente a través de RED SEGURIDAD y de su página web (www.redseguridad.com).

La revista publicará el fallo del Jurado y, en función de las circunstancias que permita la pandemia del COVID-19, se decidirá la modalidad de entrega.

¡Participa!

Alta dirección: comprometida con la ciberseguridad

La ciberseguridad importa a los responsables de las empresas. Así lo pusieron de manifiesto varios ejecutivos de importantes organizaciones en el evento "La Alta Dirección, Concienciación & Implicación con la Ciberseguridad", organizado por Red Seguridad y Fundación Borredá y patrocinado por Accenture Security y S21Sec.

Por David Marchal

La ciberseguridad debe formar parte del comité de dirección y de la estrategia corporativa de las organizaciones. Además, ha de ser una materia transversal en todas sus áreas y consustancial al negocio. Por eso, resulta fundamental abogar por una cultura de la ciberseguridad en la que prime la concienciación y la formación de los empleados en este ámbito. Estas son algunas de las ideas que se pusieron sobre la mesa durante el evento digital "La Alta Dirección, Concienciación & Implicación con la Ciberseguridad", organizado por *Red Seguridad* y Fundación Borredá, con el patrocinio de Accenture Security y S21Sec.

Este encuentro virtual reunió a más de 500 profesionales interesados en la ciberseguridad, que pudieron escuchar las opiniones de representantes de la alta dirección de diferentes compañías. La apertura corrió a cargo de **Félix Barrio**, gerente de Ciberseguridad para la Sociedad del Instituto Nacional de Ciberseguridad (Incibe), quien alertó de las nuevas ciberamenazas a las que están sometidas las organizaciones, sobre todo a raíz de la pandemia. Al respecto, recalcó que es importante que la dirección de las empresas apueste por la ciberseguridad. "De esta se sale", comentó, "pero con ciberseguridad se hará más y mejor para mantener a la sociedad y a la economía, y sobre todo para mejorar la resiliencia y la competitividad de las organizaciones".

Junto a él también participaron **Jaime Pascual-Sanchiz**, CEO de Savills Aguirre Newman; **Joaquín Cucala**, Senior Vice President and General Counsel Asia Pacific, Middle East and Africa de Procter & Gamble; **Victoria Hernández Valcárcel**, consejera en CaixaBank Payments & Consumer; **Antonio Puente**, director general de Adolfo Domínguez; **Miguel Vázquez Caride**, director de Tecnologías de la Información de Adolfo Domínguez; **Roy Donoso**, presidente de SUMAC; **Xabier Mitxelena**, Accenture Security Lead

Patrocinado por:

accenture S21 SEC

para España, Portugal e Israel; e **Igor Unanue**, CTO y cofounder de S21 sec. **Yolanda Duro**, directora de *Red Seguridad*, moderó el encuentro.

Compromiso

Todos pusieron de manifiesto su compromiso con la ciberseguridad desde sus puestos directivos. Por ejemplo, Hernández Valcárcel, de CaixaBank Payments & Consumer, confirmó que en su entidad han tenido en cuenta la ciberseguridad "desde el minuto uno". "De hecho, nos hemos incorporado al consejo de administración personas como yo, con más de 30 años en el sector de la alta tecnología y de la ciberseguridad", manifestó.

En la misma línea se pronunció Pascual-Sanchiz, de Savills Aguirre Newman. "Desde el principio tuvimos muy en cuenta la importancia de proteger los datos, y más ahora que están más expuestos que nunca a las redes". Algo a lo que Cucala, de Procter & Gamble, añadió la importancia de salvaguardar los datos de los consumidores. "Por eso, vemos la ciberseguridad desde dos puntos de vista: para potenciar la imagen reputacional de la empresa y para conservar la confianza de los consumidores", indicó.

En el caso de SUMAC, la apuesta de la compañía por la ciberseguridad viene por la propia naturaleza de su negocio. "Trabajamos con grandes multinacionales en proyectos de construcción e infraestructura y nos movemos en entornos aeroportuarios, por lo que tenemos muy presente la ciberseguridad. De hecho, nuestros clientes nos obligan a contar con las más altas medidas de seguridad", afirmó.

Claro que también esa preocupación puede provenir del ámbito personal de los propios CEO. "Hace años empezaron a suplantarme digitalmente para tener acceso a nuestra red de tiendas y filiales. Cuando esto te pasa, te das cuenta realmente de lo que podría llegar a suceder. Así que decidimos invertir en más medidas de ciberseguridad", recordó Puente, de Adolfo Domínguez. La empresa, además, apostó por la concienciación de sus empleados.

Recursos y medidas

Sobre esa cuestión coincidieron el resto de los participantes. Por ejemplo, Pascual-Sanchiz, de Savills Aguirre Newman, comentó: "Invertimos mucho tiempo y recursos en formar a nuestra gente para que sepa por dónde vienen los ciberataques y cómo podemos evitarlos".

Así lo están haciendo también los demás invitados. No en vano, esta preocupación por la ciberseguridad cada vez se va extendiendo más entre la dirección de las organizaciones. Resulta imprescindible que así sea ante el incremento de la ciberamenazas, tal y como se constató durante la sesión. "Estos últimos meses, con la pandemia, se han puesto en jaque a todas las empresas. En nuestro caso, hemos activado un comité de seguridad y hemos aumentado la frecuencia del análisis de las operaciones de protección en todos los ámbitos, incluida la ciberseguridad", afirmó Vázquez Caride, de Adolfo Domínguez.

La situación es similar en el resto de empresas. De hecho, muchos de los asistentes confirmaron que reciben cientos de intrusiones diariamente, sobre todo mediante ataques de *phishing*. Por fortuna, ninguna suele tener consecuencias, pero afirman que son conscientes de la necesidad de reforzar la seguridad digital. Y es que, como repitieron varios intervinientes durante la sesión, "una compañía es tan fuerte en este ámbito como lo es su eslabón más débil".

Por eso, hay que tener "una visión estratégica a medio y largo plazo que incluya la evolución de la innovación y nuevas tecnologías como 5G, *blockchain*, identificación biométrica…", según enumeró Hernández Valcárcel, de CaixaBank. A lo cual añadió, por un lado, la importancia de ser "proactivos en este campo", y por otro, "la necesidad de incorporar y conservar talento en ciberseguridad".

Estrategia corporativa

De ahí que, tal y como recordaron los representantes de los proveedores de ciberseguridad Accenture Security y S21Sec, es preciso contar con una estrategia corporativa de ciberseguridad bien definida. De hecho, animaron a la alta dirección a dar ese paso si aún no lo han hecho. "Hay empresas cuya dirección está muy sensibilizada con la ciberseguridad, pero otras en las que no ocurre así y solo ponen medidas cuando sufren ciberataques", confirmó Unanue, de S21Sec, quien recalcó que "la ciberseguridad siempre debe impregnar todos los procesos de negocio, no solo algunos".

Por su parte, Mitxelena, de Accenture Security, ratificó las palabras de Unanue y dio a conocer algunos casos de empresas que habían sufrido ciberataques, con el consiguiente daño reputacional y económico que les causó. Y es que, a su juicio, "las organizaciones deben tener siempre una estrategia de seguridad alineada con el negocio". No en vano, sentenció: "invertir en ciberseguridad es competir".

Precisamente, Donoso, de SUMAC, apuntó que, en este contexto, "apostar por la ciberseguridad supone para las empresas una ventaja competitiva y un elemento diferenciador en el mercado". Además, es una materia transversal a todos los *stakeholders* (clientes, proveedores, accionistas…). Y es que, como resumió Barrio, de Incibe, "la ciberseguridad es la base de la confianza y, sin ella, no hay economía, ni clientes, ni competitividad". ■

Reglamento NIS: un avance con dudas que despejar

Por Enrique González Herrero

El Gobierno aprobó el 26 de enero el Reglamento de Seguridad de las Redes y Sistemas de la Información (Reglamento NIS), que desarrolla la ley sobre esta materia que afecta a operadores de servicios esenciales y proveedores de servicios digitales. Se trata de un avance normativo que aclara cuestiones como el marco institucional de ciberseguridad, la cooperación y coordinación, la gestión y notificación de ciberincidentes o la función de los responsables de seguridad de la información. En definitiva, dibuja un marco de gobernanza y gestión de la ciberseguridad en organizaciones clave para la sociedad.

Con el objetivo de analizar el impacto de la norma en las empresas afectadas por la norma, la Fundación Borredá reunió un elenco de expertos en la materia. **Andrés Jesús Ruiz Vázquez**, consejero técnico en la Unidad de Ciberseguridad y Desinformación del Departamento de Seguridad Nacional (DSN); **Joan Puig**, CISO de Banco Sabadell; **Francisco Lázaro**, vicesecretario de ISMS Forum y CISO de Renfe; y **Félix de Andrés**, *Manager* de *Risk Advisory* de Deloitte España, participaron en una de las tertulias virtuales organizada por la Fundación Borredá. **César Álvarez**, coordinador de proyectos de esta última, condujo el encuentro.

Todos ellos coincidieron en que el impacto inicial del Reglamento NIS en las organizaciones no debería ser complejo, más bien, el primer paso será revisar qué se ha hecho hasta el momento. "Lo primero que habrá que hacer es revisar qué se había avanzado ya con la Ley NIS [Ley sobre Seguridad de las Redes y Sistemas de la Información], ver lo nuevo que se está haciendo con este reglamento y, a partir de ahí, empezar a trabajar en todos los puntos", observó De Andrés.

Una opinión con la que coincidió Puig, de Banco Sabadell, quien también llamó la atención sobre otro aspecto: la necesidad de realizar una declaración de aplicabilidad de las medidas de seguridad de las empresas. "Es un nombre que confunde, porque ya habíamos hecho un formulario de aplicabilidad en el que explicábamos sobre qué sistemas de información pensábamos que nos afectaba la Ley NIS. Ahora utilizamos la misma palabra en otra dimensión, que es la de las medidas de seguridad", expuso.

Para el representante de ISMS Forum, "la gran mayoría de las organizaciones ya tienen los deberes hechos, porque si provienen del Esquema Nacional de Seguridad (ENS), de infraestructuras críticas o de servicios esenciales, la gran mayoría de las cosas ya están asignadas, como la designación del responsable de seguridad de la información, la notificación de incidentes o incluso la declaración de aplicabilidad". "Lo que hace el Reglamento es particularizar algunos aspectos", concluyó Lázaro.

En la misma línea argumental, el representante del DSN recordó que "España aprovechó la ocasión" cuando se traspuso la Directiva NIS "utilizando la normativa sobre protección de las infraestructuras críticas para ampliar los sectores que afectan a la norma europea". "Esto ha conllevado que prácticamente todos los servicios esenciales identificados bajo el paraguas de la normativa NIS, a la vez sean operadores críticos", explicó Ruiz Vázquez. Aun con ello, este profesional opinó que todavía quedan retos respecto a la norma, como, por ejemplo, "reforzar las estructuras actuales en relación con los centros de respuesta a incidentes de referencia y a las de autoridades competentes".

Papel del CISO

Sin duda, uno de los aspectos que despertó mayor interés en torno al Reglamento NIS era conocer si tendría en cuenta la figura de responsable de seguridad de la información (RSI). Finalmente, así ha ocurrido, pues era una reclamación constante por parte del sector de la Ciberseguridad. "Cuando se recibieron los comentarios de la consulta pública del borrador del Reglamento NIS, todas las asociaciones hicieron hincapié en la importancia de incluir esta figura. Era prácticamente una obligación incluirlo y, además, hacerlo bien, con criterios técnicos y estratégicos. Porque la madurez de la ciberseguridad de una organización viene determinada muchas veces por el estatus del CISO, es decir, dónde está situada esa persona y a cuántos escalones de la alta dirección", desarrolló el representante del DSN.

La decisión ha sido aplaudida, aunque existen diferentes puntos de vista a la hora de aclarar la responsabilidad de este profesional. "Vemos bien formalizar la figura del RSI, pero vemos más relevante establecer sus responsabilidades. Podemos discutir si encajan en primera o segunda línea del organigrama, pero responsabilidades hay muchas en relación con la tecnología dentro de la organización", reflexionó Puig, de Banco Sabadell.

Lázaro sostuvo que "las responsabilidades recaen en la organización, que tienen que tener unas políticas de seguridad claras y aprobadas". "Es más, en las funciones se dice que el RSI propone las medidas al órgano correspondiente de su aprobación, y por lo tanto hay una responsabilidad de los órganos de dirección de la compañía", desarrolló.

Para el representante de ISMS Forum, "es muy importante que se haya definido esta figura" y considera "muy bueno" que la ley hable de la posición que debe tener cercada a los órganos de dirección. Aun así, también indicó la necesidad de dirimir exactamente qué quiere decir la norma cuando habla de la posición e independencia del RSI en las empresas.

De Andrés añadió que la propia Ley NIS "establece sanciones, pero para la organización", lo cual muestra que la responsabilidad final recae en esta. "Creo que se ha hecho muy bien a la hora de signar las responsabilidades y, de hecho, hay un punto que dice que el RSI puede apoyarse en servicios de terceros, pero tiene que formar parte de la propia entidad, es decir, no puede externalizarse".

Debilidades y ausencias

Pero si la designación del RSI es una de las cuestiones que han provocado más satisfacción, también existen diferentes controversias con el Reglamento NIS. Fundamentalmente porque no ha despejado todas las dudas del sector. En ese sentido se pronunció De Andrés, quien planteó interrogantes en torno a los proveedores de servicios digitales. Con esta norma "aún hay muchas empresas que tienen dudas sobre si son o no proveedores de servicios digitales; si bien es cierto que la Directiva NIS no deja mucho margen a los países, la duda sigue quedando", expresó.

Por su parte, Lázaro, de ISMS Forum, puso el acento en la seguridad de los proveedores: "está bien que tengamos la obligación de gestionar los riesgos de terceros, pero echamos de menos que los proveedores tengan también unas obligaciones marcadas". A lo cual añadió que hay grandes compañías que prestan servicios y productos, pero "no tienen detrás una figura que se preocupe por los requisitos de seguridad y sean elemento de interlocución en caso de incidente".

Algo con lo que se mostró de acuerdo el representante de Banco Sabadell, que puso como ejemplo el Reglamento General de Protección de Datos, el cual "establece normas a las empresas, aunque haya algo que no esté recogido en un contrato". Desde su punto de vista, la "norma podría haber tenido otra aproximación, estableciendo obligaciones directas sobre los proveedores".

Ruiz Vázquez, del DSN, se mostró de acuerdo con el resto de invitados y apuntó que varias de las dudas existentes ahora podrían quedar resueltas en la revisión de la Directiva NIS que está llevando a cabo la Unión Europea en este momento. Por ejemplo, la futura norma comunitaria "obligará a tener esta política a nivel nacional respecto a los proveedores y a toda la cadena de suministro".

Por otro lado, este profesional opinó que "el modelo necesita ir acompañado de información clara a los sujetos obligados y a las administraciones. Es frecuente recibir preguntas de empresas que dudan si tienen que notificar un incidente o si son operador esencial. Falta información y cultura de seguridad".

Finalmente, también planteó la necesidad de que exista una comunicación coordinada de vulnerabilidades. Ruiz Vázquez consideró importante "establecer un marco de comunicación para comunicar la vulnerabilidades, obviamente con un repositorio custodiado". ■

La ciberseguridad española

España cuenta con un amplio conjunto de organismos dedicados a la ciberseguridad, unos constituidos sobre todo en las dos últimas décadas y otros que han evolucionado con el tiempo. Juntos conforman los recursos que tiene a su disposición el Estado para hacer frente a las amenazas procedentes de la Red, entre los que se encuentran entidades de apoyo a las empresas, a la ciberseguridad del Estado, a lucha contra el cibercrimen, a la Defensa, unidades de las Fuerzas y Cuerpos de Seguridad o foros de cooperación, entre otros. En las siguientes páginas hacemos una selección de los principales órganos encargados de establecer las políticas, recursos y medidas de seguridad en el ciberespacio de la que dispone nuestro país.

Secretaría de Estado de Seguridad

AÑO DE CREACIÓN: 1994

La Secretaría de Estado de Seguridad (SES), dependiente del Ministerio del Interior, tiene entre sus funciones la dirección y coordinación de las políticas de ciberseguridad que competen a dicho ministerio. Asimismo, está encargada de dirigir el Sistema Nacional de Protección de Infraestructuras Críticas. Para ambos objetivos, el secretario de Estado de Seguridad cuenta con el asesoramiento del Gabinete de Coordinación y Estudios.

De la SES dependen el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, la Oficina de Coordinación de Ciberseguridad y la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad. Los cometidos de esta última incluyen planificar, coordinar y gestionar las inversiones en TIC para las Fuerzas y Cuerpos de Seguridad del Estado, así como promover proyectos al respecto.

DIRIGIDA POR:

Rafael Pérez Ruiz

Secretaría de Estado de Digitalización e Inteligencia Artificial

AÑO DE CREACIÓN: 2020

La Secretaría de Estado de Digitalización e Inteligencia Artificial, dependiente del Ministerio de Ministerio de Asuntos Económicos y Transformación Digital, tiene competencias relativas a la política de impulso a la digitalización de la sociedad y economía. Funciones que desarrolla a través del fomento y regulación de los servicios digitales y de la economía y sociedad digitales, la interlocución con los sectores profesionales, industriales y académicos, así como el impulso de la digitalización del sector público.

Bajo la dirección de esta secretaría está la Secretaría General de Administración Digital, responsable de la transformación digital del conjunto de la Administración General del Estado, así como el Instituto Nacional de Ciberseguridad (Incibe).

avancedigital.mineco.gob.es/es-es/Paginas/index.aspx

DIRIGIDA POR:

Carme Artigas

Secretaría General de Administración Digital

AÑO DE CREACIÓN: 2017

La Secretaría General de la Administración Digital (SGAD), dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial, es el órgano encargado de impulsar la racionalización de las TIC de la Administración General del Estado y sus organismos públicos. También es responsable de la implantación de medidas de protección en este entorno, como el Esquema Nacional de Seguridad.

La SGAD cuenta con una División de Planificación y Coordinación de Ciberseguridad a través de la que se encarga de la dirección técnica y estratégica del Centro de Operaciones de Ciberseguridad de la Administración General del Estado. Entre las funciones que asume la SGAD para dicho centro está el seguimiento y gestión del servicio, la coordinación con los actores involucrados o la coordinación de la respuesta ante incidentes.

DIRIGIDA POR:

Juan Jesús Torres Carbonell

Consejo Nacional de Ciberseguridad

AÑO DE CREACIÓN: 2013

El Consejo Nacional de Ciberseguridad (CNC) es el órgano colegiado de apoyo al Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional. Este órgano tiene múltiples funciones, como reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas administraciones públicas con competencias en materia de ciberseguridad, así como entre los sectores público y privado. El CNC también ejerce funciones de análisis y valoración de riesgos y amenazas, además de posibles escenarios de crisis y planes de respuesta. También se hace cargo de verificar el grado de cumplimiento de la Estrategia de Ciberseguridad Nacional.

www.dsn.gob.es/es/comités-especializados/consejo-nacional-ciberseguridad

PRESIDIDO POR:

Paz Esteban López

Departamento de Seguridad Nacional

AÑO DE CREACIÓN: 2012

El Departamento de Seguridad Nacional (DSN) es un órgano de asesoramiento al presidente del Gobierno en materia de seguridad nacional. Entre otras, asume las funciones de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional. Entre las muchas atribuciones del DSN, tiene encomendada la coordinación y el desarrollo de la Estrategia de Seguridad Nacional, así como de la Estrategia de Ciberseguridad Nacional. A través de este órgano, el Consejo de Seguridad Nacional actúa como punto de contacto único de enlace para la cooperación con otros países de la Unión Europea y gestiona aquellas situaciones de crisis que desborden las capacidades de respuesta de los mecanismos habituales.

www.dsn.gob.es

DIRIGIDO POR:

General de Brigada
Miguel Ángel Ballesteros

Foro Nacional de Ciberseguridad

AÑO DE CREACIÓN: 2020

El Foro Nacional de Ciberseguridad es un órgano de colaboración público-privada dependiente orgánicamente del Consejo Nacional de Ciberseguridad. Su composición está encabezada por el Departamento de Seguridad Nacional, con dos vicepresidencias correspondientes al Centro Criptológico Nacional y al Instituto Nacional de Ciberseguridad. Además, está formado por representantes de la sociedad civil de entidades privadas, asociaciones, organizaciones sin ánimo de lucro, universidades o *think thanks*.

En este momento, el Foro trabaja en tres líneas de trabajo: por un lado, generar cultura de ciberseguridad; por otro, ofrecer apoyo a la Industria e I+D+i; y finalmente, la formación y el talento en ciberseguridad.

foronacionalciberseguridad.es

PRESIDIDO POR:

General de Brigada
Miguel Ángel Ballesteros

Mando Conjunto del Ciberespacio

AÑO DE CREACIÓN: 2013

El Mando Conjunto del Ciberespacio es el órgano subordinado al Jefe de Estado Mayor de la Defensa responsable del planeamiento y la ejecución de las acciones de ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa. En términos generales, se encarga de dar respuesta en el ciberespacio a las amenazas o agresiones que puedan afectar a la Defensa Nacional.

Entre sus competencias está dirigir y coordinar la actividad de los Centros de Respuesta a Incidentes de Seguridad de la Información de los ejércitos, ejercer la respuesta en el ciberespacio ante amenazas o agresores que puedan afectar a la Defensa Nacional, así como definir, dirigir y coordinar la concienciación y la formación en esta materia.

emad.defensa.gob.es/unidades/mcce

COMANDANTE:

General de División
Rafael García Hernández

Dirección General de Armamento y Material del Ministerio de Defensa

AÑO DE CREACIÓN: 1977

La Dirección General de Armamento y Material (DGAM) es el órgano directivo al que corresponde la preparación, planificación y desarrollo de la política de armamento y material del Ministerio de Defensa, así como la supervisión y dirección de su ejecución. Tiene responsabilidades en cuatro áreas, en las que están incluidos proyectos y armamento relacionado con la ciberdefensa.

Las cuatro áreas en las que trabaja son: planificación, actividades de I+D, gestión de las adquisiciones y logística de los sistemas de armas. La Política de Armamento y Material da respuesta a las necesidades de las Fuerzas Armadas determinadas por sus actuaciones, tanto de carácter nacional como las derivadas de los compromisos internacionales de España.

DIRIGIDA POR:

Almirante Santiago Ramón
González Gómez

Centro de Sistemas y Tecnologías de la Información y las Comunicaciones

AÑO DE CREACIÓN: 2015

El Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) depende de la Secretaría de Estado de Defensa. Entre sus funciones están las de definir, planificar y coordinar las políticas de los sistemas de información, telecomunicaciones, transformación digital y seguridad de la información del departamento. El CESTIC proporciona los servicios de la infraestructura Integral de Información para la Defensa.

Asimismo, provee servicios a todos los usuarios del departamento: Órgano Central del Ministerio, Estado Mayor de la Defensa, Ejércitos y la Armada, Unidad Militar de Emergencias y unidades desplegadas en el exterior en operaciones. Cuenta con un área de Operaciones de Red y de Seguridad que funciona todos los días del año para asegurar el correcto funcionamiento y la provisión de servicios a todo el Ministerio de Defensa.

DIRIGDO POR:

General de División José
María Millán Martínez

Centro Criptológico Nacional

AÑO DE CREACIÓN: 2002

El Centro Criptológico Nacional (CCN) es un organismo dependiente del Centro Nacional de Inteligencia, responsable de garantizar la ciberseguridad en la Administración y de las múltiples entidades del sector público. Para ello, se encarga de verificar el cumplimiento del Esquema Nacional de Seguridad (ENS) y ejerce de centro de respuesta a incidentes de seguridad en este ámbito, a través del CCN-CERT.

Entre sus funciones está elaborar y difundir normas, instrucciones, guías y recomendaciones en la materia. También realiza una importante labor en el desarrollo y obtención de herramientas y es el Órgano de Certificación de productos y servicios de ciberseguridad en España.

www.ccn.cni.es

SUBDIRECTOR:

Luis Jiménez

Instituto Nacional de Ciberseguridad

AÑO DE CREACIÓN: 2005

Incibe es un organismo dependiente del Ministerio de Asuntos Económicos y Transformación Digital, cuya misión es el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y las empresas. Presta servicios de apoyo a las empresas para que desarrollen capacidades de ciberseguridad, proporciona formación a la sociedad, elabora guías y documentos sobre ciberseguridad y apoya a las empresas en el desarrollo de capacidades. Incibe tiene entre sus órganos dependientes la Oficina de Seguridad del Internauta (OSI) y el Incibe-CERT, para la respuesta a incidentes de ciberseguridad de empresas y ciudadanos. En colaboración con el CNPIC, este centro se hace cargo también de los incidentes relacionados con infraestructuras críticas.

www.incibe.es

DIRIGIDO POR:

Rosa Díaz Moles

Oficina de Coordinación de Ciberseguridad

AÑO DE CREACIÓN: 2014

La Oficina de Coordinación de Ciberseguridad tiene entre sus funciones servir de "punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros en relación con los ataques contra los sistemas de información". También ejerce de canal específico de comunicación entre los Centros de Respuesta a Incidentes Cibernéticos nacionales de referencia y la Secretaría de Estado de Seguridad (SES), y desempeña la coordinación técnica en materia de ciberseguridad entre dicha Secretaría de Estado y sus organismos dependientes.

Esta oficina estaba integrada, hasta el año pasado, en el CNPIC para la investigación y coordinación policial en los delitos relacionados con las tecnologías de la información. Actualmente depende de la Dirección de Coordinación y Estudios de la SES.

JEFE:

Comisario Guillermo Fernández

Centro Nacional de Protección de Infraestructuras Críticas

AÑO DE CREACIÓN: 2007

El Centro Nacional de Protección de Infraestructuras Crítica (CNPIC) es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas. Dependiente de la Secretaría de Estado de Seguridad, el CNPIC es la autoridad competente en materia de seguridad de las redes y sistemas de información de los operadores de servicios esenciales en el caso de que estos sean, además, designados como operadores críticos.

Junto con Incibe, el CNPIC se encarga de operar el Incibe-CERT para la gestión de los incidentes de ciberseguridad que afectan a operadores de infraestructuras críticas.

www.cnpic.es

DIRIGIDO POR:

Fernando Sánchez

Unidad Central de Ciberdelincuencia de la Policía Nacional

AÑO DE CREACIÓN: 1995

La Unidad Central de Ciberdelincuencia (UCC) está encargada de la investigación y persecución de las actividades delictivas que impliquen la utilización de las TIC. Persigue los ciberdelitos de ámbito nacional y transnacional que estén relacionados con el patrimonio, la protección al menor, los fraudes o la propiedad intelectual, entre otros. También actúa como Centro de Prevención y Respuesta E-Crime de la Policía Nacional.

De la UCC dependen tres brigadas: la Brigada Central de Investigación Tecnológica, frente actividades delictivas relacionadas con la protección de los menores, la intimidad y la propiedad intelectual e industrial; la Brigada Central de Seguridad Informática, para la investigación de las actividades delictivas que afecten a la seguridad lógica; y la Brigada de Fraude Informático, que investiga el fraude en la Red.

JEFE:

Comisario principal Agapito Hermes de Dios

Departamento de Delitos Telemáticos de la Guardia Civil

AÑO DE CREACIÓN: 1996

El origen de este departamento de la Guardia Civil es el Grupo de Delitos Telemáticos, creado en 1996 en el seno de la Unidad Central Operativa de la Guardia Civil. Desde hace un par de años, esta unidad ha incrementado su importancia, aumentando sus capacidades y ámbito de actuación. Actualmente, cuenta con dos grupos específicos que dependen del departamento: el Grupo de Investigación, que investiga delitos contra los sistemas, fraude y el abuso de menores; y el Grupo de Desarrollo e Innovación, que se ocupa de buscar herramientas y soluciones para mejorar la lucha contra las ciberamenazas. Cuenta además con equipos de investigación tecnológica (EDITE), presentes en todas las comunidades autónomas.

www.gdt.guardiacivil.es

JEFE:

Tte. coronel Juan A. Rodríguez Álvarez de Sotomayor

Unidad de Coordinación de Ciberseguridad

AÑO DE CREACIÓN: 2019

La Unidad de Coordinación de Ciberseguridad (UCCiber) está integrada en la Dirección General de la Guardia Civil. Su cometido es coordinar y optimizar el potencial disponible de la Benemérita para hacer frente a las amenazas procedentes de medios cibernéticos o transmitidas a través de ellos. Es, además, el punto de contacto y referencia en aspectos relacionados con la ciberseguridad, manteniéndose al margen de la labor investigadora, que compete a las unidades operativas especializadas de la Guardia Civil. Para ello, la UCCiber fija determinados procedimientos de armonización en la gestión de los recursos humanos, materiales y financieros relacionados con la ciberseguridad. Coordina las acciones a diferentes unidades de la Guardia Civil relacionadas con la ciberseguridad, ya sea directa o indirectamente.

JEFE:

Coronel Juan Salom

Unidad de Ciberseguridad de los Mossos d´Esquadra

AÑO DE CREACIÓN: 1997

La Unidad Central de Delitos Informáticos se enmarca actualmente en la División de Investigación Criminal y es el servicio de referencia de Mossos d'Esquadra en la lucha contra el cibercrimen.

Las principales responsabilidades que tiene asignadas esta unidad incluyen las investigaciones tecnológicas del ámbito de las personas (como el *grooming*, *sexting*, sextorsión, etc.), las investigaciones tecnológicas del ámbito del patrimonio, las investigaciones tecnológicas de delitos ciberdependientes, el soporte a las investigaciones tecnológicas de otras unidades de policía judicial, impartir formación en investigación tecnológica al resto de unidades de policía judicial y ejercer de interlocutores en el ámbito del cibercrimen con operadores tecnológicos externos.

JEFE:

Subinspector Albert Álvarez Fontanet

Sección Central de Delitos en Tecnologías de la Información de la Ertzaintza

AÑO DE CREACIÓN: 1998

La Sección Central de Delitos en Tecnologías de la Información, englobada en la Sección Central de Investigación Criminal y Policía Judicial de la Ertzaintza, se encarga de las indagaciones y de la lucha contra los ciberdelitos. Entre la actividad de esta sección destaca el descubrimiento e investigación de los delitos relacionados con las nuevas tecnologías e Internet y ofrece cobertura a las actuaciones de la Ertzaintza de este tipo.

Esta sección cuenta con un servicio de denuncias para que cualquier ciudadano que se considere víctima de un delito relacionado con las TIC pueda comunicarlo. Además, mantiene un contacto permanente con otros cuerpos de seguridad autonómicos, nacionales e internacionales y forma parte del Basque Ciber Security Centre.

www.ertzaintza.eus/lfr/web/ertzaintza/grupo-especializado

JEFE:

Oficial Manu Viota Maestre

Embajador en misión especial para las Amenazas Híbridas y la Ciberseguridad

AÑO DE CREACIÓN: 2014

La función del embajador especial para las Amenazas Híbridas y la Ciberseguridad es dar cobertura a los compromisos internacionales asumidos por España y hacer valer su posición en foros internacionales sobre la materia. Este representante, perteneciente a la estructura del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, forma parte de las negociaciones de los instrumentos multilaterales o acuerdos bilaterales sobre seguridad en el ciberespacio, especialmente en grupos pertenecientes a Naciones Unidas o la OTAN. En el ámbito nacional, representa al Ministerio de Exteriores en órganos como el Consejo Nacional de Ciberseguridad.

Aunque ahora el cargo es de embajador en misión especial para las amenazas Híbridas y la Ciberseguridad, este cometido se creó hace años con otras denominaciones.

EMBAJADOR:

Nicolás Pablo Pascual de la Parte

Red.es

AÑO DE CREACIÓN: 2002

Red.es es una entidad pública dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Su misión es impulsar la economía digital en España a través del fomento del uso de las TIC y facilitando la competitividad de las empresas. Este organismo desarrolla programas nacionales y europeos destinados a la innovación, el emprendimiento, la formación y el apoyo a pymes mediante el fomento eficiente de las tecnologías de la información y las comunicaciones. Asimismo, gestiona el Observatorio Sectorial de las telecomunicaciones y de la Sociedad de la Información (ONTSI). Trabajan en proyectos de ciberseguridad en colaboración con Incibe.

www.red.es

DIRIGIDA POR:

David Cierco

Agencia Española de Protección de Datos

AÑO DE CREACIÓN: 1994

La Agencia Española de Protección de Datos (AEPD) es la autoridad estatal encargada de velar por el cumplimiento de la normativa sobre protección de datos. Entre sus funciones principales se sitúa controlar la aplicación de las normas relacionadas con esta cuestión.

También se encarga de recibir y tramitar las reclamaciones relacionadas con la protección de datos, así como a aprobación de la designación de los delegados de protección de datos de las organizaciones. La AEPD es la autoridad de control española responsable de recibir y gestionar las notificaciones de incidentes de seguridad de los datos personales que puedan sufrir las empresas.

www.aepd.es

DIRIGIDA POR:

Mar España

Protegiendo las empresas en tiempos de ciberpandemia

La pandemia del COVID-19 ha supuesto para las organizaciones un reto en el que la tecnología ha sido fundamental, especialmente la seguridad de las redes y sistemas de la información. El teletrabajo ha sido el máximo exponente de una transformación laboral en el que los ciberdelincuentes, ávidos de extender sus tentáculos, se han mostrado más activos que nunca.

Preguntamos a varios expertos en ciberseguridad sobre el cambio que ha supuesto el coronavirus en este contexto desde el punto de vista de la ciberseguridad. En concreto, han respondido a la siguiente cuestión:

¿Hasta qué punto cambiará la pandemia el paradigma de la ciberseguridad corporativa en los próximos años y cuáles serán las prioridades del CISO en ese sentido?

"El CISO será clave para la sostenibilidad de su organización en la nueva normalidad"

Guillermo Llorente
Subdirector general de Seguridad y Medio Ambiente de Mapfre

El COVID-19 ha provocado que las empresas hayan ampliado significativamente las posibilidades de teletrabajo. Esto ha tenido importantes implicaciones en materia de ciberseguridad: dilución del perímetro tradicional; uso de *endpoints* sin medidas adecuadas de seguridad; reducción de la interacción personal y proliferación de las *fake news*; y especialización de los "malos" en atacar los sistemas de teletrabajo y los *endpoints* o en engañar a los empleados.

Ello, unido a la evolución del *malware* y a la facilidad de monetizar los ataques, ha ampliado la amenaza a cualquier tipo de empresa y sector. Esta situación ha venido para quedarse, y va a constituir la "nueva normalidad" en la que el CISO jugará un papel clave para la sostenibilidad de su organización. En este sentido, algunas de sus prioridades serán redefinir el perímetro de la compañía y la "identidad", así como garantizar un control de acceso robusto; securizar los *endpoints* y el control de los datos; aumentar las capacidades de monitorización y respuesta; plantear nuevos escenarios de recuperación ante ciberataques; incrementar la cultura de seguridad; y aumentar la colaboración, tanto público-privada como privada-privada.

"Los responsables de Ciberseguridad deberán priorizar la gestión de las identidades"

Antonio Fontiveros
Responsable de Ciberseguridad de Abertis Autopistas

La pandemia ha precipitado y acelerado dos procesos en muchas compañías: el despliegue de herramientas de conexión remota para facilitar el trabajo desde fuera de las oficinas y el traspaso de información desde sistemas *on-premises* a sistemas *cloud*.

En ambos casos queda obsoleto el paradigma de la fortaleza amurallada en la que se protegía a la información reforzando el perímetro. Nos movemos hacia un paradigma *Zero Trust*, en el que la seguridad se debe centrar en la protección del dato y de la identidad.

Los CISO y los responsables de Ciberseguridad deberán priorizar la gestión de las identidades, el principio de mínimo privilegio, la autenticación multifactor y los sistemas IRM (*Information Rights Management*). Sin dejar de lado los sistemas de seguridad tradicionales con los que deberemos seguir conviviendo.

Por otra parte, tendrán que acompañar y orientar a sus organizaciones para afrontar los retos del teletrabajo, que ha llegado con vocación de permanencia. Entre estos desafíos destacan la flexibilidad horaria, el despliegue de herramientas adecuadas y la desconexión digital.

"La importancia de la ciberseguridad ha aumentado durante este último año"

Jose Lóbez
Responsable de Ciberseguridad de El Corte Inglés

El negocio de la venta *online* de las grandes empresas va aumentando en detrimento de las tradicionales superficies comerciales físicas. Este cambio se ha precipitado de manera significativa durante la pandemia, lo que ha obligado a las compañías a realizar un esfuerzo para optimizar sus sistemas y continuar ofreciendo el servicio esperado.

Pero esta tendencia conlleva también una mayor superficie de exposición. Y esto acarrea un aumento de la ciberdelincuencia. Una situación que afecta a la ejecución de las ventas, las operaciones *online* y la reputación. Por tanto, ha sido necesario actualizar los métodos de defensa y protección existentes y reforzar la formación y concienciación de los usuarios.

La importancia de la ciberseguridad ha aumentado durante este último año, principalmente debido a la mayor madurez cibernética de las direcciones de las empresas y a la publicación de normativa nacional y europea. Esto va a conllevar un aumento en las funciones y responsabilidades del CISO, cuyas nuevas competencias vendrán acompañadas de la necesidad de aumentar los conocimientos en campos ajenos a los técnicos, como la protección de datos o la regulación digital, entre otros.

"La pandemia ha acelerado el derrumbe del concepto de perímetro"

Francisco Lázaro
CISO de Renfe Operadora

La pandemia ha acelerado el derrumbe del concepto de perímetro. No decimos nada nuevo cuando señalamos que en ciberseguridad el concepto de perímetro ya no existe. La superficie ha aumentado tanto que ya no tiene contorno. La confianza basada en el concepto primario de "dentro" frente a "fuera" se ha quedado obsoleta.

Los riesgos asociados a la tecnología y a la práctica de las actividades relacionadas directamente con el teletrabajo son viejos conocidos (aunque ahora hipervitaminados). La desconfianza frente a la confianza predeterminada articula la necesidad de creer e implantar el modelo de seguridad de *Zero Trust*. Pero la técnica sin el factor humano no es nada. Por eso también debemos potenciar la concienciación, formación y capacitación de nuestros empleados y, por supuesto, exigir estos mismos esfuerzos a la cadena de suministro. En este escenario es necesario un constante liderazgo de la alta dirección y una gestión por parte del CISO acorde a la necesidad.

Evaluar, asesorar, verificar, supervisar, registrar, investigar y comunicar son verbos que deberemos conjugar en todo momento, incluso en circunstancias difíciles.

WOMEN 4CYBER

EUROPEAN CYBER SECURITY ORGANISATION

SPAIN CHAPTER

¡Únete a nuestra comunidad!

Ayúdanos a impulsar y apoyar la participación de las mujeres en el ámbito de la ciberseguridad.

www.women4cyberspain.es

@Women4Cyber_SP Women4Cyber Spain Women4Cyber Spain

"La ciberseguridad corporativa siempre está en continuo cambio, evolución y urgencia"

Juan Cobo

CISO de Ferrovial

La ciberseguridad corporativa siempre está en continuo cambio, evolución y urgencia, fundamentalmente por la dependencia exponencial sobre todo lo digital, el protagonismo absoluto de la tecnología y el disparado crecimiento de la amenaza, que ha encontrado un filón al que sacar partido, bien de forma económica o con intereses más perversos.

En mi opinión, la pandemia solo ha acelerado esta dependencia de todo lo digital y el cambio inevitable hacia un modelo de trabajo, de relación y de vida mucho más virtual; lo que, obviamente, también ha intensificado la amenaza.

Dentro de este escenario cambiante y urgente en el que los CISO vivimos permanentemente, algunos de nuestros próximos retos de cara a gestionar correctamente los riesgos y amenazas pasarán por implementar un modelo realmente operativo de *Zero Trust*, el control obsesivo de la identidad, la evolución de nuestras capacidades de ciberinteligencia, el entrenamiento de la respuesta a incidentes, la preparación rigurosa de la recuperación, el entendimiento y el cumplimento del marco legal y la mejora de la cultura y la responsabilidad de nuestros empleados en relación con las ciberamenazas y la ciberseguridad.

"El fin de la pandemia abrirá un escenario que exigirá un refuerzo de la cadena de suministro"

Francisco Blázquez

Director de Seguridad Corporativa de Iberdrola para España y Portugal

La emergencia sanitaria ha obligado a todas las organizaciones a afrontar una serie de desafíos y a enfrentarse a situaciones inéditas que han impulsado cambios que serán duraderos y que han llegado para quedarse.

Como primer aspecto, ha puesto de manifiesto la necesidad de tener preparados los mecanismos precisos para afrontar situaciones excepcionales, contemplando tanto los servicios internos como los proporcionados por nuestros proveedores, con una disponibilidad no prevista ni siquiera imaginable.

Ha provocado también un incremento crítico de la utilización de diferentes soluciones tecnológicas, para las cuales hemos tenido que garantizar un nivel de ciberseguridad acorde.

Una vez que finalice la pandemia, las soluciones para el teletrabajo y las herramientas de colaboración habrán consolidado su papel fundamental en la empresa y habrán supuesto una nueva manera de hacer negocios. También se abrirá un escenario que exigirá una mayor flexibilidad y que requerirá un enfoque basado en riesgos en el que se ajuste nuestro concepto de perímetro de seguridad, en el que reforcemos la gestión del riesgo en nuestra relación con terceros y aseguremos la cadena de suministro.

"La estrategia de ciberseguridad debe ir asociada a la protección del dato"

Sergi Carmona

CISO de AGBAR para España y Latinoamérica

Pocas sociedades pueden operar hoy sin depender de la tecnología. La pandemia ha sido el mayor impulsor de la transformación digital que han podido vivir las empresas. No ha sido una decisión estratégica defendida por el CIO, el CISO o el propio CEO, sino que, para poder seguir prestando un servicio de calidad, no ha quedado otra opción que transformar o adaptar el negocio al nuevo paradigma. Se han puesto a prueba los planes de continuidad de negocio y resiliencia, así como las medidas de ciberseguridad implementadas, y esto ha traído consigo nuevos riesgos y amenazas a tener en cuenta.

En cuanto al paradigma de la ciberseguridad, el modelo de protección ha cambiado. El dato ahora puede estar en cualquier ubicación. La estrategia de ciberseguridad debe ir asociada a la protección del dato y a asegurar que la identidad de aquel que accede a la información es quien dice ser, ofreciendo así controles muy robustos frente a intentos de acceso indebidos.

Por último, los proveedores y la cadena de suministro han tomado cada vez mayor relevancia hasta convertirse en piezas clave y *partners* de confianza, lo que nos ha permitido seguir desarrollando nuestro negocio con total normalidad.

"La prioridad de los CISO es la de siempre: trabajar para asegurar todo lo que conocemos"

Rafael Hernández

CISO de Cepsa

El global de la sociedad ya había empezado a tratar la transformación digital como una forma de mejorar nuestras vidas, y esta pandemia ha acelerado este proceso de forma vertiginosa.

La ciberseguridad no es ajena a este cambio de situación. Las conexiones remotas y el aumento de los servicios que ciudadanos, empleados y consumidores tenemos cada vez más en Internet nos llevan a tener un aumento exponencial de los riesgos que debemos analizar y gestionar.

Creo que esta situación no va a revolverse. Es más, irá en aumento. Por lo tanto, nos hemos de preparar para seguir trabajando en asegurar todos nuestros servicios y sistemas.

En este sentido, la prioridad de los CISO es la de siempre: trabajar para asegurar todo lo que conocemos. Tendremos que centrarnos en gestionar las identidades de nuestros usuarios, la identidad digital global. Habremos de mejorar los servicios de detección y respuesta: nuestros SOC deberán ser cada vez más ágiles y rápidos en sus servicios. Los servicios de CSIRT serán la estrella de estos próximos años; tendremos que recuperar los servicios de forma inmediata.

"Pensando en los clientes, el objetivo es minimizar el impacto por fraude"

Gustavo Lozano

CISO de ING

La gestión de la crisis ha supuesto un gran reto para todas las empresas. En nuestro caso, contar con una base tecnológica sólida nos ayudó a adaptarnos rápidamente al nuevo contexto y a dar una respuesta ágil a las nuevas necesidades. En esas primeras fases de pandemia, en un entorno totalmente desconocido para todos, fueron clave la anticipación, la colaboración y la compartición de información con otros países del grupo.

La pandemia sí ha reforzado algunos aspectos que quizás no eran prioridad para todos los sectores hasta el momento. Pensando en los clientes, el foco está en reforzar las medidas tecnológicas y los procesos para luchar frente al *phishing*, *smishing*, *vishing*, etc., con el objetivo de minimizar el impacto por fraude.

En cuanto a la infraestructura, la continuidad de negocio ha cobrado más valor tanto para proteger las redes y sistemas de información ante ataques de denegación de servicio distribuido como para asegurar el acceso remoto del empleado y el *endpoint* ante nuevos riesgos.

Por último, y no menos importante, el cumplimiento de la legislación vigente es una absoluta prioridad para ING.

"El reto planteado ahora es lograr que todos los procesos sean seguros de forma remota"

Javier Tobal

CISO de Fintonic, Servicios Financieros

La pandemia ha demostrado, entre otros muchos temas, que el trabajo remoto debe ser la primera opción en el futuro siempre que sea posible. Es cierto que muchas compañías ya teníamos las herramientas para garantizar que el teletrabajo fuera tan seguro como el presencial. Incluso en nuestro caso, los procedimientos, herramientas y controles de seguridad estaban diseñados por principio en el trabajo remoto (siguiendo la máxima "lo que es seguro para trabajar de forma remota en un entorno no controlado es, con más motivo, también seguro para trabajar desde las instalaciones de la compañía").

El reto planteado ahora es lograr que todos los procesos sin excepción sean seguros de forma remota: desde la provisión de identidades, credenciales y dispositivos de seguridad hasta la autorización de servicios de forma dinámica.

Con estas premisas tenemos que priorizar las herramientas y procesos que nos permitan el gobierno de las identidades; la gestión dinámica de accesos a plataformas *cloud*; la autorización, registro y certificación de operaciones remotas; y, por encima de todo, la monitorización efectiva que asegure el cumplimiento de las políticas de la compañía en todos los entornos.

"Es imprescindible que los empleados conozcan los riesgos a los que se enfrentan a diario"

Enrique Rubio-Manzanares
Director de la Unidad de Seguridad y Riesgos TI de Banca March

Una parte de la estrategia de la ciberseguridad en los próximos años va a continuar siendo ampliar el perímetro de las organizaciones. Es decir, ya era habitual el trabajo con equipos y movilidad, pero ahora también se está operando mucho más con equipos personales o no corporativos. Esto hace necesario tener unas buenas políticas y estrategias de conexiones remotas para dar respuesta a la demanda de los empleados y de las compañías, que es básicamente la conectividad desde cualquier dispositivo y lugar de manera segura.

Por otro lado, será muy importante disponer de una buena clasificación de la información para aplicar políticas y herramientas para controlar qué información ha salido de nuestra organización y qué acciones podemos realizar con dichos datos.

Por último, y para mí primordial, la concienciación debe ser otro aspecto a tener muy en cuenta: con estos nuevos entornos es imprescindible que todos los empleados conozcan los riesgos a los que se enfrentan a diario y que las organizaciones ofrezcan las herramientas y cauces necesarios para gestionarlos. Eso se consigue con proyectos de concienciación de larga duración que generen una cultura interna que normalice los riesgos tecnológicos.

"Hay un diluvio de ataques de 'ransomware': ya no hay víctimas insignificantes"

Julio Sánchez
Jefe del Departamento de Seguridad de la Información de la Sociedad Estatal Loterías y Apuestas del Estado

El mundo ha cambiado. Es cierto que, si la pandemia llega a estar bajo control, podremos retomar en gran parte nuestra forma de trabajo. Pero la caja de Pandora está abierta. Lo que quedaba de perímetro ha volado por los aires. Los viajes y las reuniones cara a cara perderán importancia. El uso de los canales telemáticos será mayor. Y, con ello, la posibilidad de incidentes.

Hay un diluvio de ataques de *ransomware*: ya no hay víctimas insignificantes. Factores como el uso de mecanismos de autenticación con debilidades más o menos fáciles de explotar, protecciones insuficientes de los puestos de trabajo remotos, carencias en la monitorización de estos y en la aplicación de parches y actualizaciones, mayor uso de equipos no corporativos en los que estos problemas se exacerban y el distanciamiento entre los empleados, entre otros elementos, propician un escenario sombrío.

Pero, en realidad, nada de esto es nuevo; cada una de estas cosas ya era un área de preocupación. Aunque es un cambio de escala. La adaptación a este nuevo escenario va a requerir atención y recursos. Afortunadamente, el nivel de sensibilización a nivel directivo está en máximos.

"Teletrabajar crea un falso entorno seguro, por lo que es clave incidir en la concienciación"

Félix Rodríguez

Director de Seguridad en Triodos Bank NV SE

La crisis de la COVID-19 ha traído un giro radical en el escenario de la ciberseguridad, y creo que ha calado en la alta dirección, incorporando la seguridad en el negocio corporativo. El crecimiento exponencial del teletrabajo, apenas contemplado antes de la pandemia, nos está llevando a situar la protección de la persona (el eslabón más débil en la cadena de la seguridad) y el dato en el centro de nuestra estrategia de seguridad, cuando hace unos meses el epicentro era la red corporativa.

El puesto de trabajo se ha diversificado en distintas redes y dispositivos y se han incrementado los tipos de acceso. Todo esto hace necesario, por un lado, establecer un nuevo perímetro de seguridad; y por otro, aplicar políticas de "confianza cero" en el usuario y fortalecer la gestión de accesos e identidades.

Ahora, el usuario está más expuesto al ciberataque. Trabajar desde casa crea un falso "entorno seguro", por lo que es clave incidir más en la concienciación y la formación.

Para mí estas son nuestras prioridades como responsables de Seguridad, sin olvidar la revisión y cambios en los procesos, la adecuación de políticas, el despliegue de nuevas tecnologías, etc. En definitiva, adaptarnos al acelerón de la transformación digital.

"La pandemia no es el motivo del cambio de paradigma de la ciberseguridad"

Eva Cristina Cañete

Directora de Ciberseguridad (CISO) de Unicaja Banco

La situación generada por la pandemia del COVID-19 no es realmente el motivo del cambio de paradigma de la ciberseguridad. Sin embargo, sí ha conllevado agilizar el cambio que ya se estaba produciendo. De hecho, se ha acelerado el proceso que desdibuja las fronteras de protección, y ante esto, la ciberseguridad debe adaptarse con más rapidez.

En sí misma, esta última ya es un gran reto, y en los próximos años no será menos. Tendremos que ser más ágiles y flexibles potenciando, para ello, la ciberseguridad.

En el caso de las entidades financieras, son muchos los retos a los que se enfrenta el sector al implantar una estrategia de seguridad adecuada: asumir el impacto en costes para la disponibilidad de los recursos necesarios o la adaptación a un contexto de aumento de regulaciones en las que se recogen apartados específicos sobre seguridad. Y también operar sin problemas en un ciberespacio más inseguro debido al crecimiento tan exponencial de los servicios ofrecidos por Internet y ante unas nuevas generaciones de potenciales clientes eminentemente tecnológicos.

"Ahora debemos adecuar la postura de riesgo de nuestras compañías"

Iván Sánchez

CISO de Sanitas

La adaptación de los equipos de ciberseguridad al entorno de trabajo en pandemia se vio acelerada por la necesidad de los primeros meses. En ese momento se llevó a cabo un enorme esfuerzo para asegurar una transición hacia la "movilidad segura"; y ahora, pasado un año, tenemos que echar la vista atrás y sacar lecciones de lo que hicimos. Pero, sobre todo, debemos mirar hacia delante y redefinir nuestra estrategia en base al análisis del impacto del escenario actual, así como adecuar la postura de riesgo de nuestras compañías.

En ese sentido, las prioridades se orientan hacia áreas como securización del dispositivo remoto y evolución de las herramientas con un enfoque de *Zero Trust* en un entorno donde no siempre es un requisito trabajar conectado a la red corporativa; agilidad en la respuesta a incidentes para seguir siendo capaces de gestionar la respuesta en un escenario de movilidad; gestión de la identidad con un enfoque de seguridad basada en comportamiento; gobierno, control y securización de cargas de trabajo en la nube; y eficientar el modelo de costes de ciberseguridad, porque en este entorno, el modelo tradicional de compra de tecnología se convierte en un modelo de pago por uso.

"El plan de continuidad de negocio es fundamental para sobrevivir"

Roberto Valencia

CISO de Rural Servicios Informáticos (RSI)

Con la pandemia, las empresas se enfrentaron a grandes cambios en muy poco tiempo. Incluso aquellas que tenían un plan de continuidad de negocio (PCN) definido y probado se encontraron con un escenario desconocido. Esto ha provocado que las corporaciones se hayan volcado en sus PCN para poder dar una respuesta rápida a situaciones de riesgo como la que vivimos. Creo que este es el mayor cambio de paradigma: nuestro PCN es fundamental para sobrevivir y el concepto de resiliencia se ha visto potenciado.

Otro gran cambio ha sido que la pandemia ha acelerado de forma brutal algo que ya estábamos viviendo: la transformación digital. El teletrabajo y la nueva forma de relación con clientes y entre empresas se han implantado de forma inmediata, en muchos casos aumentando el riesgo de forma exponencial. Todo ello, acompañado de un entorno normativo cada vez más exigente.

Una de las prioridades del CISO es manejar todos estos componentes, PCN, transformación digital y normativa, dentro de un entorno de crisis que limita las inversiones presupuestarias de todo tipo.

"La pandemia constata que los riesgos de baja probabilidad y alto impacto ocurren"

Antonio Simón Martínez
Coordinador de Seguridad Informática y Ciberseguridad de Metro de Madrid

La pandemia ha supuesto un revulsivo y una oportunidad a partes iguales, así como la constatación de que los riesgos de baja probabilidad y alto impacto ocurren. Esto mismo supone que el paradigma que pudiésemos tener en el ámbito de la ciberseguridad, y que ha venido evolucionando, se ha visto significativamente alterado en aspectos como el análisis de riesgos. Se ha mostrado así la necesidad de un enfoque más dinámico, con más variables y que posibilite anticipar los eventos, afrontar las crisis y tomar decisiones rápidamente.

En cuanto a los entornos de trabajo, la consecuencia más notoria ha sido el cambio de los límites físicos de la empresa (con la llegada del teletrabajo) y, por ello, la ampliación de la superficie de ataque y de los vectores de riesgo. También destaca el incremento exponencial de las prácticas ilícitas contra las empresas.

¿Y cuáles deben ser las prioridades del CISO?: realizar análisis de riesgos dinámicos y constantes alineados con los objetivos del negocio, asegurar los recursos económicos para adoptar las medidas, reforzar la concienciación y formación de los empleados, apostar por el talento en sus equipos y reforzar la gestión de crisis.

"El nivel de seguridad ha de ser independiente del lugar de trabajo"

Luis Ballesteros
CISO de WiZink

Una de las consecuencias de la pandemia es la consolidación del teletrabajo, que ha llegado para quedarse. Ha pasado de tener un uso puntual a formar parte de los procesos críticos de la compañía en el día a día.

Seguimos profundizando en un modelo en el que los datos están en múltiples lugares (distintos *data centers*, proveedores, nubes...), y a los que se accede desde diferentes sitios y dispositivos. En los próximos años veremos más cambios en este sentido que incrementarán todavía más la eficiencia de los trabajadores y de los sistemas de información.

Los CISO tenemos que trabajar para facilitar estos cambios manteniendo el nivel de seguridad requerido.

Respecto al trabajo en remoto, algunos puntos relevantes que se han revisado son: medidas técnicas (el nivel de seguridad debe ser independiente del lugar de trabajo), formación y concienciación (el usuario sigue siendo el eslabón más débil), proveedores (se delega el proceso, pero no la responsabilidad) y planes de continuidad de negocio (el trabajo en remoto ha pasado de ser una estrategia de continuidad de negocio a ser una parte fundamental de la actividad cotidiana).

"La seguridad de la información se verá reforzada a nivel presupuestario"

Miguel J. Vázquez
Director del Departamento de Tecnologías de la Información de Adolfo Domínguez

La pandemia del COVID-19 ha acelerado el proceso de transformación digital de todas las compañías, creciendo en gran medida la superficie de exposición, riesgo y número de ciberataques. En este nuevo contexto, donde las tecnologías y la seguridad de la información han puesto de manifiesto su criticidad para la continuidad del negocio, estas se verán reforzadas a nivel presupuestario como consecuencia de la concienciación manifiesta en los órganos de dirección. Además, se producirán avances en materia de normativa o regulación, así como en políticas, procedimientos y arquitecturas que permitan una operación más segura dentro de las organizaciones.

También cobrarán especial importancia no solo los planes de continuidad de negocio y recuperación ante desastres, sino los procedimientos de respuesta ante incidentes de seguridad que permitan una gestión ágil y eficiente de los mismos en el momento en que se produzcan.

El CISO se focalizará en la gestión de los riesgos derivados del teletrabajo, en la gestión de las vulnerabilidades, en la detección y respuesta extendidas, en la gestión de la identidad digital y en la seguridad en la nube como prioridades.

"La pandemia ha cambiado el paradigma de la ciberseguridad de arriba abajo"

Manuel Buitrago del Burgo
Responsable de Seguridad de la Información de Fertiberia

La pandemia del COVID-19 ha cambiado el paradigma de la ciberseguridad de arriba abajo. Se han desarrollado numerosos elementos esenciales, como el trabajo en remoto, pero también ha servido para tener un concepto muy claro sobre los riesgos cibernéticos que abundan en las redes.

Como consecuencia de todo ello, la principal prioridad del responsable de Seguridad de la Información se concretará en el desarrollo de políticas de seguridad de la información entendibles, así como en difundirlas y aplicarlas en toda su amplitud.

> "El COVID-19 ha servido para tener un concepto muy claro sobre los riesgos cibernéticos que abundan en las redes"

Contención de las ciberamenazas

El Plan de Recuperación, Transformación y Resiliencia de la Economía Española destinará una dotación presupuestaria cercana a los 260 millones de euros en 2021 a fortalecer e impulsar nuestro ecosistema de ciberseguridad. Esta situación impactará de lleno no solamente en las empresas de este sector, muchas de las cuales ya cuentan con centros de operaciones de ciberseguridad (SOC) y equipos de respuesta ante incidentes informáticos (CSIRT), sino también en aquellas administraciones públicas que deseen contar con alguno de estos equipos para gestionar los ciberincidentes. Por lo tanto, previsiblemente, las comunidades autónomas y determinadas organizaciones públicas y privadas que no dispongan de estos centros o equipos desearán hacerse con ellos. Un hipotético crecimiento de la demanda que el sector deberá hacer frente con garantías.

No obstante, los SOC y CSIRT más importantes actualmente a nivel estatal, autonómico, europeo y corporativo son los destacados a continuación.

SOC de la AGE

Este centro de operaciones de ciberseguridad (COCS) persigue la protección de la seguridad perimetral de la Administración General del Estado (AGE) y de sus organismos públicos frente a amenazas externas.

Entre sus servicios se encuentran la alerta temprana de amenazas, la detección, respuesta coordinada y soporte a la resolución de incidentes de seguridad, así como la investigación de ciberataques y ciberamenazas. Además, desempeña la operación, monitorización y actualización de dispositivos de defensa perimetrales, un análisis de vulnerabilidades de aplicaciones y servicios y un servicio antiabuso de identidad digital.

Igualmente, como extensión de este centro se ha implementado el SOC de la Subdirección General de Nuevas Tecnologías de la Justicia del Ministerio de Justicia.

ADMINISTRACIÓN GENERAL DEL ESTADO

- **Año de creación**
  2019
- **Web**
  administracion.gob.es
- **Contacto**
  soc.age@correo.gob.es

CCN-CERT

Es el Centro de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN). Su misión es contribuir a la mejora de la ciberseguridad española. Ayuda a responder de forma rápida y eficiente los ciberataques y a afrontar de forma activa las ciberamenazas. Dispone de un sistema de alerta temprana que busca actuar antes de que se produzca un incidente o detectarlo en un primer momento para reducir su impacto y alcance.

Además, publica periódicamente informes, guías y buenas prácticas sobre el mundo de la ciberseguridad, todas ellas de acceso público. También ofrece distintos cursos formativos para mejorar las competencias de los profesionales del sector. Por otro lado, desarrolla soluciones tecnológicas que garantizan la seguridad de los sistemas y contribuyen a una mejor gestión de la ciberseguridad.

ccn-cert

- **Año de creación**
  2006
- **Web**
  www.ccn-cert.cni.es
- **Contacto**
  info@ccn-cert.cni.es

Incibe-CERT

Es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y las empresas, así como para las infraestructuras críticas. Está operado por el Instituto Nacional de Ciberseguridad (Incibe), aunque cuando se trata de proteger infraestructuras críticas lo hace conjuntamente con el Centro Nacional de Protección de Infraestructuras Críticas.

Ofrece respuesta a incidentes 24x7x365, apoyo a crisis cibernéticas, monitorización de activos, detección de incidentes, alerta temprana e intercambio de amenazas. Asimismo, proporciona información y contenidos especializados, celebra ciberejercicios para entrenar y evaluar de forma práctica la capacidad de respuesta de una entidad ante un incidente de ciberseguridad, publica informes de ciberseguridad y mide y mejora la ciberresiliencia, entre otras funciones.

incibe-cert_

- **Año de creación**
  2007
- **Web**
  www.incibe-cert.es
- **Contacto**
  incidencias@incibe-cert.es

CERT del Mando Conjunto del Ciberespacio

Es el centro de respuesta a incidentes del Ministerio de Defensa, conocido por las siglas ESP-DEF-CERT. Su ámbito de actuación son las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la defensa nacional.

Para ello, este órgano cuenta con capacidades de detección de incidentes y de alerta temprana. Elabora periódicamente documentación propia para establecer procedimientos de actuación ante diferentes incidentes de seguridad.

También desarrolla herramientas de ciberseguridad y programas específicos para realizar su labor, así como cursos, seminarios y otras actividades formativas en colaboración con otros centros de respuesta ante incidentes.

- **Año de creación**
  2013
- **Web**
  emad.defensa.gob.es
- **Contacto**
  esp-def-cert@mde.es

AndalucíaCERT

Entre los principales objetivos de AndalucíaCERT se encuentran proporcionar la capacidad de detección y respuesta eficaz y coordinada ante incidentes de ciberseguridad a su grupo atendido (constituido por los organismos y entidades de la Administración de la Junta de Andalucía) y potenciar la formación, concienciación y sensibilización en seguridad.

Los servicios que ofrece son alerta temprana de ciberamenazas (difusión de amenazas que puedan afectar gravemente a los sistemas informáticos), detección y respuesta a incidentes (detección automatizada a través de la plataforma SIEM y recepción de notificaciones, análisis experto y asesoramiento en la respuesta a incidentes de seguridad) e información, formación y concienciación (elaboración de boletines e impartición de cursos y ponencias).

- **Año de creación**
  2011
- **Web**
  www.andaluciacert.es
- **Contacto**
  consultas.cert@juntadeandalucia.es

Basque CyberSecurity Centre CSIRT

Entre los servicios que ofrece se encuentran la gestión de incidentes de ciberseguridad y vulnerabilidades, el análisis de *malware*, la publicación de avisos y alertas, la formación y la concienciación. Además, este organismo lleva a cabo otro tipo de servicios de valor añadido, como son la monitorización de las redes públicas vascas, la promoción de ayudas, la coordinación de iniciativas relacionadas con la investigación, el desarrollo y la innovación, el apoyo al emprendimiento en materia de ciberseguridad y la ayuda e identificación de talento ante la vocación de seguridad de la información.

Y es que, en términos generales, la misión del Basque CyberSecurity Centre es desarrollar una cultura de ciberseguridad entre la sociedad vasca, dinamizar la actividad económica relacionada con la ciberseguridad y fortalecer el sector.

- **Año de creación**
  2017
- **Web**
  www.basquecybersecurity.eus
- **Contacto**
  info@bcsc.eus

Catalonia-CERT

Los servicios que ofrece el CSIRT de la Agencia de Ciberseguridad de Cataluña se agrupan en tres categorías. La primera son los reactivos, destinados a responder a una amenaza o un incidente de seguridad sufrido por un sistema de información y a minimizar su impacto.

La segunda son los proactivos, cuya función es reducir los riesgos de seguridad de la comunidad mediante la distribución de información e implantación de sistemas de protección y detección. Estos servicios están diseñados para mejorar los procesos de infraestructura y seguridad antes de que se produzca un incidente o de que sea detectado.

Y la última son los de gestión y coordinación, mediante los que se pretende mejorar los procesos de trabajo gracias a la educación, sensibilización y formación.

Año de creación
2009

Web
ciberseguretat.gencat.cat

Contacto
cert@cesicat.cat

CSIRT CARM

Los servicios que presta el CSIRT de la Comunidad Autónoma de la Región de Murcia (CARM) se pueden agrupar en: gestión de incidencias de seguridad (detección, resolución y análisis forense de incidencias de seguridad), detección de amenazas e incidencias de seguridad (monitorización, colección y correlación de eventos y *logs* de dispositivos y sistemas de información), configuraciones de seguridad, gestión de la seguridad, alerta temprana (compilación, publicación y envío de alertas, noticias, vulnerabilidades, amenazas, incidencias, guías e informes), validación de seguridad, revisiones técnicas de seguridad (uso de herramientas de seguridad y/o revisión de configuraciones y *logs* para detectar vulnerabilidades y auditar el estado de seguridad), gestión de vulnerabilidades y amenazas, gestión de certificados y asesoría en seguridad de la información.

Año de creación
2010

Web
www.carm.es

Contacto
csirt@listas.carm.es

CSIRT-CV

El principal objetivo del CSIRT de la Comunidad Valenciana es contribuir a mejorar la seguridad de los sistemas de información, así como promover una cultura de seguridad y buenas prácticas en el uso de las nuevas tecnologías. Todo ello, para que se minimicen los incidentes de seguridad y se puedan afrontar de forma activa las nuevas amenazas que pudieran surgir.

El centro consigue todo esto a través de la realización de tres tipos de servicios. Los primeros son los reactivos, que incluyen la gestión y monitorización de alertas, el análisis y respuesta a incidentes y la detección de intrusiones. Los segundos son los preventivos, que proporcionan asistencia e información para ayudar a preparar, proteger y asegurar los sistema. Y los terceros son los de valor añadido, que contribuyen a reducir la cantidad de incidentes.

Año de creación
2007

Web
www.csirtcv.gva.es

Contacto
csirtcv@gva.es

CSIRT.gal

Pretende mitigar el impacto de los incidentes de seguridad en los sistemas de información de la Xunta de Galicia, administrados por la Agencia para la Modernización Tecnológica de dicha comunidad. Su objetivo principal es mejorar la seguridad y la calidad de los servicios públicos prestados a través de los sistemas de información de la mencionada Xunta. Proporciona una capacidad efectiva y coordinada de detección y respuesta ante incidentes de ciberseguridad.

Los servicios que realiza van desde la monitorización continua de los sistemas de información y el tratamiento y análisis de incidentes de seguridad y vulnerabilidades, hasta la difusión de información relacionada con la seguridad, amenazas emergentes y otras actividades maliciosas. Además, desarrolla auditorías y ejercicios de sensibilización, comunicación y formación en ciberseguridad.

- **Año de creación**
  2018
- **Web**
  amtega.xunta.gal
- **Contacto**
  csirtgal@xunta.gal

IRIS-CERT

Se trata del servicio de seguridad de RedIRIS, la red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional. Su finalidad es la detección de problemas que afecten a la seguridad de las redes de estos centros, así como la actuación coordinada con dichas instituciones para poner solución a estos problemas. También realiza una labor preventiva. Para ello avisa con tiempo de problemas potenciales, ofrece asesoramiento a sus afiliados, organiza actividades de acuerdo con ellos y brinda servicios complementarios.

También ofrece soporte de coordinación de incidentes a centros ajenos a la red. Particularmente, actúa como último punto de contacto para los incidentes graves que puedan afectar al dominio ".es".

- **Año de creación**
  1995
- **Web**
  www.rediris.es
- **Contacto**
  seguridad@rediris.es

OSSI-CERT SERMAS

Es el Centro de Respuesta a Incidentes de la Oficina de Seguridad de Sistemas de Información del Servicio Madrileño de Salud. El objetivo de este órgano es impulsar y dar soporte a la implantación de las medidas de seguridad por parte de dichos centros.

Este CERT realiza una labor preventiva. Avisa con tiempo de problemas potenciales, ofrece asesoramiento y auditoría a los centros sanitarios y organiza actividades para fomentar la ciberseguridad. Entre sus funciones también se encuentra la monitorización constante de eventos de seguridad; el análisis de *software, hardware, malware* y análisis forense de incidentes; y la realización de informes periódicos. Y también realiza una labor de comunicación y formación a personal de estos centros en materia de seguridad de la información.

- **Año de creación**
  2006
- **Web**
  www.madrid.org
- **Contacto**
  oficina.seguridad@salud.madrid.org

CERT-EU

El equipo de respuesta ante emergencias informáticas para las instituciones, órganos y agencias de la Unión Europea (CERT-EU) está compuesto por expertos en seguridad informática de las principales instituciones de este territorio.

El CERT-UE coopera con otros CERT de los Estados miembros y con empresas especializadas en seguridad informática para responder a incidentes de seguridad de la información y a ciberriesgos.

Su cometido es contribuir a la gestión de las amenazas a los sistemas informáticos de los estamentos europeos. Para ello apoya a los equipos de seguridad informática de cada institución de la Unión Europea y se mantiene en permanente contacto con las entidades correspondientes del sector público de los países miembros.

- **Año de creación**
  2012
- **Web**
  cert.europa.eu
- **Contacto**
  services@cert.europa.eu

European Commission DIGIT CSIRC

El Computer Security Incident Response Capability (CSIRC) de la Comisión Europea publica multitud de documentos y normativas en lo referido a incidentes de seguridad de la información. Entre los más recientes se encuentran los relacionados con el papel del gobierno digital en Europa durante 2020, la evaluación final del programa de soluciones de interoperabilidad y marcos comunes para administraciones públicas, empresas y ciudadanos europeos (programa ISA²), la evaluación de la implementación del Marco Europeo de Interoperabilidad y la propuesta de una estrategia de interoperabilidad de los gobiernos de la Unión Europea.

Asimismo, divulga diversos boletines informativos y *newsletters* sobre estas temáticas.

- **Año de creación**
  2014
- **Web**
  ec.europa.eu
- **Contacto**
  ec-digit-csirc@ec.europa.eu

CSIRT-ECB

El Equipo de Respuesta ante Emergencias Informáticas del Banco Central Europeo (ECB) trabaja en estrecha colaboración con todos los bancos centrales nacionales de la Unión Europea para garantizar la confidencialidad, disponibilidad e integridad de los datos. También coopera con otras instituciones europeas, como el Parlamento, el Consejo y la Comisión Europea. Esto ayuda a proteger tanto al Banco como al Eurosistema en su conjunto contra los ciberataques, a limitar las consecuencias en caso de una violación de datos y a garantizar que la institución pueda seguir operando en todo momento.

El CERT-EU advierte a sus miembros sobre nuevas amenazas, realiza pruebas y ofrece servicios de asesoramiento. Y también apoya a sus miembros a la hora de responder a ciberataques.

- **Año de creación**
  2013
- **Web**
  www.ecb.europa.eu
- **Contacto**
  csirt@ecb.europa.eu

Accenture CSIRT Iberia

El Accenture CSIRT Iberia defiende a las organizaciones de los ataques de manera proactiva y con métodos inteligentes específicos para cada tipo de sector. De esta manera, ayuda a sus clientes a lograr una postura de defensa cibernética resistente para continuar operando sus negocios independientemente de las amenazas cibernéticas a las que se enfrentan.

Este centro combina servicios gestionados de seguridad, analítica avanzada y automatización inteligente para ayudar a las organizaciones a ser más innovadoras que los ciberdelincuentes.

Gracias a los servicios de Accenture, los clientes pueden escalar rápidamente las operaciones de seguridad y de cumplimiento a través de tecnología innovadora, capacidades y servicios de ciberseguridad.

Año de creación
2016

Web
www.accenture.com

Contacto
csirt.spain@accenture.com

ERIS-CERT

Sothis reforzó en 2020 este centro de Valencia con un nuevo emplazamiento e importantes mejoras. Desde él se vigilan y monitorizan incidentes relacionados con ciberataques. Alrededor de este centro neurálgico, Sothis ha desarrollado un portafolio de soluciones de ciberprotección, cibervigilancia y ciberrespuesta con capacidades tanto de seguridad analítica como de seguridad operativa que se adaptan a las necesidades de seguridad de cada cliente.

El SOC cuenta con perfiles específicos para los distintos verticales de conocimiento de seguridad, infraestructuras, SAP, IT y OT. Además de certificaciones en otras tecnologías de fabricantes que complementan la amplia gama de servicios prestados, desde auditoría, detección y protección de entornos SAP y entornos industriales hasta el Servicio Global de Seguridad Gestionada.

Año de creación
2017

Web
www.eriscert.es

Contacto
security@sothis.tech

SOC de S21sec

El SOC de S21sec, que cuenta con 500 metros cuadrados y con más de 50 trabajadores, monitoriza en tiempo real toda la actividad y los incidentes de ciberseguridad. Esta compañía ofrece servicios de monitoreo y administración de dispositivos para detectar y responder rápidamente las ciberamenazas y minimizar así su impacto.

El centro de ciberseguridad dispone de Servicios de Seguridad Gestionada modulares que se adaptan al nivel de madurez de cada tipo de organización y que le permiten, mediante una dedicación adecuada de los recursos internos, mitigar de la manera más efectiva posible todos sus riesgos tecnológicos dentro del marco de actuación NIST (Instituto Nacional de Estándares y Tecnología de Estados Unidos).

Año de creación
2000

Web
www.s21sec.com

Contacto
cert@s21sec.com

OTROS CENTROS DE RESPUESTAS PRIVADOS	ORGANIZACIÓN
Aiuken CERT	Aiuken Solutions
Auren CERT	Auren
Banco Sabadell CERT	Banco Sabadell
BBVA CERT	BBVA
CaixaBank CSIRT	CaixaBank
CERT Oesía	Grupo Oesía
CERT UC3M	Universidad Carlos III de Madrid
CSA Global CSIRT	Centro Regional de Servicios Avanzados
CSIRT Global Telefónica	Telefónica
CSUC-CSIRT	Consorcio de servicios Universitarios de Cataluña
CyberSOC de Deloitte	Deloitte
Entelgy Innotec Security CSIRT	Entelgy Innotec Security
esCERT-UPC	Universitat Politècnica de Catalunya
eSOC Ingenia	Ingeniería e Integración Avanzadas, Ingenia
Eulen-CCSI-CERT	Eulen Seguridad
everis CERT	everis
Global CSIRT	Centro Regional de Servicios Avanzados
GMV CERT	GMV
Iberdrola Cyber-Security Incident Response Team	Iberdrola
IECISA CERT	El Corte Inglés
Inditex CSIRT	Inditex
ISA SYS CiberSOC	ICA Sistemas y Seguridad
ITS-CERT	ITS Security (Integrated Technology Systems)
LE CERT	Light Eyes
Mapfre-CCG-CERT	Mapfre
MINSAIT CSIRT	Indra Soluciones TI
Mnemo CERT	Mnemo
NestleSOC	Nestlé
Nunsys-CERT	Nunsys
Prosegur CERT	Prosegur
Renfe CERT	Renfe Operadora
Repsol CERT	Repsol
S2 Grupo CERT	S2 Grupo
Santander Global CERT	Santander
Secure&IT CERT	Secure&IT
SIA-CEC CERT	Sistemas Informáticos Abiertos
UAM CERT	Universidad Autónoma de Madrid

SÚMATE A NUESTRO
NUEVO ECOSISTEMA DIGITAL

red seguridad

Mapa de empresas de ciberseguridad

Según los últimos datos de Incibe, España cuenta con una industria de la ciberseguridad formada por más de 1.600 compañías, cuya facturación ronda los 1.300 millones de euros anuales. No obstante, el buen momento en el que se encuentra el sector y la llegada del Plan de Recuperación, Transformación y Resiliencia del Gobierno (que prevé invertir en los próximos tres años más de 450 millones de euros en impulsar la ciberseguridad y en fomentar el talento) auguran un mayor crecimiento.

Aunque este mapa cambie en lo sucesivo, RED SEGURIDAD destaca una amplia selección de fabricantes, consultoras, distribuidores y empresas de servicios en materia de seguridad de las tecnologías de la información y las comuniaciones. Todo ello, con el objetivo de representar el tejido corporativo de este sector dentro de nuestras fronteras.

José Manuel Villanueva

Country Manager para Iberia de Everbridge

"Automatizamos los procesos, haciendo más fácil y rápida la solución a una crisis de TI"

Mantener a las personas seguras y a las empresas funcionando más rápido en momentos de crisis. Este es el objetivo de Everbridge, una compañía que ha creado una plataforma compuesta por un conjunto de soluciones para ayudar a sus clientes a estar mejor preparados, tomar óptimas decisiones y responder con precisión durante los eventos críticos. Hablamos con su responsable en España para conocer mejor esta compañía.

David Marchal
Fotos: Everbridge

¿Cuál es la actividad principal de Everbridge y qué líneas de negocio tiene?

Nuestra actividad se centra en ayudar a empresas e instituciones en la gestión de un evento crítico, una crisis o una amenaza. Para ello, a lo largo de estos años, Everbridge ha creado una plataforma compuesta por un conjunto unificado de soluciones para ayudar a nuestros clientes a estar mejor preparados, tomar mejores decisiones y responder con rapidez, precisión y confianza durante los eventos disruptivos o críticos. Tenemos más de 5.400 clientes en todos los sectores, de los cuales los más remarcables son banca, industria manufacturera, energía, sector público, *utilities* y salud.

¿Podría hacer balance de cómo ha sido 2020, un año marcado casi en su totalidad por la pandemia, en términos de negocio para Everbridge?

El año 2020 ha sido difícil para todo el mundo por la pandemia que estamos sufriendo. No obstante, nosotros nos hemos encontrado en una mejor posición, ya que las empresas e instituciones se han visto en la necesidad de acelerar sus planes a la hora de implementar sistemas de comunicación y gestión de crisis.

La compañía cuenta con una Plataforma de Gestión de Eventos Críticos. ¿Qué ofrece esta solución?

La plataforma CEM (*Critical Event Magement*) permite a nuestros clientes gestionar el ciclo completo de un evento crítico, poniendo a las personas a salvo y permitiendo que su actividad y sus negocios sigan funcionando sin interrupciones.

Todos los días, de manera continua, están ocurriendo en todo el mundo eventos críticos de diferentes tipos,

como atentados terroristas, virus informáticos, huelgas de controladores aéreos, disturbios públicos, climatología adversa, etcétera. La capacidad de comprender el impacto potencial de estos eventos y mitigarlos de manera efectiva requiere de un equipo bien coordinado para compartir información y un manual de estrategias común. Y es que cualquiera de estos eventos puede impactar en la seguridad de las personas (empleados o residentes, dependiendo si hablamos de una empresa o los residentes de un área geográfica) y de las infraestructuras (fábricas, edificios, cadena de fabricación o suministro, etc.), afectando a los ingresos, los beneficios y la reputación de una marca.

Cada día, las empresas y organizaciones se enfrentan a diferentes tipos de eventos críticos, cada uno con diferentes partes afectadas. Al mismo tiempo, se les exige que respondan de una manera más rápida y efectiva, pero a la vez con menos recursos. Por eso necesitan ayuda y automatización.

Es aquí donde Everbridge pone al servicio de las empresas las soluciones que componen su plataforma. Estas soluciones nos permiten tener conocimiento sobre los eventos que están sucediendo en ese momento y que pueden provocar una situación de crisis.

Una vez detectada la amenaza, la plataforma nos da herramientas para analizar de manera rápida si esa amenaza puede provocarnos un problema, una crisis. Si confirmamos que nos puede hacer daño, el siguiente paso es localizar a quién le afecta y quién puede ayudar a las personas, grupo de personas, infraestructuras, etcétera, afectadas.

Posteriormente pondremos en marcha un plan de actuación coordinando, orquestando todas las acciones entre los diferentes equipos para mitigar el impacto de esa amenaza.

Además, la plataforma Everbridge permite tener la capacidad de poder hacer un análisis de cómo hemos actuado para mitigar la amenaza y solucionar la crisis. De esa manera podemos mejorar el patrón o modelo de actuación cuando volvamos a tener una crisis similar.

¿Qué infraestructura tecnológica se encuentra detrás de su Plataforma de Gestión de Eventos Críticos para que puedan ofrecer un servicio adecuado e ininterrumpido a sus clientes, sobre todo en momentos complicados como la gestión de un evento crítico?

Las soluciones que componen nuestra plataforma están en la nube. Actualmente tenemos 15 centros de datos con capacidad flexible y redundancia de datos completa. Los nodos están geográficamente distribuidos con un soporte de 24 horas los 365 días del año. Pero además de las soluciones que tenemos en la nube con las que operan nuestros clientes, disponemos de acuerdos con múltiples proveedores de SMS, voz, etcétera, para garantizar las comunicaciones sin interdependencias, optimizadas para la entrega local. En una crisis el mensaje siempre va a llegar a la persona correcta, en el momento adecuado y por el canal más rápido.

Everbridge mantiene medidas de seguridad rigurosas en todos los niveles, que abarcan personas, procesos y tecnología, para proteger todas las facetas de la información del cliente.

¿De qué manera ayuda su tecnología a mitigar los problemas de seguridad y ciberseguridad acrecentados por la extensión de la pandemia en el mundo?

Nuestra tecnología ayuda a mitigar los problemas de seguridad con soluciones como Mass Notification y Crisis Management, tanto en los procesos de comunicación de crisis como durante la gestión de esta.

Para ciberseguridad, tenemos una solución complementaria que es IT-Alerting. Esta solución nos permite alertar a los usuarios y, a la vez, poner en comunicación a quienes han de resolverlos; es decir, contactar y organizar a las personas adecuadas del departamento de Informática para que de una manera rápida tengan conocimiento de la situación, puedan analizar el problema y lanzar un plan para solucionar la crisis.

> ”La plataforma Everbridge permite analizar cómo ha actuado la organización para mitigar una amenaza y solucionar una crisis”

Además, tenemos desarrollados conectores con las diferentes aplicaciones que se usan en estos departamentos integrando estas en el proceso; y proporcionamos herramientas de comunicación efectivas como chat privados, sistemas multiconferencia, etcétera. De esta manera automatizamos los procesos, haciendo más fácil y rápida la solución a una crisis de TI.

¿Qué aporta Everbridge a las organizaciones para mejorar tanto su seguridad como su ciberseguridad?

En el día a día nuestros clientes realizan comunicaciones acerca de diferentes peligros que pueden impactar en sus oficinas, como cuando hay manifestaciones o revueltas cerca de sus oficinas, descuideros en la zona, cortes de suministros, etcétera. Esto repercute en el servicio al cliente, y estos valoran tener una herramienta como Everbridge, que les ayuda a incrementar su buena imagen y prestigio. Para entenderlo mejor, pondré dos ejemplos reales.

Un cliente que sufrió *ransomware* usó la plataforma Everbridge para comunicar rápidamente las acciones a seguir y para coordinar a los diferentes miembros del equipo y sus actividades. Durante la gestión de un ciberataque, el uso de Everbridge fue fundamental en dos aspectos, según palabras de nuestro cliente. En primer lugar, les permitió gestionar la comunicación en tiempo real con el equipo ejecutivo de los distintos países cuando los canales de comunicación habituales estaban desconectados por motivos de seguridad. En segundo término, les permitió convocar los comités de crisis y usar sistemas alternativos de audioconferencia cuando no estaban funcionando los medios habituales.

Por otro lado, uno de nuestros clientes con presencia internacional está estableciendo comunicación y gestión a todas sus oficinas de las diferentes acciones que han tenido que poner en marcha puntualmente o de manera generalizada para mitigar los problemas derivados del COVID-19.

En definitiva, en estos casos se ha puesto en valor el hecho de disponer de un sistema paralelo, totalmente independiente de los sistemas corporativos, que permita una vía alternativa de comunicación y trabajo en momentos donde no puedes contar con los canales habituales.

En el caso de las empresas españolas, ¿cree que deberían avanzar más en términos de gestión, además de en la fase de prevención, para afrontar el problema del *malware* y los ciberataques?

Para afrontar el problema del *malware*, la prevención y la educación del personal es fundamental, ya que conforman la primera línea de defensa. El mayor desafío al que se enfrentan las organizaciones de hoy en día es la falta de una comunicación interna y externa eficaz, antes, durante y después de un ciberataque. Por eso, mi recomendación es la implementación de un sistema de comunicación y gestión de crisis, así como la preparación de los diferentes escenarios de crisis con los que nos podemos encontrar. En Everbridge tenemos mucha experiencia, ya que nuestro departamento de Servicios Profesionales ha desarrollado esto en diferentes clientes de distintos sectores, teniendo ya un gran repositorio de buenas prácticas para aplicar en según qué casos.

¿La pandemia ha incrementado el interés de las organizaciones por implementar herramientas relacionadas con la ciberseguridad? ¿Qué les piden sus clientes en este sentido?

La pandemia nos ha llevado a todos a un nuevo escenario y ha cambiado el modelo de trabajo, en unos casos más que en otros. Las nuevas situaciones han abierto la puerta a los ciberdelincuentes y a que las empresas sufran un incremento grande de problemas que han tenido que solucionar de manera rápida. En muchos casos se han echado en falta la comunicación efectiva y la necesidad de herramientas de gestión específicas para entornos de TI. Empresas que habían visto algunas presentaciones de nuestra solución IT-Alerting se han vuelto a poner en contacto con nosotros para hablarnos de los casos que han sufrido y cómo les podemos ayudar.

¿Qué expectativas tienen puestas en este año que acabamos de empezar?

Este año notamos que hay una mayor conciencia a la hora de adoptar soluciones de comunicación y gestión de crisis, así como en torno a la actualización de los planes de continuidad de negocio. Hay muchas empresas con las que trabajamos desde hace algún tiempo que en estos momentos quieren acelerar la adopción de planes y herramientas para poder estar bien preparadas para afrontar futuras crisis. ■

Aceleración digital y seguridad

Os esperamos el 22 de junio

Organiza

SEGURITECNIA
REVISTA DECANA INDEPENDIENTE DE SEGURIDAD

red seguridad

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Los retos son numerosos, aunque yo destacaría los siguientes. Por un lado, la transformación digital y "cloudificación" de los procesos, unido a la pandemia y la identidad digital, abren nuevos retos y preocupaciones. Por eso, es fundamental saber securizar entornos y adaptar la seguridad al negocio de nuestros clientes.

Por otro lado, es clave gestionar la seguridad de los colaboradores o terceros en el *end to end* del proceso, cuidando todas las puertas de conexión, así como la gestión de seguridad del dato. Además, resulta fundamental definir planes de resiliencia que permitan a las organizaciones estar preparadas para prevenir y recuperarse ante los potenciales ataques.

Por último, otro de los grandes retos es contar con profesionales multidisciplinares que entiendan no solo de seguridad, sino también de los procesos y negocios de los clientes.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Uno de los puntos débiles en la cadena de tratamiento de la información son los usuarios, internos o externos, que, con técnicas de suplantación de identidad y modificación de las configuraciones en la cadena de suministro, consiguen acceso a la información de las organizaciones.

Los ataques persistentes evolucionan en los vectores de entrada a las empresas a través del compromiso en la cadena de suministro y sus relaciones de confianza. Así, convierten en cómplices involuntarios del ataque a proveedores de servicio, *software* o *hardware*.

Además de encontrar nuevas formas de atacar a las empresas con *ransomware*, los atacantes buscan otros métodos como amenazar con publicar información confidencial y crítica de las empresas que se ha exfiltrado antes del ataque.

Los atacantes también están mejorando sus capacidades de movimientos laterales dentro de las redes de las compañías, combinando técnicas y canales y alcanzando entornos tanto IT como OT. Estos ataques exigen un cambio en la mentalidad de los equipos de defensa, siendo más proactivos y partiendo de un espíritu de caza de amenazas (*Threat Hunting*).

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

Nuestro conocimiento tecnológico e industrial nos permite entender los negocios de los clientes y desarrollar una seguridad innovadora que permita buscar eficiencias y, a su vez, dotar a las compañías de visibilidad sobre su estado de resiliencia, protegiendo con técnicas diferenciales sus activos y estudiando proactivamente las nuevas amenazas.

Ayudamos a definir planes de resiliencia ajustados a las amenazas reales de los clientes y teniendo en el foco el concepto "protección del dato" y la realidad de estar preparados o no a un ataque, colaborando en las transformaciones digitales desde el inicio, "*Security By Design*".

Nuestro conocimiento multidisciplinar nos permite trabajar en equipo las distintas líneas de protección y defensa dentro de las compañías, alineando con los más estrictos estándares de OT e IT y regulaciones de seguridad, en distintos modelos con *frameworks* dirigidos.

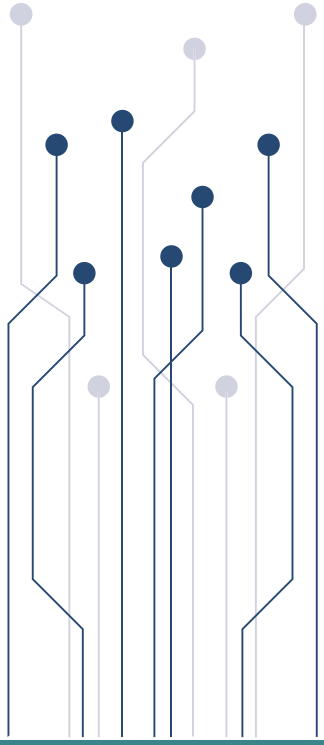
Además, diseñamos y evolucionamos los servicios de monitorización avanzada con SOC de nueva generación y correlación de fuentes e indicadores de compromiso, dotando de inteligencia a los sistemas para un autoaprendizaje.

Más información en:
www.accenture.com/es-es

accenture

Alexis Alonso Arévalo

RESPONSABLE DE ACCENTURE APPLIED CYBERSECURITY SERVICES EN ESPAÑA, PORTUGAL E ISRAEL



Superar la incertidumbre

El teletrabajo ha eliminado las barreras que protegían tu organización. Conoce las acciones que deben tomar los líderes para mantener sus negocios seguros para el futuro.

accenture.es/security

accenture

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

La era de la convergencia generalizada y entornos híbridos de Tecnologías de la Información (IT), la Operatividad Tecnológica (OT) y el Internet de las Cosas (IoT). El gran reto requiere una nueva mirada a la estrategia híbrida de ciberseguridad y seguridad integral.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Las organizaciones, tanto públicas como privadas, siguen adoptando tecnologías IT, OT e IoT para entornos industriales o críticos sin las medidas de seguridad, por lo que se avecina una mayor actividad delictiva en sectores críticos como plantas de ensamblaje, productos farmacéuticos y otras organizaciones industriales.

Nuestros hogares y organizaciones se vuelven más inteligentes con dispositivos cada vez más asequibles del denominado IoT. Este problema se intensificará una vez que 5G tenga una huella significativa.

El aumento de las capacidades de computación y la Inteligencia Artificial podrían hacer que este 2021 fuera un año en el que los *deepfakes* y la evasión de técnicas biométricas comiencen a utilizarse más ampliamente para su uso en ciberdelitos.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

Bidaidea es una consultora boutique, global, independiente y multinacional española orientada a la ciberseguridad, inteligencia y transformación digital de la seguridad integral de extremo a extremo a organizaciones públicas y privadas. Está especializada en el desarrollo e implementación del cambio organizativo y cultural.

Son 14 años de trayectoria en los que nos hemos adaptado a las necesidades del mercado, reuniendo a los mejores profesionales para obtener la confianza del cliente como nuestro mayor objetivo.

Somos expertos en el diseño e implantación (traje a medida) de planes integrales de seguridad 360 grados (física, electrónica, lógica, ciberseguridad e inteligencia) para usuarios y organizaciones de cualquier tamaño.

Empezamos en 2006 y hemos evolucionado nuestra propuesta desde la estrategia hasta la transformación digital de la seguridad integral de las organizaciones, dando servicio a las principales empresas del país y a clientes pequeños y medianos (SMB).

En Iberia y Latinoamérica somos ya un referente en infraestructuras críticas y estratégicas. No existe sector de riesgo que se nos resista, ni aspectos de seguridad que no tengamos controlado.

Actualmente, tenemos un abanico de posibilidades para mejor la prevención, protección y respuesta (24x7x365): consultoría GRC & BC (gobierno, riesgo, cumplimiento y continuidad de negocio), auditoría técnica (*Ehtical Hacking & Red Team*), productos y soluciones especializadas (DemoLAB), centro de operaciones de seguridad integral 360 grados (iSOC), servicios de inteligencia y seguridad internacional (iNTELL), formación y concienciación (Bidaidea Academy), *outsourcing* especializado, laboratorio de industria 4.0 (iLAB) e I+D+i.

Por último, cabe destacar que contamos con oficinas con equipo local en España, Estados Unidos, Brasil, Colombia, Perú, Portugal y México.

Más información en:
ciberseguridadbidaidea.com

bidaidea
CYBERSECURITY & INTELLIGENCE

Mikel Rufián Albarrán
GLOBAL MANAGING DIRECTOR - HEAD OF GLOBAL CYBERSECURITY & INTELLIGENCE LEAD

bidaidea

CYBERSECURITY & INTELLIGENCE

- Líderes en infraestructuras críticas
- Líderes en convergencia IT / OT/ IoT
- Transformación digital de la seguridad
- Inteligencia en materia de Ciberseguridad

Servicios de Inteligencia

GRC & BC

Auditoría Técnica

Centro de Servicios 24x7 (iSOC)

Industria 4.0 (iLAB)

I+D+i

Productos Especializados

Outsourcing

Formación y Concienciación

España
Portugal
Brasil
México
Colombia
Perú
U.S.A.

"La Ciberseguridad no es un estado, es un proceso continuo que involucra a toda la organización"

Mikel Rufián
Managing Global Director
Head of Global Cybersecurity & Intelligence Lead

Telf +(34) 670 025 091 – www.ciberseguridadbidaidea.com

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Los retos de esta nueva realidad laboral pasan por mejorar la ciberseguridad y la formación de los trabajadores. Las empresas han tenido que enfrentarse en 2020 a la incorporación del teletrabajo a la velocidad que requerían las circunstancias, pero esto plantea nuevos retos como los ciberataques. Si los ciberdelincuentes consiguen monetizar sus amenazas, estas seguirán creciendo, de manera que las compañías deberán plantearse seriamente la incorporación de verdaderas estrategias de seguridad que protejan sus activos.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

La primera del top 3 será el *ransomware*. Como hemos visto en estos primeros meses del año, este *malware* sigue afectando a empresas y corporaciones. Hemos visto ejemplos como el del SEPE o el Ayuntamiento de Castellón y, desgraciadamente, muchas corporaciones afectadas. La previsión, por tanto, es que estas amenazas continuarán en 2021 y más allá.

En segunda posición, destacaríamos los *exploits*. El aprovechamiento de vulnerabilidades provocará que los atacantes sigan utilizando herramientas *exploit* para obtener datos, información de determinados equipos e incluso continuar con el cifrado malicioso a través del *ransomware*.

Y, en tercer lugar, estaría el *phishing*. Los *emails* que suplantan web, identidades o empresas para sustraer información o el robo de datos personales siguen al alza en lo que va de año y, seguramente, continuarán en los siguientes meses.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

Desde Eset nos preocupamos por estar a la última en tecnología mejorando nuestras soluciones de seguridad para garantizar la mejor protección de nuestros clientes. Por eso es importante para nosotros la innovación y la mejora continua. Gracias a los 13 centros de I+D que tenemos en todo el mundo hemos conseguido unas soluciones de ciberseguridad potentes y eficientes que, junto a actualizaciones diarias, permiten que empresas y particulares estén lo mejor protegidos posibles.

Además, venimos ofreciendo como protección avanzada a nivel de ciberseguridad en los últimos años dos herramientas que están destinadas a cubrir una parcela muy importante: Eset Dynamic Threat Defense, una *cloud* tipo *sandbox* que nos permite analizar cualquier archivo desconocido para saber al instante si es malicioso o no; y Eset Enterprise Inspector, nuestro EDR avanzado posibilita monitorizar cualquier evento que se produce en nuestra red para poder responder y actuar lo antes posible y remediar una posible amenaza o ataque, sobre todo las conocidas como APT.

Por otro lado, ofrecemos servicios de ciberseguridad que permiten que un cliente que no esté instruido en esta materia o no tenga personal especializado pueda contar con Eset España para que seamos nosotros los que monitoricemos sus equipos y le mantengamos protegido en todo momento, sin que se tenga que preocupar de nada.

Destacar también la concienciación, educación y formación. Desde las páginas web blogs.protegerse.com y www.welivesecurity.com/la-es mantenemos informados a los lectores sobre ataques, alertas, tendencias de amenazas, así como novedades en ciberseguridad.

Más información en:
www.eset.com/es/

ENJOY SAFER TECHNOLOGY™

David Sánchez
DIRECTOR COMERCIAL

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN

ESET Threat Intelligence
ESET Virus Radar
WeLive Security

PREVENCIÓN

Endpoint Protection Platform
ESET Mail Security
ESET Gateway Security
ESET SharePoint Security
ESET Secure Authentication
ESET Endpoint Encryption
ESET Security Management Center
ESET Cloud Administrator

RESPUESTA

ESET Enterprise Inspector
ESET Dynamic Threat Defense
ESET Security Management Center
ESET Cloud Administrator

DETECCIÓN

Endpoint Protection Platform
ESET Dynamic Threat Defense
ESET Enterprise Inspector
ESET Mail Security
ESET Gateway Security
ESET SharePoint Security
ESET Secure Authentication
ESET Endpoint Encryption
ESET Security Management Center
ESET Cloud Administrator

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Son varios, pero como punto de partida creo que la seguridad debe ser considerada como un elemento clave desde el inicio de cualquier cambio improvisado o acelerado en la infraestructura o en los procesos. En España, especialmente, la transformación digital se ha visto forzada a avanzar a pasos de gigante estos últimos meses, y esta aceleración pasa, entre otras cosas, por la adopción de arquitecturas *serverless* y el traslado de *apps* y APIs a la nube, para acomodar al creciente volumen de actividad *online* y trabajadores remotos.

Para ello, es interesante aprovechar las soluciones de seguridad de fácil implementación que luchan contra los intentos de amenazas –en lugar de contra amenazas concretas– y que pueden funcionar tanto bloqueando ataques desde el inicio como monitorizando el tráfico –sin bloquearlo–, y sin sobrecargar a los equipos de seguridad y operaciones.

La visibilidad u observabilidad es, sin duda, otro gran reto especialmente importante. Los ataques en tiempo real precisan reacciones en tiempo real. Y en esta área existe una creciente necesidad de pasar de tecnologías antiguas con visibilidad limitada o aislada a *stacks* modernos, capaces de integrar y acoplar mayores volúmenes y fuentes de datos y ofrecer así observabilidad completa, permitiendo a desarrolladores y equipos de seguridad y IT trabajar conjuntamente.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Uno de los efectos de la aceleración digital es el auge de la aparición de nuevos servicios, aplicaciones y APIs que están abriéndose paso en el mercado. Esto hace que se conviertan en potenciales objetivos de ciberataques. También se incrementa el riesgo de sufrir ataques para lograr accesos o datos a través de las APIs que muestren algún tipo de vulnerabilidad. Por este motivo, y por el papel cada vez más importante de las propias APIs, es clave garantizar su seguridad.

En 2021 seguiremos evolucionando hacia servicios *online* cada vez más completos, con códigos sofisticados y en los que entran en juego un mayor volumen de datos de clientes. Ambos son elementos altamente codiciados por los ciberdelincuentes. Este año será clave para las compañías encontrar soluciones de seguridad unificadas en las que apalancar su innovación.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

La reciente adquisición de Signal Sciences por parte de Fastly nos ha permitido configurar una moderna y completa solución de protección de aplicaciones web y de APIs unificada en el momento actual, en el que la seguridad en el borde está cobrando vital importancia.

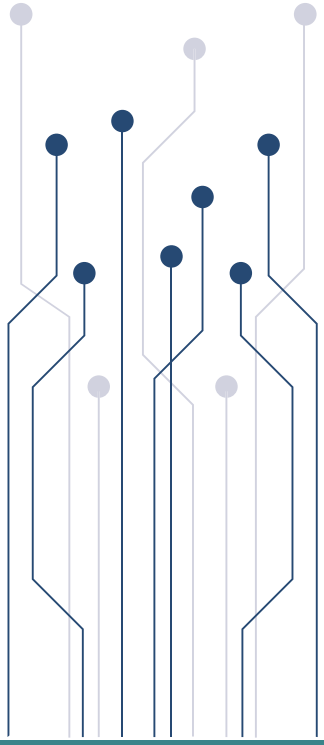
Estamos muy contentos de poder ofrecer a los clientes un sólido porfolio con el cual continuar securizando sus sitios web. Los requerimientos en materia de seguridad por parte de los clientes han evolucionado enormemente, y desde Fastly nos tomamos muy en serio la misión de poner a disposición del mercado una solución unificada para dar respuesta a estas nuevas necesidades. Nuestra plataforma está diseñada para observar la intención del tráfico. Ayudamos a defender a nuestros clientes contra ataques conocidos como inyecciones SQL o *cross-site scripting*, así como contra ataques más avanzados, tipo ATO y *bots* maliciosos, sin sacrificar el rendimiento.

Más información en:
www.fastly.com

fastly

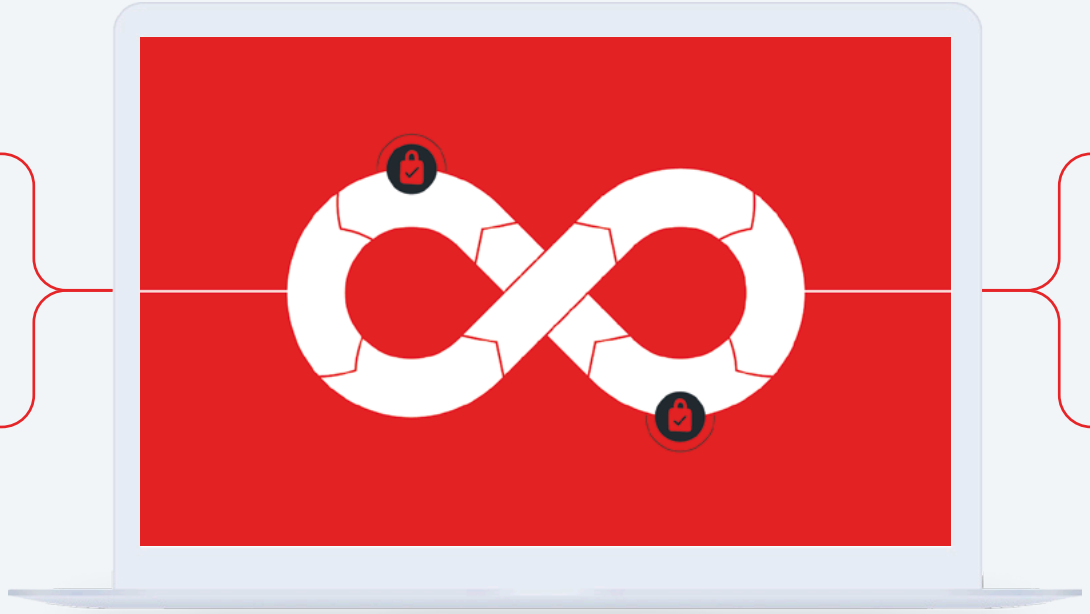
Jesús Martín Oya

SENIOR SALES DIRECTOR SOUTHERN EUROPE & MIDDLE EAST



fastly

Signal Sciences
Now part of fastly



Fastly y Signal Sciences han unido sus fuerzas para transformar el panorama de la seguridad.

Juntos creamos una plataforma de seguridad unificada, creada para DevOps de hoy en día. Signal Sciences, reconocida como visionaria en el informe Gartner Magic Quadrant 2020 para Web Application Firewalls, aporta a la familia Fastly soluciones de seguridad líderes en el sector.

Más información en:

fastly.com/es/signalsciences

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

La industria debe desarrollar un proceso de continua innovación, no solo porque las amenazas cambian constantemente, sino también para ganar en competitividad y acercarse aún más al usuario final. La demanda en el campo de la ciberseguridad seguirá incrementándose como consecuencia del crecimiento del tráfico y de las redes, el aumento del negocio digital, el impacto de los dispositivos del Internet de las Cosas, así como por una mayor preocupación de las corporaciones en materia de seguridad económica. Parte de esa nueva demanda podrá ser atendida gracias a la tecnología; pero, dada la complejidad y la interdependencia de nuestro modelo de vida, la importancia de los recursos humanos expertos será cada vez más relevante.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

El *ransomware* y los ataques mediante *phishing* seguirán siendo las amenazas predominantes, pero iremos viendo crecer el número de ciberataques contra las personas que dirigen las grandes corporaciones o las áreas críticas de las organizaciones.

Durante estos años, las compañías han ido mejorando la defensa de sus activos empresariales y sus sistemas. Sin embargo, no han avanzado tanto en la protección de sus directivos y empleados, sin tener en cuenta que sus dispositivos personales y sus rutinas los convierten en un vector de ataque para los cibercriminales, bien por su posición o bien por la información que manejan.

También seguirá creciendo el uso de medios cibernéticos y electrónicos para la localización, espionaje, persecución y ataque a las personas.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

GH Crecemos ha desarrollado una plataforma, denominada Ciberescolta, que incluye servicios y productos basados en inteligencia diseñados para proteger a las personas.

Sabemos que la seguridad nunca es absoluta, pero Ciberescolta reduce el riesgo de éxito de los ataques a nuestros clientes en más de un 90 por ciento.

Este sistema se basa en cuatro pilares. El primero de ellos es la anticipación. Mediante el máximo conocimiento de la vida digital y física del cliente y con la experiencia acumulada por los diferentes profesionales de GH Crecemos, elaboramos una estrategia específica orientada a hacer fracasar los intentos de agresión o de intrusión.

El segundo es la protección: dotamos a las personas de las herramientas necesarias para conocer si están siendo objeto de una acción de espionaje, robo, persecución o cualquier otro tipo de ataque.

El tercer pilar es la detección, es decir, que somos capaces de alertar a los profesionales de seguridad sobre la presencia activa de ataques electrónicos, sistemas espías o conductas reiteradas que puedan tener como objetivo las personas a las que protegemos.

Y el último es la mitigación: si a pesar de haber tomado las medidas anteriormente descritas, el cliente fuera finalmente objeto de un ataque, nuestro sistema pone en marcha las medidas de mitigación necesarias orientadas a minimizar el daño, partiendo de un análisis forense de lo ocurrido, trazando, dificultando su uso o, si es posible, inutilizando los activos sustraídos.

Más información en:
ghcrecemos.com

Constantino Méndez-Martínez
SOCIO FUNDADOR

CIBERESCOLTA

PERSON CENTERED SECURITY
IN THE DIGITAL ERA

Los elevados costes de los ciberataques justifican la inversión en ciberseguridad

Las personas se convierten en una puerta importante de entrada para los ciberdelincuentes

Casi todas las soluciones del mercado están dirigidas a salvaguardar los activos de la compañía

Ciberescolta se dirige a proteger a los directivos, garantizando la reducción de las vulnerabilidades en un 90%

crecemos

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Los ciberataques tipo *ransomware* durante 2020 y principios de 2021 son ejemplos de la sofisticación del atacante con un alto grado de intencionalidad. Se demuestra que no solo se busca producir un impacto negativo en una organización, sino que también se tiene la capacidad de hacerlo, ya que el acceso al *malware* es demasiado sencillo y su lanzamiento no requiere de apenas recursos. Si no existiera oportunidad de atacar, entonces el daño no se produciría; y la forma de reducir esa oportunidad al mínimo pasa por plantear al atacante un escenario tan poco atractivo que desistiría de sus planes.

Por lo tanto, el gran reto de la industria de la ciberseguridad, tanto en España como a escala mundial, es convertir a las organizaciones en objetivos sin interés ninguno de ser atacados por los cibercriminales.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Durante este año veremos un predominio de aquellas ciberamenazas que busquen sacar partido del estado de excepcionalidad marcado por la pandemia. La cadena de suministro de vacunación COVID-19 es un objetivo claro de los ciberdelincuentes.

El sector sanitario en particular, junto con el farmacéutico, están en la diana de los delincuentes, que pueden emplear métodos tecnológicamente rudimentarios aunque tremendamente efectivos, como campañas de *phishing* hacia organismos concretos como gancho, con contenido que apela al miedo por la situación económica (ERTE, ayudas estatales, sanciones…) o sanitaria (citaciones de vacunación, cambios en revisiones médicas rutinarias…).

Si a lo anterior añadimos los ataques exitosos de alto impacto que han sufrido grandes organizaciones, podríamos intuir que en 2021 es posible revivir una situación similar.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

En GMV nos dedicamos a la prestación de servicios de ciberseguridad a nuestros clientes; en especial, grandes organizaciones y administraciones públicas. Tenemos servicios y soluciones específicas para distintos sectores, como el financiero, el industrial o de la salud.

Esos servicios cubren todas las actividades definidas en marcos como el NIST CSF e incluyen el análisis y diagnóstico del estado de la ciberseguridad, la elaboración de planes de adecuación a normativa o legislación, la gestión y operación de las soluciones tecnológicas instaladas en los clientes y la detección, visibilidad e inteligencia para la toma de decisiones y buen gobierno.

Nuestra especialización es máxima en servicios como ciberinteligencia, la puesta en marcha y operación de infraestructuras de ciberprotección y la respuesta ante incidentes a través de nuestro centro GMV-CERT.

Más información en:
www.gmv.com/es/

Javier Zubieta Moreno

DIRECTOR DE MARKETING Y COMUNICACIÓN

¿Cuáles serán las ciberamenazas que predominen este año y cómo ayuda su empresa a los usuarios a abordar sus necesidades de seguridad?

El ciberriesgo ocupa el primer puesto en casi todas las encuestas, y además con el añadido de que ahora desarrollamos nuestras funciones teletrabajando. Este aspecto es parte de lo que nosotros venimos realizando desde hace años porque creemos firmemente que es necesaria una gestión integral de los riesgos que esté presente en todos los niveles de la compañía. Esa gestión del riesgo debe estar englobada con una solución tecnológica que permita tomar decisiones en el día a día. Esto, junto con una estrategia GRC (Gobierno, Riesgo y Cumplimiento), ayuda a las empresas a mitigarlo y reducirlo. La adopción de estrategias GRC dentro de las compañías es pilar nuclear dentro de la digitalización. No podemos vivir instalados en la incertidumbre del riesgo.

En GlobalSUITE Solutions tenemos más de diez años de experiencia en la implantación de estrategias GRC, ayudamos a identificar y valorar los sistemas de información para detectar posibles riesgos y amenazas a los que pueda estar sometido, y sobre todo contamos con GlobalSUITE® como solución de apoyo para la implantación y gestión de sistemas GRC, seguridad, continuidad, auditoría, privacidad y ciberseguridad, etc.

Más información en:
www.globalsuitesolutions.com/es

GlobalSUITE SOLUTIONS

Antonio Quevedo Muñoz
CEO

La solución para optimizar los procesos de riesgos, seguridad, continuidad, auditoría, privacidad y compliance en tu negocio

- Risk Management
- Information Security
- Business Continuity
- Compliance Management
- Privacy Data Protection
- Audit Management

www.globalsuitesolutions.com

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

El principal reto está relacionado con la desaparición del tradicional perímetro de seguridad, consecuencia del uso creciente de los dispositivos móviles, el trabajo en remoto y los servicios en la nube. Este hecho hace que la gestión de la seguridad se convierta en una tarea mucho más compleja, pues supone administrar un número creciente de dispositivos no protegidos en un entorno de trabajo con innumerables vectores de vulnerabilidad y una menor capacidad de control de la red por parte de la empresa.

Mantener segura y productiva a la plantilla dentro de esta complejidad requerirá no solo de la adaptación de una arquitectura y estrategia de seguridad *Zero Trust* (confianza cero), sino también supondrá un incremento de los procesos de automatización en el descubrimiento y en la remediación. Es decir, debido a su complejidad, ya no es viable la gestión manual de la ciberseguridad, por lo que habrá que recurrir a la automatización con sistemas inteligentes.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

En general, preveo que habrá una continuidad del aumento de las ciberamenazas que hemos visto en 2020, muy en la línea del *phishing* y el *ransomware*.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

Disponemos de una arquitectura de extremo a extremo *Zero Trust* capaz de descubrir, gestionar y proteger a todos los puntos de acceso que están involucrados en las aplicaciones y en los servicios de la empresa. En este sentido, ofrecemos una respuesta a la forma en la que las empresas necesitan abordar la ciberseguridad en el actual entorno sin perímetro. Un entorno complejo en el que resulta necesario no solo implementar una estrategia de seguridad *Zero Trust* sostenible, sino también hacerla evolucionar incorporando una capa de hiperautomatización, de forma que sistemas vanguardistas de inteligencia artificial y automatización puedan asistir a los CISO y adelantarse a los problemas antes de que ocurran.

Incorporar la hiperautomatización es un paso necesario en el actual entorno *Zero Trust*, pues la propia complejidad de la red sin perímetro supera las posibilidades de una gestión manual de la operativa de seguridad.

También resulta especialmente importante en este nuevo entorno desarrollar una excelente gestión de la experiencia del usuario. Este, al no trabajar desde la oficina, va a requerir que su experiencia como usuario en relación a los servicios corporativos sea similar a la que tenía cuando trabajaba desde la empresa.

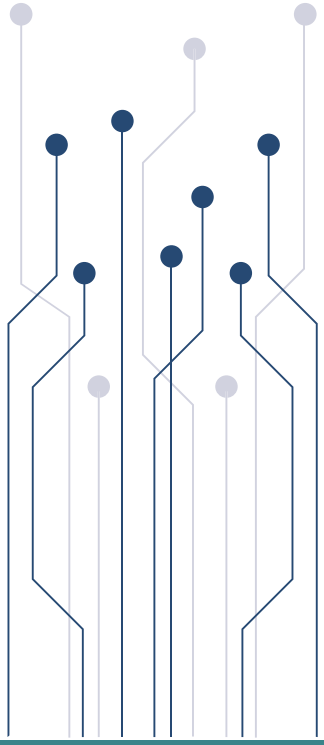
Esta experiencia debería ser similar a la del mundo del consumo, donde la gestión de cara al usuario es ágil y sencilla. Es algo parecido a lo que ofrecen aplicaciones como WhatsApp o Facebook, que se desarrollan pensando en un usuario que no es experto en tecnología.

Como conclusión, nuestro modelo se basa en conseguir ese nivel de experiencia de consumo para el usuario, cuidando su privacidad dentro de un modelo de arquitectura de seguridad *Zero Trust*, a la que incorporamos una capa de inteligencia y automatización integrada que ayude a remediar los problemas antes de que ocurran, respondiendo a las exigencias del negocio y reduciendo los costes operativos.

Más información en:
www.ivanti.es

ivanti

Daniel Madero
REGIONAL SALES DIRECTOR



¿Cuáles serán las ciberamenazas que predominen este año y cómo ayuda su empresa a los usuarios a abordar sus necesidades de seguridad?

En 2021, los ataques basados en *ransonware* continuarán siendo protagonistas de las amenazas para empresas y administraciones públicas. Simplemente porque funcionan para los atacantes, que siguen consiguiendo sus objetivos con porcentajes de éxito realmente alarmantes.

Otras amenazas tradicionales, como *phishing* o el fraude del CEO (BEC), estarán muy presentes. Y aprovechando el teletrabajo masivo que continuará este año, los ataques con foco en los accesos remotos y servicios en la nube seguirán viéndose igualmente.

Hay que seguir vigilando las ciberamenazas dirigidas a la cadena de suministro e infraestructuras críticas, que también tuvieron un impacto importante en 2020.

En Ingenia ayudamos a prevenir con planes estratégicos de ciberseguridad, vigilancia digital, despliegue de soluciones tecnológicas de los principales fabricantes del mercado y formación específica de concienciación para empleados y directivos. Monitorizamos la seguridad 24x7 de nuestros clientes y, si se produce un incidente, ayudamos con la contención y recuperación desde nuestro Centro de Operaciones de Seguridad (eSOC), miembro de FIRST y CSIRT.es, garantizando de esta forma la continuidad del negocio.

Más información en:
ingenia.es

Ingenia

Carlos Cortés Danta
DIRECTOR ADJUNTO DE CIBERSEGURIDAD Y SERVICIOS GESTIONADOS

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Desde nuestra posición como agencia de calificación de ciberseguridad vemos un gran reto el asegurar la cadena de suministro, tanto de servicios como de productos. Hoy en día, nadie puede considerarse aislado del exterior y todos dependemos, en mayor o menor medida, de terceros para realizar nuestra actividad. Cómo asegurar que dichos terceros no suponen un riesgo para nuestra compañía no es trivial y va a requerir de un cambio de mentalidad en todas las compañías.

En particular, en este escenario –que, por otra parte, está cada vez más regulado– supone un reto adicional la seguridad de pequeñas y medianas empresas que, al fin y al cabo, son la mayoría del tejido empresarial y que necesitan no solo que se las exija un mayor grado de seguridad, sino que se las acompañe en ese proceso, porque no cuentan (ni tienen fácil acceso) al conocimiento necesario para ello. Aquí, organismos como el Instituto Nacional de Ciberseguridad tienen mucho que decir en esa labor, porque pueden ser la clave para mejorar la ciberseguridad del ecosistema empresarial.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Aunque es difícil predecir por dónde van a sorprendernos los distintos agentes que suponen una amenaza, pienso que vamos a ver una cierta continuidad en la corriente actual en la que los ataques de *ransomware* (complementados con amenazas de exfiltración) van a seguir siendo la estrella. Creo también que van a ser cada vez más corrientes los ataques a la cadena de suministro, tanto proveedores de servicios relevantes (estilo a lo que hemos visto de Exchange) como proveedores de piezas de *software* clave en la operación (tipo SolarWinds).

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

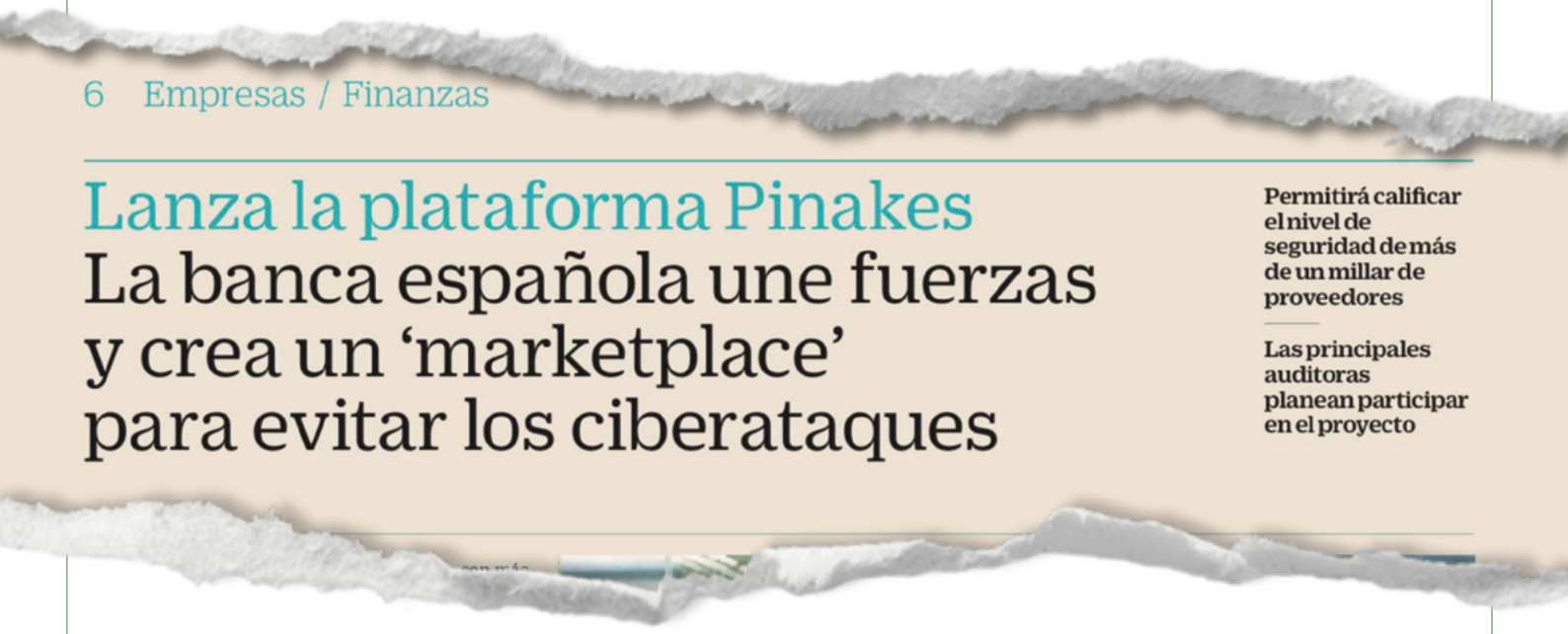
La labor de Leet Security es, fundamentalmente, aportar transparencia sobre el estado del nivel de ciberseguridad del ecosistema de servicios tecnológicos o que hacen uso de tecnología. En este sentido, nuestra metodología de calificación permite a los usuarios, por una parte, conocer el nivel de ciberseguridad de todos aquellos que pueden suponer un riesgo para ellos; es decir, les permite conocer hasta qué punto esos terceros pueden ser el eslabón más débil de su ámbito de protección.

Y por otro lado, permite a los proveedores de servicios mostrar a sus clientes, de manera eficiente y objetiva, el nivel de ciberseguridad de los servicios que les ofrecen, a la vez que pueden usar la metodología de evaluación para entender cuáles son sus puntos débiles y establecer planes de mejora basados en criterios objetivos.

En resumen, permite mejorar el nivel de ciberseguridad de todo el ecosistema gracias a la transparencia y la objetividad de la metodología de calificación. Esto ha quedado de manifiesto en el apoyo que el sector financiero nacional ha dado a esta forma de abordar el reto de la seguridad en la cadena de suministro, con el lanzamiento del servicio de calificación de proveedores del sector financiero Pinakes.

Más información en:
www.leetsecurity.com

Antonio Ramos
CEO Y FUNDADOR



6 Empresas / Finanzas

Lanza la plataforma Pinakes

La banca española une fuerzas y crea un 'marketplace' para evitar los ciberataques

Permitirá calificar el nivel de seguridad de más de un millar de proveedores

Las principales auditoras planean participar en el proyecto

Cinco Días, 3 de marzo de 2021

Ahorro y eficiencia
en el **sector financiero**
gracias a nuestra metodología

LEET SECURITY

CyberSecurity
Rating Agency

#TransmiteConfianza

www.leetsecurity.com/pinakes

+34 915 798 187 info@leetsecurity.com @LEET_Security @Leet Security SL

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Desde nuestra perspectiva, visualizamos tres grandes retos: respuesta a amenazas internas, ataques *malware* más rápidos y dificultades serias de cumplimiento de normativa de protección de datos.

Los ataques de *malware* mediante instalación de *software* malicioso podrán ser más rápidos en su implementación; el tiempo total desde el inicio de una actividad maliciosa hasta su ataque real podrá verse acortado. Se hace necesario disponer de herramientas de detección temprana, y ya es imperativo contar con tecnología que permita la detección en tiempo real para amenazas internas o externas. Los tiempos de análisis posteriores a las brechas de seguridad empiezan a estar anticuados; es preciso poder detectar y poder suprimir los ataques en tiempo real.

También vemos una ausencia alarmante dentro de muchas organizaciones de herramientas prácticas de cumplimiento de normativa de protección de datos: ¿quién sabe qué datos personales tienen en sus sistemas y dónde se almacenan? ¿Quién puede contestar a la pregunta de "qué datos míos tienen ustedes"? ¿Quién puede certificar que se han borrado de todos sus sistemas los datos personales de una determinada persona?

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

En un entorno como el actual con el COVID-19 omnipresente y donde se ha impuesto como medida de prevención el trabajo remoto, las empresas están más expuestas. Así que durante este año vemos tendencia a más ataques de *ransonware*, y ya que los trabajadores se encuentran dispersos, con conexiones remotas y utilizando mayor número de ordenadores portátiles y teléfonos móviles, se observan mayores dificultades en las empresas para evitar ataques internos.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

Sin descartar el trabajo preventivo, que es del todo imprescindible, facilitamos sistemas de protección en tiempo real, precisos y capaces de detectar amenazas internas y externas.

Para este cometido, instalamos un pequeño agente en todos los terminales y servidores de la organización a fin de monitorizar en tiempo real actividades maliciosas. Con estos sistemas somos capaces de velar por la seguridad de los datos, pero también de mantener la privacidad, de forma que los datos personales de los empleados estén a salvo. No se trata de vigilar a los empleados; se trata y se consigue vigilar accesos no autorizados y detectar actividades ilícitas de atacantes internos o externos. Los datos personales deben estar completamente protegidos.

Nuestros sistemas permiten adicionalmente una visibilidad total de los ordenadores que va a facilitar la organización, respetando el acceso a datos personales, el poder realizar investigaciones internas de forma discreta, realizar gestión documental y cumplimento de normativa RGPD, PCI DSS y de seguridad internas. Este tipo de investigaciones ayudarán a evitar fraudes internos, así como filtraciones de datos y de información confidencial.

Es alentador ver la actuación de los directivos que se marcan como objetivo no solo cumplir normativas sobre el papel; sino de una forma eficaz, que proteja a la organización y evite las importantes sanciones relacionadas con el RGPD.

Más información en:
www.ondata.es

Alfredo Ruiz
CEO

opentext™

ondata INTERNATIONAL | distribuidor **oficial**

EnCase Endpoint Security

DETECCIÓN MÁS TEMPRANA, DECISIONES MÁS RÁPIDAS Y RESPUESTA A AMENAZAS SIN PRECEDENTES.

Visibilidad completa de los endpoint para detección temprana de amenazas internas y externas, configuración de alertas y respuesta a incidentes con garantía forense.

- RESPUESTA AUTOMÁTICA A INCIDENTES
- PREVENCIÓN
- RESPUESTA A PÉRDIDAS DE DATOS
- INVESTIGACIÓN DE DELITOS

Más información:
900 101 334 (gratuito)

ondata INTERNATIONAL

Data Recovery & Forensics
www.ondata.es

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Dotar a las infraestructuras críticas que aportan servicios esenciales a la sociedad de soluciones digitales que les permitan identificar con todo detalle los riesgos de carácter ciberfísicos, poniendo foco principal en el área de tecnologías de la operación (OT). Estas herramientas ágiles deberán ir enfocadas al gobierno de la seguridad, gestión del riesgo en tiempo real, notificación de incidentes, pruebas de resiliencia, intercambio de información, privacidad, diagnósticos rápidos por sectores, estándares para cumplimento (ISO/IEC), orquestación de personas y tecnología a través de la automatización inteligente de procesos y presentaciones visuales globales de indicadores y tendencias.

Asimismo, es importante que todo el gobierno relativo a riesgos ciberfísicos en las infraestructuras críticas se transmita claramente a su cadena de suministro, donde los diferentes TIER deberán aplicar de manera ágil los requerimientos de los primeros para que todos los servicios y/o productos que presten estén libres de vulnerabilidades y amenazas.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Tendemos a separar las amenazas del mundo físico de las del mundo lógico y a tratarlas de manera independiente; pero la actual transformación digital ya ha comenzado a poner de manifiesto que una amenaza física puede explotar una vulnerabilidad de un sistema IT/OT y viceversa.

La concienciación que se está creando sobre la digitalización de las personas, procesos y modelos de gobierno de las *smart cities* e Industria 4.0 afecta de lleno a los servicios esenciales que prestan las infraestructuras críticas y otros sectores que, sin ser considerados infraestructuras críticas, son de vital importancia en nuestro día a día.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

RKL dispone de un equipo de profesionales formados y desarrollados durante los últimos 25 años en las cuatro áreas principales de la seguridad integral.

La Ley PIC y la Directiva Europea NIS exigen la implantación de planes estratégicos y específicos a las infraestructuras críticas designados por el CNPIC mediante el desarrollo de los planes de seguridad operativos y planes de protección específicos; pero en RKL Integral vamos mucho más allá, mediante la posibilidad del despliegue de servicios y soluciones operables.

En consultoría, estos servicios son la base del diagnóstico y planificación de la seguridad integral que ayuda a alinear objetivos estratégicos y operativos de nuestros clientes.

En ingeniería ofrecemos servicios profesionales para el diseño e implementación de soluciones de seguridad integral y TIC que permiten a nuestros clientes aplicar las mejores soluciones. También contamos con soluciones SaaS para la explotación, operatividad y certificación de los diferentes planes exigidos por la ley.

Y, por último, cabe destacar VES PaaS, un *software* desarrollado por RKL Integral en un proceso de I+D+i testado mediante pruebas de concepto (PoC) para operar en tiempo real los riesgos ciberfísicos de infraestructuras críticas.

Conseguimos que todos esos planes sean operativos, certificables y resilientes en un entorno de seguridad integral, donde los mundos físicos y lógicos estén cada día más unidos.

Más información en:
rklintegral.com

José María Sanz Yarritu
CEO Y FUNDADOR

Los riesgos ciber físicos de tu empresa son una prioridad.

Te ayudamos a identificar, proteger, detectar, responder y recuperar desde una perspectiva global de las amenazas físicas y lógicas que pueden impactar en tu empresa, profundizando en las Tecnologías de la Operación (OT).

Consultoría

Ingeniería

Automatización de Procesos

VES PaaS

RKL integral

+34 946 40 10 11
contacta@rklintegral.com
rklintegral.com

Safety&Security
Cyber Physical
Threat Management

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Por nuestra experiencia en este último año tan complejo, debemos estar preparados y prevenidos para que continúe aumentando de manera progresiva la actividad cibercriminal, alimentada por las prematuras transformaciones digitales y acrecentada por la sofisticación y automatización de las técnicas empleadas por los ciberdelincuentes.

Para el sector, el gran reto consistirá en incrementar nuestras capacidades proactivas, así como de inteligencia de amenazas; es decir, tratar de adelantarnos en la medida de lo posible a este tipo de ataques, mejorando también aquellas capacidades de detección y reacción para mitigar daños y reducir impactos.

Estamos convencidos de que el sector de la ciberseguridad, apoyado en una colaboración público-privada cada vez mejor estructurada, continuará desarrollándose para adaptarse a estos retos y estar cada vez mejor posicionado y con una mayor capacidad de respuesta.

Por otro lado, también nos enfrentamos a un reto importante a la hora de encontrar talento y fomentar la diversidad en una situación de gran déficit y escasez de profesionales dentro del sector.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

En particular, habrá que estar particularmente prevenidos contra tres tipos de ataque que ya hemos sufrido en los últimos años y que continuarán su tendencia ascendente. Los primeros son los ataques de *phishing*, que utilizan el envío masivo de millones de correos electrónicos con ficheros que contienen *malware* muy avanzado. Además, cuentan con múltiples herramientas para conseguir una rápida propagación por las redes empresariales y así poder llegar a secuestrar infraestructuras y datos críticos para la continuidad de negocio de las empresas afectadas. El objetivo último, más allá de la disrupción del servicio que pueden buscar los ataques auspiciados por naciones Estados que contemplen objetivos sociopolíticos, seguirá siendo la petición de rescates a cambio de supuestamente proporcionar las claves que permitan recuperar la infraestructura y datos afectados.

En segundo lugar se encuentra el aumento de los ataques de *Ransom Distributed Denial of Service* que afectan a las grandes empresas, con la amenaza de repercutir también en sus servicios *online* de forma masiva y continuada si no se accede al pago de la cifra que pidan a modo de extorsión.

Y por último, el crecimiento de los ataques que afecten a terminales móviles como siguiente "eslabón más débil" de las organizaciones y como objetivo de ataque desde el cual conseguir credenciales de usuario y/o datos bancarios para poder utilizar en posteriores acciones fraudulentas.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

Llevamos más de 20 años ayudando a nuestros clientes en todas las fases de sus programas de ciberseguridad: desde identificar amenazas y riesgos, integrar planes de protección y activar planes de detección de ataques hasta dar respuesta a los mismos y gestionar la actividad de recuperación y respuesta.

Tenemos un equipo tremendamente cualificado y un porfolio de soluciones muy amplio. Desde S21sec tratamos de ofrecer una visión holística e innovadora sobre cómo maximizar las inversiones en ciberseguridad.

Más información en:
www.s21sec.com/es/

Lucila Kominsky
VP STRATEGIC MARKETING

S21 SEC

CYBERSECURITY YOU CAN TRUST

Ciberseguridad 360°

Acompañamos a nuestros clientes en todas las fases de sus programas de ciberseguridad, gracias a nuestro portfolio amplio y completo junto con el personal más especializado y cualificado del sector con más de 25 años de experiencia.

PROTEGE A TU EMPRESA DE LOS CIBERATAQUES

Desde S21sec ayudamos a securizar las organizaciones de los ciberataques más peligrosos y complejos de manera rápida y eficiente.

Malware

Phishing

Ransomware

RRDoS

Hacktivismo

Desinformación

APTs

Vulnerabilidades

Brechas de seguridad

www.s21sec.com

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?
Cada día surgen nuevas fórmulas para acceder a datos corporativos por parte de terceros. El *malware* para versiones móviles está muy extendido, pero también existen filtraciones de datos corporativos a través de troyanos o ataques DoS.

La crisis del COVID-19 ha extendido la adopción del puesto de trabajo digital. Según un estudio realizado por IPSOS para Samsung, un 36 por ciento de los españoles ha teletrabajado durante el confinamiento y la ciberseguridad ha sido un desafío: un 48 considera que existen mayores riesgos en este nuevo escenario laboral.

Las empresas deben ser conscientes de que la transformación digital no solo consiste en la adquisición de terminales. Los profesionales deben estar cualificados para desarrollar su productividad con nuevas herramientas digitales y evitar posibles brechas de seguridad. Las compañías se encuentran ante el gran reto de proteger el *hardware* y el *software* de sus equipos, y cada vez es más necesario tener una única solución integral que ofrezca la máxima seguridad: desde la etapa de producción hasta la integridad del *software* y las aplicaciones.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?
Este año, nuestras relaciones serán principalmente digitales y vamos a estar conectados a todo tipo de dispositivos. Los modelos Galaxy incluyen una amplia gama de soluciones de seguridad para proteger los datos personales. Samsung Knox aísla y protege los datos desde el *hardware*, mientras que WiFi Segura proporciona un entorno seguro para navegar por Internet en conexiones inalámbricas públicas. Y en caso de pérdida o robo, Find My permite a los usuarios ubicar de forma remota el *smartphone*, así como hacer copias de seguridad y proteger los datos almacenados.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?
Somos el único fabricante de dispositivos que adopta una estrategia amplia e integral para garantizar la seguridad de nuestros dispositivos. Todo ello gracias a Samsung Knox –nuestra plataforma de seguridad– y tecnologías de vanguardia como el chip de seguridad más fuerte de la industria, el elemento seguro integrado (eSE) y un procesador seguro para proteger contra ataques físicos; además de Knox Vault, que agrega otra capa de seguridad.

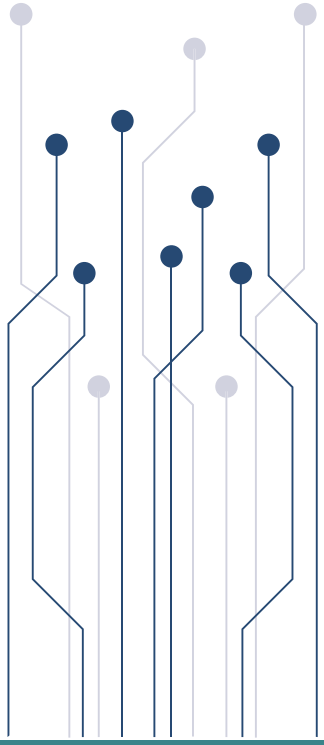
Por otra parte, con Samsung Knox Suite damos cobertura a la necesidad completa de una compañía en términos de seguridad y gestión del ciclo de vida del dispositivo. De esta forma, ofrecemos con una única licencia una gama completa de soluciones de seguridad, gestión de políticas, control de las versiones del sistema operativo y registro automático de la flota completa de terminales de la empresa. Gracias a una experiencia de usuario unificada entre las consolas de los distintos servicios y al acceso Single Sing On, las gestiones de TI pueden ser más productivas y se puede trabajar con unas herramientas sencillas e intuitivas.

Por último, nuestros usuarios de dispositivos Galaxy pueden estar seguros, ya que recibirán actualizaciones de seguridad regulares durante un mínimo de cuatro años después del lanzamiento inicial. Al extender el soporte para las actualizaciones de seguridad que se realizan mensual, trimestral o semestralmente, ofrecemos a los usuarios la tranquilidad de saber que sus datos estarán siempre protegidos mientras utilizan su Galaxy.

Más información en:
www.samsung.com/es

SAMSUNG

David Alonso
DIRECTOR DE EMPRESAS



SAMSUNG

Knox Suite

Proteger | Implementar | Administrar

La solución todo en uno para los dispositivos móviles de su empresa

Seguridad de grado de defensa

Fácil configuración y utilización

Manejo sencillo e inteligente

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Como gestor de riesgos sanitarios, desde Sham (grupo Relyens) trabajamos para fomentar una cultura de prevención en ciberseguridad para el sector sanitario español. Se trata de un aspecto crucial. Y es que la digitalización del sector ha incrementado los ciberriesgos, hasta el punto de convertirlos en una amenaza directa para la seguridad del paciente.

Así, el principal reto es incorporar la gestión del ciberriesgo como uno de los procesos críticos al más alto nivel de las organizaciones. Para ello, es necesario considerar la ciberseguridad en cualquier proceso tecnológico o de innovación, para abordarla desde su diseño y aumentar el presupuesto, de tal forma que hayamos reforzado la seguridad de los dispositivos conectados. Una estrategia a la que hay que añadirle un refuerzo necesario de la formación, tanto de usuarios como de los equipos técnicos.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Centrándonos en el sector sanitario y sus últimas tendencias, especialmente ahora con la actual pandemia, es previsible que continuemos con los ataques dirigidos a los datos y la operación sanitaria. El principal objetivo de los atacantes es conseguir un beneficio económico; y para ello, utilizan principalmente dos fórmulas: robo de datos personales de salud y cifrado de la información, paralizando así su operativa y exigiendo un rescate que permita recuperar los datos y continuar con la atención a los pacientes. Además, los datos de investigaciones médicas o los relacionados con las vacunas también son un objetivo, como hemos podido ver con el ataque a la Agencia Europea del Medicamento.

El teletrabajo y la presión en el sistema hospitalario son otros aspectos que incentivan a los ciberdelincuentes a tratar de acceder a sistemas de información mediante ingeniería social y *phishing* para introducir *malware* en los sistemas. En 2021, además, veremos evolucionar los ataques de *ramsomware* a otros más sofisticados y dirigidos. De hecho, ya estamos viendo ejemplos como Egregor Ramsomware, *malware* que ha afectado este mismo año a centros sanitarios en Francia.

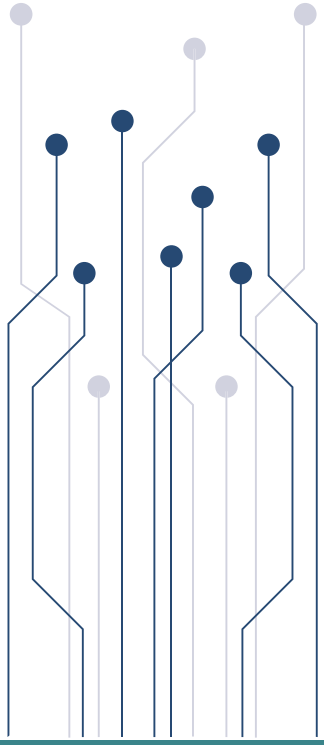
¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

Lo hacemos a través de una respuesta preventiva, gracias a nuestra alianza con CyberMDX. Se trata de una solución de ciberseguridad, específicamente diseñada para el ámbito sanitario, que permite identificar y clasificar todos los activos conectados a la red en tiempo real, incluidos los dispositivos médicos, además de detectar vulnerabilidades y el riesgo de los equipos. Así puede detectar tráfico y conexiones indebidas, alertando de un posible ataque en las etapas iniciales y proponiendo las actuaciones de mitigación y control necesarias. Hay que tener en cuenta que materiales como los dispositivos médicos son muy vulnerables en las redes hospitalarias. Igualmente, las soluciones de ciberseguridad generalistas tienen dificultades para inventariar y gestionar estos activos sensibles. Por ello, como el riesgo cero no existe, hemos lanzado Sham Cyber Protection, un ciberseguro con el que queremos acompañar a nuestros clientes en la gestión de todos sus riesgos, más allá de los "tradicionales", ofreciéndoles una mejora de sus procesos de seguridad y ayudándoles a reforzar la seguridad del paciente.

Más información en:
www.sham.es

sham
SEGUROS Y GESTIÓN DE RIESGOS
una sociedad del grupo relyens

Laura Prats
CYBER RISK MANAGER EN ESPAÑA



¿Cuáles serán las ciberamenazas que predominen este año y cómo ayuda su empresa a los usuarios a abordar sus necesidades de seguridad?

La pandemia hizo en 2020 que todas las predicciones de ciberseguridad que se hicieron para ese año quedaran alejadas de la realidad debido a todos los cambios que surgieron, principalmente en entornos laborales, a raíz de este hecho.

Esto condiciona también las tendencias de la ciberdelincuencia y principales retos de la ciberseguridad en 2021. Entre ellas, desde S2 Grupo podemos destacar la enorme incidencia de los ataques de *ransomware*. Por eso, es esencial contar con sistemas que nos protejan, como Microclaudia. Esta herramienta diseñada por S2Grupo y el Centro Criptológico Nacional pretende vacunar todos nuestros equipos e inmunizarlos contra estas amenazas.

Asimismo, cabe mencionar el mantenimiento del teletrabajo. Esto hace que se tenga que reforzar la ciberseguridad de las empresas, los dispositivos personales y los hogares. Otro de los objetivos directos de los ciberdelincuentes serán los sistemas de videoconferencias, Dropbox, mensajería, etc. Y habrá una mayor presencia de *malware, phishing, scam* y dominios "Covid" registrados.

También será relevante el ciberespionaje, sobre todo el relacionado con las vacunas e investigaciones sanitarias. Y cada vez se están dando más ciberataques muy sofisticados contra la cadena de suministro.

Más información en:
s2grupo.es

S2 GRUPO
Anticipando un mundo ciberseguro

Rafa
Rosell Tejada
DIRECTOR COMERCIAL

Nos hemos reinventado para ti

red seguridad
www.redseguridad.com

Móvil Responsive
Google Ad Server
Active Campaigne
Marketing Automation
Audiencias de Facebook, Linkedin y Google

TE ESPERAMOS

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Los principales retos, después de la situación de crisis pandémica que estamos viviendo, pueden sintetizarse en tres. El primero de ellos es que las inversiones en tecnología podrán verse afectadas por el impacto económico de la crisis sanitaria del COVID-19 y, por derivada, las inversiones en ciberseguridad. Por esta razón, el cibercrimen puede aprovechar esta situación de "debilidad" para aumentar los ataques. El segundo es que las amenazas y riesgos de ciberseguridad están aumentando, y cada vez la forma de defenderse es mas compleja. Por eso, es importante un control efectivo del perímetro y los activos corporativos. Por último, en una situación extrema como la actual, debemos abrazar medidas extremas. Es fundamental reforzar las medidas de seguridad de la información, poniendo foco en la formación y concienciación al usuario.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Las principales amenazas que predominarán durante los próximos años son las relacionadas con la ingeniería social. Las empresas empezarán a estar más preparadas tecnológicamente y esto empujará, cada vez más, a los ciberdelincuentes a utilizar técnicas de ingeniería social para conseguir eludir los sistemas de defensa.

Por otro lado, los dispositivos móviles también se han convertido en centro de los ataques debido a que cada vez realizamos más actividades de nuestra vida diaria con ellos. Finalmente, el despliegue de *ransomware* seguirá siendo una de las amenazas con mayor impacto.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

En Sothis apostamos por la ciberseguridad como punto de partida de cualquier proyecto tecnológico. No solo damos la solución tecnológica más adecuada a las necesidades de nuestros clientes, sino que la diseñamos y la pensamos con la seguridad en mente desde las fases más tempranas de diseño.

Además, esto nos permite identificar mejoras de seguridad en los entornos de nuestros clientes, aportando una visión integral de la ciberseguridad y no solo enfocada al proyecto a desarrollar. Entendemos el negocio de nuestros clientes, desarrollamos los procedimientos pertinentes e implantamos los cambios necesarios para ayudar a madurar su seguridad.

Entendemos también que se debe abordar de forma progresiva y que los recursos son limitados, por lo que hacemos mucho foco en una primera aproximación que maximice el resultado con el trabajo realizado, de manera que tengamos cubiertas las necesidades más inmediatas y planificando a futuro los siguientes pasos necesarios para mejorar la seguridad.

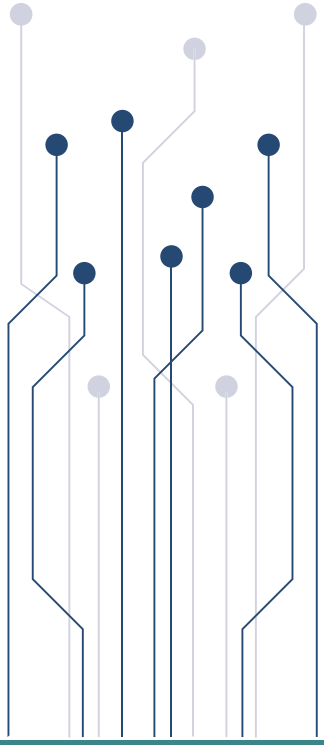
Acompañamos a nuestros clientes en el camino a recorrer, asesorándoles en todo momento y tomando las decisiones conjuntamente, así como valorando el impacto de un posible incidente de seguridad frente a la inversión realizada para minimizarlo todo lo posible. Y no solo en la parte técnica, sino también en la formación de todo el componente humano de la empresa, desde la alta dirección hasta los operarios, pasando por Administración o Recursos Humanos. Podemos manejar gran parte de las amenazas si las personas están informadas de los riesgos y las técnicas que usan los ciberdelincuentes para conseguir engañarles.

Más información en:
www.sothis.tech

sothis

Miguel Monedero Gómez

DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN



sothis

¿Si hubieras sabido que iba a pasar, hubieras actuado de otra forma?

Aún estás a tiempo de hacerlo.

Sothis, Seguridad de la Información.

Gobierno de la Seguridad de la Información

- Análisis de riesgos
- Plan de tratamiento de riesgos
- KPIs & KRIs
- Metodología by Sothis
- Plan director de seguridad
- Oficina de seguridad
- DPO as a service
- CISO as a service
- Cultura de seguridad

Ciberseguridad

- Monitorización amenazas 24x7
- Respuesta a incidentes
- Arquitecturas de protección
- Inteligencia de amenazas
- Formación y concienciación
- Análisis forense digital
- Auditorías y red team
- ISO 27001, ENS, NIST, LEY PIC...
- Plan de continuidad TIC
- Protección de datos
- Clasificar información
- Securización de entorno industrial

CSIRT.es

TF-CSIRT Trusted Introducer

www.sothis.tech

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

El gran reto es, sin duda alguna, consolidar el talento nacional sustanciado en un crecimiento de profesionales dedicados a la ciberseguridad y la ciberinteligencia. Por supuesto que la tecnología es importante, pero más todavía lo es continuar formando y detectando el talento nacional, que lo hay, y mucho.

Además de eso, encarar una internacionalización que permita a la ya bastante madura industria de ciberseguridad española poder ser un referente fuera de nuestras fronteras.

Y, sobre todo, continuar aportando valor en el día a día de las empresas. Debemos ser un compañero de viaje y un aliado, y para eso hay que adaptarse a las necesidades y lenguaje de las compañías.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Sin ninguna duda, el *ransomware* continuará creciendo y teniendo un impacto directo en los incidentes. Esto traerá como consecuencia un aumento de los servicios de ciberseguridad y ciberinteligencia.

Veremos un aumento, o quizás una mayor detección, de ataques sofisticados a infraestructuras críticas y compañías del tejido corporativo español. Pero, ojo, que hay vida más allá del IBEX35, con empresas muy de nicho con un importante *know how* y desarrollo de negocio internacional a las que tenemos que prestar atención.

Veremos también más ciberataques en el ámbito de la toma de decisiones de las compañías, tanto desde el punto de vista del "ciberfraude clásico", como del *bussines email compromise*; así como a ellos directamente por ser un vector de ataque muy interesante para cualquier ciberdelincuente.

Y cada vez tendrá más importancia para las organizaciones lo que suceda con sus proveedores, puesto que en estos residen datos de interés para los ciberatacantes que pueden ser usados para dañar la continuidad de negocio de las empresas.

Un ejemplo de ello son los últimos incidentes de seguridad, donde determinados actores vulneraron la seguridad de servicios *online* relacionados con la ofimática y salvaguarda de archivos. Esto, que se irá repitiendo con bastante frecuencia, es un foco donde las compañías tradicionales van a necesitar ayuda por parte de los proveedores de ciberinteligencia, al objeto de conocer cómo impactan este tipo de hechos en las mismas.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

Mediante un enfoque que aporta valor en el ámbito de la ciberseguridad, midiendo lo que llamamos "riesgo dinámico" de una compañía, que enriquece los servicios tradicionales.

Y también mediante un enfoque proactivo como son los ejercicios de *Red Team* y ciberinteligencia.

Más información en:
www.tarlogic.com

TARLOGIC
CYBERSECURITY EXPERTS

Francisco Javier Rodríguez

DIRECTOR DEL DEPARTAMENTO DE CIBERINTELIGENCIA Y RIESGOS GLOBALES

DOMINA EL JUEGO

PROTEGE TU NEGOCIO

CYBERINTELLIGENCE & GLOBAL RISK

Strategic Corporate Cyberintelligence, Online Piracy & Fraud Investigation, Insider Threat Assessment

www.tarlogic.com

TARLOGIC
CYBERSECURITY EXPERTS

¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

En estos momentos, los principales retos consisten en encontrar un equilibrio entre seguridad y la correspondiente inversión económica, ya que ahora más que nunca debemos de ser capaces de mostrar el valor que aporta la ciberseguridad; proteger el nuevo paradigma laboral, con muchos empleados teletrabajando ya de manera permanente; incorporar nuevas tecnologías de manera segura como *cloud*, DevOps, SaaS, IaaS, PaaS, etc.; y la evolución de sistemas tradicionales, los cuales deben mantenerse activos, pero adaptados a los nuevos tiempos. Este es el caso, por ejemplo, de las tecnologías OT, las cuales, utilizando sistemas obsoletos anteriormente desconectados, ahora comienzan a dotarse de conectividad, con el riesgo que eso supone.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Cabe esperar que la situación sea una evolución de lo experimentado en los últimos años, donde la ciberextorsión continuará siendo la gran protagonista, principalmente en forma de ataques *ransomware*, que, a su vez, se descomponen en subataques.

Y si a esta circunstancia le sumamos que el teletrabajo ha venido para quedarse, los atacantes van a continuar explotando esto para conseguir el punto de entrada que necesitan para iniciar sus ataques, intentando engañar al usuario para que acceda a URL infectadas, ejecuten adjuntos maliciosos o introduzcan sus credenciales corporativas en páginas de autenticación falsas.

Pero el *ransomware* no es la única amenaza que se incrementará en 2021. Otros ataques como el BEC (suplantación de identidad de algún directivo o pieza fundamental de la compañía para conseguir acciones por parte de empleados) continuarán creciendo de manera progresiva aprovechando precisamente el nuevo paradigma laboral.

Por último, no debemos dejar de lado los ataques a infraestructuras OT, ya sean de tipo infraestructura crítica (relacionadas con entidades o servicios gubernamentales) como de carácter privado. Los entornos OT, tradicionalmente aislados en una burbuja desconectada basada en tecnología específica, están evolucionando hacia un modelo híbrido donde se combinan tecnologías IT, IoT y OT donde la conectividad entre dispositivos es la norma. Esta evolución comienza a mostrar serios problemas de seguridad que exponen estas infraestructuras a riesgos anteriormente no existentes.

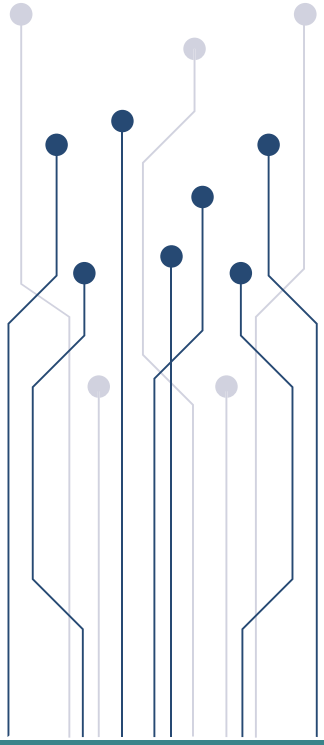
¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

Trend Micro dispone de un porfolio único en el mercado, tanto por cobertura –pues somos capaces de cubrir todos los vectores de ataque posibles (*endpoint*, *cloud*, navegación, *email*, entornos colaborativos, redes privadas/cloud, OT, etc.)–; como por tecnología, ya que combinamos tecnología de última generación junto con la experiencia que nos aporta los más de 30 años de historia de la compañía.

Un claro ejemplo de esta evolución es la tecnología XDR, introducida en el mercado por Trend Micro, la cual aprovecha la información recabada por los distintos vectores (*endpoint*, servidores, correo, red, etc.). XDR extiende las capacidades del EDR tradicional aportando contexto a los ya citados ataques multivector permitiendo a nuestros clientes identificarlos y bloquearlos de manera prematura.

Más información en:
www.trendmicro.es

José de la Cruz
DIRETOR TÉCNICO PARA IBERIA



TREND MICRO™

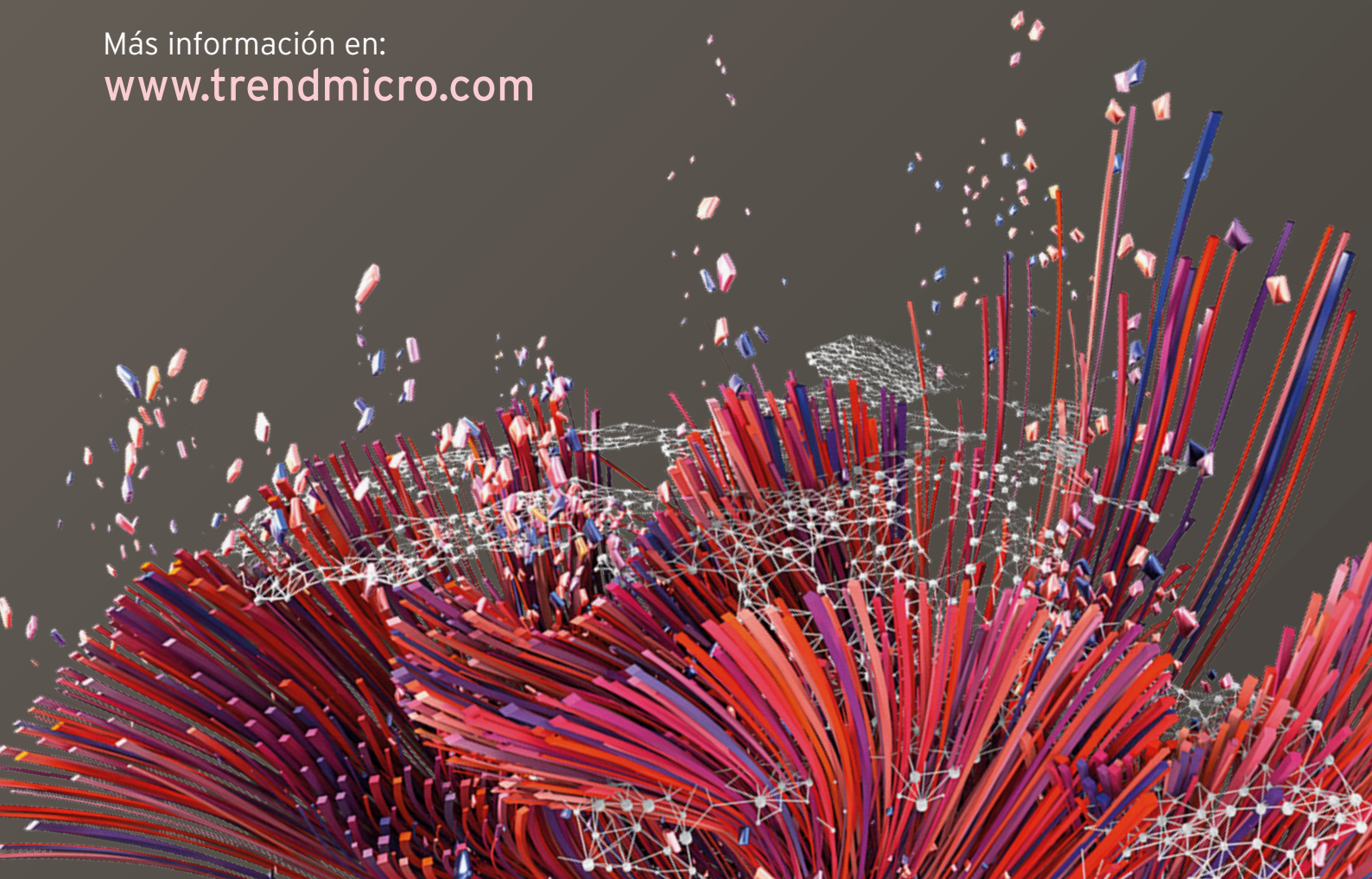
THE ART OF CYBERSECURITY

Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

Una plataforma especialmente diseñada para la defensa contra amenazas que va más allá que otras soluciones XDR

Más información en:
www.trendmicro.com



¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

La ciberseguridad es un ámbito crítico que atañe a nuestro día a día, lo que hace que los retos a los que se enfrenta la industria estén relacionados tanto con el aumento de las amenazas como con la falta de personal cualificado. A esto se le suma la situación provocada por la COVID-19 y el aumento de los entornos híbridos de trabajo.

En este sentido, la industria necesita cada vez más soluciones que simplifiquen la actividad y que trabajen conjuntamente de verdad. También hay una necesidad de entregar soluciones y servicios de seguridad, no únicamente una tecnología de seguridad. Esto está muy vinculado con la propuesta de los proveedores de servicios de seguridad gestionada, una figura que cobra protagonismo de cara poder cubrir las necesidades de seguridad de las empresas. En WatchGuard nos ocupamos de dar una respuesta eficaz a todo esto.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Dentro del panorama de amenazas destacaría el *ransomware*, que ha comprometido millones de dispositivos en todo el mundo y que sigue creciendo de manera alarmante. A esto hay que añadir el *phishing* y sus diferentes modalidades, el *criptomining* y el robo de información.

Por otro lado, la pandemia ha disparado el teletrabajo, lo que ha provocado que los ataques se centren más en el usuario final, con todos los riesgos que eso conlleva.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

WatchGuard es un proveedor de referencia en el mercado que cuenta con 25 años de experiencia y que destaca por ofrecer tecnología que da respuesta a todas las necesidades de seguridad de las empresas. Nuestras soluciones abarcan desde la seguridad de red hasta el *endpoint*, pasando por la autenticación multifactor o la seguridad WiFi.

Desde el punto de vista de las nuevas necesidades a raíz del teletrabajo, destaca la herramienta DNSWatchGo, un servicio de protección de DNS y filtrado de contenido para usuarios en cualquier lugar, independientemente desde dónde se conecten.

Por otro lado, la plataforma de MFA, AuthPoint, ayuda a proteger las credenciales de los usuarios confirmando su identidad cuando tratan de conectarse a la red corporativa, evitando la suplantación de identidad.

Por su parte, la protección del *endpoint* queda cubierta con la potente solución EDR Adaptive Defense 360, que ofrece inteligencia de prevención, detección, visibilidad y adaptación antes, durante y después de un ataque.

Adicionalmente, la solución de Punto de Acceso Remoto da a las empresas la flexibilidad de ampliar el SSID corporativo a lugares de trabajo remoto, manteniendo la productividad y la seguridad de la fuerza laboral remota.

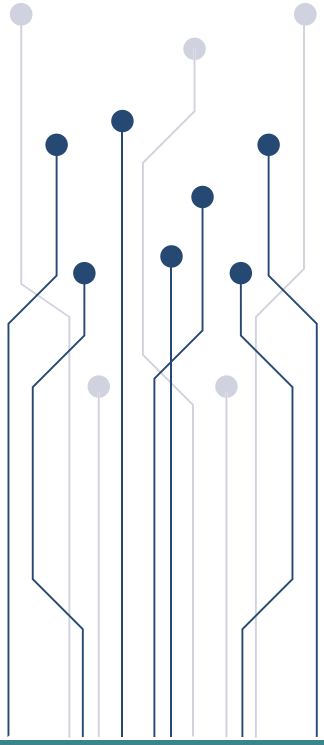
La seguridad que espera de WatchGuard WiFi Cloud puede ahora ampliarse a estas ubicaciones de trabajadores remotos, lo que permite un completo cumplimiento y supervisión del entorno inalámbrico confiable en cualquier lugar.

Del mismo modo, ofrecemos protección para entornos híbridos, donde junto con MFA ofrecemos seguridad de red con nuestros UTM, Firefox que protegen todo el perímetro contra *malware* y otras amenazas, además de toda la seguridad.

Más información en:
www.watchguard.com/es

Guillermo Fernández

MANAGER SALES ENGINEERING



SMART SECURITY, SIMPLY DONE.

SEGURIDAD DE RED • AUTENTICACIÓN MULTIFACTOR • WI-FI SEGURO • SEGURIDAD DE ENDPOINTS

PROTECCIÓN INTELIGENTE

Múltiples servicios trabajan juntos de manera inteligente para prevenir, detectar y responder instantáneamente a los ciberataques con políticas automatizadas, así como supervisar e informar sobre el estado de tu infraestructura de TI.

VISIBILIDAD ACCIONABLE

Las herramientas de visibilidad accionable te permiten identificar amenazas de manera proactiva, al tiempo que proporcionan acciones correctivas contra los problemas conocidos.

GESTIÓN SIMPLIFICADA

Nuestra plataforma de gestión basada en la nube despliega, configura y mantiene tu seguridad de forma rápida y sencilla en múltiples productos de seguridad, empresas y sitios.

PIONEROS EN CIBERSEGURIDAD DURANTE 25 AÑOS.

25 ANNIVERSARY WatchGuard

900 90 70 80

spain@watchguard.com

©2021 WatchGuard Technologies, Inc. Todos los derechos reservados.
N.° de pieza WGCE67463_032221

Herminio del Campo
Director general del Centro de Cooperación Interbancaria

Antonio Ramos
CEO de LEET Security

"El objetivo de Pinakes es aligerar la auditoría de los proveedores del sector financiero"

El Centro de Cooperación Interbancaria y LEET Security acaban de anunciar la puesta en marcha del proyecto Pinakes. Se trata de un servicio destinado a las entidades financieras para facilitar la auditoría de ciberseguridad de todos sus proveedores, tal como les obliga la nueva normativa EBA. Pero este marco de referencia no solo beneficia a las entidades, sino también a los propios proveedores. Herminio del Campo y Antonio Ramos, que han coordinado este proyecto, nos explican sus principales claves.

Por Enrique González

¿Qué actividad desarrolla el Centro de Cooperación Interbancaria, especialmente en lo referido a riesgos y seguridad de las entidades?

Herminio del Campo (HC): El Centro de Cooperación Interbancaria es una asociación sin ánimo de lucro que aglutina a las entidades de depósito que operan en España. Está formado por bancos, cajas de ahorros y cooperativas de crédito. Somos una asociación que trabaja en modo colaborativo, no competitivo.

Nuestros fines son servir de foro para el diálogo y la innovación interbancarios, desarrollar ideas de interés para el sector y ejercer de vehículo para el desarrollo y funcionamiento de los proyectos que las entidades consideren necesarios.

La actividad se vertebra en cuatro grandes áreas: Riesgos, Seguridad y prevención del fraude, Estándares y operaciones y Regulación. Es en la segunda de ellas, a través de la Comisión de Seguridad y Fraude, desde donde se ha abordado esta iniciativa.

Acaban de anunciar la puesta en marcha del proyecto Pinakes. ¿Cuál es el origen de esta iniciativa?

Antonio Ramos (AR): Las primeras conversaciones fueron a finales de 2019. A partir de ahí, constituimos un grupo de trabajo del Centro de Cooperación Interbancaria y durante 2020 trabajamos en la definición del servicio, la preparación del marco contractual, de las relaciones, de las herramientas que hacen falta, etcétera.

El origen del proyecto está en la normativa de la Autoridad Bancaria Europea [EBA, por sus siglas en inglés] que obliga a las entidades financieras a supervisar la seguridad de sus proveedores. Las entidades se han dado cuenta de que, con sus propios medios, solo pueden llegar a un grupo muy reducido de proveedores críticos y buscan una forma más eficiente de dar cumplimiento a ese requisito.

Pinakes será también mejor para los proveedores porque, al fin y al cabo, hablamos de un proceso que aligera muchísimo las necesidades de *due dilligence*. Básicamente porque, en lugar de tener un proceso de este tipo en la parte de ciberseguridad por cada entidad, pasan a tener uno solo.

A grandes rasgos, ¿en qué consiste este proyecto?

HC: Como decíamos, uno de los requisitos de la regulación de la EBA es verificar los niveles de ciberseguridad de los proveedores. Una de las opciones que ofrece la normativa es que las entidades hagan esta verificación mediante una calificación de un tercero externo, y ahí es donde encaja Pinakes.

En el servicio intervienen cuatro actores: el propio *hub*, las entidades adheridas, los proveedores y los evaluadores. Estos últimos son empresas de auditoría que cumplen unos requisitos y que están homologadas por el propio Pinakes.

El flujo del proceso comienza cuando la entidad financiera va a contratar un servicio con un proveedor. En ese caso, una de las opciones que tiene la entidad para verificar la seguridad de su proveedor es pedirle su calificación en el *hub*. Es el propio proveedor el que, una vez consultado a Pinakes qué evaluadores están homologados, elige y contrata a aquel que es de su elección en una relación bilateral ajena al *hub*.

La empresa elige al auditor que quiera y tendrían un contrato al margen del *hub*. En el momento en el que haya finalizado la auditoría, el propio proveedor presentará el resultado y, con ello, se le otorga una calificación.

Dicha calificación la publicamos en la plataforma que da soporte a todo el servicio y estaría a disposición de todas las entidades adheridas, de manera que pueden saber qué proveedores tienen determinada calificación para un servicio concreto. Es decir, el proveedor no tiene que volver a pasar por el proceso de calificación en caso de que otra entidad financiera adherida a este servicio quiera contratar el servicio auditado.

¿Qué criterios tiene que cumplir un evaluador para formar parte de Pinakes?

AR: Básicamente, hemos hecho un esquema de homologación equiparable al que ha propuesto la Comisión Europea para la certificación de seguridad en *cloud* o al que pide la autoridad de Luxemburgo para la certificación de protección de datos. Es un marco que coge lo mejor de los dos mundos, que es, por un lado el ISAE 3000, que es un estándar que permite emitir los informes de tipo SOC 2; y por otro lado, la ISO 17065, que permite la certificación de producto y es la que utiliza el Esquema Nacional de Seguridad como marco de referencia. Juntando esos dos mundos, hemos creado un marco de condiciones que tienen que cumplir los evaluadores, que abarca competencias, responsabilidad sobre los informes emitidos, independencia respecto de los clientes, capacitación del personal que realiza las funciones, permitir la supervisión por parte del *hub* y de las entidades financieras, así como el supervisor, etcétera.

Estamos viendo que las entidades que estarán dentro de este esquema son las auditoras que conocemos típicamente, como las Big Four más todas las que están haciendo en España informes de tipo SOC 2.

Aparte de eso, también como LEET Security, optaremos a esa homologación por tener la condición de certificadora 17065 y además estar reconocida por ENISA para aspectos de seguridad.

¿Cuál será el papel de LEET Security una vez puesto en marcha el proyecto?

AR: Este es un tema que hemos revisado con mucho cuidado por temas de competencia. Por un lado, LEET Security es la licenciataria de la metodología de evaluación, lo que conlleva una serie de trabajos relacionados con el mantenimiento y la evolución del referencial. Y por otro, actuaremos como evaluador homologado en las mismas condiciones que el resto. A partir de ahí, somos uno más en la ecuación.

> "Pinakes proporciona la evaluación más completa posible de todos los aspectos de ciberseguridad de los proveedores de entidades financieras"

Además de formar parte de Pinakes, ¿las entidades financieras llevarán a cabo otro tipo de contrataciones o evaluaciones con terceros para mantener cierta independencia del proyecto?

AR: Hay que tener en cuenta que el servicio de Pinakes sirve para la evaluación de aspectos de ciberseguridad. Pero cuando una entidad hace un proceso de *due dilligence*, tiene que incluir otros aspectos en la ecuación, no solo ciberseguridad. Lo que busca el *hub* es aligerar esa parte del proceso, pero las entidades financieras tendrán su toma de decisión y su proceso de *due dilligence* que deberá ser más completo.

Herminio del Campo.

Además pueden existir aspectos concretos que la entidad quiera revisar de manera puntual. Por ejemplo, hemos visto entidades que requieren a sus proveedores que tengan unas VPN configuradas a través de unos dispositivos de una marca y manera concretas para una determinada interconexión.

No obstante, la adhesión de las entidades Pinakes se hace para aceptar la evaluación que salga de Pinakes, con independencia de que luego puedan hacer auditorías adicionales.

¿Qué van a evaluar de un proveedor?

AR: Nos hemos basado en el marco que teníamos ya en LEET Security, que llevamos probando cinco años, y hemos añadido los requisitos de todas las entidades para construir un referencial más completo. Se van a evaluar desde aspectos genéricos, como pueda ser el sistema de gestión que tenga implementado el proveedor, pasando por aspectos de operación de seguridad, seguridad personal, seguridad de las instalaciones, protección frente a *malware*, continuidad y contingencia, desarrollos seguros, gestión de incidencias, criptografía, monitorización... Es decir, la evaluación más completa posible de todos los aspectos de seguridad.

Siguiendo la filosofía de la calificación, hemos establecido para la evaluación 14 dominios, 76 secciones y en torno a 350 capacidades distintas de seguridad. Lo que se evalúa son cada una de esas 350 capacidades y en esos resultados se basa Pinakes para construir la calificación final. No todas las capacidades aplicarán en todos los casos, obviamente; por ejemplo, si se trata de un servicio que no conlleva desarrollo, pues el desarrollo no se evalúa.

Si hubiera un incidente de ciberseguridad con alguno de los proveedores adscritos a Pinakes, ¿qué papel desempeñaría el *hub*?

AR: Las propias entidades financieras nos han pedido que pudiera haber un punto único de información para simplificar el acceso al estado más actualizado posible de un incidente. Pinakes no pretende actuar ni como CERT ni como mecanismo de coordinación a respuesta de emergencias, pero queremos es simplificar el acceso a la información. Lo que nos dicen las entidades es que han tenido situaciones en el pasado donde un proveedor que daba servicio a 25 entidades ha tenido un incidente. Qué ocurre, que hay 25 personas llamando al responsable de ese proveedor para preguntarle cómo está el incidente y al final no da abasto para atender al teléfono. Por eso buscamos un punto donde podamos tener un report actualizado de cómo está ese incidente y luego ya habrá que llamarle y preguntarle dudas puntuales. Pero no hará falta llamarle simplemente para que nos dé un status; para eso se pueden conectar a la web y ver cómo está la situación. Así descargamos un poco al proveedor y le dejamos centrarse en resolver el incidente, que es lo verdaderamente importante de estas situaciones.

Antonio Ramos.

HC: Seremos cuidadosos en ese aspecto porque hay proveedores con cláusulas de confidencialidad firmadas con sus propios clientes y ahí no podemos entrar.

¿Cuál será la vigencia de las calificaciones?

HC: La calificación tiene una vigencia temporal de un año y aparejado a la calificación están los servicios de coordinación de la información y de monitorización de incidentes.

AR: Durante la vigencia de la duración del contrato de la calificación habrá por parte de Pinakes una supervisión del nivel de seguridad digital. Está basada en los típicos raiting de IP de huella en Internet del proveedor, y lo que se va a hacer es una vigilancia, una monitorización exhaustiva de cada uno de los proveedores que estén formando parte de Pinakes para que, si se produce una modificación significativa de su nivel de calificación, el equipo de gestión Pinakes se pueda poner en contacto con él para preguntarle qué está pasando. Porque lo que se busca no es solo la calificación inicial, sino también la supervisión y la vigilancia, que es otro de los requisitos de la EBA. ■

VISIBILITY

agencia digital

VISIBILITY

La agencia que
revoluciona el marketing digital

Te ayudamos a vender más
Comunicando. Fidelizando. Visualizándote

Servicios: redes sociales, SEO y conversión CRO, email marketing, webs, e-commerce y marketplaces, Facebook y programática, planificación en medios digitales de Google.

BORRMART

Grupo Borrmart S.A.
C/ Don Ramón de la Cruz, 68 - 6º. 28001. Madrid. Tel.: 911976047. visibility@borrmart.es

A3Sec

Integrador
a3sec.com

Grupo empresarial especializado en soluciones de monitorización, inteligencia de negocio y ciberseguridad. Mediante estas últimas, apoya en minimizar los impactos contra su información e infraestructura tecnológica mediante servicios soportados en tecnologías como *Big Data* y *cloud*.

Aiuken

Fabricante/integrador
www.aiuken.com/es

Multinacional de origen español orientada al desarrollo de soluciones de ciberseguridad para medianas y grandes corporaciones. Ofrece servicios de identificación de amenazas, detección, respuesta a incidentes, administración y gestión de plataformas tecnológicas.

Akamai

Fabricante
www.akamai.com

Cuenta con una amplia cartera de soluciones de seguridad perimetral, rendimiento web y móvil, acceso empresarial y distribución de vídeo. Su oferta está respaldada, además, por un servicio de atención al cliente, análisis y supervisión ininterrumpida.

Aruba

Servicios
www.arubanetworks.com

Proveedor de soluciones de redes de próxima generación para cualquier empresa. Ofrece soluciones de seguridad TI que ayudan a usuarios expertos en dispositivos móviles que confían en aplicaciones basadas en la nube en su vida laboral y personal.

AT&T Cybersecurity

Servicios
cybersecurity.att.com

Entre sus productos y servicios se encuentran recursos para construir un programa de seguridad unificado, evaluación de la postura cibernética basada en el riesgo y escaneo rápido de sistemas y aplicaciones para identificar posibles exposiciones.

Atos

Servicios
www.atos.net/es

Compañía de transformación digital que permite vivir, trabajar y desarrollarse de manera sostenible y con confianza en el espacio de las tecnologías de la información. Cuenta con experiencia en sistemas críticos, y por ello, proporciona seguridad a sus clientes.

Auren

Consultoría/legal
www.auren.com/es

Firma de servicios profesionales de auditoría, asesoría legal y fiscal, consultoría y *corporate*. A través de su servicio de auditoría, ayuda a las entidades a gestionar sus riesgos y a mejorar la calidad de la información económico-financiera y de la no financiera.

Bitdefender

Fabricante
www.bitdefender.es

Fabricante global de soluciones de seguridad TI. Cuenta con más de 20.000 *partners resellers* cualificados. Ofrece productos de seguridad e Inteligencia Artificial sobre amenazas para personas, hogares, empresas y sus dispositivos, redes y servicios en la nube.

Blueliv

Fabricante/integrador
www.blueliv.com

Proveedor de inteligencia de ciberamenazas. Sus herramientas y servicios detectan amenazas externas sofisticadas en tiempo real y permiten identificar enemigos, conocer los vectores y patrones de ataque preferidos y proteger la organización de fuera hacia adentro.

Capgemini

Servicios
www.capgemini.com

Multinacional de servicios de consultoría, tecnología y transformación digital. Presta servicios de protección en la nube, *compliance*, identidad, simulación de ciberataques, gestión de identidad y acceso, pruebas de seguridad y prevención del fraude.

Check Point

Fabricante
www.checkpoint.com

Check Point ofrece una arquitectura de seguridad multinivel que protege la información de las empresas almacenada en la nube, en la Red y en los dispositivos móviles, además de un sistema de gestión de la seguridad completo e intuitivo.

Cipher

Integrador
cipher.com/es

La división de ciberseguridad de Prosegur, Cipher, presta una amplia variedad de servicios: detección y respuesta gestionada; seguridad gestionada; ciberinteligencia; *Red Team*; gestión, riesgo y cumplimiento; e integración de tecnología de ciberseguridad.

Cisco

Fabricante/distribuidor
www.cisco.com

Esta multinacional cuenta con herramientas como *firewalls* de última generación, protección frente a *malware* avanzado, *email security*, seguridad de puntos terminales, seguridad de las cargas de trabajo, autenticación de varios factores y *Threat Response*.

Cymulate

Fabricante
cymulate.com

Plataforma de validación continua de la seguridad que permite conocer el nivel de seguridad corporativa. Realiza miles de ataques de manera automatizada, exponiendo las brechas de seguridad y proporcionando las mitigaciones necesarias.

Cyrity

Consultoría
www.cyrity.com

Ofrece servicios de inteligencia de riesgos que ayudan a respaldar los procesos de toma de decisiones relacionados con las amenazas. Su objetivo es generar inteligencia imparcial y procesable que permita a sus clientes ingresar en un nuevo paradigma de seguridad.

Deloitte

Consultoría
www2.deloitte.com

Brinda un modelo global de servicios de ciberseguridad que conecta, en una única red, más de 30 centros operativos en todo el mundo. Cuenta con más de 90 equipos especialistas a nivel global que dan servicio 24/7 a cientos de clientes.

Devo

Servicios
www.devo.com

Especializada en análisis de seguridad y registro nativa de la nube, su plataforma ofrece visibilidad en tiempo real, análisis, escalabilidad, multipropiedad y bajo coste. Todo ello, con el objetivo de monitorear y asegurar las operaciones corporativas según se cambian al *cloud*.

Double Security

Servicios
www.double-check.es

Double Security Technologies está enfocada en la innovación tecnológica en el sector de la criptografía, manejo de identidad y acceso del usuario. Gracias a su solución DoubleCheck, cada usuario podrá generar las claves necesarias para cada operación segura.

ElevenPaths

Fabricante/integrador
www.elevenpaths.com

División de negocio de Telefónica Tech especializada en ciberseguridad. Se trata de un proveedor de servicios de seguridad gestionada inteligente enfocado en la prevención, detección y respuesta con el fin de disminuir los ataques y de proteger los servicios digitales.

Eulen Seguridad

Servicios
www.eulen.com

Compañía de servicios de seguridad privada que también se ha especializado en ciberseguridad. Su oferta cubre todas las necesidades de seguridad en el ámbito de la gestión corporativa y en los sistemas de control utilizados en entornos industriales.

Everbridge

Servicios
everbridge.es

Compañía de *software* global que proporciona aplicaciones de *software* corporativo que automatizan y aceleran la respuesta operativa de las organizaciones a eventos críticos. Así se mantienen seguras las personas y las empresas funcionan más rápido.

everis

Servicios
www.everis.com

Ofrece un enfoque integral de la ciberseguridad con el fin de promover una ciberseguridad proactiva, identificando y gestionando los riesgos para los ciudadanos, las empresas y los gobiernos. Lidera ambiciosos proyectos de ciberseguridad en todo el mundo.

Exclusive Networks

Integrador/distribuidor
www.exclusive-networks.com

Distribuidor de valor agregado especializado en ciberseguridad y transformación *cloud*. Es especialista global en infraestructura digital de confianza que impulsa la transición hacia un futuro digital totalmente fiable para todas las personas y organizaciones.

EY

Consultoría
www.ey.com/es_es

El área de Ciberseguridad de EY está estructurado en cinco pilares estratégicos. Entre ellos, estrategia de ciberseguridad, gestión de riesgos, cumplimiento normativo y resiliencia; protección de datos y privacidad; y gestión de identidades y accesos.

FireEye

Fabricante
www.fireeye.com

Ayuda a las empresas a protegerse de las ciberamenazas. Entre sus soluciones se encuentran una plataforma unificada de operaciones de seguridad, de protección del puesto de trabajo y del correo electrónico. Además, evalúa y responde incidentes.

Forcepoint

Fabricante
www.forcepoint.com

Esta compañía ofrece un enfoque orientado a los sistemas para la detección y el análisis de amenazas internas, protección de aplicaciones y usuarios basados en la nube, defensa de redes de última generación, seguridad de datos y visibilidad de sistemas.

Fortinet

Fabricante
www.fortinet.com

Fortinet protege empresas, proveedores de servicios y organizaciones gubernamentales. Brinda a sus clientes una protección inteligente y sin fisuras en la superficie de ataque. Más de 500.000 consumidores de todo el mundo confían en sus soluciones.

G-Data

Fabricante
www.gdata.es

G-Data es una multinacional con una dilatada experiencia en el desarrollo de soluciones de seguridad informática especializada en la protección *online*. Ofrece soluciones de seguridad tanto para organizaciones como para usuarios particulares.

Global Technology

Integrador/consultoría
www.globalt4e.com

Esta compañía ayuda a las organizaciones a proteger sus activos críticos de las amenazas más comunes, aportando técnicos altamente cualificados y tecnología probada con el objetivo de minimizar el riesgo de sufrir incidentes de alto impacto.

Google

Servicios
www.google.es

Empresa subsidiaria de la multinacional estadounidense Alphabet. Google ha impulsado su apuesta por la ciberseguridad a través de la formación y desarrollo de tecnologías. Cuenta, además, con un programa de aceleración de *startups* de ciberseguridad.

Grupo ICA

Servicios
www.grupoica.com

Empresa española especializada en transformación digital, ciberseguridad, infraestructuras e integración TIC, y servicios profesionales y *outsourcing*. En ciberseguridad, ofrece servicios relacionados con la prevención, la monitorización, la mitigación y la contención.

Guardicore

Fabricante
www.guardicore.com

Empresa de seguridad de centros de datos y nube. Protege los activos corporativos al utilizar controles de microsegmentación flexibles, de rápida implementación y sencillos de comprender. Sus soluciones garantizan una seguridad persistente y consistente.

HP

Fabricante
www8.hp.com/es/es

Ofrece *hardware* y soluciones empresariales como *software*, servicios y seguridad. En este último, está especializada en dos áreas: seguridad informática, con funciones de protección reforzadas por *hardware*; y seguridad de la impresión, para proteger estos entornos.

IBM

Fabricante
www.ibm.com/es-es

Entre sus divisiones se encuentra IBM Security, especializada en el ámbito de la seguridad. Esta ofrece su experiencia en gestión de identidades, inteligencia de amenazas, protección contra el fraude, orquestación, seguridad en *cloud*, etc.

Icraitas

Servicios
www.icraitas.com

El objetivo principal de Icraitas es proteger el negocio, asegurando sus principales activos: la información, los procesos y las personas. Para ello, ofrece servicios en tres áreas específicas, como son la ciberseguridad, el *compliance* y la formación.

Iman Seguridad

Consultoría/distribuidor
www.imancorp.es

Sus servicios de ciberseguridad están destinados a minimizar los riesgos de seguridad para que las empresas se centren en su negocio y aumenten su competitividad. Brinda servicios de auditoría, consultoría, integración, seguridad gestionada, *outsourcing* y SOC.

Ingecom

Distribuidor
www.ingecom.es

Fundada en 1996, esta empresa se centra en servicios críticos para las organizaciones, como el control, monitorización y seguridad de los sistemas de información. Además, proporciona soluciones probadas y homologadas a los integradores de seguridad.

Innotec-Entelgy

Servicios
www.entelgy.com

La división Entelgy Innotec Security proporciona las soluciones y la inteligencia necesarias para prevenir y proteger de ciberataques y brechas de seguridad. Para ello, cuenta con un equipo de 400 expertos que dan servicio a más de 250 clientes.

Ireo

Integrador/distribuidor
www.ireo.com

Esta empresa actúa como una extensión de los fabricantes que tiene en cartera aportando valor en cada fase del ciclo de venta. Cuenta con un amplio catálogo de soluciones y servicios de fabricantes internacionales especializados en ITSM y seguridad.

Isdefe

Servicios
www.isdefe.es

Ingeniería de Sistemas para la Defensa de España (Isdefe) es una empresa pública especializada en ofrecer soluciones de protección y seguridad a la Administración Pública mediante servicios de ingeniería, consultoría y asistencia técnica.

Kaspersky

Fabricante
www.kaspersky.es

Kaspersky ofrece soluciones y servicios de seguridad destinados a proteger empresas, infraestructuras críticas, gobiernos y consumidores de todo el mundo. Cuenta con una amplia cartera de productos dirigidos a luchar contra toda clase de ciberamenazas.

KPMG

Consultoría
home.kpmg

Con más de 4.000 profesionales ubicados en 16 oficinas situadas en España, la consultora KPMG presta servicios de auditoría, fiscales, legales y de asesoramiento en fusiones y adquisiciones, reestructuraciones; así como consultoría de riesgos y de negocio.

Lidera

Distribuidor
www.lidera.com

Especializada en el ámbito de la ciberseguridad desde hace más de 20 años, Lidera ofrece distribución tecnológica a proveedores de servicios, compañías de telecomunicaciones y proveedores de soluciones TIC de todos los segmentos.

Logicalis

Servicios
www.es.logicalis.com

Proveedor internacional de soluciones tecnológicas orientado a ofrecer servicios que van desde la modernización del *data center* y el *cloud* hasta la administración de las operaciones de TI, las estrategias de datos e información y la seguridad e infraestructura de redes.

McAfee

Fabricante
www.mcafee.com/es-es

Con el lema "soluciones de ciberseguridad desde los dispositivos hasta la nube" se presenta la oferta de productos de la compañía norteamericana McAfee, con soluciones dirigidas tanto para usuarios particulares como para empresas de cualquier tamaño.

Microsoft

Fabricante
www.microsoft.com

Entre otras soluciones, esta compañía ofrece servicios de seguridad inteligente, que agrupa sus propuestas para la administración de identidades y acceso, la protección de la información contra amenazas y la salvaguarda de la información en la nube.

Mnemo

Consultoría
www.mnemo.com

Consultora española especializada en ciberseguridad con presencia en México y Colombia y más de 700 empleados. En este ámbito, la empresa ofrece servicios de ciberinteligencia, protección de infraestructuras industriales y críticas y análisis forense, entre otros.

Netskope

Fabricante
www.netskope.com/es

Netskope salvaguarda a la empresa distribuida a través de una solución unificada que escala de forma transparente para soportar más usuarios adicionales, nuevos servicios de seguridad, funcionalidades de monitorización y evaluación de seguridad continuas.

NovaRed

Servicios
www.novared.net

Su objetivo es acompañar a sus clientes en el diseño, implementación y gestión de una arquitectura adaptativa con un modelo de ciberinteligencia que incremente la consistencia, la eficacia y la eficiencia para protegerlos y prevenirlos de los ataques cibernéticos.

Nunsys

Fabricante/integrador
www.nunsys.com

Fundada en 2007, en el ámbito de la seguridad, esta empresa es especialista en temas relacionados con proyectos de cumplimiento y auditoría, servicios de seguridad "todo en uno" y soluciones de protección y gobierno de la información, así como de *hacking* ético.

On Security

Servicios
www.onsecurity.co.uk

Compañía inglesa especializada en ciberseguridad que ofrece a empresas de todo el mundo servicios de pruebas de aplicaciones web y móviles, testeos de infraestructura externa y simulaciones de campañas realistas de correo electrónico y *phishing*.

OneseQ

Integrador
www.oneseq.es

OneseQ es el área de ciberseguridad de la empresa tecnológica Alhambra-Eidos. Con ella, la compañía aporta un valor añadido a sus clientes, siempre bajo la experiencia y el conocimiento de la integración de soluciones y servicios *cloud* de Alhambra.

Open Cloud

Servicios/consultoría
www.opencloud.es

Empresa especializada en servicios y soluciones integradas de *open source*, virtualización y *cloud computing*. Su porfolio va desde la planificación, el diseño y la integración hasta el soporte, la gestión, la formación y la optimización.

Oylo Trust Engineering

Integrador
trustoylo.com

La principal actividad de esta compañía es la ciberseguridad en tecnologías de la operación e IoT, con una especial atención al tratamiento avanzado de datos de ciberseguridad en procesos críticos. Para ello cuenta con las certificaciones ISO-27001 e ISO-22301.

Palo Alto Networks

Fabricante
www.paloaltonetworks.es

Especializada en soluciones de ciberseguridad para empresas, Palo Alto Networks ofrece herramientas de protección que combinan los últimos avances en seguridad, automatización y análisis. Para ello, el fabricante cuenta con dos soluciones: Prisma y Cortex.

Proofpoint

Servicios
www.proofpoint.com

Proofpoint cuenta con una plataforma basada en datos que brinda visibilidad crítica para comprender el contexto y la escala de un ataque, así como la información práctica necesaria para resolverlo de la manera más rápida y efectiva posible.

PwC

Consultoría
www.pwc.es

PwC ofrece servicios de auditoría, consultoría, asesoramiento fiscal y legal, transacciones y aceleración de la transformación digital. En el segundo aspecto se centra en gestión de riesgos, aceleración de la transformación digital, protección de activos, etc.

Qualys

Servicios
www.qualys.com

Ayuda a las empresas a simplificar las operaciones de seguridad y a reducir el coste del cumplimiento al brindar inteligencia de seguridad crítica bajo demanda y automatizar el espectro completo de auditoría, cumplimiento y protección para sistemas de TI y web.

Radiant Logic

Fabricante
www.radiantlogic.com

Proveedor de sistemas de identidad federados basados en la virtualización que ofrece acceso simple y lógico basado en estándares a todas las identidades dentro de una organización. Entre sus soluciones destaca su servicio de identidad RadiantOne FID.

Realsec

Fabricante
www.realsec.com

Empresa tecnológica de ciberseguridad que desarrolla soluciones propias de cifrado y firma digital para la protección de las transacciones y de los medios de pago, basadas en *hardware security*, firma digital, sellado de tiempo y sistemas de cifrado, entre otros.

RedTrust

Servicios
www.redtrust.com

Cuenta con una plataforma 360 para gestionar las claves y certificados digitales que permite al usuario y administrador tener su total control y disponibilidad. Esto surge debido a la necesidad de disponer de una identidad digital confiable y verificable por todos.

Rohde & Schwarz

Fabricante
www.rohde-schwarz.com

Empresa que ofrece soluciones completas para el cliente, incluidas de ciberseguridad. Realizan la instalación completa, puesta en marcha, protocolos de prueba, formación del personal y asistencia técnica durante toda la vida útil de la instalación.

RSA

Servicios
www.rsa.com

Multinacional que ofrece un enfoque unificado e impulsado por el negocio para gestionar el riesgo digital. Entre sus productos se encuentra RSA NetWitness, que dota a los equipos de seguridad con una gran capacidad para detectar rápidamente los ataques dirigidos.

SailPoint

Servicios
www.sailpoint.com

SailPoint permite a sus clientes gestionar de forma eficiente las identidades digitales, desde la seguridad y la confidencialidad con la que deben contar las empresas. Por ello, ha creado la plataforma *cloud* SailPoint de gobierno inteligente de la identidad.

Secura

Consultoría
www.secura.es

Consultora especializada en servicios y soluciones de seguridad informática cuyo objetivo es cuidar de los activos tecnológicos de sus clientes, optimizar su rendimiento y productividad y protegerlos de cualquier amenaza externa e interna con total integridad.

Secure&IT

Servicios/consultoría
www.secureit.es

Empresa española dedicada a las tecnologías de la información y comunicación que ofrece a sus clientes servicios de formación, auditoría, consultoría, ejecución de proyectos, soporte y mantenimiento a grandes, medianas y pequeñas compañías.

Seidor

Servicios
www.seidor.es

Multinacional tecnológica que cuenta con un amplio abanico de soluciones y servicios de consultoría, implantación, *outsourcing*, desarrollo y mantenimiento de aplicaciones. También dispone de un servicio de supervisión y tratamiento de incidentes de ciberseguridad.

SIA

Servicios
www.sia.es

Adquirida por Indra para aglutinar su oferta de ciberseguridad, SIA está dedicada a ofrecer soluciones y servicios en el área de la informática corporativa: gobierno de la identidad, cumplimiento, firma electrónica, inteligencia artificial, gobierno TIC, *Big Data*...

Sidertia

Servicios
www.sidertia.com

Sidertia es una compañía española que ofrece múltiples soluciones para proteger el activo fundamental de una organización: el dato. Para ello, la empresa apuesta por el I+D+i, así como por la alta cualificación y especialización de sus profesionales.

SonicWall

Fabricante
www.sonicwall.com

SonicWall ofrece ciberseguridad ilimitada para las empresas en un entorno remoto, móvil y no seguro. Esta compañía protege a las organizaciones deteniendo los ciberataques más evasivos en cualquier punto de exposición y acceso a la información.

Stormshield

Servicios
www.stormshield.com/es

Sus soluciones permiten hacer frente a los desafíos que plantean las TI y OT para proteger las actividades de las empresas. En este contexto, su misión es "cibertranquilizar" a las organizaciones para que puedan centrarse en su actividad principal.

Symantec

Fabricante
www.symantec.com

Symantec, de Broadcom, es un proveedor de defensa cibernética que crea soluciones para todas las infraestructuras, ya sea se encuentren en local, la nube o en ambas. Sus productos cubren el *endpoint* y el acceso seguro a la nube, entre otros aspectos.

TechHeroX

Servicios
www.techherox.com

Conciencia a las empresas en materia de ciberseguridad a través de la generación de hábitos y la protección de datos. Dispone de un acceso ilimitado a contenido actualizado, así como a alertas de acuerdo a cómo evoluciona el cibercrimen.

Thycotic

Servicios
www.thycotic.com

Empresa especializada en servicios de ciberseguridad enfocada en la administración de acceso privilegiado en la nube. Su objetivo es proteger a las compañías ante posibles amenazas mediante el desarrollo de tecnologías innovadoras que aseguren dichas cuentas.

T-Systems

Servicios
www.t-systems.com

T-Systems es la unidad especializada en clientes corporativos de Deutsche Telekom. Con una infraestructura global de centros de datos y redes, gestiona los sistema TIC y la ciberseguridad en corporaciones multinacionales y organismos públicos.

Víntegris

Fabricante
www.vintegris.tech

Víntegris fabrica sistemas y aplicaciones innovadoras para gestionar certificados digitales, firmas digitales legalmente vinculantes y autenticación robusta. Estas soluciones son utilizadas especialmente por bancos, seguros, salud, minoristas y gobiernos.

VMware

Servicios
www.vmware.com

Esta empresa optimiza la transformación digital de las organizaciones. En concreto, ofrece a sus clientes la posibilidad de ejecutar, gestionar, conectar y proteger todas sus aplicaciones en cualquier *cloud* para que puedan reducir costes y aumentar la eficiencia.

Wallix

Fabricante
www.wallix.com

Compañía de *software* que brinda soluciones de ciberseguridad especializada en cuentas privilegiadas. Sus productos, presentes en mercados como banca, industria o salud, se comercializan a través de una red formada por más de 160 revendedores e integradores.

Westcon-Comstor

Distribuidor
westconcomstor.com

Distribuidor de tecnología empresarial que trabaja con los principales fabricantes para brindar soluciones a través de un canal de socios. Ofrece una serie de servicios financieros, atención proactiva, de cadena de suministro, soporte y renovaciones.

WhiteBearSolutions

Fabricante
whitebearsolutions.com

Compañía responsable del desarrollo de tres soluciones de rango empresarial orientadas a la mediana y gran organización: WBSAirback (almacenamiento y *backup*), WBSVision (gestión de servicios de directorio e identidad) y SmartLogin (gestión de acceso).

Zerolynx

Servicios
www.zerolynx.com

Grupo empresarial español especializado en ciberseguridad, inteligencia y seguridad patrimonial. Entre sus clientes se encuentran grandes compañías, las cuales tienen a esta firma como primera línea de defensa frente a los ataques físicos y lógicos.

SOMOS LA **REALIDAD DIGITAL** QUE NECESITAS

+ 10.000 inscritos a nuestros Webinar y eventos digitales
+ 10.000 inscritos a nuestra Newsletter semanal
+ 20.000 seguidores en redes sociales
+ 60.000 lectores de Red Seguridad Digital en Kiosko Pro por número
+ 122.000 páginas vistas en **www.redseguridad.com**

Red Seguridad es miembro de Google Editor Program

Súmate a red seguridad

Si no te ven no existes

Anúnciate: https://www.redseguridad.com/anunciate.html

EMPRESA	WEB
A2SECURE	www.a2secure.com
ACERODOCS	www.acerodocs.com
ADVANTIO	www.advantio.com
AJOOMAL ASOCIADOS	www.ajoomal.com
ALHAMBRA	www.alhambrait.com
ALL4SEC	all4sec.es
ALTEN	www.alten.es
ANADAT TECHNOLOGY	www.anadat.es
APPLUS	www.applus.com
ARROW	www.arrow.com
ARSYS	www.arsys.es
ARTICA PANDORA	artica.es
ASTREA	astrea.es
AUTEK	www.autek.es/es
AUTH USB	www.authusb.net
AUTHCOMM	www.authcomm.es
AVANSIS	www.avansis.es
BALIDEA	balidea.com
BARRACUDA NETWORKS	www.barracuda.com
BIT 4 ID	www.bit4id.com/es
BLUEVOYANT	www.bluevoyant.com
BOTECH	botechfpi.com
BUGUROO	www.buguroo.com
BYTE SECURITY	bytesecurity.com
CALS	www.calogistics.com/es
CARTRONIC GROUP	grupocartronic.com
CEFIROS	www.cefiros.net
CERANODE	www.ceranode.com
CHECKMARX	www.checkmarx.com
CIBER SEGURIDAD SUR	www.ciberseguridadsur.com
CITRIX	www.citrix.com/es-es
CLICK DEFENSE	www.clickdefense.io
CMC	www.grupocmc.es
CONTINUUM SECURITY	iriusrisk.com
COUNTERCRAFT	www.countercraftsec.com
CRIPTOCERT	www.criptocert.com
CROWDSTRIKE	www.crowdstrike.com
CYBENTIA GRUPO	www.cybentia.com
CYBERARK	www.cyberark.com/es
CYBERBLUE	www.cyberblue.io

EMPRESA	WEB
CYBEREASON	www.cybereason.com
CYBNUS	www.cybnus.es
DATALIA	datalia.info
DAVINCI GROUP	www.davinci-ti.es
DERTEN	derten.com
DFTOOLS	dftools.net
DINOSEC	www.dinosec.com
DIRECT DUMP	dftools.net/directdump/
DOTFORCE	www.dotforce.es
DRAINWARE SYSTEMS	www.puffinsecurity.com/es
DXC SECURITY	www.dxc.technology/security
ECLECTICIQ	www.eclecticiq.com
EFFICIENT IP	www.efficientip.com/es
ELASTIC	www.elastic.co/es
ELECTRONICID	www.electronicid.eu/es
ENSOTEST	www.ensotest.com/es
ENTRUST	www.entrust.com
EPUNTO	epunto.es
EUROCYBCAR	eurocybcar.com
F5 NETWORKS	www.f5.com/es_es
FACTUM IT	factum-it.es
FARADAY	faradayvp.com
FIBRATEL	www.fibratel.com
FORTYTWO SECURITY	fortytwo.nl
GAPTAIN	gaptain.com
GIESECKE+DEVRIENT	www.gi-de.com/es/es
GRADIANT	www.gradiant.org
GREEN LIGHT	www.greenlight.es
GRUPO TRC	www.grupotrc.com
HIBERUS	www.hiberus.com
HISPASEC SISTEMS	hispasec.com/es
HISPAWEB NETWORK	hispaweb.com
HORNET SECURITY	www.hornetsecurity.com
IBERLAYER	www.iberlayer.com/es
IDAVINCI	idavinci.es
INFOBLOX	www.infoblox.com
INFONET	infonet.es
INIXA	www.inixa.com
INPROSEC	inprosec.es
INSSIDE	www.insside.net

EMPRESA	WEB
INTEC	intec2.com
IRIUSRISK	iriusrisk.com
IRON CHIP	www.ironchip.com
ITS	www.its-security.es
JTSEC	www.jtsec.es/es
JUNIPER NETWORKS	www.juniper.net/es/es
KEYNETIC	keynetic.tech
KEYTRON	www.keytron.com
KYMATIO	kymatio.com/es
LOGRHYTHM	logrhythm.com
MDTEL	www.mdtel.es/web
MEE (THE CYBER NOTARY)	www.mee-thecybernotary.com
MICROFOCUS	www.microfocus.com
MINSAIT-INDRA	www.minsait.com/es
MOXA	www.moxa.com/en
NCC GROUP	www.nccgroup.trust/us
NEWRALERS	newralers.com
NOMOREPASS	www.nomorepass.com
NORAVAN	www.noravan.com
NOVA3 INFORMÁTICA	nova3informatica.com
NOZOMI NETWORKS	www.nozominetworks.com
OESIA GRUPO	grupooesia.com
OKTA	www.okta.com
ONE IDENTITY	www.oneidentity.com
ONRETRIEVAL	onretrieval.com
PHISHING HUNTERS	phishinghunters.com
PROCONSI	www.proconsi.com
PUE	www.pue.es
PUFFIN SECURITY	www.puffinsecurity.com/es
PULSE SECURE	www.pulsesecure.net
QUANTIKA 14	quantika14.com
RADWARE	www.radware.com
RANDED	randed.com
RED HAT	www.redhat.com/es
REDADVISOR	www.redadvisor.es
REDBORDER	redborder.com
REDYTEL COMPUTER	www.redytelcomputer.com
RISKRECON	www.riskrecon.com
SAFELAYER	www.safelayer.com/es
SAMOBY	samoby.com

EMPRESA	WEB
SCASSI	www.scassi.com/ES
SCAYLE	www.scayle.es
SEALPATH	www.sealpath.com/es
SECURACTIVA	securactiva.com
SECURE KIDS	securekids.es
SECUTATIS	www.secutatis.com
SEMICROL	www.semicrol.com
SENTINEL IT	www.sentinelit.es
SERVICENOW	www.servicenow.es
SKYBOX SECURITY	www.skyboxsecurity.com
SMART FENSE	www.smartfense.com/es-es
SMART HUMAN CAPITAL	www.smarthc.com
SMART LOGIN	www.smartlogin.cloud
SOFISTIC	www.sofistic.com
SOMOS VIRTUAL CARE	www.somosvirtualcare.com
SOPHOS	www.sophos.com
SSH TEAM	sshteam.com
SYNEIDIS	www.syneidis.com/es
TAISA	www.taisa.com
TECHVOLUCION	www.techvolucion.com/es-es
TECNALIA	www.tecnalia.com/es
TENABLE	es-la.tenable.com
THALES	www.thalesgroup.com
THREAT QUOTIENT	www.threatq.com
THYCOTIC	thycotic.com
TITHINK	www.tithink.com/es
TIXEO	www.tixeo.com
TRANSMIT SECURITY	www.transmitsecurity.com
TS FUJITSU	www.fujitsu.com/emeia
TUFIN	www.tufin.com/es
UNIVERSING	www.universign.com
VALORA DATA	www.valoradata.com
VARONIS	www.varonis.com
VECTOR ITC GROUP	www.vectoritcgroup.com
VERACODE	www.veracode.com
VERNE	www.vernegroup.com
VULNEX	www.vulnex.com
WISE SECURITY GLOBAL	www.wsg127.com
XOLIDO	www.xolido.com
ZSCALER	www.zscaler.com

Nexo de unión entre profesionales y empresas

La ciberseguridad cuenta con un nutrido grupo de asociaciones que aglutinan a todos y cada uno de los perfiles profesionales y empresariales de este sector: desde delegados de protección de datos hasta peritos informáticos y responsables de seguridad de la información, entre otros perfiles. Todas ellas tienen el objetivo de defender los intereses de sus representados a través de diversas iniciativas, entre las que se encuentran reuniones con la Administración, eventos, *webinars*, informes, cursos de formación, certificaciones, proyectos, etc.

Algunas de estas asociaciones llevan desempeñando su importante papel en el sector desde hace décadas, pero otras son de reciente creación. Un síntoma de que la ciberseguridad progresa de la mano de la evolución tecnológica.

A continuación realizamos una selección de las múltiples agrupaciones sin ánimo de lucro presentes en la ciberseguridad.

AEI Ciberseguridad

La Agrupación Empresarial Innovadora en Ciberseguridad y Tecnologías Avanzadas reúne a empresas, asociaciones, centros de I+D+i y entidades públicas o privadas interesadas en la promoción del sector de las nuevas tecnologías. Y también a sus industrias afines y auxiliares, así como a otros sectores emparejados con el ámbito nacional de las tecnologías de seguridad.

Esta organización sin ánimo de lucro otorga un Sello de Ciberseguridad para Organizaciones.

www.aeiciberseguridad.es

AENOR

Esta entidad de certificación tiene como propósito principal contribuir a la transformación de la sociedad creando confianza entre organizaciones y personas. Para ello presta servicios de evaluación de la conformidad (certificación, inspección y ensayos), formación e información.

Sus certificaciones abarcan sistemas de gestión, productos y personas. Y su acción de información incluye la distribución de normas, publicaciones técnicas y distribución de información sectorial.

www.aenor.com

AMETIC

Patronal que representa al sector de la industria tecnológica digital en España. Entre sus socios se encuentran empresas globales de TI, telecomunicaciones, electrónica, servicios y contenidos digitales, transformación digital y diversas asociaciones del sector.

Su principal objetivo es promover la política económica y el entorno legislativo que mejor faciliten el desarrollo y la utilización de las tecnologías digitales. Trabaja y colabora con instituciones nacionales y europeas públicas y privadas.

ametic.es

ANCITE

La Asociación Nacional de Ciberseguridad y Pericia Tecnológica se ocupa de temas relacionados con la informática y la ciberseguridad. Entre ellos, auditorías periciales, forenses, mediaciones, defensa jurídica tecnológica, pruebas de estrés de seguridad, etc.

Los servicios que ofrece esta asociación se dividen en cinco categorías: ciberseguridad y *pentesting*, peritajes informático y tecnológico, auditoría informática y forense, y derecho tecnológico y defensa judicial.

www.ancite.es

ANPhacket

La Asociación Nacional de Profesionales del *Hacking* Ético es una entidad sin ánimo de lucro compuesta por profesionales del ámbito de la ciberseguridad, juristas especializados en nuevas tecnologías y miembros de las fuerzas de seguridad y del orden público (a título particular) pertenecientes a las secciones de investigación de delitos informáticos y telemáticos.

Todos ellos se han marcado como objetivo conseguir que la sociedad de la información e Internet sean un sitio más seguro.

anphacket.es

ANTPJI

La Asociación Nacional de Tasadores y Peritos Judiciales Informáticos está compuesta por expertos en diferentes especialidades informáticas. Se trata de una entidad especializada en peritajes informáticos para empresas, particulares y administraciones.

Esta entidad ofrece, de manera gratuita, los conocimientos y experiencia acreditada de sus expertos para prestar auxilio o prevenir ciberdelitos. Así lucha contra el cibercrimen y apuesta por la formación, investigación e innovación.

antpji.org

Centro de Ciberseguridad Industrial (CCI)

Centro de Ciberseguridad Industrial

Misión y objetivo:
El Centro de Ciberseguridad Industrial (CCI) es el punto de encuentro de los profesionales y las entidades público-privadas que trabajan para mejorar el nivel de ciberseguridad de la industria. Además, es la referencia internacional para el intercambio de experiencias y conocimiento, así como para la dinamización de los sectores involucrados en este ámbito.

Esta asociación ha conformado el mayor ecosistema de organizaciones industriales (usuarios finales), proveedores de servicios y soluciones de ciberseguridad industrial, ingenierías, integradores y organizaciones públicas; pero, sobre todo, a sus profesionales.

Su misión es impulsar y contribuir a la mejora de la ciberseguridad industrial utilizando las perspectivas de personas, procesos y tecnologías.

Áreas o comités:
El CCI está compuesto por un equipo directivo, coordinadores que colaboran en diferentes países y regiones del mundo y expertos con experiencia en ámbitos específicos y delimitados en ciberseguridad industrial.

Actividades:
Encuentros, eventos, participación en diversos foros, espacios de diálogo para profesionales, publicaciones (informes, análisis estratégicos, guías, estudios de situación, documentos y herramientas específicos de ciberseguridad industrial), boletín semanal gratuito (con noticias, recursos, eventos específicos de la materia), blog, redes sociales, equipos de conocimiento, Escuela Profesional, plataformas facilitadoras de conocimiento y desarrollo para profesionales/organizaciones y el Programa Academia para estudiantes y profesionales de la enseñanza.

Formación y certificación:
El CCI cuenta con los siguientes cursos, máster y talleres:

- Curso Multidisciplinar de Seguridad Digital en la Industria 4.0 y Protección de servicios esenciales.
- Curso de Responsable de Ciberseguridad en IACS (Sistemas de Automatización y control Industrial).
- Máster Profesional *Online* de Ciberseguridad Industrial.
- Taller de Evaluación de Madurez del Proceso de Ciberseguridad en Organizaciones Industriales.
- Taller de Diagnóstico de ciberseguridad en un entorno de automatización industrial.
- Taller de Ciberseguridad en el Ciclo de Vida de un Proyecto Industrial.
- Taller de Aplicación de un Sistema de Gestión de la Ciberseguridad Industrial.
- Taller de Análisis Forense en un entorno de automatización industrial.

Dirigida por:

José Valiente

Año de creación

2013

Página web

www.cci-es.org

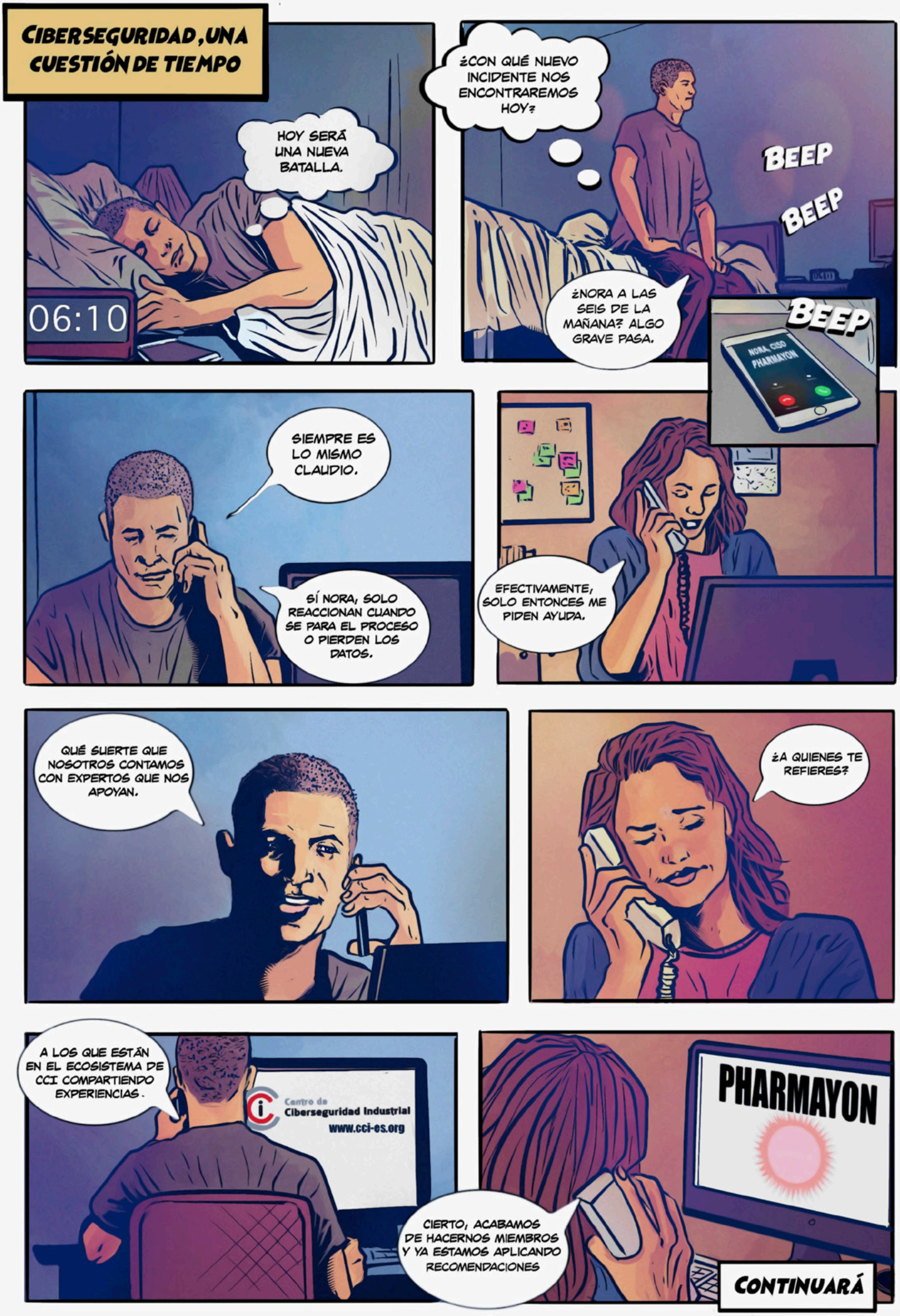
Perfil del socio

Profesional individual y organizaciones industriales.

Certificados o títulos que expide

Credencial profesional niveles blanco, verde o negro.

Ciberseguridad, una cuestión de tiempo



ISACA Madrid

Misión y objetivo:
ISACA Madrid es una asociación sin ánimo de lucro con más de 1.300 asociados. Su principal misión es contribuir a la calidad y excelencia del gobierno, gestión de riesgos, cumplimiento, seguridad, control y auditoría de las tecnologías de la información y la comunicación, así como fomentar la formación y la capacitación de los profesionales en estos ámbitos.

El objetivo de ISACA Madrid es ser un referente en sus áreas de especialización, contribuir y fomentar la formación continua de los asociados, promover su reconocimiento profesional y generar un beneficio mantenido de servicios para los mismos.

ISACA Madrid es parte de ISACA, asociación internacional sin ánimo de lucro con más de 156.000 asociados en 180 países. El fin de esta organización es ayudar a los profesionales globales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución ofreciendo conocimiento, estándares, relaciones, acreditaciones y desarrollo de carrera innovadores y de primera clase.

Áreas o comités:
ISACA Madrid está constituida por las siguientes vocalías, que tienen como objeto contribuir a la consecución de los objetivos de la asociación: Presidencia, Vicepresidencia, Secretaría, Tesorería, Formación y Relaciones Académicas, Relación con Asociados y Jóvenes Profesionales, Eventos y Jornadas, Relaciones Institucionales (Administración Pública y Empresa Privada), Investigación e Innovación y, finalmente, Comunicación, Contenidos y Marketing.

Actividades:
Entre los recursos de la asociación destacan tanto los cursos de formación, certificaciones y certificados como los congresos anuales y seminarios especializados. ISACA Madrid presta especial atención, en este sentido, a la selección de las temáticas y a la calidad de los ponentes que participan en ellos. Además, publica material especializado, boletines y trabajos de investigación con el objeto de contribuir a la consecución de su misión. Estos últimos son realizados a través de grupos de trabajo y comisiones, considerando nuevas tendencias en seguridad y temas innovadores de interés para sus asociados.

Formación y certificación:
ISACA pone a disposición de sus asociados una serie de certificaciones de seguridad, internacionalmente reconocidas, que acreditan que se dispone de habilidades y conocimientos críticos para el negocio en diferentes áreas de especialización: Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC), CSX Cybersecurity Practitioner (CSX-P) y Certified Data Privacy Solutions Engineer (CDPSE).

También ofrece certificados internacionalmente reconocidos, como CSX Cybersecurity Fundamentals y Control Objectives for Information Technologies (COBIT), entre otros.

En el ámbito de la formación, la asociación trabaja de forma continua para ofrecer formación y certificaciones de calidad en sus áreas de especialización que respondan a las necesidades de sus asociados, en constante evolución.

ISACA Madrid Chapter

Presidida por:

Vanesa Gil

Año de creación

1987

Página web

www.isacamadrid.es

Perfil del socio

CISO; director de Seguridad, Tecnología o Auditoría; Manager de Seguridad, Tecnologías de la Información o Auditoría; consultor de Seguridad o IT; profesionales especializados en ciberseguridad, *compliance*, gestión de riesgos, privacidad, etc.

Certificados o títulos que expide

Certified Information Systems Auditor, Certified Information Security Manager, Certified in the Governance of Enterprise IT, Certified in Risk and Information Systems Control, CSX Cybersecurity Practitioner, Certified Data Privacy Solutions Engineer, Information Technology Certified Associate, Control Objectives for Information Technologies, CSX Cybersecurity Fundamentals, Certificate of Cloud Auditing Knowledge, Cybersecurity Audit y IT Risk Fundamentals.

GOBIERNO, GESTIÓN DE RIESGOS, CUMPLIMIENTO, SEGURIDAD, CONTROL Y AUDITORÍA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

ISACA®
Madrid Chapter

APUESTA POR EL FUTURO, ¡CERTIFÍCATE!

CERTIFICACIONES

CISA Certified Information Systems Auditor®
An ISACA® Certification

CISM Certified Information Security Manager®
An ISACA® Certification

CRISC Certified in Risk and Information Systems Control®
An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT®
An ISACA® Certification

CSX-P CSX Cybersecurity Practitioner®
An ISACA® Certification

ITCA Information Technology Certified Associate
An ISACA® Certification

CDPSE Certified Data Privacy Solutions Engineer™
An ISACA® Certification

CERTIFICADOS

CSX CYBERSECURITY
FUNDAMENTALS CERTIFICATE

COBIT®
An ISACA® Framework

IT RISK FUNDAMENTALS
An ISACA® Certificate

CYBER SECURITY AUDIT
An ISACA® Certificate

CCAK™
Certificate of Cloud Auditing Knowledge
A Cloud Security Alliance® and ISACA® Credential

LA MEMBRESÍA DE ISACA MADRID INCLUYE ASISTENCIA GRATUITA A TODOS LOS CONGRESOS Y CONFERENCIAS QUE ORGANIZAMOS, MUCHAS OPCIONES DE PARTICIPACIÓN ACTIVA EN LA ASOCIACIÓN, ACCESO A DOCUMENTACIÓN, OFERTAS DE EMPLEO, ¡Y MUCHO MÁS!

WWW.ISACAMADRID.ES

ISMS Forum

Misión y objetivo:
ISMS Forum (International Information Security Community) es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la seguridad de la información en España y actuar en beneficio de toda la comunidad implicada en el sector. Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de seguridad de la información. Cuenta con más de 250 empresas y de 1.250 profesionales asociados.

Áreas o comités:
ISMS Forum trata de fomentar la cultura de la seguridad de la información a través de cuatro grandes áreas: el Cyber Security Centre (CSC), el Data Privacy Institute (DPI), la Cloud Security Alliance (CSA-ES) y el IoT Security Centre (ISC).

También ha desarrollado distintos capítulos en ciudades como Barcelona, La Coruña o Valencia con el objetivo de hacer llegar todo su conocimiento, proyectos e iniciativas a aquellas empresas y profesionales no ubicados en Madrid que se encuentran con la necesidad de mantener una actividad mayor fuera de la capital española.

Actividades:
La asociación se centra en la realización de eventos relacionados con sus cuatro grandes áreas. Estos son el Foro de la Ciberseguridad (CSC), el Foro de la Privacidad (DPI), el Encuentro de Cloud Security Alliance España (CSA-ES), el Foro de la Movilidad e Internet de las Cosas (ISC) y la Jornada Internacional de Seguridad de la Información. Esta última aúna todas las áreas tratadas anteriormente y se constituye como un congreso privado nacional de referencia para los sectores de la ciberseguridad y la protección de datos, reuniendo cada año a más de 800 profesionales.

Por otro lado, ISMS Forum dispone de diversas prácticas anuales relacionadas con la concienciación sobre los riesgos en ciberseguridad en grandes organizaciones, como son los ciberejercicios multisectoriales, el Proyecto de Gestión de Crisis Cibernéticas y el Proyecto de Generación de Indicadores de Compromiso.

Asimismo, dedica una parte de sus recursos a realizar actividades de formación orientadas al ciudadano. Se trata de la realización de *masterclass* con profesionales del sector, colaboraciones con universidades e institutos de negocios a través de la impartición de charlas y de la elaboración de guías que abarquen temas de interés.

Formación y certificación:
ISMS Forum cuenta con dos formaciones: el Curso de Especialización en Ciberseguridad, que ofrece profundos conocimientos sobre los fundamentos y el gobierno de la ciberseguridad; y, bajo el DPI, el Curso de Especialización en Protección de Datos, adaptado al esquema de certificación de DPD de la Agencia Española de Protección de Datos y actualizado según la nueva LOPD-GDD.

Por último, dispone de dos certificaciones propias: Certified Cyber Security Professional y Certified Data Privacy Professional. Y también de una oficial, el Certificado de Delegado en Protección de Datos, impulsado por la mencionada Agencia.

Presidida por:

Gianluca D'Antonio

Año de creación

2007

Página web

www.ismsforum.es

Perfil del socio

Los socios de ISMS Forum responden a un perfil de expertos en seguridad de la información y protección de datos. Abarcan áreas como la ciberseguridad, privacidad, seguridad en la nube y en los dispositivos IoT y la continuidad de negocio.

Certificados o títulos que expide

Certified Cyber Security Professional, Certified Data Privacy Professional y Certificado de Delegado de Protección de Datos.

Fundación Borredá

Misión y objetivo:
La Fundación Borredá es una organización de naturaleza fundacional privada, sin ánimo de lucro, con vocación de servicio a la seguridad en todos sus ámbitos y profesiones.

Su objetivo fundacional es diseñar, promover, estudiar, mejorar y realizar todas aquellas actividades relacionadas con la seguridad tanto pública como privada y con ámbitos similares para favorecer la cultura de la seguridad en España.

Áreas o comités:
El **Patronato** se encarga del gobierno y la representación de la Fundación Borredá, así como del cumplimiento de los fines fundacionales, la administración y la gestión de sus bienes patrimoniales. Está integrado actualmente por hijos y nietos de Ramón Borredá, además de por profesionales de la seguridad de reconocido prestigio.

El **Comité Asesor**, formado por expertos en distintos ámbitos del mundo de la seguridad, es el órgano de asesoramiento, consulta y apoyo al Patronato en lo referente al desarrollo y cumplimiento de sus fines.

El **Consejo de Expertos**, órgano consultivo, está integrado por los socios protectores y por prestigiosos profesionales de la seguridad.

> La Fundación Borredá ofrece un porfolio formativo impartido en modalidad presencial, 'online' o 'in company'

Actividades:
Las actividades de la Fundación Borredá son: desarrollo de estudios, libros, manuales e investigaciones en materia de seguridad; organización, promoción y colaboración en congresos, foros, conferencias, tertulias o reuniones profesionales relacionados con sus objetivos; creación y fomento de actividades técnicas, formativas y de capacitación profesional; instrucción y participación en distinciones que destaquen los valores propios de la Fundación, como es el Trofeo Ramón Borredá; y creación de grupos de trabajo con líneas de estudio permanente con el objetivo de formular propuestas de mejora en el ámbito de la seguridad tanto a nivel operativo como normativo.

Formación y certificación:
La Fundación Borredá ofrece un porfolio formativo impartido en modalidad presencial, *online* o *in company*. Los cursos cuentan con una estructura preparada por expertos y orientada al aprendizaje y capacitación de profesionales donde se realizan pruebas o evaluaciones que acreditan haber adquirido las habilidades y competencias necesarias.

Presidida por:

Ana Borredá

Año de creación

2012

Página web

www.fundacionborreda.org

Perfil del socio

La Fundación Borredá cuenta con distintas formas de colaboración que le permite afrontar sus fines fundacionales. Las empresas pueden colaborar a través de las figuras de Socios Protectores y Patrocinadores. Para las asociaciones o entidades sin ánimo de lucro existe la modalidad del Colaborador. Y como apoyo a título individual está la figura de Amigo de la Fundación o voluntario, en la que ya participan más de 1.000 profesionales de la seguridad.

Asociación Española de Normalización (UNE)

Misión y objetivo:
El propósito de la Asociación Española de Normalización (UNE) es impulsar la competitividad de las empresas y el desarrollo de la sociedad con estándares que generan confianza.

Áreas o comités:
UNE cuenta con 192 comités técnicos de normalización activos en los que se desarrollan estándares.

Actividades:
UNE es la entidad legalmente responsable del desarrollo de las normas técnicas, más conocidas como estándares. Estas normas recogen el consenso del mercado sobre las mejores prácticas en aspectos clave para la competitividad de las organizaciones, siendo el resultado de la labor conjunta de los sectores económicos y administraciones. Así, ayuda a las organizaciones a superar con éxito los desafíos a los que se enfrentan en campos como la ciberseguridad, digitalización, Industria 4.0, innovación, *compliance* y responsabilidad social o el despliegue eficaz de las políticas públicas.

Es el representante español ante los organismos de normalización internacionales (ISO e IEC), europeos (CEN y Cenelec) y en Copant (América). Asimismo, es el organismo de normalización español en el Instituto Europeo de Normas de Telecomunicaciones. UNE lleva la voz de los expertos españoles a los foros mundiales en los que se discuten normas clave para su competitividad.

Igualmente, desarrolla una intensa labor de cooperación internacional, con más de 900 actividades ya ejecutadas que apoyan el desarrollo de una infraestructura de la calidad sólida en regiones relevantes para los intereses comerciales españoles.

Por tanto, UNE es un actor relevante en el ámbito de la ciberseguridad en España. A través del Comité Técnico de Normalización CTN 320 Ciberseguridad y protección de datos personales desarrolla normas técnicas que dan respuesta eficaz a los nuevos retos relacionados con la ciberseguridad y la protección de datos personales en aspectos como gestión de evidencias electrónicas, servicios en la nube, Internet de las Cosas, Inteligencia Artificial o *Big Data*. Además, lleva la voz de los expertos de la industria española a los foros internacionales y europeos de normalización donde se elaboran estándares en apoyo al nuevo marco regulatorio europeo.

España es, en este sentido, y según afirman desde la propia asociación, un referente mundial en la elaboración de estándares para ciberseguridad. Por ejemplo, recientemente se ha publicado la Norma UNE 320002 Arquitecturas de confianza para el intercambio de Inteligencia de Ciberamenazas, el primer estándar mundial sobre modelos de gestión y compartición de inteligencia de ciberamenazas. Por su parte, la nueva norma UNE 320001 es el primer estándar español para la evaluación de ciberseguridad de productos TIC basado en la metodología Lince.

Finalmente, cabe destacar que UNE ayuda a lograr el éxito en la transformación digital de las empresas en España. Puede encontrar más información al respecto en el informe titulado *Apoyo de la Normalización a la Transformación Digital*.

Presidida por:

Carlos Esteban

Año de creación

1986

Página web

www.une.org

Perfil del socio

Más de 500 miembros, la práctica totalidad del tejido productivo español. Entre ellos, relevantes asociaciones sectoriales españolas de ámbito nacional.

Women4Cyber Spain

Misión y objetivo:
Women4Cyber Spain (W4C Spain) es una iniciativa que nace con el objetivo de convertirse en un referente en el impulso y visibilización del papel de la mujer en ciberseguridad en España, así como de la diversidad de género en el sector. Persigue construir entre todos un mundo digital más seguro e inclusivo.

La asociación es el capítulo español de Women4Cyber.eu, fundada por la Organización Europea de Ciberseguridad (ECSO), y la primera asociación de mujeres en ciberseguridad en España que cuenta con respaldo europeo.

A través de diferentes proyectos e iniciativas, Women4Cyber Spain se convierte en un espacio de colaboración donde mujeres en ciberseguridad del mundo académico, la investigación y la industria pueden compartir conocimientos, experiencias y red de contactos, además de motivar a otras féminas a considerar la ciberseguridad como una profesión en la que desarrollarse y crecer.

Áreas o comités:
La asociación cuenta con diferentes grupos de trabajo que abarcan las siguientes áreas dentro del ámbito de la ciberseguridad: innovación e investigación, emprendimiento, talento joven, recursos humanos, formación y *mentoring*.

Actividades:
Dentro de nuestra amplia agenda de actividades, Women4Cyber Spain ofrece cursos de formación, *webinars*, talleres, programa de *mentoring* y desarrollo profesional para mujeres en todas las etapas de sus carreras en ciberseguridad.

Imagen del webinar de presentación oficial de Women4Cyber Spain.

Dirigida por:

Eduvigis Ortiz

Año de creación

2020

Página web

www.women4cyberspain.es

Perfil del socio

Empresas, profesionales y estudiantes.

APEP

Entre los fines de la Asociación Profesional Española de Privacidad está integrar a aquellas personas que, en el ejercicio de su actividad, se dediquen a la protección de datos. Además, pretende fomentar y difundir los derechos fundamentales a la protección de datos de carácter personal, al honor, a la intimidad personal y familiar y a la propia imagen, entre otros objetivos.

Engloba a más de 980 miembros de diversos perfiles: abogados, académicos, auditores, consultores, ingenieros, etc.

www.apep.es

ASIS España

Representante en nuestro país de ASIS International, una comunidad global de unos 35.000 profesionales que engloba todos los aspectos relacionados con la seguridad: continuidad de negocio, gestión de riesgos, amenazas internas, incidentes, delitos cibernéticos, etc.

Entre los beneficios de sus socios se encuentran acceso a información y contenidos específicos, descarga gratuita de cada estándar y pauta de ASIS, certificación en determinadas tecnologías, etc.

asis-spain.org

@ASLAN

Está formada por más de 120 empresas tecnológicas. Su misión es dinamizar el mercado y divulgar las nuevas tecnologías en torno a la Red. Para ello realiza un gran número de actividades anuales. La más importante es la organización del Congreso&EXPO.

Además, realiza periódicamente, junto a otros coloquios y encuentros anuales, los Foros de Tendencias Tecnológicas. Un *tour* tecnológico por varios ciudades que acerca distintos aspectos de las nuevas tecnologías.

aslan.es

ASPEI

La Asociación Profesional de Peritos Informáticos, creada en 2010, tiene como objetivo general promover la divulgación del peritaje informático. Y lo hace como una herramienta indispensable para todos los ciudadanos y organizaciones que deseen aportar información digital como medio de prueba en un proceso judicial y para definir y proteger la figura del perito informático.

ASPEI ofrece sus servicios tanto a sus asociados como a los ciudadanos en general.

www.aspei.es

ATI

La Asociación de Técnicos de Informática tiene como objetivo la defensa, promoción y desarrollo de la actividad de estos profesionales. Gracias a sus actividades facilita el intercambio de experiencias entre sus socios, así como la formación y la información sobre la tecnología.

Entre sus fines están también contribuir a la promoción y desarrollo de las TIC, mantener relaciones con el entorno social y económico y estudiar el impacto de las tecnologías en la sociedad.

www.ati.es

AUTELSI

El objetivo de la Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información es desarrollar la sociedad de la información en España.

Entre sus ámbitos de actuación también se encuentran prestar servicios de asesoramiento y formación a los usuarios; proponer, colaborar y difundir acciones para la estandarización de procedimientos; y promover la armonización de las disposiciones relativas a dichos temas que establezcan las administraciones.

www.autelsi.es

Cybasque

La Asociación de Industrias de Ciberseguridad del País Vasco pretende articular la oferta privada en tecnología y conocimiento sobre ciberseguridad de las empresas vascas, sensibilizar al tejido empresarial y posicionar Euskadi en este sector de actividad.

Entre sus actividades, acompaña la internacionalización de sus socios a través de la generación de alianzas. Además, intensifica la búsqueda y creación de talento especializado en materia de ciberseguridad.

www.cybasque.eus

Continuam

La misión del Instituto de Continuidad de Negocio es crear, divulgar y fomentar a todos los niveles de la sociedad la cultura de la continuidad de negocio en su visión holística. Asimismo, promueve la resiliencia y las buenas prácticas sectoriales, ayudando a empresas y gobiernos en sus políticas de actuación.

Agrupa a los profesionales de la continuidad de los servicios prestados por todo tipo de organizaciones, incluso ante catástrofes de gran envergadura.

www.institutodecontinuidad.com

(ISC)²

Esta organización internacional cuenta con certificaciones reconocidas a nivel mundial. De hecho, dispone de más de 140.000 miembros certificados. Igualmente, ofrece amplias oportunidades laborales y una amplia red de colaboración. Y dispone de un Instituto de Desarrollo Profesional y herramientas de liderazgo.

Adicionalmente, (ISC)² se compromete a educar al público en general a través de su apoyo al Centro para la Educación y la Ciberseguridad.

www.isc2.org

OWASP

La iniciativa Open Web Application Security Project está dedicada a la búsqueda y la lucha contra las vulnerabilidades en el *software*. A partir de ella se creó la Fundación OWASP, una organización sin ánimo de lucro formada por empresas, organizaciones educativas y particulares de todo mundo. Todos ellos forman parte de una comunidad que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser utilizadas gratuitamente.

owasp.org

PESI

La Plataforma Tecnológica Española de Seguridad Industrial proporciona una visión global e integradora de la seguridad industrial que permita planificar, promover e impulsar las actividades de I+D+i. Para ello cuenta con varias áreas de trabajo de seguridad medioambiental, de productos e instalaciones, de la salud en el trabajo y patrimonial de la empresa.

Sus líneas de acción incluyen el apoyo a las compañías para conseguir y desarrollar proyectos de I+D+i de la Unión Europea.

www.pesi-seguridadindustrial.org

RENIC

La Red de Excelencia Nacional de Investigación en Ciberseguridad engloba centros de investigación y otros agentes del ecosistema investigador en ciberseguridad de España. Su fin principal es fomentar la investigación científica, el desarrollo tecnológico, la innovación, la trasferencia de conocimiento y tecnología a la industria y el desarrollo de proyectos de I+D+i en el sector de la Ciberseguridad en nuestro país.

Entre sus objetivos se encuentran fomentar la excelencia.

www.renic.es

La regulación avanza al ritmo de los retos en el ciberespacio

La normativa relacionada con la seguridad de las tecnologías de la información y las comunicaciones evoluciona a medida que surgen nuevas necesidades en esta materia en nuestra sociedad. En 2020, por ejemplo, asistimos a la aprobación del Reglamento sobre Redes y Sistemas de la Información, que desarrolla el real decreto-ley al respecto. Este año probablemente alumbrará nuevas regulaciones tanto nacionales como en el ámbito de la Unión Europea, de manera que se vayan cubriendo los espacios que abre la innovación de la tecnología y las necesidades de empresas, ciudadanos o el propio Estado. En cualquier caso, la normativa supondrá un importante impulso en cuanto que sus sujetos obligados han de implementar cambios encaminados a una finalidad global concreta: crear una sociedad segura en el ámbito digital para que puedan hacer frente a los retos del ciberespacio.

Directiva NIS

La Directiva UE 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio, establece unos requisitos mínimos comunes para todos los países de la Unión en materia de desarrollo de capacidades y planificación, intercambio de información y cooperación y seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales. La norma insta a estos grupos de organizaciones a adoptar las medidas oportunas para gestionar los riesgos de seguridad y notificar a las Autoridades Nacionales los incidentes que tengan un efecto perturbador significativo. Propone, además, la creación de una red de cooperación entre Estados miembros.

Ley de Seguridad de las Redes y Sistemas de la Información

Con la aprobación del Real Decreto-ley 12/2018, de 7 de septiembre, se transpuso al ordenamiento jurídico español la conocida como Directiva NIS. La norma nacional identifica los sectores esenciales en los que es necesario garantizar la protección de las redes y sistemas de información, así como los procedimientos para identificar las organizaciones sujetas a esta norma (operadores de servicios esenciales y proveedores de servicios digitales). Uno de los aspectos importantes de esta regulación es el establecimiento de un sistema de notificación de incidentes de ciberseguridad a diferentes centros de respuesta. Asimismo, el Real Decreto-ley establece un marco institucional para su aplicación y para la coordinación entre autoridades competentes nacionales y europeas.

Reglamento sobre Seguridad de las Redes y Sistemas de la Información

El Real Decreto 43/2021, aprobado en enero de este año, tiene como finalidad desarrollar la Ley NIS (Real Decreto-Ley 12/2018 de Seguridad de las Redes y Sistemas de la Información). El texto, que afecta a los operadores y proveedores de servicios esenciales con actividad en España, recoge aspectos relativos al marco institucional en la materia, la cooperación y coordinación, la gestión y notificación de incidentes, las medidas a implementar, la supervisión de los requisitos de ciberseguridad o la función del CISO. Destacan entre sus disposiciones la designación de autoridades competentes para los operadores esenciales, así como la creación de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes para la coordinación y colaboración entre los CSIRT.

Estrategia de Seguridad Nacional 2017

Mediante el Real Decreto 1008/2017, de 1 de diciembre, se aprobó la Estrategia de Seguridad Nacional 2017, la primera que vio la luz de acuerdo con las previsiones de la Ley de Seguridad Nacional. Se trata de una importante actualización de la Estrategia de Seguridad Nacional anterior (2013) para adecuarla al cambiante entorno de la seguridad internacional.

La estrategia analiza las dinámicas de transformación de la seguridad global, establece objetivos en materia de seguridad nacional e identifica las principales amenazas actuales para el país, entre ellas, las cibernéticas. Este documento también establece iniciativas para reforzar el Sistema de Seguridad Nacional y para mejorar la coordinación y eficacia de la acción del Estado.

Estrategia Nacional de Ciberseguridad 2019

Mediante la aprobación de la Orden PCI/487/2019, de 26 de abril, se publicó la Estrategia Nacional de Ciberseguridad 2019, la cual desarrolla las previsiones de la Estrategia de Seguridad Nacional en el ámbito de la ciberseguridad, considerando los objetivos generales y las líneas de acción establecidas para conseguirlo. El documento se estructura en cinco capítulos, en los que establece la necesidad de proteger el ciberespacio de las actuales amenazas y de sus desafíos. Para ello, estipula una serie de propósitos, principios y objetivos de ciberseguridad que encajan en el Sistema de Seguridad Nacional, basados en aspectos como la colaboración publico-privada, la creación de una cultura de ciberseguridad, el apoyo a la industria y la I+D+i o la construcción de capacidades para la ciberseguridad del Estado.

Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad (ENS) se aprobó en 2010, si bien fue actualizado cinco años después a través del Real Decreto 951/2015. Esta norma tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de las administraciones públicas. El ENS establece los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información de las administraciones públicas, así como para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos que gestionen.

Entre sus objetivos están crear las condiciones necesarias de seguridad en el uso de los medios electrónicos, promover la gestión continuada de la seguridad, promover la prevención detección y corrección o servir de modelo de buenas prácticas.

Ley de Sociedad de la Información y del Comercio Electrónico

La Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico fue actualizada por última vez en 2014. Esta normativa establece tanto a los proveedores de servicios de intermediación, como a las empresas que ofrecen sus productos y a los ciudadanos que posean una página web, las reglas necesarias para que el uso y disfrute de esta red, así como la posible actividad económica generada en torno a la compra y venta de todo tipo de productos y servicios, sea una experiencia positiva, segura y confiable. Entre los prestadores de servicios incluye aquellos que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica o la información previa y posterior a la celebración de contratos electrónicos.

Reglamento e-IDAS

El Reglamento europeo 910/2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior, tiene como objetivo reforzar el Mercado Único europeo otorgando un nivel de seguridad adecuado a los medios de identificación electrónica y los servicios de confianza. Entre sus disposiciones, establece las condiciones en que los Estados Miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro. Asimismo, dispone las normas para los servicios de confianza, así como el marco jurídico para las firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, documentos electrónicos, servicios de entrega electrónica certificada y los servicios de certificados web.

Ley de Secretos Empresariales

La Ley 1/2019 de Secretos Empresariales adapta al ordenamiento jurídico español la Directiva UE 2016/943 del Parlamento Europeo y del Consejo, de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales). El objetivo de esta norma es la protección de los secretos empresariales, es decir, cualquier información o conocimiento que sea secreto para la empresa y tenga valor empresarial.

La norma también procura la protección del titular de un secreto empresarial, que es cualquier persona física o jurídica que legítimamente ejerza el control sobre el mismo, y se extiende frente a cualquier modalidad de obtención, utilización o revelación de la información.

Reglamento General de Protección de Datos

El Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, regula la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Conocido como RGPD, incorpora aspectos como la necesidad de que las organizaciones designen un delegado de protección de datos en su seno para encargarse del cumplimiento de la normativa al respecto, la obligación de realizar un análisis de riesgos y evaluaciones de impacto en el tratamiento de esos datos.

La norma también incluye entre sus principales aspectos la necesidad notificar a las autoridades nacionales de protección de datos las violaciones de datos personales, sean fruto de un ciberataque o accidentalmente, sin dilación indebida y a más tardar 72 horas después de que hayan tenido constancia de la violación.

Ley Orgánica de Protección de Datos y Derechos Digitales

La Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales adapta al ordenamiento jurídico español el RGPD. La norma contempla aspectos como el registro y tratamiento de los datos personales, la evaluación de los riesgos en la materia por parte de las organizaciones, el papel de la AEPD, la notificación a esta de incidentes en la materia o nuevas figuras de la empresas, como el delegado de protección de datos. Además, amplía el catálogo de derechos de los ciudadanos al respecto, como el de portabilidad de datos o el derecho a ser informado de las brechas de datos.

Uno de los aspectos más sensibles de esta norma es el establecimiento de un régimen sancionador que podría llegar a los 20 millones de Euros o el cuatro por ciento de la facturación anual de la compañía en los casos mas graves de incumplimiento.

Protección de Infraestructuras Críticas

La Ley 8/2011 y su reglamento de desarrollo 704/2011 componen la principal la normativa que regula la protección de las infraestructuras críticas en España. Estas normas establecen la composición del Sistema Nacional de Protección de Infraestructuras Críticas, así como los diferentes instrumentos de planificación del mismo, como son: el Plan Estratégico Sectorial, el Plan de Seguridad del Operador, los Planes Específicos de Seguridad y los Planes de Apoyo Operativos. Para velar por el cumplimiento de estas normas y el eficaz funcionamiento del sistema, crea el Centro Nacional de Protección de Infraestructuras Críticas,

Uno de los rasgos distintivos de esta regulación es el enfoque integral de la seguridad de estos servicios indispensables, obligando a los operadores afectados a establecer medidas de protección tanto físicas como lógicas.

Reglamento sobre Ciberseguridad

El Reglamento 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación. Esta norma otorga muchos más poderes a la ENISA de los que mantenía hasta este momento y la convierte en el organismo de referencia para la supervisión, el asesoramiento y el conocimiento de instituciones y organismos de la Unión.

Otro aspecto importante del reglamento es la creación del marco europeo de certificación de la ciberseguridad que persigue un planteamiento armonizado de esquemas europeos de certificación de la ciberseguridad en la Unión Europea, con el objetivo de crear un mercado único digital para los productos, servicios y procesos de TIC.

Ley de Firma Electrónica

La Ley 59/2003, de 19 de diciembre, de firma electrónica fue actualizada por última vez en 2019, para adaptarla a otras normas. Dicha ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación. Aclara los conceptos de certificado electrónico y del firmante, los certificados reconocidos, así como dispositivos para la firma electrónica. Igualmente, establece las obligaciones que deben cumplir los prestadores de este tipo de servicios y establece su supervisión y control.

La ley distingue entre dos tipos de firma: la firma electrónica avanzada y la firma electrónica reconocida. La primera es la que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, mientras que la segunda queda definida como la firma basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Ley de Conservación de Datos en Comunicaciones Electrónicas

La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones fue modificada en 2014. Esta ley tiene por objeto regular la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación.

Asimismo, regula el deber de cesión de dichos datos a los agentes facultados, siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

Reglamento de Evaluación y Certificación de la Seguridad de las TI

El Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por la Orden PRE/2740/2007, tiene por objeto la articulación del Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) en el ámbito de actuación del Centro Criptológico Nacional. El ámbito de actuación del Organismo de Certificación comprende las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TI en el marco del ENECSTI. También comprende a estas entidades cuando sean fabricantes de productos o sistemas de TI que quieran certificar la seguridad de dichos productos, en el marco de dicho Esquema.

Ley de Seguridad Privada

La Ley 5/2014, de 4 de abril, derogó la anterior Ley de Seguridad Privada, que se mostraba insuficiente para las necesidades actuales en la materia. Una de las principales novedades de esta norma es que incluye en su ámbito de aplicación a las empresas "prestadoras de servicios de seguridad informática", y reserva la posibilidad de que el reglamento de desarrollo incluya requisitos específicos para ellas. Por ejemplo, la obligación de inscribirse en el Registro Nacional de Seguridad Privada y en registros autonómicos.

También establece la aplicación de medidas de seguridad informática para las organizaciones designadas como "sujetos obligados".

Directiva sobre Servicios de Pago

La Directiva europea 2015/2366 sobre servicios de pago en el mercado interior modifica la normativa anterior al respecto en el seno de la Unión Europea, como consecuencia de la entrada en el mercado de nuevos operadores, como por ejemplo las *fintech*. Esta norma, conocida popularmente como PSD2, afecta a entidades de crédito, de pago, de giro postal o entidades financieras, entre otras. Esta Directiva establece normas en materia de requisitos de transparencia y de información para los servicios de pago, así como los derechos y obligaciones respectivos de los usuarios de servicios de pago y de los proveedores de servicios de pago en relación con la prestación de dichos servicios con carácter de profesión u ocupación habitual.

Esta norma regula dos clases de servicios no incluidos en la normativa anterior: por un lado, los servicios de iniciación de pagos (PIS) y, por otro, los servicios de información de cuenta (AIS).

Teniendo vacuna, ¿No te vas a vacunar?

#CampañaVacunación

µclaudia

S2 GRUPO
Anticipando un mundo **ciberseguro**

Las fuerzas que se asocian para el bien
no se suman, se multiplican (Concepción Arenal)

www.fundacionborreda.org