Nº 154 Abril 2023 – Año XXXII

SiC

www.revistasic.com

Revista
Ciberseguridad, seguridad de la información y privacidad

ENTREVISTA

Sergio Fidalgo
CSO Global y CISO Global
BBVA

CAIXABANK
Innovación en ciberseguridad y soberanía digital

EXPERTOS
Cómo resolver el talento de ciberseguridad en la empresa

EN CONSTRUCCIÓN
E pur si muove!

SECTOR ASEGURADOR
Despliegue de un marco de control integrado y automatizado

CISOs

LA ENCRUCIJADA REGULATORIA

V-Valley
enhancing your business

ESPECIALISTAS EN ADVANCED SOLUTIONS

Mayor rentabilidad y valor en tus proyectos de Ciberseguridad Corporativa

Acompañamos a los clientes a potenciar, aún más, sus proyectos de transformación digital dirigidos a clientes finales y Administraciones Públicas.

Network | Cloud | Workplace | Aplicación | Dato | Gestión

A10 · BACKBOX · VU · BROADCOM · CHECK POINT · CLOUDFLARE · CounterCraft · CyberRes · ENTRUST · ravenloop · kaspersky · McAfee · SONICWALL · MICRO FOCUS · Trellix · Skyhigh Security · TREND MICRO · WatchGuard

www.v-valley.es
seguridad@v-valley.com

YOU DESERVE THE BEST SECURITY

Sólo la mejor seguridad puede protegerte de las complejas ciberamenazas actuales.
Los ataques multivectoriales a gran escala ahora amenazan el tejido de las organizaciones en todo el mundo. Check Point Software te protege completamente contra estos ataques Gen V. En un mundo donde las amenazas son cada vez mayores, te mereces la mejor seguridad,
Check Point Software.

Quantum
Secure the Network

Harmony
Secure Users & Access

CloudGuard
Secure the Cloud

CHECK POINT™

MÁS INFORMACIÓN: www.checkpoint.com/es

info_iberia@checkpoint.com

SiC
Nº 154
Abril 2023

>> Sumario

>> en este número

• Con las regulaciones actualmente existentes (NIS2, DORA, ENS…), ¿es más fácil o no ser CISO? Esta es la pregunta que SIC ha formulado a cerca de 100 CISO, a la luz de lo que teníamos, tenemos y –que haya noticia– vamos a tener en materia regulatoria en la UE y España sobre ciberseguridad o en íntima relación con ella.

En general, y a tenor de las respuestas, se da por bueno el esfuerzo de cumplimiento que hay que afrontar, "a cambio" de que dicho esfuerzo traiga aparejado una mejor dotación presupuestaria y un apoyo mayor de los consejos y de las altas direcciones para poder ejecutar proyectos de adaptación a esa legislación, y otros que la misma va a permitir emprender para modernizar y alcanzar el hito de llevar a cabo transacciones completas con base en procesos digitales confiables y seguros para todos los intervinientes.

Aunque el paquete legislativo de la UE no está disponible al completo, la mayoría de los responsables de ciberseguridad que han contestado se sienten optimistas, aunque no pocos llaman la atención sobre la dificultad de interrelación entre tanta norma y el peligro de orientar las tareas al cumplimiento y no a la protección efectiva.

Una cosa es cierta: no ya los CISO, sino los CIO, van a tener que ponerse las pilas y bajar a la arena, porque la responsabilidad de cumplimiento (y ante incumplimientos) la tienen los máximos órganos de dirección de las entidades esenciales, importantes y… lo que toque.

Como diría un ejecutivo curtido: estamos entrando en el siguiente nivel.

• Nueva Estrategia de Ciberseguridad de EE.UU. Ya está publicado este interesante documento, en el que como aspecto muy destacable se considera al *ransomware* no solo como un delito (o varios concurrentes) sin más, sino como una amenaza a la seguridad nacional. Este hecho es relevante, porque abre nuevas vías para luchar contra este imparable fenómeno.

En la sección de Noticias de esta edición se publica un excelente resumen de esta Estrategia, incluyendo las iniciativas inmediatamente posteriores de la Casa Blanca para dotar presupuestariamente a algunas Agencias y Departamentos.

Hay otro frente que, al igual que a la UE, preocupa a la Administración americana: la ciberseguridad de la cadena de suministro en los entornos públicos y privados. La agencia de Seguridad de la Infraestructura y Ciberseguridad, CISA, ha abierto una oficina específicamente para gestionar riesgos en este entorno.

• Espacio TiSEC. Seguros Cibernéticos y otras incógnitas. Ciberseguridad endeble y ciberpólizas. Esta publicación sigue dando continuidad a uno de los temas que desde hace años tiene asociados a su Espacio TiSEC (13 y 14 de junio): el papel de los seguros en las estrategias empresariales para minimizar algunos daños causados por ciberataques, y la reacción de las aseguradoras y reaseguradoras ante el fenómeno del crecimiento en la superficie de ataque y la escasa formalización de procesos de ciberseguridad medibles.

El evento tendrá lugar en fechas en las que es de prever se haya calentado al máximo el debate sobre la idoneidad o no de que las organizaciones víctimas de *ransomware* notifiquen el pago de rescates, y las responsabilidades de este particular ante terceros.

Edita: Ediciones CODA, S.L. Goya, 39. 28001 Madrid (España) Tels.: 91 575 83 24 / 25 Fax: 91 577 70 47 **Correo-e:** info@revistasic.com www.revistasic.com **Editor:** Luis Fernández Delgado **Director:** José de la Peña Muñoz **Redacción:** Ana Adeva, José Manuel Vera **Sección Laboratorio SIC:** Javier Areitio Bertolín **Colaboran en este número:** Diego Alegre, Alberto Bernáldez, Juan Antonio Calles, Jorge Dávila, Carlos Fragoso, Mario Maawad, Ramon Martín de Pozuelo, Alberto Partida, Jennifer Sesmero, Jesús Urién, Jorge Uyá, José Valiente **Departamento de Marketing/Publicidad:** Rafael Armisén Gil, Fernando Revilla Guijarro **Administración y suscripciones:** Susana Montero, Maite Montero, Mercedes Casares **Fotografía:** Jesús A. de Lucas **Ilustración:** Fernando Halcón **Diseño y producción:** MSGráfica | Miguel Salgueiro **Imprime:** Monterreina **ISSN:** 1136-0623

SECURMÁTICA 2023

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

3 · 4 · 5 OCTUBRE

En buena compañía

Organiza

Revista SIC

www.securmatica.com

La IA sapiens y el antropoide con carné

José de la Peña Muñoz
Director
jpm@codasic.com

Cuando la evolución del clima fue cambiando el bosque y mutándolo en sabana, los homínidos tuvimos que desplazarnos por tierra para alcanzar el siguiente árbol. Y eso marcó nuestro destino. De ahí a pensar y a servirnos de herramientas para hacer cosas todo fue uno.

Queda claro que, desde entonces, la especie humana ha llevado impreso en sus genes el ánimo de explorar, de descubrir, de conquistar, de someter… Comemos de todo, vivimos en donde toque, adaptamos el medio a nuestras querencias y hemos ido criando un acervo lleno de luces y sombras, ciencias y creencias, que justifican una cosa y la contraria.

Al tiempo que en unos meses el Gobierno de España deberá presentar un proyecto de ley de grandes simios, los Homo nos hemos percatado de que sin los servicios de nube de algunos hiperescalares privados, Ucrania no se hubiera mantenido como Estado tras el ataque de Rusia.

Es curioso que en pleno proceso de transformación descontrolada, motivada por el uso intensivo de unas TIC con las que se aspira a automatizar todo lo que se menea, cuando la sociedad y millones de sus individuos, presas de un ánimo inagotable por hacer y deshacer, andan aplicando las matemáticas para ser como los dioses, crear algoritmos inteligentes y manipular la vida… nos encontremos en España con uno de esos deliciosos peteretes que nos regalan de vez en cuando nuestros congéneres Homo gubernamentales y parlamentarios. ¿A qué me refiero? Pues a la Ley 7/2023, de 28 de marzo, de protección de los derechos y el bienestar de los animales, en cuya Disposición adicional cuarta podemos leer lo siguiente: "En el plazo de tres meses a contar desde la entrada en vigor de la presente ley, el Gobierno deberá presentar un proyecto de ley de grandes simios".

Lo paradójico de todo esto es que, en España, el sapiens sapiens ha llegado casi a la vez a desarrollar su Estrategia Nacional de Inteligencia Artificial y los derechos de los antropoides. Lo primero se lleva en la SEDIA, y lo segundo, no. Y es muy posible que el reconocimiento de derechos a los póngidos (estoy de acuerdo) nos vaya a traer menos quebraderos de cabeza que hacer y usar una IA que merezca tener derechos.

Para empezar en el seno del Consejo Asesor de IA hay revuelo. Resulta que el Gobierno de España y un Laboratorio de Emiratos Árabes habían acordado que el segundo pusiera su sede europea en Granada. Y ante esto, varios miembros han dimitido por no considerar que en el proyecto se vayan a respetar principios éticos y de seguridad en el desarrollo de nuevas tecnologías.

Y en otro orden de cosas, aunque con cierta relación, Microsoft ha dado noticia de su Security Copilot, una IA "moldeada por la IA generativa GPT-4 de OpenAI", que ayudará a las empresas a minimizar los riesgos de ciberseguridad. Tiene pinta de que será más barata que los servicios de un buen analista.

Todo esto demuestra que nuestra especie sigue siendo curiosa, viajera, descubridora, arriesgada. Y que, ya de forma consciente ya inconsciente, lleva gestionando riesgos desde hace miles de años.

Estos tiempos que nos está tocando vivir nos están enseñando cosas nuevas; por ejemplo, que sin los servicios en la nube de grandes hiperescalares privados, Ucrania no se hubiera mantenido como Estado tras el inicio de la "operación especial" de Putin; o que el *ransomware*, si las cosas siguen así, será considerado globalmente (y no solo por EE.UU.) como una amenaza a las seguridades nacionales; o que los estados democráticos en los que el entramado público-privado alcance cotas significativas van a tener que revisar la idea de que los únicos que pueden en derecho usar armas (incluidas las cibernéticas) en guerra sean los militares.

Una cosa más: los delitos con sabor cibernético se están disparando. Y el sistema judicial y policial que tenemos no va a poder dar curso a tanto suceso y tanta denuncia. Menos todavía a su feliz resolución. Este es un buen territorio para cambiar, descubrir, arriesgarse… y aplicar IA e ingeniería de automatización. De las buenas. ●

SIEMENS

Maximiza la disponibilidad e integridad de tus **sistemas OT**

Identifica sus vulnerabilidades y solvéntalas con el Servicio de Consultoría IEC 62443

Las ciberamenazas en entornos OT son una realidad creciente. En Siemens lo sabemos bien. Nuestras fábricas y nuestro equipo de profesionales les hacen frente día a día siendo la norma IEC 62443 una de nuestras mejores herramientas.

Por eso, nuestra sólida experiencia aplicando la IEC 62443 nos convierte en tu mejor aliado para incrementar la protección de tus sistemas de automatización y control industrial durante todo su ciclo de vida.

Te ayudamos a identificar las vulnerabilidades más críticas de estos sistemas y proporcionamos las medidas más adecuadas para su mitigación, con servicios a medida y casos de uso concretos. Todo ello, independientemente del tipo de sistema y fabricante instalado. Estamos a tu lado para que puedas proteger lo que es importante para ti.

Maximiza ya la disponibilidad e integridad de tus sistemas de control industrial con Siemens.
siemens.com

Luis Fernández Delgado
Editor
lfernandez@codasic.com

El CISO áureo y el CISO fistro

Ha querido el destino y un centenar de ellos –que asoman su figura en esta edición de SIC–, que sea el CISO el tema central de mi tribuna y de este número de abril de la revista. No es para menos. Corren tiempos efervescentes para la llevanza de la profesión, disciplina, oficio o como queramos llamarlo, un cometido que enfila ya su próximo futuro con menos incógnitas y encaramado a lomos regulatorios de un más halagüeño porvenir.

Uno, con ya 32 años tras de sí en este 'negociado' de la ciberprotección, no puede por menos que echar la vista atrás y rememorar las vicisitudes de una encomienda tanto tiempo incomprendida y arrinconada, y a la vez vista como incómoda y objeto de vituperio. Nadie en este asunto se libraba del sanbenito de ser etiquetado como paranoico y 'stopper' pero hete aquí que la odisea digital de nuestra sociedad, decididamente abalanzada a un incierto y despendolado destino, se ha visto forzada a consagrar la existencia del CISO, so pena de que el quebradizo y desconfiable entramado internáutico que edifica acabe yéndosele al garete.

La odisea digital de nuestra sociedad, decididamente abalanzada a un despendolado destino, se ha visto forzada a consagrar la existencia del CISO, so pena que el quebradizo y desconfiable entramado internáutico que edifica acabe yéndose al garete.

Se dice que tanto los antiguos griegos como el renacentista sabio da Vinci estuvieron obsesionados con la llamada proporción áurea, esencial para sus ideales de belleza y geometría, y que Leonardo la aplicó al cuerpo humano y a la arquitectura desde que realizó el dibujo del célebre Hombre de Vitruvio. Metafóricamente la áurea y divina proporción viene que ni al pelo para definir las bondades profesionales de lo que hoy día debería ser un buen CISO.

Por otra parte, sin temor al yerro puede decirse que estamos enfrascados ya en la tercera generación de CISOs y bien está que así sea, pero quien esto firma, en claro homenaje a los pioneros, no quiere dejar de mentar a algunos de aquellos precursores que, a tientas y con indómito valor, lidiaron con unos tiempos pretéritos ásperos y desagradecidos. Vaya así desde SIC el cálido recuerdo a Manuel Palau (Iberdrola), Aurelio Hermoso (Iberia), Javier Valdés (Bankinter), Manuel Carpio (Telefónica), Ángel Bernaldo de Quirós (Renault), Lluis Salas (Allianz), Pedro Pablo López Bernal (RSI)… y también a aquellos que prematuramente nos dejaron: Jaime de Pereda (Amena), Fernando Víctor Ferrá (Banca March), Gabriel Arriero (Defensa)…*

Tampoco quiero dejar de mentar, ahora que algunas *güimenforsaiber* dicen no conocer referentes, que ya en su momento hubo auténticas colosas de la llevanza: Toñi García Redondo (Iberia), Mª Esther Vidal (Banco de España) o Idoia Mateo (Grupo Santander) –aún hoy una referencia ineludible de *savoir faire*–. Por cierto, todas ellas Premio SIC.

Y llegados a esta tercera generación, no poca de ella aterrizada en modo 'voluntarismo forzoso' por mor de ser nombrados precipitadamente, impelidos por la opresiva atmósfera regulatoria y por escamados CISOs más veteranos con gran mosqueo por la endeble consistencia de sus frágiles cadenas de suministro, huérfanos las más de las veces de interlocutores apropiados, y con órdenes de la superioridad incluso de tener que inmolarse en casos de fatal obediencia debida.

Así que hoy no es extraño toparse con especímenes de perfil peculiar –si no generalizado sí bastante relevante– conformado por gente pelín bisoña, tecnoréxica y con más querencia por *apatrullar* el ciberespacio empresarial cazando cibergüenzas que por entender cómo maridar su pericia con el tuétano negocial de la empresa que abona su nómina.

Estos genuinos ChiquitoCISOs de la Calzada cibernética, tejemanejan *fistramente* la ciberseguridad *diodenal* desde sus fuera*Boards* cual *condemores* de la pradera digital.

Con todo, y a pesar de los tiempos perros que nos toca vivir, en los que la ciberprotección hialurónica fija discontinua, ansiolítica, exfoliante y retrofuturista, hace no poca mella, todo CISO que se precie y desee refulgir, frente a la creciente madurez que experimenta la profesión y el tsunami legislativo que le sobreviene, bien que le aplica el sabio aforismo asociado a nuestra querida ciberseguridad: "Contigo porque me matas y sin ti porque me muero". ●

** Con gran consternación, al cierre de esta edición tuvimos conocimiento del fallecimiento inesperado de una veterana compañera en lides de la ciberseguridad: Ana Prieto, Security Manager de Ericsson. Transmitimos nuestro pésame a toda su familia y allegados.*

Identi::SiC

Organiza:

Revista SiC

www.revistasic.com/identisic

Madrid_
15 y 16 de noviembre_2023
Hotel Novotel Campo de las Naciones

Europa

Aún sin fecha de aprobación, obligará a todos los fabricantes de productos vendidos en la UE a actualizar su protección a lo largo de su vida útil, entre otros aspectos

La Ley de Ciberresiliencia europea comienza a tomar su forma final estableciéndose sus líneas de acción y cómo se vigilará su cumplimiento

La **Unión Europea** continúa dando pasos para mejorar la ciberseguridad de sus infraestructuras. En los últimos meses, ha sido notable el paso dado hacia la aprobación de la **Ley de Ciberresiliencia** (**CRA**), que busca que los productos que se comercialicen en la Unión traigan unos mínimos de ciberprotección por defecto. Entre los últimos avances en el proyecto que se está trabajando, se ha aceptado ajustar la definición del ciclo de vida del producto a la especificidad del mismo y mover el informe de vulnerabilidades a nivel nacional en un nuevo compromiso, según se dio a conocer tras la reunión de febrero del **Grupo de Trabajo Horizontal sobre Cuestiones Cibernéticas,** el órgano técnico del **Consejo de la UE** que establece el trabajo preparatorio para la aprobación ministerial. Un objetivo que, desde hace muchos años, ya cumplen sectores como el de bienes de consumo o el de automoción.

Así, en ella también se debatió sobre la evaluación de la conformidad y la lista de productos críticos que deberán pasar por una evaluación de terceros antes de ser comercializados en el mercado europeo.

El texto se ha modificado para explicar mejor los ciclos de vida de los diferentes productos. "Los fabricantes se asegurarán de ofrecer un producto con elementos digitales en el mercado y durante un período de tiempo posterior a la comercialización apropiado para el tipo de producto y su vida útil esperada", se lee en el documento de trabajo.

En cualquier caso, si el dispositivo conectado de un producto tiene más de cinco años, el fabricante debe proporcionar parches de seguridad durante al menos ese tiempo. La fecha de caducidad del soporte técnico de seguridad debe figurar en el embalaje del producto. Si el fabricante identifica un problema de seguridad, tiene la obligación de diligencia debida de implementar actualizaciones de seguridad durante, al menos, 10 años. El mismo plazo se aplica si se entera o tiene razones para creer que su producto ya no cumple con los requisitos de seguridad de la regulación.

La propuesta original obligaba a los fabricantes a informar a la **Agencia de Ciberseguridad de la UE** (**Enisa**), sobre cualquier vulnerabilidad de producto explotada activamente. Este enfoque planteó preocupaciones respecto a la capacidad del organismo para manejar cientos de miles de estas notificaciones y crear un posible "punto único de falla" de información confidencial que es atractivo para los piratas informáticos. Por lo tanto, el Consejo de la UE parece estar apartándose de esta idea y optar por alinear la obligación de notificación con las de la Directiva NIS2, trasladando la notificación al Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT).

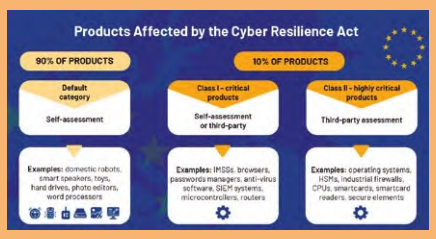
Luego, los CSIRT enviarían la notificación a Enisa y a las autoridades de vigilancia del mercado de todos los estados miembro interesados. La propuesta ahora será discutida a nivel técnico hasta que se encuentre una posición común.

Vulnerabilidades conocidas

El texto inicial requería también que los fabricantes no lanzaran ningún producto con vulnerabilidades explotables conocidas en el mercado único de la UE. Ahora, se ha cambiado el enfoque, condicionando esta obligación a la evaluación del riesgo de ciberseguridad por parte de los fabricantes. En otras palabras, los productos aún podrían venderse si los fabricantes consideran que el riesgo es muy bajo. La idea es reducir la burocracia y dar mejor cuenta de los casos en los que una vulnerabilidad podría corregirse más tarde con una actualización de seguridad.

Productos que se consideran 'críticos' y 'altamente críticos', incluyendo los de ciberseguridad

En el nuevo borrador de la Ley presentado, se destaca que, mientras que para la mayoría de los dispositivos conectados, los fabricantes podrán autoevaluar el cumplimiento de dichos requisitos, para algunos productos específicos considerados 'críticos' o 'altamente críticos' será necesaria una auditoría externa. Ese es el caso del software de detección de *malware,* los sistemas de monitorización de tráfico de red para control de flujo y rendimiento, información de seguridad y sistemas de gestión de eventos, sistemas que implementan actualizaciones y parches de seguridad, cortafuegos, certificados digitales y dispositivos domésticos inteligentes con funcionalidades de seguridad como sistemas de alarma.



Otro subgrupo de productos digitales se considera 'crítico' si desempeñan un papel central en la gestión de un sistema más amplio o si tienen el potencial de dañar varios productos, como la gestión de red y el control de configuración. Estarían en este grupo, por ejemplo, los navegadores independientes e integrados, la gestión de recursos de red, el software de acceso remoto, las interfaces de red físicas y virtuales, los enrutadores, los microprocesadores y los sistemas operativos y los productos industriales, así como los sistemas de control no incluidos en la categoría 'altamente crítica'.

En cuanto a los 'altamente críticos' serán considerados como tales los que tienen una función de seguridad importante y son fundamentales en un entorno de IoT más amplio. Ejemplos de ellos son los sistemas de gestión de identidad, así como las herramientas de autenticación, Redes Privadas Virtuales (VPN), sistemas de gestión de red para la configuración, monitorización y actualización de dispositivos de red, hipervisores, microprocesadores para elementos seguros, dispositivos basados en chips de seguridad, hardware de seguridad modelos, criptoprocesadores seguros y lectores de tarjetas inteligentes.

También, estarían en este bloque los *firewalls* para uso industrial que se clasificarán si tienen una función relacionada con la ciberseguridad y se utilizan en entornos sensibles, incluida la configuración de control industrial para entidades designadas como 'esenciales' en virtud de la NIS2. Para facilitar el cumplimiento de la normativa en este aspecto se ha incluido en el anexo al proyecto de ley una lista que, se espera, pueda actualizarse más fácilmente que el cuerpo del texto.

¿Qué es más perjudicial: la pérdida de datos o de confianza?

Un ciberataque puede destruir intangibles tan valiosos para tu organización como la confianza. Para salvaguardarla, tu estrategia de ciberseguridad debe enfocarse en la prevención de forma proactiva. Descubre cómo desde EY podemos ayudarte.

The better the question.
The better the answer.
The better the world works.

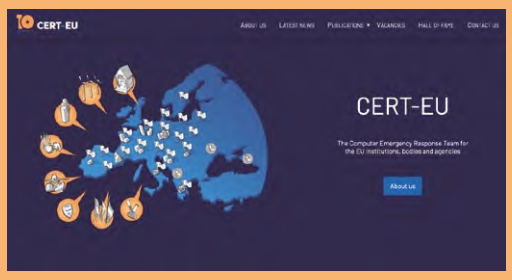
EY
Building a better working world

Europa

EN BREVE

EUROPA intensifica la detección y respuesta frente a APTs, con una alerta a todos los países de Enisa y CERT-EU

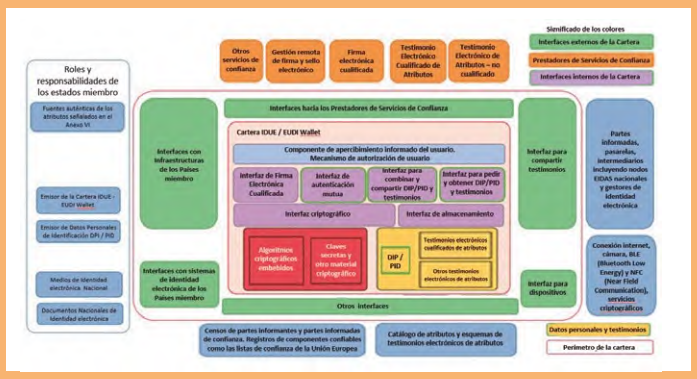
En un documento firmado en febrero, de forma conjunta, por **Enisa** y el **Equipo de Respuesta a Emergencias Informáticas para las instituciones, organismos y agencias de la UE** (CERT-EU) se alertó a empresas y organismos públicos del posible impacto de amenazas persistentes avanzadas (APT) de grupo concretos como APT27, APT30, APT31, Ke3chang, Gallium y Mustang Panda. "El 19 de julio de 2021, la UE instó a las autoridades chinas a tomar medidas contra las actividades cibernéticas maliciosas realizadas desde su territorio y vinculadas a APT31", se lee en la publicación. Estos ataques "tuvieron efectos significativos, se dirigieron a instituciones gubernamentales y organizaciones políticas en la UE y los estados miembro, así como a industrias europeas clave", destaca el documento, que recuerda que "las operaciones recientes por estos actores se centraron principalmente en el robo de información".



Para defenderse de estos y otros actores de amenazas similares, las agencias europeas presentan una serie de recomendaciones en el documento entre las que están seguir las mejores prácticas de los proveedores para fortalecer productos, administrar cuentas de administrador y activos críticos, y garantizar controles de acceso adecuados para usuarios finales y contratistas externos.

La normativa eIDAS2 avanza hacia su aprobación, entrando ya en la fase de su negociación interinstitucional

El nuevo marco de identidad digital europeo, eIDAS2, espera proporcionar a los ciudadanos de la UE acceso digital a servicios públicos clave a través de las fronteras de la UE. De momento, continúa avanzando después de ser votado y aprobado por la **Comisión de Industria, Investigación y Energía**. En sus enmiendas, los eurodiputados proponen hacer de la Cartera de Identidad Digital Europea una herramienta que también pueda leer y verificar documentos electrónicos y permitir interacciones entre pares. Cabe recordar que el uso de la billetera de la UE siempre será voluntario, ya que los eurodiputados también quieren asegurarse de que los ciudadanos que decidan no adoptarlo no sean tratados de forma diferente a los que sí lo hagan. El esquema requeriría que cada estado miembro notifique al menos una 'cartera' bajo un esquema nacional de identificación electrónica para que sean interoperables a nivel de la UE. El proyecto de ley incluye disposiciones para solicitar, obtener, almacenar, combinar y utilizar de forma segura datos de identificación personal y certificados electrónicos, que pueden utilizarse para autenticarse en línea y fuera de línea, y para acceder a bienes y servicios públicos y privados.



Precisamente, según destacó en su blog 'Todo es electrónico', **Julián Inza,** con la publicación del documento 'European Digital Identity Wallet Architecture and Reference Framework' (en la imagen), se proporciona un conjunto de especificaciones necesarias para desarrollar una solución interoperable de Cartera Europea de Identidad Digital (IDUE) basada en normas y prácticas comunes.

EUROPA aprueba una inversión de 2.400 millones para una nueva red de satélites que permita, también, hacer frente a ciberataques

El pleno del **Parlamento Europeo** aprobó, en febrero, un presupuesto de 2.400 millones de euros para la primera constelación de satélites multiorbitales de Europa, bautizada como IRIS² (Infraestructura para la Resiliencia, la Interconectividad y la Seguridad por Satélite), que tendrá el objetivo de garantizar una red de telecomunicaciones segura y protegida contra posibles ciberataques. Se espera que pueda proporcionar una infraestructura de comunicaciones segura para los organismos y agencias gubernamentales de la UE, los servicios de emergencia y las delegaciones europeas en todo el mundo.

La iniciativa también busca garantizar la autonomía estratégica de la UE en el ámbito de las comunicaciones gubernamentales, en un contexto en el que las amenazas a la ciberseguridad son cada vez más importantes, especialmente tras la guerra de Rusia contra Ucrania.

comforte

¿ESTÁ LISTO PARA MEJORAR LA DEFENSA DE LOS DATOS?

Mantenga sus datos seguros, donde quiera que circulen mediante comforte Data Security platform

www.comforte.com

EE.UU.

Basará su acción en cinco pilares y considera el *ransomware* un problema de seguridad nacional

La CASA BLANCA publica su nueva Estrategia Nacional de Ciberseguridad poniendo foco en los proveedores de software y servicios para que sean realmente seguros por diseño

Tras muchos meses de espera, en marzo, la **Casa Blanca** publicó finalmente la Estrategia Nacional de Ciberseguridad. Entre sus aspectos más llamativos destaca que, a partir de ahora, EE.UU. tratará los ataques de *ransomware* como amenaza a la seguridad nacional y no como un mero delito. Con ello se pretende dar a este tipo de ciberataques la máxima prioridad, permitiendo a los **Departamentos de Estado** y del **Tesoro** emitir sanciones contra las entidades responsables de ejecutarlos. Una iniciativa que, según fuentes de la Casa Blanca, espera sumar fuerzas con el apoyo de otros países. La Estrategia también identifica a Rusia, China, Corea del Norte e Irán como los cuatro principales "actores maliciosos" a combatir e, incluso, destaca de forma concreta la "visión del autoritarismo digital" chino que intenta exportar y de Rusia sus esfuerzos para desestabilizar las democracias occidentales, mediante ciberataques o interferencias en sus elecciones a través de la labor de grupos cibercriminales a los que da asilo.

Además, es especialmente llamativo, según han destacado muchos expertos, que la Estrategia cambia el enfoque actual buscando trasladar el peso de la gestión del riesgo cibernético de los individuos y las pequeñas empresas a las compañías tecnológicas, al tiempo que adopta un enfoque más ofensivo para tratar con los actores de amenazas. "Demasiados proveedores ignoran las mejores prácticas para el desarrollo seguro, envían productos con configuraciones predeterminadas inseguras o vulnerabilidades conocidas e integran software de terceros de procedencia no examinada o desconocida", explica el documento. En este sentido, también deja entrever que el Gobierno apostará por más regulación en el ámbito cibernético,

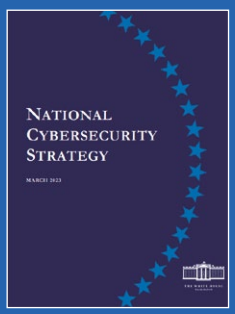
Kemba Walden

quizá, siguiendo los pasos que está marcando Europa en este tema, apostando por más normativas y auditorías.

Cinco pilares

El documento destaca cinco pilares, muchos de los cuales ya se están aplicando esta legislatura: la defensa de infraestructuras críticas, como la red eléctrica; la disrupción de amenazas; el impulso de la ciberseguridad a través de estímulos al mercado; la inversión en el futuro; y el desarrollo de alianzas internacionales. De hecho, en ámbitos muy específicos, como el de infraestructuras críticas, se van a pedir unos requisitos mínimos de ciberseguridad a los principales operadores, algo que Europa también hará a través de la Directiva NIS2.

Presupuesto para 2023



Una semana después de publicarse la Estrategia, el gobierno presentó su propuesta de presupuesto para el año 2024 destinando, entre otros conceptos, 2.878 millones de dólares a la infraestructura de ciberseguridad, 134 millones a la **Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA)**, 91 millones para la implementación de la Ley de Informes de Incidentes Cibernéticos para Infraestructuras Críticas, y 394 millones para mejorar las capacidades analíticas y de ciberseguridad interna de CISA, así como otros 227 millones para mejorar la protección de las tecnologías de energía limpia y la cadena de suministro de energía.

También, el **Departamento de Justicia** contará con una partida para mejorar su ciberseguridad con 58 millones más que en 2023, al igual que el **Departamento del Tesoro**, que pasará de 106 a casi 200 millones, sobre todo, para ciberproteger sistemas e información confidenciales. El Departamento de Estado recibirá 366 millones, de los que una parte irá destinado a implementar las iniciativas que tiene en marcha. Además, habrá una partida de 371 millones para luchar en el ciberespacio contra China y casi 700 millones para Ucrania, "contrarrestando la influencia maligna rusa y satisfacer las necesidades de la sociedad civil", en este ámbito.

Situación crítica

También, ha sido notable que la **Oficina de Responsabilidad Gubernamental** (GAO) emitió un informe en el que recomienda a la Casa Blanca trabajar más para implementar una "estrategia nacional integral de seguridad cibernética" que incluya una supervisión sólida y aborde la gama completa de "características deseables de las estrategias nacionales". "Hasta que el gobierno federal desarrolle e implemente completamente una estrategia nacional integral, no tendrá una hoja de ruta clara para superar los desafíos cibernéticos que enfrenta nuestra nación", destacó el organismo de control.

Oficina para proteger la cadena de suministro

De forma paralela, CISA ha abierto una oficina de gestión de riesgos de la cadena de suministro para ayudar a los sectores público y privado a implementar políticas y orientación recientes del organismo.

También ha presentado, junto con el departamento de **Colaboración Conjunta de Defensa Cibernética (JCDC)**, una 'Iniciativa de notificación previa al *ransomware*', para ofrecer a las empresas advertencias tempranas que permitan anticiparse al cifrado de datos por *ransomware*.

No ha faltado un movimiento laboral importante por cuanto el primer director cibernético nacional de los Estados Unidos, **Chris Inglis,** se jubiló a principios de febrero, ocupando su cargo, de forma interina, **Kemba Walden**.

Soluciones de Seguridad de Negocio

Nuestra dependencia de la tecnología va en aumento y las amenazas son cada vez mayores y más sofisticadas.

Por ello, en PwC disponemos de soluciones de seguridad del negocio y servicios profesionales adaptados a nuestros clientes para acompañarles en la gestión del riesgo tecnológico, proteger sus empresas de ataques críticos y ayudarles a construir una cultura de ciberseguridad sólida.

Juntos, podemos construir una sociedad digital más segura.

www.pwc.es/bss

pwc

EE.UU.

EN BREVE

El NIST publica su propuesta de Marco de Gestión de Riesgos de Inteligencia Artificial

El **Instituto Nacional de Estándares y Tecnología de EE.UU.** (**NIST**) ha publicado dos documentos de referencia. Por un lado, su esperado Marco de Gestión de Riesgos de Inteligencia Artificial (AI RMF), tras más de año y medio de trabajos.

Un informe que aspira a ser utilizado por organizaciones de todo el mundo y en todo tipo de sectores. Con él, se espera ofrecer una ayuda para las organizaciones para desarrollar sistemas de IA de bajo riesgo, entre otras cuestiones. Tras los comentarios recibidos hasta febrero se presentará una versión actualizada de este documento antes de verano.

Además, el organismo ha presentado el Estándar de firma digital (DSS), **FIP 186-5,** que reemplazará a FIPS 186-4, que especifica un conjunto de algoritmos que se pueden utilizar para generar una firma digital de forma más segura y ha seleccionado algoritmos de 'criptografía ligera' para proteger dispositivos pequeños.

En concreto, el elegido en este aspecto fue **Ascon**, que se publicará como el estándar de criptografía ligera del NIST en 2023, y permitirá proteger mejor la información creada en dispositivos IoT.

Actualización del Marco de Ciberseguridad

Asimismo, NIST ha presentado un documento conceptual para actualizar su marco de ciberseguridad (CSF 2.0) nuevamente -se publicó por primera vez en 2014 y se evolucionó en abril de 2018 con CSF 1.1-. De momento, está abierto a revisión y comentarios hasta este mes de marzo. También ha publicado las pautas actualizadas de gestión de la identidad para organismos con el objetivo de ayudar a la administración a combatir el fraude y el delito cibernético. El borrador, titulado formalmente 'Directrices de identidad digital (NIST Special Publication 800-63 Revisión 4)', cubre los requisitos técnicos para establecer y autenticar representaciones digitales de personas de la vida real, como empleados de un contratista del gobierno o miembros del público en general.

La OFICINA DE RESPONSABILIDAD GUBERNAMENTAL exige que las agencias federales se tomen más en serio la ciberseguridad

La **Oficina de Responsabilidad Gubernamental (GAO)** ha publicado un nuevo informe en el que destaca que tres importantes agencias federales, concernidas en temas de ciberseguridad, deben intensificar y hacer mejor su trabajo, pidiendo que se tomen más en serio sus recomendaciones. Además, recuerda que, desde 2010, se han hecho 712 recomendaciones en informes y que "hasta que estas se implementen por completo, las agencias federales estarán más limitadas en su capacidad para proteger los datos privados y confidenciales que se les confían".

Asimismo insta a la **Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA)** a "mejorar la implementación de las iniciativas de ciberseguridad en todo el gobierno", a la **Oficina de Administración y Presupuesto** (OMB) que aborde las debilidades en los programas de seguridad de la información de las agencias federales y finalmente considera que el Departamento de Defensa (DoD) debe mejorar su respuesta a los incidentes cibernéticos. "Además, el organismo también emitió una alerta destacando que muchas de sus recomendaciones para proteger los servicios de infraestructura crítica de las amenazas cibernéticas no se han implementado desde 2010". En concreto, encontró que de las 106 publicadas desde entonces, hasta diciembre de 2022, solo 46 se han implementado.

El PENTÁGONO ultima la publicación de su estrategia de fuerza laboral cibernética y cómo aplicarla

El **Departamento de Defensa** ha dado a conocer su nueva 'Estrategia de fuerza laboral cibernética', así como su propuesta para llevarlo a cabo y que ha llevado casi un año de trabajo. En concreto, se basa en cuatro pilares que son la identificación, reclutamiento, desarrollo y retención del talento, además de varias recomendaciones para que la búsqueda de profesionales esté acorde a los desafíos actuales de capacitación, retención y reclutamiento.

Un aspecto preocupante en áreas críticas como la Seguridad y Defensa, ya que se ha constatado en un reciente informe que en la administración estadounidense había más de 40.000 puestos sin cubrir a abril de 2022 en este ámbito. Una cifra que se incrementa a 700.000 en el privado.

Esto, según fuentes del Pentágono está afectando a sus operaciones por lo que, con esta estrategia, se quiere hacer atractiva la oferta laboral en las agencias de Defensa tanto para civiles, como militares y contratistas.

El documento también recomienda basar su trabajo en el uso de análisis predictivos, para poder identificar de manera más efectiva qué tipo de profesionales cibernéticos o funciones de la fuerza laboral cibernética faltan o serán necesarios en el DoD según evolucione la situación geopolítica.

Implemente un Acceso Zero Trust a cualquier recurso.

Descubra una alternativa mas segura y rápida a las VPNs.

barracuda.com

Barracuda®
Your journey, secured.

Celebrará la próxima reunión de su Junta de Gobierno, antes de verano, ya en su nueva sede en Bucarest

El CENTRO EUROPEO DE COMPETENCIA EN CIBERSEGURIDAD avanza en su Agenda Estratégica y en cómo vertebrar sus inversiones

El **Centro Europeo de Competencia en Ciberseguridad** (ECCC), que actualmente tiene como director ejecutivo interino al español **Miguel González Sancho,** celebró la quinta reunión de su Consejo de Administración en Varsovia (Polonia), a mediados de marzo, y continúa dando pasos hacia la futura inauguración de la sede en Bucarest (Rumanía), en la que se celebrará la próxima cita de este tipo, antes de verano. De momento, en ella se debatieron diferentes asuntos relacionados con las prioridades y operaciones del Centro. Además, previa a esta jornada de dos días de duración, se realizó otra reunión de la Red de Centros Nacionales de Coordinación (NCC).

Durante esta jornada, la Junta de Gobierno del ECCC hizo un balance del progreso de varios Grupos de Trabajo centrándose en aspectos como la comunidad de ciberseguridad, las habilidades cibernéticas, el apoyo a Ucrania, la red de NCC o la Agenda Estratégica del Centro. Además, se identificaron sus prioridades de inversión para "fortalecer el liderazgo y autonomía de la UE, mediante el desarrollo de capacidades de investigación, académicas, sociales, tecnológicas e industriales de ciberseguridad", así como "apoyar las capacidades y habilidades tecnológicas de la UE en relación con la resiliencia de la infraestructura de redes y sistemas de información, incluida la infraestructura crítica y el hardware y software de uso común en la Unión". Asimismo, manifestaron su apuesta por "aumentar la competitividad global de la industria de la ciberseguridad de la Unión con un fuerte enfoque en las pymes y las empresas emergentes".

Objetivo 2027

Para ello, tanto el ECCC como su Red de NCC, en la que está presente España a través del **Incibe,** implementarán hasta 2027 una serie de medidas, entre las que destaca la de financiar a las pymes europeas, a través de un mecanismo coordinado a través del NCC, con cofinanciación nacional; diferentes iniciativas para "apoyar y hacer crecer la fuerza laboral profesional, tanto en cantidad como en calidad, incluso a través de la estandarización y certificación de habilidades de ciberseguridad e inversiones en educación y capacitación de profesionales"; así como, "el desarrollo e implementación de un plan de acción eficiente y coherente para fortalecer la experiencia en investigación, desarrollo e innovación y la competitividad en ciberprotección de la UE".

Para lograrlo, el Centro gestionará parte de la financiación dedicada a la ciberseguridad en el Programa Europa Digital y el Horizonte Europa, en colaboración con la inversión que acometan en este ámbito los estados miembros. Precisamente, se ha realizado una convocatoria recientemente, por valor de 176 millones de euros, en el marco de la primera, para diferentes propuestas en este ámbito.

ENISA alerta de las vulnerabilidades en el sector del transporte, analiza el mercado de ciberseguridad en la nube y nombra su nuevo Grupo Asesor

La **Agencia de Ciberseguridad de la UE** (Enisa) publicó, en marzo, su primer informe sobre el panorama de las ciberamenazas dedicado al sector del transporte en el que mapea y analiza los incidentes cibernéticos en relación con el transporte aéreo, marítimo, ferroviario y por carretera, centrándose en el período de enero de 2021 a octubre de 2022. En él, destaca los ataques de *ransomware*, habiéndose casi duplicado, pasando del 13% en 2021, al 25% en 2022. Les siguen de cerca las amenazas relacionadas con los datos (brechas, fugas), ya que los ciberdelincuentes tienen como objetivo las credenciales, los datos de empleados y clientes, así como la propiedad intelectual con fines de lucro.

También, es reseñable el informe de Enisa sobre el mercado de la ciberseguridad de la nube, en el que actualiza su marco de análisis, así como la puesta en marcha de su nuevo Grupo Asesor, con vigencia hasta 2025, con 33 expertos de todos los países del sector industrial, académico, organizaciones de consumidores y asociaciones profesionales y entidades de referencia.

Además, la Agencia celebró, en febrero, su séptima conferencia anual, sobre normalización, en colaboración con las **Organizaciones Europeas de Normalización (ESO), CEN, CENELEC** y **ETSI,** bajo el lema 'Normalización europea en apoyo de la legislación de ciberseguridad de la UE'. Y publicó un nuevo informe en el que explora cómo desarrollar programas e iniciativas armonizados de vulnerabilidad nacional en la UE –del que SIC se hizo eco de su anterior edición en el nº150–.

EUSKADI e IBM sellan una alianza en el campo de la computación cuántica, apostando por San Sebastián como referente

Ikerbasque, la **Fundación para la Ciencia en el País Vasco**, e **IBM** han cerrado un acuerdo para seguir a la región como *hub* tecnológico en la adopción de la computación cuántica, a través del lanzamiento del **IBM-Euskadi Quantum Computational Center**, que proporcionará servicios Qiskit Runtime desde un IBM Quantum System One de 127 qubits, ubicado en San Sebastián y gestionado por la multinacional. El IBM-Euskadi Quantum Computational Center es el segundo IBM Quantum Computational Center que se desplegará en Europa.

Más detección y respuesta

Por otro lado, IBM Security ha publicado su índice anual de Inteligencia de Amenazas, el 'X-Force Threat Intelligence Index', en el que destaca que, aunque la proporción de incidentes de *ransomware* disminuyó ligeramente de 2021 a 2022 (4%), ha aumentado el éxito en la detección y prevención. Pese a ello, los atacantes han continuado innovando pasando de necesitar dos meses de promedio para completar un ataque de *ransomware* a menos de cuatro días.

De acuerdo con el informe, el despliegue de 'puertas traseras' fue la acción más habitual ejecutada por los atacantes durante 2022. Alrededor del 67% de esos casos estuvieron relacionados con intentos de *ransomware*. Los ciberdelincuentes llegan a vender hasta por 9.400 euros los accesos existentes, mientras que los datos de tarjetas de crédito robadas, se venden hoy día por menos de nueve euros. La investigación también resalta que el principal objetivo de los ataques en 2022 fue la extorsión a partir del *ransomware*.

Aiuken Cybersecurity

Aiuken Cybersecurity de nuevo en la lista de 2023 de las 40 empresas importantes en MDRS publicada por Gartner®

Managed Detection & Response Services
la evolución de un MSSP.

www.aiuken.com

La directora del Centro Nacional de Inteligencia-Centro Criptológico Nacional, Esperanza Casteleiro, visita el Instituto Nacional de Ciberseguridad para impulsar la coordinación en ciberprotección entre ambos organismos

CCN e INCIBE se ven las caras en León

A finales de marzo, la directora del **Centro Nacional de Inteligencia (CNI), Esperanza Casteleiro,** y el subdirector general del **Centro Criptológico Nacional (CCN), Luis Jiménez**, acudieron a la sede leonesa del **Instituto Nacional de Ciberseguridad** (**Incibe**) para celebrar una reunión con su actual director, **Félix Barrio**. Este hecho, sin duda nada habitual, visibiliza una decidida vocación de avanzar por parte de dos de las principales entidades españolas con encomienda en las tareas de cibeprotección.

De izd. A dcha: Carla Redondo, Esperanza Casteleiro, Félix Barrio y Luis Jiménez

Tras el encuentro ambos responsables coincidieron en que la relación de cooperación entre el CNI e Incibe, que se articula a través del CCN, es cada vez más profunda e intensa, y acordaron establecer nuevas sinergias para seguir protegiendo el ciberespacio de ataques externos y combatir de manera conjunta las ciberamenazas que afecten a España. Aprovechando la visita, la Secretaria de Estado también tuvo la ocasión de conocer el servicio nacional del 017 y los nuevos programas desplegados por Incibe desde León.

Estrecha colaboración

De momento, la actual colaboración entre ambos organismos se plasma en varias iniciativas notables. La primera de ellas, hace foco en el trabajo conjunto en la gestión de incidentes de ciberseguridad mediante apoyo y soporte mutuo en incidentes que afectan a los sectores del ámbito competencial de cada entidad, además de intercambiar información sobre ciberamenazas. Así, el Incibe y el CNI, a través del CCN, comparten, de forma dinámica, información sobre amenazas cibernéticas que pueden afectar al sector público y privado, ampliando su capacidad de monitorización, detección y respuesta ante ciberataques. En este contexto, la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (PNNSC), desarrollada por el CCN en colaboración con el Incibe y el **Mando Conjunto del Ciberespacio (MCCE),** constituye una pieza clave en la colaboración entre los tres organismos. Del mismo modo, ambas organizaciones desarrollan una representación coordinada de la red de CERT y CSIRT nacionales en el ámbito europeo, a través de la **CSIRT Network** y colaboran en el desarrollo de prácticas y recomendaciones en ciberseguridad para los ámbitos competenciales de las dos entidades para ampliar las sinergias con organismos similares de otros países, como sucede con la organización conjunta de las próximas 'Jornadas STIC en República Dominicana', coordinadas junto al MCCE, del 19 al 21 de abril, y la reunión de alto nivel que la red CERT-CSIRT mantendrá en León durante la presidencia española de la UE.

Por otro lado, aprovechando la visita de la Directora del CNI, el organismo ha firmado un convenio de colaboración con la Diputación, a través de su presidente, **Eduardo Morán,** para el intercambio de información así como la cooperación en el impulso de proyectos y nuevas soluciones de seguridad para las entidades locales de la provincia. Además, Morán adelantó que se está trabajando en la implantación de un Centro de Ciberseguridad Provincial, el primero de estas características en todo el territorio nacional, para el que la institución contempla una inversión de 850.000 euros para los próximos tres años. "Estamos hablando de casi cinco millones de euros destinados a la seguridad informática de la Diputación y de los ayuntamientos de la provincia", destacó Morán.

Autoridades de ambas instituciones abordaron asuntos de mutuo interés

El portal web dedicado al ENS con información más accesible y actualizada, renovado

El **Centro Criptológico Nacional** (CCN) ha renovado el portal dedicado al Esquema Nacional de Seguridad (ENS) con una interfaz mucho más accesible y estructurada en torno a cuatro bloques temáticos: gobernanza de la ciberseguridad, certificación, marco normativo y formación. El apartado dedicado a la gobernanza detalla aspectos relativos a la gestión de la ciberseguridad a través de las herramientas Inés, Amparo y Marga. Por otra parte, la certificación permite consultar la relación de entidades privadas y públicas cuyos sistemas

han sido certificados en el ENS.

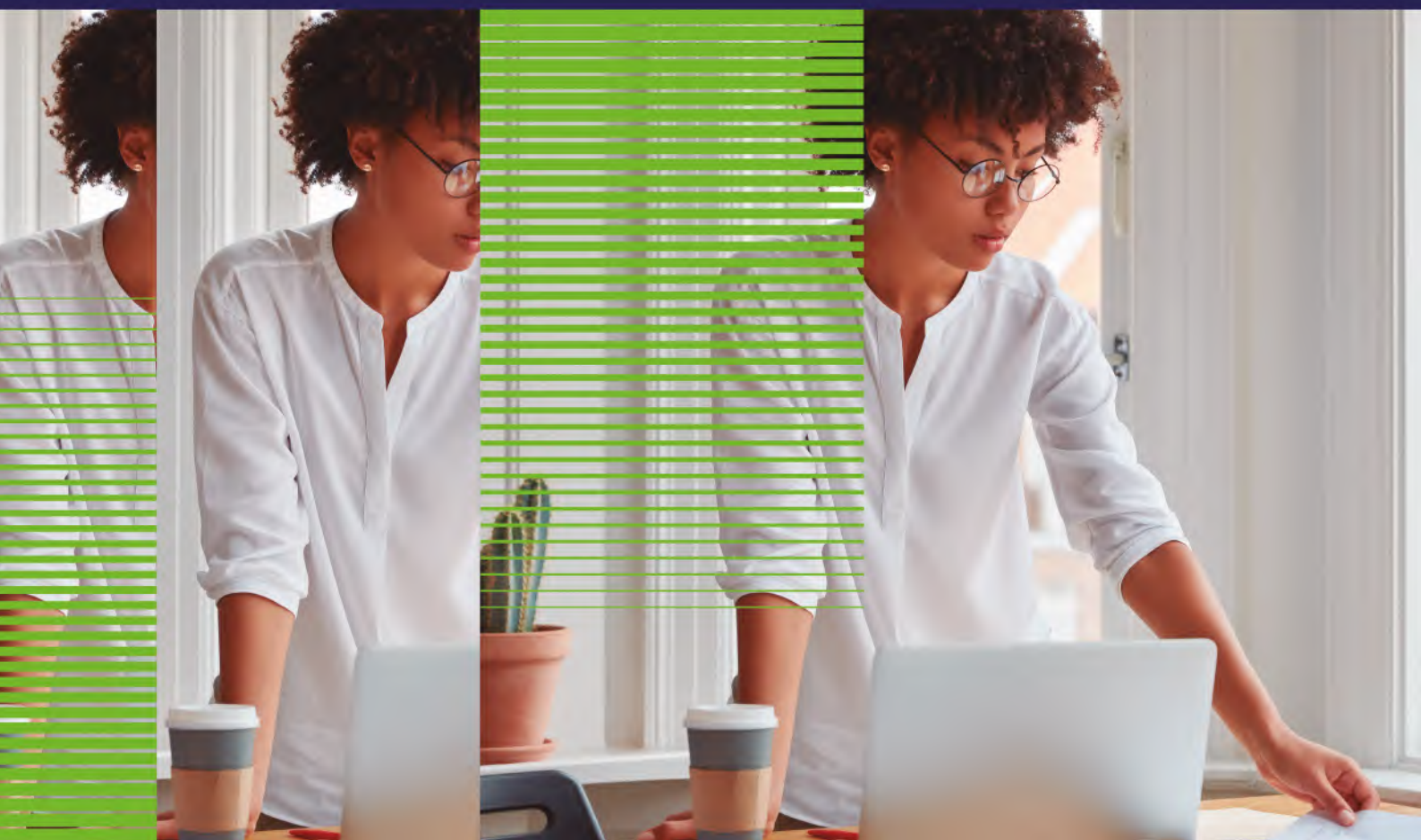
En tercer lugar, el apartado dedicado al marco normativo engloba todas las disposiciones y normativas aplicadas al ENS. Finalmente, el usuario encontrará en el apartado dedicado a la formación los cursos disponibles de la plataforma Ángeles, orientados al conocimiento y formación en el ENS. Además, incluye todas las empresas certificadoras, las certificadas, tanto del sector público, como privado y ayuntamientos, con su acreditación oficial conseguida y que se muestra en PDF.

Delinea

Accesos sin excesos

Simplifica la gestión de tus accesos privilegiados e impulsa el crecimiento de tu empresa

www.delinea.com/es/



Los ciberdelitos crecen un 72% en cuatro años y ya suponen uno de cada cinco de los cometidos en España

INTERIOR dedica, por primera vez, una partida específica a ciberprotección y da más peso a la OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

Interior comienza a dar a la lucha contra el cibercrimen con los medios acordes a la amenaza que supone. En una intervención en febrero, el titular de la cartera**, Fernando Grande-Marlaska,** presentó el diseño estratégico realizado por el departamento para hacer frente al incremento de la ciberdelincuencia, que incluye una campaña de concienciación y sensibilización ciudadana. "El doble efecto de descenso de criminalidad convencional y aumento de los ciberdelitos nos ha llevado a un punto de inflexión: hoy, uno de cada cinco delitos en España se comete en la red", explicó.

El ministro junto al secretario de Estado de Seguridad, Rafael Pérez; el director general de Coordinación y Estudios de la Secretaría de Estado de Seguridad, José Antonio Rodríguez; y los máximos responsables de la Policía Judicial en la Policía Nacional y la Guardia Civil, el comisario principal Rafael Pérez y el general Ángel Alonso.

Durante su intervención, recordó que las plantillas de las unidades centrales y periféricas especializadas en ciberseguridad de **Policía Nacional** y **Guardia Civil** se han doblado en cuatro años, pasando de 714 agentes en 2018 a 1.352 en 2022. Además, por primera vez, la **Secretaría de Estado de Seguridad** contará con una dotación específica de cinco millones de euros para mejorar las capacidades tecnológicas tanto de la **Oficina de Coordinación de Ciberseguridad** (OCC), como de las unidades de **Policía Nacional** y **Guardia Civil** especializadas en la lucha contra el cibercrimen.

Asimismo, como parte del Plan Estratégico contra la Cibercriminalidad de 2021, se darán mayores capacidades ejecutivas a la OCC, órgano que enlaza a la citada Secretaría de Estado de Seguridad con los centros de respuesta a incidentes cibernéticos nacionales de referencia. La Oficina verá reforzada su plantilla y se constituirá como el **Centro de Respuesta a Incidentes Cibernéticos** de Interior de apoyo a la **Policía Judicial** (CSIRT-MIR-Policía Judicial). Con ello, dará apoyo técnico a las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado, erigiéndose en la autoridad competente en materia de protección de las redes y sistemas de información para los operadores de servicios esenciales y críticos. La OCC también se va a constituir en Observatorio de la Cibercriminalidad.

Álvaro Lossada, Jefe de la Oficina de Coordinación de Ciberseguridad

"Los retos de la OCC suponen un enorme desafío en materia de coordinación, supervisión y desarrollo de inteligencia"

– ¿Qué aporta ahora la OCC en el ecosistema de la ciberseguridad nacional junto a organismos como el Incibe, el CCN-CERT, el MCCD o el CNPIC?

– La OCC, como parte integrante de la Secretaría de Estado de Seguridad, participa de pleno en el actual ecosistema de ciberseguridad diseñado en la ENCS. Es el órgano de ejercicio de la autoridad de la SES en materia de ciberincidentes que afecten a operadores esenciales y críticos. Funciona también como canal coordinador entre CSIRTs y autoridades de referencia con la Fiscalía General del Estado y las Fuerzas y Cuerpos de Seguridad del Estado para aquellos incidentes con características delictivas. Este triple enfoque sitúa a la OCC en un lugar privilegiado de interlocutor y puente entre diferentes actores del sistema de ciberseguridad nacional y con el ámbito de la persecución de la cibercriminalidad.

– ¿Cuáles son sus grandes retos como nuevo jefe de la OCC?

– Las nuevas capacidades de la OCC suponen un enorme desafío en materia de coordinación, supervisión y desarrollo de inteligencia.

– Por primera vez, la SES contará con una dotación presupuestaria específica. ¿Es suficiente inversión?

– La dotación presupuestaria del plan para 2023 supone un enorme esfuerzo de inversión en materia de ciberseguridad y lucha contra la cibercriminalidad. Representa un 500% de incremento sobre 2022 y es posible que siga creciendo en el futuro.

– También es destacable que la OCC se "va a constituir en el Centro de Respuesta a Incidentes Cibernéticos de Interior"…

Álvaro Lossada

– Efectivamente, el establecimiento del CSIRT-MIR-Policía Judicial reforzará la capacidad de coordinación técnica de la OCC hacia las Fuerzas y Cuerpos de Seguridad del Estado. Al mismo tiempo, facilitará a Policía Nacional y Guardia Civil herramientas de apoyo a la investigación y de generación de inteligencia de cara a una respuesta y persecución más eficiente de los ciberincidentes de carácter delictivo y, muy especialmente, aquellos que afecten a servicios esenciales y críticos. Su puesta en marcha está prevista de manera modular en un plazo de, al menos, cuatro años.

– La OCC también se convertirá en "Observatorio de la Cibercriminalidad"…

– Sí, el Observatorio quiere ser una potente herramienta que permita tener una fotografía lo más global, completa y actualizada posible sobre el estado de la Cibercriminalidad. Para ello, buscaremos la elaboración de inteligencia. Por un lado, con un enfoque preventivo, analizando de tendencias y *modus operandi*, estudiando perfiles de víctimas y diseñando campañas preventivas. Por otro, con un enfoque hacia la respuesta, captando información y elaborando productos de inteligencia que ayuden a una mayor eficacia de las FCSE, la Fiscalía y el Poder Judicial en la lucha contra la Cibercriminalidad.

– La OCC ha sido muy activa, como representante español, en la iniciativa internacional 'International Counter Ransomware Task Force (ICRTF)'…

– La OCC trabajó de manera muy activa en el seno de la Counter Ransomware Initiative (ICRTF), liderando el grupo de trabajo de colaboración público privada. Fruto de ello, la OCC, en colaboración con el Ministerio de Asuntos Exteriores, la CISA y el Departamento de Estado de EE.UU., está promoviendo el desarrollo de una herramienta *online* de identificación e implantación de modelos de buenas prácticas de colaboración público privada, que será impulsada dentro del ámbito de construcción de capacidades de la ICRTF.

wisesecurity
GLOBAL

wsg127.com

WISE CSOC

VIGILANCIA DETECCIÓN ANÁLISIS RECUPERACIÓN AUTOMATIZACIÓN RESPUESTA

MCDR WISE SERVICES

• Alert and Event Management 24/7 • Vulnerability Management & Threat Intel
• SOAR • DFIR • Blue & Purple Team

MCDR WISE SOLUTIONS

HAUNT® KEEPER bastet® NET ALARM

We build CyberTrust. We create CyberSecurity

hello@wsg127.com | +34 910 700 549 | wsg127.com

También ha dedicado una jornada a estudiar los retos de la internacionalización de las empresas españolas del sector

INCIBE escenifica la puesta de largo del programa RETECH dotado con casi 150 millones de euros para impulsar la ciberprotección, junto con 15 autonomías

La secretaria de Estado de Digitalización e Inteligencia Artificial, **Carme Artigas,** presentó a finales de marzo, en León, la puesta en marcha de la iniciativa **Retech** (**Redes Territoriales de Especialización Tecnológica**) **Ciberseguridad**, en un acto organizado por el **Instituto Nacional de Ciberseguridad** (**Incibe**), que gestionará los programas de ciberprotección y que ya detalló SIC en su edición anterior. El acto también contó con los responsables de las 15 comunidades autónomas participantes en los denominados 'tres nodos' de ciberseguridad. El director general del Incibe, **Félix Barrio,** destacó que se trata del "programa más ambicioso de estrategia, de nodos de desarrollo tecnológico en ciberseguridad, de la historia de España, Europa y seguramente a nivel mundial". Además, se debatió sobre los inminentes retos de esta iniciativa a través de una mesa redonda, moderada por la secretaria general del organismo, **Carla Redondo,** en la que participaron representantes de Castilla y León, Cataluña, Navarra, Asturias y País Vasco.

Félix Barrio, Director de INCIBE


Carme Artigas (SEDIA) y los representantes de las 15 Comunidades Autónomas coparticipantes en RETECH durante el acto de formalización.

Retech Ciberseguridad

Como se sabe, Retech Ciberseguridad es una iniciativa estratégica para el desarrollo del ecosistema (capacidades, industria, I+D+i y talento) que aglutina el trabajo en este ámbito de 15 de las 17 comunidades autónomas con un presupuesto inicial de 149 millones de euros y que espera ser un modelo de colaboración entre Incibe y los entes autonómicos para el desarrollo de la ciberseguridad en sectores productivos estratégicos relevantes. Además, esta estructura de Retech formará parte de la Comunidad Nacional española en torno al Centro Europeo de Competencia en Ciberseguridad, donde el Instituto ha sido nombrado **Centro de Coordinación Nacional (NCC-ES).** En concreto, los tres programas de ciberseguridad de Retech serán el de 'Red de Nodos de Ciberseguridad', denominada **Red Argos,** y coordinada por Castilla y León, con la participación de Andalucía, Comunidad de Madrid y País Vasco, el de 'Espacio de datos de Ciberseguridad del Centro de Competencia en ciencias de la salud, transporte inteligente, industria conectada y excelencia operativa', liderado por Cataluña, con el apoyo de la Comunidad Valenciana y Galicia y, por último, el de 'Impulso a la Ciberseguridad desde los Territorios', bautizado como **Ciberreg,** con Navarra al frente y el trabajo de Asturias, Cantabria, Castilla-La Mancha, Extremadura, Murcia, Islas Canarias e Islas Baleares. En global, Retech movilizará en torno a 10 proyectos y 530 millones de euros.

Internacionalización

Por otro lado, Incibe organizó en febrero una jornada bajo la denominación 'España: nación ciber, nación global', en la que participaron más de 50 representantes de la industria de la ciberseguridad española de compañías como **Devo, CounterCraft o VU**, entre otras. Su objetivo fue abordar cuáles son las distintas fases y mejores prácticas del proceso de internacionalización, presentando los programas públicos sobre esta temática y las fortalezas de España en el sector. El organismo, también anunció que, junto con **Fundación Universia,** invertirán 1,3 millones de euros para impulsar la formación en ciberseguridad de hasta 900 personas con discapacidad para incrementar el nivel de competencias digitales, básicas y avanzadas, a través del programa 'Cyberskills', con tres años de duración.

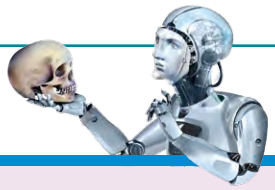
El MINISTERIO DE JUSTICIA prestará sus servicios a una nueva oficina de ciberseguridad para el conjunto de sus organismos competentes

El **Mº de Justicia** atenderá la prestación de servicios de la nueva **Oficina de Gobierno de Ciberseguridad**, creada en el seno del **Comité Técnico Estatal de la Administración Judicial Electrónica** (CTEAJE), para reforzar en todo el Estado la seguridad de la información digital de la Administración de Justicia frente a ciberamenazas y ciberataques. Esta iniciativa sitúa a la Justicia española "a la vanguardia en ciberseguridad y da, con este servicio, una respuesta adecuada a los nuevos retos y riesgos que surgen en internet", ha destacado la ministra de Justicia, **Pilar Llop**. En este sentido, esta oficina se inscribirá en un nuevo Subcomité de Seguridad, puesto en marcha para salvaguardar esa información homogénea en el ámbito de la Administración de Justicia estatal.

A través de ella, "un equipo de profesionales especializados ofrecerá un catálogo de servicios de seguridad atendido por el Mº de Justicia, a través de la subdirección General de Calidad de los Servicios Digitales, Ciberseguridad y Operaciones, con el objetivo de que la información y los servicios de la Administración de Justicia cuenten con similares niveles de seguridad, mejorando la protección, vigilancia y detección de incidentes, así como optimizando la capacidad de reacción y respuesta ante cualquier amenaza", han destacado desde el ministerio que, a la vez, recuerda que entre los servicios ofertados se incluye la elaboración del desarrollo normativo de la política de seguridad de la información, en línea con la legislación vigente en la materia, como el ENS, el Esquema Judicial de Interoperabilidad y Seguridad (EJIS) y la legislación sobre la protección de datos de carácter personal.


a3sec
<SHIELDING DIGITAL ASSETS GLOBALLY>
Más de 10 años innovando
en servicios de ciberseguridad
para proteger a nuestros clientes
¡Conoce más!
www.a3sec.com
España | México | Colombia | Ecuador

CAVILACIONES SEGURAS



¿De la casa o de fuera... y, si es de fuera, de qué sector?

La polimatía, como sabiduría que se extiende por muy diversos campos del conocimiento, ya sea arte, ciencias exactas o sociales, tuvo su mayor expresión durante el Renacimiento, con nombres tan ilustres como Leonardo da Vinci o Galileo Galilei. Tanto es así que aún empleamos la expresión *"es una verdadera persona del Renacimiento"* para referirnos a aquellos generalistas expertos en muy diversos campos.

En el terreno de la ciberseguridad, el grado de especialización dentro de nuestra profesión aumenta día a día: desde los especialistas en desarrollo de aplicaciones seguras hasta los expertos en pruebas de intrusión, pasando por los gurús de la gestión de identidades.

Veo dos principales razones para esta "sectorización de facto" de los roles de gestión de ciberseguridad. La primera es la amplia regulación existente en algunos sectores, como el financiero, que demandan expertos con experiencia en el cumplimiento de estas regulaciones. La segunda razón es el conocimiento del negocio.

La posibilidad de encontrar polímatas dentro de nuestra profesión, capaces de abarcar un amplio conocimiento de muy diversos campos de trabajo dentro de la ciberseguridad, en ocasiones se convierte en un gran desafío. La búsqueda de un CISO global es un ejemplo paradigmático: la gestión de una función de ciberseguridad es una posición ideal para un polímata de la seguridad.

Analizando los nombramientos de nuevos CISOs publicados por esta revista en la última década, se repite con frecuencia el hecho de que el nuevo fichaje procede de un puesto similar dentro del mismo sector. En alguna ocasión es el resultado de una promoción interna, y, muy raramente, vemos incorporaciones procedentes de otra industria.

Veo dos principales razones para esta "sectorización de facto" de los roles de gestión de ciberseguridad. La primera es la amplia regulación existente en algunos sectores, como el sector financiero, próximamente impactado, por ejemplo, por DORA, la legislación europea de resiliencia operacional, o el mundo de las infraestructuras críticas nacionales, ligado a regulaciones como NIS2. Los expertos en seguridad con experiencia en el cumplimiento de estas regulaciones están mejor posicionados para seguir en dichos sectores.

La segunda razón es el conocimiento del negocio. Este argumento priorizaría naturalmente las promociones internas dentro de una misma empresa. Nadie mejor que un interno que "conozca la casa" para poder desarrollar una estrategia compatible con el consejo de dirección actual. Sin embargo, observamos que es más común el fichaje de un externo dentro del mismo sector que el de un interno. Estaría encantado de ser refutado con cifras reales y evidencias más científicas que el ejercicio de repasar los nombramientos reseñados por esta publicación. Quizás un estudio más detallado proporcione otras conclusiones.

Desde esta columna, mis irreverentes cavilaciones proponen un cambio de paradigma: si al buscar una nueva gestora, nuestro objetivo es encontrarla dentro del mismo sector, probemos a promocionar dentro de nuestras filas internas. Si, por el contrario, nos atrae más contratar a alguien externo, atrevámonos y contratemos profesionales de la ciberseguridad que trabajen en otros sectores muy distintos. A largo plazo, esta decisión puede ser un gran motor de innovación.

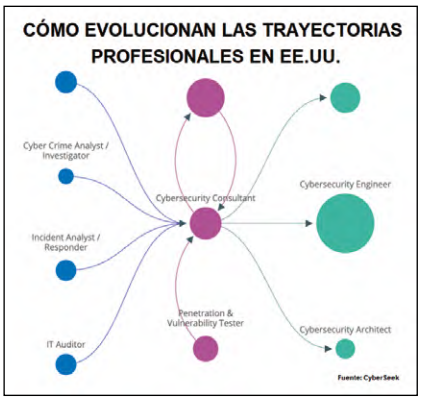
Dr. Alberto Partida

linkedin.com/in/albertopartida

La desaceleración económica mundial no frena la demanda de profesionales de ciberseguridad en EE.UU., con más de 530.000 puestos sin cubrir

A pesar de los ingentes despidos de la industria tecnológica de alto perfil –en los últimos meses superaron los 60.000 profesionales– la demanda laboral de expertos en ciberseguridad continúa siendo alta según un estudio de **CyberSeek**, en colaboración con la Asociación por **la Iniciativa Nacional para la Educación en Seguridad Cibernética** (NICE) de **NIST**, **CompTIA** y **Lightcast.** Según sus datos el número de trabajadores en ciberprotección en EE.UU. se ha mantenido estable en 2022 rondando los 1,1 millones. "A pesar de las preocupaciones sobre la desaceleración de la economía, la demanda en este sector sigue siendo históricamente alta. Las empresas saben que el delito cibernético no se detendrá por una recesión, por lo que los empleadores no pueden darse el lujo de pausar su contratación", destacó el vicepresidente de investigación aplicada de talento de Lightcast, **Will Markow.**

Un indicador clave de la situación del mercado, dice el documento, es la proporción de trabajadores de seguridad cibernética empleados actualmente en relación con las nuevas vacantes, lo que da una idea de cuán grande es la escasez de trabajadores. La relación oferta/demanda es ahora de 68 trabajadores por cada 100 vacantes, superando la relación del período anterior de 65 trabajadores por cada 100 vacantes. A la vista de estas cifras, hacen falta en torno a 530.000 trabajadores de ciberprotección en EE.UU. para dar abasto a la demanda del mercado –según un reciente estudio en España ya superan las 75.000–.



Además, el incremento de contratación en 2022 respecto a su año precedente es positivo. En concreto, en el país norteamericano, en el sector público, se creció en torno al 25 %, mientras que en el privado este incremento fue del 21%. Analizando los datos, a tres años, el crecimiento de contrataciones fue de un 36% en el privado y de un 58% en el público. Como dato curioso, el área metropolitana de Washington DC representó en este periodo el 19% de toda la demanda en el sector público en el país, con un déficit estimado de 52.634 trabajadores.

CROWDSTRIKE

Orgullosos de ser líderes
en ciberseguridad.

**Siendo los primeros,
nuestros clientes son los que ganan.**

CrowdStrike es reconocido líder constantemente por analistas, evaluadores y clientes.
Más información en: **crowdstrike.com/leader.**

Proponen un marco con una metodología propia, con 31 habilidades claves para atraer y desarrollar una carrera en este ámbito

La COMISIÓN cuenta con CAIXABANK y LA SALLE-URL para definir el futuro de la formación en ciberseguridad con el proyecto REWIRE

Un total de 23 entidades y universidades de la UE –entre las que se incluyen, por parte de España, **CaixaBank, La Salle Campus Barcelona** y la **Agència de Ciberseguretat de Catalunya–,** han puesto en marcha un proyecto para definir un marco de competencias internacional para futuros profesionales de la ciberseguridad. Bautizado como **Rewire**, con financiación del programa **Erasmus+.** Su objetivo es definir itinerarios formativos, así como habilidades y competencias que deben tener los estudiantes que elijan este sector como trayectoria profesional. "En definitiva, se trata de identificar los *stakeholders* clave desde todos los puntos de vista y ámbitos posibles, así como proporcionar una herramienta interactiva, disponible públicamente, que contenga la información y orientación profesional necesaria para los profesionales y estudiantes que evalúan una carrera en esta profesión", destacan desde el proyecto que busca diseñar un marco de competencias que permita tanto a los estudiantes como a los profesionales existentes tener claro cómo mejorar sus habilidades, volver a capacitarse o cambiar de dirección profesional.

Primer paso

Como primer paso, el consorcio presentó en febrero un documento en el **Barcelona Cybersecurity Congress** (BCC) conteniendo un marco de habilidades concretas, describiéndose los diversos perfiles profesionales e identificando conocimientos relevantes que han de tener los especialistas en ciberseguridad. Además, analiza el mercado de trabajo y la demanda laboral en esta materia.

Está estructurado en varios apartados entre los que está desde una instrucción, con una descripción del Marco Europeo de Habilidades en Ciberseguridad (ECSF), de la **Agencia Europea de Ciberseguridad** (**Enisa**) del que SIC se hizo eco proifusamente en su nº 152, o el desarrollado en EE.UU. por **NIST,** el NICE, hasta una descripción precisa de cómo atraer más gente al sector "desde una etapa temprana", a través de juegos, talleres, desafíos y *hackatones*. Además, Rewire propone una estrategia de ciberseguridad para desarrollar este talento y ofrecerle una trayectoria, según sus intereses, con una metodología escalable. No faltan en el documento recomendaciones, así como propuestas de cursos, esquemas de certificación y herramientas, incluso, que podría acometer en otra fase esta iniciativa.

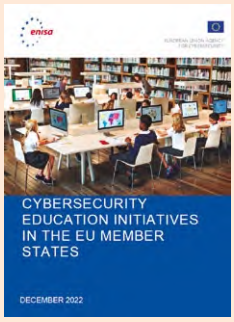
Además, el proyecto determina "varios mapas de identificación de habilidades", poniendo en valor cuatro proyectos piloto europeos en este ámbito, como **Concordia, Cybersec4Europe, Echo** y **Sparta.** También, el informe insiste en la necesidad de contar con una metodología precisa, por ejemplo, a partir del marco de Enisa con 104 habilidades y 85 áreas clave de conocimiento, estableciendo finalmente Rewire un conjunto crítico y prioritario de 31 habilidades.

El documento, además, destaca la necesidad de desarrollar herramientas con dos objetivos: por un lado, para el desarrollo de habilidades a través de los denominados Cyberrange -plataformas de entrenamiento-. Y, por otro, para plantear trayectorias profesionales claras que permitan "una carrera interesante y seguir siendo útil y relevante en el mercado laboral". Unos objetivos que se trasladarán a la 'Cyber Hability Platform' que se creará en el marco de este proyecto.

El informe también subraya la necesidad de contar a medio y largo plazo con una organización que mantenga y enriquezca lo generado en este proyecto, proponiendo como candidatos desde a los cuatro proyectos piloto mencionados, hasta organizaciones privadas como **ECSO**, públicas como Enisa o el **JRC (Centro Común de Investigación de la Comisión)** o el **Centro Europeo de Competencia en Ciberseguridad (ECCC)**. De cualquier forma, termina resaltando que el proyecto aún tiene mucho recorrido, recomendando conocer las actualizaciones en su web: https://rewireproject.eu.

ENISA apuesta por una plataforma común europea, colaborativa, para formación en primaria y secundaria

La **Agencia de Ciberseguridad de la UE** (ENISA) publicó a finales de 2022, una nueva edición de su informe 'Cybersecurity education initiatives in the EU member', en el que se ofrece una excelente visión de las diferentes iniciativas de cada país en la formación, en educación primaria y secundaria, en este ámbito –en el caso español, se cita el trabajo del **Incibe** a través de su iniciativa **Internet Segura para Niños** (IS4K)–.



En este ámbito, el 'Plan de Acción de Educación Digital' de la UE apuesta por fomentar el desarrollo de un ecosistema de educación digital de alto rendimiento, así como mejorar las habilidades y competencias digitales para la transformación digital. En este sentido, Enisa destaca la "importancia de abordar y remodelar los programas de educación en ciberseguridad existentes y los cambios continuos en el panorama para alinear los conocimientos y habilidades requeridos". Así, también ofrece en el documento una hoja de ruta integral hacia la implementación de una campaña de colaboración a nivel de la UE para fomentar las buenas prácticas y el intercambio de conocimientos.

Enfoque colaborativo

Entre sus recomendaciones están desde adoptar un enfoque colaborativo para involucrar a todas las partes interesadas, hasta apostar por un enfoque pedagógico para garantizar la participación de los estudiantes, confiar en el principio de Pareto para maximizar los esfuerzos, construir anualmente planes para asegurar la mejora continua y educar a los padres en lugar de crear una reacción en cadena. Enisa también lamenta haber detectado una "cultura rígida de los ministerios responsables de las iniciativas de ciberseguridad educativa, la falta de tiempo y recursos (baja disponibilidad de docentes, rotación de personal) y la falta de reconocimiento de las partes interesadas".

TE PROTEGEMOS CON UN PAR

#NEXTLEVELSECURITY

Threat Hunting, Vulnerability Management 24x7, Digital Surveillance

www.tarlogic.com

TARLOGIC
CYBERSECURITY EXPERTS

Proponen a la ONU crear una unidad de 'ciber cascos azules' para ayudar a combatir ataques informáticos

En marzo se ha propuesto a la **ONU**, en Buenos Aires, la posibilidad de crear, a partir de los centros de ciberseguridad de cada país, un grupo de profesionales que, bajo su autoridad, actúe a modo de 'ciber cascos azules' para ayudar a los países que cuentan con un menor grado de protección cibernética.

Se trata de una de las ideas que se han debatido en las jornadas organizadas por la **Unión Interparlamentaria** (UIP) en las que ha tenido especial protagonismo esta propuesta por parte del senador español, **José Cepeda,** elegido por la UIP, que agrupa a 178 cámaras legislativas del mundo, para hacer el informe 'Ciberataques y delitos cibernéticos, nuevas amenazas a la seguridad global'.

En este sentido, el político español ha recordado a EFE que "Europa, por ejemplo, no tiene una estructura continental de ciberdefensa, es una cosa que está por desarrollar. Lo que estamos intentando es avanzar un poco por delante de lo que se nos viene encima", destacó Cepeda, miembro del Comité Permanente de Paz y Seguridad Internacional de la UIP, que ya ha estado en varios países para reunirse con legisladores y otras autoridades, incluidos representantes de organismos del continente americano, académicos y expertos, y potenciar en este lado del mundo el debate sobre los desafíos que deja la proliferación de los ciberdelitos.

Desde la cibertrinchera

El renacer de los 'Forensicadores'

Otra noche más frente a mi computadora, ataviado con una confortable bata de Homer Simpson y grandes cascos de "gaming", alumbrado tras estrambóticas luces LED ambientales. Cueva convertida en cuartel general de la lucha contra el "crimen", solitaria pero encandilada por chats y videoconferencias. Todo se desvanece cuando el vástago despierta reclamando atención: "No puedo dormir papá, cuéntame otra vez sobre los forensicadores".

Como "abuelete cebolleta", me acomodo recuperando esos lejanos recuerdos archivados en recónditos "*backups*" mentales. Esa Internet de hace años, sin nubes y a velocidad de pocos "Megas", llena de estaciones de grandes torres con un puñado de aplicaciones conviviendo en discos duros de pocos "Gigas". Extraerlos era como adentrarse en una sombría cueva llena de polvo. Ataviado con clonadora en mano esperando el ansiado "hash" que encumbraba la cadena de custodia. Pilotando herramientas abiertas, o ese software forense de seis letras que todo hijo de vecino conocía, olfateando el rastro como perrito sabueso que condujera a jugosos hallazgos. Un bonito informe y sanseacabó, a otra cosa mariposa mientras llega el siguiente.

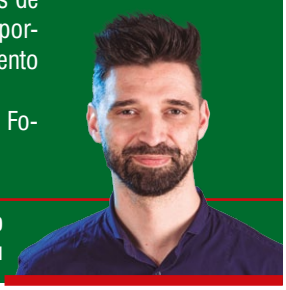
Es momento de dar un paso adelante, como industria y como profesión. La velocidad, agilidad y escalabilidad se han vuelto claves. Rompamos con los silos de información, convirtiendo los productos forenses en ricos conjuntos de datos

Arropas a tu criaturilla dormida por la "emocionante" batallita. Momento para suspirar y exclamar …¡Cuánto hemos cambiado! El *forensicador* es ahora hombre de batalla, sin tiempo para respirar. Malabarismos con decenas de casos en paralelo y con muchos otros en la despensa esperando un poco de atención. Portátiles, tabletas, teléfonos inteligentes, cacharrería de la Internet de las Chorraditas … Sistemas o bien vulnerables o debilitados por los humanos, repletos de aplicaciones de su padre y de su madre. Nuestra amiga la "nube" aterriza millares o millones de ficheros acumulados, dispersos en múltiples lugares e históricos de navegación esquizofrénicos. Utilizando herramientas forenses para dar y repartir, "sacando punta" a la evidencia y recorriendo cada recóndito artefacto. Sin embargo, no hay entuerto resoluble sin mirar más allá: sistemas clave, *logs* a mamporro, tráfico de red para aburrir, y la valiosa información de inteligencia.

Ahora 'forensicadores' somos muchos: a la caza de cualquier indicio de compromiso, sobrevolando a toda velocidad para ayudar a contener la sangría durante la respuesta, o bien destripando en profundidad buscando respuestas que permitan entender y corregir. Incluso algunos magos de la narrativa y los dibujitos con bonitas líneas de tiempo y diagramas de compromiso.

Es momento de dar un paso adelante, como industria y como profesión. La velocidad, agilidad y escalabilidad se han vuelto claves. Rompamos con los silos de información, convirtiendo los productos forenses en ricos conjuntos de datos. Soñemos con productos interoperables siguiendo una ontología y semántica común, aplicando un razonamiento basado en la experiencia. Es necesario conectarlos y automatizarlos (*SOARizarlos*), ansiando olvidar esos "copia-pega" y los clics de ratón humanos sin razón. Dejemos que la ForensIA acerque a esos "copilotos" que acompañen al investigador en su viaje y, evitando sesgos en la medida de lo posible, le arrojen algo de luz en la oscuridad. Colaboremos de verdad, sin tickets y "ping-pong" de informes, cuando toca y aportando valor. Sin olvidar los entregables, construyamos conocimiento que sirva para madurar y crecer.

Es inevitable. Se acerca un nuevo amanecer, el renacer de los Forensicadores.



Carlos Fragoso
carlos@fragoso.eu

Más de 15.000 clientes confían en Sophos Managed Detection and Response

Sophos Managed Detection and Response

Actúe contra las amenazas con un servicio gestionado de expertos en respuesta ante incidentes, compatible con las herramientas de ciberseguridad que ya tiene.
Más información en es.sophos.com/mdr

SOPHOS

230320 ES [PC]

La quiebra del Silicon Valley Bank también impacta en las inversiones de los fondos de capital en compañías del sector

¿Cuál es el techo de la ciberseguridad como inversión? A las operaciones millonarias acontecidas en la primera mitad de 2022 les ha seguido un fuerte frenazo por parte de los fondos de capital riesgo en la última parte del año, según datos de Momentum Cyber. Y eso antes de conocerse la bancarrota del Silicon Valley Bank, 'corazón económico' de muchos de los inversores en este ámbito y que ha supuesto un duro golpe, a pesar del rescate de la Reserva Federal de EE.UU. (FED). Eso sí, la firma analista destaca que el año pasado fue el segundo con las cifras de inversión más altas por cuanto "la necesidad de productos y servicios de ciberseguridad no ha disminuido".

La quiebra del **Silicon Valley Bank** ha supuesto un tsunami entre los fondos de inversión y compañías tecnológicas, entre ellas las españolas **Cabify** y **Carto,** que los analistas, al cierre de esta edición de SIC, aún no han sido capaces de cuantificar pero que sí les hace vaticinar que habrá un antes y un después en cuanto a inversiones en *startups,* también, de ciberseguridad. Una quiebra que ha afectado, aunque de forma limitada, a compañías de origen español, como **Devo** o **CounterCraft.**

Uptime se hace con Leet, V-Valley, de Esprinet, con Lidera, Allurity, del que forma parte Aiuken, con Securix AG y Securix Deutschland, Francisco Partners compra Sumo Logic, Radiant Logic a Brainwave, Accenture adquiere Morphus, Zscaler a Canonicy, Trend Micro a Anlyz, Atos negocia con Airbus la venta de Evidian, Cisco se hace con Valtix, además de notables rondas de financiación, como la de Opscura, heredera de la vasca Enigmedia, entre otras.

De cualquier forma, 2022 fue un buen año para el mercado de ciberseguridad en el que las operaciones alcanzaron casi los 110.000 millones de euros, frente a los 74.250 millones de 2021, con más de 600 operaciones. Por nicho, el área que más fondos atrajo en 2022 fue el de gestión de contraseñas e identidad, con 3.100 millones, seguida de la de cumplimiento normativo e inteligencia de amenazas con más de 2.000 millones.

Esta fiebre inversora también se ha materializado de forma notable en España, en el primer trimestre. En concreto, destacó la compra de **Leet Security** por parte de **Uptime Institute**, una autoridad global en infraestructuras digitales. Esta operación permitirá a la compañía española "acelerar el desarrollo y continuar liderando el camino en el campo de las calificaciones de ciberseguridad, al tiempo que proporciona un conjunto adicional de herramientas, servicios y soluciones, con la profundidad y amplitud necesarias para cumplir con los requisitos cambiantes de nuestros clientes". Además, **V-Valley Advanced Solutions**, del **Grupo Esprinet,** se hizo con el distribuidor **Lidera** en una operación valorada en algo más de 5,5 millones de euros.

Mercado internacional

Fuera de nuestras fronteras, **Allurity,** el gigante europeo de la ciberseguridad que ha creado el fondo **Trill Impact** y en el que está integrada Aiuken, se hizo con las compañías germanas **Securix AG** y **Securix Deutschland GmbH** para aprovechar sinergias "en las áreas de IAM, observabilidad y seguridad de TI". Asimismo, fue llamativa la compra de **Sumo Logic,** proveedor de soluciones SIEM, gestión de registros y monitorización en la nube, por más de 1.500 millones de euros, por parte de la firma de capital privado **Francisco Partners.** La compañía ofrece análisis SaaS nativos en la nube, lo que ayuda a las organizaciones a hacer que sus aplicaciones sean más seguras y confiables.

Además, **Radiant Logic**, la empresa Identity Data Fabric, llegó a un acuerdo definitivo para adquirir **Brainwave GRC,** centrada en Identity Governance and Analytics (IGA), con sede en Francia. Su idea es ofrecer un mayor portafolio de casos de uso de identidad.

Por su parte, **Accenture** adquirió la totalidad de las operaciones de la tecnológica de capital brasileño **Morphus,** como parte de su apuesta por ampliar la presencia en el ecosistema de la ciberprotección en Iberoamérica. La adquisición trae consigo, además, la creación de Accenture Morphus Labs, un centro de investigación de ciberseguridad y análisis de vulnerabilidades y amenazas.

Zscaler anunció su intención de hacerse con **Canonic Security,** con una innovadora plataforma de seguridad de aplicaciones SaaS, y **Trend Micro** adquirió a **Anlyz,** proveedor de tecnología de centro de operaciones de seguridad (SOC).

Por su parte, **Atos**, viéndose venir, informó finalmente de forma oficial que ha entrado en fase de conversaciones con **Airbus** para formar una asociación estratégica y tecnológica a largo plazo y vender una participación minoritaria de **Evidian.** También, el gigante de telecomunicaciones, **AT&T,** está abriéndose a la posibilidad de vender su unidad de ciberseguridad como parte de sus esfuerzos para optimizar sus operaciones y reducir la deuda. En este contexto cabe recordar que el grueso del negocio de ciberseguridad de la compañía incluye **AlienVault,** de origen español, que fue adquirida en 2018 por más de 560 millones de euros para atraer nuevos clientes y conservar a los existentes. Asimismo, **Cisco** adquirirá **Valtix** en su primera operación de 2023. El gigante tecnológico ha apostado por esta *startup* de seguridad de red en la nube como parte de su estrategia unificada de Cisco Security Cloud.

Financiación con ADN español

En España, destacó la iniciativa de **Opscura Inc,** empresa de ciberseguridad de sistemas de control industrial (ICS), que fue fundada bajo el nombre de **Enigmedia,** y que ha cerrado una ronda Serie A de 9,4 millones de dólares, liderada por **Anzu Partners** y con inversiones de **Dreamit** y **Mundi Ventures.** Se convierte así en la nueva marca de la compañía y fija su intención de ser una empresa global, apoyada por un equipo internacional y por la actualización y desarrollo de nuevos productos. También, fue importante la ronda de la compañía de origen germano, **Build38,** con amplia representación de ejecutivos españoles, que la ha permitido captar 13 millones de euros, apoyada por **Tikehau Capital,** a través de su 'Fondo Europeo de Crecimiento en Ciberseguridad'. Una operación en la que también participaron como inversores **Caixa Capital Risc,** que ya estaba presente en el capital, y **eCapital Entrepreneurial Partners.** Además, se incorpora a la compañía, como consejero **Oliver Gajek** y el español **Javier Polo**, exconsejero delegado de la empresa de videojuegos **PlayGiga**, comprada por Facebook en 2019.

La compañía de origen israelí, fundada en 2020, **Wiz** logró una ronda de financiación de 275 millones de euros, alcanzando una valoración de más de 9.000 millones. **Sentra** obtuvo casi 28 millones de euros, y **Skybox Security,** 46 millones.

BABEL

Business focused CYBERSECURITY

eSOC Centro de Operaciones de Seguridad

eSOC INDUSTRIAL

Red Nacional de SOC

ens

FIRST

CSIRT.es

ISO 20000

ISO 27001-2

• EFEMÉRIDES •

CCI: Una década del Centro de Ciberseguridad Industrial

Hace una década pusimos en marcha el **Centro de Ciberseguridad Industrial (CCI)** con el objetivo de agrupar a empresas del sector industrial para impulsar y contribuir a la mejora de su ciberseguridad, tanto en España como en Latinoamérica, y proporcionar un punto de encuentro de organismos, públicos y privados, y profesionales relacionados con las prácticas y tecnologías de la ciberseguridad industrial.

CCI, durante estos años, se ha convertido en un claro ejemplo de comunidad profesional que, con el esfuerzo, el conocimiento y las experiencias de muchas personas de todo el mundo y el apoyo de los patrocinadores ha sido capaz de consolidarse como un ecosistema global para avanzar juntos en la ciberseguridad industrial. Esta comunidad ha crecido, pasando de sus primeros 500 miembros en 2013, hasta los más de 5.000 profesionales en la actualidad.

El ecosistema de CCI se ha extendido a más de 40 países, gracias a los coordinadores [1] que nos representan en múltiples países de Oriente Medio, América y Europa. Como también nos representan en el ecosistema académico [2] los mentores que atraen a estudiantes de universidades y centros de formación.

Un equipo multidisciplinar de expertos [3] contribuye a compartir conocimiento y experiencias en una de las mayores bibliotecas documentales sobre ciberseguridad industrial del mundo. Algunas de estas publicaciones son la base de los talleres, cursos y Máster de la Escuela [4] profesional de ciberseguridad industrial que ha formado ya a más de un millar de alumnos, que cuentan con credenciales [5] del programa de reconocimiento de compromiso con la ciberseguridad industrial.

También los congresos, los eventos de la voz de la industria y las reuniones de equipos de conocimiento se han convertido en un espacio ideal de *networking* para reflexionar, debatir y en definitiva proporcionar experiencias valiosas que permiten a muchas organizaciones mejorar la gestión del riesgo de las tecnologías de automatización y digitalización industrial.

Además de todos los recursos ya mencionados, en CCI trabajamos desde hace algunos años, junto a los profesionales de organizaciones industriales, ingenierías, fabricantes de tecnología industrial y proveedores de ciberseguridad en diversas plataformas [6] que permiten compartir con todo el ecosistema proyectos industriales que incorporan requisitos de ciberseguridad o escenarios de riesgos de alto impacto, así como soluciones y servicios de proveedores que ayudan a cumplir con los principales estándares, *frameworks* y buenas prácticas en ciberseguridad industrial.

Hoy, tras estos diez años de actividad, en CCI seguimos desarrollando nuevas iniciativas que contribuyen al crecimiento de las relaciones dentro del ecosistema y a compartir entre todos los miembros valiosas experiencias.

José Valiente
Director
CCI-CENTRO DE CIBERSEGURIDAD INDUSTRIAL

REFERENCIAS

1 Coordinadores https://www.cci-es.org/ecosistema/coordinadores/
2 Programa Academia https://www.cci-es.org/ecosistema/programa-academia/
3 Expertos https://www.cci-es.org/ecosistema/expertos/
4 Escuela https://www.cci-es.org/recursos/escuela/
5 Credenciales https://www.cci-es.org/ecosistema/credenciales/
6 Plataformas https://www.cci-es.org/recursos#plataformas

El sector de drones crea una certificación de ciberseguridad, Green UAS, para usar modelos comerciales en labores de defensa y seguridad

La **Asociación Internacional de Sistemas de Vehículos No Tripulados (AUVSI)** ha puesto en marcha el programa 'Trusted Cyber Program' para implementar sistemas y capacidades de ciberprotección por diseño en modelos comerciales que, sin embargo, puedan emplearse por fuerzas y cuerpos de seguridad de EE.UU. y de otras partes del mundo.

Entre los primeros resultados de esta iniciativa destaca el denominado 'Green UAS', basado en una propuesta anterior (Blue UAS) y que permite garantizar la seguridad cibernética de los vehículos aéreos no tripulados (UAV), diseñados inicialmente para el entorno civil. La certificación, basada en otros estándares cibernéticos, será gestionada por AUVSI, y ha contado también con los expertos de la compañía **Fortress Information Security** y ha sido apoyada por la **Unidad de Innovación de Defensa** (DIU) de Estados Unidos. Por ello, entre otros aspectos, los drones certificados por 'Green UAS' cumplirán con los requisitos de la cadena de suministro de la Ley de Autorización de Defensa Nacional de EE.UU.

Además, sus impulsores también han destacado que se trata de una certificación 'dinámica', ya que se espera que evolucione "rápidamente" acorde a la progresión de las ciberamenazas, tanto en lo que atañe al software, como al hardware y a los sistemas de comunicación utilizados en los drones.

Para impulsar esta iniciativa, varias empresas que trabajan con el Departamento de Defensa han manifestado que están dispuestas a adquirir y ofrecer, para labores militares o policiales, los aparatos que hayan superado la certificación y, por lo tanto, cuenten con la máxima ciberseguridad certificada.

De esta forma este programa busca ser un "primer paso para certificar la seguridad cibernética de todo tipo de sistemas no tripulados", comentó el vicepresidente de estrategia y política de Fortress, **Tobias Whitney,** recordando que esta iniciativa también coloca a la ciberseguridad como un "criterio crítico" en el proceso de adquisición de UAVs.

xMDR

powered by cipher
a Prosegur company

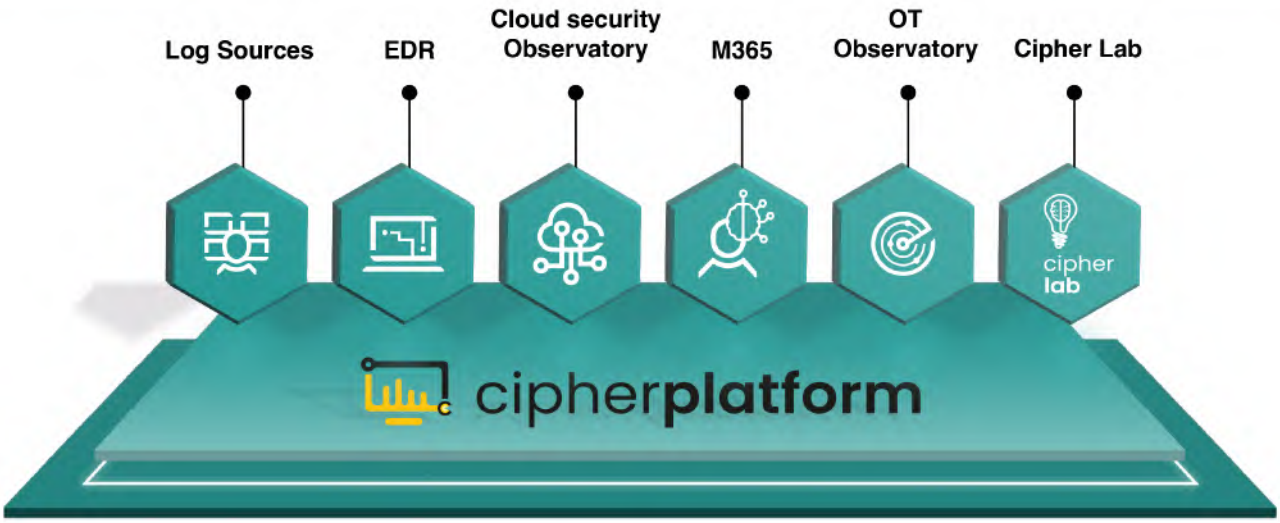
Modelado digital del adversario y aplicación de procesos cognitivos

xMDR es la plataforma de servicios de ciberseguridad desarrollada por Cipher para dar respuesta a los problemas de visibilidad, fragmentación de la tecnología y escasez de profesionales que impiden la mejora continua de la postura de ciberseguridad de las empresas.

Con **xMDR** consigues:

- Bajar el ratio de falsos positivos por debajo del 1%
- Alertas de alto valor con capacidad de anticiparse a los incidentes
- Retorno de la inversión con despliegues ágiles en horas

MODELADO DEL ADVERSARIO + COGNITIVE → **CIPHER PLATFORM** → **SISTEMA DE DETECCIÓN SIN PRECEDENTES**



Habla con nosotros: **contacto@cipher.com**

www.cipherxmdr.io in cipher ciphersec ciphersec

También ofrece varias recomendaciones de privacidad que los organismos deben cumplir en el tratamiento de datos y uso del *cloud*

El SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS subraya la necesidad de que los organismos públicos cumplan con el RGPD en la nube y tengan capacidad de auditoría sobre los proveedores

El **Comité Europeo de Protección de Datos (EDPB)** ha realizado un exhaustivo y ambicioso informe dentro de su Marco de Ejecución Coordinada (CEF), para contar con una visión integral e identificar y fomentar las mejores prácticas en el trabajo de las agencias europeas de protección de datos sobre el uso de servicios en la nube por parte del sector público. Se trata, en definitiva, de detectar posibles deficiencias y realizar recomendaciones en la contratación y el uso de servicios *cloud* por parte de los organismos públicos. En este sentido, el EDPB ha subrayado la necesidad de que éstos actúen en pleno cumplimiento del RGPD.

El estudio ofrece una visión europea del sector público en esta materia, aglutina los resultados de las 22 autoridades de protección de datos que han participado en la iniciativa y el EDPB. En total, se han estudiado un centenar de organismos públicos en el conjunto de los estados miembro, 12 de ellos analizados por la **Agencia Española de Protección de Datos** (AEPD), abarcando una amplia gama de sectores como salud, finanzas, impuestos, educación y proveedores de servicios de TI. La finalidad del informe global es contribuir a elevar el nivel de cumplimiento y la protección de los datos personales de los ciudadanos, no sólo a nivel nacional sino, también, en el conjunto de la UE.

Las autoridades de protección de datos, aun siendo conscientes de las dificultades que pueden tener los organismos públicos para contratar proveedores de servicios *cloud* con garantías, ponen de manifiesto en el informe la importancia de cumplir con los requerimientos del RGPD, teniendo en cuenta la naturaleza y la cantidad de datos personales que manejan.

Entre otras recomendaciones, cuando utilicen productos o servicios basados en la nube, el documento destaca implicar más al delegado de protección de datos (DPD), realizar siempre una Evaluación de Impacto en la Protección de Datos, garantizar que los roles del responsable del tratamiento y encargado estén clara e inequívocamente determinados, así como que el proveedor de *cloud computing* actúe como encargado siguiendo las instrucciones que le ha facilitado el organismo público. Además, destaca la necesidad de que el organismo público siempre pueda oponerse a que otros encargados traten los datos, que pueda vigilar que los datos personales sólo se traten para los fines determinados, así como que sea capaz de revisar si los tratamientos se realizan de acuerdo con la evaluación de impacto. No deja de lado la importancia de tener la capacidad de comprobar que el organismo público tiene la posibilidad de realizar auditorías al proveedor de servicios *cloud*.

Delegados de protección de datos

Por otro lado, la AEPD está participando en una acción europea coordinada para analizar la designación y situación de los DPD en 30.000 entidades del sector público y privado en España. Se trata de una nueva iniciativa puesta en marcha en colaboración con el EDPB y que tiene como objetivo evaluar la situación de los DPD en sus organizaciones, en los 27 países de la UE.

Los resultados de esta acción se analizarán de manera coordinada y las autoridades pertinentes podrán decidir sobre posibles acciones adicionales de supervisión y aplicación en sus respectivos países.

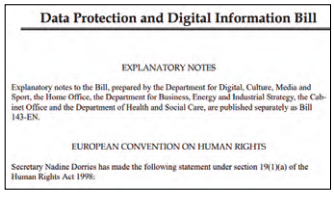
LEY DE DATOS: los eurodiputados respaldan nuevas reglas para el acceso justo y el uso de datos industriales recopilados

Como es sabido, la denominada como 'Ley de datos' (*Data Act*) tiene como objetivo impulsar la innovación mediante la eliminación de las barreras que obstruyen el acceso de los consumidores y las empresas a los datos. Así, tras muchos meses de trabajo, en marzo se aprobó el proyecto de ley que se espera que "contribuya al desarrollo de nuevos servicios, en particular en inteligencia artificial, donde se necesitan grandes cantidades de datos para el entrenamiento de algoritmos y que puede generar mejores precios para los servicios posventa y las reparaciones de los dispositivos conectados".

Así, entre otros aspectos de interés, esta normativa establece reglas comunes que rigen el intercambio de datos generados por el uso de productos conectados o servicios relacionados (por ejemplo, Internet de las Cosas, máquinas industriales, etc.) para garantizar la equidad en los contratos de intercambio de datos. Los eurodiputados también facilitan con su voto que se pueda permitir que los usuarios accedan a los datos que generan, ya que se calcula que el 80% de los datos industriales recopilados nunca se utilizan, según la **Comisión Europea**. El texto también define cómo los organismos del sector público pueden acceder y utilizar los datos en poder del sector privado que son necesarios en circunstancias excepcionales o emergencias, como inundaciones e incendios forestales.

REINO UNIDO busca poner en marcha una nueva Ley de Protección de Datos e Información Digital con un ahorro de 5.200 millones de euros

El país quiere contar con una Ley de Protección de Datos e Información Digital (DPDI) y el parlamento ya está tramitando el proyecto de ley que, según ha anunciado el gobierno, podría ahorrar a las empresas del país hasta casi 5.200 millones de euros, facilitando su ejecución, además de reforzar la protección de datos y la privacidad. Se trata de una iniciativa con la que el ejecutivo quiere mostrar que salir de la UE también puede ser beneficioso en este ámbito, buscando reducir el papeleo para las empresas y brindar más flexibilidad sobre cómo pueden cumplir con la versión localizada del RGPD.


Data Protection and Digital Information Bill

EXPLANATORY NOTES

Explanatory notes to the Bill, prepared by the Department for Digital, Culture, Media and Sport, the Home Office, the Department for Business, Energy and Industrial Strategy, the Cabinet Office and the Department of Health and Social Care, are published separately as Bill 143-EN.

EUROPEAN CONVENTION ON HUMAN RIGHTS

Secretary Nadine Dorries has made the following statement under section 19(1)(a) of the Human Rights Act 1998.

Así, entre otras novedades, plantea eliminar el requisito de que la mayoría de las empresas mantengan inventarios de datos personales, aunque muchos expertos han criticado que ello podría "generar dificultades para comprender cómo y dónde guardan los datos, lo que no beneficia a nadie". Además, consideran que las compañías con presencia en la UE no podrán aprovechar las nuevas eficiencias o se verían obligadas a cambiar sus marcos de cumplimiento existentes. Como la **Unión Europea** es el mayor socio comercial del país, con 42% de las exportaciones y un 45% de las importaciones, esta nueva normativa y su encuadre respecto al RGPD europeo afectará a gran parte de las empresas del país, con presencia fuera de sus fronteras.

ARMIS

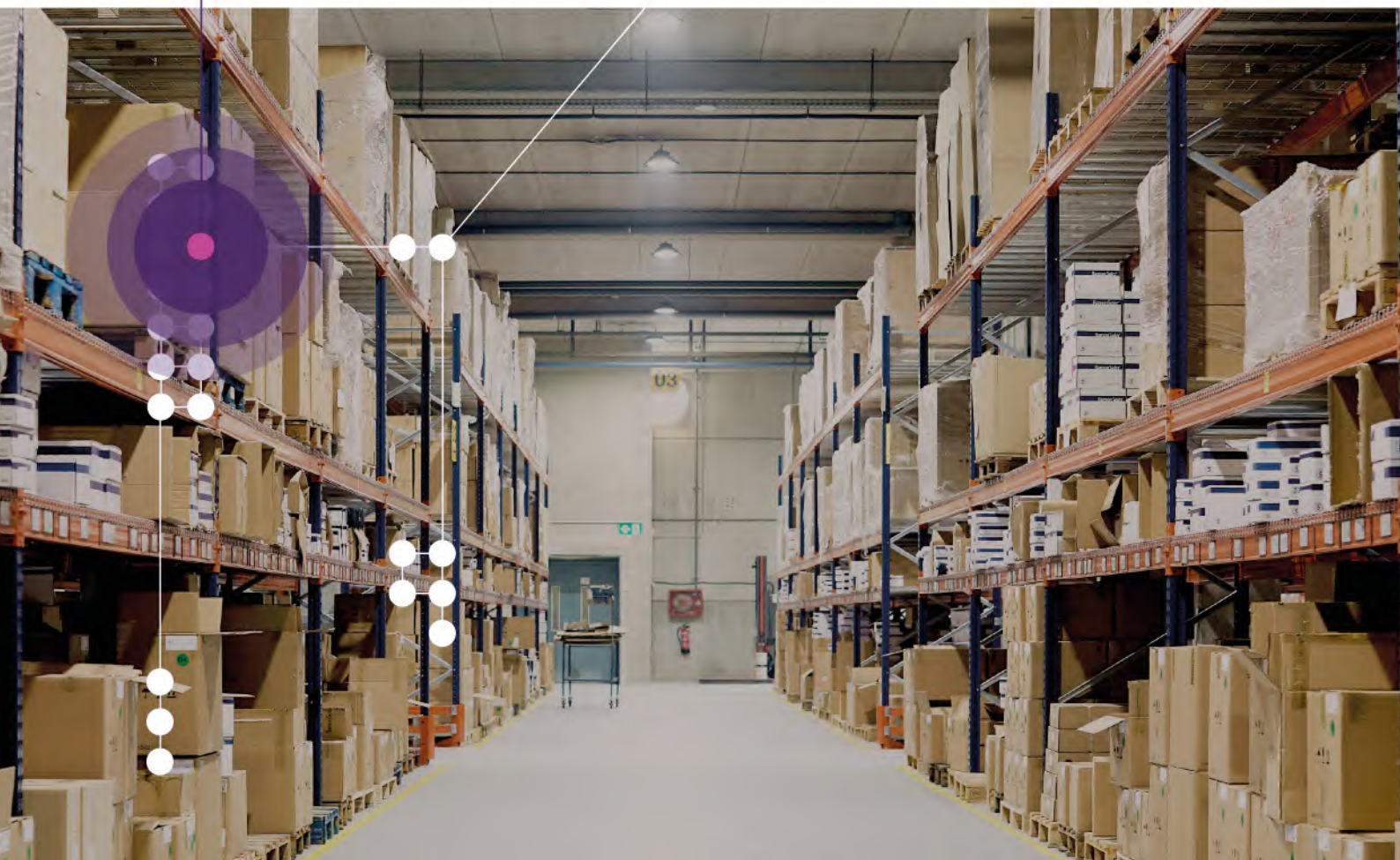
Visualiza y asegura todos tus activos.

Armis, la compañía líder en la industria de visibilidad y seguridad de activos.

IT IoT IIoT OT IoMT Virtual Cloud

Contacta hoy con nosotros.
Vesku.turtia@armis.com

www.armis.com



• EFEMÉRIDES •

Zerolynx: cumple un lustro y se consolida como referencia en el mercado

Zerolynx es un grupo empresarial que nació hace 5 años de la mano de un conjunto de inversores con gran experiencia en el sector y que buscaban lanzar un proyecto líder que, a medio plazo, se consolidase como una referencia internacional. Dejando a un lado la estabilidad de nuestros respectivos proyectos anteriores, decidimos emprender una nueva aventura en un momento en el que aún no se vislumbraba toda la inestabilidad global acontecida tras el Covid-19.

Teníamos claro lo que queríamos alcanzar y cómo queríamos llevarlo a cabo; buscábamos un proyecto sin tabúes orientado a lo que realmente necesitaban los clientes, dinámico, atractivo y centrado en la calidad por encima de todo. Y eso es lo que hemos conseguido cinco años después, sobreponiéndonos a los vaivenes de un mercado que, aún en auge, padece una gran inestabilidad. Este mes hemos cumplido nuestro primer lustro y hemos consolidado un proyecto que ya tiene nombre, que convence por sus valores, integridad y transparencia, y que responde a un hueco del mercado que apenas ocupan un puñado de boutiques especializadas como la nuestra.

Hablar de uno mismo siempre es difícil. Se corre el riesgo de entrar en la arrogancia y de ensalzar de más los méritos y las metas alcanzadas, pero bajo una valoración plenamente objetiva, todo lo logrado no entraba ni en la mejor de nuestras quinielas, y esa es la conclusión con la que preferimos quedarnos. Hace cinco años no nos imaginábamos haber llegado hasta aquí, con un equipo de más de 50 compañeros, con multitud de premios y reconocimientos y siendo el proveedor de referencia para más de 100 clientes, en su mayoría multinacionales y entidades del Ibex-35.

Pero aún con un proyecto consolidado, seguimos teniendo presente que el camino acaba de iniciarse. Zerolynx sigue siendo una organización joven que debe seguir creciendo y madurando a la vez que lo hace un mercado como el español, que poco a poco va forjándose un nombre internacional y que ya ocupa el 4º puesto a nivel mundial. Y es precisamente en esa internacionalización donde hemos puesto nuestro próximo objetivo. Una quinta parte de nuestras operaciones ya se realizan fuera de nuestras fronteras, cifra que esperamos siga creciendo a lo largo de este 2023.

El futuro es incierto y probablemente ninguno podremos aventurar si Zerolynx vivirá cinco, 50 o 500 años más, pero lo que sí podemos afirmar es que hacemos lo que nos apasiona, disfrutamos cada minuto del día y nos alegramos de cada proyecto ganado y de cada enhorabuena de un cliente como si fuese el primero, y cuando haces de tu pasión la razón de tu vida, todo es más sencillo.

Y no queríamos despedir el artículo sin haceros partícipes de nuestra celebración o, mejor dicho, de nuestras celebraciones. A lo largo de este 2023 realizaremos cinco eventos en diferentes formatos para que podáis disfrutar de un rato junto a nosotros, conocer nuestras nuevas instalaciones de Madrid y aprender y disfrutar acerca de lo que más nos apasiona y nos une: la ciberseguridad. ¡No dudéis en escribirnos si os apetece acompañarnos!

Juan Antonio Calles
CEO
Grupo ZEROLYNX

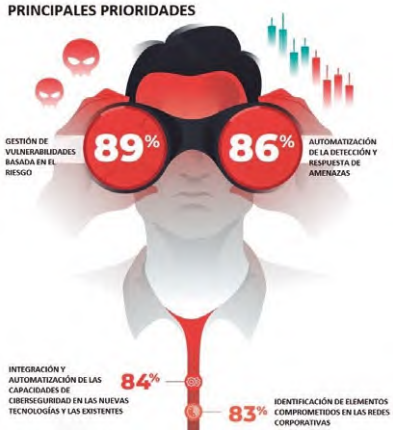
Automatización, gestión de alertas del SOC y confianza cero, prioridades de los CISO en 2023

La compañía **Lumu** ha realizado un informe en EE.UU., titulado 'Lumu CISO Priorities Flashcard', con la opinión de más de 213 CISO y ejecutivos de la alta dirección para conocer sus prioridades este año. En él destaca, en primer lugar, una clara apuesta por la automatización, además de buscar cómo aprovechar de forma más intensiva nuevas tecnologías, incluida la IA y el aprendizaje automático, para aumentar la eficiencia y la eficacia de su talento existente en ciberseguridad.

Aunque el número de profesionales en el país se mantuvo estable en 2022, según datos de la **Iniciativa Nacional para la Educación en Ciberseguridad del Instituto Nacional de Estándares y Tecnología, CompTIA** y **Lightcast,** también es cierto que en los últimos meses muchas tecnológicas han realizado despidos masivos para ahorrar costes, "lo que obligará a las organizaciones a reajustar sus prioridades en 2023 para llenar el vacío", destaca el informe que, también, alerta de que este año podría darse de forma imperativa la necesidad de "hacer más con menos para mantener sus redes seguras", según ha explicado el director ejecutivo y fundador de Lumu, **Ricardo Villadiego.**

Apuesta generalizada

Así, entre otros datos, de interés, un 86% de los responsables de ciberseguridad consultados destacaron que priorizarán la automatización de la detección y respuesta a amenazas, un 81% el cambio de las plataformas de ciberseguridad heredadas a las plataformas nativas de la nube y un 84% también resaltó que trabajará en la integración y automatización de las capacidades de ciberseguridad con tecnologías nuevas y existentes.



A ello se suma que, como respuesta al actual panorama de ciberincidentes, un 79% planean adoptar o mejorar sus capacidades de 'caza de amenazas', el 74% llevará parte de sus operaciones de ciberseguridad de forma interna, para administrar estratégicamente las vulnerabilidades, el 73% piensa optimizar la administración de alertas de su Centro de Operaciones de Ciberseguridad (SOC) y también un 73% adelantará que implementará una estrategia de confianza cero.

Entelgy Innotec
SECURITY

Live confident,
be (cyber) secure

The winning teams

Red Team

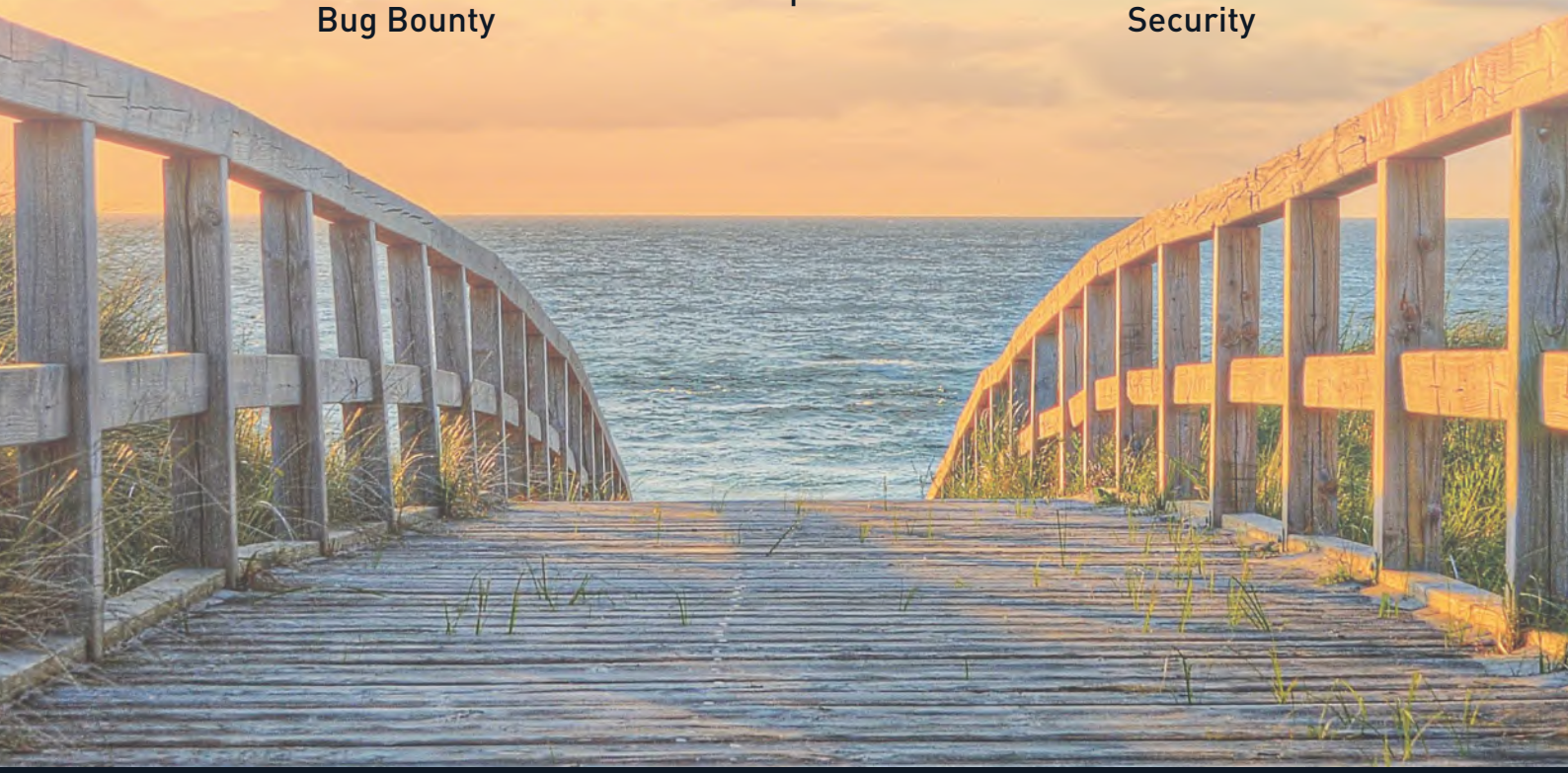
- Pentesting
- TIBER Exercises
- Atomic & Purple Team
- Private Bug Bounty

Golden Team

- Strategy & Governance
- IT / OT Risk
- Resiliency
- Compliance

Blue Team

- Detection & Response
- Digital Risk Protection
- Attack Surface Reduction
- Infrastructure Security



innotec.security

Argentina | Brasil | Chile | Colombia | España | México | Perú | USA

FIRST · TF-CSIRT Trusted Introducer · Centro de Ciberseguridad Industrial · CSIRT.es · Red Nacional de SOC · ISACA · isms forum

El galardón recayó en la francesa Mindflow, con una solución SaaS sin código para automatizar las tareas repetitivas en la gestión de incidentes

La ECSO entrega el premio STARTup en un evento que se realizó por primera vez en España, de la mano del BASQUE CYBERSECURITY CENTRE e INCIBE

Bilbao fue el escenario elegido por la **Organización Europea para la Ciberseguridad** (**ECSO**), para celebrar el 7 y 8 de marzo, y por primera vez en España, la tercera edición del 'Premio STARTup', creado para aumentar la visibilidad y fortalecer el ecosistema innovador europeo de ciberprotección, y que fue organizado por el **Basque CyberSecurity Centre** (BCSC) con la colaboración del **Instituto Nacional de Ciberseguridad** (Incibe).

Javier Diéguez, BCSC

Premio STARTup a Mindflow


Axel Deininger, ECSO

El evento congregó a más de 200 asistentes de alto perfil compuesto tanto por los miembros de las entidades organizadoras, como por especialistas de ciberseguridad, CISOs y más de 30 entidades inversoras de Europa, de América y Oriente Medio.

El acto de inauguración contó con personalidades como **Estébaliz Hernáez**, viceconsejera de Tecnología, Innovación y Transformación Digital del Gobierno Vasco, y **Carme Artigas**, secretaria de Estado de Digitalización e IA.

La presentación del encuentro también corrió a cargo de **Axel Deininger**, presidente de la ECSO, quién resaltó la labor de la Organización y la de la recién creada **Comunidad Europea de Ciberseguridad** (ECCO) –de la que SIC ya informó en su nº153–.

El directivo recordó que "Europa representa la tercera economía del mundo y, por ello, también, es uno de los principales objetivos de los cibercriminales". Por ello, "es importante hacerles frente, no solo a través de las regulaciones sino, también, con la generación de un entorno propicio para la creación y crecimiento de las empresas de ciberseguridad que conduzca, además, hacia un verdadero mercado único europeo".

Tras su intervención, se llevaron a cabo las rondas de presentación de las 11 empresas europeas seleccionadas, durante 2022, en los 'Cyber Investor Days' de la ECSO: **Mindflow, Angoka, brighterAI, Cryptomage, Alcyconie, Exalens, Omnios, Vaultree, Cyscale, Strong Network** y **ResQuant.** Cada uno de sus responsables subió al escenario para explicar, en un máximo de cinco minutos, en qué consiste su proyecto y por qué merecía el premio.

Premio a la automatización de gestión de incidentes

Finalmente, durante la tarde, se llevó a cabo la votación por parte de los miembros del jurado, presidido por **José Palacio**, responsable Global de Operaciones de Seguridad y Detección de Amenazas de **Grupo Santander**, siendo reconocida con el galardón de este año la empresa francesa **Mindflow**. **Xabier Mitxelena**, presidente de **Cybasque,** fue el encargado de otorgárselo poniendo en valor su plataforma SaaS sin código, para la automatización de las tareas repetitivas de la gestión de ciberincidentes. Como vencedora, recibirá un año gratis la etiqueta 'Cybersecurity made in Europe' de la ECSO, horas de mentoría a cargo de uno de los socios organizadores y mayor visibilidad dentro de la comunidad europea de ciberprotección.

Foto conjunta de las *startups* finalistas, la ganadora y los miembros del jurado

Innovación europea

Sin embargo, todas las finalistas destacaron por su innovación en soluciones que buscan desde una mejor protección de la privacidad y la anonimización, hasta mayor seguridad para el IoT, protección ante las futuras amenazas de la computación cuántica o soluciones ciberfísicas de detección y respuesta para fábricas, y tecnología de cifrado para datos en uso. Entre ellas, también fue notable la presencia de una *startup* española, Omnios, de origen catalán, con una propuesta basada en inteligencia artificial para clasificar y extraer información relevante de datos desestructurados de ciberseguridad, para ser más competitivos en el mercado.

Women4Cyber STARTup Award

Además, y por primera vez, se otorgó el primer 'Women4Cyber STARTup Award' en reconocimiento a las empresas de ciberseguridad fundadas por mujeres o que cuentan, al menos, con un 50% de mujeres empleadas. El galardón recayó en **Angoka**, una firma de seguridad IoT para proteger las comunicaciones de máquina-a-máquina (M2M) en ciudades inteligentes y entornos móviles. El premio fue entregado por **Annet Mádi-Nátor**, presidenta de Women4Cyber, y **Ana Ayerbe**, directora de Digital Cores de **Tecnalia**.

Junto con la entrega de premios, durante las dos jornadas del encuentro también se abordaron aspectos de gran interés para el sector, a través de diversos los paneles de discusión en los que se analizó cómo impulsar el mercado de la ciberseguridad en Europa, la repercusión de las regulaciones en el éxito comercial y la importancia de que política industrial europea de ciberprotección funcione bien.

Asimismo, se presentó a los asistentes internacionales como caso de éxito el programa BIND 4.0 Open Innovation & Acceleration Platform, promovido por el **Grupo Sprí** y el gobierno vasco hace siete años para conectar y generar simbiosis entre *startups* y compañías ya consolidadas.


Premio Women4Cyber STARTup otorgado a Angoka

Finalmente, durante el acto de clausura, el director del BCSC, **Javier Diéguez**, destacó la importancia del ecosistema de ciberseguridad del País Vasco que, "en mi opinión, es el más avanzado del sur de Europa". Además, "hemos diseñado un plan estratégico con el sector para hacer que este ecosistema sea aún más competitivo. Nuestra ambición es dirigir la especialización a los riesgos de ciberprotección, especialmente, en los sectores de energía y fabricación como, por ejemplo, de dispositivos médicos", puntualizó. Asimismo, destacó el carácter 'out of the box', como filosofía del encuentro para "hacer cosas diferentes", animando a las empresas a desarrollar un pensamiento disruptivo.

Texto: **Ana Adeva**

NEGOCIO Y CIBERSEGURIDAD

HAGA QUE SU NEGOCIO ESTÉ CIBERTRANQUILO

En la era de la transformación digital y en un momento en el que la soberanía digital plantea interrogantes, **hacer que su negocio esté cibertranquilo es vital dado el impacto financiero de los ciberataques.**

Para la protección de redes, datos, estaciones de trabajo y servidores: al elegir las soluciones Stormshield, recurre a un actor de la ciberseguridad en el que puede confiar.

STORMSHIELD

www.stormshield.com

Hasta siempre, Ana

Justo al cierre de esta edición de abril, en SIC recibimos la trágica noticia del fallecimiento de **Ana Prieto**, Security Manager de Ericsson, una excelente profesional que venía prestando sus servicios durante los últimos dieciséis años en la multinacional sueca de comunicaciones.Experimentada profesional de la protección en todas sus dimensiones, Prieto acumulaba una dilatada trayectoria de solvente desempeño en las áreas de TIC y servicios para la industria. Su denso bagaje profesional acumulaba enorme experiencia en seguridad física y personal, en gestión de crisis y continuidad de negocio, y en el último tramo con intenso foco en seguridad de la información. Master en ISMS por la UPM y lead autor en ISO 27001, colaboró con la revista en repetidas ocasiones. En sus tiempos de ocio gustaba de disfrutar de deportes de alta intensidad. Todo el equipo de SIC transmitimos nuestro pésame y condolencias a la familia, allegados y compañeros de empresa. Hasta siempre y gracias, Ana. **SIC**

La COMISIÓN lanza un *sandbox* normativo europeo para *blockchain*

La **Comisión Europea** presentó en febrero el *sandbox* regulatorio europeo para *blockchain.* Como se sabe, los *sandboxes* son entornos controlados donde las empresas pueden probar sus productos y servicios mientras interactúan con los reguladores pertinentes. Este *sandbox* proporcionará seguridad jurídica para las soluciones tecnológicas descentralizadas, incluida la cadena de bloques, al identificar los obstáculos para su implementación desde una perspectiva legal y regulatoria, y brindar asesoramiento, experiencia y orientación en un entorno seguro y confidencial.

European Blockchain Sandbox
European blockchain regulatory sandbox for Distributed Ledger Technologies

TRIBUNA SIC

La conquista del planeta de los simios (o del analista de ciberseguridad) por ChatGPT

Como en la saga de películas de *El planeta de los simios*, los pobres analistas de ciberseguridad, en sus múltiples facetas (inteligencia, alertas, incidentes...) son permanentemente cuestionados y las apuestas cotizan al alza con cada nuevo concepto, tecnología y/o herramienta que viene a sustituirlos. Elementos que permitirán, ahora sí, que todo funcione de manera "automágica", inteligente, sin falsos positivos (ni negativos) y, por supuesto, a una décima parte del coste actual. Si a ello le unimos la escasez actual de profesionales que quieren y pueden dedicarse a esta tarea, tenemos la tormenta perfecta para que florezcan cada vez más teorías y tecnologías que jubilan anticipadamente al analista de ciberseguridad.

El futuro real es la convivencia de ambas especies, donde cada una (las tecnologías de automatización e inteligencia artificial y los analistas) realice lo que mejor sabe hacer

Más allá de las frases "marketinianas" tan en boga en estos momentos como SOCLess o automatización inteligente, o más allá de las soluciones, empresas y charlas que prometen un SOC sin analistas, totalmente automatizado y sin apenas intervención humana, donde la propia IA es quién avisa si se les necesita, la experiencia diaria dista mucho de ello. Por este motivo, los analistas de ciberseguridad todavía tienen una larga vida por delante. Es cierto que su labor se ha venido transformando en los últimos años y tiene que seguir siendo así, igual que en aquellos ámbitos tecnológicos donde surgen elementos disruptivos de verdad (no de marketing). Quién no lo hace se queda obsoleto y tiende a desaparecer, ya sean los propios analistas o sus empresas.

Evolución

Entonces, ¿cuál es la evolución esperada de esta figura? Si recurrimos a la bola de cristal (y sobre todo a la experiencia), podemos augurar que se les va a requerir salir del barro; es decir, huir del trabajo con poco valor; de infinitas alertas que revisar y donde la orquestación y la automatización están consiguiendo resultados excelentes. Recordemos que, gracias a la mejora de las técnicas de detección y la sofisticación de los ataques, los analistas están desbordados. Cada vez hay más silos de información (alertas, *logs*, inventario, vulnerabilidades, arquitectura, identidades, cambios, incidencias de TI, excepciones de negocio o de operativa, *playbooks*…). Será preciso, por tanto, centrarse en los casos que requieran investigación, contexto, análisis y razonamiento. Aplicar una vez más la desgastada teoría del 80-20. Así, el uso de tecnologías de orquestación y automatización, como la utilización real de IA o *machine learning*, permitirá desprenderse de ese 80% que tiene que gestionarse, aunque no sea glamuroso. El 20% restante quedará para la figura del analista que, además, contará con estas mismas herramientas para obtener información, conseguir respuestas o interconectar fuentes de información.

Para terminar, y volviendo al símil de *El planeta de los simios*, el futuro real es la convivencia de ambas especies donde cada una (las tecnologías de automatización e inteligencia artificial y los analistas) realice lo que mejor sabe hacer. Por un lado, la IA reduciendo las tareas repetitivas y gestionando los casos particulares y excepciones y, de otro, nuestros queridos analistas, a los que les daremos tiempo y espacio para investigar las cosas relevantes, atender los casos en los que la automatización falle o no sepa cómo gestionarlo (que también ocurre) y, por supuesto, aportar el contexto y el razonamiento a las situaciones que así lo requieren.

Este perfil requiere de un gran esfuerzo por parte del analista, pero, como dije al principio, los que no se vean capaces de desenvolverse en estas funciones terminarán por desaparecer (esto da para otro artículo).

***

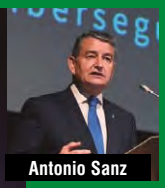
Nota: Este texto ha sido generado por ChatGPT ante la temática planteada muy acertadamente por nuestros amigos de la Revista SIC; a saber: el espacio que le va a ir quedando al analista de ciberseguridad en los terrenos de la detección+correlación/comprensión, frente al incremento de la superficie de ataque y la tendencia a la automatización inteligente.

Jorge Uyá
Director de Operaciones
INNOTEC SECURITY

La autonomía formará parte de un nodo del programa Retech, con un presupuesto de 14 millones de euros

El Congreso de ciberprotección de Andalucía pone en valor el nuevo CENTRO DE CIBERSEGURIDAD en Málaga, su rol en RETECH y la apuesta de GOOGLE

Andalucía celebró, a finales de marzo, la segunda edición de su Congreso de Ciberseguridad, organizado por la **Agencia Digital (ADA)**, que contó con más de 2.000 asistentes y buena parte de actores oferentes del sector, en el Palacio de Ferias y Congresos de Málaga (FYCMA).



El evento fue inaugurado por el consejero de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa, **Antonio Sanz,** junto al alcalde de la ciudad, **Francisco de la Torre.** "Desde la ADA se están poniendo en marcha diferentes estrategias para coordinar y acometer cada uno de los aspectos de la transformación digital de Andalucía. Un ejemplo de ello es la Estrategia Andaluza de Ciberseguridad, presentada en el marco de la primera edición del congreso y ya aprobada, además de otras que se encuentran en estado de redacción bajo la coordinación de la ADA como la Estrategia de IA, que se llevará en las próximas semanas al Consejo de Gobierno, o la de Administración Digital, centrada en las personas", destacó Sanz.

Arranca el trabajo del Centro

Mientras que en la primera edición una de las grandes novedades dadas a conocer fue el denominado Ciberescudo andaluz, fruto de la colaboración público-privada a través del **proyecto Alba**, en esta ha sido la confirmación de que en la última semana de marzo comenzará a ponerse en marcha, de forma progresiva, el denominado **Centro de Ciberseguridad** de la Comunidad, sito en el Puerto de Málaga, con un presupuesto de 60 millones de euros y cuya coordinación ha recaido en **Enrique Rando**.

Entre otras responsabilidades, el ente será el encargado de coordinar la estrategia andaluza, así como el seguimiento y la respuesta frente a ciberataques contra la Administración Pública autonómica y local, ya que también dará servicio a todo tipo de instituciones, diputaciones, ayuntamientos, universidades, incluso a empresas y a la ciudadanía en este ámbito.

Programa Retech y Proyecto Argos

Además, Sanz anunció que Andalucía participará en el programa Retech –ver sección noticias de este número– y, de forma concreta, en el Proyecto Argos, para crear una red de nodos de ciberseguridad, junto a las comunidades de Castilla y León (que lo coordina), Madrid y País Vasco. "Se trata de un proyecto que estará ubicado en el Centro de Ciberseguridad de Málaga y cuyo objetivo es impulsar una industria especializada en el desarrollo de ciberseguridad y OT en los sectores de la salud y ciudades inteligentes", añadió.

Así, durante dos días, los profesionales pudieron escuchar a muchos de los grandes referentes como representantes de la Dirección General de Informática de la Comisión Europea, la participación de **Natalia Aristimuño**, responsable de Servicios Digitales en el área de Informática del ente europeo y la presencia de expertos, como **Antonio Calderón** (CTO de NCI Agency) o **Chema Alonso**, Chief Digital Officer en Telefónica, que ofreció la ponencia 'Bad Guys en la era de IA', entre otros.

En paralelo a las ponencias, se celebró un ciclo de nueve talleres prácticos, impartidos por grandes corporaciones como **Vodafone, NTT Data** o **42 Málaga,** el centro de formación e innovación de la Fundación Telefónica en la ciudad.

Las empresas pueden conocer la labor que se hace desde el Centro de Operaciones de Seguridad de Orange en un taller que busca explicar a las pymes la importancia de anticipar, detectar y responder a las ciberamenazas. También, se dedicó un espacio para la experiencia de las mujeres TIC en el campo de la ciberseguridad a través de un taller de **Women4Cyber**.

El Centro de Ciberseguridad de GOOGLE, abrirá a mitad de este año

Como ya es bien conocido, la multinacional estadounidense apostó hace tiempo por Málaga, la pujante ciudad andaluza como el referente mundial en ciberprotección, decidiendo situar en ella unos de sus Centros de Ciberseguridad, concretamente en las instalaciones del antiguo gobierno militar. Tras unas obras que han durado casi un año, por fin verá la luz en los próximos meses.

Con la categoría de Centro de Ingeniería de Seguridad de Google (GSEC), es el tercer centro que abre la compañía en Europa, tras los de Múnich y Dublín, especializados en privacidad y responsabilidad de contenido y funcionará como un 'observatorio mundial del cibercrimen', además de colaborar con instituciones públicas y privadas y fomentar la formación de ciudadanos y empresas.

Ciberstartups españolas

Google también ha anunciado las 15 *startups* que han sido seleccionadas para el programa 'Google for Startups Growth Academy: Cybersecurity,' cuatro de ellas de origen nacional, como son la gallega **Alice Biometrics**, centrada en la verificación de la identidad de los clientes de plataformas o servicios digitales; **BlackDice**, con instalaciones en Leeds (Reino Unido) y Málaga, que proporciona defensa cibernética de nivel empresarial a operadores de telecomunicaciones a través de herramientas de *machine learning* y tecnologías predictivas que identifican patrones; y la germano española **Build38,** con soluciones y servicios de protección de aplicaciones móviles, que incluyen inteligencia artificial y tecnología de protección de aplicaciones. También, está por parte de nuestro país la vasca **Nymiz,** especializada en software de anonimización de datos personales basado en IA, que detecta datos personales en archivos no estructurados y también en datos estructurados y los anonimiza o seudonimiza de forma reversible o irreversible.

Además de un programa práctico de tres meses de duración, este grupo de empresas se beneficiará de tutorías con expertos de Google, entre ellos, de las antiguas *startups* como **VirusTotal** (adquirida en 2012) y **Mandiant** (2022). En paralelo, podrán establecer contactos con otros emprendedores del sector en distintos encuentros que tendrán lugar en Europa a lo largo de este año.

Descubre nuestro valor

Westcon

Potenciamos tu negocio con las mejores soluciones IT

ANOMALI · at&t · ATTACKIQ · audiocodes · AVAYA · CHECK POINT · CLAROTY · CROWDSTRIKE
efficient iP · Extreme Networks · f5 · FIREMON · Microsoft · Mitel
NETSCOUT · noname · okta · ORACLE · ordr · paloalto networks · poly · hp · ribbon communications · SANDVINE
SKYBOX SECURITY · spectralink · sumo logic · Symantec · zscaler

www.westconcomstor.com

Como parte del acuerdo continuarán al frente Antonio Ramos como CEO y Alfonso Pastor, responsable de las relaciones comerciales

LEET SECURITY es adquirida por UPTIME INSTITUTE, una Autoridad Global en Infraestructuras Digitales, que impulsará su crecimiento internacional

Otra empresa española más. **LEET Security** ha sido comprada por **Uptime Institute**, una Autoridad Global en Infraestructuras Digitales. Esta operación llega tras una importante inversión por parte de **Dominus Capital**, en Uptime Institute, a principios de 2022. "Durante más de 25 años, Uptime Institute ha establecido las referencias líderes en la industria de los centros de datos para su rendimiento, resiliencia, sostenibilidad y eficiencia, lo que brinda a sus clientes la seguridad de que su infraestructura digital puede funcionar en una amplia gama de condiciones operativas a un nivel consistente con sus necesidades comerciales", destaca el CEO de Leet Security, **Antonio Ramos**, que recuerda que el modelo 'Tier' de Uptime es el estándar global más confiable y adoptado de la industria de TI para el diseño, construcción y operación de centros de datos.

De esta forma, desde Leet esperan que la "unión brinde los recursos para acelerar nuestro desarrollo y continuar liderando el camino en el campo de las calificaciones de ciberseguridad al tiempo que proporciona un conjunto adicional de herramientas, servicios y soluciones, con la profundidad y amplitud necesarias para cumplir con los requisitos cambiantes de nuestros clientes".

Así, la compañía también ha destacado la importancia para sus clientes de la 'Evaluación de riesgos de infraestructura integral estandarizada para instituciones del sector financiero' (SCIRA-FSI) de Uptime Institute. Una evaluación que ha sido especialmente diseñada para ayudar en el cumplimiento de la normativa sectorial de la Autoridad Bancaria Europea (EBA) y el reglamento DORA recientemente publicado. La evaluación SCIRA-FSI complementa la plataforma PINAKES, desarrollada por Leet Security y gestionada por el Centro de Cooperación Interbancaria (CCI) para dar servicio a las entidades financieras que operan en España. Tras esta operación, Leet Security seguirá actualizando y realizando evaluaciones con su metodología de calificación. Como parte del acuerdo, continuará al frente, Antonio Ramos como CEO, reportando a **Martin V. McCarthy,** director ejecutivo de Uptime Institute. **Alfonso Pastor** será responsable de las relaciones comerciales con los clientes actuales y nuevos.

IKERLAN presenta la *spin-off* ORBIK CYBERSECURITY, primera empresa en España orientada a certificar productos electrónicos de fabricantes industriales

En 2024 se prevé que existan 22.300 millones de dispositivos IoT conectados a internet en todo el mundo. Un escenario perfecto para el crecimiento exponencial de la ciberdelincuencia, pero también una gran oportunidad para desarrollar el negocio de la ciberseguridad y generar empleo tecnológico de calidad protegiendo a la industria de ciberataques. En ese contexto, el centro tecnológico vasco **Ikerlan** identificó, hace ahora dos años, una ventana de oportunidad: ofrecer a la industria un sello externo que certifique que sus productos son ciberseguros. Aquella idea ha germinado en **Orbik Cybersecurity,** su nueva *spin-off*, basada en el *know-how* y la experiencia de Ikerlan y la única de España orientada a dar servicio a fabricantes europeos industriales de equipamiento electrónico que quieren posicionarse en el mercado como compañías que ofrecen productos ciberseguros certificados antes de que sea obligatorio hacerlo, por ejemplo, en cumplimiento de normativas como la Ley de Ciberresiliencia europea.

Con sede en Euskadi y vocación internacional, la compañía aspira a consolidarse como laboratorio de evaluación de conformidad respecto a normativas internacionales y servicios añadidos de ciberseguridad, como el análisis activo y continuo de vulnerabilidades, en todo el ciclo de vida de operación de los productos industriales.

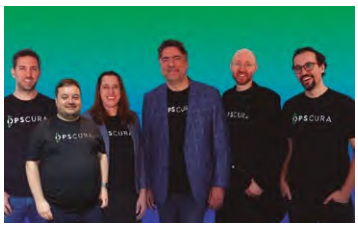
La compañía sale al mercado con el foco puesto en empresas del sector eléctrico, fundamentalmente fabricantes de componentes y sistemas, y a medio plazo, prevé extender su actividad a empresas de bienes de equipo industriales, transporte, máquina herramienta y productos de ciberseguridad.

Para 2027, Orbik Cybersecurity aspira a contar con un equipo de veinte profesionales, estar presente en el mercado europeo y alcanzar dos millones de euros de facturación. **Salvador Trujillo,** hasta ahora responsable del área de ciberseguridad en Ikerlan, será el CEO de la nueva compañía.

Durante una primera fase, Orbik Cybersecurity se va a ubicar en las recientemente inauguradas instalaciones del laboratorio Digilab de Ikerlan en Gipuzkoa. Además, durante el año 2023, Digilab se convertirá en el primer laboratorio de ciberseguridad industrial del España acreditado por ENAC conforme a la norma UNE17025.

OPSCURA, heredera de Enigmedia, cierra una ronda de 8,6 millones de euros para su protección industrial

Opscura Inc, empresa de ciberseguridad de sistemas de control industrial (ICS) que fue fundada en España bajo el nombre de **Enigmedia** hace doce años, ha cerrado una ronda Serie A de 8,6 millones de euros liderada por **Anzu Partners** y con inversiones de **Dreamit** y **Mundi Ventures**, por la que se convierte así en la nueva marca de la compañía y fija su intención de ser una empresa global, apoyada por un equipo internacional y por la actualización y desarrollo de nuevos productos. Un movimiento con el que la empresa espera captar más socios y clientes estadounidenses que busquen proteger y conectar sus operaciones críticas en OT.



"Conseguimos extender la vida de los sistemas industriales desde la seguridad y no impactamos en las comunicaciones de las empresas, lo que nos permite reducir los riesgos operativos como el *ransomware*. Nuestra labor ha sido reconocida por varios proveedores industriales globales", detalla el cofundador y CTO de Opscura, **Gerard Vidal**.

Los cofundadores de Opscura, Gerard Vidal y **Carlos Tomás,** asumirán los cargos de director de Tecnología (CTO) y vicepresidente de Ingeniería, respectivamente, como parte de un nuevo equipo directivo global liderado por el nuevo CEO, **David Hatchell.** El equipo ejecutivo de Opscura también incluye al director de Producto, **Michael Garrison Stuber,** al director de Clientes y director de Seguridad de la Información, **Brian Brammeier,** y a la asesora estratégica **Allison J. Taylor,** que anteriormente ocupaba el cargo de directora de Marketing interina.

CIBERSEGURIDAD

Nuestro reto, tu tranquilidad

Apostamos por un tratamiento global de la ciberseguridad, **identificando** las amenazas existentes, **protegiendo** los activos, **detectando** intentos de ataque y, si se producen, **restableciendo** la situación lo antes posible, todo orquestado mediante los sistemas de gestión más exigentes.

¿Qué podemos hacer por ti?

- Descubrimos las **vulnerabilidades** existentes y nos aseguramos de que queden resueltas.
- Te mostramos cómo aprovechar las capacidades que **cloud** ofrece para detectar malware avanzado o parar ataques de denegación de servicio.
- Adoptamos la filosofía **SecDevOps**, para que tus procesos de desarrollo sean más ágiles y resilientes.
- Utilizamos **Inteligencia Artificial** para combatir el fraude de forma certera y totalmente personalizada.
- A través de **ciberinteligencia**, interpretamos adecuadamente la información a nuestro alcance para tomar las mejores decisiones en tiempo real.
- Te ayudamos a cumplir con la **legislación** vigente de tu sector para que consigas el óptimo nivel de ciberseguridad y privacidad.

marketing.TIC@gmv.com

gmv.com

gmv®
INNOVATING SOLUTIONS

Se ha consolidado en menos de cuatro años como una referencia en el ámbito de la protección de los entornos OT

SIEMENS amplía su nodo de Ciberseguridad en Madrid, superando los 100 empleados y trabajando con sus homólogos de China, EE.UU., Portugal y Alemania

Siemens ha reforzado su apuesta por España con la ampliación de su nodo de ciberseguridad en Madrid y la contratación, en los últimos dos años, de 50 nuevos expertos en gestión de riesgos y software en la nube. Con este paso adelante, la compañía eleva a más de un centenar la plantilla del Centro, desde el que se monitoriza y gestiona protección de infraestructuras y clientes del Grupo en todo el mundo.

El 'hub' de Madrid se abrió en 2019 con la contratación de una decena de ingenieros expertos y, ante el auge de la demanda de servicios de seguridad de los clientes y de la propia compañía, solo un año y medio después ya contaba con 45 especialistas que daban cobertura a varios proyectos globales. Esta tendencia no ha parado de crecer y hoy este nodo es ya una referencia consolidada en la red internacional de protección de Siemens, que cuenta con otros centros similares en China, EE.UU., Portugal y Alemania. El 'hub' madrileño está dotado con profesionales de distintos perfiles especializados en gestión de riesgos, operaciones, soluciones y estrategias que trabajan en el desarrollo de tecnologías y sistemas de prevención, protección y detección de ciberamenazas.

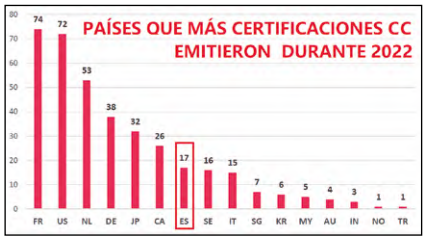
Profesional de referencia

Junto al 'hub' de Ciberseguridad, desde Madrid opera también la responsable global del área de ciberdefensa, **Karen Gaines,** que trabaja con un equipo internacional integrado por 160 expertos en nuevas tecnologías y que, además, recientemente ha tomado el liderazgo del equipo global de desarrollo de negocios para impulsar la presencia de la ciberseguridad de Siemens en el mercado.

"La ciberseguridad es esencial cuando se trata de proteger infraestructuras críticas y datos confidenciales. La creciente aplicación del Internet de las Cosas (IoT) afecta de lleno a los equipos industriales. Esto puede contribuir a desarrollar amenazas en la cadena de producción y aumentar la exposición a los ciberataques. Para evitarlo, Siemens aplica el concepto de defensa en profundidad que implementa la ciberseguridad a lo largo de todo el ciclo de vida del producto o servicio", destacan desde Siemens a la vez que recuerdan que disponen de un equipo de 1.300 expertos en ciberprotección, además de impulsar el **'Charter of Trust'**, para promover un protocolo conjunto que logre crear un mundo digital más seguro mediante normas y estándares.

Las certificaciones COMMON CRITERIA registran una desaceleración en 2022, por primera vez en cinco años, según un informe de JTSEC de APPLUS+

La necesidad de estar certificado para generar confianza y, también, por razones regulatorias continúa impulsando el mercado de las certificaciones de ciberseguridad. La más popular en este ámbito es la Common Criteria (Criterios Comunes, CC), que data de los años 90. Prueba de su vigencia es que, en 2022, según un amplio informe de la compañía española **jtsec**, de **Applus+,** se completaron un total de 370 certificaciones en todo el mundo, una cifra ligeramente menor que la del año anterior, con 399. Esto supone que, por primera vez en cinco años, disminuyó el número de certificaciones de este tipo.



Entre las razones que explican esta situación, según el informe, destacan tanto "la falta de capacidad de los laboratorios u organismos de certificación para gestionar un mayor número de certificaciones, como la de disponibilidad de algunos fabricantes para llevar a cabo la certificación Common Criteria, ya sea por tiempo y coste, entre otras cuestiones". A ello, se suma que frente a CC, han surgido en los últimos años otros estándares de ciberseguridad por los que cada vez apuestan más compañías como, por ejemplo, la certificación ligera 'Lince', impulsada por el **CCN.** Buena prueba de ello, dice el documento, es que mientras que jtsec inició el año pasado 60 procesos de evaluación de tipo Lince, solo acometió tres de CC. Eso sí, España ocupa la séptima posición mundial en emisión de CC en 2022, tras Francia, EE.UU., Países Bajo, Alemania, Japón y Canadá.

De cualquier forma, el informe también destaca que las razones para explicar la desaceleración que está sufriendo Common Criteria "no están claras", por lo que habrá que esperar a ver "los números de 2023 para conocer y comprender mejor el mercado de CC". Además, desde jtsec destacan que gracias a haber pasado a formar parte de Applus+ y de su Applus Cybersecurity Labs, en 2022, junto a **Lightship.**

En dos años, uno de cada tres países regulará los pagos y las negociaciones por incidentes con *ransomware* para frenar la financiación del cibercrimen

Los analistas de **Gartner** han pronosticado en su 'Security & Risk Management Summit 2023 India' que hasta 2025, el 30% de los estados nacionales aprobará una legislación que regule los pagos, las multas y las negociaciones de *ransomware*, frente a menos del 1% en 2021. "Reconocer el impacto de pagar. Las

pandillas modernas de *ransomware* se han desplazado para robar datos y cifrarlos. El pago significa que los datos robados no se publicarán, pero es muy posible que se vendan o se divulguen en una fecha posterior si la información tiene valor", destacaron sus expertos.

Durante el evento, también se puso el valor que, según sus investigaciones, el 60% de las organizaciones adoptará Zero Trust como punto de partida para la seguridad en 2025. Además, para dentro de dos años, el 60% de las empresas utilizarán el riesgo de seguridad cibernética como un impulsor para la realización de transacciones de terceros y compromisos comerciales.

zscaler™

Experience your world, secured

Transformación de la seguridad

Pase de la seguridad heredada a un modelo de confianza cero

Modernización de la infraestructura

Simplifique la conectividad de las sucursales y la nube

Habilitación del lugar de trabajo moderno

Obtenga un acceso rápido y seguro a las aplicaciones desde cualquier lugar y dispositivo

www.zscaler.es

Durante la 'Hacker Night' se reportaron 60 y se repartieron más de 36.000 euros entre los participantes que las encontraron

ROOTEDCON hace públicas numerosas vulnerabilidades y bate su récord de asistentes con más de 4.000

Román Ramírez, cofundador y resto del equipo RootedCON

Arantxa Sanz entrega a Chema Alonso el premio Raúl Jovér

Con José Manuel Vera (SIC), no faltó el humor

En su décimo tercera edición, el que es considerado el mayor y más destacado congreso de ciberseguridad técnica en España, superó con creces la barrera de su madurez. Del 9 al 11 de marzo, con más de 4.000 asistentes y la presencia de importantes empresas, se pudieron disfrutar de las ponencias de 80 expertos que realizaron demostraciones de casos prácticos, además de novedosas herramientas para luchar contra los cibercriminales y, de forma inédita, vulnerabilidades descubiertas en sistemas críticos.

Entre los más seguidos, destacaron ponentes como **David Meléndez, Juan Antonio Calles, Ana Junquera, Pablo San Emeterio Alfonso Muñoz, Sandra Bardón, Elías Grande, Ana de la Torre, Jordi Murgó, Lorenzo Martínez, David Marugán, Juan Antonio de Sotomayor, Fran Ramírez, Rafa Troncoso, Tomás Isasia**, **Emilio Rico** y **Antonio Sanz,** entre otros, batiéndose también el récord de conferenciantes femeninas.

"Si algo caracteriza a este congreso es la premisa de neutralidad. Es decir, acogemos a todo tipo de perfiles, pues el objetivo es que la Comunidad adquiera todo el conocimiento necesario para seguir luchando contra el cibercrimen", destacó la presidenta del congreso, **Arantxa Sanz,** en su presentación. Además, la cita reconoció este año la labor de todo un 'clásico': **Chema Alonso**, de Telefónica con el 'Premio Raul Jover', que destinó a la **Fundación Gomaespuma**.

Nueva vulnerabilidad

En esta edición RootedCON contó con responsables de ciberseguridad de empresas de referencia, representantes de FF.CC.SS. e instituciones públicas. Precisamente, entre las ponencias más valoradas estuvo la de los dos investigadores de la empresa gallega **Tarlogic**, **Antonio Vázquez** y **Jesús Mª Gómez**, que presentaron una vulnerabilidad descubierta, reportada y bautizada como 'BlueTrust' (un fallo de seguridad que permite a potenciales atacantes interferir en las redes de dispositivos con conexión *bluetooth*, pudiendo extraer datos personales e información de quién se conecta, con quién, etc).

Esta edición, además, una serie de colaboradores nutrieron el congreso con diversos contenidos, con *tracks* paralelos: **Criptored**, **ProtAAPP**, **Hacktricks**, **Securiters** e **ISACA Madrid**. No faltó una amena ponencia a cargo del redactor de **Revista SIC, José Manuel Vera,** bajo el título 'Hacker Memes'.

Por último, en la denominada 'Hacker Night', con la participación casi un centenar de investigadores, se reportaron más de 60 vulnerabilidades, siete de ellas críticas, y se repartieron 36.300 euros como recompensa.

TELEFÓNICA, primera empresa del Ibex 35 en certificarse en el nuevo ENS por AENOR

Telefónica ha conseguido ser la primera empresa del **Ibex 35** en obtener el certificado de la entidad independiente **Aenor,** por cumplir con los requisitos recogidos en el nuevo Real Decreto RD 311/2022 sobre el Esquema Nacional de Seguridad (ENS), que entró en vigor en mayo de 2022. En la actualizada normativa, además de establecer las condiciones mínimas para una prestación segura y adecuada de los sistemas de información, soluciones y los datos que producen, se ha introducido una nueva familia de medidas para los servicios en la nube. Además, se ha incorporado el principio de vigilancia continua para detectar cuanto antes los posibles ataques.

"Obtener esta certificación del ENS 2.0. en servicios como la nube privada VDC en Cloud, y la gestión y soporte de los dispositivos en ciberseguridad muestra nuestro altísimo nivel de exigencia en los servicios que prestamos y nuestro máximo compromiso con nuestros clientes", ha explicado la CEO de Ciberseguridad y Cloud de Telefónica Tech, **María Jesús Almazor.**

De izq. a dcha.: María Jesús Almazor (Telefónica Tech), Rafael García Meiro (Aenor), y Adrián García (Telefónica España)

"Aenor ha concedido 240 certificaciones ENS desde 2013 y es la primera entidad acreditada por la Entidad Nacional de Acreditación (ENAC) en la nueva versión del esquema. En Telefónica, nuestros auditores siempre encuentran una organización orientada a la vanguardia en cuestiones de ciberseguridad y servicios tecnológicos, conscientes de su importante papel tractor de buenas prácticas en el conjunto del tejido económico", ha añadido el CEO de la entidad AENOR, **Rafael García Meiro.**

Telefónica España es, además, la empresa con el mayor número de sistemas de información y servicios de categoría alta de seguridad por Aenor en el ENS, con 58.

Por otra parte, la compañía ha dado a conocer que ha evolucionado su solución de Gestión de Vulnerabilidades basada en Riesgos (NextDefense-VRM) y lanza globalmente 'Web Application Scanning 2.0.' Basado en la tecnología de **Tenable,** se trata de un nuevo servicio de escaneo y análisis avanzado que ayudará a las empresas a poder identificar y corregir vulnerabilidades de seguridad en sus aplicaciones web.

LOGICALIS
Architects of Change

Seguridad integral de todos los datos y entornos IT

IBM Security Guardium

Proteger todos los activos tecnológicos de una organización es posible, tanto en entornos locales como en Cloud.

IBM Security Guardium lo logra y permite a los equipos IT afrontar las múltiples amenazas que acechan a sus sistemas, datos y aplicaciones.

Gracias a una monitorización completa de la infraestructura IT en tiempo real, que facilita también el despliegue de estrategias Zero Trust, impide cualquier acceso no autorizado a la información.

Ofrezca experiencias digitales de calidad a sus empleados, en nubes públicas y privadas, con total seguridad, comodidad y eficacia.

Adelántese y evite fugas de datos, entradas no permitidas o ciberataques a sus instalaciones con IBM Security Guardium. La protección más avanzada y completa de todos sus entornos IT.

La seguridad de la información más sensible para su negocio ya está aquí. En cualquier entorno y en todo momento.

Y con tecnología IBM.

¿Qué podemos hacer por su organización?

Contacte con Logicalis y conozca cómo podemos ayudarle.

Para más información, visite www.es.logicalis.com

Email: marketing-es@es.logicalis.com

¿Necesita una mejor estrategia de defensa?

Si quiere saber más sobre IBM GUARDIUM descárguese el siguiente QR

El fulgor de la ciberseguridad crepita nuevamente en las Fallas

Por cuarta vez en su dilatada historia, y entre la variadísima temática que jalonan sus imaginativas creaciones, las **Fallas** en Valencia volvieron a acoger en su reciente edición de 2023, a mediados de marzo, un tema decididamente inhabitual en su temática convencional: la ciberseguridad.

Este hecho se debió una vez más al innovador proyecto puesto en marcha por la compañía especializada valenciana **S2 Grupo** en conjunción con la **Falla Chiva-Francisco de Llano**, plasmándose en su ideario: "Concienciemos a la sociedad en materia de ciberseguridad para seguir avanzando sin riesgos por el camino digital".

Esta apuesta de S2 Grupo y las Fallas de Valencia por mejorar la calidad de vida digital de la sociedad, se concreta en la pretensión de sus directivos de que, con sus iniciativas de divulgación y concienciación, poder contribuir a que colectivos especialmente vulnerables en estos temas, los menores y las víctimas de cualesquiera violencias, adquieran los conocimientos adecuados para protegerse de actos y ataques cibernéticos, y de eventuales intromisiones y agresiones a la privacidad.

Actividades en unas Fallas ciberseguras

En este contexto "La Falla Cibersegura" 2023, se diseñó y construyó en torno a conceptos de ciberseguridad subyacentes a los juguetes conectados. Expertos de la compañía han asesorado en la creación del monumento para poner énfasis en los ciberpeligros más comunes asociados a este tipo de artículos y consejos para disfrutarlos de una forma cibersegura.

El artista **Salva Dolz** ha mostrado a través de las diferentes escenas y ninots las dos caras de los juguetes conectados a Internet: la más lúdica y con la que hay que tener precaución. En este sentido, como se pudo observar en el monumento infantil de la Falla Chiva-Francisco de Llano, algunas de las principales ciberamenazas relacionadas con los juguetes inteligentes o 'smart toys' son los ataques mediante suplantaciones de identidad, la manipulación, la divulgación de información privada, las denegaciones de servicio y las elevaciones de privilegios, entre otras.

Todas las personas que visitaron esta Comisión tuvieron la opción de descargarse a través de un código QR un informe sobre ciberseguridad en los juguetes conectados realizado por el equipo de expertos de S2 Grupo para que las familias tuvieran un mayor conocimiento sobre este ámbito y pudieran tomar las precauciones necesarias a la vez que disfrutar de este tipo de juegos. De esta forma, se unió la tradición de una fiesta centenaria con la tecnología.

32,7 MILLONES DE FACTURACIÓN

A tenor de los resultados cosechados, la trayectoria de S2 Grupo desde su creación continúa siendo fulgurante, habiendo cerrado 2022 con un volumen de negocio de 32,7 millones de euros, implicando un crecimiento del 30,2% con respecto al anterior y contando con medio millar holgado de especialistas en sus filas. Su vocación y pujanza expansiva genuinamente española les ha convertido en un referente internacional en ciberseguridad, presente en sectores de Distribución, Energía, Banca y Seguros, Sanidad, Industria y Administración Pública. Entre sus objetivos para este 2023, destaca continuar creciendo y aumentando la presencia de la ciberprotección en la industria 4.0, principalmente en el ámbito de OT. De momento, ya cuenta con instalaciones en Valencia, Madrid, Sevilla, Barcelona, San Sebastián, Bruselas, Bogotá, Brindisi, Santiago de Chile, México, Róterdam y Lisboa.

José Rosell y Miguel Juan

Es de destacar asimismo que en 2022 su inversión en I+D+i fue notable alcanzando los 2,2 millones y la previsión para este año es aumentarla hasta los 2,4 millones de euros, destinados a proyectos dedicados de ciberseguridad industrial, protección frente a ataques avanzados, de dispositivos IoT, IC e IA, entre otros, para conseguir "la soberanía digital europea".

La convergencia IT-OT en el sector ferroviario acelera las inversiones en ciberseguridad

El sector del ferrocarril está dando pasos importantes en mejorar su ciberprotección con notables inversiones. En Revista SIC 153, entre otras iniciativas, se ponía en valor el primer centro de ciberseguridad especializado en este ámbito en nuestro país, puesto en marcha por **Renfe,** en Galicia. Precisamente, la firma de inteligencia tecnológica **ABI Research** ha elaborado un informe sobre las inversiones en OT e IoT en el sector ferroviario, entre 2022 y 2027, en el que se destaca que la ciberseguridad acaparará en torno al 7,65% de la inversión, rondando en todo el mundo para dentro de cuatro años más de 280 millones de euros al año. Una cifra media en concordancia con lo previsto para el sector industrial y su gasto en ciberprotección OT que oscila para ese periodo entre el 3% y el 5%. Estas cifras están siendo impulsadas por la adopción de los sistemas en línea conectados y la convergencia de los sistemas OT y TI, la seguridad de la red y el intercambio de datos entre estos al sector, así como por las nuevas normativas, como NIS2 en la UE o la Directiva de Pruebas y Acciones de Mitigación de la Ciberseguridad Ferroviaria de EE.UU., de octubre de 2022.

De cualquier forma, "confiar exclusivamente en el crecimiento promedio del gasto en ciberseguridad de OT no es suficiente para garantizar redes seguras, especialmente dado que el gasto en OT del sector fue globalmente de escasos 123 millones de dólares estadounidenses en 2022", explica el analista senior de ciberseguridad industrial de ABI Research, **Michael Amiri.** "La disparidad indica mayores riesgos de ciberseguridad de OT en el futuro si los operadores ferroviarios no aumentan los presupuestos de seguridad de las tecnologías operativas".

Symantec™

Data-Centric SASE

Westcon | Symantec by Broadcom Software

La seguridad de los datos debe ser la prioridad para tu empresa.
Solicita las soluciones de ciberseguridad de Symantec en Westcon.

Contacto:

- westconcomstor.com/es/es
- symantec.es@westcon.com
- broadcom.com

El incremento de la nube en el ámbito empresarial ha crecido un 29% en un solo año, según la compañía

NETSKOPE alcanza con éxito una nueva ronda de financiación de 370 millones y anuncia 15 centros de datos más en su red NewEdge

El trabajo híbrido y remoto se ha convertido en la nueva realidad y el uso de la nube se está acelerando. Prueba de ello es que, según el 'Netskope Threat Labs February Report Europe', publicado recientemente, la adopción de la nube por parte de las empresas ha crecido un 29% en un año. Ello supone que, en los últimos doce meses, un 92% de usuarios descargó datos regularmente desde aplicaciones en la nube al mes, frente a un 53% que cargó datos.

Precisamente, por el incremento de la demanda de la protección de este entorno, **Netskope,** uno de los referentes en la protección SASE, "vive un momento histórico", impulsado, además, por la inyección de 370 millones de euros a principios de año, en una nueva ronda de financiación, además de ser reconocida como Líder en el Cuadrante Mágico de **Gartner** para Security Service Edge (SSE) de 2022.

La compañía se ha convertido así es un referente en soluciones Intelligent Security Service Edge (SSE) y Borderless SD-WAN, "todas ellas cruciales para proporcionar el acceso optimizado y la seguridad basada en la confianza cero e impulsada por IA que se requieren en una pila tecnológica moderna de red y seguridad", explican desde la empresa. Y es que, para la compañía, "la transformación de la seguridad no tiene éxito sin la transformación de la red. Si la seguridad degrada la experiencia de la red o la experiencia de la red pasa por alto la seguridad, cada una de esas compensaciones introduce más riesgo".

Por ello, Netskope destaca, además, por contar con una red de centros de datos denominada NewEdge en la que ha invertido más de 100 millones de dólares para su creación, desde 2018, con el objetivo de que la protección no impacte en el rendimiento. Con ella, proporciona una gran cobertura a sus clientes de todo el mundo, incluida, España, donde la compañía abrió en julio de 2022 un centro de datos en Barcelona, que se une al que ya tiene en Madrid.

Chris Andrews, SVP Worldwide Sales en Netskope

"Nuestra inversión se dirige a dar un acceso remoto de confianza cero a las aplicaciones privadas y en la nube, así como en entornos híbridos"


Chris Andrews

– Netskope nació con la 'seguridad como servicio' en su ADN. ¿Cómo ha evolucionado y qué supone hoy este concepto?

– Hace alrededor de una década, poco antes de unirme a la compañía, las empresas no entendían realmente que la seguridad se podía entregar en la nube como un servicio; hoy ya no es así y quieren asegurarse de que sus datos están protegidos en dos vertientes: los que no deberían salir, que no se filtren fuera de la empresa y que las ciberamenazas no interrumpan las operaciones comerciales. Para, ello disponemos de gran variedad de controles y gestión de actividades muy sofisticados, entre otras muchas capacidades.

– Según explicó la propia compañía, los criminales usan servicios legítimos de nube para distribuir *malware*, ¿cómo responde Netskope a ello?

– El mayor desafío no es que estén usando una nube legítima, sino que el usuario no se da cuenta y continúa haciendo clic en esos enlaces. Ahí es donde entra la amenaza. En Netskope contamos con capacidades avanzadas *antimalware* y, en general, anti amenazas, muy amplias para detectarlas y evitar que proliferen, se detonen, etc.

– Han cerrado una ronda de financiación de 370 millones de euros, ¿a qué irán destinados?

– Netskope siempre ha tenido la visión de ser una empresa de seguridad en la nube conocida, respetada y segura a largo plazo. Construimos lo que creemos que es la nube de seguridad privada más grande y con mejor rendimiento y queremos brindar servicios de protección reales a clientes de todo el mundo. Ello requiere gran inversión. Ahora contamos con 65 centros de datos en todo el mundo, dos de ellos en España, y desplegaremos 15 más este año. Invertir en el producto y la capacidad de entregarlo requiere esfuerzo, por lo que lo destinaremos a tecnología y la entrega de esa tecnología a los clientes.

– ¿En qué áreas se enfocará la compañía?

– Una de ellas es ampliar la capacidad de proteger los datos de los clientes. Hay que tener en cuenta que existen muchos tipos de datos y muchas formas de entregarlos. Así que, para ello, por ejemplo, recientemente llevamos a cabo dos pequeñas adquisiciones, WootCloud, ampliando las capacidades de Zero Trust al IoT empresarial, así como la compañía Infiot. Así que, seguiremos invirtiendo en este sentido. En general, nuestro objetivo de inversión es dar un acceso remoto de confianza cero a las aplicaciones, tanto las privadas, que aún residen en los centros de datos de los clientes, como las basadas en la nube, así como entornos híbridos, y hacerlo a través de nuestra red de seguridad de alto rendimiento..

– Netskope lleva años apostando por la IA y el Aprendizaje de Máquina (AI/ML). ¿Qué rol juega en la actualidad para la compañía?

– Hemos categorizado más de 50.000 aplicaciones que usan las empresas, de las que solo unas pocas centenas están administradas por TI. En Netskope tenemos alrededor de 10 formas principales de categorizarlas y, en última instancia, definir si son muy seguras, moderadamente o nada seguras. Por ejemplo, entre otras capacidades, al usar nuestra propuesta de IA/ML, podemos ofrecer una política predeterminada para bloquear las aplicaciones con mayor riesgo, sin tener que verificarlas realmente.

– Respecto a España, ¿cuáles son sus retos?

– Europa representa alrededor del 20 al 25% de nuestro negocio y España es un mercado muy importante para nosotros. Tenemos dos centros de datos, en Madrid y Barcelona, y una base de clientes bastante buena, tanto empresas pequeñas y medianas, como compañías más grandes, como entidades bancarias, y organismos públicos. Además, contamos con importantes proveedores de servicios y socios de canal que nos ayudan y que trabajan más de cerca con los clientes más pequeños. De hecho, el mayor desafío es convertir a estos clientes más pequeños, –que son una gran parte del mercado español, y que no cuentan con profesionales altamente cualificados o un departamento de TI–, en que sean completamente operativos.

Texto: **Ana Adeva**


cisco
If it's connected,
it's protected.
La Seguridad de Cisco brinda visibilidad de amenazas
en toda su red, sin importar cuán lejos llegue.
Todo ello respaldado por uno de los equipos ciberinteligencia
más grandes y fiables del planeta.
Fuimos la primera empresa en conectar el mundo.
Y somos la mejor opción para proteger el mundo.

Se 'populariza' el software malicioso de borrado de datos y se incrementa la actividad de los grupos APT, según ESET

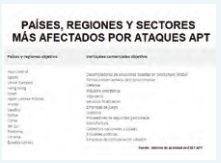
Desciende el uso de *malware*, pero crecen los ataques de *phishing* dirigidos en España

El director de Investigación y Concienciación de **Eset**, **Josep Albors,** dio a conocer en una reciente rueda de prensa los datos más relevantes del 'Informe de amenazas' de la compañía, correspondiente al tercer cuatrimestre de 2022, a nivel global. En él, destacó los "cambios de tendencia en las amenazas con respecto al año anterior", aunque lo que no ha variado mucho es la situación del ranking de España en el número de detecciones de amenazas a nivel global, ya que seguimos siendo uno de los que más registra en todo el mundo, junto con Japón, Turquía, Italia o Estados Unidos, por ejemplo. Como dato relevante, en el cómputo anual se observa un descenso en casi todas las categorías de *malware* monitorizadas, excepto en la del dirigido a dispositivos Android, lo que se traduce en un descenso total de amenazas detectadas del 13,2% a nivel global. Este dato, sin embargo, no debe llamar a engaño, ya que según Albors, también supone que los ataques cada vez son más dirigidos para optimizar el resultado.

Así, el experto hizo hincapié en el cuidado con las campañas de *phishing* dirigidas a obtener credenciales de empresas, ya que cada vez están mejor hechas y van más dirigidas. "En este sentido, tecnologías como ChatGPT o Bard pueden ayudar a los delincuentes a hacer más creíbles sus correos maliciosos, por lo que es fundamental tener mucho cuidado con este tipo de amenaza", añadió.

Actividad APT

Eset también ha publicado un informe de actividad de amenazas persistentes avanzadas (APT), que resume los descubrimientos sobre grupos seleccionados especializados en este tipo de ataque. Entre otros datos de interés, entre septiembre y finales de diciembre de 2022, destaca que los grupos APT alineados con Rusia continuaron particularmente involucrados en operaciones dirigidas a Ucrania, desplegando limpiaparabrisas destructivos y *ransomware*. El estudio también destaca que los grupos alineados con Irán continuaron operando con mucha intensidad.



En Ucrania, Eset detectó al grupo cibercriminal **Sandworm** atacando a una empresa del sector energético.

"Los actores del estado-nación o patrocinados, generalmente operan grupos APT y el ataque descrito ocurrió en octubre, durante el mismo período en que las fuerzas armadas rusas comenzaron a lanzar ataques con misiles contra la infraestructura energética", destaca la investigación. Además de un nuevo *malware* de borrado de datos, Eset descubrió ataques que usaban *ransomware* como 'limpiador'. O dicho de otra forma: bajo la conocida denominación de software malicioso, el objetivo era el borrado de datos sensibles de infraestructuras críticas.

DEFENSA pone en marcha el MANDO DEL ESPACIO, como parte del EJÉRCITO DEL AIRE para operaciones militares y la protección de sistemas ultraterrestres

La necesidad de dar protección a los sistemas ultraterrestres, críticos para la Defensa y el mundo civil con sistemas como el GPS, al igual que han hecho otros ejércitos, **Defensa** ha creado un **Mando específico para el Espacio,** integrado en la **Fuerza Aeroespacial del Ejército del Aire**. Su objetivo es centralizar la preparación de las unidades expertas en este ámbito, además de la dirección, planeamiento, organización y coordinación que permiten la vigilancia, control y operación en el espacio.

Así, según la orden publicada en el BOE sobre la reorganización del Ejército del Aire y el Espacio, el Mando "proporcionará a la estructura operativa de las Fuerzas Armadas la capacidad de libre acceso y explotación del espacio de manera segura, eficiente y coordinada", explica la orden ministerial.

Para ello, la unidad contará con sistema *ad hoc* de mando y control con las capacidades para "generar los efectos que garanticen el planeamiento y ejecución de las operaciones de las Fuerzas Armadas y la libertad de acción de la Fuerza Conjunta". En cuanto a su organigrama, el mando dispondrá de un cuartel general, con una jefatura y el Estado Mayor del Mando del Espacio.

Por otra parte, la ministra de **Defensa, Margarita Robles,** ha inaugurado la Oficina del Programa del **Centro Tecnológico de Desarrollo y Experimentación** (CETEDEX), especializado en vehículos autónomos y conectados, inteligencia artificial y sistemas de antidron, con una inversión de 220 millones de euros, que también incluirá la ciberseguridad de este tipo de sistemas.

ENTELGY INNOTEC SECURITY consigue la certificación más alta en el ENS con LEET SECURITY

Entelgy Innotec Security ha obtenido esta semana la certificación con la categoría más alta de seguridad en el Esquema Nacional de Seguridad (ENS), cuatro años después de recibir la de nivel medio. La empresa ha logrado su acreditación tras un proceso de evaluación llevado a cabo por **Leet Security** y después de superar con éxito la correspondiente auditoría. En concreto, se han certificado los sistemas de información que dan soporte a los servicios de seguridad gestionada – SmartSOC (Centro de Operaciones de Seguridad), servicios de consultoría, servicios de seguridad ofensiva y desarrollo e implementación de herramientas.

Estos servicios han sido auditados conforme a las exigencias del Real Decreto 311/2022, de 3 de mayo, por el que se regula el nuevo ENS en el ámbito de la Administración electrónica.

"Conseguir esta certificación de conformidad con el ENS, en su nivel más alto, ratifica el compromiso de Entelgy Innotec Security con el cumplimiento de los más elevados estándares de seguridad y protección de sus sistemas y de los servicios que ofrece a sus clientes", ha destacado el CEO de la compañía, **Félix Muñoz**.

ZEROLYNX

5 AÑOS VELANDO POR TU CIBERSEGURIDAD

info@zerolynx.com

www.zerolynx.com

Los responsables en España alertan de la popularización de *malware* multipropósito, más ataques a la nube y más *hacktivismo*

CHECK POINT apuesta por un enfoque 'Prevention-First' con soluciones integrales, consolidadas y colaborativas para lograr la ciberresiliencia

Check Point celebró en marzo su evento anual para clientes y socios, el **CPX360 2023**. El encuentro, de tres días, reunió a los principales expertos del sector para comentar las últimas soluciones y estrategias para hacer frente a las ciberamenazas más sofisticadas. "En pocos años, la industria ha experimentado un cambio importante y actualmente estamos en medio de la revolución de la Inteligencia Artificial (IA). Durante la última década, Check Point ha estado invirtiendo e incorporando esta tecnología en sus sistemas, con más de la mitad de nuestros motores de amenazas utilizándola para que las infraestructuras más complejas puedan permanecer protegidas", explicó **Gil Shwed,** fundador y CEO de la compañía.

Por su parte, el vicepresidente de Gestión de Productos, **Eyal Manor**, compartió las últimas novedades, como la presentación de su servicio de seguridad de extremo a extremo, Infinity Global Services.

Eusebio Nieva y Mario García

En general, durante las tres jornadas, diferentes especialistas de la empresa mostraron su enfoque de ciberseguridad asentada sobre tres pilares fundamentales: una solución de carácter integral, consolidada y colaborativa. Para la compañía, "resulta vital que las empresas cuenten con la capacidad de cubrir todos los vectores para evitar que ocurra ningún incidente, pero también alcanzar una arquitectura que mejore la coordinación y efectividad de la seguridad y se integre con sistemas de terceros para entregar los datos más precisos en tiempo real".

De forma paralela, la empresa presentó en su sede en Tel Aviv, el Check Point Cyber Center, un centro educativo de acceso gratuito que explora la historia y el futuro de la ciberseguridad.

Más ataques a la nube

Por otro lado, en España, la compañía mantuvo un encuentro con la prensa especializada de la mano de su director general, **Mario García**, y de su director técnico, **Eusebio Nieva,** quienes destacaron que, entre las tendencias de 2023 llega el *malware* multipropósito, resurge el *hacktivismo* político, con el riesgo de que la IA, tipo ChatGPT, puede usarse para ciberataques complejos. Además, según el 'Security Report 2023', de Check Point Research, durante el último año se ha podido apreciar un aumento en el interés de los ciberdelincuentes por las infraestructuras críticas, tales como la educación o la investigación, los sectores más atacados junto con el sanitario. En nuestro país, se espera ver una nueva oleada de desinformación, así como amenazas *deepfakes* y campañas de *phishing* en relación con las inminentes campañas electorales.

Frente a ello, también pusieron en valor que existe un gran abanico de soluciones para afrontar los retos más prominentes, pero actualmente se aprecia un cambio hacia el uso de herramientas y paneles de administración únicos, más fáciles de usar y que permiten disminuir la complejidad para poder centrar los esfuerzos en solventar las amenazas. No obstante, todavía existe una evidente escasez de personal cualificado y los presupuestos continúan sin ser suficientes para hacer frente al actual aumento de los ciberataques, quedando cada vez más por detrás de los ciberdelincuentes.

BITDEFENDER alerta del éxito de ataques usando vulnerabilidades conocidas y ofrece gratis un nuevo descifrador para *ransomware*

Bitdefender ha publicado una investigación sobre una nueva ola de ataques que utiliza vulnerabilidades conocidas y cadenas de *exploits* ProxyNotShell/OWASSRF para atacar implementaciones locales de Microsoft Exchange. Los expertos de Bitdefender Labs comenzaron a notar un aumento de estos ataques a finales de noviembre de 2022.

Dentro de los ataques a los servidores Microsoft Exchange, destacan los ataques de falsificación de solicitud del lado del servidor (SSRF). Se trata de un tipo de ataque que permite a un ciberdelincuente enviar una solicitud creada desde un servidor vulnerable a un servidor diferente. Esto permite al atacante acceder a recursos o información que de otro modo no serían directamente accesibles para ellos y les permite realizar acciones en nombre del servidor vulnerable. En cuanto al impacto geográfico, los objetivos del ataque se encuentran principalmente en los Estados Unidos. También, se han registrado incidentes en Polonia, Austria, Kuwait y Turquía.

Por otro lado, ha comenzado a ofrecer de forma gratuita un descifrador universal para el *ransomware* MortalKombat. Hasta el momento, la compañía ha lanzado 32 descifradores, entre los que destacan los dirigidos a *ransomwares* tan significativos como GrandCrab, Darkside o REvil.

AKAMAI presenta su 'Connected Cloud' que integra centros de *cloud computing* centrales y distribuidos con una red de escala masiva en el borde

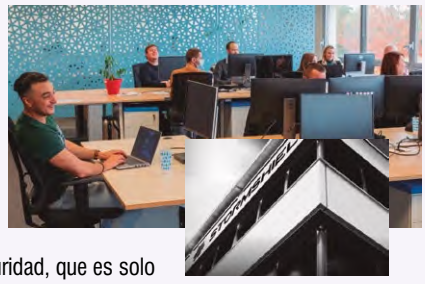
Akamai Technologies ha presentado su 'Connected Cloud', una plataforma en el *edge* y en la nube distribuida masivamente para *cloud computing,* seguridad y distribución de contenido que mantiene las aplicaciones y experiencias más cerca del usuario y aleja las amenazas. Para su creación, la multinacional añade sitios centrales y distribuidos sobre la misma red troncal subyacente que impulsa su red perimetral actual, que abarca más de 4.100 ubicaciones en 135 países.

Más concretamente, está acercando los recursos informáticos, de almacenamiento, de bases de datos y otros servicios a una amplia población, al sector y a los centros de TI. El resultado está diseñado para crear un flujo continuo de recursos informáticos, desde el núcleo hasta el *edge*, permitiendo a las empresas crear, implementar y proteger de forma más eficaz cargas de trabajo de alto rendimiento que requieren una latencia de pocos milisegundos y un alcance global.

La compañía también ha anunciado nuevos servicios estratégicos de nube para que los desarrolladores creen, ejecuten y protejan cargas de trabajo de alto rendimiento más cerca de los lugares de conexión a internet de empresas y usuarios. Así, la empresa pondrá en marcha tres nuevos centros *core* de *cloud computing* para el ámbito corporativo en EE.UU. y Europa, que se conectarán a la red troncal de la empresa.


HORNETSECURITY
Las nuevas amenazas demandan
SOLUCIONES DE SEGURIDAD
DE ÚLTIMA GENERACIÓN
BACKUP
COMPLIANCE
EMAIL SECURITY
SECURITY AWARENESS
MEJORAMOS NUESTRA SUITE DE SEGURIDAD PARA MICROSOFT 365
CON NUEVAS TECNOLOGÍAS
QR CODE ANALYZER
SECURE LINKS
ESI® BENCHMARKING
SPEAR PHISHING SIMULATION
CONTINUOUS AWARENESS TRAINING
¡PROTÉGETE!
WWW.HORNETSECURITY.COM

STORMSHIELD continúa su crecimiento en Europa apostando ya por la innovación en criptografía postcuántica para proteger sistemas críticos



Desde que comenzara en 2014, fruto de la fusión de dos empresas francesas de ciberseguridad -aunque contaba con la experiencia previa de la compañía **Netasq** que creó el primer cortafuegos con un IPS integrado en 1998-, la multinacional europea, propiedad de **Airbus,** no ha dejado de crecer fruto de la innovación y de su apuesta por garantizar la 'ciberserenidad' a las organizaciones que operan infraestructura crítica y operativa. "Esta misión no se limita a diseñar proyectos de ciberseguridad, que es solo un medio y no un fin. La expansión de la tecnología digital, la proliferación de ciberamenazas a nivel mundial y las cada vez más preocupantes consecuencias de los ciberincidentes nos han llevado a redefinir nuestro propósito. No solo brindamos protección para recursos y datos de TI. A través de nuestras actividades, ayudamos a fortalecer la estabilidad social, ambiental y económica", destacan desde la compañía.

Así, su enfoque iniciado en 2018 de centrarse en negocios que operan infraestructura crítica, con el lanzamiento del primer cortafuegos industrial (SNi40), se ha plasmado en una gran madurez con las tecnologías OT que la ha permitido aportar un valor diferencial en este mercado. "El soporte único para protocolos industriales estandarizados o propietarios, además de nuestra capacidad para llevar a cabo análisis en profundidad de dichos protocolos, son claves", recuerdan sus responsables.

Entre sus recientes novedades, destacan el diseño y construcción de sistemas integrados para garantizar el cifrado de extremo a extremo de un helicóptero y la estación base, abriendo "la puerta a nuevas soluciones y valor añadido para el sector del transporte". A ello, se suma que ya está trabajando en la próxima tecnología disruptiva que desde la compañía creen que podría llegar en los próximos cinco años, la criptografía postcuántica, y acuerdos con empresas estratégicas, como el firmado recientemente con la empresa **Seela.**

Eric Hohbauer, director general adjunto y vicepresidente senior de ventas y marketing de Airbus Cybersecurity/Stormshield

"Nuestro ADN europeo y nuestra longevidad nos han convertido en el proveedor líder de *firewalls* en Francia y Europa"

– En un mundo con tantas tensiones geopolíticas, ¿qué valor estratégico en ciberseguridad aporta una compañía europea como Stormshield?

– Elegir soluciones soberanas garantiza la transparencia y evita riesgos de que los datos puedan ser explotados con fines maliciosos por parte de organismos extranjeros. Este enfoque es de vital importancia para evitar riesgo de interferencia o espionaje industrial. Mantener la independencia digital es la única forma de permitir una respuesta local y autónoma con respecto a los problemas de producción y las actividades críticas al resolver ciberincidentes. Las soluciones europeas pueden ofrecer esta respuesta local en términos de soporte técnico rápido, asistencia a equipos locales, procesos de respuesta a incidentes, etc. Y, por último, la elección de soluciones soberanas también garantiza el cumplimiento nativo de normas y estándares vigentes. No quiero decir que los clientes deban usar solo tecnologías europeas, pues no tenemos todas las necesarias aquí. En este caso, lo recomendable será utilizar una doble barrera tecnológica.

– Ha participado en un panel de un reciente evento, organizado por Airbus SLC (*Secure Land Communications*), sobre comunicaciones de misión crítica, ¿cuáles fueron sus tres aspectos más destacables?

– El propósito de esta mesa fue explicar que el paso a la banda ancha y las arquitecturas abiertas crean riesgos de seguridad cibernética cada vez mayores, y cuáles fueron los principales desafíos para asegurar estas infraestructuras. Todas estas aperturas crean un sinfín de nuevas oportunidades, pero al mismo tiempo traen consigo peligros.

Eric Hohbauer, Stormshield

En primer lugar, en los sistemas de misión crítica, las consideraciones son técnicas, pero lo que está en juego es humano. En segundo lugar, hay un tema de habilidades, con pocos expertos para una cuestión que afecta a todos. Por lo tanto, los departamentos de TI deben asegurarse de que los especialistas externos que los acompañan tengan la experiencia necesaria y sean de plena confianza. Por último, desde un punto de vista tecnológico, existe un dilema entre los sistemas heredados, desarrollados para redes aisladas, y la seguridad TI desarrollada para abrir las infraestructuras de red a otros ecosistemas garantizando la seguridad. Stormshield, para reforzar la protección de la nueva tecnología de banda ancha y del mundo de las telecomunicaciones menos tolerante a la latencia, ha adaptado su arquitectura de software para priorizar la continuidad del negocio y la misión, la seguridad física y la alta disponibilidad. Y confiamos en soluciones sólidas y de alto rendimiento, en lugar de desarrollar funciones o integrar componentes no esenciales que podrían crear riesgos de seguridad adicionales.

– También, aprovecharon dichas jornadas para mostrar los desarrollos de Airbus en proyectos de redes Tetra como el de BOSnet en Alemania…

– En caso de ataques, desastres naturales, accidentes o intervenciones policiales, la infraestructura de comunicación crítica para las fuerzas de emergencia debe estar operativa en todo momento. Por motivos de seguridad y para que este servicio no sea interrumpido por organizaciones malintencionadas, es fundamental que todas las comunicaciones estén cifradas. La ciberseguridad juega un papel clave y garantiza que los riesgos asociados a estos grandes proyectos de infraestructuras se reduzcan significativamente, con la seguridad ciudadana en el centro de su actividad.

– ¿Cuáles serán las grandes novedades de Stormshield para 2023, tanto en Europa como en España?

– El ADN europeo y la longevidad de Stormshield lo han convertido en el proveedor líder de *firewalls* en Francia y Europa. Un posicionamiento justificado por la calidad de las soluciones que ofrece y por el apoyo cercano que bridamos a los clientes, a través de una red de más de 1.200 distribuidores, integradores y revendedores.

En aras de mejorar aún más nuestra relación diaria con los clientes con problemas críticos de ciberseguridad y elevar su perfil, planeamos seguir aumentando nuestra presencia en Alemania, Polonia, España e Italia, y también estudiar nuevas oportunidades de desarrollo en los países nórdicos y el Benelux, donde la presencia de Stormshield puede satisfacer la demanda de soluciones europeas alternativas.

Texto: **José Manuel Vera**

adVens

Security for the greater good

Your new partner to face cyber threats

mySOC

SOC-as-a-Service & MDR

CISO Office

360° Cyber shared services

myCERT

Incident response, crisis management and CTI

Risk & Strategy

Cyber compliance

Offensive security

Security technology

Cloud security

Operational security

advens.com
contacto@advens.com

Madrid
Paseo de la Castellana, 163, Planta 1. 28046

Barcelona
Avinguda del Portal de l'Àngel, 40, 08002

Según Logicalis, el 81% dedican más tiempo a la innovación y casi la mitad asegura que ésta marca el grado de desempeño de su trabajo

Más de la mitad de los CIO están aumentando el gasto en gestión de riesgos en términos porcentuales y planean hacer crecer sus equipos de gestión este año

El 77% de los CIO, de ámbito global, espera aumentar el gasto en servicios gestionados y de TI subcontratados en el próximo año. Según el nuevo informe de la compañía **Logicalis,** la tendencia es que el CIO evolucione hacia un perfil más estratégico. Algo que se ha acelerado en los últimos meses. Precisamente, el estudio identifica cuatro áreas críticas de enfoque para los CIO: la de innovación, la estratégica, la de transformación digital y, también, la que permite reimaginar las asociaciones de servicios. De hecho, el 57% de los preguntados reconoció que crear y operar nuevos servicios digitales es su principal responsabilidad este año.

El informe también destaca que los CIO recurren cada vez más a los proveedores de servicios administrados para ofrecer capacidades rentables que ofrezcan innovación, eficiencia y acceso a las habilidades que tanto necesitan. Así, mientras que el 61%, en 2018, se midieron por la cantidad de dinero que podrían ahorrar, casi la mitad (46%) de los CIO actuales se

miden por su capacidad para ofrecer nuevos servicios innovadores. Sin embargo, en esta línea, como aseguran desde la compañía, "las expectativas de los CIO nunca han sido más altas, pero los presupuestos son escasos". "Muchos CIO se enfrentan a restricciones presupuestarias que hacen que sea esencial hacer más con menos", ha comentado el director territorial de Logicalis, **Pablo Carrillo,** que recuerda que frente a esto, los CIO están apostando por "el desarrollo de estrategias que impulsan el crecimiento, mejoran la eficiencia y brindan la innovación que demandan cada vez más los clientes, empleados y socios"

Más protección cibernética

Además, en lo que atañe a ciberseguridad, es notable que gran parte están apostando por contar con una estrategia sólida en ciberprotección y riesgo para desarrollar una resiliencia que permita a este rol profesional centrar su atención en impulsar la innovación continua y la mejora del servicio. Unas responsabilidades importantes por cuanto el 41% de los participantes destacaron tener algún nivel de responsabilidad de la estrategia comercial, mientras que el 81% aseguró que dedica más tiempo a la innovación. Este hallazgo refleja que el 81% de los CIO están liderando iniciativas más allá de la gestión tradicional de TI.

Además, alrededor de la mitad (52%) están aumentando el gasto en gestión de riesgos en términos porcentuales y planean hacer crecer sus equipos de gestión de riesgos este año. Y es que, un 48% creen que el *malware* y el *ransomware* presentarán un riesgo significativo para su organización en el próximo año, entre otras amenazas.

Las vulnerabilidades en el ámbito OT crecen casi un 70% en sólo tres años y más de un 20% aún no tiene parches disponibles

Las vulnerabilidades no detectadas o no parcheadas con suficiente celeridad como parar evitar que los cibercriminales se aprovechen de ellas continúan siendo un quebradero de cabeza para los responsables de ciberseguridad. De hecho, éstas han crecido en sistemas de control industrial (ICS) casi un 70% en solo tres años, basándose en las alertas de la **Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU.** (CISA) y, según datos de **SynSaber,** más de una quinta parte (21%) aún no ha sido reparada por los fabricantes.

En un informe de la compañía, sus investigadores analizaron los avisos publicados por CISA, entre el 1 de enero de 2020 y el 31 de diciembre de 2022 para comprender qué grado de exposición presentan a este tipo de problemas las plantas industriales. "El aumento de CVE no es algo malo *per se*, ya que podría indicar que los equipos de seguridad de productos están aumentando sus informes internos y la divulgación pública de vulnerabilidades a la comunidad", explican los responsables del documento de SynSaber, que también añaden que lo grave es la "falta de parches de proveedores, que sí agrava el riesgo cibernético para los propietarios de activos industriales en sectores de infraestructura crítica, como el transporte y los servicios públicos". Es más, el documento destaca que, incluso, cuando sí están disponibles no siempre son fácil de aplicar por los requisitos relacionados con el tiempo de actividad del sistema y las preocupaciones sobre la compatibilidad del software heredado.

El NCSC del Reino Unido lanza recomendaciones sobre el 'mapeo' de la cadena de suministro

El **Centro Nacional de Ciberseguridad del Reino Unido (NCSC)** presentó a principios de año una lista de recomendaciones para ayudar a las medianas y grandes empresas a 'mapear' las dependencias de su cadena de suministro para anticipar mejor los riesgos cibernéticos provenientes de sus contratistas y subcontratistas. Con esta iniciativa, el organismo espera que se comprenda mejor quiénes son los proveedores, qué proporcionan y cómo. Se intenta dar un primer paso para ayudar a terceros a repetir sus prácticas de seguridad y aplicar nuevas políticas de protección a través de contratos.

También, respaldará el cumplimiento de la seguridad y permitirá a las organizaciones mitigar el riesgo de un ciberataque o una infracción.

Entre las prácticas que incluye el listado están desde contar con un inventario completo de proveedores y sus subcontratistas, que muestre cómo están conectados entre sí, además de dejar constancia qué producto o servicio se proporciona, por quién y la importancia de ese activo para su organización, qué información fluye entre la empresa y su proveedor, así como el contacto de la aseguradora de la póliza cibernética para activarla en caso de crisis, acorde a sus coberturas, y su fecha de vencimiento. Además, de entre todas las recomendaciones, se determinan algunas como "un conjunto de alto nivel como primer paso para las empresas que realizan el SCM (mapeo de la cadena de suministro) por primera vez.

Es muy difícil recuperar la reputación perdida.

No deje que la falta de ciberseguridad acabe con el prestigio de su organización.

Es muy difícil hacerse con una buena reputación, así que una vez conseguida, **es muy importante saber conservarla para siempre con ciberseguridad.**

Si necesita más información, póngase en contacto con nosotros en: **902 882 992** y **clientes@s2grupo.es**.

Síguenos en: • @s2grupo • s2grupo.es

S2 GRUPO

Anticipando un mundo **ciberseguro**

Para los especialistas en ciberprotección lo más complicado de hablar es el incremento de presupuesto y cómo mejorar la concienciación, según Kaspersky

Un estudio muestra que casi la mitad de la alta dirección en España considera que los profesionales del sector deberían comunicar mejor los riesgos

Un reciente estudio de la compañía **Kaspersky** alerta de que uno de cada tres ejecutivos de alto nivel tiene dificultades para hablar de la adopción de nuevas soluciones de seguridad con sus compañeros de TI.

Con la participación de más de 2.300 profesionales de empresas globales, con representación en 25 países, entre los datos que competen al sector español, el informe destaca que casi la mitad de la alta dirección (43%) considera que los profesionales de seguridad TI deben comunicar mejor los riesgos para la empresa. Por su parte, el 7% de los dedicados a ciberseguridad admiten dificultades para explicar su trabajo a compañeros de fuera del departamento y altos ejecutivos.

En cuanto a los temas más complicados para debatir para los ejecutivos de la alta dirección, destacan la evaluación del desempeño del equipo de seguridad TI (31%), los cambios en dicho equipo (30%) y la adopción de nuevas soluciones de protección (28%).

Por su parte, para los trabajadores de TI españoles lo más complicado cuando se sientan con directivos de fuera del departamento, es negociar el aumento del presupuesto en ciberseguridad (48%), contratar más profesionales para el equipo (35%) e incrementar la inversión en planes de concienciación en este ámbito para los diferentes roles profesionales de la plantilla (30%).

También, es reseñable que la mayoría de los encuestados está de acuerdo en que la manera más eficaz de simplificar los debates sobre seguridad TI es elegir ejemplos de la vida real y utilizar informes y cifras.

Amenazas en entornos OT

Kaspersky también ha publicado los datos de su informe 'ICS threat landscape report', en el que destaca que España es el cuarto país europeo con más ciberataques al sector industrial. También alerta de que más del 40% de los sistemas de OT se vieron afectados por *software* malicioso durante el año pasado. En especial destacaron los ataques contra el sector energético y la automoción, que crecieron hasta el 36,9% y el 34,5%.

Respecto a los pronósticos para 2023, el CERT ICS de la compañía vaticina un cambio en las APT contra las organizaciones y dispositivos inteligentes en nuevos sectores industriales y localizaciones, especialmente el agrario, logístico, transporte, energía, alta tecnología, farmacia y fabricantes de equipos médicos, donde alertan de acciones más dirigidas.

El despliegue de redes 5G *standalone* se acelera en todo el mundo, según F5, que también alerta de riesgos de ciberseguridad

La industria de telecomunicaciones móviles está comenzando a tomarse en serio la implantación de redes 5G *standalone*, marcando el comienzo de una nueva etapa para las empresas de este sector y sus clientes. Casi dos tercios (64%) de los operadores móviles esperan que las redes *core* 5G generen beneficios en la experiencia de cliente en los próximos tres años, según un informe realizado por **Heavy Reading** para **F5**. De hecho, la mitad de los encuestados afirman que las funciones *core* 5G nativas *cloud* ya están listas para operar a gran escala, mientras que para un 28% están 'casi listas'. Además, un 65% ve valor en el *network slicing* para servicios empresariales. Un núcleo nativo *cloud* permitirá a los operadores asignar dinámicamente los recursos apropiados a clientes individuales y casos de uso. Eso sí, el estudio alerta de problemas que pueden surgir en este nuevo entorno, especialmente, relacionados con brechas funcionales en el escalado de **Kubernetes,** debido a los protocolos específicos de la industria utilizados por los operadores de telecomunicaciones, por lo que se recomienda "proteger los nuevos clústeres de Kubernetes fuera de la seguridad heredada".

Por otro lado, en el ámbito del 5G, ha destacado que Alemania, según **Reuters,** ha avanzado que prevé limitar el acceso de los operadores de telecomunicaciones germanos a la tecnología de fabricantes chinos como **Huawei** y **ZTE,** un aspecto sobre el que España aún no se ha pronunciado.

El 80% de los ciberataques del último año se aprovecharon de identidades comprometidas y el 71% no incluía *malware*, según CROWDSTRIKE

CrowdStrike ha dado a conocer los resultados de la novena edición de su 'Informe Global de Amenazas 2023', en el que ha analizado más de 200 grupos maliciosos, 33 de ellos nuevos este año. Entre sus conclusiones señala que 2022 fue un año muy destacado por el incremento de amenazas, basadas en ataques contra las identidades, en *exploits* contra la nube, así como con acciones con origen en China y del aprovechamiento de muchos grupos de vulnerabilidades que se creían resueltas, como Log4Shell.

Es especialmente llamativo que el 71% de los ataques detectados no se incluía *malware* (frente al 62% de 2021), mientras que las intrusiones interactivas (es decir, procedentes de un humano al otro lado del teclado) crecieron un 50%, lo que implica que los ciberdelincuentes tienen cada vez mayores conocimientos para evadir la protección de los antivirus y las defensas automatizadas. Además, los ataques a la nube crecieron un 95%, aunque el número de actores responsable de ellos se ha triplicado. Además, el tiempo que tarda un ciberdelincuente en acceder a un sistema se ha reducido: de 98 minutos en 2021 a 84. También, es significativo que el 80% de los ataques detectados se aprovecharon de identidades comprometidas.

Acuerdos estratégicos

Por otro lado, CrowdStrike ha firmado una alianza con **Claroty** para aumentar la visibilidad y reducir los riesgos en entornos industriales. Además, **Dell** ha ampliado su cartera de gestión de amenazas con un acuerdo con la compañía estadounidense de ciberseguridad incorporando a su SafeGuard and Response la plataforma CrowdStrike Falcon.

CIBERSEGURIDAD

En AENOR, sabemos que cuando un empleado hace clic, una empresa puede hacer crack

Cada día, millones de empleados y usuarios navegan por internet o descargan información sin pensar en lo que eso supone para la seguridad de su empresa. En AENOR, hemos trabajado en un **nuevo ecosistema digital** donde respondemos a las nuevas **necesidades de ciberseguridad y privacidad,** reduciendo el riesgo de que el clic de un trabajador provoque el crack de la compañía.

Todas las respuestas que buscas están en aenorciberseguridad.com

AENOR

Confía

WISE y ONE IDENTITY apuestan por una nueva generación de tecnología de identidad y control de accesos con *blockchain*

Los sistemas tradiciones de identidad y accesos autenticados cuentan con numerosos desafíos que se acentúan con el paso de los años y el incremento de ciberataques. La respuesta para resolver estos problemas consiste en alterar los enfoques tradicionales y centralizados de la gestión de datos de identidad, aplicando a los accesos nuevas tecnologías como la Web 3.0. Así, **Wise Security Global** y **One Identity** han sumado fuerzas integrando sus soluciones, Wise DID Authenticator y OneLogin, para obtener un sistema de identidad y accesos autenticados (IAM) con tecnología *blockchain* que aspira a ser una referencia.

Con esta unión se crea, según sus impulsores, "la primera solución IAM 3.0, que viene a dar respuesta a los innumerables problemas que los sistemas tradicionales de Identidad y control de accesos presentan en la actualidad, con procesos inseguros y experiencias de usuario frustrantes".

La integración entre OneLogin y Wise DID Authenticator consiste en una nueva generación de tecnologías IAM para la identificación y gestión de accesos sin contraseñas (*passwordless*) mediante un sistema de identidad descentralizada (DID) en *blockchain*. "El resultado es una solución de autenticación de usuarios confiable, sin contraseñas, sencilla de usar, fácilmente integrable y con criptografía *blockchain* lo que le confiere mayor seguridad e inquebrantabilidad", explica el Director de Digital Identity de Wise Security Global, **Óscar Flor.**

En definitiva, la integración de Wise DID Authenticator y OneLogin aporta las ventajas de la identidad digital descentralizada de Wise Security Global con el sistema Single Sign On provisto por One Identity para gestionar los accesos, tanto digitales como físicos, otorgando distintos niveles de privilegio a las personas involucradas.

INNOVATE-MNEMO, sella una alianza con HUAWEI CLOUD para reforzar su oferta de servicios especializados

Innovate, la compañía del grupo **Mnemo** especializada en ciberseguridad *cloud,* ha sellado una alianza estratégica con **Huawei Cloud**, la división de la multinacional china que ofrece servicios hiperescalares de nube pública sobre infraestructura propia. A través de esta alianza, Innovate ofrecerá servicios especializados y diferenciales de ciberprotección sobre las infraestructuras nativas de la plataforma de computación proporcionada por Huawei.

Además, mediante este acuerdo, se convierte en HCMSP (Huawei Cloud Managed Service Provider) y HCSP (Huawei Cloud Solution Provider) en el área de Ciberseguridad.

"Innovate, en su continua estrategia de ofrecer las mejores soluciones de ciberseguridad en la nube, se posiciona así como el primer *partner* de referencia en España certificado por Huawei en soluciones y servicios de ciberseguridad, sobre su plataforma *cloud*", destacan desde la empresa a la vez que recuerdan que es un hito que forma parte de su estrategia para "ser un proveedor de servicios de referencia para ayudar y acompañar a sus clientes en el diseño, migración y protección de sus entornos de nube".

"Innovate tiene una estrategia de servicios de seguridad para la nube y desde la nube apoyada en un número reducido de *partners* y ha realizado una apuesta estratégica por Huawei Cloud, sobre la que ofrecer soluciones específicas y avanzadas en el ámbito de la ciberseguridad", señala su CEO, **David Pérez Lázaro.**

NOMBRAMIENTOS

BBVA ha ascendido a **Roberto Ortiz** a CISO Global Software Development y a **Alberto Rey** a CISO Global Infrastructure & IT Operations. Además, ha reconocido la buena labor de **Alejandro Figueroa** nombrándole Head of Financial Crime en BBVA España, y ha designado a **Gustavo Rodríguez de la Fuente** Global Head of Security Architecture. Ortiz ha desarrollado gran parte de su trayectoria en la entidad, en la que comenzó como analista de ciberseguridad. Es ingeniero en Seguridad de la Información por la Rey Juan Carlos. Rey, desde 2020 ejercía como Head of Global Corporate Security Operations y, con anterioridad, desempeñó roles de responsabilidad en Emitares Group, Tata Consultancy Services, Novartis y Roche, entre otras. Figueroa también ha desempeñado gran parte de su labor en la entidad financiera, además de haber trabajado para Transbank y Deloitte. Es ingeniero en Información y Control de Gestión, por la Universidad de Chile. Rodríguez, ingeniero de Telecomunicaciones por la Universidad de Valladolid y MBA por la Politécnica de Madrid, ha aportado su experiencia en PwC, Azertia, Mapfre y Axa.

Banco Sabadell ha reconocido el solvente trabajo de **Adolfo Hernández** promocionándole a CISO en SABIS, la filial responsable de proporcionar servicios de tecnología, aplicaciones e infraestructuras al Grupo. Con una amplia experiencia, es subdirector y cofundador del Think Tank Thiber y ha trabajado para Telefónica, Ecix Group, Ecija, WISeKey ELA y GMV-SGI. Es ingeniero informático por la Autónoma de Madrid.

PepsiCo ha promocionado a **Santi Minguito** como International BISO (Business Information Security Officer) Senior Director para las regiones de Amesa, Apac, Europa y Latinoamérica. Ha desarrollado gran parte de su carrera en Banco Sabadell, además de ocupar puestos de responsabilidad en Deloitte.

Palladium Hotel Group ha elegido a **Ángel Guerra** como Corporate Information Security Manager. Especializado en ciberseguridad y riesgos tecnológicos, ha desempeñado con anterioridad roles de responsabilidad en Mnemo, RSI, Grupo SIA y Accenture, entre otras.

Logalty ha confiado a **Oscar Conesa** el cargo de CISO. Procedente de la recientemente adquirida Firmaprofesional –donde era CTO–, cuenta con más de 20 años de trayectoria en el sector. Anteriormente, trabajó para T-Systems, esCERT-UPC y Feste Foundation. Es ingeniero en Telecomunicaciones por la Politécnica de Cataluña.

OneseQ by alhambra

Si te pillan...

...que sea con los deberes hechos.
Gestiona Ciberincidentes antes de que ocurran.

Alerta Temprana

Respuesta

Monitorización Activa

Conoce los datos de eventos, amenazas y riesgos para dar respuesta y gestionar los incidentes de forma sencilla.

Detección de Intrusión

Detecta actividades inapropiadas, incorrectas o anómalas desde el exterior/interior de tu sistema informático.

Respuesta ante Incidentes

Responde de forma efectiva y decisiva ante un incidente de seguridad, independientemente de la superficie de impacto. Genera el entorno de contención del impacto para su recuperación.

Equipo de Respuesta ante Incidentes

Cuenta con la colaboración de equipos de trabajo multidisciplinares 24x7 para poder mitigar y recuperar los sistemas de información tras un impacto.

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD | Red Nacional de SOC | FIRST | ACCREDITED BY TI TRUSTED INTRODUCER | CSIRT.es

OneseQ.es | SERVICIOS GESTIONADOS **SOC 24X7**

AYESA presenta su propuesta para 'blindar' las centrales eléctricas e IBERMÁTICA suma fuerzas con VALIDATED ID

Ayesa ha presentado una plataforma de ciberseguridad para centrales eléctricas en el marco de un macroproyecto de innovación H2020, denominado **SDN-microsense**, que permite operar de forma inteligente y segura este tipo de activos. Para ello, la firma ha incorporado a su tecnología Gridpilot un sistema de gestión de vulnerabilidades de cada uno de los elementos de la red. Entre sus grandes aportaciones destaca que, tras la identificación de un ciberataque, el sistema genera automáticamente rutas alternativas para el viaje de la información, aislando los nodos de la red que están siendo afectados por el ataque. Es lo que se denomina *isolating* y *re-routing.* Como se sabe, Gridpilot es una plataforma tecnológica en la nube para la gestión inteligente de activos energéticos, que permite agregar la energía de diferentes fuentes como baterías o placas fotovoltaicas instaladas en entornos residenciales, comerciales o industriales, y gestionar su consumo, venta a la red y almacenamiento con inteligencia artificial. Se trata del resultado de un proyecto europeo con una inversión de 10,1 millones de euros y en el que han colaborado más de 30 organizaciones europeas.

Ibermática y Validated ID

Por otro lado, **Ibermática an Ayesa company** ha incorporado una nueva mejora en la seguridad de su generador inteligente de documentos, iberDok, integrando el servicio de firma digital VIDsigner de **Validated ID.** La unión de ambas soluciones permite a los usuarios firmar y validar documentación electrónicamente de forma presencial y a distancia. Está indicada para firmar una amplia gama de documentos, incluidos contratos, acuerdos comerciales o documentación legal, y tiene capacidad de emplear técnicas avanzadas como la biometría y criptografía para garantizar la autenticidad de las firmas electrónicas y del documento resultante.

UNISYS, primera empresa en obtener la certificación con el ENS actualizado a 2022

Unisys ha renovado su calificación de ciberseguridad con **Leet Security** siendo la primera en hacerlo con el ENS actualizado en 2022, con el RD 311/2022. En concreto, con 'Categoría Media'.

Este certificado, obtenido por Unisys para los sistemas de información de la compañía que dan soporte a los servicios prestados a clientes en desarrollo y mantenimiento de aplicaciones, y en administración y gestión, le sirve para dar confianza de su grado de seguridad al operar en el sector público y para continuar mejorando sus capacidades de ciberprotección.

Para lograrlo, la empresa ha superado una completa y rigurosa auditoría realizada por Leet Security, una de las primeras empresas en conseguir la ampliación de la acreditación de **Enac (Entidad Nacional de Acreditación)** como entidad certificadora del ENS. Con el mismo proceso de auditoría, la compañía ha obtenido también una calificación de ciberseguridad de Leet Security.

Esta certificación conjunta ENS y Leet Security le sirve a la empresa para acreditar su ciberseguridad tanto en el sector público, como en el privado. Este proceso que ahorra costes, recursos y tiempo es posible gracias al marco referencial desarrollado por Leet Security a partir de numerosas normativas nacionales e internacionales, siendo el ENS una de las regulaciones que se han recogido y mapeado (además de muchas otras, como ISO27001, PCI-DSS, NIST, etc..), lo que permite establecer una "relación de correspondencia" entre los controles y medidas de seguridad contenidos en ambos modelos y de esta forma poder verificar su cumplimiento para ambos de forma conjunta.

NOMBRAMIENTOS

Penguin Random House ha elegido a **Joan Agusti Martinez Carbonell** como Head of IT Security. Graduado en Informática de Sistemas por la Oberta de Catalunya, ha trabajado para el Consorci de Serveis Universitaris de Catalunya (CSUC), Seat y es profesor de La Salle BCN.

Clara Otin ha sido contratada por **Adidas** como Manager Information Security Governance. Entre otras responsabilidades, con anterioridad fue gestora de riesgos tecnológicos en Ibercaja y trabajó para Ecix Group e Hiberus Legal TIC.

Siemens ha fichado a **Santiago Moral García** como Head Cyber Defense Operations para Iberia. Graduado en Seguridad de la Información por la Rey Juan Carlos, de la que también ha sido profesor, cuenta con una amplia experiencia en organizaciones como PwC y Santander Global T&O, donde llegó a ser CISO IT Delivery.

Bankinter ha promocionado a **Trina de Miguel** a Directora de Riesgos Tecnológicos y a **Juan Carlos Muñoz** a Gerente de Seguridad Digital / Continuidad y Respuesta ante incidentes. De Miguel, que supera los 20 años de experiencia, ha sido la primera mujer que ocupa este cargo en la entidad, en la que lleva más de dos décadas. Es física por la Autónoma de Madrid, cuenta con un Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC y es Premio SIC. Por su parte, Muñoz, en la entidad desde 2016, donde comenzó en Riesgos Tecnológicos, ha trabajado para SIA y Decathlon Internacional. Es Graduado en ADE por la Rey Juan Carlos.

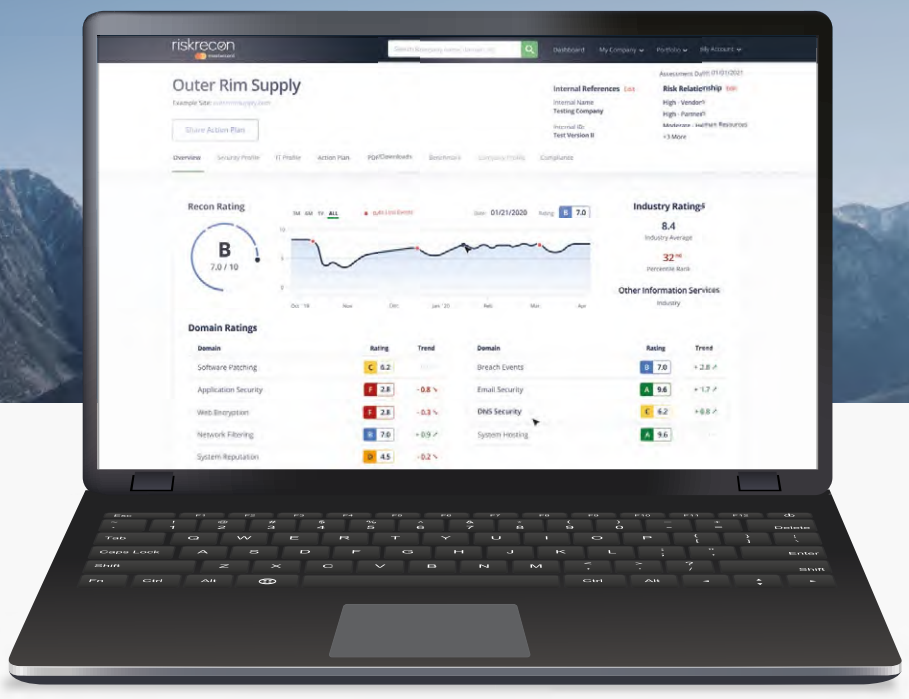
Holcim ha contratado para su Centro Digital de EMEA a dos solventes profesionales: **Antonio Delgado**, en calidad de Global IT Security Officer, y **Aitor Azpiroz** como IT Security Officer. Delgado, con más de 10 años de experiencia y relevante soltura divulgadora, ha trabajado con anterioridad en Capgemini, EY y Deloitte, entre otras. Es graduado en Ciencias de la Información por la Pontificia de Salamanca y cuenta con varios másteres. Por su parte, Azpiroz es un reconocido profesional en forensía digital y respuesta a incidentes, habiendo trabajado en empresas como One eSecurity, Insectra y Fundación Bit, entre otras.

Proteja su cadena de suministro digital

Identifique y detenga las amenazas provenientes de la red de su proveedor

RiskRecon, una empresa de Mastercard, le ayuda a mejorar la gestión de riesgos de su empresa y su cadena de suministro. Los Ratings y evaluaciones de ciberseguridad de RiskRecon le facilitan comprender y actuar sobre sus riesgos, proporcionando planes de acción precisos y con prioridad de riesgo ajustados a su medida para que coincidan con sus prioridades de riesgo.

Obtenga una prueba gratuita de 30 días de RiskRecon en www.riskrecon.com/know-your-portfolio-sic.



riskrecon
mastercard

EY pone en marcha, junto con referentes en este ámbito, su 'Quantum Resistant Network' para mitigar el riesgo de la ciberseguridad cuántica

Para mitigar el riesgo de los ataques Harvest Now Decrypt Later (HNDL), en los que agentes maliciosos recopilan datos hoy para descifrarlos más tarde con un ordenador cuántico, las organizaciones públicas y privadas están actualizando su enfoque sobre ciberseguridad. En este ámbito, la consultora **EY** ha creado, con la colaboración de **Hades,** 'Quantum Resistant Network'.

Un claro ejemplo de ello es la publicación por parte de la **Casa Blanca** de un Memorándum de Seguridad Nacional, que ordena a las agencias federales de los EE.UU. que comiencen a actualizarse para ser seguras desde el punto de vista cuántico. Otro paso importante para las empresas con relación a la criptografía post cuántica es conocer los avances realizados en el entorno normativo.

Así, este prototipo incluye varios elementos desarrollados junto con varias empresas punteras en cada uno de sus ámbitos como, por ejemplo, la capacidad de generación cuántica de números aleatorios (QRNG), junto con **Quside**; disponer de una VPN postcuántica, con **Post-Quantum**; o las denominadas Quantum Resistant y Quantum Safe, en colaboración con **Ares.** Además, permite la gestión de claves *post-quantum*, tras su trabajo con **QuintessenceLabs.** Esta propuesta ha sido impulsada por el responsable global de Innovación de EY, **Jeff Wong,** y el responsable global de Ciberseguridad de EY, **Richard Watson,** dirigido por **José María Lucía Moreno**, socio responsable de Quantum Resistant y del EY wavespace Madrid.

PROOFPOINT crea un nuevo programa de *partners* simplificado para acelerar el crecimiento del canal y facilitar su trabajo

Proofpoint ha puesto en marcha un nuevo programa para *partners* con el objetivo de fortalecer al canal para impulsar las ventas, mejorar las relaciones con los clientes y reforzar las fuentes de ingresos adicionales. Proofpoint Element Partner Program elimina la complejidad asociada a menudo con muchos programas de *partners* actuales, lo que permite a miles de proveedores de servicios gestionados (MSP), proveedores de servicios de seguridad gestionados (MSSP), distribuidores y *resellers* de valor añadido (VAR) de Proofpoint sacar partido al creciente portafolio de plataformas de ciberseguridad y cumplimiento por parte de la empresa para desarrollar su negocio y potenciar sus ingresos. Así, Proofpoint Element presenta una estructura simplificada con dos niveles, 'Core' y 'Elite', acompañados de unos beneficios bien definidos y mejorados. Con un camino marcado hacia el estatus 'Elite', todos los *partners* del su ecosistema de canal podrán diferenciar sus servicios para satisfacer las necesidades del mercado.

proofpoint. | Element Partner Program

Este programa renovado también busca proporcionar al canal las herramientas indispensables para hacer crecer sus relaciones con los clientes, al mismo tiempo que incrementa su rentabilidad, mediante amplios recursos de habilitación de ventas, formación práctica, desarrollo de marketing y soporte técnico, entre los que se incluyen desde el nivel 'Core', que supone que todos los *partners* de canal –MSP, MSSP o VAR–, comienzan por este estatus y que necesitan unos requisitos mínimos para su mantenimiento, hasta el 'Elite', que requiere cumplir con los objetivos de ingresos más exigentes, invertir en ventas y formación técnica, además de promover activamente las soluciones de Proofpoint. A cambio, recibirán importantes descuentos en el registro de acuerdos, tendrán a un Channel Account Manager dedicado, así como prioridad en la asignación de fondos disponibles para marketing, entre otras ventajas.

NOMBRAMIENTOS

● El **Ministerio del Interior** ha nombrado como jefe de la **Oficina de Coordinación de Ciberseguridad** a **Álvaro Lossada**. Inspector del Cuerpo Nacional de Policía, cuenta con un Máster en Ciberdelincuencia por la Universidad Nebrija y ha estado destinado en la Comisaría General de Policía Judicial, Unidad Central de Ciberdelincuencia, en la Brigada Provincial de Policía Judicial de Las Palmas como jefe de sección de UDEV y en la División de Cooperación Internacional, entre otros destinos.

● **Mónica Espinosa Garcés** ha sido contratada por la **Agència de Ciberseguretat de Catalunya** como Directora del Centro de Innovación y Competencia de Ciberseguridad. Ha trabajado para i2CAT Foundation, SDOS, Indra, Iecisa y ha sido experta independiente de la ONU y de Interpol, además de serlo actualmente de la Comisión Europea.

● **Opscura,** heredera de la compañía vasca Enigmedia, contará con los dos cofundadores en el equipo directivo. **Gerard Vidal** será CTO y **Carlos Tomás** ocupará el cargo de Vicepresidente de Ingeniería. Vidal ha trabajado para organizaciones como Scientifica Internacional, entre otras. Es profesor de ciberseguridad en la universidad Mondragón. Tomás, por su parte, ha sido investigador en la Politécnica de Madrid, además de haber trabajado para Altran y Xpertia Soluciones Integrales, entre otras.

● La responsabilidad de coordinación del **Centro de Ciberseguridad de Andalucía** ha recaído en **Enrique Rando.** En la Junta desde hace 25 años, ha estado dedicado a tareas vinculadas principalmente a las áreas de sistemas, despliegue de proyectos y atención a usuarios finales,compaginando esta labor con la docencia y la divulgación en el ámbito de la Microinformática y la Seguridad de la Información.

● **Miguel Trubia** ha sido contratado como Responsable del CERT por **Perseus Cybersecurity Services,** que ha ascendido a **Moisés López** a Responsable de Consultoría. Trubia, ha trabajado en Versia, ITS Security y SCC, entre otras. López ha desempeñado roles de responsabilidad en Everis Aeroespacial, Gneis y BDO Spain.

● El hasta ahora Director de Tecnología de **CrowdStrike**, **Michael Sentonas**, será el nuevo Presidente de la corporación. Además, la compañía ha ascendido a **Lorenzo Caddedu** a Senior Corporate Account Executive para el Sur de Europa. Sentonas estará al frente del desarrollo y comercialización de productos, así como de Ventas, Marketing e Ingeniería de Producto, entre otros departamentos. Caddedu tiene más de una década en el sector, donde ha trabajado en Qumulo, Huawei y HPE.

FlexiSOC, Ciberseguridad 360º en un modelo "as a service"

Apuesta por un **modelo seguro y adaptable** y obtén:

Visibilidad **Gobierno** **Soporte**

De forma sencilla y adecuado a tus necesidades.

Conoce más sobre la solución aquí ▶

Contacta con nosotros

info@ipm.es · www.ipm.es

A RICOH Company

LIDERA se asocia con CYBER GURU para distribuir su plataforma de concienciación en España y Portugal

La italiana **Cyber Guru,** especializada en concienciación en ciberseguridad en el ámbito corporativo, ha cerrado un acuerdo estratégico con el mayorista **Lidera** -recientemente adquirido por **V-Valley**, de **Esprinet**- para la distribución de sus productos. "La alianza responde a la creciente tendencia de los CISO a equilibrar sus inversiones entre hardware/software y formación al usuario. Aunque la tecnología puede contribuir en gran medida a proteger a la organización de las amenazas técnicas, las personas siguen siendo el eslabón más débil de cualquier organización y el objetivo principal de los ciberdelincuentes", destacan ambas firmas, que consideran que "para mejorar la concienciación y la resistencia de los empleados ante estos sofisticados ataques, los responsables deben invertir en una formación sobre ciberprotección que cambie la cultura de la empresa y que demuestre una mejora real de la postura de seguridad de la organización".

"Las organizaciones necesitan formar a los empleados para que se conviertan en la primera línea de defensa contra las ciberamenazas", recuerda el CEO y cofundador de Cyber Guru, **Gianni Baroni.** "Desde Lidera estamos encantados de para proporcionar a nuestros *partners* la más completa plataforma de concienciación en ciberseguridad", ha añadido el CCO de Lidera, **José Carlos Jimeno**. "La amplia experiencia de Lidera, junto con su consolidada red de distribución la convierten en el aliado ideal para alcanzar nuestros objetivos en este mercado", ha explicado la Sales Country Manager España y Portugal de Cyber Guru, **Mar Sánchez Caro.**

SANS y GOOGLE crean la SANS CLOUD DIVERSITY ACADEMY para impulsar la formación de ciberseguridad centrada en la nube

Sans Institute ha presentado, en colaboración con **Google**, la Sans Cloud Diversity Academy (SCDA), una iniciativa con la que busca proporcionar formación y certificaciones a mujeres, minorías étnicas, indígenas y otros grupos que actualmente están infrarrepresentados en el sector de la ciberseguridad.

Para lograr este reto, Sans Institute ha llevado a cabo una amplia difusión en los medios de comunicación de la industria tecnológica, así como en publicaciones centradas en la diversidad, al tiempo que trabajaba con numerosos socios del sector, como **Women in Cybersecurity, Black Girls Hack, Women's Society of Cyberjutsu** y **Cyversity**, entre otros.

Protección en la nube

Así, según han destacado Sans y Google, esta academia está pensada para proporcionar a los participantes los conocimientos necesarios para proteger la infraestructura en la nube y los datos confidenciales. Para ello, esta formación contará con becas para hasta tres cursos Sans y las certificaciones GIAC asociadas. En concreto, el **plan de estudios básico de SCDA** ofrece formación para las certificaciones GIAC Cloud Security Essentials (GCLD) y GIAC Public Cloud Security (GPCS), y los participantes que superen el programa deberán aprobar primero el examen GCLD antes de continuar. Tras aprobarlo, los estudiantes se presentarán al examen de certificación GPCS, que proporciona a los profesionales, analistas e investigadores de la seguridad en la nube un conocimiento profundo de los proveedores de *cloud* públicas más populares, como **Amazon** Web Services, **Microsoft** Azure y Google Cloud Platform. En total, la SCDA tiene previsto ofrecer, al menos, 25 plazas.

NOMBRAMIENTOS

Miguel Rego ha sido elegido como Presidente del **Clúster de Inteligencia Artificial de la Comunidad de Madrid.** Actual General Manager de Funditec, cargo que compagina, fue con anterioridad director del Incibe y ha trabajado en roles de responsabilidad en el Ministerio de Defensa, ElevenPaths, iHackLabs, Ono, EY y Deloitte, entre otras.

Marta Beltrán, profesora de la Universidad Rey Juan Carlos de Madrid, ha sido nombrada miembro del grupo de expertos que asesora al director ejecutivo de la **Agencia para la ciberseguridad de la Unión Europea** (Enisa). El Grupo Asesor de Enisa se centra en cuestiones relevantes para las partes interesadas del ámbito de las TIC.

Equinix ha nombrado a **Eulalia Flo** Consejera Delegada para España. Asume el cargo en sustitución de Ignacio Velilla, actual Vicepresidente Global de Managed Services de la compañía. Entre otros, ha ocupado roles de responsabilidad en Commvault, donde ha sido Directora General para Iberia, Capgemini, Business Objects, Symantec y Dell.

Arexdata ha designado CEO a **Alberto Tejero** y a **Cristina Gallego** como CMO & Channel Director, respectivamente. Tejero hasta ahora al frente de **ElixTech,** con el mismo rol, ha desempeñado puestos de responsabilidad en Mia Breach Hunter, Panda -donde fue Director General para Iberia-, y El Corte Inglés, entre otras. Gallego ha sido Directora de Canal Global de Elix Reg Tech y ha ocupado puestos de responsabilidad en MIA Breach Hunter, WatchGuard y Panday, donde trabajó casi dos décadas. Es licenciada en Ciencias Empresariales por la Carlos III de Madrid.

El hasta 2022 CTO y fundador de Devo, **Pedro Castillo,** ha iniciado una nueva etapa como fundador y CEO de **Signalit.** Es uno de los referentes en el sector, habiendo creado compañías como Logtrust, y desempeñado roles de responsabilidad en Bankinter o Webline, entre otras. Es químico por la Complutense de Madrid.

Hillstone Networks ha confiado a **Alberto Carrillo** el cargo de Country Manager para Iberia, habiendo sido hasta ahora responsable de desarrollar la marca en España. Asimismo, en 2023, Carrillo estará al frente del desembarco de la compañía en Portugal, Con anterioridad, trabajó en compañías como Quadient, Sangfor Iberia, Nutanix y Econocom España. Es licenciado en Informática por la Politécnica de Madrid.

Grupo Cybentia ha reforzado su equipo directivo con la incorporación de **Javier López Tazón** como Director adjunto a la Dirección General de la organización. Con más de 40 años de trayectoria periodística, tendrá bajo su responsabilidad las áreas de Concienciación y Formación, Consultoría Estratégica, Certificación y del Cyberlaboratorio. Es uno de los referentes en periodismo de tecnología habiendo trabajado en El País, El Mundo, donde creó y dirigió el suplemento 'Ariadna', además de haber fundado el videoblog 'Entre Bits & Chips'.

kaspersky 25 years

Más visibilidad.
Más potencia.
Más control.

¿No pensó estar preparado/a
para la EDR?
Ahora lo está.

Kaspersky
Optimum
Security

ORANGE y FORTINET suman fuerzas para proteger a las empresas contra el incremento de ciberataques

Orange se ha aliado con **Fortinet** para evolucionar su plataforma de seguridad perimetral Orange Security Suite. Esta se compone de una *suite* de servicios de seguridad gestionada por Orange, que combina la tecnología de Fortinet Security Fabric y su Fortigate Next-Generation Firewall más avanzado (NGFW).

Como resultado, esta evolución ayudará a todo tipo de organizaciones a proteger su actividad de una forma sencilla y adaptada a sus necesidades, con independencia de su tamaño, conocimientos y recursos dedicados a ciberseguridad.

Así, con Orange Security Suite, la red se convierte en la primera línea de defensa sobre los datos de cualquier empresa aportando, entre otros beneficios, la facilidad de implementación, la máxima disponibilidad, flexibilidad, además de contar con actualizaciones continuas para detectar y evitar las últimas amenazas. Todo ello a través de una plataforma monitorizada y atendida las 24 horas, 365 días al año, por personal especializado de la 'telco'.

"Los ciberdelincuentes aprovechan todas las tecnologías a su alcance para lanzar ataques cada vez más sofisticados y dirigidos, generando una gran disrupción y destrucción. En este contexto, las compañías deben adoptar soluciones integradas en la red que estén, además, dotadas de una inteligencia de amenazas automatizada y procesable, junto con capacidades avanzadas de detección y respuesta, basadas en el comportamiento", ha destacado el director de Fortinet para España y Portugal, **Acacio Martín.**

La UNIVERSIDAD DE MONDRAGÓN, primer centro universitario en impartir ciberseguridad aplicada a la automoción

El **Grupo Cybentia** y la **Mondragon Unibertsitatea** han firmado un acuerdo de colaboración para impulsar la formación e investigación en ciberseguridad aplicada a la automoción. Gracias a él, el alumnado y profesorado de la Escuela Politécnica Superior de la universidad vasca mejorarán sus conocimientos y capacidades sobre la ciberprotección en este pujante sector.

Javier López (Cybentia) y Carlos García (Mondragon Unibertsitatea)

Esta colaboración estratégica surge del interés de ambas entidades por explorar los productos y servicios de ciberseguridad aplicados a la automoción y la movilidad –ámbito en el que el Grupo Cybentia es un referente–, en las áreas de I+D+i, formación, concienciación y eventos, con el objetivo de mejorar el conocimiento y las capacidades del alumnado y del personal docente de la universidad.

En la misma línea, también se pretende desarrollar proyectos de investigación y transferencia sobre ciberseguridad, un campo en auge donde la universidad cuenta con un equipo de investigación. El acuerdo supondrá, como primer paso en firme, la organización de dos cursos: uno sobre la 'Normativa de Ciberseguridad para Vehículos UNECE/R155' y otro de 'Ciberseguridad en las Flotas de Vehículos', desarrollados en colaboración con **Eurocybcar** y el equipo de CyberQ-Testers de **HackerCar.**

NOMBRAMIENTOS

● **Áudea Seguridad de la información** ha reconocido los méritos de **Soraya Sabio,** ascendiéndola a Chief Commercial Officer (CCO). Licenciada en Filología inglesa, técnico superior en relaciones internacionales y postgrado en marketing y ventas, además de disponer de certificaciones como la ISO27001 e ISO22301 entre otras, y tras más de 11 años de trayectoria en la compañía, ha sido pieza clave en el crecimiento de la consultora, contribuyendo en gran medida a su actual posicionamiento como consultora especializada en Ciberseguridad, Cumplimiento Normativo y Privacidad.

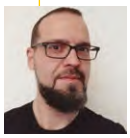
● **Mar Sánchez Caro** ha sido fichada como Business Development Manager por **Cyber Guru**, multinacional italiana con foco expreso en el aprendizaje y la concienciación. Ha trabajado para Confluent, Grupo SIA y Prosegur y BT, entre otras. Es titulada en Psicología por la Oberta de Catalunya y cuenta con un MBA por la EAE Business School.

● **Arantxa Calvo** ha sido contratada por **Grupo ITE** (Integración Tecnológica Empresarial) como Business Development Manager & Strategic Alliances. Ha ocupado puestos de responsabilidad en Factum Information Technologies, Secura IT Salvia Comunication y Publicaciones Alimarket. Es Licenciada en Publicidad y Relaciones Públicas por la Complutense de Madrid.

● **José Miguel Ruiz-Padilla** se ha incorporado como Director General IT Solutions por **Making Science.** Con más de 24 años de experiencia en IT y una década en ciberseguridad, ha desempeñado roles de responsabilidad en Babel –donde fue CISO–, Ingenia, Lidera (siendo fundador y CEO), Proximus y Ericcson.

● La potenciación del equipo de **SentinelOne** para el mercado español se ha plasmado en nuevas promociones y fichajes: **Samuel Marín** como Responsable Comercial Strategic Accounts, **Elisabetta Reato,** al frente del Channel Marketing para Iberia y **Manuela Joulageix,** como Responsable de Field Marketing para Iberia. Marín, hasta ahora Responsable Comercial para Sanidad, ha tenido en su trayectoria un especial foco en desarrollo de negocio de nube y soluciones verticales en compañías como Microsoft. Reato cuenta con una gran experiencia en el sector, donde ha trabajado como Regional Field and Channel Marketing Manager, Southern Europe de FireEye y Trellix. Joulageix posee también una gran trayectoria, habiendo sido Head of Marketing SEMEA en Rohde & Schwarz Cybersecurity, además de Senior Field Marketing Manager North/South EMEA en Imperva, entre otros.

● **Kudelski Security** ha contratado a **Luis Muñoz** como Regional Sales Manager para Iberia. Ha desempeñado roles de responsabilidad en Aiuken Solutions, WebEvolucion y Samsamia, entre otras. Es geólogo por la Complutense de Madrid.



● **Daniel Villaseñor** ha sido contratado por **LiveAction Software** como Sales Engineer. Ingeniero de Telecomunicaciones por la Politécnica de Madrid, ha trabajado para Telefónica Tech y Lookout, entre otras.

ES-CIBER

CONCIENCIAR EN CIBERSEGURIDAD NO ES UN JUEGO

pero podemos hacerlo divertido

ES-CIBER ofrece una amplia gama de tipologías de recursos desde series, gamificaciones, sesiones, tomas de decisiones, roleplay, podcast, materiales informativos y comunicativos

Concienciar a tus empleados de una forma divertida hará que consigas mejores resultados y un cambio de comportamiento **natural** frente a amenazas.

Te ayudamos a establecer y definir tu estrategia de Concienciación en Ciberseguridad con un proceso de mejora continua capaz de medir el cambio de comportamiento de tus usuarios.

www.es-ciber.com/ info@es-ciber.com

GOOGLE selecciona el Oblivious HTTP Relay de FASTLY para mejorar la privacidad en línea de miles de millones de usuarios

Fastly, conocida por su plataforma Edge Cloud, ha llegado a un acuerdo con **Google LLC** para explotar Oblivious Relay HTTP (OHTTP Relay) como parte de Fledge, la iniciativa 'Privacy Sandbox' que pretende mejorar la privacidad apoyando al mismo tiempo la publicidad personalizada.

Como se sabe, para los servicios en línea que necesitan o desean ofrecer experiencias personalizadas, la protección de la información personal identificable (IPI) de los usuarios ha demostrado ser un requisito complejo pero fundamental. En este contexto, Google Chrome dejará de admitir *cookies* de terceros en 2024, que suelen utilizarse para rastrear a los usuarios en distintos sitios web. En paralelo, se ha puesto en marcha una iniciativa, 'Privacy Sandbox', integrada por un conjunto de propuestas para reducir el rastreo entre sitios y aplicaciones, a la vez que se contribuye a mantener la gratuidad de los contenidos y servicios *online* en toda la web.

Como parte de Privacy Sandbox destaca de forma especial Fledge, para casos de uso de remarketing y publicidad personalizada, que está diseñada para elegir anuncios relevantes sin permitir el seguimiento entre sitios. Al utilizar el OHTTP Relay de Fastly, Fledge puede registrar de forma privada grupos de anuncios anónimos. En definitiva, OHTTP Relay proporciona una separación y un aislamiento rápidos y fiables de los datos personales, al tiempo que transmite solicitudes no identificativas al servidor de la empresa.

SIA impulsa la adopción de la firma-e cualificada con la verificación de la identidad de manera telemática

SIA, de **Minsait**, ha presentado su servicio de firma electrónica cualificada con registro telemático que permite verificar de forma remota la identidad del firmante mediante el uso de video identificación. De esta forma, elimina la necesidad de la presencia física del usuario para el registro y emisión de los certificados digitales requeridos en este tipo de firma, que es la que ofrece mayores garantías de seguridad jurídica.

El sistema, que ya ha sido validado, entre otros, en entornos de salud digital, permite que las firmas virtuales sean equivalentes a la manuscrita. "El proceso es realmente sencillo e intuitivo: el solicitante necesitará menos de un minuto para completar el proceso desde su PC o dispositivo móvil con cámara. Tras la verificación del proceso por parte de los operadores de SIA, en pocos minutos el ya titular de un certificado cualificado podrá empezar a realizar firmas electrónicas avanzadas y/o cualificadas", destacan desde la compañía.

Además, las aplicaciones prácticas de los certificados digitales cualificados emitidos mediante vídeo identificación y que SIA, como Prestador Cualificado de Servicios de Confianza, ofrece desde su plataforma en la nube, son amplias: las más destacadas van desde el *onboarding* digital cualificado de clientes, con las garantías de la firma cualificada con certificado electrónico, hasta la contratación de servicios, por ejemplo, bancarios, o sistemas de identificación ciudadana básica, como es el sistema Cl@ve que permite realizar numerosos trámites con las administraciones del Estado.

NOMBRAMIENTOS

Westcon ha apostado por **Miguel Almeida** como Country Sales Director. Después de su paso por CrowdStrike, vuelve al negocio mayorista, donde estuvo casi una década. También ha trabajado para Avaya y Afina, entre otras.

One eSecurity ha reconocido la buena labor de **Antonio Díaz Castaño** nombrándole Head of DFIR. Ocupó diferentes roles de responsabilidad en este ámbito en Inditex, donde estuvo casi una década, y KU Leuven. Es ingeniero técnico en informática por la Uned y cuenta con un Máster en Telecomunicaciones por la Universidad de Vigo.

Jorge Sendra se ha incorporado al equipo comercial de **Factum** como Senior Account Executive. Ingeniero Informático por la Universidad de Alicante, cuenta con una trayectoria de 20 años de experiencia y mucho foco en la identidad, habiendo sido Country Manager y Security Account Executive en compañías de consultoría y auditoría, habiendo formado parte del equipo de SailPoint, Micro Focus, DXC, HPE y PwC.

Cipher contará con **Ignacio Rodríguez Sierra** como Cibersecurity Service Delivery Manager (SDM PSG). Hasta ahora en Evolutio, ha forjado su trayectoria profesional en empresas como BT, Amper y Jazztel, entre otras. Es ingeniero técnico en Informática por la Universidad de Alcalá.

Ricardo España ha sido fichado por **Botech** como Consultor Senior y Pentester. Ingeniero de sistemas, posee varios cursos y certificaciones, entre ellos el de Qualified Security Assessor (QSA PCI DSS). Lleva más de una década desarrollando su carrera en operaciones de análisis de sistemas informáticos, implementación de sistemas financieros y transaccionales de alto rendimiento que abarcan tecnologías y métodos de pago alternativos y emergentes.

BeDisruptive ha contratado a **Beatriz Ruiz** como Executive Human Resources Director Global. Cuenta con más de 17 años de experiencia enfocada en la definición de estrategias innovadoras de RR.HH. dentro del sector TI y de telecomunicaciones. Es especialista en el cambio cultural estratégico que impactan en la satisfacción y la rotación de los empleados. En los últimos 10 años, ha centrado su labor en compañías de *big data*, *cloud* y ciberseguridad.

Zscaler se ha reforzado con **María Ramírez** como Enterprise Solutions Engineer. Ingeniera de Telecomunicaciones por la Universidad Politécnica de Madrid, ha trabajado previamente para Akamai, Airon Internacional, Panda Security y Trend Micro.

Jhonny Villafuerte ha sido fichado por **WatchGuard Technologies** como SOC Technician. Ha trabajado, entre otras, para Factum y Gran Vía detectives privados. Cuenta con el grado de Criminología por la Rey Juan Carlos.

LA CALIFICACIÓN **LEET**

TE AYUDA

En un entorno de creciente impacto regulatorio,

te ayuda a cumplir,

te ayuda a mejorar.

LEET SECURITY
ICT Rating
C B A

Utiliza y exige la calificación.

Transmite confianza.

WWW.LEETSECURITY.COM

HORNETSECURITY presenta 'Employee Security Index', el índice de seguridad que mide la capacitación de los empleados

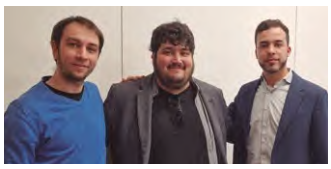
"Los empleados necesitan recibir una formación en ciberprotección de al menos tres meses para que las empresas alcancen un nivel aceptable de seguridad". Así lo destaca el informe 'Employee Security Index (ESI)' de **Hornetsecurity** en el que también se recuerda que una 'pausa' en la capacitación de sólo un mes, puede hacer que la puntuación ESI de una organización disminuya por debajo del nivel requerido, mientras que un parón de cuatro meses puede hacer que las organizaciones vuelvan al punto de inicio. El estudio, que analizó cerca de 1,8 millones de ataques de *phishing* simulados sobre 140.000 empleados y en más de 350 compañías, ha arrojado luz sobre los riesgos que los ciberataques representan para las empresas.

Entre sus conclusiones más relevantes destaca que, según sus participantes, el 90% de todos los ataques cibernéticos comienzan con ataques de suplantación y más del 40% de todos los correos-e tienen potencial de ser una amenaza para las organizaciones.

También es notable que, según la investigación, de promedio, los empleados necesitan tres meses de capacitación para llegar a la 'zona de protección'. El estudio indica que se requiere formación continua para garantizar que los empleados estén instruidos y protegidos contra el desarrollo de ciberamenazas. Por otro lado, constata que las empresas en ocasiones se preocupan por la fatiga que puede provocar en sus empleados la capacitación en seguridad. Hornetsecurity, respondiendo a estas demandas, ha integrado breves pausas en su programa, Security Awareness Service, para garantizar que los empleados no se desconecten. Los resultados también muestran que la capacitación en seguridad debe enfocarse en las necesidades individuales, en lugar de seguir un enfoque único para todos. El exclusivo 'Awareness Engine' dentro del 'Security Awareness Service' ofrece formación automatizada y de última generación basada en las necesidades individuales de cada empleado, proporciona indicadores concretos y fiables y comparaciones estandarizadas entre diferentes grupos de empleados, adaptando así el nivel de capacitación a diferentes empleados según su puntuación ESI.

Nace BLOCK-AUTH, una firma española que quiere facilitar la gestión segura de la identidad y los accesos, a través de una *blockchain* privada

Desde el 8 de marzo, España cuenta con una nueva compañía, **Block-Auth,**,en el disputado mercado de protección de las contraseñas y la identidad. Fundada por **Josué López,** al frente como CEO, así como **Yassir Doutroi,** el CMO y **Josué García,** el CTO, y con sede en Madrid, "plantea un cambio en el estándar tradicional de credenciales, sustituyendo las credenciales de usuario y contraseña por un sistema de autenticación basado en *blockchain* con diferentes capas de seguridad y trazabilidad para lo que se ha desarrollado una extensión para navegador, en una primera etapa y *login* único para todas las tecnologías que se integren".



De momento, su primer producto, que comenzará a comercializarse entre abril y mayo para navegadores, permitirá autenticarse sin contraseña gracias al uso de una *blockchain* privada. Además, en los próximos meses, "ofreceremos un sistema, a través de contratos inteligentes (*smart contracts*) que permitirán al usuario administrar la información personal que se quiere compartir y la que no", recuerda López, quien también destaca que el sistema funciona como una *wallet,* "en ciertos aspectos similar a la que podría desarrollarse con la normativa eIDAS, pero más centrada en lo que son propiamente las contraseñas".

En definitiva, "Block-Auth tiene una orientación global pudiendo ser integrado en esquemas B2B, B2C y B2E, sustituyendo los métodos de *login* tradicionales, en el ámbito corporativo", resume López.

NOMBRAMIENTOS

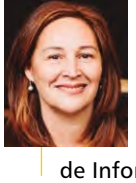
Perception Point contará con **Rafa López** como Responsable de Preventa para EMEA y Latinoamérica. Graduado en Derecho por la Uned y en Telecomunicaciones por la Oberta de Cataluña, colabora con First -es uno de los cuatro españoles nombrados Liaison-, Global Security Academy y Three Points The School for Digital Busines, además de ser cibercooperante del Incibe.

Carlos Álvarez ha sido ascendido a Presales Manager en el mayorista **Ajoomal Asociados.** Ingeniero técnico industrial por la Carlos III de Madrid, ha trabajado anteriormente para Grupo Epelsa, entre otras.

Telefónica Tech ha contratado a **Carolina Gómez** como Offensive Security Engineer y ha promocionado a **Cynthia Conesa** a Head of Cloud Managed Services. Gómez además de haber sido coordinadora del congreso cántabro de seguridad técnica Sh3llcon, ha trabajado para Deloitte, Netkia y Vass, entre otras. Cuenta con un Máster en Ciberseguridad por la Universidad de Castilla la Mancha. Conesa hasta ahora ejercía como Head Of Information Technology. Cuenta con más de 20 años de experiencia en el sector IT y es ingeniera de Telecomunicaciones por la Politécnica de Madrid.

SentinelOne se ha reforzado con las incorporaciones de **Andrea Unanue** como Responsable Comercial de Mid Market para Iberia, **Antonio Vasconcelos,** como EMEA Field CISO Director, **Carlos Molano** como Director de Partners MSSP Iberia y **Raffaello Pellegrini**, como BDR para Iberia. Unanue, hasta ahora Sales Account Manager de Midmarket en Cisco, es graduada por la Autónoma de Barcelona en Administración y Gestión de Empresas. Vasconceios ha estado una década trabajando para Microsoft, con diferentes roles de responsabilidad como Technical Sales de Unified Enterprise Management y Advanced Security, además de un lustro en el Product Group de Microsoft 365 Defender, destacando su labor en diferentes áreas de desarrollo e innovación. Molano, con anterioridad, ocupó puestos de responsabilidad en compañías como Aviatrix y Rubrik. Por su parte, Pellegrini cuenta con una gran experiencia en prospección de nuevos clientes y segmentación de mercados.

Mnemo Innovate ha incorporado a **José Antonio Otero** como Director de Alianzas. Profesional con amplia experiencia gestionando tecnología, desarrollo de soluciones y negocio en diferentes sectores. Durante la última etapa, ha sido responsable del portafolio de soluciones de infraestructura de Comunicaciones y Ciberseguridad en NTT Data para Europa y Latinoamérica, entre otros cargos de responsabilidad.



IPM, a Ricoh Company ha nombrado a **Paloma Herranz** como Directora Comercial en España. Con 20 años de experiencia, ha trabajado para Capgemini, EMC2, Dell EMC y Soluziona Indra, entre otras. Es licenciada por la CEU San Pablo y cuenta con un Máster en Sistemas de Información.

CYBER DEFENSE MNEMO

Plataforma de MNEMO para la gestión de ciber amenazas.

Muchas empresas pagan un peaje por estar en Internet. **MNEMO te ayuda a ver el riesgo latente antes de que impacte en tu organización**.

- **Visión 360° del riesgo de exposición** de una compañía y de toda su cadena de suministro en el ciberespacio.
- **Identificación temprana de amenazas** para la identidad digital, marca e información confidencial de la organización.
- **Enriquecimiento de las amenazas detectadas** con la información del área de Inteligencia de MNEMO.
- **Acceso inmediato a detalles de las alertas generadas**, seguimiento de las amenazas y baja de contenidos fraudulentos.
- **Análisis de amenazas estratégicas** para la organización en el mundo online (hacktivismo, VIPs, relacional, fake news, ...).
- **Identificación de tendencias de amenaza** mediante boletines e informes de inteligencia de relevancia local, sectorial e internacional.

Mnemo

mnemo.com

España | México | Colombia | Perú | Ecuador

SOLICITA UNA DEMO

TF-CSIRT Trusted Introducer

CSIRT.es

Red Nacional de SOC

FUJITSU impulsa en Barcelona un centro de ciberseguridad especializado en salud

Fujitsu lleva años impulsando un plan de crecimiento para reforzar su área de ciberprotección en España. Enmarcada en esta estrategia, la multinacional nipona ha decidido situar en Barcelona un centro de ciberseguridad especializado en servicios sanitarios. Al principio, tendrá el foco puesto en trabajar con centros sanitarios, públicos y privados, de toda España.

El Centro de Excelencia de Servicios de Ciberseguridad Sanitarios ha empezado a andar con el nombramiento de su coordinador, **Enric Llaudet** y se centrará en identificar la demanda específica del sector, establecer los mecanismos específicos de seguridad y definir nuevas soluciones para la gestión de los riesgos sanitarios. Inicialmente, comenzará a funcionar con profesionales de la compañía y el objetivo es consolidar un equipo de hasta 15 empleados entre este 2023 y el próximo año. Además, se complementará con el SOC que Fujitsu tiene en Sevilla.

"Se trata del primer centro de estas características que la empresa tecnológica ha creado a nivel mundial", explica Llaudet. "Se ha decidido dar este paso de especialización por la extensa implantación de la multinacional en los centros sanitarios a nivel español, además de haber visto que era un sector que necesitaba una atención más personalizada", ha destacado.

LENOVO inaugura un centro de ciberprotección en Israel para realizar pruebas e intercambiar información con organizaciones del país

La multinacional china ha inaugurado un centro de innovación en ciberseguridad, el **Lenovo Cybersecurity Innovation Center** (LCIC) en colaboración con el Centro de Investigación en Ciberseguridad de la **Universidad Ben-Gurion** del **Negev,** una institución de referencia en el sector con sede en Israel. El nuevo centro estudiará la innovación en arquitectura de hardware de confianza cero (y la seguridad subyacente a los sistemas operativos), además de actuar como un nodo para el desarrollo de futuras generaciones de soluciones de seguridad.

El LCIC ofrecerá a los clientes de Lenovo un laboratorio de pruebas, acceso a conocimientos y la posibilidad de intercambiar información mediante un centro de comunicación *in situ*.

Las soluciones desarrolladas en el LCIC serán incorporadas a ThinkShield, la cartera de hardware, software y servicios de Lenovo con características de seguridad mejorada. Esta cartera integral de protección proporciona soluciones avanzadas en forma de seguridad de plataforma integrada y protección de dispositivos, protección de los datos frente a amenazas y herramientas de gestión que contribuyen a proteger información crítica para los negocios.

Nima Baiati (Lenovo), Luca Rossi (Lenovo) y Yuval Elovici (Universidad Ben-Gurion)

NOMBRAMIENTOS

SailPoint ha apostado por **Elena Cerrada** como nueva Country Manager para Iberia. Con anterioridad, desempeñó roles de responsabilidad en Forcepoint, Check Point, Fluke Networks y Telindus, entre otras. Es graduada en Telecomunicaciones por la Politécnica de Madrid.

Forcepoint ha contratado como Country Manager para España y Portugal a **Ricardo Hernández**. Ingeniero de Telecomunicaciones por la Politécnica de Madrid y con una dilatada trayectoria en el sector, ha trabajado para Vectra AI, ForeScout, Tufin,Mandiant, Check Point, Kaspersky, Symantec, Websense, Trend Micro y Panda Software.

Armis ha nombrado como presidente a **Brian Gumbel,** quien reportará directamente a Yevgeny Dibrov, CEO y cofundador de la compañía. Con más de 20 años de experiencia, ha desempeñado roles de responsabilidad en Forescout Technologies, Tanium, McAfee y Cisco.

Eutimio Fernández ha sido contratado por **Vectra AI** como Country Manager para Iberia. Con una dilatada trayectoria en el sector, con anterioridad ha trabajado para TreatQuotient, Cisco, Sourcefire y Lumension, entre otras. Es ingeniero informático por la Universidad de Castilla la Mancha.


A3Sec ha situado a **Javier Díaz** como Director General Global y ha fichado a **Maribel Poyato** como Territory Sales Manager. Díaz, hasta ahora Chief Revenue Officer (Director de Ingresos) del Grupo, cuenta con una con amplia experiencia en el sector habiendo trabajado para Fortinet, iTrust, PwC y ATH, donde fue CISO. Poyato, por su parte, ha trabajado para empresas como Céfiros, La Latina Valley, Tixeo y BlueBottleBiz, entre otras.

Carlos Moliner ha sido contratado por **Veeam Software** como Territory Manager. Ha ocupado puestos de responsabilidad en Citrix, donde ha desempeñado gran parte de su carrera, Tecnocom, Telindus y la Universidad Antonio de Nebrija.

iC Consult contará con **Oscar González** como Director Regional para Iberia. Ingeniero de Telecomunicaciones por la Politécnica de Cataluña, ha trabajado para Omega Peripherals, AdmIT Consulting, GreenbIT Tecnologías de la Información y la Autónoma de Barcelona.

Reduzca el riesgo creado por las credenciales filtradas con inteligencia procesable en tiempo real

La autenticación multi-factor no es suficiente, las credenciales que se filtran hoy día contienen suficiente detalle como para eludir el control de los MFA.

Con el módulo Identity Intelligence de Recorded Future instantáneamente podrá:

- Detectar fugas de credenciales antes de que supongan un problema
- Automatizar verificaciones de contraseñas
- Acceder al contexto en tiempo real para la clasificación y mitigación de amenazas
- Obtener una visibilidad inigualable de las fuentes dentro de la deep y la dark web

Descubra las credenciales que se han filtrado de su organización en: recordedfuture.com/identity

EVOLUTIO continúa su crecimiento con su cuarto SOC en España, la certificación en el ENS en 'Categoría Alta' y como miembro Gold de la RNS

Para dar respuesta a las necesidades y expectativas de las compañías, y ayudarlas a protegerse ante agentes maliciosos y ataques, **Evolutio** ha mejorado en el último año su oferta y la calidad de sus servicios, obteniendo el nivel más alto en el Esquema Nacional de Ciberseguridad (ENS), una certificación que avala la seguridad de la ciudadanía en sus interacciones digitales con la Administración Pública. Además, se ha incorporado a la Red Nacional de SOC (RNS) como 'miembro Gold'.

Como parte de su hoja de ruta para 2023, Evolutio ha puesto en marcha un nuevo SOC en Linares, Jaén, siendo el cuarto del integrador en la Península Ibérica. A esta acción le acompañan otras ya realizadas en territorio andaluz, como es la apertura del primer laboratorio andaluz de ciberseguridad, impulsado por la **Cámara de Comercio de Linares** para el que se destinará una inversión de 300.000 euros. Durante 2022, la compañía también reforzó su apuesta por Andalucía con la inauguración de su centro de trabajo en Linares para crear sinergias con el tejido empresarial regional y con la red de centros formativos. El fomento del talento local se verá impulsado por la creación de 150 puestos cualificados en los próximos dos años.

Así cerró 2022 con un incremento del 10% de su plantilla, sobrepasando los 1.100 profesionales. Desde la compañía también han destacado el valor de su red de *partners* tecnológicos entre los que están **AWS**, **Cisco, Fortinet, Genesys, Google Cloud, IBM, Microsoft, Nuance, Salesforce, Oracle** y **Palo Alto.** De hecho, el año pasado obtuvo la competencia de Partner de Gobierno de AWS, que supone el reconocimiento de su experiencia como integrador de servicios *cloud*. Además, ha cerrado una alianza con **Veridas,** uno de los de los referentes en soluciones biométricas para la verificación de la identidad visual.

KPMG ESPAÑA logra la certificación ISO 27701:2019 en materia de privacidad de la información

KPMG España ha obtenido la certificación ISO 27701:2019 en materia de privacidad de la información, siendo una de las pocas firmas prestadoras de servicios multidisciplinares –y la única Big4, hasta la fecha– certificada en dicha norma. Esta certificación acredita el elevado nivel de cumplimiento de la normativa por parte de KPMG en los tratamientos de datos llevados a cabo en el ejercicio de su actividad profesional.

Esta norma, extensión de la ISO/IEC 27001, tiene como objetivo proporcionar orientación sobre la protección de la privacidad, incluida la forma en que las organizaciones deben gestionar la información personal, además de ayudar a acreditar el cumplimiento de la normativa en privacidad, como el RGPD, en todo el mundo.

Desde la Unidad Técnica de Privacidad de la Asesoría Jurídica de KPMG se coordinan las acciones necesarias para dar cumplimiento a los compromisos adquiridos tanto en el mantenimiento de un exigente nivel de cumplimiento normativo, como en la promoción de la innovación y transformación digital ética, responsable y transparente, en aquellos productos y/o servicios con tratamientos masivos de datos, en especial Inteligencia Artificial (IA), así como la promoción del Canal Prioritario como herramienta fundamental para solicitar la eliminación urgente de contenidos sexuales y violentos en Internet, entre otros.

"Esta certificación supone un refuerzo adicional al compromiso de KPMG con el cumplimiento de la normativa en materia de protección de datos como es el RGPD o la LOPDGDD, garantizando así el cumplimiento de sus obligaciones como encargado y responsable del tratamiento de la información personal necesaria para su actividad profesional", ha destacado la DPO de la consultora, **Paula Hernández Cobo.**

NOMBRAMIENTOS

María Herranz ha pasado a asumir la Dirección de Canal de **Cisco** en España, compañía en la que comenzó en 2005. Durante sus más de 17 años en la empresa, ha ocupado diversos roles en las áreas de Ventas, Desarrollo de Negocio y Canal, con responsabilidad tanto en España, como en el Sur de Europa. Sustituye en el cargo a Gabriel Maestroarena, quien venía desempeñando este puesto en Cisco España desde octubre de 2019.

El hasta ahora responsable de Marketing para Iberia de **Kaspersky**, **Alejandro Quero,** ha sido promocionado a Director de Marketing para la región sur de Europa, incluyendo entre sus nuevas responsabilidades Francia, Italia e Israel. Asimismo, la filial ibérica ha ascendido a **Javier Ildefonso** para liderar su negocio digital como Vicepresidente. Quero, en la compañía desde 2014, es licenciado en Publicidad y Relaciones Públicas por la Universidad de Valladolid y cuenta con más de 15 años de experiencia desarrollando estrategias de marketing en multinacionales de TI donde ha ocupado puestos de responsabilidad tanto regionales, como a nivel europeo. Ildefonso, con más de 20 años de trayectoria en transformación digital, ha trabajado en Sage, Wonder Workshop, Luce CEM y Symantec, entre otras.

La labor de reforzamiento de **aDvens Iberia** continúa con la reciente incorporación de **Yago Gómez-Trenor** como Account Manager y de **Javier Ortega** como Service Delivery Manager. Gómez-Trenor cuenta con una solvente trayectoria en el sector en compañías como Cipher, Sothis, Vintegris y S2 Grupo, entre otras. Ortega, por su parte, dispone de amplia experiencia también en este ámbito, habiendo trabajado para Grupo SIA, Valvonta, Satec y Everis.

Marcos Carrera se ha incorporado a **Fujitsu** como Head of Blockchain & Web3 para Iberia, aportando estrategia y conocimiento en el desarrollo de negocio. Ingeniero industrial y con un MBA, Carrera es perito judicial experto en tecnología de cadena de bloques y criptoactivos y, anteriormente, trabajó para compañías como Reental, de la que es Cofundador, Grant Thornton España, Accenture y Tutellus, entre otras.

Exclusive Networks ha contratado a **Vanesa Couto** como **Directora de Marketing** para Iberia. Con más de 15 años de experiencia en marketing, comunicación y comercial, ha trabajado para Westcon Europe, donde ha sido Responsable de Marketing, Vasa, Iaso Health, Adqueria Marketing y GPTQ.

Arturo Marín se ha incorporado al equipo de **Smart HC** como Director de Desarrollo Corporativo. Con anterioridad, desempeñó cargos de responsabilidad en Future Space, Blumara Solutions y Seguros RGA, entre otras.

FACTUM

MDR

La unión perfecta entre la tecnología y la inteligencia humana

Detectar · Analizar · Investigar · Responder · Contener

V-VALLEY incorpora a STARWIND, focalizado en hiperconvergencia y visualización del almacenamiento, en su catálogo de distribución

V-Valley ha incorporado a **StarWind**, fabricante especializado en hiperconvergencia y tecnologías de virtualización del almacenamiento, en su portafolio. Gracias a esta unión, los clientes de V-Valley podrán acceder a todo el catálogo de productos de StarWind, actualmente, "el único proveedor de hiperconvergencia *all-flash* del mercado", y pone a disposición de los clientes todos los 'bloques de construcción' necesarios para montar una infraestructura de centro de datos sin ningún sobreaprovisionamiento y adaptando cada requisito de TI a una solución de valor real, según explican desde el mayorista.

El catálogo de productos de StarWind se apoya en más de 20 años de experiencia en las áreas de virtualización y almacenamiento definido por software, como sistemas de hiperconvergencia, VSAN, SAN, NAS y bibliotecas de cintas virtuales, ofreciendo también "los mejores dispositivos de su clase". Pero, quizá, en su propuesta destaca, de forma especial, StarWind Virtual SAN.

Se trata de una solución de almacenamiento definida por software que elimina por completo la necesidad de almacenamiento físico compartido y consigue una alta disponibilidad en hardware comercial partiendo de dos nodos.

"Se trata del único almacenamiento virtual compartido del mercado que no tiene listas de compatibilidad de hardware, funciona con cualquier hipervisor y tiene un precio razonable". "Damos la bienvenida a nuestro catálogo a StarWind, una solución para la infraestructura y centro de datos donde el mercado lo que pide es flexibilidad y simplicidad que es lo que proporciona StarWind".

Trabajaremos conjuntamente para mejorar e incrementar la presencia de Starwind en el mercado español", ha destacado el Head of Sales & Marketing Cloud & Software en V-Valley, **Roberto Alonso.**

TEHTRIS se asocia con la consultora ITSICAP para impulsar las capacidades automatizadas de ciberprotección

Tehtris ha firmado un acuerdo de colaboración con la consultora especializada en sistemas tecnológicos, **ITSicap**. Un año después de su llegada a España, en febrero de 2022, Tehtris continúa afianzando su presencia en nuestro país, estableciendo alianzas estratégicas con su red de *partners*. Por su parte, gracias a esta asociación, ITSicap suma a su catálogo la solución Tehtris XDR Platform, que permite detectar y remediar los ataques informáticos de forma automatizada, sin intervención humana.

"Este acuerdo supone una alianza estratégica que demuestra que cada vez son más compañías plenamente conscientes de cómo la ciberseguridad es uno de los principales impulsores de los negocios hoy en día. Estamos muy contentos de poder contar con *partners* tan valiosos como ITSicap, que comparten nuestra visión basada en la hiperautomatización para hacer frente a las actuales amenazas", ha destacado el country manager de Tehtris en España, **Pedro Morcillo.**

"En ITSicap, contar con un *partner* como Tehtris nos permite evolucionar a gran escala en materia de ciberseguridad. Estamos agradecidos de poder contar con una solución tecnológica como Tehtris entre las muchas que existen en el mercado, solo unas pocas pueden aportar valor a las empresas. Esto nos permite ofrecer a nuestros clientes una herramienta de calidad y fiable apoyada por una empresa profesional del sector", añadía, por su parte, el CEO de ITSicap, **José María García.**

NOMBRAMIENTOS

Jesús Varela ha sido ascendido por **Fortinet** a Sales Director, habiendo sido hasta ahora Manager Regional Sales. Con una amplia trayectoria en el sector, ha estado en Open3s, CSA, Satec y Grupo Leche Pascual, entre otras.

Atalanta ha contratado a **Alejandro de la Granja** como Sales Director. Ha ocupado puestos de responsabilidad en compañías como Rocket.Chat, Cipher, Entelgy Innotec Security y Mnemo, entre otras.

Nokia ha apostado por **Gonzalo Erro** contratándole como Security Manager. Con una dilatada trayectoria, ha desempeñado roles de responsabilidad en Huawei Technologies, Accenture, Ethernalia y S21sec, entre otras.

CyberArk ha apostado por **Albert Barnwell** ascendiéndole a Sales Director para Iberia. Con más de 15 años de trayectoria, ha trabajado con anterioridad para Citrix, Acronis, VMware y Symantec, entre otras.

Commvault ha fichado a **Anna Griffin** como Chief Marketing Officer. Ha ocupado puestos de responsabilidad en compañías como Smartsheet; marcas emergentes, como Intercom; y globales como Saturn, Apple, Sony, Junipe y CA (ahora Broadcom). Ha recibido numerosos premios por sus campañas, entre ellos el Golden Effies a la eficacia en marketing y el Edgar R. Murrow a la excelencia en redes sociales.

Lynx Financial Crime Tech ha fichado como CTO a **Carlos Santa Cruz.** Físico por la Autónoma de Madrid y experto en la lucha contra el fraude, también en su ámbito de financiación del terrorismo, es uno de los profesionales españoles con mayor conocimiento de esta materia. Compagina este cargo con la docencia como profesor de informática e IA en la Autónoma desde hace más de dos décadas.

Grupo Esprinet ha contratado a **Conxi Palmero** como Directora de Alianzas Estratégicas del Grupo. Licenciada en Ciencias Económicas por la Universitat Pompeu Fabra de Barcelona, comenzó su carrera en Control de Gestión y Auditoría en el Grupo Sesa, además de haber trabajado para Computer Gross Italia, PwC y Grupo Bonmacor.

EL SECTOR INDUSTRIAL CADA VEZ SUFRE MÁS CIBERATAQUES

El reto será mayor en 2023 por:

- La situación geopolítica y económica mundial
- La digitalización industrial con mantenimiento predictivo
- El cloud industrial y la virtualización
- La creciente sofisticación y profesionalización de los ciberdelincuentes

Accede a un espacio a tu medida para formarte, compartir y conocer muchas experiencias en ciberseguridad industrial.

Si eres un profesional independiente, tienes la membresía básica o profesional del CCI

Si eres una empresa industrial o proveedor, tienes las membresías corporativas tanto para PYME como Gran Empresa

Accede a nuestras membresías: www.cci-es.org/membresias

ARMIS, uno de los centauros de más rápido crecimiento tras lograr los 96 millones de euros en ingresos recurrentes anuales en menos de cinco años

Armis ha superado la marca de los 96 millones de euros (100 millones de dólares de ingreso recurrente anual) en sólo cinco años. Con ello, se convierte en uno de los 'centauros' de más rápido crecimiento en tecnología SaaS y nube, y en la *startup* de ciberseguridad enfocada a la visibilidad, inteligencia y seguridad de activos de más rápido desarrollo. Un éxito que, según destacan desde la compañía, viene impulsado por su plataforma de visibilidad y seguridad de activos, que ya ha sido adoptada por las mayores organizaciones del mundo incluidas en la lista 'Fortune 100', como **Colgate-Palmolive, Mondelez International, DocuSign, Allegro Microsystems** y **Takeda Pharmaceuticals,** además de numerosas entidades nacionales, estatales, regionales y federales de EE.UU., EMEA y APJ.

"Ofrecemos una de las plataformas de inteligencia de activos más completa de la industria ya que proporciona visibilidad unificada de activos y seguridad para todos ellos, tanto gestionados como no gestionados, e incluidos IT, IoT, OT, IoMT, la nube y móvil-IoT", destacan desde la compañía poniendo en valor que, en 2022, la empresa amplió el número de módulos a los que los clientes pueden suscribirse, aumentando así el número de casos de uso en tiempo real a los que da soporte y ofreciendo a los clientes aún más valor.

Cabe recordar que, tras una ronda de inversión de 280 millones de euros en 2021, la organización fue valorada en 3.200 millones de euros, con el respaldo de inversores como **Insight Venture Partners, CapitalG, Brookfield, One Equity Partners** y **Georgian.**

Armis ha desarrollado un modelo de distribución y venta a través de *partners* entre los que se cuentan organizaciones como **Accenture, AWS, Booz Allen Hamilton, Capgemini, Check Point, Fortinet, Google Cloud, HCL, KPMG, Kroll, Nuvias, SentinelOne, ServiceNow** y **Wipro**, entre otras, haciendo que los clientes puedan acceder a los servicios y la asistencia desde cualquier lugar del mundo.

Dentro de sus planes de expansión, y en línea con su objetivo de facilitar al máximo el acceso a sus servicios, Armis ya está disponible tanto en Google Cloud Marketplace como en AWS Marketplace, lo que amplía su alcance en el mercado.

PUERTO DE BARCELONA renueva su plataforma tecnológica, Portic, poniendo especial foco en su ciberseguridad

El **Port Community System (PCS) de Barcelona**, el denominado Portic, ha puesto en marcha una nueva plataforma tecnológica con importantes mejoras, sobre todo, de ciberseguridad y con el objetivo de optimizar el rendimiento, la protección y la resiliencia frente a posibles ciberincidentes. Esta iniciativa supone una inversión de cinco millones de euros, según la **Autoridad Portuaria de Barcelona,** y está previsto que esta implementación comience a funcionar a finales de año, tras realizar pruebas durante 10 meses.

Con la actualización de la plataforma, las autoridades portuarias buscan dotar al sistema informático de las herramientas necesarias para abordar los retos previstos como cambios legislativos, mejora en los procesos y la inclusión de nuevas tecnologías. La modernización ha incluido, también, la reestructuración del software en microservicios, la migración a un nuevo centro de datos de alta seguridad, la instalación de un segundo centro de datos alternativo en caso de caída, además de servicios avanzados de administración, según se marcó en el IV Plan Estratégico 2021-2025 del puerto. "Con esta renovación se ha doblado la capacidad de procesamiento del anterior sistema, incrementando su rendimiento y capacidad de escalado", ha destacado el director de Sistemas de Información del puerto, **David Serral**.

NOMBRAMIENTOS



Solver4 continúa ampliando su equipo a nivel internacional, con el nombramiento de **Alberto España**, como CEO, a **Raúl Mejía** (socio fundador) como Responsable de Operaciones y **Rogelio Nova,** que estará al frente de S4 HSM, el servicio que integra administración de Cloud HSM y Key Management. Ingeniero aeronáutico de formación, España es una de las figuras más reconocidas en la industria de pagos, donde lleva 30 años desarrollando su carrera, ocupando puestos de responsabilidad para Visa Internacional, American Express, Citibank y Banco Santander en las áreas de Gestión de Riesgos, Seguridad y PCI Compliance. Fue uno de los primeros en certificar empresas en el estándar PCI DSS en Latinoamérica. Mejía cuenta con más de 15 años de experiencia en PCI DSS y es experto en evaluaciones de cumplimiento, riesgo y controles y desarrollo de planes de acción de mitigación de riesgos que respaldan a bancos, procesadores de tarjetas y grandes organizaciones en toda América Latina y el Caribe. Nova tiene más de 20 años de trayectoria centrada en el ámbito de la seguridad y de las certificaciones.


GMV ha contratado a **Ángel García Madrid** como Business Continuity Manager/ Head of Section y ha ascendido a **Enrique Fraga** a Space Systems General Manager. García posee más de 20 años de experiencia en consultoría estratégica y de operaciones, ha estado en compañías como Red Mountain Games, Fundación Gestión del Conocimiento y Minsait, entre otras. Es físico por la Complutense de Madrid. Por su parte, Fraga ha desarrollado gran parte de su carrera en la compañía, además de haber trabajado para Itstaff y Unión Fenosa. Es licenciado en Matemáticas por la Complutense de Madrid.

Legal Army ha fichado a **Flora Egea** como Socia del Área de Privacidad, Protección de Datos y Cumplimiento. Miembro del consejo asesor de APEP desde hace una década, venía siendo DPO en BBVA y antes en IBM. Es licenciada en Derecho por la Complutense de Madrid.

Pentera contará con **Andrea Sánchez Buendía** como Iberia Business Development Manager. Licenciada en ADE por la Pontificia de Comillas, durante su trayectoria ha trabajado en Auzen y Euro Funding.

Davinci Group ha ascendido a **David Rodríguez** a Director Comercial Cyber & Cloud Security. Ingeniero por la Politécnica de Cataluña, ha estado en compañías como Aidin, Sirt, UsedSoft y Fitco Consulting.

grupo ica
Sistemas y Seguridad

PROTEGE ADECUADAMENTE LA INFORMACIÓN MÁS SENSIBLE

Más de **35** años ciberprotegiendo a organismos públicos.

Sabemos cómo hacerlo.

www.grupoica.com · seguridad@grupoica.com · Tlf: + 34 913 110 487

AENOR ER Empresa Registrada ISO 9001 ER-1567/2000
AENOR ER Seguridad Información ISO 27001 SI-0055/2015
AENOR ER Gestión Servicios TI ISO 20000-1 STI-0011/2013
AENOR Gestión Ambiental ISO 14001 GA-2009/0728
CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría ALTA RD 3/2010 ENS-2016/003

Red Nacional de SOC
TI
CSIRT.es
FIRST Improving Security Together

El CESGA, en Galicia, apuesta por el Computador Cuántico de FUJITSU, uno de los más ambiciosos del Sur de Europa

El **Centro de Supercomputación de Galicia** (CESGA) ha apostado por **Fujitsu** para proporcionar en la Comunidad el que será su primer computador cuántico, con un presupuesto de 14 millones de euros. "Es la iniciativa más ambiciosa por la computación cuántica que se está realizando en España y contribuirá de una manera decisiva al desarrollo del Polo de Tecnologías Cuánticas de Galicia".

"Esta infraestructura permitirá realizar investigación de vanguardia a la comunidad investigadora, a centros tecnológicos y a empresas, situando a Galicia en la primera línea del panorama Internacional", destacan desde el Centro.

Se trata de uno de los primeros ordenadores de estas características que estará a disposición de la comunidad investigadora en el sur de Europa. El computador cuántico, que a lo largo de 2023 será instalado en el CESGA y puesto al servicio de investigadores y empresas con la ambición de liderar proyectos e investigaciones pioneras, contará con los elementos necesarios para contribuir a la generación de nuevos algoritmos cuánticos en ámbitos tan relevantes como la simulación de fenómenos físicos y químicos, el cifrado de datos, el aprendizaje automático y la solución de problemas complejos, la IA, la robótica y la ciberseguridad, entre otros.

La adquisición consta de cuatro elementos principales: un computador cuántico, un computador de altas prestaciones, un emulador de algoritmos cuánticos y un sistema de almacenamiento donde alojar los resultados de los nuevos algoritmos para su análisis y validación. Esta adquisición es posible gracias a fondos acercados por la Agencia Gallega de Innovación de la Xunta de Galicia y por la UE, en el marco del Eje REACT UE.

El MINISTERIO DE DEFENSA adjudica a EPICOM un contrato de 29 millones de euros para hacer ciberseguras sus comunicaciones

La compañía española **Epicom,** propiedad de **Duro Felguera** (al 60%) y de la **Sepi** (al 40%) ha ganado un contrato del **Ministerio de Defensa,** de 29,4 millones de euros para suministrar equipos criptográficos durante los próximos seis años. Se trata de unos equipos vitales para disponer de la máxima seguridad en las comunicaciones e intercambio de información y datos. En concreto, irán destinados a mejorar la ciberprotección de la denominada Infraestructura Integral de Informacion para la Defensa (I3D), que precisa las tecnologías de cifrado, autenticación y generación de claves para su funcionamiento óptimo. Como se sabe, la I3D es una infraestructura de comunicaciones para el despliegue e integración de diferentes sistemas que forman parte del Sistema de Mando y control Nacional. De hecho, Defensa ha destacado que esta adquisición permitirá proteger los circuitos de comunicaciones de voz y datos seguras en la red de telecomunicaciones de la I3D.

El contrato ha sido materializado en un acuerdo marco que permitirá adquirir los equipos conforme se vayan necesitando.

La compañía también resultó adjudicataria de otros tres contratos, a finales de 2022, para la actualización de cifrados de servicios y nuevos equipos para ello, para el **Estado Mayor de la Defensa** (EMAD) y el **Ejército de Tierra**, por valor de seis millones de euros.

Es la única empresa en España que garantiza la protección de la información hasta el 'nivel secreto' y sus equipos están desplegado en departamentos críticos de **Presidencia, Asuntos Exteriores y Defensa.**

BREVES

■ Como hace regularmente **Revista SIC,** en marzo, publicó una nueva actualización del cuadro de CSIRT y CERT con presencia en España, ofrecido a través de Revistasic.com. Como principal novedad destaca que **Enisa** ha comunicado que está actualizando el listado que tiene en este ámbito y que ha entrado a formar parte del foro **First** el BE-SOC de **BeDisruptive.** No hay nuevas incorporaciones nacionales ni en **Trusted-Introducer**, ni en **CSIRT.es**.

■ En el marco de **C1b3rwall,** la **Policía Nacional** continúa fomentando la ciberseguridad en la red entre estudiantes y docentes a través de 'Junior Esports'. Se trata de un proyecto educativo y tecnológico dirigido especialmente al ámbito *gaming* el que participan centros escolares de toda España con jóvenes de entre 12 y 18 años. En este proyecto, agentes de Policía Nacional informarán sobre los riesgos y del mal uso de la red y de los videojuegos.

■ Se ha presentado la 'II Guía práctica para la gestión de brechas de datos personales', realizada por el **Data Privacy Institute,** en su XV Foro de la Privacidad. "El momento actual que vive la privacidad, con cambios normativos de calado tras la llegada de la Directiva NIS2 o el reglamento DORA, aumentan el impacto de las nuevas tecnologías donde la Inteligencia Artificial y su ChatGPT acapara todas las miradas", destacaron los ponentes en muchas de sus intervenciones. Además, durante el evento se dio a conocer el nuevo esquema de certificación para empresas encargadas del tratamiento que estará operativo en unos meses y en el que se ha venido trabajando hasta ahora.

■ **Nozomi Networks** ha ampliado su alianza estratégica con **Mandiant** por el cual, esta última, amplió el número de expertos certificados de la primera en su equipo global de respuesta a incidentes de OT y utilizará las soluciones de Nozomi para profundizar en el análisis forense y la evaluación de incidentes. Las compañías también están invirtiendo en una nueva iniciativa que incluirá el intercambio de información sobre amenazas y la investigación conjunta sobre seguridad, y planean introducir la respuesta a incidentes diseñada a medida y programas de evaluación para clientes conjuntos.

■ El distribuidor **Ingecom** ha firmado un acuerdo con **Stellar Cyber** para ofrecer su plataforma, con un motor de inteligencia artificial, y especializada en detección y respuesta frente a ataques. Así su propuesta ofrece una vista integral de toda la red y la infraestructura informática que revela incluso los ataques más complejos. Además, la tecnología de aprendizaje automático de Stellar Cyber aprende patrones de ataque con el tiempo, por lo que se vuelve cada vez mejor para detectar y remediar ataques mientras funciona. La alianza recién cerrada cubre los tres países donde está presente el mayorista: España, Italia y Portugal.

TEHTRIS

FACE THE UNPREDICTABLE

OPTIMUS EDR

Endpoint Detection & Response

TODO INCLUIDO

SIN COSTE ADICIONAL

FUNCIONES *INCLUIDAS*

CTI
(ANÁLISIS AUTOMÁTICO Y EN TIEMPO REAL)
+
SANDBOX
+
INTELIGENCIA ARTIFICIAL
+
PLATAFORMA DE INTELIGENCIA DE AMENAZAS
(THREAT HUNTING Y ANÁLISIS FORENSE)

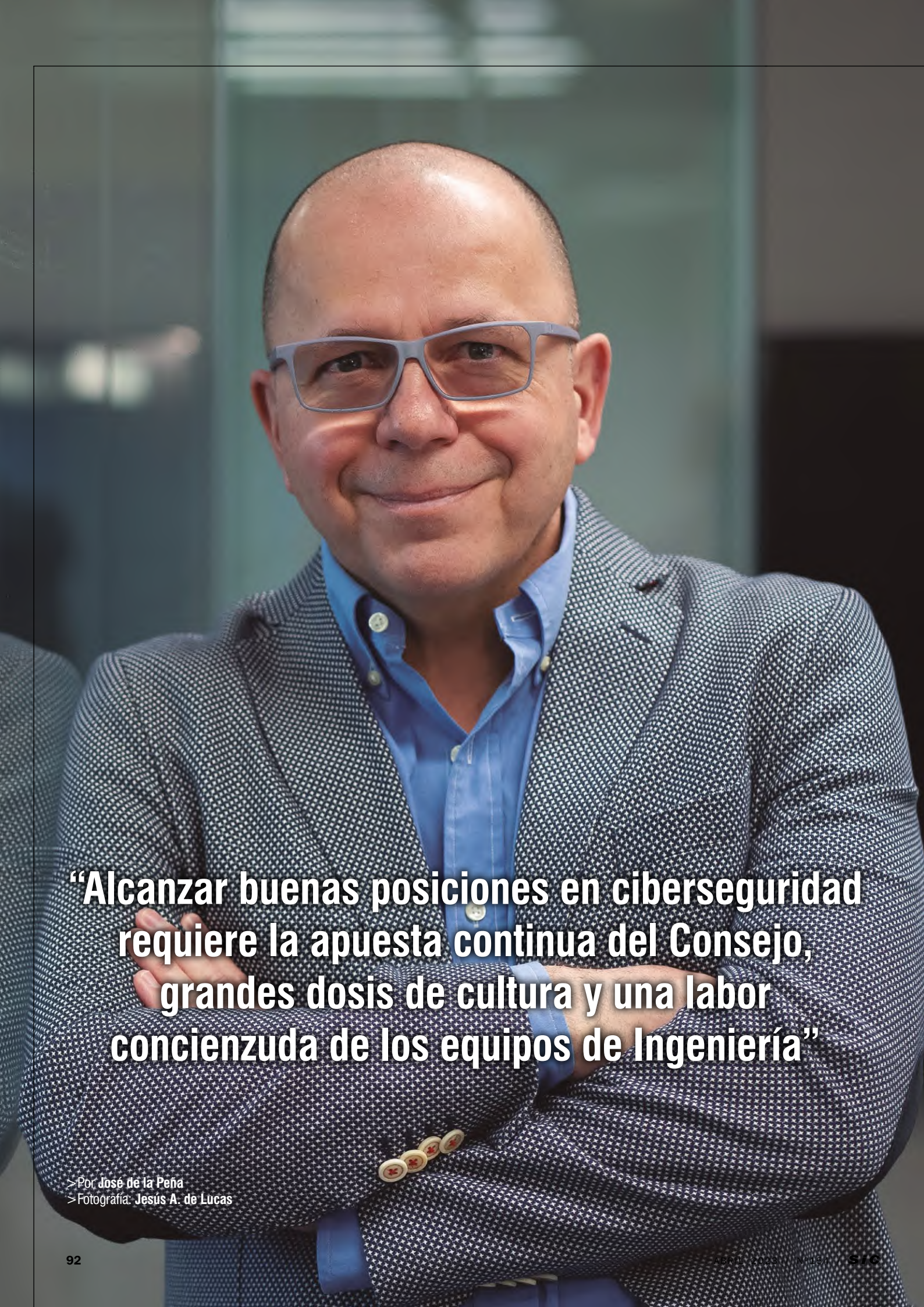
PROTEJA SUS ENDPOINTS
DE FORMA HIPERAUTOMATIZADA

MADE IN EUROPE

afaq ISO 27001 Information Security AFNOR CERTIFICATION 2009/102155

CONTACTE CON NOSOTROS

spain@tehtris.eu
tehtris.com



“Alcanzar buenas posiciones en ciberseguridad requiere la apuesta continua del Consejo, grandes dosis de cultura y una labor concienzuda de los equipos de Ingeniería”

>Por **José de la Peña**
>Fotografía: **Jesús A. de Lucas**

Sergio Fidalgo

CSO Global y CISO Global de BBVA

BBVA sigue siendo una entidad financiera pionera a escala mundial en lo que se refiere a la gestión de la ciberseguridad, que desde hace años está directamente impulsada por el Consejo de Administración, y su presidente, Carlos Torres. En esta entrevista, su actual CSO Global y CISO Global, Sergio Fidalgo, un Ingeniero de Telecomunicaciones con 25 años de experiencia en la entidad, explica cómo está organizada la función en el banco, qué relación guarda con otras y el papel que se le da al factor humano, a la tecnología y a los procesos.

– Antaño tuve la oportunidad de entrevistar a su antecesor en el cargo, Álvaro Garrido. Le voy a formular a usted la misma pregunta que le hice a él: ¿qué hace un ingeniero de telecomunicaciones en un sitio como este? Es evidente que tener a un tecnólogo como CSO Global y CISO Global es un rasgo muy definido de la casa.

– Efectivamente, soy "teleco", y de una promoción anterior a la de Álvaro Garrido. En mi desempeño profesional empecé a especializarme en consultoría orientada a banca, actividad que llevé a efecto en, entre otras entidades, BBV cuando todavía no se había fusionado con Argentaria. Llevo 25 años en BBVA, y siempre he trabajado en Ingeniería. Cuando mi antecesor dejó su posición, y ante la necesidad corporativa de cubrir el puesto, desde el banco se consideró que yo era una persona de Ingeniería con un perfil más sensible a la seguridad que otros directivos del área.

– ¿Por qué?

– En los siete años anteriores a mi nombramiento como CSO y CISO Global me tocó proteger SWIFT, la infraestructura tecnológica más crítica de todos los bancos. En ese periodo hubo un par de ataques, uno de ellos al Banco Central de Bangladesh en el año 2016, y a partir de ahí, toda la banca se puso las pilas. Ese período, precisamente, me tocó a mí pilotando la infraestructura de SWIFT. Ciertamente, sí que soy sensible a la ciberseguridad.

Por otra parte, como llevo muchos años en BBVA, quizá se haya valorado también mi capacidad para gestionar a los *stakeholders* a todos los niveles de la organización. Los conozco, me conocen, y saben que les cuento la verdad.

– Desde que lleva ejerciendo su actual cargo, ¿ha cambiado su visión de la gestión de la ciberseguridad?

– No demasiado. Eso sí, conozco más de cerca las amenazas y los riesgos asociados a nuestro sector y a nuestra compañía. Lo que no deja de sorprenderme es el dinamismo, la variabilidad y la volatilidad de la evolución de las amenazas. Aquí cada semana hay algo diferente en materia de fraude, seguridad, ataques, vectores de ataque… Si llega el miércoles y no se ha descubierto algo nuevo, hay que preocuparse.

– BBVA ha sido siempre una entidad financiera pionera en materia de gestión de la ciberseguridad. ¿Cómo la organizan actualmente?

– El departamento que dirijo se llama Corporate Security, y en él se plasma la visión holística de la seguridad de BBVA, en la que ocupa un papel muy significativo la ciberseguridad.

Una vez que, a mi llegada, redibujamos la estrategia, decidimos conceptualizar cuatro verticales de protección, que son cada una de las líneas que tenemos para proteger cuatro tipos de activo. En primer lugar, los activos digitales: nuestra infraestructura tecnológica, nuestros programas, nuestro software, nuestro código… Es la Ciberseguridad: descubrimiento de ataques, defensa, test de penetración,…

El siguiente activo objeto de protección lo integramos en Data Security, básicamente nuestros datos y los de nuestros clientes.

El tercer activo objeto de protección lo forman las personas y los activos físicos, que es lo que llamamos Seguridad Física.

Y el cuarto frente es consecuencia de los ataques que puedes recibir en las tres primeras, y se orienta a la protección de nuestro dinero y el de nuestros clientes. Me refiero a la gestión del Fraude, que representa el impacto monetario que pueden producir estos ataques.

Además de disponer de una estrategia para cada uno de estos cuatro verticales, tenemos una estrategia común con algunas líneas transversales que tratamos que crucen a los cuatro verticales. Por ejemplo, Inteligencia. Otra es la que afecta a la formación y concienciación de las personas, a cargo de Begoña García, nuestra Global Head People Information Security. Al final, tenemos necesidades de *training* en los cuatro verticales. Por ejemplo, el ámbito de Operaciones está hoy muy centrado en la ciberseguridad, pero también visualizamos que pueda tener aplicabilidad para gestión de Fraude o para la Seguridad Física…

– ¿Cómo dan apoyo organizativo a esta concepción?

– Yo soy CSO Global y CISO Global, y de mi dependen 15 CISOs, organizados en tres tipos.

El primero es el de país. Tenemos uno en cada país en el que operamos: España, México, Turquía, Colombia, Perú, Venezuela, Argentina, Uruguay… Están afectados por el eje regulatorio de su mercado y responden ante sus reguladores locales como responsables de seguridad de los bancos y oficinas locales. También en países en los que no tenemos banco, pero sí oficina, en ocasiones tenemos un CISO, como por ejemplo en Nueva York.

El segundo tipo está formado por los CISOs del *holding*, que son los que se dedican a cuidar el *core* de Ingeniería con funciones corporativas y de *Client Solutions*.

El tercer tipo está constituido por CISOs ubicados en lo que yo llamo las unidades ejecutoras de Ingeniería. Yo vengo de Ingeniería y tengo un perfil de CIO. Y, al final, las palancas para hacer todo lo que el banco necesita en Seguridad, sobre todo en Ciberseguridad y en Data Security, no las tenemos en Corporate Security, sino en los mundos de Ingeniería. Ante esta circunstancia, he situado en dichos mundos a cuatro CISOs en cada una de las cuatro funciones de Ingeniería que verdaderamente tienen que ejecutar la protección.

– Y ¿cuáles son esas funciones?

– Arquitectura, Infraestructura, Desarrollo y Data. Hay un CISO en cada una, de manera que dentro de esas unidades sean los responsables de concienciar a su director de Ingeniería y de accionar

"El negocio de la banca se basa en custodiar el dinero de sus clientes y que estos confíen en ello. Por tanto, desde la perspectiva de negocio, es crucial que se nos perciba como el banco más seguro".

las palancas para que verdaderamente toda la prescripción de medidas de seguridad que hacemos desde mi Unidad, que es pequeñita, realmente se ejecute. En suma: la nuestra es una organización compleja que responde al principio estratégico de seguridad embebida con el que perseguimos que la seguridad esté presente en todos los espacios del banco: en la mente de las personas, en todos los procesos que hacemos y en la tecnología que diseñamos y construimos. Y para llevar a efecto dicho principio, era importante instituir la función de los riesgos de ciberseguridad en desarrollo, en infraestructura, en arquitectura, en Data. El objetivo es que en todas las capas de Ingeniería exista la función de seguridad, y que sean las propias funciones las que tomen conciencia y las que accionen las palancas para gestionarla, asumiéndola como un frente propio.

– Esta concepción trae aromas a DORA...

– DORA entrará en funcionamiento a finales de 2024, y llevamos trabajando desde hace tiempo para ajustarnos escrupulosamente a su cumplimiento. Esta ley se centra en alcanzar resiliencia operativa. Y nosotros ya tenemos una estrategia de continuidad clara, en cuyo marco se desarrollan los planes de continuidad, se diseñan los BRS, se diseñan las estrategias de recuperación, y se testean y prueban.

Ante DORA vamos a diseñar un test de continuidad para saber cómo responde el banco a eventos disruptivos que le puedan generar una pérdida de servicio, estudiar de qué tipo de eventos estamos hablando: disponibilidad del centro de trabajo, disponibilidad de las personas, pandemias, disponibilidad de los sistemas,...Y, ante cada circunstancia, tener estudiada y probada una respuesta. Y en esta sistemática vamos a añadirle escenarios de ciberseguridad. Ya tenemos unos cuantos diseñados.

– ¿Por ejemplo?

– Estamos pensando en ataques de denegación de servicio, *ransomware*, ataques cibernéticos a infraestructuras críticas como SWIFT, directorio activo, ese tipo de cosas. Lógicamente, la respuesta será diferente en función de estos escenarios. La idea es alinearnos con la estrategia de continuidad del Grupo.

– ¿Cómo describiría usted el proceso en virtud del cual tiene lugar la información de ciberseguridad hacia el Consejo de Administración y su conexión con toda la entidad?

– Hay dos vertientes. De una parte tenemos un protocolo de escalado de incidentes que afortunadamente se utiliza poco, porque de momento estamos bastante bien en términos de incidentes relevantes en los últimos años. Y ahí disponemos de unos determinados niveles de escalado que, dependiendo de la criticidad y la gravedad del incidente, van activándose. Hay cosas que no pasan por mí porque son muy leves; otras menos leves de las que sí tengo un conocimiento preciso; el siguiente nivel incluye al CIO y, en la cúspide, está nuestro Presidente y Consejero Delegado.

Nuestro modelo de *reporting* formal se basa en dos órganos. Por un lado, un comité formal en el cual estamos todos los CISOs del Grupo y el CIO Global, José Luis Elechiguerra, que es mi jefe. En este foro se reporta todo lo que tiene que ver con la gestión de la ciberseguridad.

Adicionalmente a esto, tenemos en el Consejo de Administración una Comisión de Tecnología y Ciberseguridad, encabezada por nuestro presidente, Carlos Torres, y que se reúne mensualmente. Fuimos pioneros en tener un órgano así, en el que se ven todos los aspectos relacionados con los riesgos tecnológicos y con los asociados a la ciberseguridad: actualizaciones de amenazas, refinamiento y actualización de estrategias de defensa, programas de protección, incidentes relevantes, los KPI de medición de la seguridad. Todo se reporta con cierta periodicidad en esa Comisión, de manera que no solo el Consejo esté informado, sino que además está concienciado.

He de reconocer que tener en el Consejo de Administración, que es el órgano de máximo gobierno de la compañía, una Comisión dedicada en la cual se discuten con periodicidad los aspectos de ciberseguridad, es una ventaja muy relevante para gestionar este tipo de riesgos.

– BBVA es una entidad muy humana y, al tiempo, con un patrimonio tecnológico orientado al negocio bancario ultramoderno. ¿Cómo desarrollan, mantienen y refinan sus aplicaciones?

-Depende del segmento y del área de negocio. La más visible es por ejemplo nuestra multipremiada app, que ha obtenido cinco galardones consecutivos de Forrester. En este contexto hablamos de un producto que lleva dentro subproductos: el *financial health*, inversiones, gestión de gastos, la operativa transaccional de servicio... Medimos su evolución y tiene un ciclo metodológico de refinamiento y mejora trimestral.

En este frente estamos muy activos en ciberseguridad, ya que la digitalización y las acciones en remoto, además de proporcionar una superficie de contacto mucho más alta con los clientes, acarrea muchos riesgos.

El negocio de la banca se basa en custodiar el dinero de sus clientes y que estos confíen en ello. Por tanto, desde la perspectiva de negocio, es crucial que se

"En el CERT Global utilizamos el sistema Fusión, que básicamente recoge sondas de información, tanto propias como ajenas, tanto internas como externas, de todo lo que ocurre en todas las geografías, en todo el *footprint*. Dicho sistema es una cocreación del banco con Google aprovechando la potente solución de analítica de Chronicle".

nos perciba como el banco más seguro. Además, la seguridad es una palanca para la innovación y la mejora de los servicios. Y un ejemplo es nuestra tarjeta Aqua, cuya propuesta de valor se centra en la ciberseguridad que proporciona. La llevas en la cartera, no tiene números, solo el nombre del titular, no lleva fecha de caducidad ni CVV visible, y el que tiene es dinámico. Y para utilizarla, por ejemplo, en compras por Internet, necesitas la app, que incorpora autenticación biométrica y aporta otro plus de seguridad. Es decir, te está ocultando la numeración de la tarjeta, está ocultando los datos sensibles, no tiene el CVV impreso, por supuesto, y además tiene el CVV dinámico que cambia cada cinco minutos. Este es un círculo virtuoso, ponemos productos seguros y, al tiempo, educamos a las personas en ciberseguridad

– **Es un buen ejemplo de las sinergias que tiene la seguridad por diseño y la actividad de concienciación hacia los clientes y la sociedad.**

– Exacto. Y tiene mucho que ver con nuestro principio de seguridad embebida. Tengamos en cuenta que la seguridad en los procesos digitales es paradójica: tenemos que poner trampas a los malos; pero las mismas trampas que pongo a los malos se las estoy poniendo a los buenos, porque a priori yo no puedo saber quién es malo y quién es bueno. Hay que ser muy precisos para detener a los malos, a la vez que permitimos a nuestros clientes realizar sus gestiones bancarias sin fricción.

– **BBVA es una entidad pionera en la incorporación de mecanismos biométricos para autenticación de clientes en sus procesos digitales. De hecho, hace tiempo que invirtieron en la compañía especializada Veridas, que tiene unas soluciones muy interesantes, y, por cierto, reconocidas por SIC en sus Premios de 2022. ¿Van a desplegar biometría para los usuarios internos?**

– Soy muy partidario del uso de la biometría, porque nos está demostrando que guarda un gran equilibrio entre la gestión de los riesgos de fraude asociados a la autenticación y la comodidad de uso. El modelo de usuario y contraseña es débil y complica la vida a empresas y personas por tener que forzar periódicamente su cambio. Y seguir así no es modernizarse y mejorar.

Para evitar esto, ideamos una línea estratégica en BBVA, previa a las legislaciones existentes, denominada MFA Anywhere (Multi Factor Identification Anywhere), y que consiste básicamente en implantar doble factor de autenticación por todos los sitios por donde podamos: dentro de la red, fuera de la red, para accesos, accesos remotos,… Y dentro del doble factor, nos encontramos con SMS, OPT, correo de confirmación…, que son 'craqueables' con relativa facilidad.

El siguiente paso ha sido ir a la biometría, que tenemos muy implantada en clientes para autenticación y firma de operaciones. Y en el capítulo de empleados, estamos avanzando. Ahora mismo, en España por ejemplo, para conectarte a la infraestructura de BBVA desde una red que no sea local, pedimos biometría. Es verdad que todavía mantenemos algún modelo de autenticación paralelo por OTP, por correo, etc., pero al final pedimos biometría y para mí la estrategia es seguir avanzando en su utilización en clientes y empleados, como el modelo más robusto de autenticación disponible. Cada vez funciona mejor y, en nuestra experiencia, los ratios de fallo son ya muy bajos.

– **Antes he comentado que BBVA es una entidad muy humana, al tiempo que tecnológica. Vamos a lo primero: ¿por qué le dan tanto valor al factor humano?**

– Como dijo recientemente el general estadounidense Keith Alexander, director de la NSA, esto va de colaboración y personas. Nuestra práctica orientada a la cultura de ciberseguridad en personas es bastante madura. La conceptualizamos en cuatro anillos concéntricos: el de mi equipo de Corporate Security, que lo formamos unas mil personas en el Grupo. Nuestra pretensión es estar continuamente formados, reciclados en base a las certificaciones adecuadas y actualizados en el conocimiento de amenazas. El siguiente anillo es el de los empleados, en el que incluimos a todos los empleados, desde la alta dirección hasta el resto, ya sean de la red, de servicios centrales… En total, unas 115.000 personas. Usamos todo tipo de recursos formativos: cursos obligatorios, conferencias, seminarios. Con talleres hemos llegado a 75.000 personas. La verdad es que el concepto de ciberseguridad está muy asumido.

Ya no hacemos ejercicios de engaño con USB porque tenemos "capado" el puerto en los PC. Pero sí los hacemos de *phishings* cada vez más sofisticados. Y vemos una clara mejoría en la respuesta de nuestros empleados. La resistencia al

"He de reconocer que tener en el Consejo de Administración, que es el órgano de máximo gobierno del banco, una Comisión dedicada a Tecnología y Ciberseguridad en la cual se discuten con periodicidad los aspectos de ciberseguridad, es una ventaja muy relevante para gestionar este tipo de riesgos".

engaño hace tres años era del 90%, y hoy es del 98%.

El tercer anillo es el de los clientes. No podemos eliminar las amenazas de la ciberdelincuencia y los defraudadores, pero sí dotarles de herramientas para combatirlos: mensajes de aviso y alerta, vídeos y piezas informativas, formación, capacidad para apagar y encender sus tarjetas ante situaciones de riesgo… Y acabamos de firmar una alianza con Google para formación en ciberseguridad de pymes en España.

El cuarto anillo es el de la sociedad. Tenemos una alianza con la plataforma Coursera en virtud de la cual somos la primera entidad financiera que ha puesto a disposición de la sociedad cursos de ciberseguridad para la gente, los mismos que hacen nuestros *managers*. Las personas los pueden seguir gratuitamente. Ya los han realizado más de 15.000 personas.

– ¿Cómo tratan la ciberseguridad en su cadena de suministro?

– Es un asunto complejo, hay que conseguir que todos los eslabones de la cadena presenten los mismos (altos) estándares de seguridad, utilizando el principio de confianza cero. También exigimos a algunos proveedores que ciertos empleados tengan formación en ciberseguridad. Y estamos colaborando con ENISA en un esquema de certificación para proveedores de servicios de nube, porque hoy la infraestructura *cloud* es uno de los ejes más potentes de entradas no autorizadas.

– La nube. Ustedes han sido muy madrugadores en el uso de herramientas colaborativas en la nube de Google.

– Es cierto. Y es un orgullo. Sucede que como BBVA tiene una nada despreciable dispersión geográfica, hemos de gestionar la visualización que de la nube hace cada regulador.

Nos dimos cuenta pronto –sobre el año 2011– de que la *cloud* tenía unas ventajas espectaculares para el sector bancario. En realidad para todos los sectores. Para nosotros presenta ventajas desde el punto de vista de flexibilidad, de integrabilidad, de costes, de agilidad. Pero claro, la otra cara de la moneda es la seguridad que hay que ponerle a toda esa agilidad. De lo que se trata en este entorno es de tener el talento necesario para poder utilizar las herramientas que los proveedores de calidad de *cloud* dan.

– ¿Qué opina de la cobertura mediante pólizas de seguros de daños causados por cibertaques?

– Los seguros están para cubrir riesgos y, como tal, la ciberseguridad es un riesgo más. Desde el punto de vista de una empresa, sí que es positivo tener una póliza de ciberseguro. Con respecto a la polémica del *ransomware*, esa es una discusión muy complicada.

Sea como fuere, y pese a que las aseguradoras están trabajando en un territorio inexplorado desde el punto de vista actuarial y muy cambiante, creo que en su sector tienen que apostar por la cobertura de muchos riesgos de ciberseguridad y crear modelos consistentes. Es un ámbito de actividad y negocio que va a evolucionar mucho en los próximos años.

– Operación de la ciberseguridad. ¿Cuántos SOC tiene BBVA?

– Nuestro concepto de SOC o CERT es, a efectos geográficos, híbrido. Tenemos un CERT Global 24X7 en Madrid. Brindamos servicios de protección, prevención y respuesta ante amenazas de dos tipos: de un lado, las globales, es decir las poco dependientes de la geografía; y de otro, las que sean suficientemente sofisticadas como para que otros CERT no dispongan de la capacidad para responder a ellas.

Pero además de ese CERT Global, disponemos de otros más apegados a las geografías en donde se ejecutan las operaciones bancarias.

La estrategia, el método, los KPI de medición, los acuerdos de nivel de servicios, las contrataciones, están dirigidos por el CERT Global, y los territoriales se encargan de la implementación de la estrategia.

"La seguridad en los procesos digitales es paradójica: tenemos que poner trampas a los malos; pero las mismas trampas que ponemos a los malos se las estamos poniendo a los buenos, porque a priori yo no puedo saber quién es malo y quién es bueno".

– Todo esto que comenta forma parte de un activo muy importante de BBVA, que es un activo de datos y conocimiento. Supongo que mantienen ustedes un inmenso lago de datos, o una red de lagos.

– Sí. En el CERT Global utilizamos un sistema que se llama Fusión y que básicamente recoge sondas de información, tanto propias como ajenas, tanto internas como externas, de todo lo que ocurre en todas las geografías, en todo el *footprint*. El sistema está prácticamente desplegado. La ventaja es haber llegado a un acuerdo con Google para, utilizando toda la potencia de la ciberseguridad de Chronicle, cocrear un magnífico producto de analítica de datos orientado a la ciberseguridad.

– Una última cuestión: ¿tiene usted relación con los trabajos relacionados con la investigación de blanqueo de capitales?

– Ese es el lugar en el que se cruzan todos los caminos. La ciberdelincuencia, el fraude y el blanqueo de capitales son actividades muy relacionadas, y todas con el objetivo único de causar perjuicio al banco o a nuestros clientes. Aunar esfuerzos en la prevención y monitorización de estas actividades es muy relevante y en BBVA lo tenemos muy presente, colaboramos estrechamente entre las áreas que protegen al banco de los tres tipos de amenaza. ■

Los CISO ante la encrucijada regulatoria: cumplir sin dejar de proteger

Vivimos tiempos en los que se empieza a cerrar el círculo de la presión regulatoria asociada a la gestión de riesgos de seguridad de la información, ya desde la perspectiva específica de esta actividad y práctica, ya en una orientación encaminada a su contribución a la resiliencia operativa en la que empieza a tener protagonismo la cadena de suministro. Diríase que nada va a escapar a los marcos normativos inspirados en la ciberseguridad por diseño en componentes, productos y servicios, que en su mayoría estarán sujetos a evaluación y certificación.

Los responsables de ciberseguridad –regulados (esenciales, importantes…) y no regulados directamente–, tienen por delante el desarrollo de una tarea titánica. Y parte de ese trabajo consiste en poner todo de su parte (en lo que les toca) para llevar a sus organizaciones por la senda del cumplimiento normativo.

A tenor de esta circunstancia, la Revista SIC ha formulado a cerca de 100 CISO, la siguiente pregunta:

Con las regulaciones actualmente existentes (NIS2, DORA, ENS…), ¿es más fácil o no ser CISO?

* Es posible obtener una versión en pdf de este especial rellenando el formulario disponible en www.revistasic.com

CISOs

ACENS

Fernando Serrano
Responsable de Seguridad Corporativa, Calidad y Procesos

"En mi opinión, estas regulaciones refuerzan el papel del CISO dentro de las compañías, y por tanto creo que facilitan su labor, eso sí, aumentando su responsabilidad y aumentando la carga de tareas y retos que supone su cumplimiento. Desde mi punto de vista, el cumplimento de estas regulaciones son una palanca para justificar inversiones y cambios por lo que son motivos que ayudan concienciar y convencer a la alta dirección de la importancia de tener una adecuada gestión de la seguridad".

ADIF

Mª del Mar de la Fuente Sedano
Subdirectora de Seguridad en la Información

"Sin lugar a duda, la regulación ayuda a impulsar los programas de ciberseguridad en las organizaciones, así como afrontar una transformación digital segura. No obstante, la regulación en ciberseguridad es un reto importante para el CISO y muchas veces resulta complicado adaptarse a los numerosos cambios normativos y tener los recursos suficientes para realizar el cambio. En el contexto actual de incertidumbre, con entornos cada vez más interconectados, donde los desafíos y retos en ciberseguridad son cada vez mayores, es relevante disponer de un marco regulatorio europeo común para proteger nuestras redes y sistemas, mitigar las amenazas y garantizar la continuidad de los servicios ante incidentes con el fin de proporcionar un entorno digital confiable."

AGENCIA DE CIBERSEGURIDAD DE CATALUÑA

María José Martín
SOC Manager

"Si bien el cumplimento normativo supone un reto para las entidades, las nuevas regulaciones son una palanca clave para reforzar y legitimar sus capacidades de prevención, detección y respuesta ante incidentes, bajo un marco de referencia común. El desafío para los CISOs es acertar en la priorización de las medidas esenciales para hacer frente a las principales amenazas, comunicar más y mejor y aferrarse a la innovación".

AGENCIA DE CIBERSEGURIDAD DE CATALUÑA

Tomás Roy Catalá
Director

"Absolutamente sí, si se tiene la aproximación pragmática de 'Cybersecurity as Regulation', es decir el cumplimiento no es algo externo, un ejercicio más de 'Estado Actual – Estado Deseable'. El cumplimiento es un facilitador del estado deseable desde el diseño del modelo de ciberseguridad, y su seguimiento es la operación misma de ciberseguridad. Hay que priorizar modelos de cumplimiento que faciliten acciones de transformación, contra las que dificultan o son multiversos del AS IS-TO BE".

AIRBUS

Pedro Díaz-Cuadra
National Information Security Officer

"Las normas son una ayuda para una gestión ordenada y completa de la seguridad. Sin embargo, aunque persigan los mismos fines, a veces contienen requisitos discordantes o complejos de abordar con capacidades y presupuestos realistas. El conjunto normativo no siempre asienta un marco coherente, integrado, estable y con evolución predecible. Para nosotros, el cumplimiento de NIS2, CCN, ONS, OTAN, OCCAR, EU, ESA, ISO, CMMI (NIST), ISO, ITAR/EAR, RGPD, etc., se traduce en un trabajo realmente arduo".

ALMIRALL

Ramón Serres
Information Security and IT Quality Director

"Dejando de lado la aplicabilidad en cada sector, pienso que estas regulaciones acaban siendo un arma de doble filo. Nos pueden ayudar en cuanto a priorización, a lograr más presupuesto o recursos, a empujar iniciativas que por algún motivo se habían encallado, etc. Pero a la vez, conllevan un seguimiento y una disciplina que corren el riesgo de priorizar el enfoque al cumplimiento por encima del enfoque al riesgo. Y eso, en mi opinión, es contrario a la misión del CISO".

AUTORIDAD PORTUARIA DE VALENCIA

José Fernández Zapata
Responsable de Seguridad de la Información y Cumplimiento Normativo

"Las actuales regulaciones en materia de ciberseguridad y resiliencia van aportando cada vez mayor relevancia a la figura del CISO, definiendo tanto sus funciones como su posición dentro de la organización. Esto supone una ayuda para poner en valor su función y conseguir una adecuada relevancia dentro de la estructura organizativa. Sin embargo, la concienciación de la directiva en esta materia y su apoyo al CISO no se consiguen con un marco normativo, por mucho que éste pueda aportar algo de luz, sino que depende mucho de la cultura y la visión que emana de la

cima de la organización (el denominado frecuentemente como "tone of the top"). Por otra parte, en ocasiones se percibe una cierta desconexión entre los legisladores y la realidad del panorama empresarial, tratando de imponer medidas que no siempre son realistas, no están al alcance de determinadas compañías o no se adecuan completamente a un balance coste-beneficio. Este tipo de situaciones dificultan la labor del CISO, que frecuentemente encuentra resistencia para la implantación de determinadas medidas en las cuales es difícil alinearse tanto con la parte organizativa como operacional de la empresa".

AVATEL TELECOM

Adrián Quirós Godoy

Responsable de Ciberseguridad

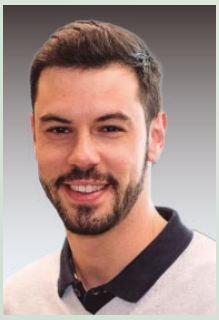
"La existencia de regulaciones y estándares con tanto impacto en Ciberseguridad beneficia significativamente a los CISOs y simplifica su trabajo. Proporcionan una guía clara y específica sobre las políticas y prácticas de seguridad que deben implementarse. También ayudan a establecer un marco útil para la seguridad de la información, lo que permite priorizar los riesgos y justificar las decisiones ante la alta dirección, donde resalta la necesidad de invertir en Ciberseguridad".

BANCA MARCH

Javier Gayoso

CISO

"Las últimas regulaciones vienen poco a poco a acercarse a la realidad de la situación actual de la ciberseguridad y pasar del concepto de simple protección a un concepto más amplio de ciber resiliencia. Esto nos ayuda a poder mover más palancas internas tanto para cumplir la regulación como para aumentar de manera más rápida nuestro nivel de madurez en ciberseguridad. Este acercamiento a la realidad actual ayuda a la figura de CISO, pero no la hace más fácil. Si, además, tenemos en cuenta el aumento exponencial de las amenazas y la sofisticación de estas en un mundo cada vez más digital y tecnológico (arquitecturas abiertas, cloud...) hace aún más difícil y estresante la figura del CISO".



BAUHAUS ESPAÑA

Sergio Juárez Calvo

Responsable de Seguridad de la Información

"Las regulaciones y los marcos de referencia siempre son de ayuda para estandarizar y mejorar las formas de trabajo. En cuanto a la seguridad de la información se refiere, estas leyes y estándares deberían enfocarse cada vez más en concretar qué controles de seguridad se deben implementar, especialmente en el caso de las leyes, que en ocasiones generan confusión, y denotan poco estudio de las limitaciones técnicas que nos podemos encontrar las organizaciones cuando deseamos implementarlas."

BANCO DE ESPAÑA

Sergio Padilla Foubelo

RSI y Responsable de Riesgos y Seguridad de la Información

"La regulación es una palanca de enorme valor que el CISO ha de saber aprovechar como una oportunidad para facilitar su labor. A pesar de que la normativa existente aumenta la presión en este rol, porque supone nuevas exigencias, también pueden ayudar a justificar la inversión en ciberseguridad. Por otro lado, dado que hay aspectos comunes en las distintas normas, el CISO ha de buscar sinergias para ser más eficiente en el cumplimiento normativo."

BANCO SABADELL – SABIS

Adolfo Hernández

CISO

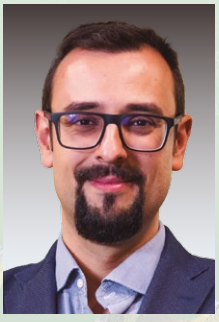
"No estamos acostumbrados a que la regulación proporcione un marco efectivo para la gestión de la seguridad. No es el caso de los últimos paquetes regulatorios que han visto la luz, ya que proporcionan un marco de medidas de protección reales, habilitan la compartición de inteligencia, apuntalan la gestión de incidentes, obligan a considerar la ciberseguridad como un elemento base en la toma de decisiones, empujándonos hacia una aproximación basada en riesgos, y empoderando, en definitiva, la figura del CISO".

BBVA

Juan Francisco Losa

CISO España

"Un marco regulatorio adecuado sin duda sirve de ayuda a la hora de impulsar iniciativas de ciberseguridad. Dicho esto, la falta de armonización actual complica la gestión de las mismas y su aplicación práctica en el día a día. Creo que será cuestión de tiempo que ocurra esta convergencia, necesaria para poder ser más eficaces y poner el foco en lo importante que es incrementar progresivamente el nivel de ciberseguridad en las compañías".



BUPA

Iván Sánchez López

Group Chief Information Security Officer

"Lo cierto es que el área de Seguridad lleva años soportando una carga de trabajo y presión cada vez mayor en el ámbito operacional pero especialmente en el regulatorio.

CISOs

Hacernos la vida más fácil o más difícil no pasa ni por más ni por menos, sino por mejor regulación. Debemos trabajar en un modelo regulatorio mínimo que, a la vez, aporte el máximo valor y sobre todo que haga entender a las organizaciones la necesaria correlación entre el cumplimiento de la regulación y la inversión dedicada para su cumplimiento. Sin los recursos adecuados, sin duda la labor del CISO será mucho más difícil".

CAF

Zigor Arosa

Responsable de Ciberseguridad IT Corporativo

"La función del CISO se está complicando junto con la digitalización de los procesos, productos y servicios. A mayor digitalización, mayor la exposición a las amenazas. Además, el CISO ha pasado de ser un rol técnico, a tener que conocer muy bien el negocio para alinear las estrategias. De todas formas, hay que reconocer que el impulso que se le está dando a la ciberseguridad a través de nuevas directivas está ayudando a incrementar la concienciación a todos los niveles y esto es una palanca que debemos aprovechar para la mejora de las medidas de seguridad, así como para dimensionar adecuadamente los equipos y recursos".

CAMPOFRIO

Jesús Alonso Murillo

CISO Europa

"Con las nuevas regulaciones, NIS2, ENS, y otras, sin duda el trabajo del CISO estará más regulado, y 'aterrizado', dado que, con la facultad de inspección aleatoria por parte de los organismos públicos, se podrá revisar temas como la gestión de incidentes, continuidad de operaciones, seguridad de la cadena de suministro, y uso de mecanismo de autenticación, entre otras. Esto, unido a las nuevas actividades, catalogadas como esenciales, más allá de las históricamente reguladas, dentro del sector financiero, supondrá el punto crítico, que hará, por fin, que las compañías se tomen en serio la Ciberseguridad, y el cada vez más crítico rol del CISO, más allá de "as a service", sino como un rol esencial, dentro del comité de dirección de las compañías".

CACEIS BANK

Eva Puerta Pérez

CISO

"¿Ha dicho alguien ya que ser CISO consiste, esencialmente, en tratar de ordenar el caos? Un día cualquiera hay que revisar un fallo en los sistemas de detección, 'securizar' infraestructura de forma urgente, evaluar un proyecto nuevo y, además, hay una nueva oleada de *ransomware* en el sector. La regulación ayuda a poner orden en este caos y a priorizar los puntos que exige la normativa. Implica más trabajo, pero son tareas que están enfocadas al objetivo final: proteger la seguridad de la información".

CECABANK

Ricardo López Lazaro

Director de Riesgo No Financiero y Cumplimiento

"Soslayando la carga del trabajo que representa la intensidad regulatoria que en el ámbito de la ciberseguridad venimos experimentando los últimos años, desde el punto de vista del CISO la regulación es un apoyo innegable, en tanto que establece directrices comunes y favorece la disponibilidad de recursos en las entidades. No es menor la importancia que en ese sentido tiene la regulación emergente como DORA, que hace extensiva la aplicación de obligado cumplimiento a ámbitos como la cadena de subcontratación y que determina la responsabilidad en materia de ciberseguridad de los Consejos de Administración".

CENTRO MUNICIPAL DE INFORMÁTICA – CEMI (AYTO. DE MÁLAGA)

Juan García Galera

Responsable de Seguridad de la Información
Delegado

"Las regulaciones existentes pueden facilitar las labores del CISO puesto que ponen en valor la figura, funciones y responsabilidades del CISO en la alta dirección. Estas normas intentan armonizar y unificar criterios a la hora de gestionar la seguridad, desde la gobernanza hasta la gestión y notificación de ciberincidentes. Por último, el CISO debe tener apoyo real de la alta dirección para que la seguridad se gestione dentro de unos niveles acordes al apetito al riesgo TIC de la organización".

CENTRO VASCO DE CIBERSEGURIDAD – BASQUE CYBERSECURITY CENTRE (BCSC)

Javier Diéguez Barriocanal

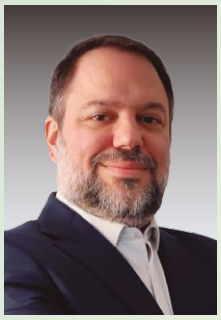
Director

"Si el esquema se limita a la aplicación de la regulación, sin mecanismos de acompañamiento (PYMEs), la persona CISO se refugiará en una estrategia de puro cumplimiento que evite las sanciones, que proteja su posición en la organización y que contenga el volumen del presupuesto dedicado a las medidas a desplegar, pero no responderá a las necesidades reales de resiliencia del negocio. El panorama regulatorio, siendo necesario, solo ayuda al (a la) CISO si hay buena coordinación entre normativas".

CISOs

CEPSA
Rafael Hernández González
CISO Global

"Las regulaciones que nos llegan vienen desde organizaciones o entes que ven la ciberseguridad como un riesgo no tratado por las empresas y por lo cual dictan unas normas que desde la lejanía y desde la generalidad quedan muy bien pero que luego es difícil de ejecutar en muchos casos. Otro factor importante a tener en cuenta es que cada vez más nuestro trabajo está ligado a entornos multinacionales donde se aceptan y se cumplen las normas internacionales, pero cuesta mucho más hacer entender las locales. El mundo global cada vez nos dicta más nuestro trabajo. El factor de la *cloud* hay que tenerla en cuenta. Creo que estas regulaciones deben de adaptarse a este escenario que ya no es nuevo, sino que es el que hay. En este punto creo que no se están enfocando de modo correcto estas normas. Las regulaciones deberían de ayudarnos a transmitir el valor de nuestra función, a que nuestras direcciones las vieran de utilidad para desarrollar productos y servicios más seguros y como empoderamiento de la función. Pero en la mayoría de los casos esto no se cumple y se ve más como una nueva carga administrativa y documentalista. Por lo tanto, ser CISO regulado es más difícil y aburrido".



CHANNELADVISOR
Juan Manuel Bahamonde
CISO Global

"Todas las regulaciones que en los últimos años se están implantando apoyan indudablemente directa o indirectamente la función del CISO, reforzando la importancia de la seguridad dentro de la propia empresa y en nuestra relación con terceros, y por ello, de manera general haciendo más fácil nuestro trabajo, aunque, los requisitos técnicos, operativos y organizativos asociados a cada regulación, impliquen una inversión de tiempo y recursos, y puedan añadir complejidad a algunos procesos".

CINTRA
Gonzalo Martínez Rioja
CISO Europa y Nuevos Mercados

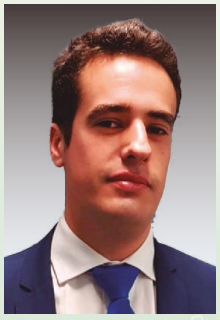
"La regulación actual es cambiante y creciente, lo que supone mayor complejidad y obliga al CISO a mantenerse actualizado y a ajustar regularmente su entorno de control. Además, las regulaciones son grandes devoradoras de tiempo y pueden reducir la capacidad del CISO para abordar otros proyectos. Por otra parte, resultan herramientas valiosas para debatir con la Dirección, obtener recursos e introducir capacidades que mejoren el "posture" de seguridad. Haciendo balance y 'mojándome', me quedo con un entorno regulado".

CIRSA
Daniel Puente Pérez
CISO Global

"Por desgracia la facilidad o dificultad no viene únicamente condicionada por las regulaciones y marcos normativos existentes, pero es cierto que pueden ayudar a visibilizar aún más la necesidad de seguridad a ojos de otros niveles decisorios en las compañías. La existencia de regulaciones dota de una mayor importancia a la materia en cuestión y hace que se deban dedicar esfuerzos extras para cumplirlas. Aunque no debemos llevarnos a engaños y tener claro que estas regulaciones muchas veces marcan unos mínimos, no los niveles deseados que a día de hoy son necesarios para sentirse algo más seguros".

CLARKE, MODET & CO
Jesús. R. Abascal Santamaría
CISO & IT Business Partner

"En mi opinión, con las regulaciones actuales como NIS2, ENS o DORA, no es más fácil ser CISO que antes de su existencia. Aunque estas regulaciones destacan la figura del CISO y proporcionan un marco legal y de seguridad que le ayuda a tomar decisiones más sólidas, también aumentan la complejidad de su trabajo. El CISO tiene que actualizarse constantemente con los cambios legislativos y asegurarse de que su organización cumple con los requisitos específicos de cada regulación".



CLOUD WORLWIDE SERVICES
Eduardo López Ruano
CISO

"La regulación en materia de seguridad tiene una gran relevancia en el cambio de las organizaciones, siendo un gran impulsor en la modernización de procesos antiguos y no eficientes. Esto se debe, en mi opinión, a que estas normas, regulaciones y buenas prácticas sirven como guía a los departamentos de Seguridad a la hora de implantar mejoras. También son útiles como medida de concienciación para departamentos fuera del mundo IT o resistentes al cambio, al provenir de organismos oficiales nacionales e internacionales, y como aspectos diferenciadores a nivel comercial en caso de empresas o aplicaciones certificadas".

CISOs

CMI – CORPORACION MULTIINVERSIONES

Rafael Parra

Director de Ciberseguridad y Riesgos TI

"La regulación ayuda a establecer mínimos exigibles en la industria, objetivar niveles de riesgo y mover la aguja interna de la organización. No obstante, existe el riesgo de apalancarse excesivamente y transmitir a la compañía que el riesgo principal es la falta de cumplimiento, cuando está muy lejos de esta realidad. El verdadero reto sigue siendo hacer entender la importancia de estas medidas más allá de la regulación, enfatizando la ganancia operativa que suponen a medio-largo plazo".

EDP ENERGÍA ESPAÑA

Arturo Eloy Díaz Rodríguez

Jefe de Seguridad Lógica

"Creo que en líneas generales va a ser más complicado debido al incremento de los controles, informes, notificaciones, sanciones y la extensión de responsabilidad a la dirección, por lo que todo ello obligará al CISO a ser todavía más consciente de su responsabilidad para hacer ver a la dirección la importancia de la ciberseguridad. También confío en que pueda servir para que las empresas sean conscientes de que la seguridad es una responsabilidad compartida: dirección y empleados, y no solo función del CISO y los equipos de seguridad".

EMASA

Pedro Mª Galdón Conejo

CISO

"Las regulaciones en materia de ciberseguridad persiguen la creación de un marco y una estrategia común de ciberseguridad, lo cual ya es un hecho positivo. El presente es digital y el futuro lo será mucho más, por lo que el cumplimiento de todas estas normativas va a requerir del CISO mucho más peso en las organizaciones. Las normativas establecen que la ciberseguridad en las empresas es una obligación, lo que para mí las convierte, a priori, en aliadas del CISO".

EMASESA

Alfonso López-Escobar Beares

CISO

"El trabajo del CISO no es otro, de forma muy simplificada, que proteger los activos de información de la organización. Este objetivo debe ser inherente a la estrategia de la compañía para su propia subsistencia, ya que en un mundo hiperconectado como el actual, estos activos resultan críticos para el desarrollo de la actividad. Desde este punto de vista, la existencia o no de leyes en materia de seguridad de la información en general, y de ciberseguridad en particular, no debería, con carácter general, impactar en la actividad del CISO, más dependiente de otros factores como el estado de digitalización de la propia organización o la evolución de las amenazas cibernéticas. No obstante, es cierto que la existencia de legislación en este ámbito facilita la tarea de trasladar hacia todos los estamentos de la compañía la importancia de adoptar medidas de seguridad adecuadas para la gestión de los ciber riesgos, ya sea por convencimiento (que sería lo deseable…) o, simplemente, por tratarse de una obligación legal. "Dura lex sed lex"; la ley es dura, pero es la ley… y, por tanto, hay que cumplirla".

ESTEVE

Sergi Torres

CISO

"Si bien es cierto que el cumplimiento de las regulaciones incrementa el nivel de presión en el CISO y la organización, cabe destacar que tienen un efecto colateral de concienciación y sentimiento de responsabilidad compartida en la Alta Dirección. Esto hace que la figura del CISO tome más relevancia y facilite la ejecución de sus tareas, ya que la organización es consciente del impacto (no sólo operacional, sino también financiero y reputacional) de no actuar con debida diligencia".

EXIDE TECHNOLOGIES

Rubén Fernández Nieto

CISO

"La aparición de estas regulaciones nos ayuda a empoderar la Ciberseguridad dentro de la empresa, así como a oficializar la figura del Responsable de Seguridad dentro de la misma. Esto por una parte ayuda a que la dirección interiorice cada vez más la importancia de contar con una protección adecuada, y por otra estandariza ciertos controles que implementar por un grupo determinado de empresas, lo que puede ayudar en algunos aspectos, pero a su vez puede suponer todo un reto aplicarlo en ciertos entornos".

FERROVIAL

Juan Cobo

CISO Global

"Las regulaciones constituyen una excelente palanca para mejorar la seguridad de una organización, y más cuando esta organización, bien por convencimiento, bien por ignorancia, vive de espaldas a ésta. En estos

escenarios, ser CISO no es sencillo y la regulación se convierte en un gran aliado, enviando a la organización dos mensajes significativos: el primero, si no crees en la seguridad de forma natural, vas a tener que creer e interiorizarlo por obligación; el segundo, no hacerlo lleva asociadas una seria de consecuencias negativas que, poco a poco, se trasladan directamente a los órganos de decisión y dirección de las organizaciones. En este contexto, el de la regulación como palanca y facilitador, sí que, bajo mi punto de vista, es más fácil ser CISO. Es un aliado natural al que no se le puede decir que no. Y luego ya pensaremos en los aspectos negativos de las regulaciones, que los tienen".

FEDERACIÓN ESPAÑOLA DE BALONCESTO

Javier Criado

Director de IT y Ciberseguridad

"Desde un punto de vista de procesos, los Frameworks de Seguridad establecen unos estándares y herramientas para gestionar y mitigar los riesgos en ciberseguridad, lo cual facilita el trabajo del CISO en materia de definición de estrategia y diseño de ese plan de acción dentro de la compañía. Sin embargo, desde un punto de vista práctico suponen también un esfuerzo de adaptación de procesos y costes que, sobre todo en soluciones con cierta antigüedad, no son alcanzables en el grado de cumplimiento necesario".

FINSA

Antonio Fernandes

CISO

"Las regulaciones son simplemente un reto más en el día a día del CISO, sin embargo, una ayuda para visibilizar su figura dentro de las organizaciones y frente a la alta dirección. Establecer una línea base obligatoria en la ciberseguridad, aunque sea para responder a criterios regulatorios permitirá focalizar en los siguientes pasos de la estrategia de Ciberseguridad. Proteger el negocio es primordial para un CISO, por lo tanto, cualquier apoyo debería ser bien recibido venga de donde venga".

FINTONIC

Enrique Cervantes

CISO

"Lo que viene, conviene", se dice en mi pueblo, donde casi ninguno es CISO, y estoy de acuerdo. Este incremento en la presión regulatoria pone la figura del CISO en valor, incrementa su relevancia en las organizaciones y, en consecuencia, nos debería hacer la vida un poco más fácil. Todo lo demás entra dentro de lo que "viene", así que, junto con nuestros equipos, tendremos que adaptarnos para optimizar nuestro trabajo, no 'retrabajar' aspectos comunes de distintas regulaciones y aprovecharlo".

GENERAL DYNAMICS EUROPEAN LAND SYSTEMS

Mario Trotta Moreu

Information Security Services

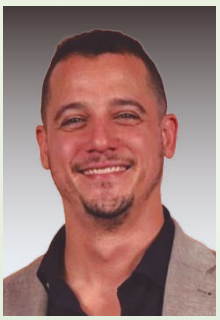
"Las distintas regulaciones ni hacen más fácil ni más difícil el trabajo del CISO. Desde la parte positiva, siempre es bueno tener un claro marco regulatorio que permita a las organizaciones la adopción de medidas para protegerse ante posibles ataques. Estas normas sirven para crear concienciación en materia de ciberseguridad además de fomentar la cooperación entre los distintos actores implicados. Por el contrario, en la parte negativa hay que comentar que el tener más y más regulaciones supone una mayor carga administrativa y financiera para el CISO y el área de ciberseguridad".

GENERALITAT VALENCIANA

Carmen Serrano Durbá

Subdirectora General de Ciberseguridad.
Dirección General de TIC

"Las regulaciones ayudan a los CISO y sirven de apoyo para reforzar su función y conseguir los recursos necesarios. A su vez las normas proporcionan una guía para acometer la adecuación sirviendo como herramienta de planificación y marcando los objetivos. Sin embargo, cuando confluye la obligatoriedad de distintas normas, la complejidad de gestión, hace cada vez más complicada la función del CISO y le pueden desviar del objetivo principal que es velar por la ciberseguridad de su organización".



GESTAMP

José Miguel Parejo

Responsable de Ciberseguridad

"Las regulaciones deben verse como un factor beneficioso y una palanca dentro de la organización, y por ello, impulsa la evolución de las capacidades de ciberseguridad que protegen nuestras empresas. Al ser de carácter obligatorio, éstas suelen disparar inversiones tecnológicas y cambios en procesos de negocio, lo cual fortalece la cultura de la compañía, y a la vez, la creación de empresas más sostenibles y resilientes. Estos aspectos facilitan la tarea del CISO dentro de las empresas".

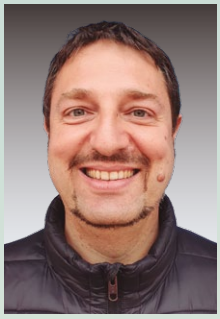
GLOBAL OMNIUM

Juan Luis Pozo

CISO

"La típica pregunta para realizar a un gallego, "depende", aunque mi respuesta es tajante: "es extremadamente difícil". No es cuestión de mirar para otro lado ni negar la evidencia con la que nos encontramos todos los días, es cuestión de

compatibilizar las obligaciones y responsabilidades con la realidad de una Organización sometida a un test de estrés económico-financiero todos los días, y al final el CISO es el responsable legal de aquello que no es posible acometer por recursos y capacidades".



GOBIERNO DE NAVARRA
Roumen Boyanov Katzarov
Jefe de Seguridad tecnológica

"Las normativas son de gran valor dentro de las AA.PP. como apoyo para la función del CISO y su equipo, pero desafortunadamente vivimos un escenario de ciberamenazas capaces de infringir un daño enorme y cada vez mayor. El reto desde nuestro punto de vista de AA.PP. es caminar hacia un marco europeo unificado de ciberseguridad con un único esquema normativo, catálogo de tecnología homologada y un apoyo en la monitorización y respuesta a incidentes por parte del CERT nacional de referencia".

GRUPO ANTOLÍN
Manuel Sánchez Cañada
Cybersecurity & IT Infrastructure Manager

"Para sectores menos regulados, la existencia de normativa de referencia, facilita al CISO acceso a los objetivos de negocio para poder alinear la estrategia de seguridad. Pese a que son regulaciones diseñadas para corporaciones con una mayor exposición al riesgo ciber, sirven como artefactos para impulsar la madurez de la seguridad. Son clave en los ejercicios de concienciación hacia la alta dirección, que debe conjugarse con el punto óptimo de inversión de recursos en base al riesgo".

GRUPO CORREOS
Jesús Mayor Sendra
CISO

"Las regulaciones siempre han sido de ayuda, aunque la realidad es que han ido incrementado la complejidad de nuestro marco regulatorio. Aun siendo una dificultad adicional para el CISO, son una palanca perfecta para corregir aquellos aspectos de la práctica ciber convenientes para minimizar el riesgo dentro de nuestras organizaciones. También es nuestro trabajo convertir esta 'carga regulatoria' en valor para el negocio, identificando las oportunidades que te brinda para crecer y/o visibilizarte".

GRUPO DIA
Enrique Miranda Salado
CISO Global

"Desafortunadamente, no todas las empresas son conscientes del riesgo real al que se enfrentan. A veces, es necesario un "impulso" para tomarlo en serio: o por un incidente grave o por regulación. Si la regulación es el motivo, es posible que se proporcionen más recursos, pero se seguirá viendo como un 'mal necesario', por lo que el CISO no lo tendrá mucho más fácil. Sólo cuando la empresa es realmente consciente, es cuando es más "fácil" ser CISO, si se puede decir que ser CISO alguna vez lo es".

GRUPO NUEVA PESCANOVA
Belén Pérez Rodríguez
Directora Corporativa de Ciberseguridad – CISO

"Las normas actuales, especialmente la NIS2, implican que el perfil del CISO haya cambiado de técnico a gestor, con interlocución directa tanto con la Administración como con la Alta Dirección de las organizaciones. En este sentido, la regulación actual facilita la labor del CISO, pero solo cuando los órganos de dirección de las compañías están implicados, son conscientes de la importancia de la ciberseguridad y entienden la función como una actividad esencial y transversal dentro de la organización".

GRUPO RUBIX
Josep Mangas
Global Cyber and Infrastructure Operations Director

"Independientemente del lugar en la cadena que te encuentres, en nuestro caso como proveedor sin regulación específica, la respuesta es SÍ. El mercado (proveedores y fabricantes) ya está acostumbrado, por lo que se dispone de herramientas a todos los niveles para la implementación efectiva. También ayudan a simplificar el argumentario. Toda la organización entiende de regulaciones en sus respectivas áreas. Además, proporcionan indicadores fáciles de compartir y hacer seguimiento. El único aspecto es que deberían converger en una única regulación paneuropea aplicable a todos los sectores y actividades. Aún sería más fácil".

HIJOS DE RIVERA – ESTRELLA GALICIA
Ana Salazar Díaz
Cybersecurity Manager

"Muchas de las empresas no estamos reguladas o solo aplica a una pequeña parte de los procesos, por lo que tenemos que basarnos en otros tipos de apoyos para hacer esa función nada sencilla de conseguir que nuestra empresa crezca segura. Proyectos de análisis de riesgos a nivel corporativo nos ayudan, permitiendo subir los KPIs de nuestro trabajo a altos niveles. Pero

la velocidad a la que está creciendo toda la digitalización de las compañías hace que participemos en la mayoría de los proyectos estratégicos y además, definamos el *roadmap* de ciberseguridad, calculemos métricas, gestionemos crisis o las creemos con los ciberejercicios. Por lo que fácil, con regulación o sin ella, no es, pero divertido sí. Si no, no seguiríamos en estas posiciones".

HOLCIM
Thomas Frueh
Director Global de Seguridad y Cumplimiento de TI

"Provengo de un entorno regulado y mi trabajo estuvo muy involucrado con PCI DSS. Más tarde, estuve trabajando con BaFin (Autoridad de Supervisión Bancaria Alemana) y KRITIS (área de infraestructura crítica en Alemania). Tengo que decir que esta normativa me ayudó mucho a estructurar mi estrategia y evitar puntos ciegos. Que no se me malinterprete, no siempre fue fácil y algunas cosas no tenían mucho sentido, pero al menos los reguladores iniciaron una discusión con el negocio. En general, creo que esta es una buena manera de influir en la cultura de la empresa".

HOLCIM EMEA
José María Labernia
Head of IT Security and Internal Control
Holcim EMEA Digital Center

"Sí, ya que permite trazar líneas más claras referente a los mínimos a cumplir y las tareas a realizar en el ámbito de la ciberseguridad, de forma objetiva y consensuada por todo el sector. Sin embargo, los CISOs se quedan en una situación más comprometida, ya que requiere de un mayor nivel de cumplimiento y responsabilidad para aplicarlas en tiempo y forma en las organizaciones que estén afectadas, y su aprobación no siempre lleva asociada una dotación presupuestaria para su consecución".

IBERDROLA
José Manuel Alonso
CISO Global

"La regulación para un CISO es un arma de doble filo. Creo que, en general, es mejor disponer de un marco regulatorio moderno que no tenerlo, así que, para dar una respuesta, sí, creo que la normativa hace más fácil el trabajo del CISO. Trabajar con los reguladores para alinear los criterios de cumplimiento de las múltiples normativas y concretar los requisitos para eliminar la subjetividad tendería a minimizar los aspectos negativos".

IBERDROLA
Fernando Ureña
BISO Renovables España

"Con estas regulaciones, cada vez más figuras de la organización van a ver crecer sus expectativas sobre la labor del CISO, presión que además viene incrementada por una sombra sancionadora. Sin embargo, estas obligaciones vienen mostrando una clara tendencia a involucrar a la alta dirección en la responsabilidad última de la Ciberseguridad, lo que se va a traducir en mayores inversiones y en el obligado entendimiento del riesgo, siendo esta *esponsorización* la mejor aliada del CISO."

IBERMÁTICA, an AYESA company
Juan Carlos Chamizo Aragón
CISO

"La protección de la información personal es un tema muy importante, ya que cada vez las empresas gestionan más información privada, la cual es considerada un objetivo muy interesante para los ciberdelincuentes para realizar posteriormente ataques más elaborados o dar mayor credibilidad a ataques de *phishing* o ingeniería social. Estos motivos hacen que la ciberseguridad y la protección de datos deban complementarse. En la actualidad, la referencia en materia de protección de datos a nivel español es la LOPDGDD y el RGPD. El cumplimiento de esta ley, aunque obligatoria, aporta mejoras a la gestión de incidentes, previene multas por posibles brechas (en caso de no tener con medidas de protección adecuadas), así como actuar correctamente ante ellas y a prevenir daños reputacionales. La ciberseguridad debe complementar a la protección de la información de una manera más técnica, ya que la ley vigente, exige que se apliquen medidas técnicas y organizativas para proteger la información. Por estos motivos, se debe hacer una gestión de la ciberseguridad correcta y precisa, que determine las medidas de seguridad necesarias, en función de los riesgos que se detecten de almacenar, procesar y gestionar la información confidencial. Así es como la LOPDGDD establece un marco legal y los requisitos, mientras que la ciberseguridad se encarga de determinar e implementar las medidas necesarias para garantizar la seguridad".

IBERPAY
Juan Manuel Nieto Moreno
Director de Seguridad y Riesgos Tecnológicos

"Tradicionalmente la regulación ha servido de palanca para la seguridad de la información. Y quienes nos dedicamos a esto, tenemos mucho que agradecerle. Sin embargo, quien todavía no haya entendido que gestionar la seguridad es una necesidad imperativa y solo busque el "compliance", tiene un problema. Desde hace años apuesto por trabajar para la seguridad, de acuerdo con lo que el negocio necesite. Y si se hacen las cosas bien, el cumplimiento normativo debe venir solo. Al revés, difícilmente".

CISOs

IB-SALUT
Miguel Ángel Benito Tovar
Delegado de Protección de Datos del Ib-Salut

"Sin duda la evolución normativa en materia de privacidad y ciberseguridad supone un reto para el sector público pero a la vez también estas normativas vienen a definir y establecer con más detalle los requerimientos mínimos que cumplir por parte de las organizaciones, lo cual supone un gran soporte para el CISO cuya figura, no nueva, también considero que se ve reforzada y reconocida con esta evolución normativa al igual que sucedió con la figura del Delegado de Protección de Datos desde la entrada en vigor del RGPD".

INCIBE
Marcos Gómez Hidalgo
Subdirector de INCIBE-CERT. CISO de INCIBE

"¿Qué duda cabe? Pues cierta, más de la que creo, más seguramente de la que creemos o deberíamos creer. En la reciente normativa de los últimos 10 o 12 años hemos visto reforzadas las diferentes posiciones de la seguridad de la información, la seguridad integral, la seguridad de los datos, y por ello roles como el de CISO, el DPO, el Responsable de Seguridad Integral, el Responsable de Seguridad de Enlace, etc., se han revalorizado y han tomado nuevas dimensiones en las organizaciones públicas y privadas. Pero al mismo tiempo las responsabilidades legales o normativas que han asaltado dichas entidades han supuesto una enorme carga de responsabilidad depositada en estos roles y sus equipos técnicos, operativos y legales. Pero seamos optimistas, no cabe otra, y pensemos que estas regulaciones son elementos e instrumentos que permiten justificar la inversión en ciberseguridad, la adopción de medidas obligatorias y la implementación de otras como buenas prácticas. Estas herramientas regulatorias tienen una doble ventaja, que atienden a problemas y que exigen responsabilidades, nada a lo que no esté acostumbrado un CISO".

INDRA
Elena García Díez
CISO

"Entender el riesgo de seguridad al que nos enfrentamos y definir la estrategia más adecuada al negocio con una visión completa, desde el diseño a la operación, están en la esencia de las regulaciones y, como tal, deben actuar como facilitador para el impulso e implantación de la seguridad. El reto: asegurar que el cumplimiento regulatorio realmente complementa la estrategia de seguridad en la que buscamos reducir el riesgo y no provoca un exceso de foco en un cumplimiento que puede no suponer una mejora efectiva en el nivel de seguridad que perseguimos".

ING
Gustavo Lozano García
CISO

"La regulación es fundamental y marca nuestro trabajo, y desde ING la vemos como una oportunidad para innovar. La regulación pretende proteger al ciudadano y nos permite ofrecer servicios más seguros, adaptados a las necesidades de los clientes. El rol de CISO se enfrenta diariamente a un contexto retador, dinámico y cambiante, por lo que pensemos en adaptarnos y adoptar las regulaciones para tener un papel más activo, visible y estratégico para la organización".

INSTITUTO MUNICIPAL DE INFORMÁTICA – IMI (AYTO. DE BARCELONA)
Neus Bellavista Arimany
Jefa del Departamento de Seguridad

"Estas regulaciones facilitan a las organizaciones ir madurando en la función de la seguridad, dado que fuerzan o aceleran el camino que muchas de ellas estaban realizando. Ubican el CISO como una figura directiva de la organización, fuera de las áreas tecnológicas y establecen estructuras para la gestión de la seguridad de la información. Cada regulación exige garantizar que se cumpla con todos los requisitos exigidos y esto en sí, complica la tarea del CISO. Pero la tarea del CISO no la complican las regulaciones sino los desafíos de la propia seguridad y el reto de responder a las amenazas emergentes y en constante evolución".

ITINERE INFRAESTRUCTURAS
Carlos Laguna García
Responsable de Ciberseguridad

"Desde el punto de vista de la cada vez mayor y mejor regulación, cabe interpretar que el papel de CISO resulte más sencillo de cumplir al encontrarnos con estándares más específicos, concretos, soberbios. Otro enfoque permite vislumbrar que el advenimiento de nuevas regulaciones trae consigo más vigilancia, responsabilidad y, por ende, incremento del nivel de estrés en su desempeño. Será determinante el grado de madurez de la organización y de los recursos que disponga. ¡Ánimo!".

LA RIOJA – Consejería de Desarrollo Autonómico

Tomás Gómez Pérez

CISO del Gobierno de La Rioja
Dirección General para el Avance Digital

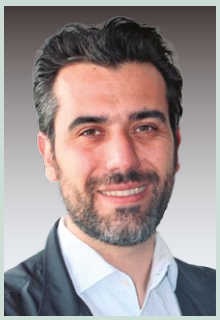
"No es fácil defender categóricamente una u otra posición sin exponerse a una serie de argumentos en contra. Por un lado, las normas establecen una serie de medidas y controles dirigidas a garantizar la seguridad de sistemas e información. Implementar estas medidas puede ser costoso y requerir una cantidad importante recursos, lo que añade presión sobre el presupuesto y los recursos de la organización. Esto, normalmente, conlleva cambios y nombramientos en la organización e incluso en los procesos y hasta en la infraestructura, lo que toma tiempo y recursos adicionales. Todo esto añade presión a la posición del CISO que, además debe equilibrar los objetivos de seguridad con los objetivos de 'negocio' de la organización. Por otro lado, las normas pueden ayudar a crear una cultura de seguridad en la organización y esto puede llevar a una mayor conciencia y a una mejor adopción de medidas, controles y políticas y puede generar confianza en la organización para proteger información y sistemas por parte de cualquier tercero. Cuando se proporciona un marco común para la evaluación de riesgos y la implantación de controles y proporcionan una mayor transparencia y responsabilidad, por el deber de informar sobre su cumplimiento, se facilita la colaboración y, sobre todo, la capacidad de evaluación entre organizaciones. Si, además de lo anterior, las normas se acompañan de guías de implantación de las medidas o controles necesarios, la vida del CISO puede mejorar".

MADRID DIGITAL

Esther Muñoz

Subdirectora General de Ciberseguridad, Protección de datos y Privacidad

"En mi experiencia como responsable de seguridad de Madrid Digital, las leyes actuales en materia de seguridad de la información, han facilitado y mucho la labor de todos los CISOs, responsables de seguridad, al regular las obligaciones, responsabilidades y medidas de seguridad que las administraciones públicas tienen que determinar y aplicar para proteger la información, las redes y sistemas que gestionan. Además, y muy importante, dejan claro que la ciberseguridad es una responsabilidad de toda la organización, de todos aquellos que gestionan información, estableciendo y diferenciando roles y responsabilidades. Al mismo tiempo, la extensa regulación en materia de ciberseguridad en España, aumenta la complejidad de nuestra función, y, por tanto, hacen más difícil nuestra tarea, ya que una de las funciones principales del CISO es la supervisión del cumplimiento de la legislación vigente".

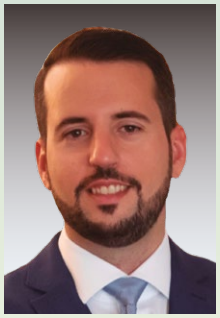


MÁSMÓVIL

Jesús Santos

Head of Infrastructure & Workplace & Security

"Parece que la frenética dinámica geopolítica, la recesión económica, la transformación digital impulsada por gobiernos e instituciones y las tendencias en ciberseguridad están generando mucha incertidumbre este año, ya que todo este escenario exige a los CISO una flexibilidad y alerta con pocos precedentes. La tecnología de seguridad está evolucionando favorablemente para mantenerse al día con los ciberdelincuentes. Nuestra impresión es que a medida que el contexto geopolítico, las inversiones y las tecnologías maduran y evolucionan a ritmo vertiginoso, especulación y análisis irán muy en paralelo, por lo que será necesario estar más que nunca actualizado en los últimos desarrollos de seguridad".



MERCEDES-BENZ EUROPA

Andrés Romero

Regional Information Security Officer IT Services Europe

"Es notorio que toda política o regulación de carácter obligatorio, nos sirve a los Responsables de Seguridad de la Información como herramienta adicional para persuadir a la alta dirección y aumentar nuestros recursos y, por consiguiente, ampliar algo la madurez en la misma. Sin embargo, debemos tener mucho cuidado porque a pesar de que a corto plazo puede ser un "arma" muy útil, es fácil caer y fijar la estrategia solo en el Compliance, lo que es un claro error (Security beyond Compliance)".

METRO DE MADRID

Antonio Simón Martínez García

Coordinador de Seguridad Informática y Ciberseguridad. Área de Comunicaciones y Tecnologías de la Información

"Las regulaciones, como garantes del cumplimiento de los objetivos en materia de ciberseguridad establecidos tanto en el ámbito europeo como en el español, han sido y seguirán siendo una pieza clave para la gestión del CISO. Así, éste verá facilitada su tarea de convertir la ciberseguridad en parte inseparable del negocio estableciendo sus prioridades en aspectos como la gestión eficiente de los riesgos, los incidentes y las crisis, la corresponsabilidad de la alta dirección, y la concienciación".

METROVACESA

Mario Moreno Martínez

Responsable de Seguridad

"Todas estas normativas pueden ayudar al CISO a: Identificar las áreas más críticas de la organización y poder priorizar los recursos; gestionar la ciberseguridad cumpliendo la normativa europea; implantar requisitos de seguridad con

CISOs

proveedores; garantizar la interoperabilidad de los sistemas entre empresas; aumentar la adopción por parte de los usuarios y así mejorar la seguridad de la empresa; promocionar tecnologías más seguras; y gestionar la privacidad y la protección de los datos".

MUTUA UNIVERSAL
Carlos Villa Ferrer
Director Técnico de Ciberseguridad – CISO

"Opino que sí, que las regulaciones ayudan al CISO a establecer y justificar los requerimientos para los ciber riesgos y fuerzan a marcar unos niveles mínimos de ciberseguridad en la cadena de suministros. Además, aunque la necesidad legal de garantizar el cumplimiento normativo con las regulaciones es un proceso complejo que consume tiempo y requiere de la colaboración del resto de áreas de la empresa, esto te obliga como CISO a mantener y reforzar ese contacto, y lo considero beneficioso".

NAVANTIA
Joaquín Castellón
CISO

"Creo que actualmente la normativa ayuda al CISO. Muy pocos sectores contaban con normativa por lo que estamos lejos de una sobrerregulación, que sería perjudicial. Es importante que la normativa, nacional o internacional, sea convergente y evite duplicidades. En general facilita que las empresas pongan a disposición del CISO los medios humanos y materiales necesarios para cumplir sus cometidos. Por otra parte, facilita también el control de las cadenas de suministro al serles aplicables unos estándares comunes".

OCASO
David Jorrín
CISO – Jefe de Área de Seguridad Informática

"La regulación actual exige más transparencia interna y externa en la gestión de los ciberriesgos pues la responsabilidad recae en el máximo nivel de la empresa, al que debe informar el CISO, y se fiscalizan los incidentes por la Administración. No obstante, las normas refuerzan el rol del CISO: asumen la posibilidad de sufrir incidentes, destacan la preparación para mitigarlos y sustentan los requisitos ante los proveedores. La ciberseguridad cada día es más exigente pero igual de apasionante".

PIKOLÍN
Javier Ramos Peribáñez
CISO

"Regulaciones, normativas, guías, referencias etc., bienvenidas sean todas ellas independientemente de su origen y nomenclatura, todas ellas contienen puntos esenciales para mejorar nuestra madurez en ciberseguridad y avanzar por el camino adecuado. Por tanto, ¿nos pueden servir de apoyo? Rotundamente SÍ, para eso se han hecho. Busquemos enfoques válidos a nuestro tipo de negocio en temas como protección, análisis, respuesta, recuperación, concienciación etc., donde nos pueden ser de utilidad".

PwC
Jaume Esteve Ballester
CISO en España

"En PwC prestamos servicios a multitud de clientes de diversos sectores que están en el alcance de estas regulaciones. Por lo tanto, como proveedores de servicios profesionales de todos ellos que somos, debemos adaptarnos y estar preparados para que se sientan confortables con nosotros. Partimos de una base centrada en estándares internacionales. Se trata de identificar el *gap* que nos plantea cada una de estas regulaciones y dar la cobertura necesaria. Esfuerzo y oportunidad más que fácil o difícil".

RADISSON HOTELS
Rodrigo Blanco
CISO

"Las regulaciones son importantes: aportan un marco de referencia contrastado y homologable, y refrendan muchas actividades de Seguridad. Sin embargo, pueden distraer de algunas necesidades, si sus objetivos de control no están totalmente alineados con la verdadera naturaleza del mapa de riesgos de la organización. En otras palabras: el total cumplimiento no siempre garantiza que todos los riesgos estén cubiertos, pero sin duda ayuda a Seguridad a legitimar ciertas políticas e iniciativas".

RECOLETAS RED HOSPITALARIA
Josep Bardallo
CISO

"Aunque las regulaciones actuales, y las nuevas que están por venir, van a incrementar la carga de trabajo del CISO y su responsabilidad, sí que facilitarán la labor del mismo ya que no solo permitirá tener una clara orientación en donde enfocar sus esfuerzos y permitirá homogeneizar en su sector las medidas, sino que en determinados ámbitos (sanitario, IoT, cadena de suministro...) es la única manera de gestionar mejor los riesgos que no controlamos desde las organizaciones".

RENFE

Francisco Lázaro Anguís

CISO y DPO

"La 'vida' del CISO es más sencilla cuando: la Alta Dirección apoya la práctica de la ciberseguridad, los requerimientos en todo nuevo producto o servicio están desde el comienzo (por ejemplo cuando se publican las especificaciones técnicas), hay una cultura de empresa (en la que no se ve al área ciber como al enemigo natural), como empresa tenemos la decisión de que no haya equipos no actualizados, los proveedores tienen un nivel aceptable en esta materia, si se dispone de presupuesto y recursos (no ya suficientes, sino los mínimos imprescindibles, que tampoco pedimos mucho), la autoridad de control ejerce como tal, hay un régimen sancionador (interno y externo). Es por estos factores por lo que creo que las nuevas regulaciones (aunque sin pensar en el CISO), al tratarlos vienen a proporcionar un apoyo; regulación y la alta dirección son dos fuertes pilares para el cambio".

RESTAURANT BRANDS IBERIA – RBI

Francisco Javier Farfán Contreras

CISO

"Para mí como CISO, son una buena palanca en la que apoyarme para mejorar los niveles de seguridad de la compañía. Por ejemplo, la ISO 27K, ayuda a definir el nivel de madurez de seguridad que tiene la compañía en un momento inicial y definir un plan/estrategia para mejorar su madurez cara al futuro. Las certificaciones nos ayudan a generar confianza en nuestros clientes. Las regulaciones bien empleadas siempre generarán un impulso positivo en la compañía".

GRUPO SANTALUCÍA

Francisco Javier Santos Ortega

CISO Corporativo

"No es nuevo que el financiero y asegurador sea un sector altamente regulado. Esta situación hace que las organizaciones estén habituadas a responder de manera eficiente a las obligaciones derivadas de estas regulaciones, pero también supone un reto el poder compaginarlas de forma que no impacten negativamente en la operativa ni en la competitividad de las empresas. Pero en el caso de la seguridad de la información, lo que es más novedoso es que la regulación está llegando de una manera más y intensa y sobre todo con una frecuencia muy elevada, lo que supone una carga extra a tener en cuenta dentro del día a día de los equipos. Lo que no hay que perder de vista es que dentro de estas regulaciones como DORA, directrices de EIOPA o NIS2 no deben suponer un solapamiento en las obligaciones de cumplimiento como puede ser la obligación de notificación a diferentes organismos de supervisión de anomalías que produzca ineficiencia, o que por la disparidad del tamaño de las empresas como por ejemplo en el sector asegurador (y por principios de proporcionalidad por ejemplo), la aplicación de las regulaciones suponga cierta arbitrariedad de como se aplican y eso haga que no todas las empresas deban aplicarlas con el mismo nivel de esfuerzo. El espíritu final de las regulaciones es garantizar que los servicios que se prestan a los clientes de las empresas sea con la máxima calidad y con las mayores garantías de servicio, confianza y seguridad posibles, de manera que redundan en la fortaleza del sector y una mejor sociedad. Y en este sentido son bienvenidas ya que permiten establecer un ecosistema más justo… pero también deben ser aplicables y que puedan suponer también un beneficio para las empresas que estamos obligadas a cumplirlas. Ese es el mayor reto que tenemos que afrontar entre todos, tanto los organismos reguladores como las empresas reguladas".

SANTANDER WEALTH MANAGEMENT AND INSURANCE

David Matesanz Ureña

CISO Global

"Mi opinión y mi experiencia es que la regulación siempre ayuda. Sirve para vencer la creencia de que algunas cosas son opcionales, y ahorrarse en ocasiones la parte de explicar el porqué de tener que establecer ciertos controles. Ahora bien, por motivos obvios, las regulaciones llegan bastante más tarde que las amenazas o los cambios tecnológicos. Como CISOs nos ha tocado entender esta situación y evaluar riesgos durante años antes de que alguna regulación, normativa o ley establezca los controles mínimos. Lo que un responsable de ciberseguridad o aún más un responsable de un negocio nunca debería asumir es que con cumplir con la regulación es suficiente. La mala noticia es que es muy probable que cumpliendo con la regulación de hoy no nos dé para sobrevivir ante las amenazas de hoy. La función de cumplimiento es altamente relevante para un CISO hoy en día, pero para mí, sigue siendo es mucho más critica la función de análisis de amenazas, tecnología y procesos de protección, prueba e implementación de controles y gestión dinámica de riesgos. En definitiva, la capacidad del CISO y su equipo de reaprender y reevaluar cada día".

SOCIEDAD ESTATAL LOTERÍAS Y APUESTAS DEL ESTADO (SELAE)

Julio Sánchez Fernández

Jefe del Departamento de Seguridad de la Información

"El CISO de hoy en día se mueve entre una demanda de seguridad endógena, procedente de las expectativas de la dirección y una demanda exógena proveniente, sobre todo, de regulaciones. La exógena puede ayudar al CISO si la endógena es débil, aunque a veces obliga a priorizar las acciones de forma inconveniente o son desproporcionadas para el tamaño de la organización. Donde las regulaciones siempre ayudan al CISO

es a obtener, si las auditorías de cumplimiento son efectivas, cierta garantía de la seguridad de otros a los que no se puede auditar directamente, por lo que veremos cada vez más".

SEUR
Firas Atassi Morales
CISO/DPO

"Me encanta la pregunta porque la reflexión, aunque en nuestro ámbito la acotamos a nuestro Rol de CISO la realidad es que como gestores de empresas y no solo nosotros (CEO, CFO, CHRO) estamos sometidos a una sobrerregulación actual que nos está llevando a que cada vez sea más difícil gestionar una compañía. Desde mi punto de vista se está sobre regulando y el intentar cumplir con todos los requerimientos que se exigen y el poder incurrir en sanciones y penalizaciones por regulaciones donde en muchos casos se detecta la deficiencias de contrastación por parte de expertos o sectorial y por ende su compleja aplicabilidad en las empresas, la respuesta es SÍ, es mucho más difícil en el entorno actual porque estas regulaciones no ayudan, ni dan las herramientas ni consiguen inversiones, ni nos resuelven la falta de capacidades y talento, solamente nos imponen obligaciones y sanciones, dificultando nuestro *scope* a la hora de gestionar y la toma de decisiones sin una aplicabilidad real en las empresas y con un desconocimiento por parte de la sociedad de las mismas y su errónea interpretación".

SGS
Manuel Barrios Paredes
Global Chief Information Security Officer
Global Information Security

"Ser CISO no es fácil nunca… e implementar estas regulaciones y adquirir un nivel de madurez en ellas no es tarea nada fácil. Lo cierto es que estas regulaciones sirven de palanca en muchas ocasiones para obtener las partidas presupuestarias y recursos necesarios para poder abordarlas y así mismo, justificar inversiones en seguridad para la implementación de mejoras en las infraestructuras y procesos de seguridad. Otro punto importante, es que se implica a otras áreas como puede ser RR.HH., Departamentos Legales, Comunicación, IT, etc., para esparcir la cultura de la seguridad de la información, ya que estas regulaciones involucran a distintas áreas de la empresa haciendo que todos remen en una misma dirección. Desde mi punto de vista, la implementación de estas normativas y regulaciones, a pesar de ser muy exigentes, favorecen a la generación de confianza ante terceros al obligarnos a reforzar nuestros procesos, procedimientos e infraestructuras, ayudando en paralelo a reducir los riesgos y evitar o reducir sanciones y multas por su incumplimiento. Y dependiendo del nivel de madurez de la empresa, la implementación de estas regulaciones puede ser un arma de doble filo para un CISO, en empresas de poca madurez implementar desde cero cualquiera de ellas, puede dar bastantes dolores de cabeza. Sin embargo, en aquellas que cuentan con una cierta madurez, pueden y deben ser uno de los principales aliados del CISO".

SINGULAR BANK
Damián Ruiz Soriano
CISO

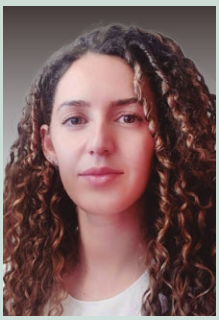
"Tendremos 'facilitadores' por el empoderamiento del CISO, y el carácter de control y sancionador de la regulación. Pero habrá que mejorar en tres ámbitos: *Gobierno*. (1) Planes Directores justificados en riesgos y costes. (2) Orientación a controles y evaluación de su cumplimiento. (3) Reportes de calidad.
Dirección-Board formados, informados y conocedores de responsabilidades. Formación en Proteger, Detectar y Responder. Informados sobre riesgos reales. Y conocedores de las consecuencias por falta de diligencia.
Tecnología. Madurez en procesos y procedimientos con controles de ciberseguridad insertados".

TELEFÓNICA
Juan Carlos Gómez Castillo
Director Global de Seguridad Digital

"La regulación y su cumplimiento siempre ha sido uno de los principales catalizadores de la seguridad (acordémonos de la LORTAD). Pero el crecimiento exponencial de los ciberincidentes, el aumento de la digitalización y el grado de concienciación sobre la ciberamenaza han sobrepasado a la regulación como catalizador. Por lo tanto, es necesario una regulación adecuada a este nuevo escenario, coherente, simple y orientada a la realidad de las empresas, y que ayude al CISO a tener una posición relevante y mucho apoyo en el desempeño de sus responsabilidades".

TENDAM GROUP
David Moreno del Cerro
Head of Technology & Security

"Creo que proporcionan un apoyo muy positivo a las funciones del CISO, en tanto que le ayudan a robustecer su misión en la corporación, ya sea pública o privada, además de fortalecer su capacidad de influencia, visibilidad en la jerarquía y nivel ejecutivo. No obstante, como contrapartida, este aumento incrementa sustancialmente los niveles de exigencia de auditoría y diligencia debida, por lo que es cada vez más importante adoptar un marco de trabajo y establecer un modelo de control maduro".



TK ELEVATOR

Sandra Cuevas López

Information Security Officer Europe-Africa

"El rol de CISO juega un papel crítico en la gestión de la seguridad de la organización, así como el cumplimento de las múltiples regulaciones. Nos supone un gran reto combinar las regulaciones que apliquen a nuestro sector y estar preparados para las nuevas que se van estableciendo. A pesar de ello, esto nos permite priorizar las áreas de la organización que requieren más atención, así como reforzar el mensaje y comunicar mejor la importancia de su cumplimiento a los directivos de la organización".

TMB – TRANSPORTS METROPOLITANS DE BARCELONA

Juan José del Río Estévez

Responsable de la Unidad de Seguridad TIC

"No cabe duda de que toda regulación facilita la labor de los CISO. Toda normativa define pautas a seguir y eso favorece la estandarización de la seguridad en las organizaciones, además van incorporando mejoras reclamadas desde el colectivo de CISOs. Desde el punto de vista organizativo también ayuda a clarificar el modelo a seguir para mejorar la eficiencia del proceso de la Ciberseguridad permitiendo un mayor rendimiento de los recursos disponibles. No todo son bondades, también hay contras. Cumplir con las regulaciones supone esfuerzos. Por un lado, requiere del análisis de la regulación para determinar qué es lo que afecta a nuestra organización, si ya está resuelto en la empresa y si no lo está determinar los esfuerzos para realizarlo. Otro escollo es presentar el plan de adecuación de la regulación al C-Level. Si no hay inversión el tema es relativamente sencillo, los problemas empiezan cuando se requieren recursos, tanto económicos como humanos, ya que en algunas organizaciones puede suponer un problema la asignación de estos recursos. Resumiendo: tener un paraguas regulatorio suaviza un poco la función, si bien sigue sin ser fácil ser CISO".

TRIBUNAL DE CUENTAS

María del Carmen Zarcero García-Risco

Subdirectora de la Oficina de Seguridad de la Información

"Tanto a nivel europeo como nacional se identifica la necesidad de establecer normativas y regulaciones para alcanzar de una manera homogénea unos adecuados niveles de seguridad en ámbitos como el financiero, sectores estratégicos, protección de datos, etc. Su cumplimiento redunda en una mejora global de la seguridad y debe encontrarse, por tanto, entre los objetivos estratégicos de cualquier organización. En este sentido, su existencia es beneficiosa y, por tanto, facilita la labor del CISO".

UNIÓN DE CREDITOS INMOBILIARIOS - UCI

Enrique Aristi

CISO

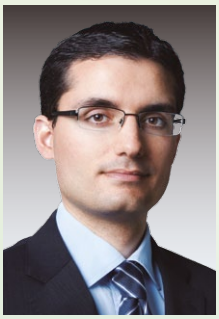
"Partiendo de que las funciones y objetivos de los CISO deberían ser similares, el contexto organizacional es clave. En función de cuán estratégica sea la Ciberseguridad en cada caso concreto y de dónde esté ubicado el CISO, tendrá más oportunidades de llevarlo a cabo con éxito. Sistemas de Gestión (ISO 27001, etc.) habrán allanado el terreno y, al no existir exigencias en torno al *cómo*, la calidad de vida del CISO dependerá de la experiencia operativa y táctica de su departamento de Ciberseguridad".

UNIVERSIDAD COMPLUTENSE DE MADRID

Miguel Ángel Perote Alejandre

Administrador de Protección de la Información
Centro de Proceso de Datos

"En mi humilde opinión y desde el punto de vista de la seguridad en las AA.PP., no creo que ahora sea más fácil ser CISO que antes. A nivel estratégico el CISO sigue teniendo las mismas responsabilidades e inquietudes que antes, si no más, con el avance de las nuevas tecnologías y técnicas de ataque. Si bien es cierto que tener un marco de referencia ayuda a no dispersarse en la estrategia de defensa, el hecho de ser de 'obligado cumplimiento' añade un punto de estrés extra, ante la posible falta del mismo".



UNIVERSIDAD REY JUAN CARLOS

José Antonio Rubio Blanco

Responsable de Seguridad de la Información

"Contar con una base normativa facilita desde luego la labor del CISO. No sólo porque traslada una línea base de controles organizativos y técnicos a implantar, sino porque 'empodera' al CISO frente a la alta dirección y áreas de negocio de su organización. Aunque sigamos teniendo que hacer una labor de concienciación continua para que se entienda la importancia de este campo, la regulación sirve a modo de cuña para dejar a un lado el dilema de hasta qué punto se han poner en marcha acciones de ciberseguridad. Por tanto, podemos profundizar en el debate, pasando de hablar de proyectos locales circunscritos al área TIC o de ciberseguridad, a proyectos transversales a toda la organización con implicaciones directas hacia el negocio de la misma. De igual modo, el mensaje se entiende mucho mejor en la capa de usuarios, al ser conscientes de que hay regulaciones a cumplir, de tal modo que la discusión pasa a centrarse en cómo implantar ciberseguridad sin que la misma entorpezca el día a día de la organización. Esto sumado a otros elementos como la designación formal de un CISO, la necesidad de contar con un foro donde la alta dirección lidere esta materia o el requerimiento de que la concienciación ha de estar siempre presente, allanan la de por sí ardua labor del CISO".

CISOs

URBASER
Manuel Cobo Couto
CISO

"No sé si la palabra es 'fácil'; las regulaciones son cada vez más exigentes y requieren de una mayor responsabilidad e implicación de toda la compañía. Pero es cierto, que son una pieza clave para posicionar la ciberseguridad como base facilitadora de negocio. Esta situación, la canalizamos, y hacen que efectivamente utilicemos las regulaciones como palanca para seguir desarrollando la cultura entre nuestros empleados y reforzando nuestros procesos corporativos desde un prisma de ciberseguridad".

VOLKSWAGEN GROUP RETAIL ESPAÑA
Sergi Mingo Fabregat
CISO – IT Security Manager

"La nueva legislación invita a asumir que el rol del CISO se convierte en obligatorio, por consiguiente, estará cada vez más presente en pymes aboliendo creencias del pasado que lo identificaban como un perfil propio de multinacionales. Esto supone un cambio de cultura en lo que a sus funciones se refiere, que van más allá de ser una figura de apoyo para el CIO en su responsabilidad de alinear la seguridad corporativa con los objetivos de la empresa, elaborar planes de seguridad y velar por su cumplimiento; así como prevenir vulnerabilidades dando respuesta a posibles incidentes de seguridad".

WiZink Bank
Luis Ballesteros
CISO

"En la actualidad es más difícil ser CISO que hace años, pero el motivo es la evolución de los ciberriesgos. Según el informe de riesgos del Foro Económico Mundial 2023, el cibercrimen y la ciberinseguridad están entre los 10 principales riesgos para la sociedad a corto y largo plazo. Las regulaciones están ayudando a la función CISO. Están poniendo foco en ciberseguridad y fuerzan a que los consejos de administración y la alta dirección tomen conciencia de estos riesgos y actúen para mitigarlos".

XUNTA DE GALICIA – AMTEGA
Gustavo Herva Iglesias
Jefe subárea de Seguridad de la Agencia para la Modernización Tecnológica de Galicia

"Partiendo de la idea de que la posición del CISO no es nunca sencilla, las regulaciones actualmente existentes tienen un papel relevante como palanca a la hora de proponer y ejecutar acciones de mejora de la ciberseguridad. En el caso de las AA.PP., el ENS es hoy en día una herramienta fundamental en ese sentido. La cara B de este asunto puede ser la confluencia en algunos casos de un exceso de regulaciones en paralelo, que pueden complicar la gestión y no aportar mejora real de la ciberseguridad".

ZURICH SEGUROS
Conxi Hernica
Business Information Security Officer (BISO)

"Las regulaciones en ciberseguridad (NIS2, ENS, DORA…) son necesarias para establecer un marco legal y regulador que ayuda a proteger los sistemas y datos en la Unión Europea. Además, promueven que las empresas sean cada vez más conscientes de los riesgos de la ciberseguridad e incluyan estrategias para combatirlo en su cultura empresarial. En términos de si estas regulaciones hacen más fácil o no la vida a un CISO, dependerá de la perspectiva desde la cual se mire. Por un lado, estas regulaciones establecen medidas de seguridad específicas, proporcionando una guía clara para que el CISO pueda planificar e implementar medidas de seguridad efectivas y minimizar el riesgo. Sin embargo, estas regulaciones también pueden significar una mayor carga de trabajo y responsabilidad para un CISO, ya que deben asegurarse de que la compañía cumple con todos los requisitos y directrices establecidos que en ocasiones son complejos de implementar, difíciles de cumplir y de mantenerlos actualizados. Lo que supone una mayor inversión de recursos, capacidades… que las empresas deben incluir en sus planes de negocio, y ahí es donde se debe incidir en divulgar, concienciar y trabajar de manera conjunta para evitar el riesgo".

El 90% de *ciberataques* pasan por Correo Electrónico

Securiza tu canal de envío y recepción de archivos y protege tu organización con

tranxfer

Año 2022 en números:

+130.000 transferencias
+5.000 Fugas de información evitadas
+400 detecciones de malware

Consigue tu demo en www.tranxfer.com

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría MEDIA RD 3/2010

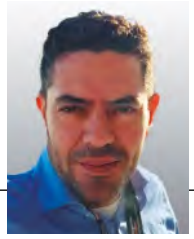
Information Security Management ISO 27001 Certified

ISO 27701

GDPR

CAIXABANK, en línea con la innovación en ciberseguridad para una soberanía tecnológica y digital en Europa

La ciberseguridad forma parte integral de los procesos y unidades de negocio de las entidades financieras, siendo fundamental en el proceso de digitalización de un entorno estrictamente regulado, competitivo y en constante evolución debido a la emersión de nuevas tecnologías, metodologías, regulaciones y patrones de ataque. Es por ello por lo que la innovación en seguridad cobra especial relevancia en el sector financiero y debe ser constante, impactando en la competitividad de las entidades, pero trascendiendo más allá de ellas, para fortalecer el sector financiero y la ciberseguridad. La colaboración entre la industria financiera y el ecosistema de investigación e innovación europeos puede y debe jugar un papel primordial en la innovación en ciberseguridad en Europa.



Ramon Martín de Pozuelo / Mario Maawad Marcos

Ciberseguridad en el entorno financiero: requerimientos y *drivers*

El sector financiero se ha convertido en uno de los principales objetivos de los ciberdelincuentes, los cuales buscan obtener mediante sus ataques básicamente dinero en efectivo o en su defecto información que posteriormente puedan utilizar también para monetizar sus ataques. La meta de estos usuarios maliciosos se focaliza en atacar directamente a las personas, ya sea clientes o empleados utilizando ingeniería social, o alternativamente explotar cualquier vulnerabilidad que puedan encontrar en las infraestructuras de una entidad financiera para obtener ganancias mediante extorsión, robo o fraude, a la propia entidad o a sus clientes. Además, el auge de nuevas tecnologías puede conducir hacia nuevos modelos de negocio y nuevas formas más eficientes de gestionar la información de los usuarios y de la entidad, pero también han traído consigo nuevas amenazas que conviene abordar en consecuencia.

Los equipos de ciberseguridad deben verse como un área más que genera valor para la entidad y son parte integral de los procesos y unidades de negocio. Su labor es fundamental en el proceso de digitalización del sector, integrando estas nuevas tecnologías a la vez que manteniendo el mismo nivel de riesgo para sus entidades. Además, el entorno altamente cambiante en el cual los ciberdelincuentes están constantemente innovando, hace completamente imprescindible la inversión en innovación por parte de la industria de seguridad.

Si analizamos las peculiaridades del sector financiero en este proceso de digitalización habría que tener en cuenta varios requisitos principales:

Seguridad: estas tecnologías son nuevas y, a menudo, los riesgos no se conocen bien o no se han evaluado por completo. Se necesitan herramientas de seguridad para facilitar esta evaluación.

Regulación: las instituciones financieras están firmemente reguladas por (principalmente) organizaciones europeas; las herramientas utilizadas deben poder facilitar el cumplimiento de políticas y estándares.

Competitividad: todas estas tecnologías deben integrarse en los servicios empresariales financieros para poder competir con otros recién llegados al sector con una mayor agilidad tecnológica (como las FinTechs o BigTechs).

La innovación en ciberseguridad para el sector financiero europeo se plantea crucial para su estabilidad a medio-largo plazo, especialmente si tenemos en cuenta los drivers que impactan en el incesante desarrollo de su ecosistema: las tecnologías emergentes, nuevas regulaciones, nuevas metodologías y vectores de ataque en constante evolución.

Usabilidad: en muchas ocasiones se ha de buscar un balance entre la seguridad y la facilidad de uso. Éste es un compromiso complejo que en muchas ocasiones puede ser crítico por su afectación al cliente final y al negocio en general. En este punto, la innovación en ciberseguridad puede facilitar dicho balance incrementando la seguridad sin complicar la usabilidad.

Con este contexto, la innovación en ciberseguridad para el sector financiero europeo se plantea crucial para la estabilidad del sector a medio-largo plazo, especialmente si tenemos en cuenta cuatro *drivers* que impactan en el incesante desarrollo del ecosistema de ciberseguridad de los bancos: las tecnologías emergentes, nuevas regulaciones, nuevas metodologías y vectores de ataque en constante evolución.

Tecnologías emergentes como 5G, la Inteligencia Artificial (IA), criptografía cuántica, controles biométricos, *blockchain* o el uso intensivo de servicios en la nube pueden ser utilizadas para mejorar los actuales sistemas y controles de ciberseguridad, pero también amplían en muchos casos la exposición de las empresas a los ciberataques, y requieren de una revisión de los actuales controles y de un análisis de riesgos. Este análisis, en algunos casos puede ser sencillo, pero siempre requiere de un estudio en profundidad de la tecnología para comprender cuales son las vulnerabilidades que conlleva la propia tecnología y el impacto que puede tener el uso malicioso de esa tecnología para escapar de los controles de seguridad actualmente implantados. Es por ello que generalmente es un proceso altamente complejo, y más si se tiene en cuenta que normalmente se carecen de ejemplos de como los atacantes pueden llegar a hacer uso de esas tecnologías en contra de la entidad.

Podríamos ampliar el análisis de cada una de estas nuevas tecnologías y el impacto que está causando en la ciberseguridad de la industria en general y de las entidades bancarias en particular, pero hay dos tecnologías que quizás merezcan una mención especial.

Por un lado, en los próximos años la computación cuántica puede cambiar drásticamente el panorama actual de ciberseguridad. La implementación de aplicaciones cuánticas en el sector bancario

puede mejorar la eficiencia, la creación de valor para el cliente, y la economía de escala, pero actualizar la ciberseguridad y los sistemas criptográficos del mundo para la era de la computación cuántica es uno de los principales retos que tenemos por delante. De nuevo, la innovación acarrea un gran potencial, pero también aumenta la superficie de exposición a ataques de las empresas y las capacidades de ataque de usuarios maliciosos.

Avances de la IA y el aprendizaje automático

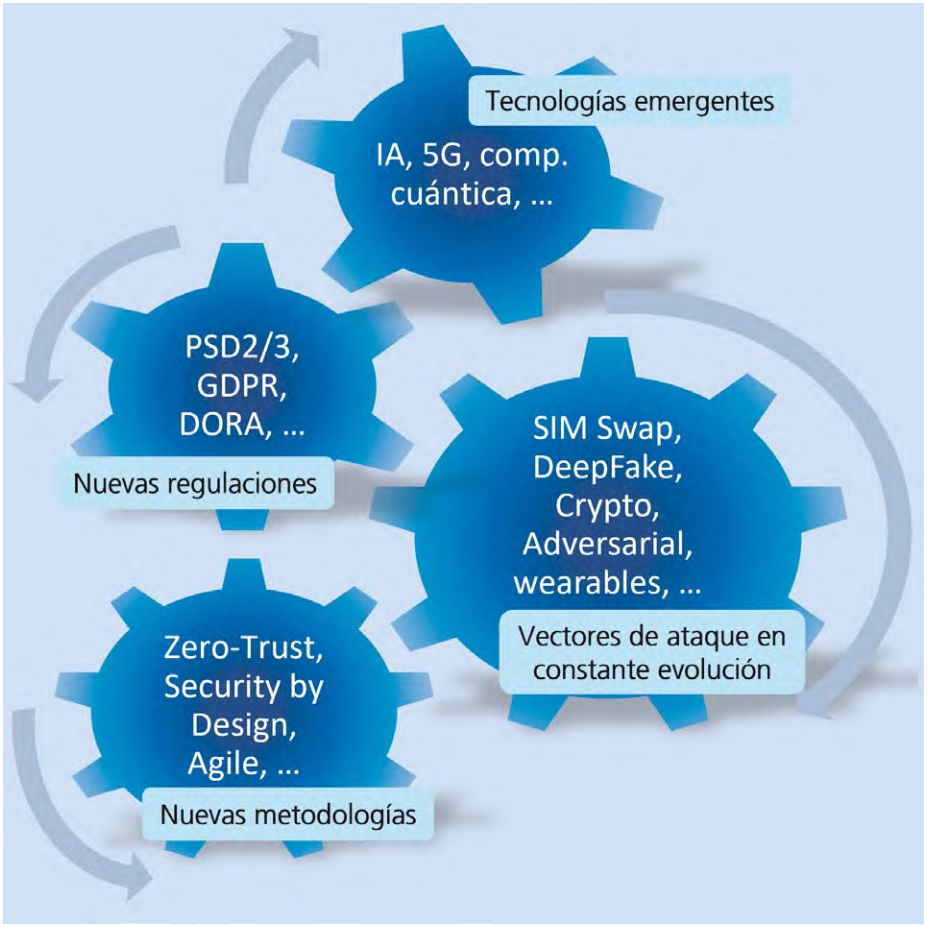
Por otro lado, los avances que brindan tecnologías como la IA y el aprendizaje automático. El uso adecuado de la IA puede tener un impacto muy positivo en la industria. Uno de los beneficios que pueden aportar y de especial interés en el sector bancario es ayudar a comprender mejor el comportamiento normal de humanos y dispositivos. Nos puede permitir la monitorización autónoma de cualquier comportamiento sospechoso y detectar desviaciones que, intencional o accidentalmente, puedan poner en riesgo las operaciones de las instituciones financieras. En este entorno cambiante, también deberían ayudar a adaptar los controles de seguridad actuales a esas variaciones necesarias para asegurar que las nuevas tecnologías cumplan al menos con el mismo nivel de seguridad que las tecnologías ya conocidas. Por ejemplo, uno de los usos potenciales de la IA que está generando más interés es en la evolución de las capacidades de detección de incidentes de las herramientas tradicionales basadas en patrones de ataque predefinidos, para hacerlas capaces de aprender y crear modelos del funcionamiento normal de forma autónoma y detectar desviaciones sin necesidad de patrones preconfigurados.

Podríamos ir más allá y hablar también del impacto que puede tener el aprendizaje automático federado o FML (de sus siglas en inglés, *Federated Machine Learning*), y de cómo la industria y en especial el sector bancario podría beneficiarse de modelos de IA colaborativos, enriquecidos con datos de múltiples entidades, que permitan mejorar la detección autónoma de ataques y sobre todo la detección y prevención del ciberfraude. Estas tecnologías acercan la posibilidad de análisis de datos de forma conjunta manteniendo la privacidad de los datos sensibles de las compañías y de sus clientes, hecho que anteriormente se planteaba imposible en la mayoría de los casos, por el riesgo que implicaba la compartición de estos datos o simplemente por la incompatibilidad con las regulaciones existentes en privacidad de datos.

La regulación, determinante

Y es que la **regulación** (la existente y la aparición de nuevas regulaciones y estándares, muchos de ellos de obligado cumplimiento en el sector financiero y el resto de las infraestructuras críticas) es otro de los factores determinantes en la innovación de la ciberseguridad. El sector bancario es un sector estrictamente regulado, con un alto nivel de supervisión de sus actividades. Regulaciones y directivas como NIS o DORA, dirigidas a incrementar la resiliencia y la protección de las infraestructuras y servicios de los *wallets* de identidad digital (planificada por la Comisión Europea durante 2024) pretenden suponer un gran cambio en la manera que los clientes podrán autenticarse con los servicios del banco y la manera como los propios clientes y las entidades financieras podrán manejar y gobernar los datos confidenciales de los clientes.

También puede parecer que algunas de estas nuevas regulaciones que serán implantadas en los próximos años limitan el potencial de innovación, como el European AI Act, que aparece para controlar el uso de la IA. Si bien es cierto que esta



tienen un alto impacto en la evolución y la innovación de la ciberseguridad implantada en la industria. Estas obligan a todas las entidades a ofrecer un mínimo de garantías en cuanto a ciberseguridad, pero también otras como eIDAS2, PSD2/PSD3 han supuesto o van a suponer un gran impacto en la operativa y la gestión de la ciberseguridad de los bancos al estar enfocadas a garantizar el acceso a los servicios financieros de una manera más abierta, pero garantizando la seguridad, permitiendo la entrada de nuevos actores y competidores a las entidades bancarias y que sin duda suponen un revulsivo a la innovación. Por poner solo un ejemplo, el uso de eIDAS por parte de la industria y la implantación a nivel europeo regulación podría acotar de alguna forma la implantación de modelos de aprendizaje automático, también resulta necesaria para no delegar completamente la operativa de la ciberseguridad y sus controles en manos de una IA evolutiva y con capacidades de razonamiento que podrían escapar de nuestra comprensión y control. Este hecho también ha focalizado el interés en la investigación e innovación de herramientas efectivas y eficientes de inteligencia artificial explicable, que permitan el uso de procesos automatizados, pero mantengan cierto nivel de explicabilidad en las decisiones de las máquinas y dispositivos gobernados por la IA, posibilitando su supervisión y corrección.

Nuevas metodologías y conceptos, como *Zero Trust*, están ayudando a los bancos a adoptar un enfoque más proactivo y estratégico de gestión y gobernanza de los sistemas IT y de la seguridad, permitiendo identificar posibles vulnerabilidades y atajándolas antes de que puedan ser explotadas por los cibercriminales, conceptos que en muchas ocasiones no son realmente nuevos y que han sido prestados de la industria de seguridad y defensa como pueden ser el *Cyber Kill Chain* que modeliza los ataques en fases o pasos para entenderlos y prevenirlos con el menor daño posible, o la implantación de un *Red Team* que pretende dar una visión objetiva de la seguridad tomando como referencia los métodos de ataque y la información que utilizaría un ciberdelincuente real. Estos cambios metodológicos están siendo otro de los *drivers* principales en la innovación de la ciberseguridad, provocando una evolución continua (y necesaria) en la forma de abordar la seguridad de la empresa.

Y, por último, es importante mencionar cómo la industria se debe enfrentar a nuevos tipos de ataques que son cada vez más sofisticados y difíciles de detectar, y cómo los bancos deben mantenerse a la vanguardia mediante la adopción de medidas de seguridad avanzadas que puedan ayudar a prevenir y mitigar este tipo de ataques. Algunos de estos nuevos ataques están justamente relacionados con la explotación de las nuevas tecnologías por parte de los atacantes, como habíamos mencionado anteriormente. Por ejemplo, el uso de la IA o de la computación cuántica para realizar y evolucionar mucho más rápido nuevos patrones (p.ej. *Adversarial Attacks*), herramientas (p.ej. *DeepFake*) o explotar nuevos entornos (p.ej. Criptomonedas).

Todo ello está convirtiendo la ciberseguridad industrial en una carrera incesante entre los atacantes y las empresas para ver quién innova más rápido los ataques y los sistemas de prevención y detección, respectivamente.

El valor de la innovación y la soberanía digital europea

Los bancos deben invertir, probablemente más que ningún otro sector, en la innovación de soluciones de seguridad que ayuden a proteger sus clientes (su dinero, obviamente, pero también sus datos, dada la sensibilidad de los datos que almacenan) y a mantener la confianza de clientes y *stakeholders* en un entorno cada vez más complejo y dinámico.

El sector bancario ha sido históricamente conservador ante la adopción de nuevas tecnologías y receloso en el intercambio de datos y en la cooperación entre entidades. La pandemia y su "nueva normalidad" ha forzado cambios bruscos en toda la humanidad y en todos los aspectos de nuestro día a día: trabajo, entretenimiento, compras, trámites, etc. Esto ha tenido un gran impacto en el sector financiero y en la gestión de la seguridad, acelerando tendencias y adopciones tecnológicas que se preveían casi imposibles hace unos años y que se han acabado produciendo en un periodo de tiempo muy corto.

En la era post-covid, creemos que esta tendencia ha llegado para quedarse, en un camino hacia la digitalización de todos los entornos, la automatización de procesos y la dependencia cada vez mayor en nuevas tecnologías que evolucionan muy rápido y requieren de una adopción más temprana.

Gran parte de esa innovación es orgánica dentro de los departamentos de seguridad de las entidades financieras y todo el ecosistema de sus proveedores, fabricantes y desarrolladores, que han entendido que requieren de una actualización continua para combatir a los ciberdelincuentes. Los propios proveedores de seguridad velan por su negocio y sus intereses evolucionando sus equipos y soluciones ante los *drivers* anteriormente mencionados, pero más allá de ello, los departamentos de seguridad son cada vez más pro-activos y estratégicos, con planes a largo plazo para la protección de sus entidades y la búsqueda continua de nuevas soluciones, con actividades de radar tecnológico de soluciones de ciberseguridad.

Podemos ver este radar tecnológico de la ciberseguridad como una actividad multidimensional en la que por un lado debe cubrir los principales aspectos de interés de las entidades financieras, desde la protección y resiliencia de infraestructuras críticas a la respuesta ante diferentes tipos de ciberataques o la gestión de identidades y usuarios privilegiados. Por otro, debe intentar cubrir todas aquellas tecnologías de mercado que puedan aportar valor, desde las provistas por grandes proveedores o integradas en grandes soluciones hasta aquellas más incipientes, de menor envergadura o con un impacto en un entorno mucho más concreto.

En ese afán ampliar la monitorización y de tener una mayor implicación del desarrollo de estas soluciones más concretas e incipientes que puedan tener un impacto en la digitalización y la seguridad del sector bancario, CaixaBank inició hace unos años su participación en proyectos Horizonte 2020. Horizonte 2020 (2014-2020) y posteriormente Horizonte Europa (2021-2027) son programas de financiación de la Comisión Europea para la investigación y la innovación. Su objetivo principal es garantizar que Europa produzca ciencia de primer nivel, elimine las barreras a la innovación y tenga impacto en la sociedad y en la competitividad del tejido industrial europeo. Entre otras formas, estos programas abordan este objetivo a través de convocatorias competitivas de proyectos, que deben ser realizados por consorcios público-privados formados por universidades, centros de investigación, pymes, grandes empresas y otras entidades.

Desde 2018, CaixaBank ha iniciado su participación en 10 proyectos con temáticas y líneas diversas, pero todos ellos con un foco en mejorar diferentes aspectos de la ciberseguridad y la prevención y detección del ciberfraude:

Es relevante el impacto que puede tener el aprendizaje automático federado o FML y de cómo la industria y en especial el sector bancario podría beneficiarse de modelos de IA colaborativos, enriquecidos con datos de múltiples entidades, que permitan mejorar la detección autónoma de ataques y sobre todo la detección y prevención del ciberfraude.

EU-SEC[1]: Desarrollar y validar un marco de trabajo innovador para la certificación de seguridad y privacidad de los servicios Cloud.

I-BIDaaS[2]: Analizar las posibilidades y beneficios de plataformas de *Big Data as a Service* en casos de uso de ciberseguridad y ciberfraude.

CONCORDIA[3]: Favorecer la colaboración intra y multisectorial en el intercambio y explotación de información de ciberinteligencia.

ENSURESEC[4]: Fortalecer las operaciones de *e-commerce* contra las amenazas físicas y ciber.

TRAPEZE[5]: Explorar el uso de *wallets* de identidad digital por parte de los clientes, permitiéndoles una gestión dinámica y en tiempo real de la privacidad de sus datos.

INFINITECH[6]: Aplicar IA para mejorar los modelos actuales de prevención de fraude en ciertas operativas bancarias.

REWIRE[7]: Establecer un marco estratégico para la cooperación europea en el ámbito de la educación y la formación en ciberseguridad.

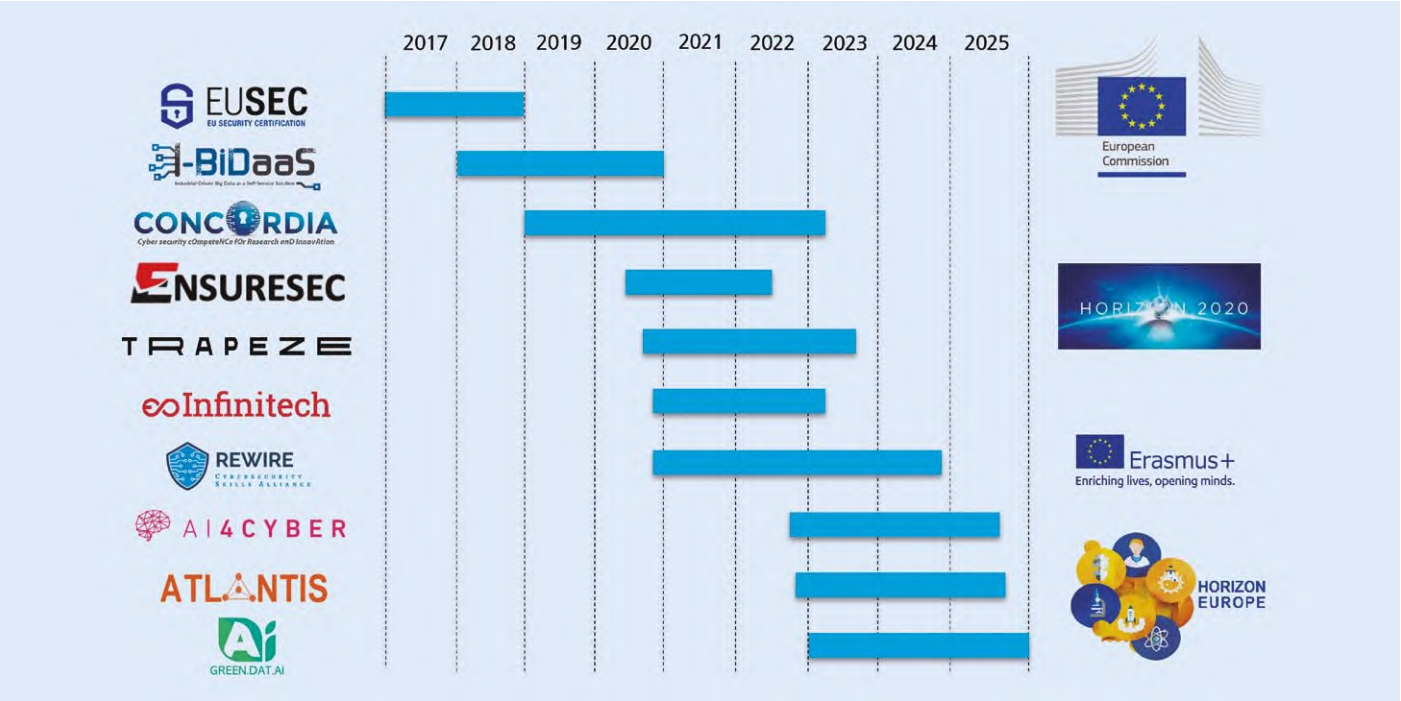
Forcepoint

Welcome to the power of ONE

Forcepoint ONE

ONE Platform
ONE Console
ONE Agent

www.forcepoint.com



AI4CYBER[8]: Desarrollar y explotar tecnologías basadas en IA para la administración de manera efectiva la seguridad, la resiliencia y la respuesta dinámica contra ataques cibernéticos avanzados.

ATLANTIS[9]: Mejorar la resiliencia y la seguridad ciberfísica de las infraestructuras críticas europeas.

GREEN.DAT.AI[10]: Aplicar herramientas de IA explicable y energéticamente eficientes en los sistemas de detección de fraude.

Tras varios años de participación en este tipo de proyectos, como se puede intuir en esta breve descripción de los mismos, las líneas evaluadas son diversas, aunque siempre alineadas con los objetivos estratégicos de la entidad. Como siempre en toda fase de innovación, los resultados y el impacto en la entidad no siempre han sido inmediatos, y requieren de un proceso de transferencia de conocimiento y transferencia tecnológica más allá del alcance de estos proyectos, y que debe recaer en las propias entidades tras la finalización de los proyectos.

Beneficios de participar en los proyectos

Aun así, basándonos en nuestra experiencia, creemos que el beneficio para las grandes empresas en la participación en este tipo de proyectos es muy alto y poco conocido. Este impacto trasciende los aspectos más tangibles como puede ser la adopción de algunas de las soluciones desarrolladas en el transcurso del proyecto, y tiene beneficios tanto directos como indirectos para la industria y para la ciberseguridad a nivel europeo.

Primero, la colaboración con el ecosistema universitario y de investigación da un punto de vista diferente que enriquece la visión de la ciberseguridad puramente operativa. Es un diálogo y un flujo de conocimiento en ambas direcciones. En muchos casos nos encontramos perspectivas completamente diferentes y que difícilmente llegan a una comprensión y alineamiento total entre ambas, pero aun así es provechoso realizar ese esfuerzo por el entendimiento y evaluar desde un prisma de un entorno empresarial real aquellas ideas que tienen el potencial de ir más allá de un laboratorio. Igualmente, en el otro sentido, es necesario que los académicos se nutran de la experiencia de las grandes empresas y entiendan las necesidades de ciberseguridad reales en la industria y el sector bancario. Solo así podrán comprender los retos reales y proponer soluciones adecuadas, aterrizando las ideas en casos concretos que pueden suponer un impacto.

Segundo, la influencia que se puede ejercer en los *roadmaps* estratégicos de la digitalización de la sociedad en Europa, participando activamente en los foros organizados por los órganos y gobiernos europeos y dando el *feedback* adecuado y necesario para alinear la innovación en Europa con las necesidades de las grandes empresas europeas.

Tercero, promover, participar y finalmente consolidar la soberanía tecnológica y digital europea. Hoy en día la dependencia de otras regiones como Estados Unidos o Asia sigue siendo demasiado grande. Si bien la debilidad tecnológica europea frente a estas otras regiones era conocida, ha sido durante la pandemia que hemos podido notar consecuencias mucho más palpables (retrasos, escasez de productos y servicios digitales, etc.). Es por ello por lo que Europa se ha marcado, más que nunca, como meta la consecución de esta soberanía tecnológica, intentando aumentar las capacidades de innovación en materias críticas para el futuro como la ciberseguridad, a la vez que marcando un marco regulatorio único a nivel global. Europa quiere mejorar su autosuficiencia, su resiliencia, y quiere jugar un rol específico y que sea indispensable a nivel global, y eso solo lo podrá conseguir con la participación activa del tejido industrial. ■

Ramon Martín de Pozuelo
Security Innovation Project Manager

Mario Maawad Marcos
Security Innovation and Red Team Director

CAIXABANK, S.A.

REFERENCIAS

[1] https://www.sec-cert.eu/
[2] https://cordis.europa.eu/project/id/780787
[3] https://www.concordia-h2020.eu/
[4] https://ensuresec.eu/
[5] https://trapeze-project.eu/
[6] https://www.infinitech-h2020.eu/
[7] https://rewireproject.eu/
[8] https://ai4cyber.eu/
[9] https://www.atlantis-horizon.eu/
[10] https://greendatai.eu/

WatchGuard

WATCHGUARD FOR SOC – EFICIENCIA Y PROACTIVIDAD

Empowering the SOC

Threat Hunting

Detección, investigación y respuesta

Ciber Resiliencia

Anticípate a las ciberamenazas en constante evolución

WatchGuard for SOC se basa en la combinación de soluciones de seguridad avanzada y plataforma de threat hunting para buscar, detectar y responder de manera eficiente a amenazas que hayan logrado evadir otras protecciones en endpoints, servidores, entornos virtuales y dispositivos móviles.

SEGURIDAD ENDPOINT AVANZADA

AUTENTIFICACIÓN MULTIFACTOR

SEGURIDAD DE RED

NUBE SEGURA WI-FI

Contacto: **900 840 407** **strategic.accounts@watchguard.com** **www.watchguard.com**

¡Cómo resolver el dilema de talento en ciberseguridad en tu empresa!

Actualmente, el talento en ciberseguridad está cobrando una mayor importancia en las empresas provocado principalmente por el aumento de amenazas cibernéticas y la necesidad de protección de datos y otros activos digitales. La falta de recursos y la escasez de profesionales de ciberseguridad cualificados para abordar estos desafíos, unido a los diferentes fenómenos psicosociales que se han dado en los últimos años, hacen que las empresas nos reinventemos y busquemos nuevas fórmulas para mitigar el impacto de la escasez de talento en ciberseguridad a nivel global.

Jennifer Sesmero

Atendiendo al contexto actual de incertidumbre y crisis económico social, se ha acelerado una profunda reflexión de los modelos de trabajo por parte de los individuos. Esta reflexión se ha materializado en el suceso denominado "la gran renuncia" que se dio en EE.UU. debido principalmente a las consecuencias del shock emocional que supuso la pandemia. Más de 47,8 millones de trabajadores de Estados Unidos en 2021, dejaron su empleo de forma voluntaria, según el Departamento de Trabajo. El efecto de este movimiento ha provocado que el 50% de los empresarios no puedan cubrir vacantes de empleo. Por otra parte, se ha visibilizado que muchos de estos perfiles que renunciaron a su puesto fue para obtener otro y con ello, mejorar sus condiciones laborales.

Esta situación ha evolucionado a otro fenómeno no menos preocupante, el denominado "*quiet quitting*", donde el propio empleado ciñe sus tareas a aquellas estrictamente descritas en su función y establece límites claros para mejorar el equilibrio entre el trabajo y la vida personal. Con esta práctica se podría llegar a suponer que el talento se autolimita y más en un mundo tan innovador y cambiante como es el de la ciberseguridad.

Una encuesta de 2021 de Gallup encontró que solo el 36% de las personas afirmaron estar comprometidas con su trabajo. Otras permanecen en sus trabajos y buscan uno diferente mientras cobran un sueldo fijo y disfrutan de sus beneficios, según otra encuesta realizada por LinkedIn.

La transformación digital agrava este problema según el reciente informe de (ISC)², el déficit mundial de talento en ciberseguridad aumentó un 26% en el último año hasta los 3,4 millones. Se necesitan en todo el mundo 8,1 millones de expertos en ciberseguridad, de los cuales actualmente estamos trabajando 4,7 millones de profesionales.

Y sin dejar de lado la gran ola de despidos en las grandes tecnológicas, que suman ya más de 150.000 bajas. Las diferentes causas y estrategias de reorganización de plantilla no permiten sacar conclusiones sobre una posible recesión en el mercado de perfiles tecnológicos, en concreto de ciberseguridad.

Las empresas tecnológicas, animadas por unos ingresos récord, emprendieron una carrera desenfrenada de contratación durante la pandemia. Los salarios alcanzaron niveles muy altos al mismo tiempo que por la competencia se disputaban a los mejores. Por este motivo, la media de un empleado en un mismo puesto, no superaba los 2 años. Y a medida que la vuelta a la normalidad se hacía más efectiva, llegaron los despidos.

Si analizamos esto último se evidencia que las compañías implicadas han integrado diversas razones para justificar esta decisión, que en su mayoría se reducen a la necesidad de minimizar costes a medida que el crecimiento económico se ralentiza a nivel global.

Pero lo más sorprendente es que el nivel medio de experiencia de los despedidos es de 11,5 años y es interesante observar que los puestos y funciones más afectados durante esta ola masiva de despidos fueron los de RR.HH., que representaron el 28% de todos los despidos, según el último informe publicado por Forbes.

Pero en lo que nos compete a nosotros, en cuanto a perfiles de ciberseguridad, para abordar este gran reto de talento, las organizaciones deberán plantear de forma diferente una estrategia com-

Figura 1

pleta en materia de gestión de talento 'end to end'.

Estrategia basada en unos principios de diseño que todas las compañías deberían integrar en su ADN acompañado de una serie de planes y programas. El objetivo es poder garantizar que en los próximos años dispongamos del mejor equipo y talento suficiente para hacer frente a las amenazas crecientes y poder mantener así los altos estándares de seguridad en las compañías.

En nuestro caso y para empezar a construir la estrategia de una forma consistente y sistemática, en BBVA nos apoyamos en cuatro principios de diseño.

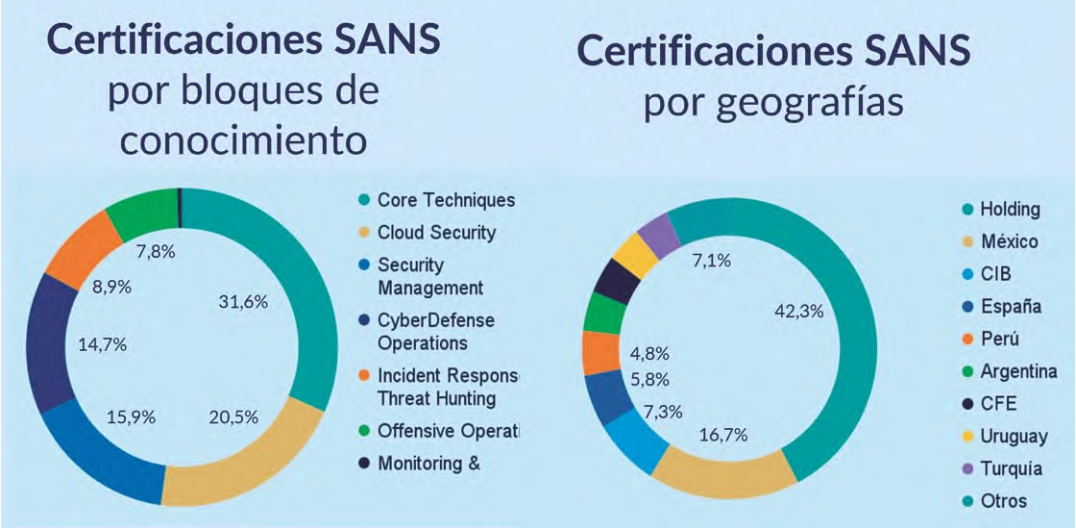


Figura 2

Estos cuatro principios son:

1. El objetivo es tener el mejor talento a nivel mundial.
2. BBVA tiene que posicionarse como marca empleadora de referencia en materia de ciberseguridad y mantenerse en el tiempo.
3. La prioridad es cuidar el talento interno.
4. Toda la gestión del talento ha de hacerse de forma global y homogénea.

Esto pasa por contratar a personas con experiencia en ciberseguridad, formar nuevos profesionales a través de programas de capacitación, tanto internos como externos, y desarrollar soluciones tecnológicas avanzadas para prevenir y detectar amenazas.

– Talento interno, de cualquier área del Grupo.
– Talento externo.

En cuanto a talento experto a continuación detallo algunas habilidades y conocimientos, que en BBVA consideramos que debe tener un perfil de ciberseguridad y en base a ello, vamos a ver de qué palancas disponemos internamente para poder desarrollar y retener al talento.

Cuando hablamos de talento experto en ciberseguridad hablamos de uno muy específico que tiene la capacidad de aprender rápidamente. El campo de la ciberseguridad es un campo muy cambiante y los profesionales deben estar constantemente actualizándose. Por ese motivo una de las herramientas que nosotros tenemos para retener el talento y desarrollarlo, es **la palanca formativa**.

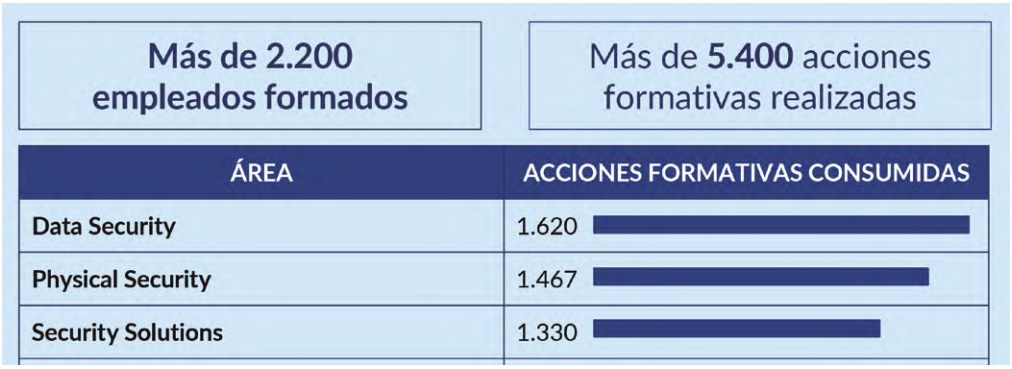


Figura 3

La estrategia se tendrá que definir atendiendo a diferentes ámbitos de actuación y para cada uno de ellos se definen planes y acciones que se deben llevar a cabo para hacer una gestión integral del talento y con ello atraer, retener, desarrollar y motivar a los profesionales.

Los ámbitos en los que se deberá centrar la estrategia son:

– Talento experto en ciberseguridad.

También necesitan disponer de una comprensión profunda de la tecnología en la mayoría de los perfiles y para ello, debemos actualizarnos constantemente con las principales tendencias del mercado. Otra de las características que define un experto en ciberseguridad es que, en la mayoría de los casos, son autodidactas y para ello deben disponer de una amplia oferta formativa para poder estar en aprendizaje continuo. Además, deben disponer de fuertes habilidades de comunicación para poder transmitir los riesgos y amenazas a los diferentes usuarios. Y, por último, a todo ello, le añadimos las habilidades de innovación para reforzar las capacidades a la hora de recopilar y clasificar la información, así como realizar análisis profundos para determinar el origen de una vulnerabilidad.

Para ello, BBVA impulsa un programa basado en certificaciones SANS con más de 395 certificaciones impartidas en todo el Grupo. Estas son reconocidas a nivel mundial como una de las mejores formas de demostrar la competencia de un profesional en materia de ciberseguridad.

Además, contamos con un amplio catálogo de formación experta compuesta por más de 80 cursos con contenidos en ciber y generada dentro de la organización por los propios expertos en ciberseguridad. Esto nos permite llevar a cabo el "reskilling" de empleados de otras áreas del Grupo y el "upskilling" entre las diferentes funciones con las que contamos en ciberseguridad.

En la **Figura 3** se muestran las cifras de los empleados formados y de las acciones formativas realizadas dentro del grupo, hasta la fecha. Más de 2.200 empleados están formados en contenidos expertos de ciberseguridad, pero cabe destacar, que a día de hoy más de 97.000 empleados en el Grupo BBVA tienen unos conocimientos básicos en materia de ciberseguridad.

Con todo ello, nos damos cuenta que las palancas más efectivas de las que se disponen en las empresas para consolidar el compromiso de los empleados son: la formación que permite el "upskilling", el

"reskilling" de los empleados, además de la implementación de políticas claras de incentivos y desarrollo de carrera. Todas estas son palancas conocidas que no necesariamente cubren las necesidades de todos los empleados.

Debido a la heterogeneidad de perfiles y circunstancias de cada uno, **si queremos ser eficientes y efectivos**, tenemos que llevar a cabo una **estrategia más personalizada** que nos permita saber las necesidades de cada empleado y dirigir los esfuerzos a aquellas tareas que serán más efectivas de cara a la retención y el aumento de compromiso.

La combinación de estos dos ejes ayuda a desarrollar la capacidad que tenemos como organización para retener el talento clave.

Por otro lado, tenemos el talento interno. Nos referimos a cualquier empleado que trabaje dentro de la organización y que no se encuentre en el equipo de ciberseguridad y que en algún momento se haya planteado realizar un "reskilling" a la función de ciberprotección y por ende, cambiar de profesión. Para la gestión de este colectivo cabe destacar que, según una noticia publicada por IBM, **contratar a un nuevo empleado puede costar de 1,5 a 6 veces más, que cubrirla con talento interno.**

Hay que apostar por capacitar y desarrollar nuestro talento interno. Y para ello, debemos activar dos palancas: La primera y la más importante es a través del conocimiento. Poner a disposición del empleado, la formación más experta desde un nivel más básico "partiendo de 0", pasando por un nivel medio y llegando al avanzado. Nos puede conducir hacia un "reskilling" completo en un periodo de dos años a la función de ciberseguridad. Además, si disponemos de una segunda palanca, un programa de *mentoring* en el que vayamos guiando al empleado en función de sus capacidades y habilidades hacía la función de ciberseguridad dónde más puede aportar, el éxito está garantizado.

Y por último y no menos importante, cómo atraemos al talento que se encuentra fuera de nuestra organización para que venga a trabajar con nosotros y nos vea una entidad atractiva para ello, donde pueda crecer y desarrollarse como profesional.

Si nos basamos en nuestros principios de diseño, tenemos que conseguir ser una marca empleadora de referencia en materia de ciberseguridad y contar con el mejor equipo. Para ello, necesitamos **escuchar las necesidades del mercado**, **identificar** cuáles son los **nichos** a los que podemos asistir para hacer marca y **captar al mejor talento.** Además, debemos apoyarnos en otros departamentos dentro de la compañía como RR.HH., marketing, comunicación y otras áreas clave que nos ayuden a activar los mecanismos para poder captarlo y seleccionarlo de una forma eficaz.

Nosotros desde el Grupo BBVA, hemos compartido de forma masiva nuestro saber y experiencia poniendo a disposición de la sociedad todo el conocimiento a través de una serie de itinerarios formativos en la plataforma internacional **Coursera.** Con este lanzamiento abierto y gratuito a cualquier persona ofrecemos contenidos específicos y pioneros de ciberseguridad al alcance de todo el mundo. A través de tres itinerarios formativos completos en materia de ciberseguridad: "Cybersecurity for Managers", "Cybersecurity for tech professionals" y por último "Data & Cybersecurity". En la **Figura 4** se muestran nuestros resultados a nivel global. Y en la **Figura 5** geográficamente, dónde se están consumiendo mayormente nuestros contenidos.

Figura 4

Nuestro objetivo como área especializada en ciberseguridad es atraer talento externo y experto a nuestra compañía, compartir nuestro conocimiento para aprender juntos y, sobre todo, llevar nuestras habilidades y experiencias a la sociedad para generar oportunidades para todos. Estas son algunas de las principales prioridades de nuestra organización.

Figura 5

Al llegar a todos los perfiles de tu organización, generas una cultura de seguridad que despierta la inquietud, activa la motivación y habilita las palancas necesarias para llevar a cabo un "reskilling" al mundo ciber de algunos perfiles. Al mismo tiempo, si aportas como valor añadido el conocimiento interno que posees fuera de las fronteras de tu compañía, contribuyes a minimizar el impacto de la brecha de talento que sufrimos en el campo de la ciberseguridad, ayudando a disponibilizar un mayor número de profesionales cualificados a nivel mundial. ■

Jennifer Sesmero Camacho
Global Talent & Training in Cybersecurity
BBVA

Cualquier nube

Transformación empresarial

Fusiones y adquisiciones

Cambios empresariales

Trabajadores híbridos

Automatización

Seguridad que está lista para + Cualquier situación

Nuevos riesgos

Convergencia

Amenazas internas

Lo inesperado

Su próximo gran movimiento

+

Netskope, líder global en ciberseguridad, está redefiniendo la seguridad de la nube, las redes y los datos, para ayudar a las organizaciones a aplicar principios de Zero Trust y proteger su información. La plataforma inteligente Netskope Security Service Edge (SSE) es rápida, fácil de usar y protege las personas, los dispositivos y los datos dondequiera que vayan, pase lo que pase.

Conozca cómo Netskope ayuda a sus clientes a estar listos para cualquier situación, visite netskope.com/es

netskope

Despliegue de un marco de control integrado y automatizado: una respuesta eficaz y eficiente a los retos de ciberseguridad de una entidad aseguradora

Nuevas directrices europeas de EIOPA y DORA están impulsando a las organizaciones del sector seguros a reforzar su función de seguridad de la información para dar una respuesta eficaz y eficiente a los retos y riesgos asociados a un entorno cada vez más complejo y competitivo. Una de las herramientas que permiten evolucionar esta función es dotarse de un marco de control integrado y automatizado. La construcción de este marco debe ser un proceso ordenado e incremental, en el que las organizaciones deben involucrar a responsables de diferentes áreas y con capacidades y conocimientos diversos. En aquellas organizaciones con un nivel de madurez adecuado, la implantación de una herramienta GRC como soporte permitirá optimizar aún más la gestión de la seguridad, ofreciendo una mayor visión del estado de la organización e involucrando a un mayor número de empleados y, como consecuencia, incrementando el nivel de concienciación global en materia de ciberseguridad.

Alberto Bernáldez / Jesús Urién

Un marco de control integrado y adaptado a las necesidades regulatorias y de negocio.

La importancia de la ciberseguridad en las organizaciones ha ido adquiriendo una mayor relevancia durante los últimos años. En demasiados casos, el crecimiento exponencial tecnológico y la transformación digital que ha ido experimentando la sociedad y, por ende, las organizaciones, no ha ido acompañado de un incremento de la inversión en ciberseguridad.

A grandes rasgos, podemos afirmar que el crecimiento tecnológico ha ido siempre un paso por delante de la ciberseguridad en las organizaciones. Ante esta situación, las compañías deben actuar rápidamente, anticipándose a los escenarios tecnológicos futuros y actuando de manera preventiva para la identificación de nuevos aspectos a incluir en sus marcos de control y en sus líneas de defensa. De esta forma, se pueden evaluar, monitorizar y controlar los diferentes escenarios de riesgo asociados antes de que se materialicen y se puede actuar con mucha más eficacia y rapidez cuando sucede.

En un escenario con cada vez más exigencias regulatorias en el marco europeo y en el que la seguridad de la información es un requisito ineludible, abordar un proceso de integración del marco de control de seguridad de la información de las organizaciones, así como a las diferentes necesidades de negocio de una forma global, facilitará la operativa y dará un mayor nivel de confort a los diferentes interesados. En este proceso, deben tenerse en cuenta algunos aceleradores como son aprovechar los recursos ya disponibles y los mecanismos desplegados y diseñar un proceso de transformación que asegure una transformación efectiva del marco de control, involucrando a las tres líneas de defensa:

- **Primera línea de defensa:** Evolución del marco de control para dar respuesta a los retos de ciberseguridad actuales y a las regulaciones europeas aplicables a la organización.

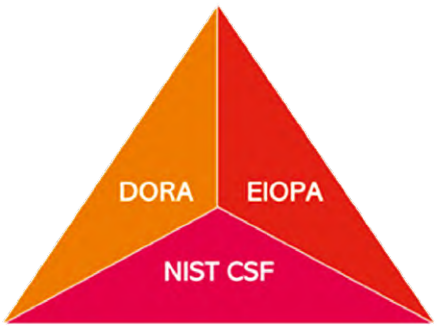


Figura 1

- **Segunda línea de defensa:** Implementación de los controles definidos en el marco de control integrado a partir de una herramienta GRC de referencia para asegurar una eficaz gestión tanto de los riesgos como del cumplimiento de los controles a través de ella.
- **Tercera línea de defensa:** Asegurar la efectividad de la implantación de este nuevo modelo de gestión de la ciberseguridad a partir del proceso de Auditoría Interna.

Otro de los aspectos clave es adoptar una visión amplia de la ciberseguridad en la que ésta no se conciba como un conjunto de mecanismos de protección independientes para salvaguardar los sistemas de información de la organización ante un ataque, sino que vaya mucho más allá y se alinee con la estrategia de negocio de la organización. Además, ésta debe de disponer de una planificación clara y de una monitorización continua para que en todo momento se mantenga este alineamiento en los diferentes niveles jerárquicos y funcionales, desde la capa de directiva, pasando por todos los empleados y llegando a proveedores y terceros.

Sin duda, un modelo con esta visión supone un gran reto para las organizaciones con el hándicap añadido de que en estos casos el tiempo no es un aliado, ya que una vez definido el modelo deseado, poder contar con él de la manera más temprana posible debe ser una prioridad que permita reducir la incertidumbre asociada a todo riesgo.

Una de las claves para conseguir llegar a un modelo adecuado es apoyarse en un estándar internacionalmente reconocido como es NIST CSF con el que poder asegurarse que se tienen en cuenta los aspectos de seguridad globalmente aceptados, siendo además el modelo reconocible por los equipos, clientes y resto de interesados de la organización en todo el mundo.

Estándares internacionales: elementos clave para la creación de un marco de control robusto

Una de las claves para conseguir llegar a un modelo adecuado es apoyarse en un estándar internacionalmente reconocido como es NIST CSF. Contando con un estándar de estas características, las organi-

zaciones podrán asegurarse de que tienen en cuenta los aspectos de seguridad globalmente aceptados, siendo además el modelo reconocible por los equipos, clientes y resto de interesados de la organización en todo el mundo. Además, integrar un estándar de referencia con las directrices aplicables en el sector de la organización facilita el despliegue de este marco de controles.

En el caso de una organización dentro del sector asegurador nacional y europeo, la integración en el marco de EIOPA y DORA no pueden faltar. Por otro lado, y en los casos en los que la complejidad sea alta y con presencia en varios mercados, gestionar el marco con el apoyo de una herramienta GRC puede ser un aspecto clave de éxito. No obstante, el marco y la herramienta deben ir acompañados de un conjunto de procesos diseñados para el contexto de cada organización y una gestión del cambio adecuada que garantice un uso efectivo.

Figura 2

Definición de la metodología adecuada: acelerador para el despliegue del marco de control integrado

Dentro del contexto planteado, no debemos olvidarnos de otro de los factores críticos de éxito: la metodología utilizada. Durante las fases iniciales del proyecto es imprescindible analizar en detalle el conjunto de estándares para partir de aquel que pueda adecuarse mejor a la organización. Una de las opciones que actualmente se encuentran entre las más convenientes a nivel general es la utilización de NIST CSF, aunque no deben olvidarse otros como ISO 27001, e incluso integrar partes de interés cuando haya aspectos de valor para la organización.

Una vez definida la base del marco a integrarse, deben plantearse posibles necesidades adicionales de la organización y los requerimientos derivados de las regulaciones europeas propias del sector (EIOPA y DORA en el caso del sector seguros) en un marco único y completamente integrado entre sí, aprovechando las sinergias detectadas entre ellas.

En este punto, una de las decisiones a considerar, y que pueden facilitar la gestión del cambio, es partir del modelo que tenga definido la organización, aprovechando de este modo las sinergias que puedan darse, así como los procesos ya definidos en la compañía, en lugar de comenzar desde cero, lo cual podría resultar más sencillo desde un punto de vista teórico, pero suponer un esfuerzo mayor de transición y adaptación para los distintos involucrados.

Para tener éxito en este ejercicio, contar con un equipo con altos conocimientos del sector, la organización, la regulación y los estándares seleccionados será fundamental. Además, analizando bien la situación, podrán identificarse aspectos que, con un pequeño reenfoque, puedan ser totalmente integrados en el nuevo modelo, acelerando el periodo de implantación.

Esta combinación y la correcta cohesión de los equipos de trabajo participantes garantizarán la consecución de los objetivos. En este contexto, algunas de las claves de éxito son (ver **Figura 2**): En primer lugar, gestionar el proceso de implantación y transformación desde una perspectiva global, resulta clave en el desarrollo del proyecto. Esto permitirá la identificación de sinergias entre los diferentes procesos y controles de la organización y adaptarse en todo momento a la realidad de las evidencias y los sistemas disponibles.

Figura 3

Definir un proceso iterativo de evaluación permitirá obtener una mejora continua e incremental en el marco de control a medida que se avance en su desarrollo. La flexibilidad de la que pueda disponer el marco de control otorgará a la organización la capacidad para dar respuesta a los retos de ciberseguridad que vayan surgiendo, permitiendo tener los riesgos asociados controlados y en unos niveles aceptables por la compañía.

Además, establecer un modelo que permita realizar un análisis para identificar el nivel de madurez al inicio del proceso, definiéndose objetivos a corto-medio plazo para incrementar el nivel de madurez de la organización de una forma progresiva permitirá gestionar expectativas y avanzar al ritmo adecuado para los diferentes interesados y necesidades de la organización.

Herramienta GRC: un apoyo de valor

Con el objetivo de optimizar al máximo el proceso de gobierno y gestión de la seguridad a través del marco de control integrado, es recomendable apoyarse en una herramienta GRC para facilitar la gestión de cambio y la puesta en funcionamiento de los procesos y la operación del marco.

La **Figura 3** resume los beneficios de apoyarse en una herramienta GRC, frente al uso de procesos manuales durante la evaluación del marco de control.

El uso de una herramienta de este tipo permite a las organizaciones que disponen de un marco de madurez maduro y bien definido, aumentar el nivel de automatización del proceso de gestión de la seguridad, reduciendo el número de tareas manuales y errores humanos asociados, aumentar el control sobre el proceso de evaluación del marco de control mediante una imagen real del nivel de riesgo de la organización y llegar a un mayor número de empleados aumentando el nivel de concienciación global de la organización en materia de ciberseguridad.

Pese a que las herramientas GRC ofrecen una solución eficaz para el gobierno del riesgo y su cumplimiento en su versión estándar, algunas organizaciones presentan necesidades muy concretas que no ha contemplado el fabricante. Para dar respuesta a estos requisitos, la adaptación de la herramienta GRC a las necesidades de cada organización se convierte en un componente muy relevante del proceso, en el que se involucran los diferentes departamentos de cada organización que la utilizarán. Cada área debe exponer sus requisitos que debe-

rán ser unificados, buscando incompatibilidades y definiendo unas bases firmes para los futuros desarrollos.

La mayoría de las herramientas GRC se comercializan con un enfoque modular, donde las organizaciones deciden cuáles son los casos de uso que incluyen en su instalación. Estos casos de uso están integrados entre sí y permiten la compartición de información entre los diferentes inventarios utilizados por las áreas. En ocasiones, el mismo módulo se puede aprovechar para dar respuesta a las necesidades de diferentes áreas de la organización. En cuanto a la decisión de adquirir nuevos módulos de la herramienta o adaptar los ya existentes, la decisión dependerá tanto del nivel de personalización que ofrezca la herramienta utilizada, como del modelo desplegado en cada organización.

Además, el uso de una herramienta GRC, permite a los diferentes empleados de una organización afectados por este nuevo marco de control, automatizar aquellas tareas que actualmente realizan de una forma manual, reduciendo el tiempo dedicado a las mismas y aumentando la cooperación entre los diferentes responsables.

Al automatizar estas acciones se reduce el número de errores humanos y los responsables pueden dedicar el tiempo del que disponen a la realización de tareas que aporten un mayor valor al proceso de evaluación. Por otra parte, a medida que se avanza en el proceso de evaluación de un nuevo marco de control, los diferentes usuarios de la herramienta identificarán nuevas oportunidades de mejora a implementar tanto en la herramienta como en el marco de control, que una vez desplegadas permitirán continuar evolucionando el proceso.

Es importante recalcar que la implantación y adaptación de una herramienta GRC a las necesidades de una organización es un proceso completo, en el que se recomienda involucrar a los diferentes responsables de cada departamento afectado.

La fase inicial de la implantación de una herramienta GRC debe realizarse en conjunto con los diferentes responsables para entender su forma de trabajar y definir unos flujos de trabajo adaptados a la organización. Una vez se han identificado los requisitos, se comenzará con el desarrollo de las adaptaciones y la carga de la información en la herramienta.

Durante esta fase de desarrollo, es importante contar con la disponibilidad de los principales responsables para identificar cualquier desviación en los requisitos solicitados. Estos usuarios, serán los encargados de realizar las pruebas de usabilidad de la herramienta y notificar los resultados al equipo correspondiente.

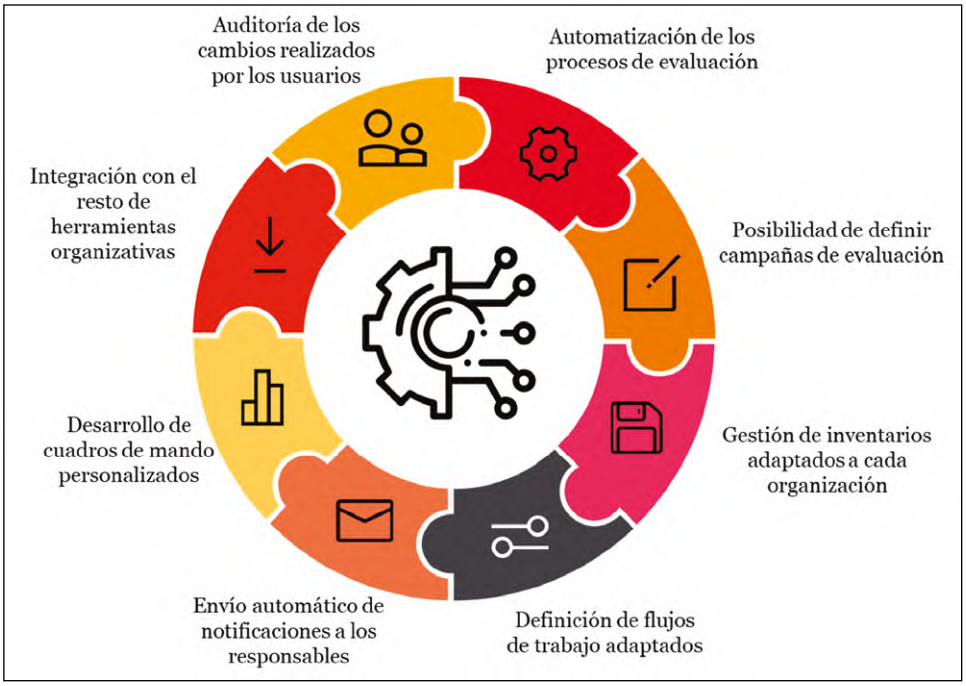


Figura 4

La mayoría de las herramientas GRC se comercializan con un enfoque modular, donde las organizaciones deciden cuáles son los casos de uso que incluyen en su instalación. Estos casos de uso están integrados entre sí y permiten la compartición de información entre los diferentes inventarios utilizados por las áreas.

En una fase final de la implementación, se debe realizar la formación a los usuarios de la organización, lo cual es un proceso clave para favorecer la adopción de la herramienta en la organización, para ello, es necesario realizar sesiones de formación y elaborar la documentación asociada para que puedan ver la herramienta en funcionamiento y conocer los diferentes menús y opciones disponibles.

Algunos beneficios que podrán obtenerse a través del apoyo en una herramienta GRC son:

- **Posibilidad de disponer de toda la información** acerca de las evaluaciones de la organización en un repositorio centralizado que permita la reutilización de las evidencias y la información ya incluida en la herramienta en otros marcos de control.
- **Gestión automática de los flujos de evaluación** y envío de notificaciones a los diferentes responsables involucrados en el proceso de evaluación, en base a las condiciones definidas en cada normativa.
- **Disponer de cuadros de mando y gráficos adaptados** a los diferentes responsables de la organización para que puedan consultar el estado del proceso de evaluación en todo momento.
- **Auditoría de todos los cambios realizados** por los usuarios en el marco de control y sus respectivas evaluaciones, generando un histórico de versiones de los diferentes controles incluidos en el marco de control.

Integrar y automatizar: Una práctica aconsejable

En definitiva, la definición de un marco de control integrado y automatizado en un entorno regulado, como es el caso del sector seguros, permite dar respuesta tanto a los requisitos de cumplimiento como a las necesidades del negocio. En el caso de aquellas organizaciones que presenten un nivel de madurez adecuado, la implementación de ese marco en una herramienta GRC que evolucione a la vez que éste, permitirá mejorar el proceso de evaluación, ofreciendo una visión global sobre el estado de la organización y generando una mayor cultura de la ciberseguridad dentro de la organización. ■

Alberto Bernáldez
CISO
Sector Asegurador

Jesús Urién
Director en Business Security Solutions
PwC

Cuando la tecnología permite el progreso,
ESET está aquí para protegerlo.

www.eset.es

ESET®
Digital Security
Progress. Protected.

>> Jorge Dávila

E pur si muove! [1]

Después de la efervescencia generatriz de algoritmos criptográficos de la última década del siglo pasado, ha venido una calma –algo chicha– a principios de este siglo. Sin embargo, las cosas no han estado completamente quietas. La previsible llegada y generalización de la IoT general y de la OT industrial, así como la amenaza de un posible computador cuántico, han hecho que la administración norteamericana (el NIST) "toque a arrebato" y se desarrollen en el mundo lo que se llaman Criptografía Ligera y Criptografía Pos-cuántica. Va siendo hora de que echemos un vistazo en esta columna de qué va todo esto.

En 1633 el humanista italiano conocido como Galileo Galilei[3] (1564-1642) tuvo que agachar la cabeza ante la imponente y arrasadora iglesia católica, materializada en la organización teoterrorista conocida como la Inquisición o el Tribunal del Santo Oficio[4]. En aquella ocasión tuvo que abjurar de su teoría heliocentrista de que es la Tierra la que gira alrededor del Sol y no al revés. Dice la leyenda que al terminar el oficio, masculló aquello de "*Sin embargo se mueve*", como queriendo no resistirse del todo ante la obcecación de los que no querían perder su poder alienante frente a las masas y seguir determinando a capricho lo que era verdad y lo que no.

El control de las masas siempre ha sido algo a lo que los poderosos siempre han prestado mucha atención. Hoy en día hablamos de noticias falsas[5], de la posibilidad más que probable de que las "redes sociales" existan sólo para poder espiar a todo el mundo. Hoy es Tik Tok la que está en los titulares[6] pero, realmente, no creo que se salve ninguna de ellas.

Es cierto que esa aplicación de videos cortos es **increíblemente adictiva** y que ya la usan más de **1.000 millones de personas** en todo el mundo, lo que le podría llegar a suponer más de 18.000 millones de dólares en publicidad sólo en este año. Es cierto también, que se concentra peligrosamente en los más jóvenes y en las personas más vulnerables[7], por lo que en si misma constituye una peligrosa y amplia ventana de riesgo para todas las sociedades, occidentales y orientales, a medio y largo plazo.

Sin embargo, la manipulación de las masas[8], el poder determinar lo que piensan, lo que creen, el modo en que se comportan, lo que anhelan y desean, siempre ha sido el objetivo de muchos poderes; el político[9], el religioso[10], el cultural[11], el empresarial[12], etc., por lo que esta amenaza no se trata de nada realmente nuevo. Lo único nuevo es la magnitud del proceso, la cantidad de seres humanos a los que se puede alienar **con sólo una aplicación informática y mucha Internet**.

Según los medios de comunicación de todo tipo, hay frentes en los que parece focalizarse toda la actividad actual en los temas de informática o desarrollo digital. Por un lado está **1)** la muy manida "Inteligencia Artificial" y su vacuo charlatán conocido como chatGPT, y por otro, **2)** la "inminente" llegada del mesías de la computación en la forma de "Computador Cuántico". Sin embargo, hay otros frentes digitales que también se mueven y sus derroteros[13] pueden poner en riesgo o salvar la evolución de nuestra realidad más global y más cotidiana a medio y largo plazo.

La escasez de algoritmos criptográficos asimétricos, la opción de utilizar planteamientos matemáticos para elegirlos y la "amenaza cuántica", han ocupado en estos últimos años a los criptógrafos de todo el mundo.

Un microcontrolador es un circuito integrado programable, capaz de ejecutar las órdenes (comandos) grabadas en su memoria. Esos dispositivos están compuestos por varios bloques funcionales diseñados para atender a tareas específicas como son la unidad central de procesamiento, la memoria y los periféricos de entrada/salida.

Se dice que el primer microprocesador lo creó la compañía Intel y fue el **Intel 4004**[14] que trabajaba con valores de 4 bits y que fue lanzado al mercado en noviembre de 1971. Poco después, ese diseño fue seguido por el muy popular **Intel 8008**[15] y otros microprocesadores más potentes. Otras fuentes dicen que fueron los ingenieros de Texas Instruments **Gary Boone** y **Michael Cochran** los que crearon el primer microcontrolador, el **TMS 1000**[16], también en el año 1971, aunque no fue comercializado hasta 1974.

En aquellos años, ZiLOG fue un fabricante de microprocesadores, siendo su producto más conocido el **Zilog Z80** que trabajaba con registros de 8 bits. De hecho, ZiLOG Inc.[17] fue la primera compañía dedicada exclusivamente a la venta de microprocesadores. Fue fundada por Federico Faggin a finales del 1974, y su desarrolló más exitoso fue el microprocesador **Z80**[18] que se popularizó en los años 1980 por ser el alma de ordenadores muy populares como el **Sinclair ZX Spectrum**[19], **Amstrad**

[1] La expresión italiana "*E pur si muove!*" o "*Eppur si muove!*" que significa "*Y sin embargo gira*", literalmente: "*y sin embargo se mueve*".
[2] Ver https://en.wikipedia.org/wiki/Public-key_cryptography
[3] Ver https://en.wikipedia.org/wiki/Galileo_Galilei
[4] Ver https://es.wikipedia.org/wiki/Inquisición_española
[5] Ver https://en.wikipedia.org/wiki/Fake_news
[6] Ver https://www.elmundo.es/economia/2023/03/23/641ca8ad21efa078638b4599.html
[7] Ver https://www.diariodesevilla.es/salud/investigacion-tecnologia/Tiktok-peligrosos-efectos-invisibles-salud-mental-jovenes_0_1727528002.html
[8] Ver https://concepto.de/propaganda/
[9] Ver https://es.alphahistory.com/guerra-Fr%C3%ADa/propaganda-de-la-guerra-fría/
[10] Ver https://compolitica.com/iglesia-y-propaganda-dos-milenios-de-persuasion-desde-la-silla-de-san-pedro/
[11] Ver https://en.wikipedia.org/wiki/Reich_Ministry_of_Public_Enlightenment_and_Propaganda
[12] Ver https://en.wikipedia.org/wiki/Marketing
[13] Derrotero; De derrota 'camino, rumbo'. 1. Camino, rumbo, medio tomado para llegar al fin propuesto. 2. Conjunto de datos que indican el camino para llegar a un lugar determinado 3. Línea señalada en la carta de marear para el gobierno de los pilotos en los viajes. 4. Dirección que se da por escrito para un viaje de mar.
[14] Ver https://es.wikipedia.org/wiki/Intel_4004
[15] Ver https://es.wikipedia.org/wiki/Intel_8008
[16] Ver https://en.wikipedia.org/wiki/Texas_Instruments_TMS1000
[17] Ver https://en.wikipedia.org/wiki/Zilog
[18] Ver https://es.wikipedia.org/wiki/Zilog_Z80
[19] Ver https://es.wikipedia.org/wiki/Sinclair_ZX_Spectrum
[20] Ver https://es.wikipedia.org/wiki/Amstrad_CPC
[21] Ver https://en.wikipedia.org/wiki/Embedded_system
[22] Ver https://en.wikipedia.org/wiki/Arduino
[23] Ver https://en.wikipedia.org/wiki/Mbed

CPC[20] o de los ordenadores de sistema **MSX** presentado por Microsoft y ASCII Corporation en junio de 1983.

El Z80 Es uno de los procesadores de más éxito del mercado y prueba de ello lo son la infinidad de versiones clónicas que se han fabricado desde entonces, y aún hoy sigue siendo usado de forma extensiva en multitud de **sistemas embebidos**[21].

Los sistemas embebidos se fabrican en el rango de los millones de unidades con lo que se puede obtener muy significativas reducciones de costes a la vez que **se implantan en innumerables escenarios de todo el mundo**. Los sistemas embebidos suelen utilizar procesadores relativamente pequeños y lentos, con una memoria también pequeña y todo lo necesario para que funcionen de forma esencialmente autónoma. Los primeros equipos embebidos los desarrolló IBM en los años 1980 y, en general, se emplean en tareas de **procesamiento en tiempo real**.

Actualmente existen plataformas desarrolladas por distintos fabricantes que proporcionan herramientas muy cómodas para el diseño y desarrollo de aplicaciones y prototipos con sistemas embebidos a través de intuitivos entornos gráficos como son los casos de **Arduino**[22], **Mbed**[23], **Raspberry Pi**[24], **BeagleBone**[25], etc. Aunque este fenómeno emana de las décadas del final del Siglo XX, su popularidad no llega hasta que se empieza a hablar[26] de la **Internet de las Cosas**[27]. Aunque algunos puedan pensar que esto de la IoT es algo moderno, deberían saber que todo esto empezó en 1982 con una máquina expendedora de Coca-Colas ubicada en la Universidad de Carnegie Mellon[28], y de la cual Internet (la comunidad) quería saber si las latas estaban frías o no.

Son dos los nichos actuales en los que la IoT se ha ido desarrollando sigilosamente; uno de ellos es la **Domótica** o **Automatización del Hogar**[29], y por otro el **cuidado de ancianos**[30]. En la domótica, los dispositivos IoT incluyen sistemas para el control de la iluminación (intensidad y color), del acondicionamiento térmico (calefacción y refrigeración), del ambiente sonoro y visual (música y video ambiental), de los sistemas de seguridad perimetral y funcional de la casa (cámaras de vigilancia, sensores y actuadores de todo tipo), etc.

En principio, de esa automatización serían esperables beneficios a largo plazo como el **ahorro energético** al poder apagar automáticamente aquello que no sea necesario en cada momento[31]. Las casas inteligentes (*Smart* o *Automated Home*) contienen plataformas agregadoras que reúnen en ellas el control de numerosos dispositivos inteligentes especializados en funciones variopintas. Ejemplos de ello hay varios; por un lado tenemos el Apple's HomeKit[32] que permite poner todo lo importante de una casa a las órdenes del teléfono iPhone o de un Apple Watch; y con ello a las órdenes de cualquier aplicación nativa IOS como pueden ser asistentes como Siri, lo cual no es excepcional.

Hay plataformas que, como parte de su atractivo comercial, se pueden conectar a diferentes agentes domésticos digitales como son Echo Dot y Alexa[33] de Amazon, Home[34] de Google, HomePod[35] de Apple, y el SmartThings Hub[36] de Samsung. Además de los sistemas propietarios, también hay iniciativas de código abierto como son Home Assistant[37], OpenHAB[38] y Domoticz[39], entre otras.

Una de las justificaciones más eficaces para la automatización y monitorización del hogar está la **asistencia a ancianos** y **discapacitados** funcionales de algún tipo. Aquí se incluyen asistentes de voz para aquellos con problemas de vista o movilidad reducida, y aquellos sistemas de alerta que van directamente conectados a los implantes cloqueares de aquellos que tienen problemas auditivos. También se pueden conectar otros sensores que son sensibles a estados de emergencia médica (caídas, lipotimias, crisis glucémicas, etc.)

Además de todos estos usos "*para particulares*", no hay que olvidar que la IoT también ha colonizado los sistemas industriales a modo de evolución natural de los sistemas de automatización industrial anteriores. En este caso, es todo el sistema productivo industrial el que se pone a los pies de la nueva **OT** (**Operative Technology**)[40], que es como gustan llamar a la IoT industrial sus promotores. Para 2019 ya se estimaba que el número de artefactos IoT superaría los 9.100 millones de dispositivos[41].

Lo curioso de esta historia, es que **sus necesidades de seguridad**, en el sentido más amplio posible y en el de la ciberseguridad en concreto, es algo que **no se han tenido en cuenta**, **están pendientes**, y que ahora parecen saltar al candelero.

El primer cifrador civil se diseñó entre 1971 y 1973, y se llamaba **Lucifer**[42]. Su razón de ser fue un encargo que hizo el LLoyd's Bank de Londres a IBM[43] para poder proteger las comunicaciones digitales de lo que era, por aquel entonces, la joya tecnológica del sistema bancario: los "cajeros automáticos"[44].

El otro frente que tiene abierto la seguridad criptográfica actual es el de la amenaza cuántica. Sin entrar en si es realmente tal o una versión moderna del clásico sacamantecas del siglo XIX utilizado, esencialmente, para meter miedo, lo que si es cierto es que la Criptografía Asimétrica[2] lleva más de cuarenta años tentando a su suerte.

Convenientemente "tuneado" por la NSA, el algoritmo Lucifer se transformó en el muy popular **DES** (**Data Encryption Standard**)[45]; que en febrero de 1977 paso a ser el estándar de cifrado[46] de la administración norteamericana. En principio esto iba a ser así durante sólo cinco años, pero ese algoritmo fue renovado en su puesto hasta el 26 de mayo de 2002, momento en que dio paso al **AES**[47] como estándar actual de cifrado.

El desgaste de los cifradores

Estos casi cincuenta años transcurridos han demostrado la validez de estos cifradores, pero también su desgaste con el tiempo y su uso, debido a cambios tecnológicos que terminan favoreciendo su criptoanálisis. Nadie en 1977 podía imaginar la aparición de Internet y su implicación en la computación distribuida[48] utilizada en ataques por fuerza bruta[49]. En 1997 Rocke Verser, junto a miles de voluntarios conectados a Internet, lograron encontrar una clave DES en **tan sólo 96 días** después de haber empezado a buscarla, y ello con la única estrategia de probar con todas las claves posibles hasta encontrar la correcta (fuerza bruta).

Aunque son muchos los cifradores simétricos que se han creado y evaluado en el último medio siglo[50], el paso del tiempo, a la vez que los consagra, los debilita. Sus diseñadores

[24] Ver https://es.wikipedia.org/wiki/Raspberry_Pi
[25] Ver https://en.wikipedia.org/wiki/BeagleBoard
[26] Ver http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf y https://web.archive.org/web/20150311220327/http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf
[27] Red de objetos físicos (o grupos de tales objetos) con sensores, capacidad de procesamiento, software específico y otras tecnologías que se conectan entre si y que intercambian datos con otros dispositivos o sistemas a través de Internet u otras redes telemáticas. Ver https://en.wikipedia.org/wiki/Internet_of_things
[28] Ver https://www.cs.cmu.edu/~coke/history_long.txt
[29] Ver https://en.wikipedia.org/wiki/Home_automation
[30] Ver https://en.wikipedia.org/wiki/Home_automation_for_the_elderly_and_disabled
[31] Ver "*Socially Intelligent Interfaces for Increased Energy Awareness in the Home*" en https://arxiv.org/pdf/2106.15297.pdf
[32] Ver https://www.cnet.com/home/smart-home/apple-homekit-everything-you-need-to-know/
[33] Ver https://alexa.amazon.com/
[34] Ver https://home.google.com/welcome/
[35] Ver https://www.apple.com/homepod/
[36] Ver https://www.samsung.com/us/support/smart-home/smartthings/hubs/smartthings-hub/
[37] Ver https://en.wikipedia.org/wiki/Home_Assistant
[38] Ver https://en.wikipedia.org/wiki/OpenHAB
[39] Ver https://domoticz.com/
[40] Ver https://en.wikipedia.org/wiki/Operational_technology
[41] Ver https://www.businessinsider.com/the-enterprise-internet-of-things-market-2014-12
[42] Ver http://www.quadibloc.com/crypto/co0401.htm
[43] Ver https://www.ibm.com/ibm/history/ibm100/us/en/icons/cryptography/
[44] Ver https://www.theatlantic.com/technology/archive/2015/03/a-brief-history-of-the-atm/388547/
[45] Ver https://en.wikipedia.org/wiki/Data_Encryption_Standard
[46] Ver https://csrc.nist.gov/CSRC/media/Publications/fips/46/archive/1977-01-15/documents/NBS.FIPS.46.pdf

nunca pudieron imaginar las capacidades tecnológicas que acabaría teniendo el atacante, por lo que no pudieron incluir contramedidas. Tengamos en cuenta que **hoy existe Internet**, y que las **GPUs**[51] son los dispositivos de cálculo más potentes que un usuario común puede comprar y que éstas se fabrican en centenares de miles de ejemplares anuales. Las **granjas o factorías de GPUs** es algo que Bitcoin ya ha puesto en pie y a prueba estos últimos años y, por si fuera poco, alguien ha levantado la **amenaza cuántica**[52]. Por todo ello convendría ir pensando en los cifradores, simétricos y asimétricos de las próximas décadas. Hay que ampliar y mejorar la oferta.

Puestos a pensar en el futuro, los hay que imaginamos un escenario muchísimo más amplio que el actual, en el que la potencia computacional quizás no sea intensiva (pocos, grandes y muy caros ordenadores generales o especializados organizados en nubes), sino más bien extensiva (muchos, pequeños y baratos dispositivos computacionales con memoria organizados en "nieblas"). Es probable que la IoT y la OT tengan sus décadas de gloria y apogeo en el futuro medio y lejano, por lo que la excusa para un escenario extensivo ya está servida.

La senda de la Criptografía Ligera

Éste debe ser enfoque de la administración norteamericana cuando decidió iniciar la senda de lo que se conoce como la **Criptografía Ligera** (*Lightweight Cryptography*)[53]. En 2018, el NIST anunció un concurso[54], al estilo de los anteriores, centrado en la búsqueda de algoritmos que pudiesen englobarse dentro de la criptografía ligera; es decir, **que fuesen seguros y adecuados para ser utilizados en entornos con capacidades muy limitadas** (redes de sensores, dispositivos sanitarios personalizados, sistemas distribuidos de control, sistemas ciberfísicos, etc.).

En esa convocatoria se especificaron lo que ellos entendían eran los requisitos técnicos que deberían satisfacer dicho tipo de algoritmos, y al concurso se presentaron 57 candidatos[55] de 25 países. De ellos, 32 pasaron a una segunda fase[56] de selección gracias a sus buenas propiedades de seguridad.

La siguiente etapa habría sido la de seleccionar ocho finalistas que sean significativamente mejores que los actuales estándares del NIST tanto en software como en hardware, sin embargo, el 7 de febrero de este año, el NIST anunció[57] la selección de la **familia de cifradores Ascon**[58] para su estandarización como algoritmos criptográficamente seguros y ligeros. Son siete los miembros de la familia Ascon, y ofrecen varias funcionalidades que son útiles para desarrollar distintas tareas muy demandadas. La más importante es el **Cifrado Autenticado** (*authenticated encryption*) **con datos de integridad asociados** (AEAD).

Otro ejemplo prometedor de algoritmo criptográfico ligero es **Xoodyak**[59], diseñado por Joan Daemen y su equipo, basado en los conceptos de **esponjas criptográficas** y **construcciones duales**[60] que están relacionados con evoluciones de la esencia empleada en el último algoritmo hash (SHA3)[61] aprobado por la administración norteamericana.

Cualquier entorno IoT/OT está marcado por estrictos restricciones en la potencia consumible, la potencia de procesado, y la seguridad física de los mismos. Algunos de los algoritmos que están dentro de la oferta del NIST son **GIFT**, **AES**, y **SPECK**, entre otros[62].

El reto esencial de la Criptografía Ligera es análogo al del mitológico enfrentamiento entre David y Goliat[63]. La esencia de ésta es desarrollar algoritmos muy sencillos y fáciles de calcular, cuya complejidad (confusión y difusión) resultante sean suficientemente altas como para ganar a cualquier otro posible o futuro sistema computacional, sin límites de potencia y recursos, que pueda dedicarse a su criptoanálisis. Está por ver si esta heroicidad es realmente posible, pero como objetivo profesional es de lo más apetecible. Del éxito de esta misión depende nuestra tranquilidad ante toda futura IoT y todos los sistemas OT industriales por venir.

El reto esencial de la Criptografía Ligera es análogo al del mitológico enfrentamiento entre David y Goliat. Está por ver si esta heroicidad es realmente posible, pero como objetivo profesional es de lo más apetecible. Del éxito de esta misión depende nuestra tranquilidad ante toda futura IoT y todos los sistemas OT industriales por venir.

La amenaza cuántica

El otro frente que tiene abierto la seguridad criptográfica actual es el de la **amenaza cuántica**. Sin entrar en si esa amenaza es realmente tal o una versión moderna del clásico *sacamantecas*[64] del siglo XIX utilizado, esencialmente, para meter miedo; lo que sí es cierto es que **la Criptografía Asimétrica**[65] **lleva más de cuarenta años tentando a su suerte**. A diferencia de los cifradores simétricos, los asimétricos optaron desde el principio, justo después de ser imaginados[66] en 1976, por recurrir a **problemas matemáticos difíciles** que permitiesen construir **funciones netamente asimétricas**; es decir, (relativamente) fáciles de calcular en un sentido, pero computacionalmente imposibles en el sentido contrario.

En febrero de 1977 Ron Rivest, Adi Shamir y Leonard Adleman, propusieron utilizar la **exponenciación modular** con un **módulo compuesto especialmente elegido** en lo que, desde entonces, conocemos como algoritmo **RSA**[67]. En este caso, la dificultad que hace asimétrica la función es la **descomposición factorial** de ese módulo especialmente construido mediante una simple multiplicación.

Además del RSA, en 1985 se propuso otro tipo del algoritmo, el de **ElGamal**[68] y el protocolo de intercambio de claves sobre canales públicos, conocido como de **Diffie-Hellman-Merkle**[69]. En ambos casos, el problema matemático subyacente es la relativa sencillez de calcular una exponenciación modular y la imposibilidad computacional de calcular **logaritmos discretos**[70] en conjuntos de puntos suficientemente grandes.

Por último, también en 1985 se propuso el uso de las **Curvas Elípticas en Criptografía**[71]. Una curva elíptica es algo conocido de tiempo atrás en matemáticas, y podríamos decir que es una curva algebraica, no singular, suave y plana, con soluciones (x, y) que satisfacen la ecuación $y^2 = x^3+ax+b$, con ciertos parámetros a y b.

La sunción básica de este tipo de criptografías es que encontrar el logaritmo discreto de un elemento cualquiera (al azar) respecto a un punto conocido es imposible (Elliptic Curve Discrete Logarithm Problem o ECDLP).

[47] Ver https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[48] Ver https://en.wikipedia.org/wiki/DESCHALL_Project y https://web.archive.org/web/20071231165331/http://www.interhack.net/pubs/des-key-crack/
[49] Ver https://en.wikipedia.org/wiki/Distributed.net
[50] Ver https://en.citizendium.org/wiki/Block_cipher
[51] Ver https://en.wikipedia.org/wiki/Graphics_processing_unit
[52] Ver https://en.wikipedia.org/wiki/Shor's_algorithm y https://en.wikipedia.org/wiki/Grover's_algorithm
[53] Ver https://csrc.nist.gov/Projects/Lightweight-Cryptography, https://www.sciencedirect.com/topics/computer-science/lightweight-cryptography
[54] Ver https://www.nist.gov/blogs/taking-measure/lightweight-crypto-heavyweight-protection
[55] Ver https://csrc.nist.gov/projects/lightweight-cryptography/round-1-candidates
[56] Ver https://csrc.nist.gov/projects/lightweight-cryptography/round-2-candidates
[57] Ver https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon
[58] Ver https://ascon.iaik.tugraz.at/ y https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/ascon-spec-final.pdf
[59] Ver https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Xoodyak-spec.pdf y https://keccak.team/xoodyak.html
[60] Ver https://keccak.team/sponge_duplex.html
[61] Ver https://en.wikipedia.org/wiki/SHA-3
[62] Ver https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9328432
[63] Ver https://es.wikipedia.org/wiki/Goliat_(personaje_bíblico)
[64] Ver https://en.wikipedia.org/wiki/Sacamantecas
[65] Ver https://en.wikipedia.org/wiki/Public-key_cryptography
[66] Ver Diffie W., Hellman, M.: "*New Directions in Cryptography*". 01 Nov 1976 - IEEE Transactions on Information Theory (IEEE) - Vol. 22, Iss: 6, pp 644-654, en https://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf

X-OD
exclusive networks.
on demand.

EXCLUSIVE NETWORKS

X

Hay una nueva versión disponible para **tu negocio**. Cámbiate a X-OD.

Actualizar

El mundo está cambiando, adáptate a él con X-OD.

Un nuevo modelo de negocio basado en suscripciones.

ThriveDX | Nuevo vendor en X-OD

FORTINET paloalto NETWORKS proofpoint. SentinelOne wasabi

La seguridad de la criptografía sobre curvas elípticas depende de la habilidad para **calcular la multiplicación de dos puntos** (de la curva) y de la imposibilidad de calcular uno de ellos conociendo el otro y el resultado del producto; vamos, que **no sabemos "dividir" números/puntos en la curva**. El tamaño de la curva elíptica, medida por la cantidad de pares de números enteros que satisfacen su ecuación, determina la dificultad computacional para resolver el problema planteado.

La criptografía post-cuántica

En esencia, la **criptografía post-cuántica** (*post-quantum cryptography* o **PQC**)[72] se refiere a algoritmos criptográficos (normalmente asimétricos) que se piensa serían seguros frente a un ataque criptoanalítico utilizando un ordenador cuántico. El problema es que los algoritmos actuales se basan en problemas matemáticos (factorización de enteros, el problema del Logaritmo discreto, y el problema del logaritmo discreto sobre curvas elípticas) que podrían ser resueltos con un ordenador cuántico suficientemente potente ejecutando algoritmos especiales como el de Shor[73] y semejantes.

Para intentar resolver esta peligrosa carencia de algoritmos criptográficos asimétricos en general, y que sean resistentes a la amenaza cuántica, la administración norteamericana, a través del NIST, ha convocado otro concurso de ideas[74] que se conoce como proyecto de Estandarización de la Criptografía Post-Cuántica (*Post-Quantum Cryptography Standardization Project*)[75]. Después de cuatro rondas de selección y después de celebrar a finales de noviembre de 2022 la cuarta Conferencia de Estandarización PQC[76], el NIST anunció cuáles son los candidatos seleccionados[77].

Para el cifrado en general, como es el caso de las conexiones TLS, el NIST ha seleccionado el algoritmo conocido como **CRYSTALS-Kyber**[78]. Entre sus ventajas están sus relativamente pequeñas claves de cifrado que los comunicantes tienen que intercambiar, así como su velocidad de operación.

Kyber es un mecanismo seguro frente a ataques adaptativos de criptograma (IND-CCA2)[79], dedicado al **encapsulado de claves** (KEM)[80], y cuya seguridad se basa en la dificultad de resolver el problema de **Aprendizaje con Errores** (*learning-with-errors* o **LWE**)[81] sobre celosías modulares (modular lattices). Su propuesta incluye tres conjuntos diferentes de parámetros para ajustar el nivel de seguridad obtenido en cada caso. En concreto, Kyber-512 pretende tener una seguridad equivalente a la del AES-128, el Kyber-768 una seguridad semejante a la del AES-192, y el Kyber-1024 una seguridad pareja a la del AES-256.

Las recomendaciones actuales son las de utilizar Kyber **en el modo denominado "híbrido"**, es decir, combinado con sistemas "pre-cuánticos" (los de siempre) como, por ejemplo, el protocolo de Diffie-Hellman sobre curvas elípticas. Kyber ya ha sido integrado en librerías y sistemas industriales como, por ejemplo, en la librería criptográfica interoperable y reutilizable de Cloudflare (CIRCL)[82], que además incluye otros candidatos poscuánticos **SIDH**[83] y **SIKE**[84] que a fecha de hoy, **ya se sabe que son inseguros**.

Amazon por su parte soporta modos híbridos de funcionamiento en los que incluye Kyber en su servicio de gestión de claves de AWS; y ya el 2019 IBM anunció el uso de ese mismo algoritmo y otro conocido como **CRYSTALS-Dilithium** en un dispositivo de almacenamiento en cinta.

Como algoritmo de firmas digitales, NIST ha seleccionado tres algoritmos: **CRYSTALS-Dilithium**[85], **FALCON**[86] y **SPHINCS+**[87]. Los dos primeros son los más eficaces y NIST recomienda utilizar Dilithium como preferido y dejar FALCON para aplicaciones en las que sea necesario firmas más pequeñas que las generadas con Dilithium. Por su parte, SPHINCS+, genera firmas más grandes y es algo más lento que los otros dos, pero tiene interés como mecanismo de salvaguardia (backup) ya que está basado en una aproximación matemática distinta a la de los otros tres algoritmos recomendados (evitando así poner todos los huevos en la misma cesta).

La escasez de algoritmos criptográficos asimétricos, la opción de utilizar planteamientos matemáticos para elegirlos y la "amenaza cuántica", han ocupado en estos últimos años a los criptógrafos de todo el mundo. En el fondo se han "re-visitado" problemas que ya se sabía que eran difíciles y poco "eficientes" (por su velocidad y tamaño de las firmas), luego no hay grandes novedades. Sin embargo, es bueno que se mueva algo en la criptografía real, en la que se utiliza en los sistemas del día a día, ya que los últimos veinte años se ha estado viviendo de algoritmos diseñados en las últimas décadas del siglo pasado.

La corrección de los algoritmos criptográficos utilizados es una condición "necesaria pero no suficiente" para que podamos tener un sistema, un procedimiento, seguro. También debemos tener implementaciones y usos realmente seguros de dichos algoritmos. Si el criptoanalista no logra hincarle el diente al algoritmo, siempre podrá atacar a sus implementaciones concretas.

Sin embrago, es necesario plantearse lo que dijo Edgar Allan Poe, a través de uno de los protagonistas de su narración "*El escarabajo de oro*" (The Gold-bug, 1843)[88]; "***es, en realidad, dudoso que el genio humano pueda crear un enigma de ese género que el mismo ingenio humano no resuelva con una aplicación adecuada***".

Hay que tener en cuenta que **la corrección de los algoritmos criptográficos** utilizados es una condición "**necesaria pero no suficiente**" para que podamos tener un sistema, un procedimiento, seguro. También **debemos tener implementaciones y usos realmente seguros de dichos algoritmos**. Si el criptoanalista no logra, hincarle el diente al algoritmo, siempre podrá atacar (con bastante éxito en muchos casos) a sus implementaciones concretas. Huyamos de los becerros de oro, aunque sea mucho su brillo y mucha su popularidad en los grandes medios. La criptografía es una actividad difícil, poco grata, pero absolutamente necesaria; por lo que **sólo se puede hacer si se hace bien**. ■

[67] Ver https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[68] Ver https://en.wikipedia.org/wiki/ElGamal_encryption
[69] Ver https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
[70] Ver https://en.wikipedia.org/wiki/Discrete_logarithm
[71] Ver https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
[72] Ver https://en.wikipedia.org/wiki/Post-quantum_cryptography
[73] Ver https://en.wikipedia.org/wiki/Shor's_algorithm
[74] Ver https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[75] Ver https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization
[76] Ver https://csrc.nist.gov/events/2022/fourth-pqc-standardization-conference
[77] Ver https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022
[78] Ver https://pq-crystals.org/kyber/
[79] Ver https://en.wikipedia.org/wiki/Ciphertext_indistinguishability
[80] Ver https://en.wikipedia.org/wiki/Key_encapsulation_mechanism
[81] LWE es un modo de esconder un valor secreto añadiéndole ruido y haciendo que éste sea muy significativo. Ver https://en.wikipedia.org/wiki/Learning_with_errors y https://dl.acm.org/doi/pdf/10.1145/2535925
[82] Ver https://blog.cloudflare.com/introducing-circl/
[83] SIDH = *Super singular Isogeny-based Diffie-Hellman protocol*. (¡algoritmo inseguro!) Ver https://en.wikipedia.org/wiki/Supersingular_isogeny_key_exchange
[84] SIKE = *Super singular Isogeny-based Key Encapsulation protocol*. (¡algoritmo inseguro!) Ver https://sike.org/
[85] Ver https://pq-crystals.org/dilithium/
[86] Ver https://falcon-sign.info/
[87] Ver https://sphincs.org/
[88] Ver https://en.wikipedia.org/wiki/The_Gold-Bug

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

Espacio TiSEC congregó en SOCorro a grandes referentes del mercado en la externalización de la operación de ciberseguridad

Los límites de la compartición de información, la automatización y la necesidad de métricas de madurez marcan el futuro de los MSSP y SOCs

Con casi 600 asistentes y dos jornadas en formato presencial y virtual, de mañana y tarde, Espacio TiSEC 'SOCorro: centros de operaciones de ciberseguridad' congregó, los pasados 15 y 16 de marzo, a importantes referentes en este ámbito que presentaron sus ideas, planes y propuestas sobre el estado y los grandes retos de los SOCs, la Red Nacional de SOC (RNS), las tecnologías que permiten su optimización, el déficit de analistas y capacidades, así como la respuesta que están dando los proveedores de servicios de ciberseguridad (MSSP) y cuáles son los límites de la compartición de información entre el sector privado y el público para mejorar la ciberprotección nacional, entre otros aspectos.

Con alrededor de 40 ponentes, seis mesas redondas y casi 600 asistentes, en formato presencial y virtual, Espacio TiSEC, de Revista SIC, se ha convertido en el pionero en acometer en un congreso los grandes retos de los, cada vez más numerosos, Centros de Operaciones de Ciberseguridad (SOC). Durante dos jornadas, el 15 y el 16 de marzo, en Madrid, en horario de mañana y tarde, bajo el título 'SOCorrro, Centros de Operaciones de Ciberseguridad: Automatización, compartición y otros desafíos', los ponentes mostraron sus preocupaciones, soluciones, tecnologías, así como las inquietudes de su trabajo en el día a día, en muchas ocasiones preguntados por los asistentes, de alto nivel profesional, entre los que se encontraban, por ejemplo, ejecutivos del ámbito público directamente concernidos, desde la Subdirectora General de Ciberseguridad, Protección de Datos y Privacidad en **Madrid Digital**, **Esther Muñoz** o el jefe de área Responsable de Seguridad del **Gobierno de La Rioja, Tomás Gómez**.

Abrió las jornadas el Director en BSS de **PwC, Jesús Urién,** con una conferencia sobre el futuro de los SOCs en la que mostró de forma ilustrativa los datos en torno a estas infraestructuras. "El 49% de las empresas ya despliegan un centro interno y un 34% cuentan con apoyo de servicios externos para reforzar sus capacidades. De hecho, sólo un 17% no considera obligatorio tener uno propio". Urién también destacó que actualmente se está apostando por un SOC único central, pero la tendencia "nos llevará a otros modelos en los que haya más colaboración con unas configuraciones mixtas". Así, avanzó que la tendencia pasa por servicios cada vez más apoyados en la nube, con una arquitectura clara y formalizada desde el inicio, para ir ganando en capacidades. Para ello, "habrá que incorporar una alta automatización, en todo lo que sea posible".

Finalizó destacando que, de momento, se está haciendo foco en la detección e integración de las diversas fuentes de datos. De cualquier forma, también lamentó que en este tipo de infraestructuras, "en muchas ocasiones, la tecnología genera expectativas superiores a lo que realmente puede hacer".

CATEGORIZACIÓN DE LOS SOC

A continuación, el CEO de **Aiuken** (hoy parte de la recién creada paneuropea **Allurity**), **Juan Miguel Velasco**, destacó "los efectos de las tecnologías nativas de la nube en la ciberseguridad, los servicios gestionados y los SOCs". Así, entre sus reflexiones resaltó que, "en contra de lo que muchos piensan, los SOCs no son un conjunto de tecnologías: son plataformas", poniendo en valor que sus centros trabajan de forma eficaz y coordinada bajo, precisamente, esa premisa. "Porque están en la *cloud* y de ahí la parte de la automatización y la orquestación", puntualizó. Especialmente llamativa fue su clasificación de los SOCs en cuatro categorías, según sus capacidades, recordando que sólo se es maduro si se consigue estar entre las dos de mayor nivel, "aunque, ahora, desgraciadamente, el 70% no pasa de la primera". También, habló de la oferta en este ámbito de los grandes referentes en la nube, como Amazon, Google y Microsoft, finalizando con la propuesta que hacen desde Aiuken con un modelo de 'SOC Cloud' y recordando la gran utilidad que ya tienen tecnologías como el *machine learning* y la IA, "aunque aún estamos muy al principio". Indicó también que, "para apostar por la ciberseguridad en la nube, hay que gozar de un nivel avanzado de madurez en los SOCs". No faltaron opiniones, no siempre compartidas por los asistentes, como su augurio de que, en dos o tres años, "todo el mundo tendrá que tener nivel de SOC 3 y 4" para disponer de una ciberprotección eficaz. "La actual evolución exige darle una vuelta a lo que se tiene para no quedarse atrás", concluyó.

SERVICIOS GESTIONADOS EN EL ÁMBITO SECTORIAL

Acto seguido, comenzó el 'Módulo 1', dedicado a servicios gestionados y la sectorización que se vive y que abrió con una interesante disertación **José María Legido**, director de Internacional de **GMV Secure eSolutions,** sobre los servicios en Espacio y Defensa. Así, destacó que "la ciberseguridad en este sector es casi inexistente, aunque todo el mundo considera que sí la tiene. Y aquí no hay botón de *reset,* una vez lanzado el satélite no hay vuelta atrás". Por eso, "en el entorno espacial, el concepto de alta disponibilidad adquiere su dimensión más amplia". En este sentido, indicó que en el sector se apuesta por un enfoque de "ciberseguridad por aislamiento", aunque se están dando pasos importantes en nuevas áreas de negocio como la denominada 'Newspace', integrada por las empresas centradas en nuevos satélites de pequeño tamaño.


Jesús Urién


Juan Miguel Velasco


José María Legido


Óscar Navarro


Javier Pérez

Después, **Óscar Navarro,** director de Área Industrial de **S2 Grupo**, comentó que, en estos entornos de fabricación, "cuando se pierde la visión global es cuando aparecen los problemas". "Llevamos muchos años trabajando en el sector industrial y los errores más comunes de los SOCs en este ámbito van desde la definición de los objetivos y la planificación inadecuada, hasta la aproximación basada únicamente en la tecnología, desconocer la infraestructura, tener un foco excesivo en la gestión de activos, contar con una visión de silo y, sobre todo, el riesgo de no obtener todo el retorno de la inversión, abandonando los sistemas desplegados". Por ello, puso en valor la necesidad de contar con los objetivos estratégicos de forma clara.

¿Por dónde empezar? Navarro recomendó hacerlo por las seis 'W' que se usan en periodismo –Qué, Quién, Cómo, Cuándo, Dónde y Por qué–, aplicada a este ámbito. En definitiva, resaltó la necesidad de contar con una estrategia de servicio poniendo en el centro el proceso y que la operativa funcione en todo momento.

Finalizó este bloque **Javier Pérez,** responsable de Ciberseguridad de **Fujitsu,** para hablar de cómo se implementan los SOCs en Salud. "Somos una empresa muy

especializada en este ámbito y nos da un conocimiento muy relevante". La multinacional, que este año celebra 50 años en España –el primer país donde abrió filial en su expansión internacional–, es un referente en el sector salud de España, "que es el tercero más atacado del mundo, con una ciberdelincuencia muy especializada". Frente a ello, recordó que los pilares de la ciberseguridad en este sector son la gestión de la identidad, la respuesta a incidentes, la protección de redes y la gestión de vulnerabilidades. Además, destacó la aproximación a este aspecto por parte de la compañía, "no como un catálogo de servicios sino como centro de excelencia en tanto generador de un ecosistema de cocreación, con empresas y hospitales, que generen valor". También mostró diferentes servicios de detección y protección IoMT que ofrece la multinacional que permiten ver, conocer, actuar y anticipar, y mejorar a través de implementar procesos y tecnologías que hacen posible contar con un inventario de activos y evitar vulnerabilidades, entre otros aspectos.

TECNOLOGÍAS DE FABRICANTE ORIENTADAS A MSSP - 1

El segundo módulo del día estuvo dedicado a conocer de primera mano cómo el auge de los servicios gestionados está cambiando el modelo de negocio de los fabricantes, evolucionando sus portafolios para poder ofrecer servicios y soluciones de seguridad que ayuden a los SOC y a los equipos de operaciones a cumplir con sus objetivos. Para ello, la capacidad de automatizar, el 'hacer más con menos' y poder descargar a los equipos de las alertas para centrarse más en los incidentes, fueron algunas de las claves más valoradas durante las exposiciones de este bloque, que comenzó **Ángel Ortiz,** director de Ciberseguridad para España de **Cisco**. El directivo empezó la jornada vespertina destacando la apuesta de la compañía en este campo con la creación de la marca Cisco+, "que permite consumir todas sus soluciones en modo suscripción y en modo servicio". Dentro de esta propuesta, resaltó la más reciente, Cisco+ Secure Connect, "el primer servicio gestionado de extremo a extremo SASE del mercado". También, recordó, entre otras, sus Cisco Managed Security Services. En definitiva, la compañía espera que, para 2025, el 45% de los productos que vendamos sean bajo la forma de algún tipo de gestión y que el 50% de los ingresos vengan puramente por los modelos de suscripción", concluía Ortiz.


Ángel Ortiz


Álvaro García


Raül Albuixech


David García Cano

Eficacia, eficiencia e inteligencia

Acto seguido, tomó el testigo **Álvaro García,** ingeniero de sistemas de **CrowdStrike**, quién comenzó su intervención con una famosa frase de Albert Einstein: "si quieres obtener cosas diferentes, haz cosas diferentes". El experto analizó el día a día en un SOC que, generalmente, "están marcados por trabajos cuyos objetivos no son realistas", necesitándose "súper humanos", para llevarlos a cabo. Para dar respuesta a esta problemática destacó cinco áreas de trabajo de la compañía: eficacia y eficiencia, atribución, visibilidad, respuesta y *reporting*. En cada una de ellas, CrowdStrike ofrece una serie de soluciones, como Falcon Fusion, incluida en su plataforma Falcon, para ayudar a los SOC a "poner todos los recursos en el centro del incidente".

Tras esta exposición, fue el turno de **Raül Albuixech**, director de Soporte Técnico y Servicios de **Eset,** quien profundizó en las claves de esta compañía para ayudar a los MSSP y que resumió en dos términos: proteger (los puntos finales, los servidores y la nube), y proveer de inteligencia "para que tanto clientes, como el personal del SOC nutran otras soluciones de seguridad y para evitar que se vean afectados por algún tipo de amenaza futura". En este último sentido, entre otras, resaltó el servicio Eset Threat Intelligence para ofrecer dicha inteligencia en forma de *feeds* (*botnets*, dominios, archivos maliciosos, URLs e IPs). En general, destacó que el portafolio de la compañía se compone de productos basados en tres pilares: robustez, alto grado de detección y facilidad de uso. Eso sí, "nuestra visión –indicó– es que sean multicapa y que puedan trabajar entre ellas de forma coral para ofrecer la máxima ciberprotección posible", puntualizó.

Tiempo y recursos

Bajo un título muy revelador, 'Tiempo y recurSOC, esos bienes tan preciados', **David García Cano,** gerente especialista en Ventas de **Fortinet,** terminaba este turno de exposiciones centrándose en la importancia de dichos elementos para que sean "lo más eficientes y eficaces posibles". Coincidiendo con los anteriores intervinientes, señaló que "las limitaciones de los SOC y la tensión de los equipos se debe a las alertas y sobrecargas de los procesos manuales, la complejidad de los productos puntuales y la carencia de *skills"*, lo que hace que "no se pueda mantener el ritmo de la evolución de los ciberataques y se reaccione tarde y mal". En este sentido, recordó que desde Fortinet ofrecen diferentes soluciones, destacando su SOC as a Service, "basado en la nube, para hacer un Centro de Operaciones más eficiente a través del canal e, incluso, con los propios clientes".

INNOVACIÓN Y VISIBILIDAD

La apertura de la segunda jornada (16 de marzo) de Espacio TiSEC correspondió a **Montserrat Valdés,** experta destacada en la Jefatura de Sistemas de Ciberdefensa del **Mando Conjunto del Ciberespacio** (MCCE), de Defensa, que habló del "SCOMCE, el Sistema de Combate en el Ciberespacio, una oportunidad para el I+D+i y la industria española de ciberseguridad". "El ciberespacio requiere de unas acciones concretas y sistemas de armas específicos", destacó adelantando que el SCOMCE permitirá el planteamiento, dirección, control, coordinación y ejecución, además de recordar que será conjunto, escalable y acreditable, además de distribuido en niveles pudiendo ser interoperable para poderlo usar tanto en España, como en operaciones con aliados.


Montserrat Valdés

MESA DE DEBATE 1

En los SOC, la compartición de información pasa por más estandarización, más cultura y mayores incentivos públicos

La primera mesa de debate de este Espacio TiSEC, moderada por **Luis Fernández,** Editor de SIC, contó con **Alejandro Aliaga,** Co-Director General de **BeDisruptive**, **Roberto Pérez,** Head of Cyberscurity Services & Solutions Business de **SIA** y **Xavi Pes,** Security Services Manager de **Wise Security Global.**

En ella, Pérez comenzó explicando que "hay que compartir información y que no necesariamente se tiene que recompensar", aunque también destacó que "sí puede haber otra forma como formar parte de una red o suponer un sello de calidad respecto a terceros", añadió, por su parte, Pes. De hecho, todos los participantes destacaron que la colaboración con la Administración debería tenerse en cuenta en las licitaciones públicas, ya que "tiene que haber algún tipo de incentivo, para que no decaiga la compartición y se estimule a colaborar".

Alejandro Aliaga, Roberto Pérez y Xavi Pes

En este sentido, Aliaga apostó por "compartir información, porque juntos somos más fuertes". De cualquier forma, los participantes estuvieron de acuerdo en la necesidad de buscar un modelo más atractivo, ya que "la experiencia que hubo en Csirt.es no tuvo éxito: todo el mundo decía que había que compartir, pero no se hacía".

Eso sí, durante el debate también se destacó la dificultad de hacerlo por los acuerdos de confidencialidad con los clientes –"y las malas experiencias que se han tenido" –, poniendo en valor la necesidad de crear más cultura en este ámbito en el que, según se dijo, hay sectores especialmente cautelosos, como el bancario. "Hay que empezar a evangelizar para intentar normalizar eso. Es un camino largo y no por eso hay que dejar de intentarlo", comentaron.

En cuanto a la búsqueda de profesionales, coincidieron en hacer un mix entre formar a personal propio y captar externos para suplir el déficit del mercado, así como utilizar de forma intensiva la tecnología. "Vivimos en un periodo de cambio, la tecnología va muy rápido… he visto ya iniciativas de SOC GPT, hay que encontrar muchas fórmulas, capacitar profesionales, generar formación de profesionales y es clave gestionar este cambio de la mejor forma posible", dijo Aliaga. "Hay que vivir aprendiendo a gestionar todo en todo momento". Y tener claro que "la tecnología tiene que soportar como queremos trabajar", comentó Perez García, aunque lo importante son los "procesos que montamos para gestionar la ciberseguridad y el reto está en automatizar y orquestar para lograr una gestión lo más eficiente posible". El problema es que, "cuando hay varios fabricantes, tienen que tener algo por encima para que se usen bien todas. O se busca la interoperabilidad entre diferentes *vendors* o se está abocado al fracaso". En este sentido, "es fundamental apostar por el buen gobierno", dijo Pes. "Nosotros somos *partners* de Microsoft, pero nuestro SIEM es Sentinel. Hay que buscar la optimización".

Como colofón, cada participante dio su opinión para mejorar en la compartición de información, un aspecto en el que Aliaga consideró vital "apostar por la estandarización para que todo funcione", para Pérez García, "concienciar más" y Pes resaltó la necesidad de "una mejora continua. Los tiempos cambian y es una necesidad".

Finalizó destacando que este proyecto busca "aunar tecnología puntera adaptada a nuestras necesidades, invitando a la industria y las universidades españolas tractoras para la autonomía estratégica".

RNS: RETOS Y OPORTUNIDADES

A continuación, el jefe del Departamento de Ciberseguridad del **CCN**, **Javier Candau**, y el Responsable de SOCs del CCN-CERT, **Ignacio Briones**, hablaron de la 'Red Nacional de SOC (RNS): la vertebración de la ciberseguridad de las Administraciones Públicas con el apoyo de los MSSP'. "No compartir es una mala aproximación", comentó Candau, poniendo en valor la importancia de compartir información de un incidente para evitar que impacte en otras organizaciones. "Contar con una respuesta integrada es lo que llamamos Red Nacional de SOC". "Si España consigue tener una plataforma sólida donde haya un intercambio continuo, la transposición que viene de la NIS2 será fácil", dijo.


Javier Candau

Ignacio Briones

Briones, durante su exposición, destacó por su parte la necesidad de facilitar información de un incidente durante su primera fase para poderlo parar en otras infraestructuras. "Entiendo" que "compartir gratis no es viable", sí puede resultar de gran utilidad "una IP o TTP genérico que se pueden compartir de forma anonimizada o los IOAs", que permiten ver si varias entidades perciben ese comportamiento anómalo. "La RNS va de personas y de compartir en los minutos iniciales de los posibles ataques para que los ciberciminales no consigan su objetivo", añadió recordando que la RNS, que ya cuenta con más de 130 participantes, también contempla que "quien no comparta será expulsado". Finalizó su intervención presentando el proyecto europeo en el que España tiene mucho peso y participan Austria, Rumanía, Portugal, Países Bajos, Luxemburgo e Italia. Y que permitirá que los diferentes SOCs de los países compartan información para sumar fuerzas.

MESA DE DEBATE 2

Los responsables de la operación de ciberseguridad buscan mayor automatización en el SOC y demandan servicios más personalizados

Cerró la mañana una mesa de debate, moderada por el director de la Revista SIC, **José de la Peña**, sobre 'Cliente final: Transformación de los servicios gestionados y SOC', en la que participaron el CISO de **Sabis, Adolfo Hernández,** director de Operaciones de Ciberseguridad de **Banco Sabadell**; **José Palacio,** responsable global de Operaciones de Seguridad y Detección de Amenazas de **Banco Santander**; **Daniel Largacha,** director del Centro de Control Global-CERT de **Mapfre**; y **Damián Ruiz**, CISO de **Singular Bank.**

Adolfo Hernández, Daniel Largacha, José Palacio y Damián Ruiz

En este sentido, Hernández comenzó destacando que, para anticiparse a las futuras amenazas, "es importante hacer un ejercicio introspectivo de lo que vas a necesitar en tres o cuatro años y de las tecnologías que vas a precisar". "Vivimos en continua transformación mirando cuál es el escenario de riesgo, qué tecnologías tenemos, cuáles hay, como 'ChatGPT', y cuáles son nuestros clientes", comentó Palacio. "El SOC se tiene que basar en estos pilares y hay que tenerlos claro".

"Ahora vemos un déficit en el SOC porque muchos usuarios no están contentos con él, hay cierto déficit de proveedores que ha motivado que se vaya a proveedores 'boutique', a medida, para tener ese dinamismo que se va a necesitar en ciertos sectores", añadió Ruiz. "La gran batalla está en la detección y respuesta", ya que "está muy verde. Y en esto los servicios gestionados tienen que espabilar".

"Aquí no hay fórmulas mágicas", dijo Largacha, "ya que el momento operativo de cada uno es diferente al del resto. Por eso, hemos apostado por un proceso de centralización de la seguridad, gestionada desde España, ya que nuestro *core* está aquí. Cada parte de la compañía tiene una estructura e ingresos, pero todas están conectadas a la red y por eso decidimos que los procesos de protección, detección y respuesta sean globales". En este sentido, también resaltó que "al automatizar se gana en eficiencia y, además, consigues enfocar los recursos humanos donde realmente sea necesario".

"No creemos en gestionar alertas individuales. Apostamos por la automatización en la respuesta, además de en la detección, muchas ya se pueden hacer, sobre todo, las relacionadas con la carga de trabajo. También, estamos usando mucho IA y aprendizaje automático en detección, para localizar qué es normal y lo que no", dijo Palacio, que recordó que el Banco Santander ha apostado por el SOC centralizado.

Los participantes destacaron nichos de mercado que aún no tienen una amplia oferta pero sí sería de su interés. "Actualmente, buscamos más servicios que tecnologías… y muy personalizados", añadió el CISO de Singular Bank. "Además, son interesantes, por ejemplo, la propuesta para *testing* automatizados, ya que con DORA y TIBER-EU no va a haber *red teaming* para cubrir todo lo necesario". Largacha también destacó la necesidad de "contar con una herramienta que permita simplificar el trabajo en las nubes, ya que cada una tiene sus propias soluciones", y tanto Hernández como Palacios demandaron más propuestas para contar con "automatismos en las pruebas", así como para la "simplificación de la gestión".

VISIÓN DEL SOC Y LOS SERVICIOS EN EL ÁMBITO AUTONÓMICO

También se trató en este Espacio TiSEC la 'Centralización de la gestión de la ciberseguridad a escala autonómica y el papel de los MSSP', un asunto en el que algunos de sus protagonistas, como el director de la **Agencia de Ciberseguridad de Cataluña, Tomás Roy**; el jefe de Subárea de Seguridad de la **Agencia para la Modernización Tecnológica de Galicia, Gustavo Herva**; el responsable del **CERT del Centro Vasco de Ciberseguridad, Asier Martínez**; y la subdirectora general de Ciberseguridad de la **Generalitat Valenciana, Carmen Serrano**, dieron su visión, alcance y retos en intervenciones con profundidad y muy ilustrativas.

Roy comenzó poniendo en valor la RNS, ya que considera que "tiene una lógica aplastante y la adhesión al proyecto es total. Es ambicioso y dará muchos frutos". Además, destacó el trabajo de las agencias de ciberseguridad, como la que dirige,


Tomás Roy


Gustavo Herva

"porque tienen como objetivo garantizar la protección cibernética de la administración pública", y generar "innovación y talento". También, resaltó que el buen trabajo de la institución se basa en varios ejes: capacitación propia pero integrando capacidades externas, alineados con el CCN, la escalabilidad de los proveedores y propia, así como dando valor a la sectorialidad, la colaboración y la innovación.

Asimismo, recordó que el organismo ha reforzado sus responsabilidades, ya que Cataluña le ha encomendado recientemente la ciberprotección de los entornos sanitarios públicos, así como el de educación y el de administración local. Frente a estos retos, Roy consideró clave la colaboración entre organismos y reclamó al CCN que apueste por la especialización de los SOCs de las agencias autonómicas para optimizar capacidades y recursos.

A continuación, Herva mostró la labor realizada en los últimos años por la Agencia para la Modernización de Galicia, que cuenta con un área de ciberseguridad en

MESA DE DEBATE 3

La eficiencia, el capital humano y el foco en la detección y respuesta, claves del éxito de los SOC

Como colofón al primer día, el encuentro reunió en una mesa de debate, moderada por **José Manuel Vera**, redactor de SIC, a los cuatro ponentes de la tarde para reflexionar sobre lo expuesto hasta el momento y responder a las inquietudes de la audiencia. Una de las primeras cuestiones recayó en las principales capacidades y servicios que los clientes demandan de un SOC. **David García Cano** (**Fortinet**) no dudó en responder "la capacidad de orquestación y respuesta automatizadas y extendidas". **Álvaro García (CrowdStrike)** añadió que, sobre todo, "se busca una solución de SOC externalizado *end-to-end,* que poco a poco se ha ido optimizando en costes", eso sí, "lo que está claro es que el cliente no busca modelos intermedios", puntualizaba. De acuerdo con lo dicho, **Raül Albuixech (Eset)**, destacó que, "también, se demanda cada vez más un valor añadido en las herramientas a través de la automatización de tareas y poder hacer más con menos". **Ángel Ortiz (Cisco),** coincidía con la automatización como un concepto clave dentro de un SOC. Además, "es importante centrarse en el incidente y no tanto en la alerta", puntualizó afirmando a su vez que "lo que marca la diferencia es ser eficaces en la detección". La audiencia también se interesó por conocer qué están haciendo estas empresas para competir con grandes tecnológicas como Google, Amazon o Microsoft. En este caso, Ortiz recordó uno de los anuncios estrella de la compañía, "la construcción de la Cisco Security Cloud, una plataforma que integrará las capacidades de comunicación y de red con la seguridad, ofreciéndose de forma unificada y que sirva de interconexión para estos tres grandes 'hyperscalers', así como las nubes privadas, híbridas, con las que pueda contar el cliente". Albuixech, por su parte, opinaba que "quien mucho abarca poco aprieta, por ello, tenemos que especializarnos y hagamos lo que hagamos, hacerlo mejor que la competencia, para que eso sea nuestro valor". García apuntó que, para las empresas más pequeñas, "la diferencia se encuentra en el capital humano". Coincidiendo con esta opción, García de Cano añadió que, además, "el valor diferencial está en escuchar a los clientes y ser un *partner* de seguridad para ellos". Otra de las preguntas que más interés generó fue la que daba título a esta mesa de debate: ¿Terminarán los fabricantes prestando servicios gestionados directamente al cliente final? García respondió de forma clara y concisa, "nosotros ya lo hacemos. Eso sí, es una opción, ya que no creemos en la canibalización". "En el caso de Fortinet", indicaba García Cano, "tenemos una oferta completa con la capacidad de dar al cliente todo tipo de servicios gestionados, siempre con la vocación de buscar el sabor adicional que pueda demandar el mercado".

David García Cano, Álvaro García, Raül Albuixech y Ángel Ortiz

Albuixech afirmaba que, por su parte, "estamos preparados para cubrir aquello que el canal no pueda o que el cliente nos demande directamente a nosotros". Ortiz consideraba que los fabricantes ofrecerán "determinados servicios de SOC, pero no todos, por su propia naturaleza y porque también es difícil que un cliente tenga todo de un mismo fabricante".

infraestructuras, "que supone ir poco a poco logrando hitos". Así, repasó algunos como la formación del Csirt.gal, en 2018, y el trabajo realizado "para sacar adelante la Estrategia de Ciberseguridad de Galicia que sirva hasta 2030". También, dio a conocer diferentes iniciativas donde se está haciendo foco, en especial en la concienciación, además de dinamizar el cumplimiento de la normativa de protección de datos en la Xunta, "que también es de nuestra responsabilidad, junto a la ciberseguridad". Para lograrlo, puso en valor que cada vez se intenta automatizar más, integrando más fuentes de inteligencia para preservar la seguridad y la información y el respeto a la privacidad, entre otros aspectos clave, como realizar muchas auditorías. No dejó de lado el valor que les aporta certificarse en el ENS y el uso de las herramientas del CCN como Inés, Lucía, Micro Claudia y Reyes, entre otros aspectos.

Por su parte, Asier Martínez, responsable del CERT del Centro Vasco de Ciberseguridad, (el Centro no tiene entidad jurídica propia, sino que es un área del departamento de innovación, SPRI), aunque explicó que se va a evolucionar hacia una Agencia Vasca de Ciberseguridad, que absorberá lo hecho hasta ahora y que se constituirá en breve como ente público de derecho privado, pero ya dependiente del Departamento de Seguridad.


Asier Martínez


Carmen Serrano

Resaltó el buen trabajo hecho hasta ahora, plasmado en el Libro Blanco de la ciberprotección en Euskadi y de los diferentes proyectos y ayudas ofrecidas, sobre todo, en el sector industrial, para mejorar la monitorización y contar con alertas tempranas eficaces. Además, comentó que se están definiendo "la estrategia vasca de ciberseguridad, estableciendo un modelo de relación entre entidades incorporando a más y evaluando de forma continua el estado de la ciberprotección".

Finalizó este bloque con la intervención de la subdirectora general de Ciberseguridad de la Generalitat Valenciana, Carmen Serrano, que resaltó su modelo centralizado de la ciberprotección. "Se trata de una entidad fruto de muchas decisiones estratégicas en la región, como la creación de una red corporativa con salida unificada, la creación de servicios corporativos, de forma horizontal y transversal, la creación en 2007 del CSIRT

MESA DE DEBATE 4

En busca de un mercado más consolidado, precios más ajustados en los concursos públicos y la tecnología para suplir la fuga de profesionales

Durante la segunda jornada, abrió el apartado de debate la mesa dedicada a los 'Requisitos que debería cumplir un SOC para ser considerado como tal para entidades esenciales, importantes y críticas' que, por su temática, también fue una de los más seguidos, con las opiniones del COO de **aDvens Iberia**, **David Marqués**, el director técnico de **A3Sec, Nacho García Egea,** y el responsable de Cipher xMDR en **Cipher** a Prosegur Company, **Carlos Fernández**.

A preguntas del moderador, el director de Revista SIC, José de la Peña, Marqués consideró muy importante mirar fuera para mejorar, teniendo claras con qué capacidades contamos. Fernández dijo que lo importante para ofrecer un SOC con garantías es apostar por solucionar varios aspectos como "la visibilidad o la fragmentación de la tecnología. La gente piensa que está haciendolo mejor, pero está peor que ayer, tanto en la tecnología, como frente al adversario y al incremento de amenazas, que nos obliga a estar en mejora continua". Por su parte, García Egea, planteó que actualmente en el mercado hay un problema de volumen. ¿Cuántos proveedores de SOC hay, por ejemplo, en Francia? Allí hay cinco y aquí 50". Un dato que no todos compartieron por cuanto Fernández recordó que "en EE.UU. hay más de 4.000 MSSP y, también, muchos clientes que cambian de un año a otro porque la calidad anunciada no coincide con la percibida".

Eso sí, todos destacaron que es vital ofrecer un nivel de respuesta adecuado, contar con certificaciones para el sector público y asegurar el servicio completo, además de apostar por la calidad. También, resaltaron la necesidad de profundidad en la catalogación de los tipos de SOC al igual que destacaron la necesidad de que las empresas tengan claras las fortalezas de los proveedores que contratan. "Al final, lo que busca el cliente es, en muchos casos, único para cada uno", añadió García Egea, quien recordó que cada vez se apuesta más por la automatización de muchos servicios, pero, también, la experiencia del equipo humano que está tras un servicio.

Carlos Fernández, David Marqués, Nacho García Egea

En la última parte del debate, surgió la polémica por el precio con el que al final se adjudican muchos concursos públicos, muy por debajo del mercado, un fenómeno en el que se encuentra inmerso la demanda y la oferta. De hecho, ello motiva, según explicó Marqués a que, por ejemplo, su compañía no se presente en España a este tipo de concursos en ocasiones. Todos coincidieron, por su parte, en que la brecha salarial y la retención del talento obliga a hacer un uso intensivo de la tecnología para suplir capacidades.

CV, el primero en el ámbito autonómico, y la centralización de las TIC en momentos de crisis", dijo. "Todo con mucha vocación de servicio público y buscando la máxima colaboración".

Además, destacó la estrategia 'TIC GVA GENDigital 2025' con diferentes líneas de trabajo para el diseño conceptual del Centro de excelencia de ciberseguridad industrial, un Observatorio, un Laboratorio de Ciberseguridad y la red de sensores ICS Honeynet, además de estar en el proyecto RETECH, con fondos europeos, para impulsar estas iniciativas.


Antonio Ramos

Durante el coloquio, fue llamativa la diferencia dada a conocer entre los presupuestos de los entes autonómicos, con la Agencia de Cataluña encabezándolos con un montante que ronda los 22 millones de euros, frente a los 2,5 de Valencia, los 2,5 de Galicia o los 2,5 del País Vasco, que previsiblemente se incrementarán a 15 millones con la puesta en marcha de su Agencia.

CLASES DE SOCs

También despertó gran expectación la ponencia del CEO de **Leet Security, Antonio Ramos,** sobre los 'Criterios para clasificar y calificar SOC'. Así, destacó que es necesario que estos centros tengan unos "requisitos mínimos, según a quién vayan orientados: no es lo mismo proteger una pyme que una gran compañía del sector energía". De cualquier forma, sí enfatizó la necesidad de tener claro qué se ofrece cuando se apuesta por un servicio de SOC, ya que, según su experiencia, "hay muchas calificaciones y variopintas" bajo esta denominación. Así, recordó que su compañía otorga diferentes puntuaciones en función de las capacidades reconocidas de cada Centro identificadas con letras –las mejores con A y las peores con D–.

De hecho, recordó que actualmente hay varios proveedores que se han sometido y tienen la 'calificación de Leet Security' pero que las diferencias en muchos aspectos son más que notables, incluso "preocupantemente insuficientes", repasando los 14 aspectos mejor y peor valorados de los proveedores de centros de operaciones que actualmente han sido valorados por la compañía, aunque de forma anonimizada.

De hecho, comentó que, tarde o temprano, se va a un mundo en el que se exija estar certificado porque, a día de hoy, "esto es el salvaje oeste". Como ejemplo, recordó la iniciativa 'Cybersecurity Service Provider Licence', de Singapur, que exigirá obtener este tipo de licencia para ser proveedor de SOC en el país u ofrecer servicios de intrusión.

TECNOLOGÍAS DE FABRICANTES ORIENTADAS A MSSP - 2

Una plataforma, una consola y un único cliente

Samuel Bonete, responsable regional de Ventas para España y Portugal de **Netskope**, fue el encargado de comenzar la sesión vespertina de esta segunda jornada ahondando en la importancia de los MSSP para ayudar a este reconocido actor en el mercado SASE (en SSE y en SD-WAN) a cubrir otras áreas como EDR, IDP, SIEM/SOAR,

MESA DE DEBATE 5

Los clientes de los MSSP demandan mejores métricas, apostando por centros multiglobales y alertan: "hay mucho margen de mejora"

Terminó la segunda jornada matinal con un ilustrador y animado debate sobre 'La tendencia hacia la verticalización de la ciberseguridad: Impacto en la selección de MSSP'. En él intervinieron una tríada de profesionales del máximo prestigio y trayectoria: los CISO de **Cepsa** (**Rafael Hernández**), **Iberia** (**Jesús Mérida**) y **Renfe** (**Francisco Lázaro**, también DPO).

Jesús Mérida, Rafael Hernández y Francisco Lázaro

Precisamente, comenzaron hablando de la necesidad de contar con lo que realmente necesitas. "Medir siempre está bien, pero el problema es contra qué mides. Es complicado encontrar una medida para todos", comentó Lázaro. Hernández, por su parte, consideró que sí es necesario medir pero también, que "el término SOC está mal usado y ha llegado un momento en el que todos deberían ir asentando la base y dar una visión global de lo que es realmente un SOC, que no debe quedarse en monitorizar sino aportar más". "Lo que me da miedo es la generalización de lo no generalizable. Cada cliente es único. Hay ciertos servicios, el SOC es uno de ellos, en los que hay que entrar a nivel de detalle conociendo muy bien al cliente", comentó Mérida.

Además, cada uno aportó su enfoque y visión sobre lo que suponen estos centros en sus compañías. Hernández destacó que, desde 2011, se apostó por contar con un "SOC avanzado que no sólo monitoriza y detecta, sino que además es el *core* de mis servicios de seguridad. Yo creo que en el mundo global en el que estamos somos multipaises, con un comité de dirección diverso, y ello obliga a ir a un sistema global en el que el SOC tiene que formar parte de tu tronco interior o tendrás problemas".

Lazaro explicó que, en el caso de Renfe, se depende mucho de "proveedores externos, porque se tiene una casuística concreta", aunque también puso en valor que la empresa ferroviaria ha apostado por la tecnología. De cualquier forma, destacó que "se pide un compromiso mayor de la cadena de suministro y que el concepto de ciberseguridad ha pasado de estar alineado con el negocio a ser el objetivo del negocio y, en el futuro, estará integrada en el negocio". También, resaltó el nuevo Centro de Ciberseguridad que la compañía ha abierto en Galicia.

Mérida comentó que, como parte del conglomerado áreo IAG, "se ha trabajado mucho en el de modelo de línea base de detección, con modelos como MITRE, para analizar los diferentes patrones de ataque contra infraestructuras y acercar el SOC al negocio", buscando "casos de uso para ser más eficientes en detección y respuesta". Además, señaló que, en aviación, hay mucha compartición de información entre compañías, "incluso a nivel de SOC".

En este sentido, todos los participantes apostaron por intercambiar información, por ejemplo, a través de la RNS, como ya se hace entre CISOs de forma sectorial en muchos ámbitos, a través de organizaciones sectoriales, como R-ISAC para el ferrocarril en Europa o de foros como First o Trusted Introducer. Eso sí, algunos participantes echaron en falta mayor compartición y colaboración de "las administraciones públicas y organismos de control". "Hay mucho margen de mejora", destacó Hernández. Lázaro consideró que sería positivo crear, como en Francia o EE.UU., una Agencia o Centro Nacional de Ciberseguridad.

etc. En este contexto, "el MSSP hace que todas las piezas puedan hablar entre sí", además, "es el aglutinador de todos los componentes en el modelo de transformación del puesto de trabajo", explicó. Para el directivo, "dentro de los proveedores de servicios es muy importante la parte de la integración", destacando Netskope Cloud Exchange, que brinda a los clientes potentes herramientas en este sentido. Terminó, recordando que los MSSP eligen a Netskope, "por la tecnología, la escalabilidad, por ser nube nativa y por poder trabajar con una plataforma, una consola y un único cliente".


Samuel Bonete


Roberto Ramírez

Cambio de paradigma

Acto seguido, **Roberto Ramírez,** Cortex sales manager para Iberia e Italia de **Palo Alto Networks,** volvió a poner encima de la mesa la sobrecarga que sufre el personal de los SOC, por lo que, "desde nuestra empresa entendemos que el SOC tiene que cambiar", afirmó. Para ello, "hay que introducir a las máquinas, los robots, para que estén en la base y sean asistidos por humanos. Se debe automatizar todo lo que se pueda". En este sentido, desde la compañía destacan su Cortex XSIAM, que añade esa capa de automatización y *machine learning*, además de ofrecer visibilidad. "La diferencia reside en nuestra arquitectura, a través de muchas fuentes de información, la procesamos y la automatizamos todo lo posible antes de que llegue al humano". Con ello, la compañía consigue una solución diseñada alrededor de tres conceptos que considera claves: datos inteligentes y analítica, automatización y seguridad proactiva, ofreciendo una transformación en la detección y respuesta, mejora de la experiencia del analista y reducción del riesgo continuos.

Detección y respuesta

Tras esta intervención, **Álvaro Fernández,** sales manager para Iberia de **Sophos,** subió al estrado para incidir en

MESA DE DEBATE 6

La importancia de los MSSP para los fabricantes, los perfiles más especializados y la interoperabilidad, entre los aspectos más debatidos

El broche de oro al evento lo puso un debate final en el que participaron los representantes de los fabricantes de la jornada vespertina del último día. En este espacio, dedicado a conocer el interés de los asistentes, destacaron asuntos relevantes como la opinión de los proveedores tecnológicos a la hora de mejorar los SOC. En este sentido, **Samuel Bonete (Netskope)** resaltó "la automatización y la IA, claves para mejorar los procesos dentro de los SOC". **Roberto Ramírez (Palo Alto Netwoks)** resaltó la importancia de que "los equipos hablen entre sí, que colaboren y una vez que se tienen claro los flujos de trabajo, que se proceda a la automatización usando *machine learning*, etc.". Para **Álvaro Fernández (Sophos)** lo importante es "hacer un ejercicio de reflexión y pensar qué es lo importante y centrarse en cómo puedo llegar a ello de la manera más eficiente y eficaz posibles". Por su parte, **Miguel Carrero** (**WatchGuard)** indicó "no perder el equilibrio entre personas, procesos y tecnología". Otra de las cuestiones que suscitaron más curiosidad recayó en si debería de haber una formación específica para profesionales de SOC. En esta ocasión, comenzó Carrero indicando que, efectivamente, "sería necesario un tipo de perfil específico, ya que no hay un entrenamiento concreto para las personas que trabajan en un SOC, especialmente, que haga exitosa la detección y la respuesta". Incluso, Bonete resaltó que "añadiría una asignatura en dicha formación: la integridad, porque la gente de los SOC trabaja con información muy sensible y de mucho valor". Los asistentes también se interesaron por la importancia de los MSSP para los fabricantes. En este sentido, Ramirez resaltó que son necesarios porque, "aunque disponemos de servicios gestionados no es nuestro núcleo de negocio, sería muy complicado proveer servicios a los 17.000 clientes de Palo Alto, necesitaríamos mucha inversión". De igual forma, Fernández indicó que "los necesitamos para seguir viviendo porque somos una empresa 100% canal. Tenemos más de medio millón de clientes a nivel mundial y el canal despliega y opera nuestra tecnología. Nosotros podemos ayudar a proveer esos servicios".

Samuel Bonete, Roberto Ramírez, Álvaro Fernández y Miguel Carrero

Para finalizar se lanzó a una última cuestión acerca de la interoperabilidad entre los propios fabricantes. Carrero resumió la opinión general de los ponentes, "intelectualmente y conceptualmente queremos, pero existen limitaciones tecnológicas. Además, existen intereses de negocio, una realidad que tampoco podemos obviar". Ramirez indicó que "hay ciertas cosas que compartimos, como en la Cyber Threat Alliance, donde no entra el negocio". Para Bonete, "una cosa es interoperar y otra cosa es compartir inteligencia porque es nuestro valor, es nuestra forma de seguir vendiendo", puntualizó. Fernández, asimismo, terminó indicando que "o te abres y colaboras con los demás, o los clientes no te eligen porque les están restringiendo".

otro de los temas candentes durante las jornadas. Y es que, "la ciberseguridad se ha vuelto demasiado compleja como para que la mayoría de las organizaciones la gestionen de forma efectiva", afirmó. En este contexto, "nuestra propuesta es entregar la ciberprotección como un servicio, donde se combina eficientemente servicios, tecnología, conocimientos y herramientas en una única solución holística", resaltó Fernández.

Entre otras soluciones, destacó sus servicios de detección y respuesta gestionados 24/7 a través de Sophos MDR, que cuenta con más de 15.000 clientes y está soportado por seis centros de operaciones de seguridad en todo el mundo. "La compañía está tan segura del servicio de MDR que, en la versión completa, ofrece una garantía de protección contra brechas de seguridad por valor de hasta un millón de dólares", concluía Fernández.

Funciones clave y beneficios del SOC moderno

Miguel Carrero, vicepresidente, Secure Service Providers & Strategic Account de **WatchGuard,** fue el encargado de cerrar este último bloque del encuentro. Centró su ponencia en las funciones clave y los beneficios del Modern SOC, que proporciona servicios de detección y respuesta a amenazas conocidas y desconocidas. "Esta función permite una respuesta más temprana minimizando daños y costes de los incidentes, además, opera y evoluciona en la intersección de personas, procesos y tecnología", puntualizó.


Álvaro Fernández


Miguel Carrero

En este sentido, destacó la propuesta WatchGuard for SOCs, que es la materialización de las soluciones de la compañía para hacer realidad dichos SOC. De todas las tecnologías, profundizó en su WatchGuard for SOCs Advanced Endpoint Security. Asimismo, destacó su plataforma WatchGuard Orion y sus Threat Hunting Services. Terminó su exposición recordando que WatchGuard for SOC se enmarca dentro de su Unified Security Platform, donde resaltó dos elementos críticos, la capa de XDR de ThreatSync y su Framework de Identidad, para configurar usuarios y dispositivos en función del riesgo, y que permiten obtener ese componente de automatización. ■

El mercado laboral en Reino Unido continúa con sueldos expansivos, sobre todo en áreas como respuesta a incidentes, GRC y gestión de accesos e identidades, según Cybershark

Uno de cada tres profesionales de ciberseguridad ya 'escucha ofertas' para cambiar de compañía, aunque el 80% vio crecer su nómina en 2022

El 83% de los consejos de administración aboga por contratar más personal de ciberprotección. Así lo destaca **Fortinet** en su último estudio 'Informe sobre la brecha de competencias en ciberseguridad', en el que recuerda que, actualmente, hay 3,4 millones de puestos sin cubrir en este ámbito.

Para conocer si este trabajo está bien pagado y cómo han evolucionado los salarios en las áreas más demandas en el último año, en el Reino Unido, el especialista en recursos humanos **Cybershark Recruitment** ha publicado la segunda edición de su 'Encuesta de salarios de ciberseguridad del Reino Unido 2023', con la opinión de más de 2.300 profesionales, 14% de ellos mujeres –en la anterior la muestra fue de 1.200–.

Un mercado impulsado por la escasez

La investigación, en colaboración con SC Media UK, constata que los trabajos mejor pagados son los de gobernanza, riesgo y cumplimiento o GRC (hasta 260.000 euros de media, al año), seguridad en la nube (hasta 251.000 euros), respuesta a incidentes (hasta 175.000) y gestión de acceso e identidades (hasta 158.000).

El informe también ha constatado un incremento de los salarios de forma notable en un año, sobre todo, en ciertas áreas como respuesta a incidentes (10,8%), gestión de acceso e identidades (10,3%) y GRC (6,6%), respecto a 2022. Por supuesto, en los salarios tiene un peso especial la experiencia ya que, en muchas áreas ejecutivas, por ejemplo, de GRC, los profesionales con más de 20 años de trayectoria cobran, de media, más de 220.000 euros. O en el caso de los centrados en la administración de acceso e identidades (IAM) se reconoce a los perfiles senior con sueldos por encima de los 147.000 euros al año, según el documento. Se trata de unas cifras que la directora ejecutiva del **Instituto Colegiado para la Seguridad de la Información (CISSec)**, **Amanda Finch**, considera lógicas, propiciadas por la

Salarios y evolución, según el área profesional, en ciberseguridad

	1-3 AÑOS	DIF. ANUAL	4-6 AÑOS	DIF. ANUAL	7-9 AÑOS	DIF. ANUAL	10-12 AÑOS	DIF. ANUAL	13-15 AÑOS	DIF. ANUAL	16-18 AÑOS	DIF. ANUAL	19-21 AÑOS	DIF. ANUAL	21+ AÑOS	DIF. ANUAL PROMEDIO
GOBERNANZA, RIESGO Y CUMPLIMIENTO	4.2750 64.980	5.33%	72.675 89.775	1.18%	84.075 101.175	6.44%	85.500 97.755	4.67%	117.420 136.800	22.92%	118.560 140.220	10.58%	131.100 159.600	-4.78%	182.400 262.200	6.62%
ARQUITECTURA DE SEGURIDAD	65.550 82.650	+7.83%	76.950 94.050	-3.70%	104.880 124.260	+10.32%	108.870 131.100	-3.14%	125.400 148.200	-3.85%	131.100 159.600	+0.50%	171.000 193.800	-2.66%	199.500 250.800	+0.76%
INGENIERÍA DE SEGURIDAD	56.715 66.405	+0.50%	68.400 85.500	-5.00%	84.075 102.600	-5.08%	96.900 114.000	-7.06%	119.700 136.800	+8.33%	128.250 151.050	+0.50%	136.800 159.600	-6.67%	•	-2.07%
RESPUESTA A INCIDENTES	51.300 72.390	+11.11%	65.550 82.650	+4.35%	88.350 108.300	+16.13%	99.750 120.270	+8.86%	114.000 133.950	+13.83%	128.250 153.900	+15.55%	142.500 176.700	+5.60%	•	+10.78%
ANALISTA DE SEGURIDAD	42.750 59.850	-6.67%	54.150 68.400	-7.37%	74.100 91.200	-0.80%	82.650 96.900	-5.86%	94.050 108.300	+5.00%	102.600 119.700	+0.00%	114.000 136.800	-12.00%	•	-3.96%
SEGURIDAD DE RED	39.900 54.150	0.00%	54.150 68.400	+5.26%	68.400 85.500	+1.67%	79.800 91.200	-2.14%	88.350 105.450	+3.78%	96.900 114.000	-2.94%	108.300 131.100	+3.16%	133.950 153.900	8.79%
INTERNET DE LAS COSAS	45.600 62.700	•	59.850 71.250	•	71.250 87.780	•	85.500 99.750	•	108.300 131.100	•	•	•	•	•	•	•
INFRAESTRUCTURA NACIONAL CRÍTICA	45.600 60.420	+13.33%	57.000 68.400	+10.00%	71.250 87.780	-4.00%	91.200 102.600	-6.25%	99.750 119.700	+3.80%	116.850 136.800	+4.39%	125.400 142.500	-6.36%	131.100 153.900	+2.13%
INTELIGENCIA DE AMENAZAS	45.600 62.700	+1.88%	62.700 76.950	0.00%	85.500 102.600	0.00%	99.750 114.000	+2.85%	102.600 128.250	+2.22%	114.000 133.950	+2.50%	125.400 142.500	0.00%	136.800 159.600	+1.35%
PRUEBAS DE INTRUSIÓN	57.000 71.250	+2.00%	70.395 86.355	-6.88%	105.450 125.400	+2.70%	125.400 142.500	-9.09%	136.800 159.600	-1.43%	•	•	•	•	•	-1.81%

necesidad de contratar profesionales en un mercado con déficit de ellos.

Ofertas y contraofertas

Además, la investigación destaca que el porcentaje de profesionales que se cambiaron de empresa por el mismo sueldo es similar al del año pasado (en torno al 12%), aunque sí es notable que un 10% de los participantes lo hicieron para ganar más. De cualquier forma, se observa que los sueldos han crecido, ya que frente al 65,3% de los profesionales que vieron incrementada su nómina en 2021, en 2022 esta cifra subió al 80,7%, seguramente impulsada por la necesidad de mantener el talento, así como la mayor remuneración fruto de la promoción y la atribución de mayores responsabilidades.

Los responsables del documento subrayan que, según su experiencia, "hay varias razones por las que las personas buscan dejar una organización, aunque el dinero, por lo general, en este sector, no es una de ellas". Asimismo, la investigación comprobó que los profesionales que aceptan una contraoferta para no irse tienen un 50% más de probabilidades de volver al mercado en tres meses y un 75% de hacerlo en medio año. "Esto se debe al hecho de que las razones iniciales para querer irse, que pueden tener que ver con la dirección, un colega o el equilibrio entre el trabajo y la vida personal".

Abiertos a cambiar de trabajo

El informe también manifiesta que se ha incrementado el número de profesionales que no esperan cambiar este año de trabajo -se ha pasado del 18,42% en 2021 a un 26,01% en 2022-, posiblemente porque, "cuando hay incertidumbre, este aumento se ajusta a la tolerancia al riesgo individual". Sí, destaca, sin embargo, que el 31% de las personas encuestadas permanecen abiertas al cambio, aunque no estén buscando activamente un puesto, lo que representa un aumento respecto al 26% del año pasado. Frente a estas cifras, un 24% confesaron estar "buscando activamente nuevas oportunidades, lo que eleva el total al 55% del mercado, ligeramente inferior al 63 % del año pasado".

Menos incentivos

En cuanto a los incentivos profesionales, los preguntados han respondido que este año se ha visto una reducción de lo ofrecido por las empresas respecto el año anterior, sobre todo, en lo que atañe a las bonificaciones relacionadas con el rendimiento, la asistencia médica privada, la cobertura de vida y el coche de empresa. Según la investigación, puede deberse a que actualmente gran parte del mercado trabaja "de forma remota o en un modelo híbrido", por lo que, por ejemplo, el coche ya no resulta tan demandado. Varios participantes también destacaron que este freno de los incentivos también se puede deber a la incertidumbre económica actual. Algo que también se constata por cuando sólo el 74% de los preguntados ha recibido el bono este año por el 91,64% de la edición anterior del estudio.

Menos brecha salarial de género

También, es notable que el trabajo en remoto se ha reducido del 52% al 50%, popularizándose el modo híbrido con tres días de trabajo desde casa y dos en oficina. Finalmente, analizando los salarios por género, resulta especialmente significativo que, mientras el de las mujeres participantes ha crecido un 11% de media al año, en el caso de los hombres esta subida ronda solo el 1,5%, lo que "indica que la brecha salarial de género se está reduciendo". ■

en Reino Unido (en euros)

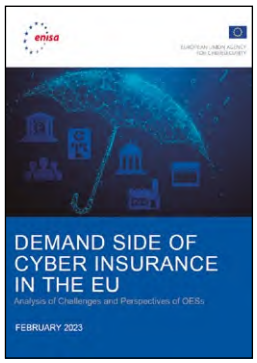
• (Datos insuficientes)

	1-3 AÑOS	DIF. ANUAL	4-6 AÑOS	DIF. ANUAL	7-9 AÑOS	DIF. ANUAL	10-12 AÑOS	DIF. ANUAL	13-15 AÑOS	DIF. ANUAL	16-18 AÑOS	DIF. ANUAL	19-21 AÑOS	DIF. ANUAL	21+ AÑOS	DIF. ANUAL PROMEDIO
RIESGO TECNOLÓGICO Y AUDITORÍA TI	41.040 56.430	+4.17%	57.000 74.100	+3.50%	76.950 94.050	+11.11%	85.500 102.600	+11.67%	94.050 112.860	+17.67%	94.050 114.000	+4.24%	99.750 119.700	-11.43%	114.000 135.090	+5.85%
GESTIÓN DE IDENTIDAD Y ACCESO	45.600 57.000	+12.50%	62.700 76.950	+18.18%	76.950 91.200	+8.15%	85.500 102.600	0.00%	102.600 125.400	+20.90%	111.150 133.950	+7.69%	119.700 142.500	+4.76%	136800 159.600	+10.31%
RESILIENCIA CIBERNÉTICA	37.050 51.300	+7.69%	54.150 68.400	+5.26%	71.250 87.780	-4.00%	79.800 91.200	-21.43%	102.600 124.260	+7.34%	108.300 125.400	-3.16%	119.700 136.800	-11.43%	131.100 171.000	-2.82%
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	34.200 48.450	+6.67%	51.300 59.850	0.00%	62.700 74.100	0.00%	76.950 93.480	-9.62%	85.500 102.600	+0.25%	102.600 125.400	-2.77%	114.000 131.100	-7.00%	136.800 159.600	-1.78%
SEGURIDAD EN LA NUBE	47.880 66.120	+16.67%	65.550 85.500	-2.61%	82.650 105.450	+10.34%	96.900 119.700	0.00%	11.4000 136.800	+8.33%	142.500 159.600	+4.00%	153.900 182.400	-18.52%	208.050 253.650	+2.6%
SEGURIDAD DE LA APLICACIÓN	51.300 68.400	•	62.700 76.950	•	79.800 96.900	•	91.200 114.000	•	102.600 125.400	•	131.100 153.900	•	136.800 16.5300	•	176.700 21.0900	•
DEVSECOPS	49.020 64.980	•	68.400 85.500	•	85.500 102.600	•	114000 125400	•	136.800 159.600	•	165.300 188.100	•	•	•	•	•
FORENSE DIGITAL	42.750 59.850	•	62.700 74.100	•	76.950 94.050	•	91200 108300	•	119.700 142.500	•	131.100 153.900	•	•	•	•	•
PUESTO FINAL DE SEGURIDAD	45.600 57.000	•	59.850 74.100	•	68.400 85.500	•	85500 102600	•	94.050 114.000	•	•	•	•	•	•	•
ZERO TRUST	42.180 54.150	•	57.000 68.400	•	74.100 91.200	•	88.350 105.450	•	108.300 131.100	•	•	•	•	•	•	•

El precio, la principal razón de contratación, aunque los procesos para conseguirlo cada vez son más largos, según Enisa

Ante el encarecimiento de las pólizas y la falta de definición de las coberturas, muchos operadores de servicios esenciales optan en su lugar por estrategias de mitigación

Si para un sector es crítico contar con una póliza de ciberriesgo, sin duda lo es para el integrado por los Operadores de Servicios Esenciales (OES). Por ello, la Agencia de Ciberseguridad de la UE (ENISA) ha profundizado en un amplio informe, con la opinión de más de 260 empresas, en cómo encaran su contratación, qué echan de menos respecto a las aseguradoras y si este tipo de seguro está realmente respondiendo a las necesidades que tienen sus posibles clientes. Precisamente, Revista SIC celebrará, el 13 y 14 de junio, una nueva edición de Espacio TiSec sobre este tipo de pólizas bajo el título "Ransomware, seguros cibernéticos y otras incógnitas: ciberseguridad endeble y ciberpólizas".



El seguro siempre ha sido un elemento fundamental de la economía, ya que permite transferir riesgos. En el ámbito cibernético, aunque aún le queda mucho por recorrer -las primeras pólizas de este tipo datan de los años 90-, ha ido ganando peso entre todo tipo de empresas que acuden a estas pólizas para reducir pérdidas en caso de incidente o, simplemente, por motivos regulatorios. Para analizar su situación actual, la **Agencia de Ciberseguridad de la UE** (Enisa) ha acometido un informe, bajo el título 'El ciberseguro europeo para operadores de servicios esenciales', en el que explora en profundidad los retos a los que se enfrentan los Operadores de Servicios Esenciales (OES) en el Viejo Continente a la hora de contratar pólizas cibernéticas, con la opinión de 262 organizaciones. En él, presta especial atención a si realmente el sector asegurador está dando respuesta a las necesidades de este tipo de compañías, incluidas las contempladas como 'instalaciones esenciales' y 'críticas' por la Directiva NIS (UE) 2022/2555, en vigor desde el 16 de enero.

Por ello, el informe es especialmente interesante por cuanto, a diferencia de otros estudios, se centra en el "lado de la demanda" del mercado de ciberseguros. Y, en este sentido, los resultados, son bastante llamativos: entre otros aspectos, destaca que tres de cada cuatro OES han reconocido que no pueden pagar las primas y que no cuentan con las coberturas que necesitan. Esto indica una contratación ligeramente más baja que los resultados ofrecidos en el informe de Enisa sobre 'Inversión por NIS de 2022', en el que el 32% de los OES/DSP afirmaron tener seguro cibernético, lo que marca "una tendencia a la baja en los últimos años".

Claroscuros del sector

El informe comienza recordando que el "seguro cibernético aún se encuentra en una fase de desarrollo y es un desafío captar cómo las expectativas sobre la cobertura pueden cambiar con el tiempo y cómo las amenazas emergentes pueden cambiar las expectativas con respecto a la cobertura". Por ello, también explica que lo esperable por parte de la industria de seguros cibernéticos es que se viva un aumento gradual de la demanda de este tipo de pólizas, que se basan en procesos muy concretos: identificación de riesgos, análisis de riesgos y establecimiento de un contrato.

Eso sí, existe un obstáculo importante que es la "comprensión detallada de los aspectos fundamentales del ciberriesgo para brindar una cobertura adecuada a los usuarios finales".

Esto también genera que los usuarios finales estén preocupados por la posible falta de divulgación o por información incompleta que provoque el rechazo de las reclamaciones. "Como resultado, es difícil determinar cuánto riesgo transferir y las aseguradoras también se pueden enfrentar a riesgos que quizás no hayan cuantificado adecuadamente", comenta el informe. También ha comprobado que, actualmente, la "falta de datos creíbles y el potencial de grandes pérdidas agregadas pueden dar lugar a pólizas con lagunas en las coberturas y límites demasiado bajos, lo que puede repercutir en una falta de indemnización por las pérdidas cibernéticas".

A ello se suman que las estadísticas sobre ciberincidentes no son completamente confiables, ya que las víctimas no siempre informan de ellos (por ejemplo, para evitar daños a la reputación). Y que, según resaltó uno de los participantes especializado en contratación de ciberpólizas, hay una preocupación sobre cómo interpretar ciertas cláusulas del contrato de seguro cibernético, mencionando la falta de estandarización en las cláusulas y la falta de precedentes disponibles para entender cómo se explicarían las cláusulas en un escenario de pérdida.

Reducir el riesgo

Frente a esto, la encuesta ha constatado que cada vez menos operadores críticos apuestan por el ciberseguro, sobre todo, por el aumento de precios, la caída de las coberturas y, en el caso de las

pymes, porque en el último año el número de incidentes de *ransomware* continuó creciendo.

De hecho, un 75% reconoció que, "actualmente, no tiene seguro ante ciberamenazas", apostando frente a ello por contar con estrategias de mitigación. En este sentido, el 77% destacó que ha puesto en marcha "un proceso formalizado para identificar los riesgos de ciberdelincuencia". Uno de los encuestados, un gran OES de Europa occidental, reveló que la organización había rechazado una póliza de seguro cibernético debido a los costos y las limitaciones en la cobertura disponible. La decisión clave en este caso fue invertir el presupuesto en la función del CISO, ya que se consideró más eficaz.

Así, en cuanto a los criterios para adquirir un ciberseguro, el precio parece ser el más importante, seguido de la reputación de la aseguradora, las coberturas, las cláusulas específicas y el respaldo.

De cualquier forma, un 64% afirmó no haber cuantificado el riesgo de ciberdelincuencia en su organización, aunque sí cuentan con programas de gestión de riesgos e implementación de controles para reducir la posibilidad de ciberincidentes. De hecho, el 56% reconoció que, a día de hoy, cree que "creía que hay otras herramientas de mitigación de riesgos más efectivas que los ciberseguros ciberpólizas".

A pesar de estos datos que evidencian que hay mucho camino por recorrer en este ámbito, los participantes resaltaron que, entre los principales motivos para contratar pólizas de seguro cibernético, están contar con una seguridad en caso de pérdida de información como consecuencia de un incidente, para el 46% de los preguntados, así como, en un 19%, la necesidad de contar con un conocimiento experto previo, necesario para ser asegurado, o posterior al incidente, cuando se reclaman las coberturas tras sufrir un ataque.

La cobertura en caso de incidente es, para casi la mitad de los encuestados, el motivo principal para contratar un seguro cibernético. Los requisitos por ley (19%), la cobertura previa al incidente (11%) y posterior al incidente (11%) fueron razones menos importantes. Los encuestados que no tenían seguro indicaron estar interesados en varios tipos de cobertura, que incluyen: continuidad comercial, soporte experto durante un incidente y cobertura de *ransomware*. Precisamente, gran parte de los participantes destacaron que "obtener cobertura ante este tipo de *malware* se ha vuelto cada vez más difícil en los últimos años".

La investigación también mostró que las empresas cada vez tienen dificultades para obtener un seguro cibernético por tres razones: en primer lugar, porque la cobertura no es suficiente para sus necesidades; en segundo, por la forma en que las aseguradoras evalúan a la organización; y, por último, porque el precio de la póliza de seguro u oferta generalmente no cumple con las expectativas. A ello, se suman que muchos participantes indicaron que el tiempo y el esfuerzo para renovar el seguro se estaban haciendo más largos y más intensos.

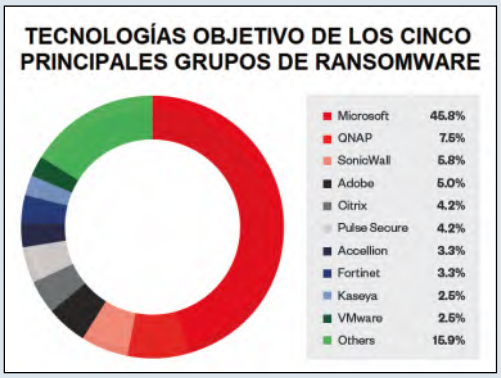
Recomendaciones finales

El documento termina con unas recomendaciones, para responsables políticos y OES, para mejorar las prácticas de gestión de riesgos de los OES, como impulsar el establecimiento de marcos para identificar y compartir buenas prácticas entre este tipo de operaciones, sobre todo, las que tienen que ver con la identificación, mitigación y cuantificación de la exposición al riesgo.

También, aconseja apostar por la estandarización y el desarrollo de guías, para contar con metodologías comunes de evaluación, sobre la cuantificación de los riesgos del delito cibernético y desarrollar alianzas con socios públicos y privados para habilitar marcos y programas de habilidades para la ciberseguridad, sobre todo, en lo que atañe a la evaluación de riesgos, los aspectos legales, la gestión de la información y la dinámica del ciberdelito del mercado de seguros. Asimismo, cree fundamental asignar o incrementar el presupuesto para implementar procesos de identificación de activos, métricas clave, realizar evaluaciones periódicas de riesgos, identificación de controles de seguridad y medición de riesgos con base en las mejores prácticas de la industria. ■

Cada pago de *ransomware* financia 10 nuevos ataques, según Trend Micro

Solo el 10% de las víctimas de *ransomware* pagan lo exigido por los cibercriminales, explica la investigación publicada por **Trend Micro**, 'What Decision-Makers Need to Know About Ransomware Risk', aunque las organizaciones que sí lo hacen financian, por cada vez, entre seis y 10 nuevos ataques, destaca el informe.



Entre las razones que llevan a las empresas a hacerlo está, según el documento, la de evitar una interrupción del negocio. De hecho, el informe explica que más del 50% que apostó por ello lo hizo en menos de 20 días.

"Es importante tener en cuenta que pagar el rescate solo aumenta el coste total del incidente para las víctimas: incluso el eventual descifrado de sus datos no deshará la interrupción del negocio y el daño a la reputación de la marca que la organización víctima podría haber sufrido por el ataque", resalta el informe que, a su vez, recuerda que "los atacantes son conscientes de que ciertas industrias y países que pagan rescates, también tienden a pagar más a menudo, por lo que tienen más probabilidades de encontrarse en el extremo receptor de los ataques de *ransomware*".

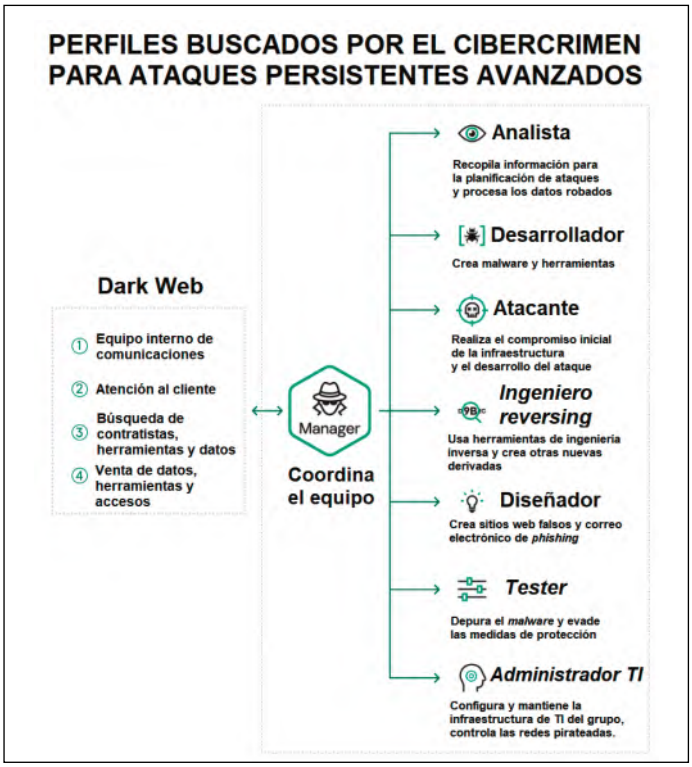
Como curiosidad, la investigación constató que, en los últimos dos años, las actividades de monetización del *ransomware* fueron más bajas en enero, y de julio a agosto. La razón es que son los meses elegidos por los ciberdelincuentes para fortalecer su estructura o tomarse vacaciones.

La ausencia de adicciones, como drogas y alcohol, es uno de los requisitos propios del proceso de reclutamiento por el cibercrimen

Ofertas de trabajo en la *Darkweb*: salarios de más de seis cifras, alta demanda, flexibilidad y mismas prácticas para atraer talento que 'los buenos'

"Le haré una oferta que no podrá rechazar", decía Marlon Brando en una de las míticas escenas de 'El padrino'. Y el cibercrimen no olvida esta máxima. Para conocer en profundidad qué ofrece, qué perfiles busca y si realmente paga más que 'los buenos', los investigadores de **Kaspersky** analizaron más de 200.000 ofertas de trabajo en 155 foros ilegales de la *Darkweb,* entre enero de 2020 y junio de 2022**.**

Y sus conclusiones no defraudan. Al igual que ocurre en el mercado clásico de ciberprotección, con más de dos millones de puestos sin cubrir, los grupos criminales también tienen déficit de 'profesionales'. Por ello, por ciertos perfiles muy 'codiciados' se ofrecen sueldos de hasta seis cifras, aunque no es lo habitual. "Los ciberdelincuentes necesitan una plantilla con habilidades específicas para las intrusiones en la infraestructura de sus objetivos, el robo de datos confidenciales o cifrar el sistema para su posterior extorsión", destacan los responsables de la investigación, que han comprobado que las ofertas buscan atraer candidatos ofreciendo tiempo libre pagado**,** bonificaciones por resultados y, además, no exigiendo requisito académico alguno, ni demanda de educación superior, ni registro de servicio militar, ni, por supuesto, ausencia de condenas previas, etc. Eso sí, curiosamente, sí tiene ciertas 'normas': se exige a los candidatos ser mayores de edad y no tener adicciones a las drogas, ni al alcohol.



Mucha demanda

En cuanto a los sueldos, las diferencias de lo pagado en función de los conocimientos y rol varían notablemente. Los más demandados son los desarrolladores (61% de las ofertas), con sueldos de hasta 19.000 euros/mes. Los *tester* (16%) y diseñadores (10%) les siguen en número de ofertas, aunque los perfiles son muy variados: desde moderadores de canales de Telegram, hasta expertos en comprometer redes corporativas. Así, por ciertos trabajos de *hacking,* los investigadores encontraron ofertas de hasta 1,1 millones de euros, en algunas ocasiones sobrepasando los 100.000. Sin embargo, estos casos tampoco son los más frecuentes, ya que los sueldos medios oscilan entre los 1.200 y los 3.800 euros por mes, por ejemplo, para expertos en ingeniería inversa. A estas cifras se ofrece, normalmente, sumar *bonus* por productividad. "Con cada asignación exitosa, obtiene un aumento y un bono instantáneo", destaca una de las ofertas. Curiosamente, algunas ofertas de trabajo no son para labores ilegales, como pasa con muchas en las que se pide perfiles que creen cursos de formación en TI.

Entrevistas prácticas

En lo referente a las 'entrevistas de trabajo', los investigadores comprobaron que para elegir a los candidatos, sobre todo para trabajar 'a largo plazo', se pide como punto de partida "piratear algunos sitios web chinos y enviar las bases de datos" para ver lo logrado. Por lo general, los candidatos suelen tener que someterse a varias rondas de selección, asignaciones de prueba que involucraban el cifrado de ejecutables de *malware* y la evasión de medidas de protección, así como un período de prueba.

Condiciones de empleo

En cuanto a la forma de atraer y mantener talento, se suele ofrecer la posibilidad de trabajar en remoto (45%), a tiempo completo (34%) y el horario flexible (33%). Los responsables del estudio destacaron que, de hecho, casi todo son trabajos en la distancia y que muchos anuncios ofrecen también "un equipo amigable". En definitiva, el informe recuerda que este tipo de trabajos intentan ser atractivos para quienes quieren ser 'autónomos' y nómadas digitales ofreciendo un alto grado de libertad: puedes tomarte tantos días libres como quieras, no hay código de vestimenta y eres libre de elegir cualquier horario, tareas y ámbito de trabajo.

Mercado pujante en las crisis

El informe también explica que, aunque no hay cifras del número de ofertas laborales totales, la contratación de más o menos profesionales también va en función de la 'situación del mercado'. Por ejemplo, entre otros aspectos, detectaron un *boom* durante la pandemia cuando la digitalización y el trabajo en remoto incrementó la superficie de exposición a todo tipo de ataques. Además, también ha constatado que los grupos más activos en contratar 'profesionales' son la delincuencia organizada y los especializados en ataques dirigidos (APT), que buscan "personas capaces de desarrollar y difundir códigos de *malware*, construir y mantener la infraestructura de TI, etc".

La investigación también comprobó que muchos de los candidatos que acuden a este tipo de ofertas, simplemente, necesitan dinero y, en otros muchos casos, "no tienen claro con quién están trabajando y se sienten atraídos por las expectativas de dinero fácil y grandes ganancias financieras. La mayoría de las veces, esto es solo una ilusión", resaltan los investigadores de Kaspersky que también consideran que muchos de los que se presentan a estas ofertas lo hacen fruto de necesitar dinero tras ser despedidos o por sufrir un fuerte recorte en su nómina, pretendiendo tener nuevos ingresos con trabajo para la ciberdelincuencia". ■

20 ANIVERSARIO

Predecir
lo que importa

La Alianza Líder que garantiza
la **gestión de vulnerabilidades**
y compliance técnico

tenable

mdtel
Platinum Partner

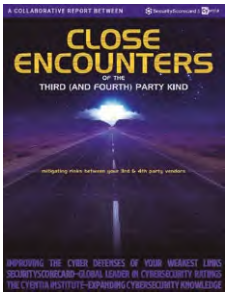
tenable ASSURE

www.mdtel.es
marketing@mdtel.es

* Tenable nombrada la única elección de los clientes de Gartner Peer Insights™ de 2021 para la evaluación de vulnerabilidades

La mayoría son maduras respecto a sus propios riesgos, pero pocas le dan la misma importancia a los que tienen a través de la cadena de suministro, según datos de SecurityScorecard y Cyentia

El 98% de las empresas hacen negocios o utilizan los productos de un tercero que ha sufrido una brecha de seguridad



El riesgo de la cadena de suministro se ha convertido en un problema de especial importancia en los últimos años y no tiene fácil solución por cuanto los expertos lo consideran de una gran complejidad. Como consecuencia, ha surgido una correlación preocupante y evidente: cuanto más depende una organización de terceros, mayor es la frecuencia de infracciones y fugas de datos.

Al menos, así lo demuestran los últimos estudios que analizan los riesgos de ciberincidentes entre terceros, el alcance de sus relacionales y su exposición. Uno de los más recientes, publicado por **SecurityScorecard**, firma especializada en calificaciones de ciberseguridad, y el **Instituto Cyentia**, focalizado en investigación y ciencia de datos, determinó que más del 98% de las organizaciones tienen relación con, al menos, un proveedor que ha sufrido una brecha en los últimos dos años.

El estudio, que analizó datos de más de 230.000 organizaciones, encontró, además, que la mitad de ellas tienen relaciones indirectas con, al menos, 200 empresas que son "cuartas partes" (proveedores de terceros) y que también sufrieron un ciberincidente en el mismo periodo de tiempo. "Esto no significa que esas organizaciones estuvieran involucradas o afectadas por esas infracciones, pero sí que casi todas están expuestas, al menos de forma indirecta, al riesgo en circunstancias fuera de su control", indican los responsables del informe.

Junto a ello, otros de los aspectos que añaden complejidad a esta problemática son las tecnologías que componen su "huella digital". Y es que, la investigación extiende el riesgo también a los proveedores de software y proyectos de código abierto. Ciberataques como el sufrido por **SolarWinds** y vulnerabilidades en componentes de software ampliamente utilizados como Log4J, son solo dos ejemplos del aumento de su exposición a sufrir un incidente cibernético.

En concreto, el documento presenta un ranking de las 50 tecnologías más utilizadas por las organizaciones en su relación con proveedores, que forman parte de su "huella digital" y, por ende, de su superficie de ataque. Las principales son **Google** Analytics, Google Tag Manager, **Amazon** Web Hosting, PHP, los productos de **Facebook,** Amazon Web Services y **Microsoft** 365, involucradas en más del 60% de las relaciones con terceros (Google Analytics, incluso, en el 82,3%), destaca el informe.

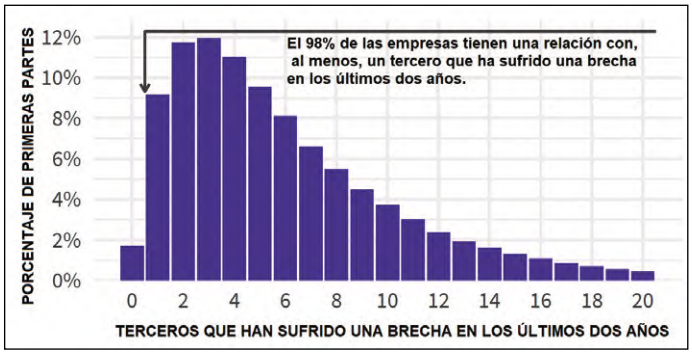
La inevitable dependencia en terceros

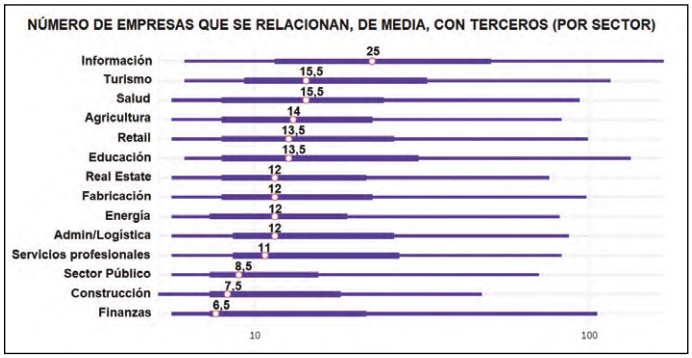
El estudio también analiza los vínculos que se establecen por sector, destacando por encima de todos el de servicios de información, con el mayor número de conexiones con proveedores (una media de 25). Le siguen turismo, salud y educación, una clasificación que no sorprende a los responsables del estudio que afirman que las empresas que operan en estos campos "dependen de los proveedores de servicios para hacer su cometido".

En el extremo opuesto se encuentran la Administración Pública, la construcción y el sector financiero, con la media más baja de relaciones con terceros (menos de ocho empresas). Esto se debe, según el informe, a que "el sector público y las entidades financieras están fuertemente regulados lo que se traduce, en general, en una mayor diligencia y requisitos de cumplimiento".

En cuanto a la dimensión regional de estas relaciones, la investigación subraya que el 59% de las organizaciones tienen conexiones con empresas de, al menos, cinco países, un 14% trabaja con proveedores de 10 naciones o más, y solo un 7% opera sin vínculos con el extranjero. Eso sí, "hacer negocios con una empresa en otro país no aumenta o disminuye necesariamente el riesgo cibernético, pero sí expone a una organización a nuevas leyes, requisitos de seguridad y otros problemas geopolíticos que debe de tener en cuenta", matiza el informe.

En concreto, el 99% de las organizaciones tienen relación con compañías en Estados Unidos y Canadá; el 61,6%, con el sur de Asia; y el 51,6%, con el norte de Europa.





Comprender los riesgos asociados

A pesar de estos datos, los responsables del estudio señalan que "todo esto tampoco significa que las organizaciones deban reducir el número de relaciones con terceros para reducir su exposición. Más bien, el objetivo es que tanto ellas como sus MSSP comprendan los riesgos asociados y tomen medidas para mitigarlos".

El problema, no obstante, es que "muchas organizaciones aún desconocen las dependencias y exposiciones inherentes con la cadena de suministro y simplemente se enfocan en administrar su propia postura de seguridad. Otras son conscientes de esos problemas, pero no toman decisiones basadas en la protección, ni exigen que los proveedores cumplan con ciertos estándares. Incluso, aquellas que sí establecen requisitos de ciberseguridad con terceros tienen dificultades para monitorizar de forma continua el cumplimiento y el progreso", explica el informe.

Así pues, la gestión de riesgos con la cadena de suministro debería de ser un componente fundamental de los programas de seguridad y cumplimiento de cualquier organización. "Ninguna empresa puede permitirse el lujo de encerrarse en sí mismo en cuanto a su ciberseguridad", ya que, "aquella que invierte mucho esfuerzo en asegurar su propia infraestructura podría ver esos esfuerzos socavados por proveedores que no mantienen un nivel similar de protección", concluye la investigación. ■

235%

Akamai ha observado un aumento del 235% en los ataques de phishing.

¿Tú solución de MFA está a prueba de phishing?

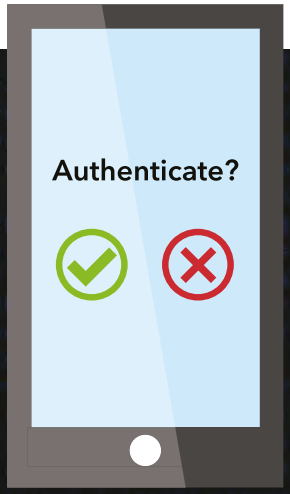
Akamai MFA: Seguridad FIDO2 sin claves de seguridad físicas

Protege tu empresa contra el robo de cuentas de empleados, y filtración de datos con la tecnología MFA de última generación. Convertimos tu smartphone en una llave de seguridad, con una autenticación sencilla, y sin carga de trabajo para tu equipo de TI.

Máxima seguridad

Push mobile a prueba de phishing

Gestión de TI unificada y sencilla



Akamai MFA – pruébalo gratis durante 60 días

Solicita una prueba gratuita en: contact-spain@akamai.com
o si lo prefieres, llámanos al Tel. 91 793 32 43

La falta de automatización, el cambio de las exigencias regulatorias y la complejidad de investigación principales causas, según Magnet Forensics

Agotamiento generalizado de los especialistas forenses en respuesta a incidentes (DFIR) ante el incremento de amenazas y la falta de profesionales

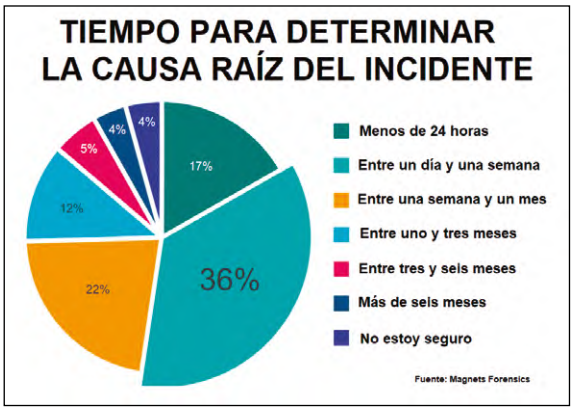
La rápida evolución del delito cibernético está afectando a los equipos de seguridad mucho más que el año pasado, lo que está llevando a un agotamiento generalizado y un posible riesgo regulatorio. Así lo destaca una investigación, de finales de 2022, de la compañía canadiense **Magnet Forensics,** bajo el título 'State of Enterprise DFIR 2023', para la que ha preguntado a casi 500 especialistas en análisis forense digital -el 60% integrado en el equipo del Centro de Operaciones de Ciberseguridad- de empresas de EE.UU., Europa, Oriente Medio y África. "Los equipos de análisis forense digital y de respuesta a incidentes han demostrado ser indispensables para combatir a los ciberdelincuentes, pero la complejidad y el volumen de los ataques, así como la escasez de talento disponible para hacerles frente están provocando un cansancio sin precedentes", explica en el informe el director ejecutivo de la compañía, **Adam Belsher**.

Entre sus datos más relevantes, destaca que más del 40% de los encuestados describieron la evolución de las técnicas de ciberataque como un problema "grande" o "extremo" que afecta a sus investigaciones. De hecho, el 45% cree que el incremento de la complejidad de los ataques, también conlleva un trabajo, cada vez, más exhaustivo y largo en el tiempo para determinar el origen del incidente.

Además, consideran que los equipos de ciberseguridad están tardando demasiado en llegar a la raíz de estos ataques. Más del 43% de los participantes reconoció que les lleva entre una semana y más de un mes conseguirlo. Y, aproximadamente, uno de cada tres participantes reveló que para reducir estos plazos hay que acometer, en la forma de trabajo y en los medios, una "revisión completa" o "mejoras importantes".

De hecho, el 64% confesó que se nota una "fatiga de alerta e investigación" que lleva al "agotamiento" de muchos profesionales, motivado también por la falta de automatización en el ámbito forense. Ello obliga a los profesionales a realizar tareas repetitivas y de forma manual que se podrían evitar, con más tecnología, permitiéndoles centrarse en las labores que demandan mayores conocimientos y experiencia.

Además, el 37% de los profesionales se quejó de que la empresa no tiene una estrategia coherente de respuesta a incidentes y un 36% lamentó no contar, en esas situaciones, con procesos estandarizados que permitan, además de cumplir las diferentes normativas de cada ámbito y rol profesional, actuar de forma más rápida y eficaz.



Correo-e

En cuanto a los vectores de ataque que más trabajo suponen para los especialistas forense, el primero es el compromiso del correo electrónico corporativo. Esta amenaza ya supone, al menos, el 14% de los casos investigados y, según el estudio, ya supera, en frecuencia, a las posibles infecciones por *ransomware*, la amenaza de seguridad más común en la anterior edición del informe. Además, el 50% de los participantes explicó que el compromiso del correo-e lleva tanto trabajo que suele requerir de recursos de terceros para ayudar con la investigación.

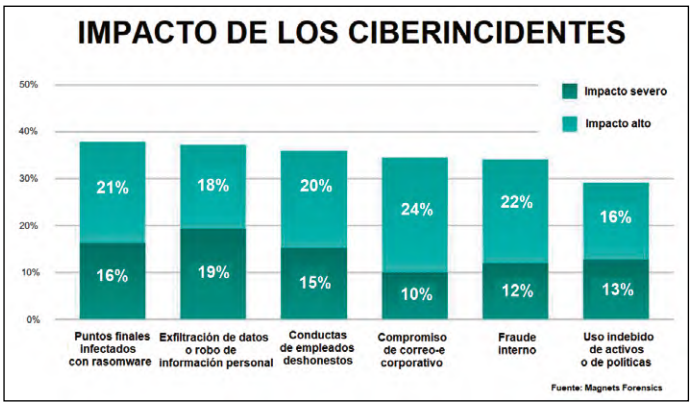
Problema regulatorio

Esta situación, explica el documento, también hace que, al no poder llevarse a cabo todos los trabajos de investigación necesarios, el 46% considere que no "tiene tiempo para comprender las nuevas regulaciones de ciberseguridad". Por eso, el informe recomienda que los equipos legales trabajen con los expertos en DFIR para explicarles cómo cumplir, de forma fácil, las nuevas normativas proporcionándoles los recursos que necesitan.

El documento también resalta que uno de cada tres encuestados también ha destacado el problema que supone reclutar y contratar a profesionales, por el déficit existente en este ámbito (sólo en EE.UU. se calcula que hay sin cubrir en torno a 750.000 vacantes).

Por ello el 50% de los participantes destacó la necesidad automatizar lo máximo posible muchos trabajos de DFIR, incluyendo la identificación remota de puntos finales que pueden ser objetivo de ciberataques y el procesamiento de las evidencias digitales, por cuanto "el tiempo es esencial cuando se produce un potencial compromiso".

De hecho, el documento recuerda que "los retrasos en descubrir la causa raíz de un incidente de ciberseguridad exponen potencialmente a la organización a más riesgos y al impacto en la continuidad de negocio". También, resalta la importancia de que las empresas cuenten con una estrategia de respuesta a incidentes dinámica, que se pueda adaptar a las nuevas ciberamenazas y a la situación estratégica de la organización.



Problema común al de los CISO

Por otro lado, **Gartner** publicó un informe, en febrero, del que se desprende que casi la mitad de los responsables de ciberseguridad aspiran a cambiar de trabajo para 2025 e, incluso, uno de cada cuatro no descarta abandonar el sector. "Los CISO intentan constantemente equilibrar las altas expectativas con la ausencia de las herramientas necesarias para cumplir con ellas", destaca el documento a la vez que recuerda que, actualmente, "los programas de seguridad cibernética centrados en el cumplimiento, el apoyo ejecutivo significativamente bajo y la madurez a nivel de la industria por debajo del promedio son indicadores de una organización que no considera que la gestión de riesgos cibernéticos sea fundamental para el éxito comercial". Por ello, según explica la analista directora de la firma, **Deepti Gopal,** este rol también se está enfrentando a unos "niveles de estrés insostenibles". ■

NOVARED

Innovación en CiberSeguridad

EXPERTOS EN CIBERSEGURIDAD

Para mitigar los riesgos de su negocio

27 AÑOS EN IBEROAMÉRICA

protegiendo a nuestros clientes

novared.net

comunixgroup.com

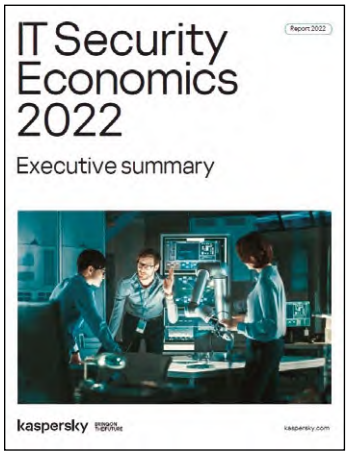
Escuela de Hacking Ético de Novared

Calle Orense 16 6ºC. 28020, Madrid
+34 91 771 23 90
infoesp@novared.net

Un 48% también confió en personal externo para responder mejor a los ciberincidentes, según Kaspersky

La complejidad de las soluciones tecnológicas obliga a las empresas a contratar proveedores de servicios para gestionar mejor su ciberseguridad

Disponer de una buena solución de ciberseguridad no garantiza la mejor protección si no se cuenta con un equipo que la gestione debidamente. Y ponerle remedio no es tarea fácil dado el conocido déficit de profesionales altamente cualificados existente en el mercado. Según el 'Cybersecurity Workforce Study de 2022', de **(ISC)²,** se necesitan 3,4 millones de trabajadores en todo el mundo; en EMEA son 317.050 de puestos sin cubrir y en España la cifra estimada llega a más los 60.400. Esta situación está forzando a las empresas a externalizar determinadas tareas a proveedores de servicios gestionados (MSP) o proveedores de servicios de seguridad gestionada (MSSP), ya que disponen de profesionales con una alta especialización y en constante evolución.



3.230 responsables de TI

Así se desprende del informe 'IT Security Economics', que **Kaspersky** realiza cada año y que, para esta edición, contó con 3.230 responsables de TI, tanto de pymes (de 50 a 999 empleados) como de grandes empresas, de 26 países.

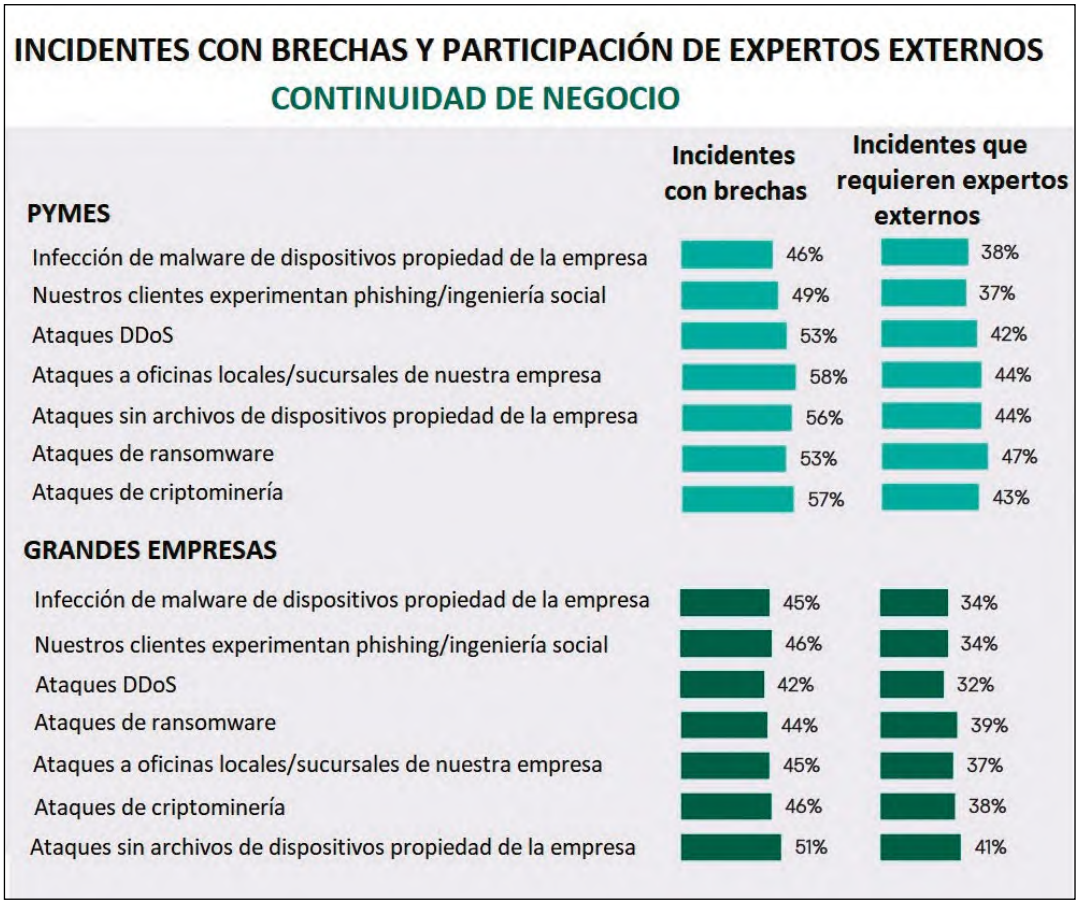
La investigación destaca que, concretamente, en Europa, un 54% de las pymes y corporaciones que transfirieron tareas de seguridad TI a MSP y MSSP el año pasado, lo hicieron por la eficiencia que otorgan los trabajadores externos. Esas organizaciones también mencionaron la necesidad de tener conocimiento especializado en la plantilla (48%), la complejidad de los procesos comerciales (40%), la escasez de empleados TI (34%) y los requisitos de cumplimiento (33%).

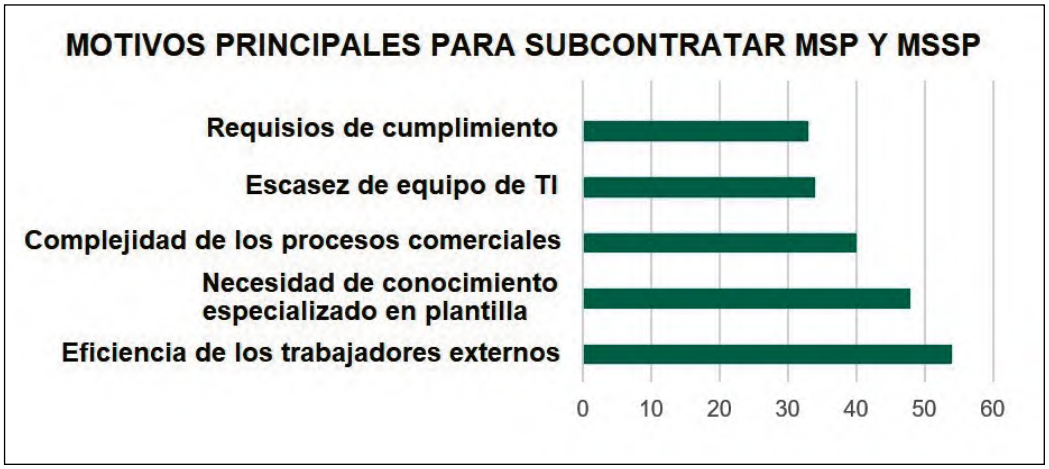
Más de la mitad de las empresas europeas (64%) también aseguró trabajar con dos o tres proveedores, mientras un 10% de pymes y el mismo porcentaje de las grandes corporaciones reconocen tratar con más de cuatro proveedores de seguridad informática distintos al año.

Eso sí, "es importante entender, en cualquier caso, que la empresa debe tener conocimientos básicos de seguridad de la información para evaluar adecuadamente el trabajo que realiza el personal subcontratado", explica **Konstantin Sapronov**, jefe de Equipo Global de Respuesta a Emergencias de Kaspersky.

Soporte a incidentes

Otros de sus datos más destacados es que casi la mitad de los encuestados (48%) confió en profesionales externos, en 2022, para



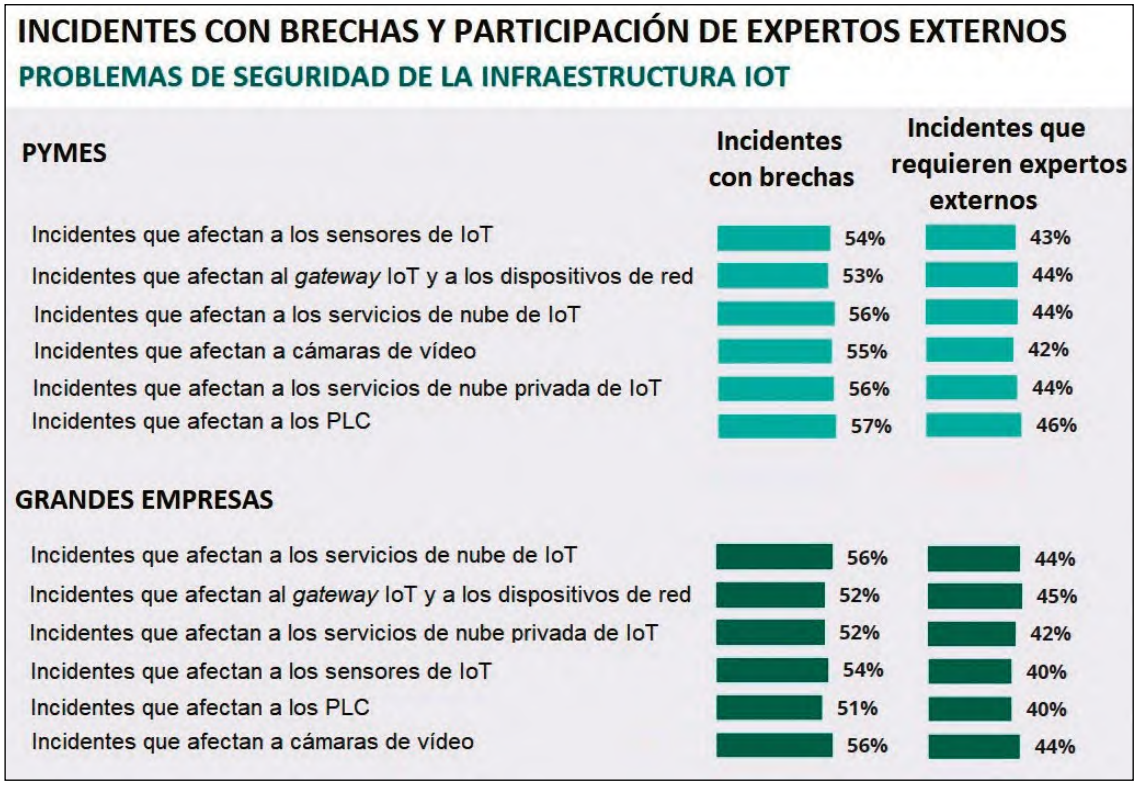


responder mejor a los incidentes que sufrieron. Contratar analistas de seguridad de TI o personal especializado en respuesta a incidentes de ciberseguridad fue la mejor solución para el 52% de las pymes y el 56% de las grandes empresas. De hecho, la mitad de las pymes y el 46% de las grandes empresas establecieron nuevos equipos o personas dedicadas a la seguridad de TI después de un ciberincidente. Para acelerar la situación, el 57% de las pymes y el 62% de las empresas emplearon servicios externos o consultores para evaluaciones de riesgos de ciberseguridad (32% pymes y 38% grandes empresas), o servicios de ciberprotección de respuesta a incidentes (un 28 y 33%, respectivamente).

En concreto, los incidentes principales que se consideraron lo suficientemente complejos como para requerir expertos externos afectaron al 76% de los entornos virtuales de las grandes empresas y al 79% de los de las pymes. También, afectaron en gran medida a sus servicios en la nube de IoT (72% y 84%, respectivamente) y a su infraestructura de TI (82% y 79%).

Por ejemplo, en el caso de las pymes, requirieron la ayuda de expertos para paliar los estratos del *ransonmware* que afectaron a la continuidad del negocio en el 47% de los casos), por ataques DDoS en un 44%, así como a los dirigidos a sus oficinas o sucursales (44%). Las grandes empresas recurrieron a la contratación de terceros para ofrecerles soporte ante ataques sin archivos a dispositivos propiedad de la empresa (41%), ataques DDoS (39%), criptominería (38%) y *ransomware* (37%).

En general, los incidentes relacionados con la violación de las políticas de seguridad de TI y el uso inadecuado de los recursos de TI, por parte de los empleados, fueron los casos en los que se requirieron menos asistencia externa, tanto para las pymes como para las corporaciones, según el documento.



Protección de datos y transparencia

Con todo, la protección de datos es la mayor preocupación para más de la mitad de las empresas encuestadas (53%). Le siguen el coste de asegurar entornos tecnológicos cada vez más complejos (43%) y los problemas con la adopción de la infraestructura de la nube (38%).

Como resultado, el estudio señala que se está poniendo mayor atención a las políticas de transparencia de los proveedores y contratistas ya que se están convirtiendo en un problema de seguridad para las empresas, especialmente, en lo que tiene que ver con la gestión de los datos. Así pues, el 91% de los encuestados cree que las políticas de transparencia, o su ausencia, son cruciales a la hora de pensar en trabajar con un contratista. Y, si bien el 78% de las organizaciones encuestadas ya cuentan con estándares de transparencia, el 81% dijo que estaría dispuesto a invertir para ampliarlas. ■

Incrementar personal, automatizar más y tener planeada la negociación del rescate entre las opciones que más suben, según Cybereason

Los ciberataques de *ransomware*, en fines de semana y vacaciones, amplifican su impacto por la falta de personal y lentitud de respuesta

Hace pocos años, a **Joaquín Castellón,** hoy CSO de **Navantia** y entonces director operativo del **Departamento de Seguridad Nacional** (DSN), le gustaba recordar que los principales ataques, con impacto, se producen los viernes o fines de semana. Incluso, explicaba que tenían un cartel colgado que lo recordaba. Sirva como ejemplo que el mediático WannaCry se produjo un viernes. Y es que, según los expertos, los ataques que aprovechan los festivos o las vacaciones son parte de la estrategia del cibercrimen para lograr el mayor impacto. Por eso, es especialmente interesante el informe que ha realizado la compañía **Cybereason,** 'Organizaciones en riesgo 2022: atacantes de *ransomware*. No te tomes vacaciones", sobre los incidentes del cibercrimen en los días de libranza en el sector de la ciberseguridad.

Realizado con la opinión de más de 1.200 profesionales de EE.UU., Reino Unido, Alemania, Francia, Italia, Emiratos Árabes Unidos, Sudáfrica y Singapur, entre septiembre y octubre, constató que, tal y como se suele decir, con cifras, los principales incidentes de *ransomware* se sufren los fines de semana y días festivos, lo que complica la detección, detención y recuperación por falta de personal en esas jornadas.

Así lo reconocieron más de un tercio de los preguntados que, además, destacaron que en 2022 experimentaron unas pérdidas por este motivo un 19% mayores que en 2021. Es más, en sectores como el educativo, los ataques de *ransomware*, en fines de semana o vacaciones, subieron un 42% y en el turismo un 48%, los más afectados. Y no son cifras desdeñables, ya que, según el informe, el *ransomware* está presente en casi la mitad (49%) de los ciberincidentes a los que los equipos de los Centros de Operaciones de Ciberseguridad (SOCs) hicieron frente el último año.

Una situación preocupante por cuanto un 44% de los participantes destacaron que los fines de semana y festivos, el personal dedicado a la protección cibernética se reduce hasta el 70% por libranza. Además, un 21% destacó que sus compañías tienen para esos días un equipo mínimo. Sólo un 7% explicó que, por su estrategia organizativa, sí cuenta con entre el 80% y el 100% de los puestos de ciberseguridad cubiertos.

El estudio también hace una comparativa por países y sectores de los diferentes niveles de rotación de personal para en días festivos. Así, entre los que menos profesionales dedican a ciberprotección en días festivos destaca Alemania, con un 91% de las empresas con el 50% de su plantilla en esta área, seguido de Emiratos Árabes, con un 75%, Francia con un 72% e Italia con un 71% de las organizaciones a 'medio gas'. Curiosamente, EE.UU. cuenta con mayor preparación: la mitad de las empresas dedican más personal que ese 50% de media.

Bajar la guardia

De cualquier forma, no tener personal dedicado en la justa medida los festivos suponen mayor impacto. Uno de cada tres encuestados (34%) reconocieron que invirtieron una cantidad mayor en recuperarse tras un incidente los fines de semana, por lo que supuso organizar rápido a su equipo de respuesta a incidentes esos días; un 37% también destacaron que tardaron más en analizar y tener claro el alcance del ataque y el 36% señalaron un mayor tiempo de recuperación, especialmente en EE.UU., donde este aspecto fue manifestado por el 44% de los preguntados, un 19% más que en 2021.

Lógicamente, cuanto mayor es la empresa, más complejo y lenta fue la respuesta. El 43% de los responsables de ciberseguridad de compañías con más de 2.000 empleados así lo destacó, el 48% de este perfil también reconoció su mayor tiempo en evaluar el incidente y el 40% en pararlo, además de un 36% en recuperarse.

IMPACTO DE UN ATAQUE DE RANSOMWARE EN FESTIVO RESPECTO A DÍAS LABORABLES

34%	37%	36%	31%	37%
Llevó más tiempo contar con el equipo	Llevó más tiempo detener el ataque	Llevó más tiempo recuperarse del ataque	Tuvo mayor impacto económico	Llevó más tiempo evaluar el alcance del ataque

Por sector	Educación	Finanzas	Salud	Telecomunicaciones	Fabricación	Restauración y ocio	Transporte viajes
Nos llevó más tiempo evaluar el alcance del ataque	54%	39%	30%	35%	38%	41%	33%
Nos llevó más tiempo responder / detener el ataque	42%	40%	31%	31%	37%	40%	43%
Supuso mayor impacto económico	42%	24%	34%	24%	32%	31%	38%

Sin tiempo para la familia

El problema es que muchos profesionales de la ciberseguridad consideran que su trabajo requiere horas más allá de lo habitual. Por ejemplo, en este informe, el 88% de los preguntados reconocieron que se habían perdido una celebración navideña o una celebración de fin de semana por un incidente de *ransomware*. Es más: en EE.UU. Alemania esta cifra alcanzó los 91% y 95% y, por sectores, en el financiero el 95%. Por eso, el informe destaca que, en el ámbito de la ciberseguridad, se precisa otro planteamiento que el clásico horario laboral de lunes a viernes, destacando la correlación directa que hay entre el incremento de ataques y los periodos festivos, tendencia que también confirmó la anterior versión de esta investigación.

En este sentido, el documento termina con unas recomendaciones entre las que destacan estudiar diferentes modelos de contratación de personal para analistas de SOC y especialistas de respuesta a incidentes, así como establecer un nivel mínimo de personal para los fines de semana y festivos, además de establecer un plan para contactar y contar con profesionales clave a cualquier hora y día, en caso de detectarse un incidente. También, recomiendan implementar una estrategia de detección y respuesta administrada (MDR), con la contratación de proveedores de servicio, para disponer de capacidades de monitorización, detección y respuesta a incidentes 24x7. Asimismo, recomienda proteger, de forma especial, las cuentas privilegiadas esos días, ya que son el objetivo prioritario de los cibercriminales para alcanzar sus objetivos e, incluso, contar con la capacidad de desactivarlas en caso de ataque de *ransomware,* entre otros aspectos.

De cualquier forma, el estudio también enfatiza que un 31% de las empresas –una cifra baja de cualquier forma– ya está incrementando su personal para que responder más rápido a ataques de *ransomware*, un 29% también apuesta por la automatización para acelerar la detección y respuesta e, incluso, un 27% está aprendiendo a negociar el rescate con los cibercriminales y poniendo en marcha sistemas de pago específicos. ■

fastly

Signal Sciences
Now part of fastly

Protege las experiencias que impulsan tu negocio.

No importa dónde despliegues tus aplicaciones: Fastly puede protegerlas a escala. Ofrecemos a los equipos de desarrollo y seguridad soluciones que aportan visibilidad, control y acceso a información útil.

- **Una protección que no afecta al rendimiento.**
- **Despliegue flexible y gestión sencilla.**
- **La seguridad para aplicaciones que sí querrán tus desarrolladores.**

Más información en:

fastly.com/es/products/cloud-security

xMDR de Cipher: servicio para centralizar todas las herramientas de detección de incidentes de seguridad del cliente, con integración rápida y sencilla

xMDR es la nueva línea de servicios de Cipher. Se trata de un servicio modular, de última generación, basado en inteligencia de amenazas, *threat hunting*, inteligencia artificial y robotización, que permite a la detección y respuesta de incidentes la evolución continua necesaria para adaptarse, tanto a las amenazas cambiantes que pueden impactar a nuestros clientes, como a la propia evolución TI de los mismos, habilitando, mediante la información accionable del servicio, la mejora continua en ciberseguridad. El servicio combina la caracterización del adversario digital para la priorización de casos de uso con el objetivo de mejorar continuamente la eficiencia y eficacia en el mismo (falsos positivos por debajo del 1%). Es un servicio ágil y fácilmente integrable en el ecosistema del cliente.

Propósito

La misión de Cipher es proteger a las empresas e instituciones mediante la mejora continua de su postura de ciberseguridad en su entorno digital, ya sea IT, OT, IoT o Cloud.

xMDR es la materialización de nuestra misión, una **solución adaptable para proporcionar a nuestros clientes resultados accionables**, siendo este un desarrollo a partir de nuestra propia tecnología que evoluciona de los productos existentes. Se trata del desarrollo propio de la plataforma (CipherPlatform) con un marco común que cuenta con **múltiples módulos** que interactúan y enriquecen alertas e incidentes que cubren múltiples ángulos para reducir la exposición al riesgo de un cliente.

Modalidades del servicio

xMDR está diseñado para ser modular. Se pueden añadir a la plataforma varios módulos dirigidos a funciones específicas para ampliar su funcionalidad básica. El objetivo del servicio xMDR de Cipher es responder a la **mejora de la visibilidad y mejora continua**.

En la siguiente imagen, se ven los diferentes módulos que pueden ser añadidos al servicio xMDR y a la plataforma de manera que trabajen coordinados desde un punto de vista de la detección y respuesta ante incidentes.

El camino hacia la anticipación

Nos basamos en el **panorama de adversarios digitales** del propio cliente, analizando todas las fuentes de datos pertinentes. De este modo, le ayudaremos a vencer rápidamente a cualquier adversario que tenga como objetivo sus activos y aumentaremos su resistencia frente al *ransomware*, distintas campañas y otras ciberamenazas.

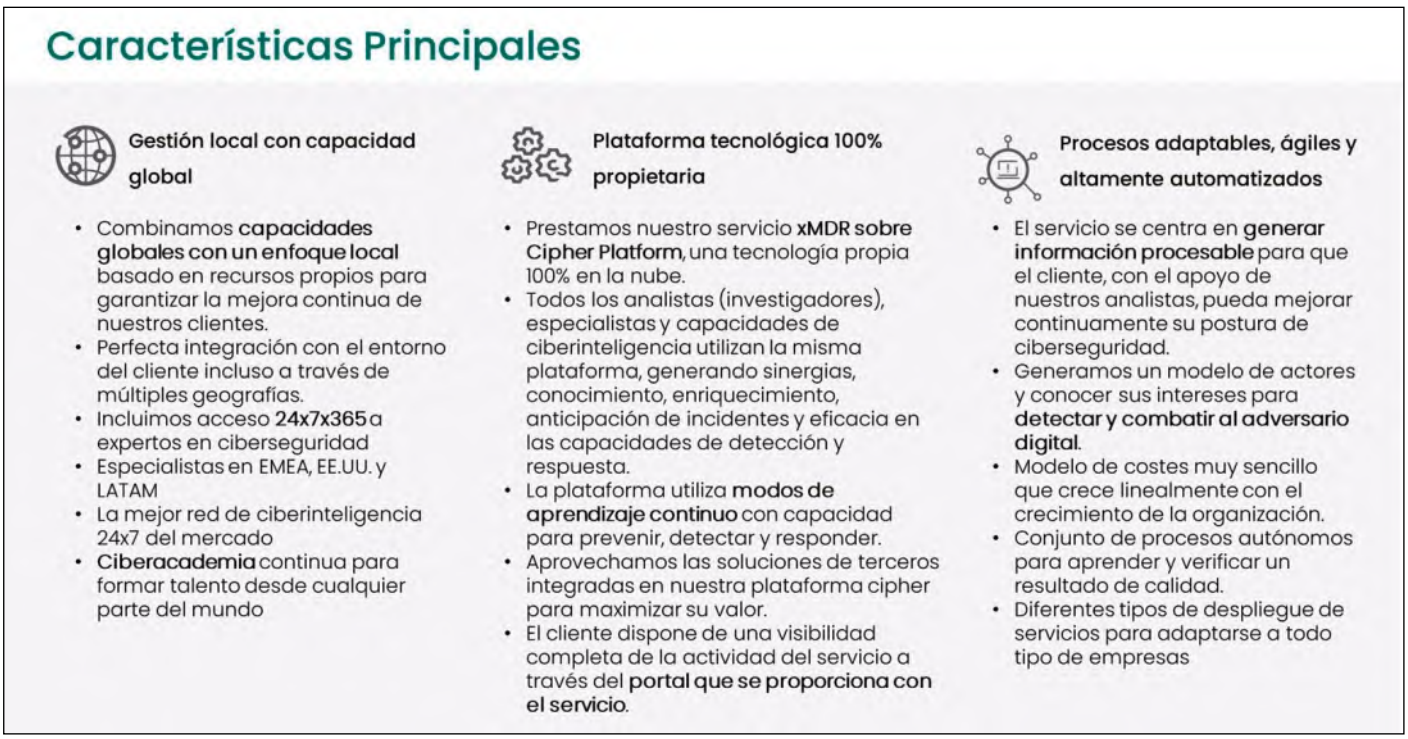
Modelado digital del adversario

Nuestro servicio parte siempre de una aproximación real al nivel de exposición del objetivo (cliente) por parte de los adversarios digitales, **queremos conocer a nuestro enemigo** para poder defendernos correctamente.

Por ello, nuestra primera aproximación es **generar un modelo del adversario digital** y conocer sus intereses, patrocinadores, campañas activas, técnicas y herramientas que utiliza para aplicar las **reglas y *queries*** necesarias para detectar y combatir al adversario digital.

Perfilamos al adversario digital por medio de los actores o grupos APT, herramientas o malware que pueden usar y CVE para aquello que ya es conocido y estadísticamente podemos detectar y que sabemos que impactará en mayor medida a nuestros clientes.

Con toda esta información, especialmente con el conjunto de investigaciones que tenemos y cruzándolo con nuestras metodologías como D3FEND y con nuestra Inteligencia de



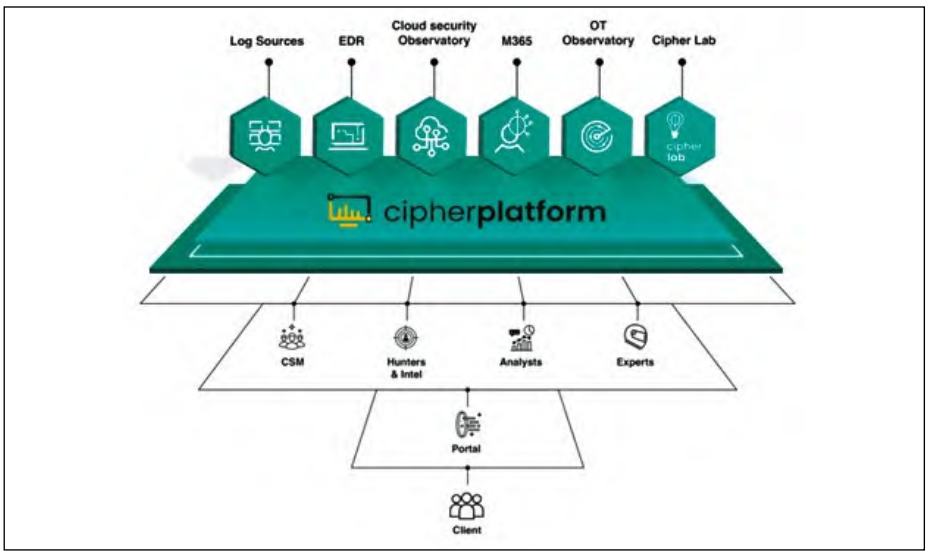
Amenazas, se genera un catálogo de reglas que operativizaremos en los clientes en función de su perfil, y que se utilizarán posteriormente para la generación de los diferentes casos de uso, y que se ampliarán y enriquecerán internamente a lo largo del ciclo de vida del servicio (mejora continua).

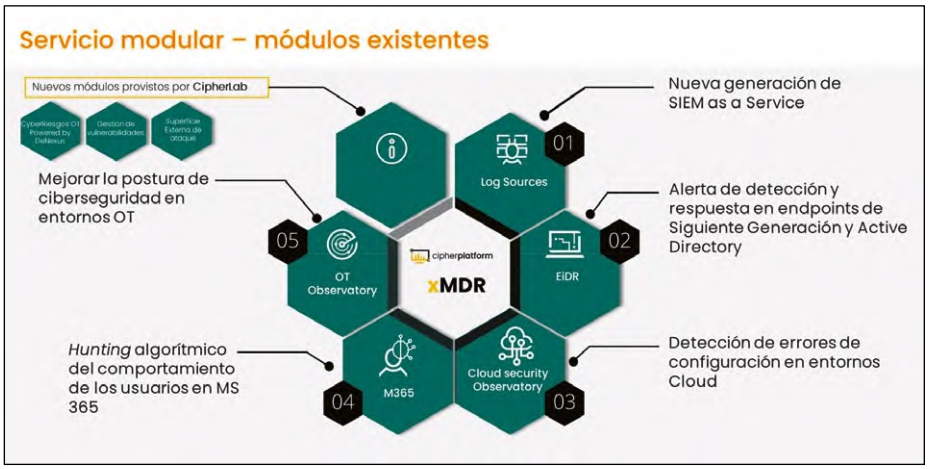
Transformando el modelo de adversario digital en casos de uso

Usamos para los casos de uso estándares como son la taxonomía de D3FEND y la categorización de MITRE. De esta forma se clasifica su relevancia dentro del ciclo de vida de un ataque con los diferentes procesos que se efectúan (tácticas), los procedimientos para su práctica (técnicas) y las acciones ya confirmadas por parte de actores y tecnologías para la explotación de dicho proceso en la cadena de ataque.

Robotizado y asistido

El catálogo de reglas obtenido a partir del **Mapa Digital del Adversario** se construye de forma autónoma. Esto permite extraer una situación de superficie de ataque centrada en los problemas emergentes, el tipo de negocio y las características específicas de los clientes.





Tanto la creación como el muestreo de una regla existente se transfieren de manera robotizada a la función de **inteligencia**, que identificará y extraerá de la base de datos de conocimientos las referencias anteriores en sus atributos, nomenclatura y entidades (Ip, usuario, proceso, etc..). Además, se verificará la presencia de telemetría con escenas específicas para cada una de las fases de un ataque en las que se identifiquen los pasos.

Diferenciación

El modelo operativo compuesto por la CipherPlatform es una característica diferenciadora, ya que se apoya en los procesos de Robotización y Asistencia junto con el proceso de conocimiento de nuestros motores cognitivos, permitiendo a los recursos, analistas y expertos, columna vertebral del servicio, completar sus tareas de forma eficiente y alcanzar los objetivos finales del servicio: **la reducción de falsos positivos, la reducción de alertas inútiles y la mejora de las capacidades de detección, acercándonos a la anticipación de las situaciones maliciosas.**

La información de salida de cualquiera de los procesos mencionados persiste en la **información del portal**, de forma que la agregación de indicadores e información para el analista y el cliente tiene una riqueza y fiabilidad **diferenciadora**, pudiendo identificar la línea de evolución para cada diversificación de ataque complejo. Toda esta información es indispensable, por ejemplo, para poder **evaluar** de forma real la **efectividad** de las medidas de ciberseguridad que nos marca la nueva directiva europea NIS2.

Adaptabilidad y versatilidad para cada cliente

xMDR de Cipher es un servicio que se **integra de una manera rápida y sencilla para centralizar todas las herramientas de detección de incidentes** de seguridad del cliente que ya posea (somos agnósticos a la tecnología). Para los clientes que no tengan una solución SIEM, o no están aprovechando plenamente sus características y quieran cambiarlo, podemos ofrecer un SIEM de primera categoría con automatización y aprendizaje automático, y lo gestionamos desde el servicio xMDR para ofrecer un servicio con todas las funciones.

Beneficios para el cliente

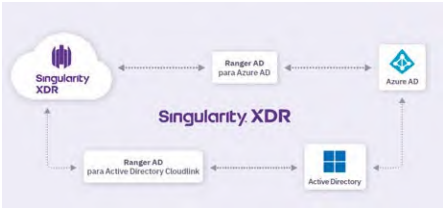
- Servicio de **suscripción** sin costes ocultos.
- Servicio **ilimitado de eventos por segundo.**
- Servicio **ilimitado de Casos de Uso.**
- Casos de Uso específicos en la plataforma para el cliente desde el inicio del Servicio.
- Servicio con posibilidad de crecer en base al crecimiento de la organización de forma sencilla y transparente.
- **Despliegues sencillos**, rápidos y flexibles.
- Colector a la Nube (Colector en la Sede del cliente con la Nube de Cipher).
- **Sin necesidad de comprar licencias** ni pagar por el mantenimiento de licencias que pueden estar mal dimensionadas.
- **Precio fijo sin límite de fuentes de clientes a integrar**. Se definen desde el Modelado Digital.
- **Portal de la plataforma** donde se puede consultar el estado del servicio.
- **Customer Success Manager (CSM) dedicado** y nominal.
- **Alertas e incidencias tratadas por analistas** y no operadores e interacción con el cliente en escalados por parte de los mismos. ■

Diego Alegre Torbado
Manager de Preventa xMDR
CIPHER
Diego.alegre@prosegur.com

SENTINELONE REFUERZA LA PROTECCIÓN DE LA IDENTIDAD CON SINGULARITY IDENTITY, HOLOGRAM, MOBILE Y RANGER AD

Con la intención de ofrecer más seguridad corporativa frente a los ataques o violaciones basados en la identidad que, según **SentinelOne**, han sufrido el 84% de las organizaciones, la compañía amplió recientemente su portafolio de soluciones entre las que destacan: **Singularity Identity, Singularity Hologram, Singularity Ranger AD** y **Singularity Mobile.**

La primera está diseñada para la detección en tiempo real de ejecución de los ciberataques basados en la identidad contra Active Directory y Azure AD, incluidos los de *ransomware*. Para ello, ofrece protección para todos los recursos, ya sean gestionados o no gestionados, y en todos los sistemas operativos, incluidos los dispositivos IoT y TO. Además, posee tecnología de camuflaje para confundir a los ciberdelincuentes y proteger las credenciales de valor, entre otras capacidades



También, destaca su integración con la mencionada Singularity Hologram, la herramienta de engaño de SentinelOne. Ésta emplea una tecnología avanzada para engañar a los atacantes que han accedido a la red y a los autores de amenazas internas, mediante señuelos. Y es que, Hologram imita sistemas operativos, aplicaciones, datos, etc., para desenmascarar al adversario.

Por su parte, Singularity Ranger AD se presenta como una solución de evaluación de la configuración de identidades que identifica errores de configuración, vulnerabilidades y amenazas activas dirigidas también contra Active Directory (AD) y Azure AD. Ranger AD proporciona información práctica del nivel de exposición de la superficie de ataque en cuanto a identidad. Tanto Singularity Identity, Hologram, como Ranger AD forman parte de la plataforma SentinelOne Singularity XDR de protección de los *endpoints*, la nube y las identidades.

Finalmente, Singularity Mobile es una solución MTD (*Mobile Threat Defense*), basada en IA, que proporciona de forma autónoma protección, detección y respuesta para amenazas dirigidas contra dispositivos iOS, Android y ChromeOS, con un enfoque de confianza cero.

SENTINELONE
www.es.sentinelone.com

DELINEA CREA UNA PLATAFORMA CON LA ÚLTIMA VERSIÓN DE SECRET SERVER PARA REUNIR LAS CAPACIDADES DE SUS SOLUCIONES PAM

Bajo el nombre **Plataforma Delinea**, la compañía ofrece una base nativa en la nube para todas sus soluciones PAM reconocidas en el sector, que mejora y refuerza la visibilidad de extremo a extremo, los controles dinámicos de los privilegios y una seguridad que se adapta fácilmente. La plataforma soporta la última versión de **Secret Server**, su solución de bóveda, así como un Servicio de Acceso Remoto seguro sin VPN para proveedores y trabajadores en remoto, y un amplio ecosistema de integraciones a través del *marketplace* de Delinea.

En concreto, proporciona autorización para todas las identidades controlando el acceso a la infraestructura de nube híbrida más crítica de una organización y a los datos sensibles. Con ella, las empresas pueden gestionar de forma centralizada y acceder a las credenciales privilegiadas a través de Secret Server, administrar el acceso remoto seguro sin VPN y la monitorización de sesiones para proveedores y contratistas externos con Remote Access Service. Además, permite integrar las soluciones críticas de IT y seguridad disponibles en el *marketplace* de la compañía, desde la misma interfaz en la nube.

Para Delinea, "el soporte de estas capacidades críticas de PAM en la Plataforma Delinea es el primer paso hacia una madurez de PAM menos compleja". Y es que, a medida que estén disponibles más capacidades en ella, las organizaciones podrán gestionar la autorización de todo tipo de identidades de forma unificada y centralizada. "Se consigue así optimizar la productividad y mejorar la seguridad", explican sus responsables. Además, las futuras mejoras "seguirán permitiendo una seguridad sin fisuras, con controles de acceso basados en el análisis y la automatización de los privilegios, que se pueden adaptar a toda la infraestructura de IT, para garantizar que las identidades tengan el acceso correcto con los permisos aprobados, en el momento oportuno", añaden.

DELINEA
www.delinea.com

CYBERARK OPTIMIZA WORKFORCE PASSWORD MANAGEMENT CON PROTECCIONES AVANZADAS PARA LAS EMPRESAS

CyberArk ha llevado a cabo una serie de mejoras en su solución de gestión de contraseñas empresariales, basada en la nube, **Workforce Password Management**, que permite capturar, almacenar y gestionar de forma segura aplicaciones basadas en contraseñas y otros secretos. Así, las nuevas capacidades brindan a los administradores mayor flexibilidad y control para reducir el riesgo y mejorar la seguridad de las aplicaciones web.

Entre sus novedades se incluyen controles de acceso a aplicaciones basados en nombres de usuario, con los que los administradores pueden evitar que los usuarios finales agreguen cuentas confidenciales y privilegiadas como *root*, *admin* y *dba* al repositorio de Workforce Password Management. Esto proporciona a los administradores un mayor control sobre los tipos de credenciales almacenadas por los usuarios finales y puede reducir el riesgo de que se agreguen, accedan y compartan cuentas con muchos privilegios. Además, ofrece compatibilidad con aplicaciones web habilitadas para CAPTCHA e informes mejorados para aplicaciones agregadas por el usuario, lo que permite a los administradores de Workforce Password Management realizar auditorías periódicas de las aplicaciones agregadas por el usuario y hacer cumplir las pautas de seguridad de TI establecidas.

Además, la solución se puede usar junto con CyberArk Secure Web Sessions para fortalecer aún más el acceso a aplicaciones confidenciales. Además, cabe recordar que Con CyberArk Identity Security Platform las organizaciones pueden habilitar Zero Trust y privilegios mínimos con visibilidad completa.

CYBERARK
www.cyberark.com/es

WATCHGUARD AMPLÍA SU LÍNEA DE CORTAFUEGOS Y SU ARQUITECTURA UNIFIED SECURITY PLATFORM CON THREATSYNC PARA LA DETECCIÓN Y RESPUESTA EXTENDIDAS

WatchGuard ha incorporado a su catálogo de cortafuegos las familias **Firebox T25/T25-W** para pequeñas oficinas, oficinas domésticas y entornos de *retail*, **T45/T45-POE/T45-W-POE** para pymes, y el **T85-POE** para empresas que necesitan mayor rendimiento. Además, ha lanzado **ThreatSync**, como parte de su arquitectura Unified Security Platform, que proporciona tecnología de detección y respuesta extendidas (XDR) para los productos de WatchGuard Network y Endpoint Security.

Los nuevos equipos Firebox incorporan su arquitectura Unified Security Platform para ofrecer una seguridad mejorada y WatchGuard Cloud para simplificar su gestión. Además, cuentan con más memoria y mayor velocidad de procesamiento para mejorar el rendimiento, permitiendo proteger sucursales, equipos de oficina, dispositivos remotos, software punto de venta (TPV) del *retail*, así como usuarios remotos, frente a amenazas complejas y emergentes, con menos requisitos de configuración y gestión de la red.

La compañía, además, completa esta propuesta con servicios de seguridad de clase empresarial como APT Blocker (detección de *malware* en *sandbox*) y ThreatSync para compartir conocimientos entre el *endpoint* y la red, que hacen que "los nuevos Firebox sean óptimos para pequeñas empresas que carecen de un equipo de seguridad designado", destacan desde la compañía.

Cabe destacar también que, la nueva línea Firebox incluye SD-WAN para optimizar el rendimiento de la red mediante la distribución dinámica del tráfico, a través de múltiples conexiones basadas en políticas definidas.

Simplificando la ciberprotección

Por su parte, WatchGuard ThreatSync proporciona capacidades XDR para centralizar las detecciones entre productos y orquestar la respuesta automatizada a las amenazas, desde un único panel de control. Con ello, simplifica la ciberseguridad y, a su vez, mejora la visibilidad y respuesta a las amenazas de forma más rápida, reduciendo el riesgo y el coste, y dando una mayor precisión.

WATCHGUARD
www.watchguard.com/es

CHECK POINT FOCALIZA EN LAS PYMES SU SOLUCIÓN INFINITY SPARK, QUE INTEGRA 5G, WI-FI 6, SD-WAN Y PREVENCIÓN DE AMENAZAS

Con **Infinity Spark, Check Point** pone foco en la protección para las pequeñas y medianas empresas a través de una solución de prevención de amenazas basada en inteligencia artificial creada especialmente para este tipo de compañías.

Con ella, la compañía proporciona seguridad empresarial abarcando tanto la red corporativa, como la nube, *endpoints* y dispositivos móviles, con protección frente a amenazas avanzadas como *phishing*, *ransomware*, robo de credenciales y ataques DNS.

Para ello, el paquete Check Point Infinity Spark se compone de, entre otros recursos, los nuevos *firewalls* de última generación Quantum Spark 1500 Pro para pymes, con protección integrada de inteligencia artificial, 5G, SD-WAN y Wi-Fi 6. Según sus responsables, ofrece "Wi-Fi tres veces más rápido", además de una conexión WAN de alta velocidad de 1 Gbps con 5G y SD-WAN integrada para un mejor rendimiento de las aplicaciones y el máximo tiempo de actividad. En general, los *gateways* Quantum Spark brindan protección para empresas con hasta 1.000 empleados y, para facilitar su gestión, posee un panel de administración unificado.

Infinity Spark también proporciona a los MSPs "un suministro inmediato con licencias de pago por uso e informes de consumo, facilitando a los proveedores la capacidad de ofrecer unas soluciones de seguridad más comprensivas".

Además, integra cuatro consolas en un único panel de control con suministro *zero touch* y servicios de nube escalables, "ahorrándoles a los MSPs tiempo y recursos, reduciendo los costes operacionales de manera significativa", destacan desde la compañía.

CHECK POINT SOFTWARE
www.checkpoint.com

SOPHOS SUMA LOS EQUIPOS 7500 Y 8500 A SU FAMILIA DE FIREWALLS XGS PARA GRANDES EMPRESAS

Con los modelos **XGS 7500** y **8500**, **Sophos** amplía su portafolio de cortafuegos de última generación para grandes empresas, reforzando así la estrategia SASE de la compañía. Estos equipos destacan por incorporar los procesadores de flujo Xstream de alto rendimiento y a las unidades centrales de procesamiento (CPU) con aceleración de alto nivel.

La arquitectura Xstream es el impulsor de las avanzadas capacidades de protección frente a amenazas, rendimiento y visibilidad de estos cortafuegos. Con ella, ofrece protección con inspección detallada de paquetes en un único motor DPI para el control de aplicaciones, antivirus, web, IPS e inspección TLS. Además, su tecnología FastPath de red permite la descarga inteligente y automática basada en políticas del procesamiento del tráfico de confianza a velocidad de cable.

A ello, se le unen otras características técnicas de estos modelos como la capacidad del *firewall* de hasta 190 gigabits por segundo

(Gbps), un rendimiento de hasta 141 Gbps en redes privadas virtuales (VPN) IPsec, compatibilidad con hasta 58 millones de conexiones simultáneas y soporte de hasta 1,7 millones de conexiones nuevas por segundo, entre otras.

Asimismo, los cortafuegos de Sophos se integran en tiempo real con Sophos Central, así como con Intercept X detección y respuesta, y Central Firewall Reporting, para la generación de informes, entre otros recursos de la compañía.

En paralelo, la compañía ha presentado una serie de innovaciones en su oferta de seguridad para *endpoints*. Entre ellas se encuentran una nueva capa de protección adaptativa contra adversarios activos, protección mejorada contra *malware* en Linux, funciones de comprobación del estado de las cuentas y un agente integrado de Zero Trust Nerwork Acces (ZTNA) para dispositivos Windows y macOs,

SOPHOS
www.sophos.com/es-es

QUALYS REFUERZA SU PLATAFORMA TRURISK CON MAYORES CAPACIDADES VMDR, GESTIÓN DE PARCHES Y EDR MULTIVECTOR

Qualys ha ampliado las capacidades de su plataforma TruRisk con nuevas soluciones que combinan las capacidades de gestión integral, detección y respuesta ante vulnerabilidades (VMDR) de la compañía, con la administración de parches y funcionalidades EDR multivector. Se trata de: **VMDR TruRisk, VMDR TruRisk FixIT, VMDR TruRisk ProtectIT** y **Enterprise TruRisk Management**, que están orientados a reducir los riesgos cibernéticos de las pequeñas y medianas empresas.

Por un lado, VMDR TruRisk aúna las capacidades de Qualys Cloud Platform y de VMDR proporcionando visibilidad de activos, gestión de vulnerabilidades, evaluación de riesgos y prioridad en la remediación de flujos de trabajo. Por otro, VMDR TruRisk FixIT ofrece todos

los beneficios de VMDR TruRisk, así como de Qualys Patch Management para una detección y remediación basadas en riesgos. Así, con esta solución, los clientes pueden priorizar las vulnerabilidades y automatizar la aplicación de parches según su criticidad.

A ello se suma VMDR TruRisk ProtectIT que ofrece los beneficios de FixIT más una protección adicional contra amenazas y anti*malware* basada en un contexto de negocio y multivector de todos los puntos finales para bloquear tanto software malicioso, como *ransomware*.

Visión unificada de los riesgos

Qualys ha presentado, asimismo, Enterprise TruRisk Management (ETM) para proporcionar una visión unificada de los riesgos. ETM permite a los clientes llevar al ecosistema de Qualys hallazgos de seguridad y vulnerabilidad externos, de herramientas de terceros. Con este enfoque la compañía busca comunicar y administrar el riesgo de manera más efectiva, además de integrar seguridad y operaciones de TI (ITOps) para minimizarlo con mayor rapidez.

QUALYS
www.qualys.com

HORNETSECURITY PRESENTA QR CODE ANALYZER Y SECURE LINKS PARA MITIGAR LAS AMENAZAS EN LOS CÓDIGOS QR Y EL *RANSOMWARE*

Para mitigar los riesgos que suponen el aumento de los cibertaques a través de códigos QR falsos y los constantes incidentes de *phishing* -representan un 40% de todas las amenazas cibernéticas-, **Hornetsecurity** ha desarrollado dos herramientas especializadas: **QR Code Analyzer** y **Secure Links.**

Con la primera de ellas, la compañía amplia las capacidades de su Advanced Threat Protection y su *suite* 365 Total Protection para Microsoft 365 ayudando, con dicha tecnología, a determinar si los códigos QR acceden a sitios maliciosos cuando son escaneados. A ello, se suma el lanzamiento de la funcionalidad Secure Links que trata de limitar los ataques cibernéticos, especialmente los de *ransomware*. Para ello, "este nuevo servicio revisa todos los enlaces de un mensaje y los analiza antes de permitir al destinatario abrirlo", explican sus responsables.

Migración de buzones segura y eficiente

Hornetsecurity ha desarrollado también una solución, **Mailbox Migration Tool**, de migración automatizada de buzones de correo-e, que ayuda a los *partners* a implementar y a operar Microsoft 365 en la nube, de forma más eficiente y segura. Con ella la compañía busca dar respuesta a los desafíos de seguridad que surgen a la hora de transferir buzones de correo-e de las instalaciones locales a la nube de Microsoft 365, complementando las capacidades de su herramienta 365 Total Protection. Además ha presentado su **VM Backup V9**, la última versión de su solución de copias de seguridad.

HORNETSECURITY
www.hornetsecurity.com/es

COUNTERCRAFT AÑADE A 'THE PLATFORM V3' MÁS DE 170 FUNCIONES Y ÁRBOLES DE ATAQUE PARA UNA DEFENSA ACTIVA

CounterCraft ha llevado a cabo una importante actualización de una de las principales herramientas de técnicas de engaño (más conocido por su término en inglés, *deception*), para implementar una defensa activa, añadiendo a la **Versión 3** de su **The Platform** más de 170 funciones y árboles de ataque.

Con este lanzamiento, la compañía consigue que la implementación de engaños sea más intuitiva y centrada en el usuario. Con ella, es posible "diseñar campañas de última generación que desvíen ataques y recopilen información de amenazas contextualizada en minutos, simplemente arrastrando y soltando elementos", explican sus responsables.

Así, entre las nuevas características se incluyen un despliegue más rápido e intuitivo de las campañas de engaño, análisis de amenazas más eficiente, así como un realismo más eficaz que mejora los resultados de la campaña. A ello, se le unen, entre otras muchas, mayor automatización en el filtrado de eventos y análisis incorporado, más rendimiento y los árboles de ataque.

Con estos últimos, "los equipos de seguridad pueden esbozar y diseñar campañas de engaño arrastrando y soltando *hosts*, servicios y *breadcrumbs*, y luego implementarlas con un solo clic", comentan desde la compañía. Además, permite conocer, de un vistazo, la ruta del ataque 'engañoso', los componentes y el estado operativo; un desglose de la actividad del adversario por evento, *host*, servicio o la ruta de navegación con el acceso, con un solo clic, y una vista detallada del explorador de datos prefiltrado. También permite acceder, de forma sencilla, desde un solo panel, a las notificaciones, a otras campañas de engaño y al resto de menús de configuración.

COUNTERCRAFT
www.countercraftsec.com

FORTINET AVANZA EN SU TECNOLOGÍA ASIC PARA LA CONVERGENCIA Y SEGURIDAD DE RED Y AMPLÍA SUS SERVICIOS PARA SOCs

Fortinet lleva más de dos décadas invirtiendo e innovando en la tecnología ASIC para acelerar e incrementar la seguridad y las capacidades de red de los entornos distribuidos. Fruto de ese esfuerzo, ha presentado el chip **FortiSP5** que representa su último avance en este campo. Además, la compañía ha ampliado su oferta de servicios y de formación para apoyar a los equipos SOC en la prevención y defensa frente a las ciberamenazas.

El chip FortiSP5 tiene la capacidad para acelerar y ejecutar simultáneamente el doble de aplicaciones –por ejemplo, cortafuegos de nueva generación (NGFW), acceso a la red de confianza cero (ZTNA) y SD-WAN– en comparación con la generación anterior. También, posee cifrado Ci más veloz para proteger datos sensibles y asegurar redes privadas virtuales.

A ello, se le unen 2,5 Gbps de inspección SSL profunda, arranque seguro para permitir que sólo se inicie el software de sistema operativo aprobado y validado, protección DDoS volumétrica, encapsulación acelerada por hardware VXLAN/GRE para la interconectividad segura de redes distribuidas y calidad de Servicio (QoS) acelerada por hardware para aplicaciones sensibles como sistemas de videoconferencia.

Respuesta a la escasez de personal

En paralelo, ha puesto en marcha nuevos y mejorados servicios para proporcionar apoyo a los equipos de los (SOC) con déficit de personal. Entre ellos, se incluyen la ampliación de su oferta **SOC-as-a-Service** y el nuevo **Outbreak Detection Service**, de detección de focos y 'brotes' de ataques que alerta sobre los principales incidentes, de última hora, que podrían tener un impacto notable. También ha añadido **servicios de Respuesta y Preparación ante Incidentes** (IR&R) en los que ha cambiado el modelo de adquisición para priorizar la prevención.

La compañía también ha presentado **FortiCNP**, una solución de protección nativa en la nube, creada para simplificar la protección *cloud* y gestionar de forma proactiva sus riesgos. Asimismo, ha introducido mejoras en **FortiSASE**, para ofrecer una mayor flexibilidad y nuevas capacidades de acceso seguro para los recursos digitales a través de aplicaciones privadas, SaaS e Internet.

Asimismo, y con el objetivo de avanzar hacia su compromiso de formar a un millón de personas en ciberseguridad para 2026, la compañía, a través de su Instituto de Formación, está creando programas dirigidos a aumentar el acceso a la formación y a certificaciones reconocidas para los profesionales de TI y seguridad de todo el mundo. Por ejemplo, haciendo que el examen práctico para el nivel 8 de NSE sea más accesible. También, anunció que ya se ha completado el programa de la primera promoción de mujeres del *bootcamp* de Fortinet y Mujeres en Ciberseguridad (WiCyS).

FORTINET
www.fortinet.com

STORMSHIELD PONE EN MARCHA UNA NUEVA OFERTA DE FORMACIONES DE E-LEARNING EN ASOCIACIÓN CON SEELA

Stormshield ha extendido su colaboración con la plataforma de *e-learning* sobre ciberseguridad, **Seela**, añadiendo su **CyberTraining** a su catálogo de formaciones **CSNA** (Certified Stormshield Network Administrator) y **CSNE** (Certified Stormshield Network Expert).

Estos cursos tienen como objetivo apoyar la evolución de las competencias de ingenieros, técnicos y otros perfiles tecnológicos, a través de un alto nivel técnico y libertad de aprendizaje, pudiéndose organizar en función de su carga de trabajo y del tiempo asignado a la formación.

En total, se componen de más de 700 horas de clases teóricas, acompañadas de ejercicios prácticos. La aplicación práctica de estos cursos de formación tiene lugar a través de la plataforma de simulación de formación en el mundo real CyberRange de la empresa matriz de Stormshield, **Airbus**, que ya se utiliza para las formaciones de clientes y socios, facilitando la integración de los contenidos.

De momento, Stormshield ha puesto a disponibilidad de los interesados seis programas personalizados: **Ethical Hacker, DevSecOps, Information Systems Security Manager** (ISSM), **SOC Analyst Operator**, así como los programas de **Administrador de Soluciones de Seguridad** y el de **Coordinador de Seguridad**.

Asimismo, la asociación con Seela se inscribe en el marco de la Academia Stormshield, que aporta formación y apoyo a los profesores en profesiones y temas relacionados con la ciberseguridad. De este modo, también ofrece ahora todos sus cursos de formación CyberTraining a los profesores de las instituciones asociadas.

STORMSHIELD
www.stormshield.com

ESET PONE A DISPOSICIÓN DE LOS CLIENTES INFORMES PRIVADOS SOBRE TÉCNICAS Y VECTORES DE ATAQUE

Como parte de su catálogo de servicios, **Eset** ha puesto a disposición de sus clientes la posibilidad de acceder a informes privados con información más exhaustiva y práctica recogida por sus reconocidos equipos de investigación sobre vectores de ataque y técnicas específicas usadas por ciberdelincuentes.

En concreto, la nueva oferta incluye, **Informes sobre Amenazas Persistentes Avanzadas (APT), donde se** comparten las investigaciones en curso de Eset sobre APTs, incluyendo resúmenes de su actividad. El paquete APT Reports Premium proporciona a los clientes acceso a un analista de la firma eslovaca durante un máximo de cuatro horas al mes.

A ellos, se les unen los *feeds* de *Eset Threat Intelligence,* que ofrecen a los clientes una visión en tiempo real del panorama mundial de amenazas basada en *feeds* de sus centros de investigación, para permitir a los equipos de seguridad actuar con mayor rapidez ante IoCs en su entorno. Los *feeds* disponibles (en formato JSON o STIX 2.0) incluyen archivos y dominios maliciosos, *botnets*, IPs y URLs maliciosas e información sobre APTs (incluida en la oferta de informes APT).

Estos nuevos servicios de inteligencia sobre amenazas de la compañía, disponibles comercialmente, amplían las investigaciones que se publican en su *blog* WeLiveSecurity, una importante fuente de información de primer nivel, y sus informes trianuales sobre amenazas y APTs.

ESET
www.eset.com/es

KASPERSKY AVANZA EN SU ESTRATEGIA CYBER IMMUNITY CON NOVEDADES PARA LA PROTECCIÓN DEL IIOT Y DEL TRABAJO EN REMOTO

Kaspersky aprovechó el Mobile World Congress de Barcelona para presentar sus más recientes novedades como parte de **Cyber Immunity**, su modelo de desarrollo de sistemas con seguridad por diseño, con productos que incluyen protección "inherente", es decir, "capacidad para resistir ciberataques sin necesidad de herramientas de seguridad adicionales", explican sus responsables.

Los productos que la compañía ofrece, en la actualidad, bajo el paraguas de la 'ciber inmunidad', se caracterizan por estar basados en su sistema operativo KasperskyOS, diseñado para aumentar la seguridad del Internet de las Cosas Industrial, y que poseen, por ejemplo, sus **IoT Secure Gateways, KISG 100** (para aplicaciones industriales) y **KISG 1000** (para ciudades inteligentes, videovigilancia, infraestructuras ferroviarias, etc). Estos dispositivos permiten, entre otras capacidades, la recopilación y transferencia directa y protegida de datos telemétricos de equipos (como cámaras de videovigilancia, etc.) a la nube y a plataformas empresariales digitales.

Otros de las novedades desarrolladas con KasperskyOS, en esta ocasión como corazón para la construcción y protección de la infraestructura del espacio de trabajo remoto, ha sido **Kaspersky Thin Client**, el elemento central de Kaspersky Secure Remote Workspace. Este cliente tiene las características "tradicionales" de un PC para manejar archivos y documentos, puerto USB, reenvío y soporte de los medios de almacenamiento más comunes, a las que se le suman funciones como la conexión segura a sistemas de virtualización y el control de acceso.

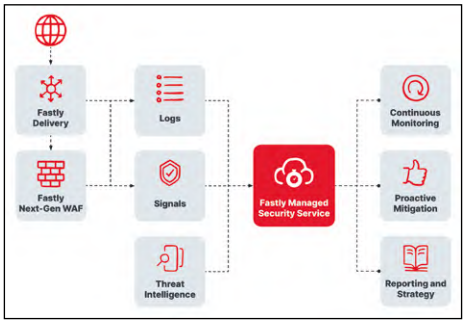
Junto a ello, Kaspersky también continúa trabajando en las soluciones de automoción como **Kaspersky Automotive Adaptive Platform**, un avanzado kit de desarrollo de software especializado (SDK) que permite crear soluciones seguras para diversas unidades de control electrónico en coches inteligentes.

Asimismo, la compañía destacó la investigación y desarrollo de activos que está llevando a cabo para la implementación de KasperskyOS en dispositivos móviles profesionales, mediante la ejecución del concepto de Cyber Immunity.

KASPERSKY
www.kaspersky.es

VISIBILIDAD Y PERSONAL EXPERTO PARA IDENTIFICAR Y MITIGAR AMENAZAS A APLICACIONES WEB, MISIÓN DE FASTLY MANAGED SECURITY SERVICE

Fastly ha creado un servicio de detección y respuesta de amenazas 24/7 para ayudar a reducir el riesgo de ataques a aplicaciones web y el impacto en costes como consecuencia de transacciones perdidas. Con ello, quiere dar respuesta al desafío de las empresas para hacer frente a los ataques a las aplicaciones web que, según el DBIR 2022 de Verizon, son el vector número uno y pueden estar relacionados con el elevado número de ataques de denegación de servicio. "Este binomio, junto con el creciente uso de credenciales robadas (normalmente dirigidas a algún tipo de aplicación web) es coherente con lo que hemos visto en los últimos años. Los equipos de seguridad existentes están muy dispersos y no siempre tienen la experiencia o el tiempo para supervisar y detectar continuamente este tipo de amenazas", explican desde la compañía.



Así pues, **Fastly Managed Security Service** amplía la protección a los clientes de su solución Fastly Next-Gen WAF, proporcionando monitorización continua y mitigación proactiva de ataques a aplicaciones web, "respaldado por un acuerdo de nivel de servicio (SLA) de tiempo de respuesta de 15 minutos para incidentes de seguridad críticos", destacan sus responsables, a la vez que recuerdan que lo combinan todo con informes consistentes posteriores a los incidentes y consultas de seguridad estratégicas periódicas para aportar el máximo nivel de protección de las aplicaciones y reforzar así la estrategia de seguridad global de una organización.

Atendido las 24 horas del día, los siete días de la semana, por el Centro de Operaciones de Seguridad del Cliente (CSOC) global de Fastly, este servicio permite a los equipos internos, en definitiva, mejorar su estructura general de seguridad y centrarse en sus competencias clave.

FASTLY
www.fastly.com/es

ATOS PRESENTA 5GUARD PARA PROTEGER A LOS OPERADORES Y A LAS ORGANIZACIONES QUE DESPLIEGUEN REDES 5G PRIVADAS

Atos ha anunciado una nueva propuesta para aquellas organizaciones que quieran desplegar redes 5G privadas y para los operadores de telecomunicaciones que apuesten por habilitar una seguridad integrada, automatizada y orquestada para proteger y defender sus activos y clientes.

Se trata de **5Guard**, desarrollada para ayudar a las organizaciones a identificar los riesgos y desarrollar una estrategia de seguridad *end-to-end*. Así, 5Guard minimiza los riesgos a través de la red de acceso de radio (RAN), *edge computing* de acceso múltiple (MEC), el *core* 5G y las plataformas multi-nube.

En concreto, la propuesta de la compañía permite, por un lado, contar con el apoyo de su consultoría en la definición de su estrategia de seguridad 5G. Y, por otro, ofrece sus soluciones de protección, entre las que se encuentran desde sus herramientas de cifrado de Atos (Trustway), hasta su *software* de gestión de identidades y accesos, sus soluciones de infraestructura de clave pública (IDnomic) y la plataforma Atos Managed Detection and Response (MDR), que mejora la seguridad de los elementos de red 5G, las aplicaciones y las cargas de trabajo, detectando y respondiendo a las amenazas potenciales casi en tiempo real. También, permite acceder a las soluciones de sus *partners* como la propuesta de ciberprotección de 5G de Fortinet.

Por último, 5Guard incluye la operación de la ciberseguridad en este entorno, basada en los servicios de seguridad gestionados de Atos, para la detección y respuesta multi-nube, y la protección de la red 5G.

ATOS
https://atos.net/en

S21SEC

CYBERSECURITY YOU CAN TRUST

Ransomware

82%

Crecimiento de ataques de ransomware entre 2020 y 2021.

5%

La cantidad pedida como **rescate** supone entre el **0,7% y el 5%** de los ingresos anuales de la víctima.

15%

El coste del rescate es solo el **15% del total**, afectando a pérdidas en el negocio, costes recuperación, daño reputacional, etc.

El 73% de los extorsionados que pagan, vuelven a ser atacados. **¡Pagar no es la mejor alternativa!**

Hay que focalizarse en **prevenir**, **proteger** y **detectar** lo antes posible, sin descuidar la necesidad de estar preparado para dar **respuesta rápida y eficiente**.

Desde S21Sec cubrimos todo el espectro de soluciones y servicios dirigidos a proteger, defender y ayudar en la respuesta a los clientes, entre ellos:

- Análisis de la arquitectura del cliente frente a un ataque con Ransomware.
- Diseño, implementación y gestión de arquitecturas de protección y respuesta.
- Implementación y gestión de plataformas de protección del dato.
- Servicios de protección y respuesta desde el endpoint (MEDR).
- Servicios de respuesta ante incidentes críticos (DFIR)

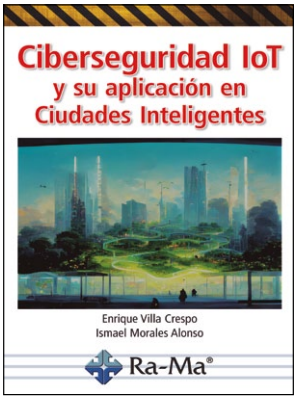
Solicita una llamada con un experto de S21sec

¡Desde S21sec queremos que cuentes con nosotros desde ya para realizar un plan de contención de ciberataques!

(+34) 916 616 679

www.s21sec.com/es/ransomware/

CIBERSEGURIDAD IOT Y SU APLICACIÓN EN CIUDADES INTELIGENTES



Autores: Enrique Villa e Ismael Morales
Editorial: RA-MA Editorial
Año: 2022 – 290 páginas
ISBN: 978-84-19444-73-8
www.ra-ma.es

El Internet de las Cosas (IoT) está directamente relacionado con todos los ámbitos y, sin duda, uno en el que mayores repercusiones tendrá son las ciudades 'inteligentes' y su gestión, las denominadas *smart cities*. Sin embargo, la apuesta por la gestión digital de las grandes urbes, con los beneficios que aporta, también supone un reto en el ámbito de la ciberseguridad y la privacidad digital.

Para ofrecer visibilidad a lo que se está acometiendo, así como las necesidades en ciberprotección que plantea este paso, los dos autores, reconocidos expertos en la materia, ofrecen a lo largo de los cinco capítulos de esta obra una completa introducción a las tecnologías IoT, su evolución en todo tipo de sectores, como el industrial y el de salud, además de información detallada sobre qué necesidades surgirán de las ciudades inteligentes en el ámbito de la ciberseguridad IoT.

Además, en su cuarto capítulo proponen un *framework* de ciberseguridad *para smart cities*, con una guía de implementación, dedicando la última parte del libro a la posible evolución del IoT en las ciudades inteligentes y qué se precisa para llevarla a cabo de forma segura.

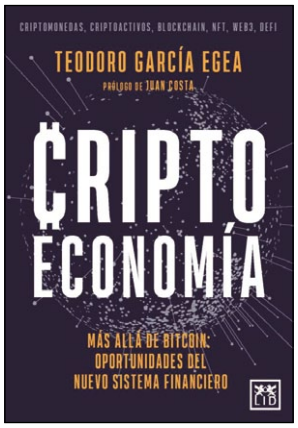
DE LA CAVERNA AL METAVERSO: UN RELATO DISRUPTIVO DE LA TECNOLOGÍA

Autor: Felipe Colorado
Editorial: 0xword
Año: 2023 – 266 páginas
ISBN: 978-84-09-45152-4
https://0xword.com/

Singular aportación, por cuanto hay poco publicado, con rigor y profundidad sobre el tan nombrado y polémico metaverso, en el que **Felipe Colorado** presenta cómo se ha evolucionado "desde el sílex al silicio", hasta llegar al cibermundo que vivimos. "Desde que el hombre tomó una piedra en su mano, supo que podría transformar el mundo. Tecnología para la guerra, la represión y el delito. También, para la difusión universal del conocimiento, la mejora de la calidad de vida y la lucha contra enfermedades y pandemias", destaca Colorado.

A través de una fusión de arqueología, narrativa y ficción, también con humor, el autor transporta al lector a un viaje por nuestra historia, con amplia presencia de la seguridad de la información y de muchos de sus hitos, partiendo de 1834 y mostrando la actividad de los hacktivistas, además de recordar qué riesgos plantean "los bajos fondos de una Web 2.0, pronta a dar el relevo a su sucesora y al naciente Metaverso". Por supuesto, no faltan reflexiones sobre la ética de muchos de los aspectos digitales que nos rodean. Para facilitar la profundización del lector en este ámbito, la obra viene acompañada de un PDF descargable con más de 150 referencias 'webgráficas' y 23 imágenes exclusivas.

CRIPTOECONOMÍA. MÁS ALLÁ DEL BITCOIN: OPORTUNIDADES PARA EL SISTEMA FINANCIERO

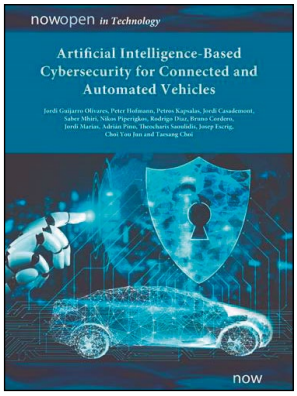


Autor: Teodoro García Egea
Editorial: LID Editorial
Año: 2023 – 208 páginas
ISBN: 9788417277499
www.lideditorial.com

"*Tokenización* de activos, préstamos seguros entre particulares, contratos inteligentes que se ejecutan automáticamente, financiación de proyectos sostenibles... Aunque en la mente de muchas personas la criptoeconomía equivale tan solo a invertir en bitcoins, el intercambio de valor a través de la red ya ha puesto en marcha un nuevo sistema económico que está cambiando el mundo", destaca el autor de este libro, conocido por su etapa política como secretario general del Partido Popular de 2018 a 2022, **Teodoro García Egea**.

Apasionado por la ciberseguridad y las nuevas tecnologías, Egea, en su retorno a estos ámbitos, está centrando su actual trabajo en el entorno de las criptomonedas y fruto de ello es este ensayo presentado en marzo pasado en el que repasa y profundiza en las consecuencias de lo que denomina la criptoeconomía. Un concepto que considera que "va a generar una disrupción similar a la que generó la llegada de internet", transformando por completo muchos de los sectores que conocemos. Se trata sin duda de un libro divulgativo para expertos y no expertos que permite conocer, de forma sencilla y amena, qué son tecnologías como el *blockchain* y qué impacto económico están teniendo en todo tipo de entornos.

ARTIFICIAL INTELLIGENCE BASED CIBERSECURITY FOR CONNECTED AND AUTOMATED VEHICLES



Autores: Jordi Guijarro, Peter Hofmann, Petros Kapsalas, Jordi Casademont, Nikos Piperigkos, Rodrigo Díaz, Bruno Cordero, Jordi Marías, Adrián Pino, Theocharis Saoulidis, Josep Escrig, Choi You Jun, Taesang Choi
Editorial: Now publishers Inc
Año: 2022 – 166 páginas
ISBN: 978-1-63828-061-3
https://nowpublishers.com

Los vehículos conectados ya son una realidad en las carreteras y, en pocos años, también llegarán los coches autónomos. Por ello, los efectos de los ataques cibernéticos sobre ellos pueden ser tremendos, incluyendo los daños físicos a ocupantes y peatones. Para anticiparse a estos riesgos, entre otras iniciativas, la UE está financiación el proyecto Caramel (Ciberseguridad basada en inteligencia artificial para vehículos conectados y automatizados), que ha desarrollado varias soluciones antipiratería para la nueva generación de vehículos.

Cofinanciado por la UE, en el marco del programa Horizonte 2020, este consorcio cuenta con 15 organizaciones de ocho países europeos junto con tres socios coreanos. Su reto es aplicar un enfoque proactivo basado en técnicas de Inteligencia Artificial y Aprendizaje Automático para detectar y prevenir posibles amenazas de ciberseguridad para vehículos autónomos y conectados.

Este enfoque se ha abordado en base a cuatro pilares: Movilidad Autónoma, Movilidad Conectada, Electromovilidad y Vehículo a Control Remoto. Este libro presenta la teoría y los resultados de cada una de estas direcciones técnicas.

SPACE ROGUE: HOW THE HACKERS KNOWN AS L0PHT CHANGED THE WORLD

Autor: Cris Thomas
Editorial: Independiente
Año: 2023 – 362 páginas
ISBN: 979-8987032411
www.barnesandnoble.com

Interesante relato sobre uno de los grupos hackers más conocidos de EE.UU., en los años 90. En mayo de 1998, el Congreso invitó a los siete miembros del denominado 'L0pht' a testificar sobre el estado de la seguridad informática del gobierno. Dos años más tarde, sus integrantes se profesionalizaron fundando la consultoría de seguridad @stake. "En el camino, se enfrentaron a gigantes tecnológicos como Microsoft, Oracle, Novell y otros para exponer las debilidades de los principales productos de esas empresas", recuerda su autor que también destaca que "a pesar de la destreza técnica de L0pht, el grupo no pudo mantener lo que habían construido juntos cuando el dinero y la política interna se volvieron amigos contra amigos".

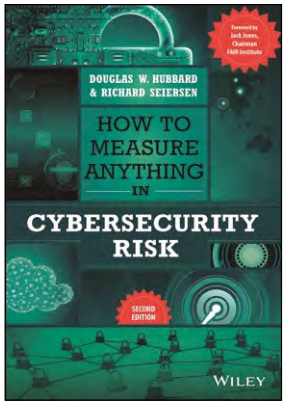
Se trata en definitiva de un excelente relato sobre la historia de la ciberseguridad, la influencia hacker y sus aportaciones a la industria, llevando al lector a través de un apasionante viaje en el que el talento, las habilidades técnicas y, también, el afán de destacar permite disfrutar de lo que fueron los orígenes de los investigadores de ciberseguridad. "El colectivo de hackers L0pht ya no existe, pero su legado sigue vivo", subraya su autor a la que vez recuerda que L0pht estableció el estándar sobre cómo la industria de la seguridad cibernética publica ahora información sobre vulnerabilidades.

CLAVES DE INTELIGENCIA ARTIFICIAL Y DERECHO

Autor: Pablo García Mexía
Editorial: La Ley
Año: 2022 – 184 páginas
ISBN: 978-8419032850
https://tienda.wolterskluwer.es

La inteligencia artificial (IA) constituye uno de los avances tecnológicos clave para la humanidad como también que representa uno de los retos más críticos desde el punto de vista social, ético y jurídico. "Tal contraste confiere a este libro su más profunda razón de ser. Si las sociedades son al menos significativamente escépticas sobre el impacto de la IA, parece más que justificado que aquellos de sus componentes que puedan suponer más riesgos sociales encuentren un contrapeso ético y, en lo que aquí más interesa, desde el Derecho", destaca, tan preclaro como en él es habituaL, el autor, que "explora las causas y consecuencias de todo y contribuye a enriquecer el debate sobre los aspectos jurídicos de las tecnologías de IA". Una obra pionera en la materia en España que ha sido escrita con un enfoque abierto, por cuanto, aunque se centra en los aspectos jurídicos, no prescinde de los tecnológicos.

Así, en ella el lector podrán encontrar un punto de partida para tener una buena visión de los retos que la IA plantea al Derecho, además de contar con información especializada de cómo se está acometiendo su regulación en Europa y España, tanto para los que tienen que trabajar con ella en su día a día como para los que piensen comenzar a aprovechar sus capacidades.



HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK

Autores: Douglas W. Hubbard y Richard Seiersen
Editorial: Wiley
Año: 2023 – 368 páginas
ISBN: 978-1119892304
www.wiley.com

Segunda edición, revisada y actualizada de esta obra de referencia, a cargo de uno de los pioneros de la ciberseguridad y un reconocido analista, ofreciendo un texto revelador permite sacar partido "del lenguaje cuantitativo del análisis de riesgos a la ciberseguridad", destacan sus autores. Así, en este libro el público profesional encontrará una aproximación rigurosa y en detalle de cómo cuantificar la incertidumbre en este ámbito en entornos corporativos, con numerosas referencias a cómo medir objetivos aparentemente intangibles.

En definitiva, se trata de una "una hoja de ruta imprescindible" con la que los ya consolidados profesionales en este tema mejorarán sus conocimiento y los que se aproximen a este tema podrán dar una gran pasos a través de los abundantes consejos detallados de **Hubbar** y **Seiersen** para mejorar la evaluación de riesgos con un marco directo y simple para una variedad de casos de uso entre los que están desde cómo acometer una auditoría rápida de riesgos, para una primera evaluación cuantitativa, hasta cómo medir el impacto real del daño a la reputación, acompañado de nuevos ejemplos bayesianos para evaluar el riesgo con pocos datos, además de diferentes materiales sobre medición y recomendaciones de e cómo combinar la opinión de expertos.

CYBER SECURITY IN MERGERS & ACQUISITIONS: THE INDUSTRY HANDBOOK

Autor: Rajinder Tumber
Editorial: CRC Pres
Año: 2022 – 252 páginas
ISBN: 978-0367676780
www.routledge.com

Esta novedad bibliográfica se torna, por lo poco tratado de su tema, en una lectura más que recomendable para cualquier profesional de ciberseguridad. Su autor que, reconocido por la Cámara de los Lores, en Reino Unido, aborda con profundidad, aunque con una prosa de fácil lectura, el reto de cómo evaluar la madurez cibernética de una organización durante la fase previa a la negociación de su adquisición. "Una violación de datos imprevista durante una fusión o adquisición podría resultar en la eliminación de cientos de millones de euros", recuerda Tumber poniendo como ejemplo la rebaja de 317 millones de euros que tuvo que realizar Yahoo a Verizon, en 2016, por una brecha que comprometió más de 1.000 millones de cuentas de correo-e.

Se trata, pues, de un libro, pensado sobre todo para los que trabajan en inversiones y fusiones o compras de compañías en este sector, pero también para los que quieran tener una visión clara de qué aspectos aportan más valor en este tipo de operaciones y cómo apostando por las mejores prácticas de seguridad se puede contar con ella como multiplicador del valor de cualquier compañía. Además, proporciona el marco 'CyberDD6' para llevar a cabo este tipo de operaciones.

El 13 y 14 de junio, en formato híbrido, en Madrid

Espacio TiSEC regresa con dos jornadas para analizar los retos de las pólizas cibernéticas frente al *ransomware* y las cada vez más complejas amenazas

Bajo el título '**Ransomware, seguros cibernéticos y otras incógnitas: Ciberseguridad endeble y ciberpólizas**', **Espacio tiSec**, organizado por **Revista SIC**, celebrará una nueva edición el 13 y 14 de junio, en el Hotel Novotel, en Madrid, en formato híbrido.

Durante dos jornadas, expertos del sector mediador y asegurador, CISOs, clientes, grandes corporaciones, agentes públicos frente a la criminalidad informática y FSE, así como proveedores de tecnologías y servicios de ciberprotección referentes en el mercado, analizarán con rigor y foco expreso todos los asuntos nucleares que vertebran el ecosistema digital de la sociedad cibernética, tan vapuleado y desestabilizado en estos recientes años por las agresivas prácticas delictivas de la ciberdelincuencia, creciemente organizada.

A esta quiebra en la confianza digital no están ajenas las denominadas pólizas cibernéticas, cuya eficacia a la hora de transferir riesgos está hoy en cuestión y conmina a sus principales oferentes a conformar nuevas propuestas que hagan posible su viabilidad y, al tiempo, satisfagan las necesidades de los asegurados.

Así pues, este evento de SIC, con varias y exitosas ediciones a sus espaldas centrado en la materia, volverá a convocar a los principales referentes para seguir arrojando luz ante fenómenos inquietantes como el que se plantea a raíz del incremento de precios y la reducción de coberturas por parte de las aseguradoras, la polémica del pago –con mayor transparencia y/o realismo en asumirlo– de las extorsiones, y las iniciativas locales, europeas y mundiales por entender, legislar y poner orden en este desbarajuste.

Programa e inscripciones en: **revistasic.es/espacio-tisec/propuesta-ransomware-mayo2023**

Del 19 al 21 de abril en formato presencial y en línea

Los referentes de ciberseguridad pública en España llevan su enfoque y propuesta a las 'III Jornadas STIC Capítulo República Dominicana' para dar visibilidad al sector en Iberoamérica

Las III Jornadas STIC Capítulo República Dominicana, que se celebrarán bajo el lema **'Un ciberescudo único para Iberoamérica: el intercambio es la clave'**, se llevarán a cabo del 19 al 21 de abril. Constarán de tres módulos que coordinarán cada uno de los actores involucrados en la organización del evento, para exponer desde un punto de vista internacional todos los retos y desafíos que la ciberseguridad plantea en estos momentos.

Organizadas por el **Centro Criptológico Nacional** (CCN), el **Instituto Nacional de Ciberseguridad** (Incibe), el **Mando Conjunto del Ciberespacio** (MCCE) de España y el **Departamento Nacional de Investigaciones (DNI)** de República Dominicana, con el apoyo institucional de la **Organización de los Estados Americanos** (OEA) y el **Banco Interamericano de Desarrollo** (BID), reunirán a los principales actores de esta materia en Iberoamérica. Además, contarán con el apoyo de seis organismos del país: el Centro Nacional de Ciberseguridad, la Procuraduría General de la República y el Banco Central y el Ministerio de Defensa, entre otros.

Ciberprotección con 'ñ'

El evento, que se podrá seguir de manera presencial y en línea, incluirá las ponencias de referentes en España e Iberoamérica, como **Omar Avilez**, del CSIRT del país, el polifacético **Francisco Martínez López**, que hablará sobre cómo investigar incidentes de ciberseguridad utilizando técnicas de cacería de amenazas basadas en inteligencia, expertos del CCN quienes darán a conocer su experiencia para crear un SOC gubernamental, y **Adolfo Arreola** de la **Universidad Anáhuac México.** También, contará con paneles de debate como el protagonizado por **Juan Ramón Anria**, de **AIG Panamá**, **Leonardo Ferreira,** del **Ministerio de Gestión e Innovación de Brasil** y **Mauricio Papaleo,** del **AGESIC de Uruguay,** sobre proyectos de implementación de Planes de Ciberseguridad a nivel país, además de ponencias de uno de los expertos del **FBI** sobre ciberterrorismo, deu exCISO de BBVA, **Santiago Moral**. Asimismo, entre otros especialistas de interés **Carlos Seisdedos** y **Vicente Aguilera,** de **Internet Security Auditors,** impartirán un taller sobre cibervigilancia y OSINT, y **Álvaro García** y **Pablo Navarro,** de **Chainalysis** otro sobre Técnicas de investigación y rastreo de criptoactivos. Programa e inscripciones: www.ccn-cert.cni.es

El 19 y 20 de abril en Leganés (Madrid)

El CCI celebra su décimo aniversario con un congreso que repasará sus grandes éxitos y retos, de la mano de los expertos en este ámbito

El **Centro de Ciberseguridad Industrial** (CCI) celebrará sus 10 años de vida con su encuentro 'La voz de la industria', los días 19 y 20 de abril, en Madrid, en formato presencial y virtual. Bajo el título 'Una década de experiencias en Ciberseguridad industrial', las jornadas, que tendrán lugar en la Finca Solimpar, en Leganés (Madrid), constan de un programa con algunos de los actores más relevantes del sector en este ámbito que, además, han participado de forma activa en esta década en los eventos del CCI. "Serán dos días para reunir mucho talento, compartir experiencias con viejos y nuevos amigos de la ciberseguridad industrial y reflexionar sobre el presente y el futuro de la ciberprotección en la digitalización industrial", destacan desde la asociación.

Así, se repasará, en un panel de expertos, la evolución de la ciberseguridad en el ámbito OT en los últimos años, poniendo en valor las experiencias de compañías referentes en este ámbito, como **Rockwell Automation, S21sec, GMV, Entelgy Innotec Security, Forescout, Tenable, Kaspersky, Nunsys-Sothis** y **TXOne Networks.**

Además, se dedicará una tarde a mostrar, de forma distendida, la propuesta del CCI en concienciación y formación a través de su juego para ejecutivos, 'Ciber Impacto', que permite simular y preparar a los profesionales ante un ciberataque divididos en dos equipos: el de *red team* y *blue team*, enfrentándoles a diferentes cuestiones y situaciones en un juego inmersivo y divertido.

El congreso finalizará con la entrega de premios del concurso de la asociación 'Construyendo una arquitectura segura 2022-2023'. Inscripciones y programa en www.cci-es.org

NO PENSAR EN LOS RIESGOS PUEDE SER FATAL PARA TU NEGOCIO

NUESTRA MISIÓN ES PROTEGERLO

- Análisis y Consultoría Seguridad
- Formación y Sensibilización de Empleados
- Implantación de Soluciones tecnológicas
- Soporte, Monitorización y Mantenimiento
- Auditoría de Seguridad y test de intrusión
- Procedimientos y Cumplimiento normativo
- Outsourcing & Headhunting
- Ciberseguridad para PYMES

European Commission
Horizon 2020
European Union funding for Research & Innovation
SEAL OF EXCELLENCE

www.all4sec.es | info@all4sec.es
916 366 544

S·C PREMIOS 2017

Actos y Convocatorias

Actividades CCI. Centro de Ciberseguridad Industrial
- **Una década de experiencias en ciberseguridad industrial,** 19/20-4-2023.
- **Ciberseguridad en el diseño, operación y mantenimiento industrial del sector eléctrico,** 26-3/4-5-2023.
- **Diagnóstico de ciberseguridad en un entorno de automatización industrial,** 17/18-5-2023
- **Ciberseguridad en el diseño, operación y mantenimiento industrial del sector agua,** 22/25-5-2023.
- **Curso multidisciplinar de Seguridad Digital en la Industria 4.0 y protección de servicios esenciales,** Segundo semestre 2023.

Organiza: Centro de Ciberseguridad Industrial-CCI.
Tel.: 910 910 751
Correo-e: info@cci-es.org
Sitio: cci-es.org

III Jornadas STIC
- **Capítulo República Dominicana**

Organizan: CCN, INCIBE, MCCE y DNI-RD
Fechas: 19/21-4-2023
Lugar: Barceló Bávaro. Punta Cana. República Dominicana.
Sitio: ccn-cert.cni.es/iiijornada-rdominicana-programa.html

RSA Conference
Fechas: 24/27-4-2023
Lugar: San Francisco, EE.UU.
Correo-e: information@rsaconference.com
Sitio: rsaconference.com

VICON
- **Congreso de ciberseguridad de Vigo**

Fechas: 28/29-4-2023
Lugar: Círculo de Empresarios de Galicia, Vigo.
Correo-e: vicon@galicia.com
Sitio: vicon.gal

Hack-én
Fechas: 5/7-5-2023
Lugar: Campus Científico y Tecnológico de Linares. Jaén.
Correo-e: hackencon@gmail.com
Sitio: hack-en.org

Osintomático Conference
Fechas: 12/13-5-2023
Lugar: La Nave Villaverde. Madrid.
Sitio: 2023.osintomatico.com

JNIC 2023
- **Jornadas Nacionales de Investigación en Ciberseguridad**

Organiza: Gradiant, Incibe y atlanTTIc (Universidad de Vigo)
Fechas: 21/23-6-2023
Lugar: Vigo (Pontevedra).
Correo-e: jnic2023@uvigo.es
Sitio: 2023.jnic.es

Espacio TISEC
- **Ransomware, seguros cibernéticos y otras incógnitas. Ciberseguridad endeble y ciberpólizas.**

Organiza: Revista SIC
Fechas: 13/14-6-2023
Lugar: Hotel Novotel Campo de las Naciones. Madrid.
Tel.: 91 575 83 24
Correo-e: info@codasic.com
Sitio: revistasic.com/tisec

NextSecure OT Cybersecurity. XXIV Ed.
Organiza: S21Sec
Fechas: 30-5-2023
Lugar: Palacio Euskalduna. Bilbao.
Correo-e: marketing@s21sec.com
Sitio: s21sec.com/nextsecure

SECURMÁTICA 2023
- **En buena compañía**

Organiza: Revista SIC
Fechas: 3/5-10-2023
Lugar: Hotel Novotel Campo de las Naciones. Madrid.
Tel.: 91 575 83 24
Correo-e: info@securmatica.com
Sitio: securmatica.com

Identi::SIC 2023
- **Ser… para creer**

Organiza: Revista SIC
Fechas: 15/16-11-2023
Lugar: Hotel Novotel Campo de las Naciones. Madrid.
Tel.: 91 575 83 24
Correo-e: info@codasic.com
Sitio: revistasic.com/identisic

Formación en Ciberseguridad especializada
- **CEH (Ethical Hacking and Countermeasures v11)**
- **CND (Certified Network Defender)**
- **CCISO (Certified Chief Information Security Officer)**
- **CHFI (Computer Hacking Forensic Investigator)**
- **CSCU (Certified Secure Computer User)**
- **CPENT (Certified Penetration Testing Professional)**

Organiza: M2i Formación
Tel: 91 578 23 57
Correo-e: info@m2iformacion.com
Sitio: m2iformacion.com

AENOR Formación
- **Delegado de Protección de Datos**
- **Gestión de la Continuidad de Negocio**
- **ISO 20000**
- **ISO 27000**

Organiza: AENOR
Tel: 91 432 61 25
Sitio: aenorciberseguridad.com

Cursos Ciberseguridad Westcon-Comstor
Organiza: Westcon-Comstor
Lugar: Madrid
Tel: 91 419 61 00
Correo-e: academy.es@westcon.com
Sitio: academy.westconcomstor.com/es

Cursos ES-CIBER
Organiza: Escuela Superior de Ciberseguridad, ES-CIBER
Correo-e: info@es-ciber.com
Sitio: es-ciber.com

Centro de Formación Exclusive
Organiza: Exclusive Networks
Tel.: 91 197 66 01
Sitio: training.exclusive-networks.com/es-ES

Cursos SANS INSTITUTE
- **Hacker tools, techniques and incident handling,** otoño 2023
- **Windows forensis analysis,** otoño 2023

Organiza: One eSecurity
Lugar: Madrid
Tel.: 911 011 000
Correo-e: sans@one-esecurity.com
Sitio: one-esecurity.com/events_training.html

INDICE DE ANUNCIANTES

SANS EMEA

SANS INSTITUTE EN ESPAÑA
LA EXCELENCIA EN LA FORMACIÓN EN CIBERSEGURIDAD

(one) eSecurity

One eSecurity, empresa líder en servicios DFIR y ciberseguridad, te brinda la posibilidad de **formarte y certificarte en España** en los prestigiosos cursos de **SANS Institute**.

Aprende y comparte con nuestros instructores de talla mundial como **Jess García, SANS Senior Instructor,** con más de 14 años compartiendo y difundiendo conocimiento.

Formato Live Online

- Sesiones interactivas con los instructores de SANS
- Laboratorios prácticos
- Acceso a las grabaciones durante 4 meses tras el curso
- Programa y materiales en formato electrónico
- Flexibilidad de tiempo (2 semanas)

CALENDARIO 2023

SEC504 | GCIH |
Hacker Tools, Techniques and Incident Handling
OTOÑO de 2023
De Lunes a Viernes

Carlos Fragoso

FOR500 | GCFE |
Windows Forensic Analysis
OTOÑO de 2023
De Lunes a Viernes

Aitor Azpiroz

El precio de los cursos es de 7.695 € + IVA. Todos los cursos deben abonarse un mes antes de su inicio.
La certificación GIAC tiene un precio adicional de 850 € + IVA (válido solo si se reserva en conjunto con el curso).

Información de contacto
www.one-esecurity.com | sans@one-esecurity.com | one-esecurity | Teléfono: +34 911 011 000

espacio tiSec

Ransomware, seguros cibernéticos y otras incógnitas

Ciberseguridad endeble y ciberpólizas

Organiza: Revista SIC

Madrid
13 y 14 de junio_2023
www.revistasic.com/tisec