

SITC

**Ciberataques
2024**



**LA CIBERDELINCUENCIA
SE AFILA LOS DIENTES**

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.

Amplia gama de tecnologías que
se ofrecen en modelos on-premise o como servicio

Organización altamente especializada

Extenso conjunto de servicios
a disposición de los players del sector

Network Cloud End Point Protection Secure Identity and Access Management
Security and Vulnerability Management Advanced Threat Protection
Content Security Automated and Monitoring Solutions



A PLENO SOC

AUTOMATIZACIÓN, COMPARTICIÓN Y OTROS DESAFÍOS

Centros de operaciones de ciberseguridad

Organiza:

Revista **SIC**

Madrid

12 y 13 de marzo _2024

www.revistasic.com/tisec

SIC

www.revistasic.com

**Revista
Ciberseguridad, seguridad de la información y privacidad**

**PROYECTOS
Abanca**

**OPEN FINANCE
Ciberfraude
y regulación**

**NUEVO ESTÁNDAR
Llega la ISO 42001**

ENTREVISTA



**Agustín
Muñoz-Grandes**
Responsable
ACCENTURE SECURITY
IBERIA

Félix Muñoz
Director General
INNOTECH SECURITY,
part of Accenture

Ciberataques 2024



**LA CIBERDELINCUENCIA
SE AELLA LOS DIENTES**

9,
856,
348*

Cyber attacks **prevented** today.

Just another day of
Security In Action.

checkpoint.com/action

Estimate based on average calculation from ThreatCloud AI May 2023, an AI-powered threat intelligence engine that makes over 2 billion security decisions daily allowing us to provide accurate prevention in under 2 seconds to hundreds of millions of enforcement points worldwide. We'd say more but...you get the point.



>> Sumario



8	EDITORIAL	193	PROPUESTAS
10	DOBLE FONDO	194	NOVEDADES
12	SIN COMENTARIOS	199	EVENTOS Y FORMACIÓN
14	NOTICIAS	200	BIBLIOGRAFÍA
100	PROYECTOS	202	ACTOS Y CONVOCATORIAS
184	INFORMES Y TENDENCIAS		



104 ENTREVISTA
AGUSTÍN MUÑOZ-GRANDES
y FÉLIX MUÑOZ

>> en este número

- 110** ESPECIAL: LA CIBERDELINCUENCIA SE AFILA LOS DIENTES
Amenazas y ciberataques en 2024: ¿cuáles serán los más complejos y de gran impacto, se esperen o no?
- Previsiones y vaticinios
 - El canto de la Sibila en la ciberseguridad de 2024, por JORGE DÁVILA
- 162** Open Finance: Ciberfraude y retos regulatorios en el cambio multisectorial del paradigma de pagos, por PEDRO CERVERA y JUAN GALDÓN
- 170** Sí a la Inteligencia Artificial, pero con garantías, por BORIS DELGADO y CARLOS MANUEL FERNÁNDEZ
- 174** BSAM: Creando un ecosistema Bluetooth seguro y confiable, por MIGUEL TARASCÓ y ANTONIO VÁZQUEZ
- 178** Crónica de IdentiSIC 2023



• **Vaticinios.** “La ciberdelincuencia se afila los dientes”. Al amparo de este efervescente titular SIC vuelve a tomar la temperatura a los vaticinios de ciberamenazas que bien podrían perfilar el desasosiego de una sociedad digital que mira este 2024 con ansiedad e incertidumbre y se pregunta: “¿Cuáles serán los ciberataques más complejos y de gran impacto, se esperen o no?”. Esta es pues la pregunta que este año hemos formulado desde la revista a dos centenares largos de entidades y expertos; a saber: UE, ONU, otros actores internacionales relevantes, Autoridades Públicas Competentes españolas y departamentos de la AGE, Fiscalía General del Estado y Fuerzas y Cuerpos de Seguridad, policías y entidades autonómicas y locales, aseguradoras y mediadoras, asociaciones y analistas, centros y laboratorios de investigación y evaluación, industria y servicios, organizadores de congresos especializados, actores del mercado de *bug bounty*, hackers y, cómo no, a algunas de las más célebres IAs.

De esta guisa, son 231 los que han escrutado la bola de cristal, sin duda una relevante y muy representativa cifra que da buena cuenta de la calidad de quienes han aportado su ‘savoir prévoir’ en esto de la ciberprotección, a nivel local y planetario.

El trabajo, que forma parte de una serie periódica que SIC inició hace ya varios años en su edición de febrero, es una pieza de valor, porque encierra información en diversos niveles de abstracción de lo que se va esperando. Los actores interpellados, además, están segmentados en base a criterios razonables para que también personas (físicas y jurídicas) ajenas al sector, o que desempeñan funciones en otros frentes –geopolíticos, por ejemplo–, puedan valorar la importancia y alcance de la gestión de riesgos de ciberseguridad con la justa amplitud y seriedad que este gremio merece. Y, de paso, se contribuye a depreciar, por contraste, las deficientes aportaciones de consultores aficionados, analistas de guardarrópia y observatorios miopes, tan paracaidistas ellos en estos tiempos de vacuidad *cool*.

• **A pleno SOC.** Los días 12 y 13 de marzo en Madrid, bajo su divisa **Espacio TiSEC**, SIC volverá a hacer foco intenso en esos ‘agentes’ esenciales para la operación de la ciberseguridad que son los SOC (*Security Operations Centers*). Su rol, crucial en la vertebración de una sociedad digital necesitada de actores de confianza que refuercen, cual mallas, al colectivo participante en los escenarios y actividades cibernéticas, propicia que la pujanza de los Centros de Operaciones de Seguridad siga imparabile y deslumbrando –cuando no cegando– a su protagonistas y demandantes.

Y como la potente expansión de los SOC, ya sean de cliente final, de compañía proveedora de servicios (MSSP) o de fabricantes que prestan algunos servicios directamente a clientes finales, e incluso de redes de ellos –europeas, sectoriales...– está siendo desenfadada, voces autorizadas continentales y sectoriales abogan por la regularización de sus distintas dimensiones, incluyendo una definición real, consensuada y con prestaciones y ‘cimientos’ certificables. De todo ello se hará eco **A pleno SOC**, que igualmente tendrá como invitada especial a la mediática IA, auténtica catalizadora del devenir de estos servicios, con notable repercusión en su sofisticación y eficiencia, en el mercado de trabajo, en los precios y en la propia conformación del sector. Al tiempo, la catalogación de entidades esenciales y críticas, el rol de una Europa que se despereza, la necesaria sectorización ya por lo fino (por ejemplo, del entramado de actores de los medios de pago normalizados (PCI-DSS), de la lucha contra el fraude, o de suministradores de identidad) y la flagrante necesidad de compartir en serio y a mansalva, son también ejes informativos del evento. Estos contenidos conformarán **A pleno SOC**, cuyo lema, dicho sea de paso, parafrasea visualmente el célebre cuadro de Van Gogh con el astro rey como protagonista, capaz simultáneamente de deslumbrar y/o de cegar a quienes, según su prisma, deciden hacer buen uso de él o idolatrarlo visualmente.

• **Efemérides.** Todos los que aún piensan que la experiencia es un grado, y que de bien nacidos es ser agradecidos, se congratulan de las efemérides que en este sentido acontecen en nuestro sector. De hecho, desde hace ya tiempo y cuando corresponde, SIC cede tribuna en sus páginas para que las compañías, entidades y organizaciones objeto de celebración plasmen, adalides mediante, las razones de su éxito y de lo conseguido. Sin duda, un justo reconocimiento a quienes la excelencia es un estímulo.

Mismamente en esta edición, **Telefónica** (100 años), **Akamai** (cinco lustros), el **Centro de Análisis y Prospectiva** de la **Guardia Civil** (25 años) y el **Centro Criptológico Nacional** (dos décadas) conmemoran la culminación de sus respectivas y exitosas trayectorias. Solventes logros que desde SIC consideramos de justicia visibilizar.

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 **Colaboran en este número:** Francisco Arnau, Enrique Ávila, Esperanza Casteleiro, Pedro Cervera, Jorge Dávila, Boris Delgado, Carlos Manuel Fernández, Juan Carlos Gómez Castillo, Alberto Partida, Miguel Tarascó, Antonio Vázquez, (y restantes firmantes del especial) **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

SIC CIBERSEGURIDAD, SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD no comparte necesariamente las opiniones vertidas por los autores de los artículos. Prohibida la reproducción total o parcial de cualquier información digital, gráfica o escrita publicada en SIC sin autorización escrita de la fuente.

espacio

tisec

LOS CIBERRIESGOS,
EN LA ENCRUCIJADA

EL RANSOMWARE TIENE UN PRECIO



Organiza:

Revista **SIC**

Madrid
19 y 20 de junio 2024
www.revistasic.com/tisec



JOSÉ DE LA PEÑA MUÑOZ
Director
jpm@codasic.com

Se busca director para la orquesta nacional de la ciberseguridad

El año pasado se reportaron más de 120 ciber incidentes críticos en España. Para 2024 se espera un punto más de desparrame en la descentralización, adobado generosamente con las prisas en seguir metiéndonos el gusanillo de la hiperconectividad. Solo con esto, y con la inclinación de mucho CIO transformador asfixiado por la superioridad jerárquica con el dulce veneno de la eficiencia *ad infinitum*, la confianza completa (por contraste con la *Zero Trust*), y atento a marcarse un tanto implantando sistemas de IA molones “que aporten valor al negocio”, la actividad de CISO va a ser más compleja.

Para colmo, la legislación (particularmente la de la UE) ha vuelto su mirada hacia los órganos de gobierno y gestión de las empresas, que son los responsables de que las cosas pudieran no hacerse todo lo bien que cabría esperar. (Ojo aquí, que las normativas todavía no traspuestas van a exigir una buena ponderación de riesgos

se ubica en el perímetro de la seguridad nacional, en la que la ciberseguridad juega cierto papel, pero sin ponerle detrás -como sí a la primera- lo de nacional. ¿Por qué? Porque los que pueden decidir no deben saber por dónde tirar. (A lo mejor esa futura ley de ciberseguridad de la que ha hablado recientemente el ministro Escrivá lo deja todo niquelado).

En la edición de febrero del año pasado, Lorena Boix Alonso, Directora para la Sociedad Digital, la Confianza y la Ciberseguridad de la DG CONNECT de la Comisión Europea, en una entrevista amablemente concedida a SIC, manifestó que “Es fundamental que cada país disponga de una autoridad nacional a cargo de la supervisión y el cumplimiento de las obligaciones de ciberseguridad derivadas de la NIS”. Muchos países de la UE ya la tienen. Les ganamos a otros países europeos en muchos frentes de la gestión de la ciberseguridad, pero en este, no. ¿Estaremos acaso esperando a la trasposición de la NIS2 y a la actualización de

ese documento gubernamental que es nuestra vigente Estrategia Nacional de Ciberseguridad?

Las comunidades autónomas llevan tiempo organizándose, si bien es cierto que no del mismo modo: Cataluña y País Vasco con agencia; Madrid, también recientemente; Comunidad Valenciana con su ejemplar CSIRT; Galicia (Amtega-CSIRT-Gal); Andalucía ADA-AndalucíaCERT); Canarias; Región de Murcia (CSIRT); Aragón (servicios de CERT a través de AST); Castilla y León; Castilla-La Mancha (SOC este año);

Navarra y Baleares (que montarán agencias en 2024) y cuatro comunidades autónomas más están definiendo cómo van a centralizar sus procesos de ciberseguridad. Falta que, a efectos generales, se sigan moviendo los ayuntamientos.

Y es que por cualquier lado nos la pueden liar los ciberatacantes: privados, públicos, clientes, suministradores, internos, externos, grandes, pequeños, medianos... esto es lo que tiene hoy lo cibernético y lo ciberfísico. ¿Quién dijo que la transformación era barata?

Tenemos de todo en el solar patrio: método para análisis y gestión de riesgos y herramienta asociada, ENS, Lucía para el intercambio de incidentes, inteligencia compartida con Reyes, respuesta integrada con la RNS, proyecto de certificación de SOC (¡ojo, lector de MSSP!), grupo de caza de amenazas, certificación de tecnologías. Y participamos en la iniciativa de la red europea de SOC, ENSOC, junto a Italia, Luxemburgo, Portugal, Bélgica, Austria y Países Bajos. Y para emprendedores y creación y retención del “talento”, dicen que disponemos de mucha pasta.

Pero no tenemos director de orquesta para el constructo que estamos montando. Esperemos que el asunto no caiga en el bucle ideológico de la época previa a los Juegos Olímpicos de Barcelona y la Expo de Sevilla, en la que la mitad de España creía en las autovías y la otra mitad en las autopistas. ●

Tenemos muchos MSSPs con SOC. Y como ya dijo un experto español hace tiempo en SIC, ha llegado el momento de definir “qué elementos físicos, operacionales, de seguridad y de control hay que tener en tu centro para que se considere un SOC”. Y pueda aspirar a certificarse.

asociados con el cumplimiento legal en materia de idoneidad y mejora de controles para que el deseo de dar facilidades a los posibles clientes para abrir cuentas bancarias con sencillez, desde cualquier sitio y por todos los canales posibles (es solo un ejemplo), no se traduzca en un incremento en engaños, posteriores fraudes y denuncias. Si hay sectores (banca y “telco”, por poner dos clásicos muy regulados) que pueden cooperar para que esto no suceda, mejor que lo hagan. Y si descubren que la cosa cuesta dinero, mejor que consensúen fórmulas intersectoriales de corresponsabilidad, antes de que se las impongán.

Estas cuestiones abren un debate al que desde hace un quinquenio se va acercando el sector de la ciberseguridad. A saber: ¿qué ciberprotección es lícita vender a los clientes finales y cuál debe estar incorporada en los servicios que se ponen a su disposición? Pagarla la vamos a pagar. Pero la geometría del negocio y la actividad cambia mucho. Con la apuesta de la ciberseguridad por diseño, políticamente la dirección está marcada. Al menos por ahora.

Sucede, además, que por la propia importancia de los ciberataques para la estabilidad de los estados democráticos y las entidades supranacionales e internacionales, estos han ido tomando cartas en el asunto (en general con retraso) para mejor defender a las administraciones públicas, la ciudadanía (no solo a los consumidores) y, en suma, al país. Esto último, en España,

Identi :: **Sic**

Identidad digital

cebo y
salvoconducto

Organiza:

Revista **Sic**

www.revistasic.com/identisic

Madrid_
20 y 21 de noviembre_2024
Hotel Novotel Campo de las Naciones



LUIS FERNÁNDEZ DELGADO
Editor
lfernandez@codasic.com

Cisoencers, hackertubers y selfiréxicos

Con pesar e inevitable resignación digiero que ‘polarización’ fue en estos lares el vocablo estelar de 2023. Este lamento, apenas disimulado, lo veo más apropiado al aplicarlo, esta vez con mejor tino, a las eternas fuerzas contrarias de nuestros escenarios ciber, siempre a la greña. Por contra, sí simpatizo más al conocer que el término triunfante del pasado año en Galicia fue curiosamente el palabra ‘cibercocharro’, denominación gallega para epitetar a un ciberdelincuente, en atinado uso por la Amtega en su campaña de sensibilización.

A esta pareja de voces definitorias de un agitado año como fue el anterior, siguen sumándose mesnadas de barbarismos anglosajones, mucho más espabilados para colonizar –tecnogerga mediante–, la lengua actual y anticipatorios de calamidades de

La banalización y uso espurio de esta nuestra especialidad, ni es buena ni ayuda. Ya se vaticinó en el The New Stateman, en 2021 “Los CISOs son extremadamente caros, ¿por qué no automatizarlos? Es mucho más barato, seguro y eficiente dejar la toma de decisiones en manos de algoritmos”.

nuevo cuño. En este empeño, adosar prefijos o sufijos ‘cool’ a términos comunes, es práctica exitosa confiriéndoles perspectivas nuevas. ¿Ejemplos? Comiéncese con Ciber...

Al albur de esto, asistimos al desembarco de los ciberinfluyentes, que, en abultado cardumen, han descubierto en estos pastos cibernéticos nuevos caladeros para abreviar y parasitar, y, de paso, guarecerse un tiempo de las regulaciones gubernamentales que sobre ellos se ciernen, planeadas para meterles en cintura tributaria. Unos ‘usuarios de especial relevancia’, a los que, seguramente –real decreto mediante–, se les va a denominar ‘Prestadores del Servicio de Comunicación Audiovisual’ y, subsiguientemente, a observar muy de cerca.

Pero claro, hasta a ellos incluso les puede llegar su San Martín. De hecho, ya ha comenzado a pasar. Atónitos, observan contrariados cómo sus fermosos envoltorios carnales son sustituidos por avatares digitales que, con su prístina factura, dan muy bien el pego.

Como resultado de este carajal mediaticodigital, ya atisbamos cómo conviven, en un sopicaldo ácrata de IAs y *ciberencers*, toda suerte de marionetas virtuales, infómatas, digisapiens y virtuooides, abriéndose paso en dura competencia con los voluntariosos *behumans* del emprendedor Rames y similares. Las redes sociales, ya claramente sobredopadas, sufren colapso y a sus nautas nos les resulta sencillo distinguir entre un avatar y un calamar. Eso sí, todo entre emulaciones muy resultonas.

En este caldo de cultivo, ya asoman algunos *cisoencers* –no muchos, afortunadamente– que también se dejan engatusar por cantos de cybersirenias y minutillos de gloria en cansinos paneles vacuos... con afán de visibilización incontenible. A ellos se suman también *hackertubers* y *crackertokers* de insacia-

ble frenesí congresual y más pendientes de los *likes* que de las vulnerabilidades. Y, cómo no, inspiratrices de acusada selfirexia, que en vez de aportar propelente solvente para persuadir del ‘oficio’ a desnortadas damas Stems, las disuaden de ello con actitudes paradójicamente rociadas con sesgo perfumado. Así no se las gana para la causa.

La banalización y uso espurio de esta nuestra especialidad, ni es buena ni ayuda. Evocando un artículo aparecido en The New Stateman, en 2021, su fatídico vatininio aun inquieta al verlo impreso y, sobre todo, en estos días: “Los CISOs son extremadamente caros, ¿por qué no automatizarlos? Es mucho más barato, seguro y eficiente dejar la toma de decisiones en manos de algoritmos”. Esta aseveración concuerda lamentablemente con el sufijo guiri de moda: *less*, que aplicado a la denominación genérica del responsable de ciberprotección, conforma el fatídico palabra *CISOless*.

También GPCISOs (*Generative Pre-trained Chief Information Security Officers*) es acrónimo efervescente y augura tecnozarandeos a la profesión. Cabe temer que en breve veremos sixpacks de Cisoides en los lineales de los supermercados, junto a los ordenadores cuánticos chinos a 8.000 euros unidad que ya se anuncian.

Frente a esta algarabía cibernética, anacrónicamente vamos quedando algunos a quienes todavía nos sigue gustando que las neuronas alboroten nuestras azoteas y nos marquen rumbo, aunque sigamos topándonos con encrucijadas y desconozcamos, en ocasiones, qué cambios adoptar o qué decisiones tomar. Y en esa tesitura nos viene a colación lo dicho por el filósofo y matemático René Descartes, autor de esa frase tan cruda y sapiente: “Razonar es dudar”.

Mucho me temo que las máquinas no dudan. Por lo que no cabe descartar que la carne de CISO sea sustituida por la de silicio. Y la clonación digital a mansalva propicie obedientes responsables de seguridad digital infalibles, infatigables, antiestresantes, baratos y *always on*. Y, claro, con *deepfakeCisos* a las puertas.

A las ciberamenazas, sobrecogedoras diría, que nos sobrevienen –baste leer el especial de esta edición de SIC sobre ellas–, no se las combate con postureo sino con erudición y saber hacer ejemplarizante; con formación, concienciación, puesta en común, trabajo en equipo y compartición real y recíproca. Con las lecciones aprendidas, hoy ya a montones, nuestro querido oficio, sabiduría y culo pelado, deberían bastar para lidiar con razonable soltura el emponzoñado tsunami de amenazas que nos sobreviene.

Parafraseando a la gran diseñadora francesa de la alta costura Coco Chanel –traída a colación por ‘Balenciaga’, la estupenda serie hoy tan en candelero–, si ‘cosiera’ en nuestro ámbito, tan innovadora y rupturista ella, seguramente diría: “Una IA puede decir de todo menos vulgaridades”. Gente del sector, aplíquemonos el cuento.

Como empecé termino: aludiendo a una palabra con pegada. Si el intelecto humano no lo remedia, a buen seguro el término que postramente triunfará en este 2024 será **piñA**. ●

Innotec Security is now part of Accenture



En enero también puso en marcha una normativa para mejorar la ciberprotección de las instituciones europeas, a través del UE-CERT

La UE da un paso notable hacia 'un escudo común' con los acuerdos finales sobre la Ley de Ciberresiliencia y la de Ciberseguridad

Ante las elecciones europeas que tendrán lugar entre el 6 y el 9 de junio, las instituciones intensificaron su trabajo a finales de 2023, coincidiendo con la presidencia española, para aprobar normativas en su fase final. Entre otras iniciativas, la **Comisión** y el **Parlamento** acordaron un texto final de la Ley de Ciberresiliencia (GRA), propuesta en septiembre de 2022.

Con ella, se espera mejorar el nivel de ciberprotección de los productos digitales en beneficio de los consumidores y las empresas en toda la UE, ya que introduce requisitos de ciberseguridad obligatorios y proporcionados para todo el hardware y software, desde monitores para bebés, relojes inteligentes y juegos de ordenador, hasta cortafuegos y enrutadores. Los productos con diferentes niveles de riesgo asociado tendrán diferentes requisitos de seguridad.

En cuanto entre en vigor la CRA, los fabricantes de hardware y software tendrán que implementar medidas de ciberseguridad a lo largo de todo el ciclo de vida del producto, desde el diseño y el desarrollo hasta después de su comercialización. Los productos de software y hardware llevarán el 'Marcado CE' para indicar que cumplen con los requisitos del Reglamento y, por tanto, pueden venderse en la UE.

Actualizaciones

La ley también introducirá la obligación legal para los fabricantes de proporcionar a los consumidores actualizaciones de seguridad oportunas

durante varios años después de la compra. Este período debe reflejar el tiempo que se espera que se utilicen los productos. A través de estas medidas, la normativa permitirá a los usuarios tomar decisiones mejor informadas y más seguras.

Próximos pasos

Al cierre de la edición de este número de SIC, el acuerdo estaba sujeto a la aprobación formal, tanto del Parlamento como del Consejo. Publicado en el Diario Oficial, entrará en vigor 20 días después, a partir de los que fabricantes, importadores y distribuidores de productos hardware y software tendrán 36 meses para adaptarse a los nuevos requisitos, con excepción de un período de gracia más limitado de 21 meses en relación con la obligación de informar de las incidencias y vulnerabilidades de los fabricantes.

Ciberseguridad

Además, poco antes de terminar el año, los representantes de los Estados miembros (Cooper) alcanzaron una posición común sobre el proyecto de la llamada Ley de Ciberseguridad (CSA), que busca una Europa más resiliente y reactiva frente a las ciberamenazas, al tiempo que fortalece los mecanismos de cooperación. Además, se prevé la creación de un mecanismo de emergencia cibernética para aumentar

la preparación y mejorar las capacidades de respuesta a incidentes. Y establece la puesta en marcha de un 'escudo cibernético europeo', que se materializará en una infraestructura paneuropea compuesta por SOC's nacionales y

transfronterizos en toda la UE.

Se calcula que esta iniciativa contará con un presupuesto que rondará los 1.100 millones de euros, de los que dos tercios serán financiados por la UE a través del programa Europa digital.

Ciberprotección para organismos de la UE

Además, en enero entró en vigor el Reglamento de Ciberseguridad (Euratom), aprobado por el Consejo y el Parlamento, que establece medidas para un alto nivel común de ciberseguridad en las instituciones, órganos, oficinas y agencias de la UE.

En concreto, propone un marco interno de gestión, gobernanza y control de riesgos para cada entidad y crea un **Consejo Interinstitucional de Ciberseguridad (IICB)** para supervisar y apoyar su implementación por parte de las entidades de la Unión.

Además, ofrece un mandato ampliado del Equipo de Respuesta a Emergencias Informáticas para las instituciones, órganos, oficinas y agencias de la UE (CERT-EU), que pasará a llamarse Servicio de Ciberseguridad para las instituciones, órganos, oficinas y agencias de la Unión, manteniendo sus siglas.



EN BREVE

Reglamento de Datos: el CONSEJO adopta nueva legislación sobre el acceso justo a los datos y su utilización

Para hacer de la UE una referencia en protección y gestión de los datos, el **Consejo** y el **Parlamento** alcanzaron, a finales de año, un acuerdo provisional sobre el Reglamento de Datos, que quiere ofrecer acceso justo a los datos y su utilización en el Viejo Continente. Entre sus objetivos están desde garantizar la equidad en la asignación del valor de los datos entre los agentes del entorno digital, hasta estimular un mercado de datos competitivo, generar posibilidades para la innovación basada en los datos y hacer que sean más accesibles para todos.

Además, busca facilitar el cambio de proveedor de servicios de tra-



tamiento de datos, establecer salvaguardias contra las transferencias ilegales de datos y prevé la elaboración de normas de interoperabilidad para la reutilización de datos entre sectores.

El Reglamento entrará en vigor a mediados de 2025. Eso sí, lo marcado para productos conectados y a los servicios relacionados con ellos tendrá un plazo de carencia de 32 meses.

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



EN BREVE

En tiempo de Presidencia española se cierra el acuerdo del reglamento para crear una identidad digital europea única y segura, a través del eIDAS2

Tras un intenso trabajo, la Presidencia española del Consejo de la UE consiguió el acuerdo entre la **Comisión** y el **Parlamento** para aprobar el Reglamento (UE) n°910/2014, conocido como eIDAS: el marco legal vigente en Europa para la identificación electrónica y servicios de confianza en transacciones electrónicas, cuya segunda versión (eIDAS2) se espera que entre en vigor este año. Gracias a él se podrá garantizar el acceso universal de las personas y las empresas a una identificación y autenticación electrónicas seguras y fiables, obligando a los estados a emitir, dentro de los 24 meses posteriores a la entrada en vigor, al menos una cartera de identidad digital europea (European Digital Identity Wallet), en forma de aplicaciones móviles, que serán voluntarias para los ciudadanos y empresas.

También, se establece la ampliación de servicios de confianza a los libros mayores electrónicos (*electronic*



ledgers) y a la gestión de dispositivos de creación de firmas y sellos electrónicos a distancia, así como la expedición electrónica de atributos de identidad por parte de prestadores cualificados.



Al cierre de esta edición de SIC, ya sólo quedaba presentar el texto final al **Comité de Representantes Permanentes de los Estados miembros** (Coreper) para su aprobación,

además de ser adoptado formalmente por el Parlamento y el Consejo –en la imagen la arquitectura y marco de referencia de la cartera de identidad digital de la unión europea, traducida por el especialista **Julian Inza** y pertenecientes a la versión V1.2 del documento–.



La presidencia belga de la UE apuesta, entre sus grandes prioridades, por impulsar una mayor ciberseguridad y ciberresiliencia europeas

Sucediendo a España, Bélgica estará al frente de la **Presidencia del Consejo** hasta el 30 de junio. Así, entre otras iniciativas, la ciberseguridad será una de sus prioridades y, de hecho, su lema para este semestre será ‘Proteger, fortalecer, preparar’. Ya se ha avanzado que apostará por impulsar un enfoque conjunto para la ‘ciberprotección activa’, fortalecer la confianza en el ámbito digital y mejorar la ciberresiliencia. Además, intentará finalizar cualquier trabajo restante sobre la Ley de Resiliencia Cibernética, así



como concluir lo hecho con la Ley de Ciberseguridad. De cara a una nueva legislatura, también ha avanzado que acometerá revisión de la política cibernética de la UE y del panorama institucional para evaluar el progreso e identificar las brechas y disparidades restantes que deben abordarse. Como curiosidad, ha destacado que se centrará también en impulsar la ciberresiliencia de la infraestructura espacial. La agencia belga de ciberseguridad (CCB) será la responsable de coordinar estas iniciativas.

Los ESTADOS MIEMBROS acuerdan una posición común sobre una modificación específica de la Ley de Ciberseguridad para servicios de seguridad gestionados

Para mejorar la ciberresiliencia de la UE al permitir la futura adopción de sistemas de certificación europeos para los ‘servicios de seguridad gestionados’, los representantes de los estados miembros (Coreper) alcanzaron una posición común, a finales de año, sobre la propuesta de modificación específica de la Ley de Ciberseguridad (CSA),



que atañerá a dichos servicios. Presentada junto con una propuesta de Ley de Ciberseguridad de la UE, el nuevo texto aclara la definición de “servicios de seguridad gestionados” alineada con la directiva NIS2, así como con los objetivos de los diferentes sistemas de certificación en este ámbito de la UE.

ES-CIBER

ATENCIÓN

Este 2024 conciencia a tus empleados en Ciberseguridad y ponlos a prueba con nuestros recursos formativos.

¡PARA MÁS INFORMACIÓN!

Info@es-ciber.com



La Casa Blanca espera publicar este año la versión 2.0 de su Estrategia Nacional cibernética con notables mejoras

EL DEPARTAMENTO DE DEFENSA aumenta su presupuesto para ciberprotección, prestando también especial atención a la IA y su seguridad

La ciberprotección ha vuelto a ser una de las partidas que han crecido en el proyecto de Ley de Autorización de Defensa Nacional de la administración Biden, alcanzando aproximadamente los 11.269 millones de euros (12.270 millones de dólares), para el año fiscal 2024, de un montante total de 813.000 millones. En su mayoría, se destinarán a respaldar su estrategia de ciberseguridad, tanto en lo que atañe a los servicios del gobierno y federales, así como a mejorar la protección de la infraestructura crítica y las tecnologías esenciales.



Drenan Dudley



Harry Coker

e implementar las acciones de mitigación necesaria. Además, se solicita al secretario de Defensa elaborar un plan estratégico para el desarrollo, uso y ciberseguridad de la IA generativa en el ámbito militar.

La Ley también aprueba la creación de un programa, denominado 'Asociación para la Conectividad Digital y la Ciberseguridad', para impulsar las mejores prácticas y estándares comunes para un enfoque nacional.

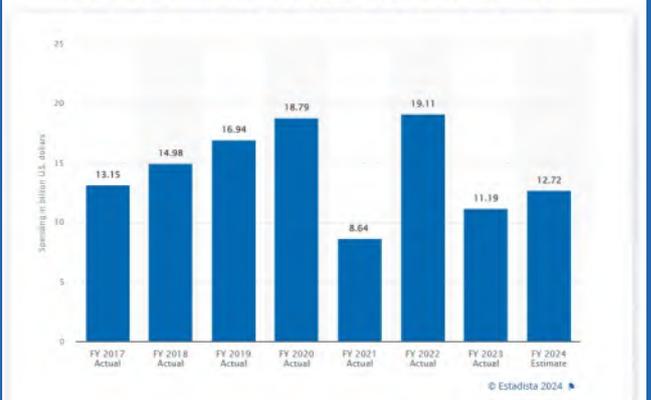
Además, dedica un presupuesto al Departamento de Estado, "para promover un ciberespacio seguro y estable ayudando a los países a prepararse, defenderse y responder a actividades cibernéticas maliciosas y adoptar estrategias nacionales para mejorar la ciberseguridad, entre otros aspectos".

De hecho, la ciberprotección es uno de los aspectos notables en la ley con propuestas que buscan contrarrestar, por ejemplo, el tráfico ilegal por parte de organizaciones criminales transnacionales mexicanas en el ciberespacio, así como cooperar con Taiwán en

ciberseguridad militar, establecer un grupo de trabajo sobre vulnerabilidades en dispositivos médicos y farmacéuticos militares, crear un programa piloto relacionado con la cadena de suministro de semiconductores, con la participación del Centro de Colaboración en Ciberseguridad de la NSA, entre otros aspectos.

Como curiosidad, el texto también autoriza un programa piloto sobre la 'Reserva Civil de Ciberseguridad', que permite establecer un grupo de cibervoluntarios que puedan trabajar con el Comando Cibernético de EE.UU. Una idea que se ha planteado sin éxito varias veces también en España.

PRESUPUESTO ESTIMADO DEL GOBIERNO DE EE.UU. PARA CIBERSEGURIDAD EN EL AÑO FISCAL 2017 a 2024



EUROPA y EE.UU. suman fuerzas en su 'noveno diálogo cibernético' aprobando varias iniciativas conjuntas para impulsar una "ciberresiliencia global"

La UE y EE.UU. celebraron, a finales de año, su noveno 'Diálogo Cibernético', en el que apostaron por "promover la seguridad y la estabilidad internacionales en el ciberespacio y mejorar la capacidad de todos los estados para aprovechar los beneficios que brindan la tecnología".

Durante el encuentro, también intercambiaron puntos de vista sobre el entorno global de amenazas cibernéticas, marcado por la agresión de Rusia contra Ucrania, y expresaron su preocupación por el aumento de actividades cibernéticas maliciosas dirigidas a las cadenas de suministro, la infraestructura crítica y la propiedad intelectual.

No faltó el compromiso de ambas partes con el marco de las Naciones Unidas sobre comportamiento estatal responsable en el ciberes-



El encuentro estuvo copresidido por Joanneke Balfoort, Directora de Política de Seguridad y Defensa del Servicio Europeo de Acción Exterior (SEAE); Lorena Boix, Directora de Sociedad Digital, Confianza y Ciberseguridad, D.G. de Redes de Comunicaciones, Contenidos y Tecnología (DG Connect), Comisión Europea; y Liesyl Franz, Subsecretaria Adjunta para Seguridad Internacional del Ciberespacio en la Oficina de Ciberespacio y Política Digital del Departamento de Estado de EE.UU.

pacio, basado en la aplicación del derecho internacional y las normas de comportamiento estatal responsable.

Además, se firmó un acuerdo de trabajo entre la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) de EE.UU. y la de Ciberseguridad de la UE (Enisa) para impulsar la concienciación y capacitación así como el intercambio de mejores prácticas y de conocimientos. También, se avanzó en el 'Plan de Acción Conjunto

de Productos CyberSafe', apostando de forma conjunta por "mejorar aún más la ciberresiliencia global" y "profundizar en la cooperación para abordar los desafíos de ciberseguridad relacionados con las tecnologías emergentes, con especial atención a la IA y la criptografía postcuántica".

¿Puede la complejidad ser un riesgo para la ciberseguridad de la empresa?

Descubre los datos del estudio EY *Global Cybersecurity Leadership Insights 2023* y cómo desde EY podemos ayudarte.



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

The EY logo, consisting of the letters 'EY' in a bold, white, sans-serif font. A yellow diagonal bar is positioned above the 'Y'.

Building a better
working world

Modelo de Madurez

El DoD también aprobó, a finales de 2023, su programa de Certificación del Modelo de Madurez de Ciberseguridad (CMMC) con el que pretende que todos sus contratistas tengan una ciberprotección certificada por un tercero (en el caso de los que manejan información no clasificada controlada (CUI)), implementando con éxito 110 controles de ciberseguridad.

Cambios en 2024

Además, ha sido especialmente notable que, según el director nacional adjunto de Ciberseguridad, **Chris DeRusha**, la administración Biden ya está analizando el plan de implementación de su estrategia nacional de ciberprotección publicada el año pasado y que, este año, tendrá su versión 2.0. Asimismo, se ha conocido que se está trabajando

en mejorar el 'Plan Nacional de Respuesta a Ciberincidentes', a través de una mayor coordinación público-privada para abordar, entre otros aspectos, las amenazas a las infraestructuras críticas.

Precisamente, para reforzar su equipo, el gobierno nombró a **Harry Coker**, director nacional cibernético y a **Drenan Dudley**, como subdirectora cibernética nacional de Estrategia y Presupuesto.

EN BREVE

EL DEPARTAMENTO DE SERVICIOS FINANCIEROS de Nueva York obligará a las empresas a informar de pagos de rescates de *ransomware*

El **Departamento de Servicios Financieros del Estado de Nueva York**, que supervisa bancos, compañías de seguros, corredores hipotecarios y otras

comités de dirección conservar un nivel adecuado de experiencia para comprender los problemas cibernéticos, además de apoyar con medios y propuesto a los CISO para que tengan los "recursos suficientes".



instituciones financieras, ha publicado nuevas medidas que tendrán que cumplir las empresas afectadas por su control financiero. En concreto, en ellas se da un papel más protagonista a los responsables de ciberseguridad, como responsables de que las empresas cumplan con estas directrices, que recuerdan a las aprobadas en 2023 por la **Comisión de Bolsa y Valores (SEC)**, aunque son más detalladas en muchos aspectos por cuanto exigen a las juntas directivas y

Además, obliga a las compañías reguladas a informar cualquier pago realizado a criminales por ataques de *ransomware*, dentro de las 24 horas posteriores de haberlo realizado, así como a implementar la autenticación multifactor e incluir el plan de ciberseguridad dentro de continuidad del negocio —y continúa exigiendo informar sobre los incidentes de ciberseguridad en un plazo de 72 horas—.

Además, obliga a las compañías reguladas a informar cualquier pago realizado a criminales por ataques de *ransomware*, dentro de las 24 horas posteriores de haberlo realizado, así como a implementar la autenticación multifactor e incluir el plan de ciberseguridad dentro de continuidad del negocio —y continúa exigiendo informar sobre los incidentes de ciberseguridad en un plazo de 72 horas—.

El mundo al revés: los cibercriminales denuncian a una empresa a la SEC por no informar del incidente que han causado

Tras atacar a la empresa de software **Meridian-Link**, exfiltrar sus datos y exigir un pago a cambio de



parte de Meridian-Link de las reglas de divulgación de incidentes de ciberseguridad adoptadas recientemente. Nos ha llamado la atención que MeridianLink, a la luz de una violación significativa que compromete los datos del cliente y la información operativa, no ha presentado la divulgación requerida según el Artículo 1.05 del Formulario 8-K dentro de los cuatro días hábiles estipulados, según lo dispuesto por la nueva SEC", dice en su denuncia.

parte de Meridian-Link de las reglas de divulgación de incidentes de ciberseguridad adoptadas recientemente. Nos ha llamado la atención que MeridianLink, a la luz de una violación significativa que compromete los datos del cliente y la información operativa, no ha presentado la divulgación requerida según el Artículo 1.05 del Formulario 8-K dentro de los cuatro días hábiles estipulados, según lo dispuesto por la nueva SEC", dice en su denuncia.

Tras atacar a la empresa de software **Meridian-Link**, exfiltrar sus datos y exigir un pago a cambio de parte de Meridian-Link de las reglas de divulgación de incidentes de ciberseguridad adoptadas recientemente. Nos ha llamado la atención que MeridianLink, a la luz de una violación significativa que compromete los datos del cliente y la información operativa, no ha presentado la divulgación requerida según el Artículo 1.05 del Formulario 8-K dentro de los cuatro días hábiles estipulados, según lo dispuesto por la nueva SEC", dice en su denuncia.

El NIST publica el borrador de una guía que ofrece orientación para medir y mejorar el programa de ciberprotección de una empresa

El **Instituto Nacional de Estándares y Tecnología (NIST)** ha publicado un documento, con dos volúmenes, bajo el título 'Publicación especial NIST (SP) 800-55 Revisión 2: Guía de medición para la seguridad de la información', que buscar servir de hoja de ruta "para crear un programa práctico de medición de la seguridad de la información", destacan sus responsables. En concreto, la publicación está diseñada para usarse junto con cualquier marco de gestión de riesgos, como el Marco de Ciberseguridad o el Marco de Gestión de Riesgos del NIST y que los responsables de ciberprotección puedan tener una "imagen coherente basada en datos concretos", de su madurez en



este ámbito. "Todo el mundo gestiona el riesgo, pero muchas organizaciones tienden a utilizar descripciones cualitativas de su nivel de riesgo, utilizando ideas como colores de semáforo o escalas de cinco puntos", ha destacado una de las autoras de la publicación, **Katherine Schroeder**. "Nuestro objetivo es ayudar a las personas a comunicarse con datos en lugar de conceptos vagos".

De momento, NIST admite comentarios públicos sobre el borrador inicial hasta el 18 de marzo.

La NASA da a conocer su primera guía "de mejores prácticas de ciberseguridad espacial"

Bajo el título 'Control terrestre para la industria espacial: lleve sus prácticas estáticas de ciberseguridad y actualícelas a un modelo dinámico', la **NASA**



ha dado a conocer la que es su primera guía de mejores prácticas de ciberprotección para comunicaciones espaciales, como parte de sus esfuerzos para lograr que los requisitos de ciberseguridad en este ámbito sean más accesibles para los expertos.

Por ello, la guía pretende alinear

el lenguaje del proyecto de vuelo de la NASA con los controles de seguridad descritos en el catálogo de controles de seguridad para agencias gubernamentales del

Instituto Nacional de Estándares y Tecnología, conocido como SP 800-53. "Los principios de ciberseguridad deben ser fácilmente alcanzables independientemente del tamaño o alcance de la misión, el programa o el proyecto, o si es internacional, corporativo o universitario", destaca el documento.

Nuestros colores favoritos son
el rojo, azul y morado...

¿Y LOS TUYOS?



Blue team con mySOC, red team
con nuestros auditores, purple team
cuando mezclamos ambos...

Elige tu favorito.

advens

La región refuerza sus capacidades con la creación de agencias, policías nacionales de ciberseguridad, además de actualizar sus ciberestrategias

Según el informe **Latam CISO 2023**, en Iberoamérica se tuvo constancia en torno a 1.600 ciberataques por segundo, un dato muy ilustrativo de lo que supone la región para los principales grupos cibercriminales. A ello, se le suma la conocida falta de profesionales en todo el mundo y que “se presenta de manera exacerbada en América Latina y el Caribe, generando fuertes presiones en las organizaciones tanto públicas como privadas con el subsiguiente impacto en la ciberseguridad de los países de la región”, según pone de manifiesto el más reciente ‘Reporte sobre el desarrollo de la Fuerza Laboral de Ciberseguridad en una era de escasez de talento y habilidades’, de 2023, de la **Organización de los Estados Americanos (OEA)**, junto con **Cisco**.



Iniciativas nacionales



Comisión sexta de la Cámara de Representantes de Colombia



La región, según el último estudio de **(ISC)2** -ver sección informes de este número-, sufre un déficit de cerca de 350.000 profesionales que, de acuerdo con el documento

de la OEA, se debe a: “esfuerzos aislados para el desarrollo de la fuerza laboral y la promoción de alianzas nacionales e internacionales; un marco regulatorio débil; insuficiente información estratégica, a nivel nacional, para la toma de decisiones; e insuficiente sensibilización y divulgación sobre recursos, herramientas e información en este ámbito”.

“Para robustecer el ecosistema de ciberseguridad resulta necesario trabajar de forma integral y de manera coordinada en el desarrollo de la fuerza laboral”, dijo al respecto la secretaria ejecutiva del Comité Interamericano contra el Terrorismo de la OEA, **Alison Treppel**.

Aunque queda camino por recorrer para dar respuesta a este problema, “los sistemas educativos en la región han comenzado a movilizarse, con un gran número de instituciones y entidades educativas creando y lanzando nuevos títulos y cursos de ciberseguridad”, según el informe. Además, en los dos últimos meses de 2023, diferentes países de la región impulsaron notables iniciativas que buscan impulsar la protección cibernética en 2024 y minimizar dicha problemática.

Por ejemplo, en **Colombia** destacó el acuerdo de la compañía española **S2 Grupo** y el **Ministerio de Tecnologías de la Información y las Comunicaciones**, que sumaron fuerzas para fomentar la ciberseguridad y el uso seguro de las TIC entre los ciudadanos, las empresas, el Gobierno y en los sectores industriales e infraestructuras críticas de todo el país. Entre las iniciativas, destaca fortalecer las capacidades del ColCERT, entre otras entidades, participar en proyectos estratégicos de I+D+i, así como fomentar la formación en habilidades digitales y en ciberseguridad e incorporar talento joven a las organizaciones en este sentido, entre otros aspectos.



gobernanza y coordinación; marcos legales y normativas; educación, capacitación y concienciación; así como, cooperaciones y alianzas.

Junto a ello, cabe destacar que Colombia, además, aprobó, en un primer debate, su Proyecto de Ley 023 de 2023, con el que pondrá en marcha su **Agencia Nacional de Seguridad Digital y Asuntos Espaciales**. Será un organismo, de carácter técnico, especializado, que tendrá como objeto planificar, articular y gestionar los riesgos de seguridad digital en el país, previniendo amenazas internas o externas. Eso sí, aún quedan tres debates más para aprobar el Proyecto de Ley que cuenta con el apoyo de diferentes entidades del sector TIC y del ecosistema digital del país.

Protección colaborativa

A finales de año, la **Corte Suprema de Justicia de la Nación de Argentina** anunció la

creación de una **Oficina de Ciberseguridad**, bajo la órbita de la **Dirección de Sistemas** que tendrá como misión gestionar la seguridad del tribunal en esta materia, salvaguardando “la integridad, confidencialidad y disponibilidad de la información y sistemas, mediante una gestión proactiva frente a amenazas cibernéticas y promoviendo una cultura robusta de seguridad informática”, según indican desde la Corte.

En paralelo, **República Dominicana**, a través de su **Centro Nacional de Ciberseguridad** y de su **CSIRT-RD** dio a conocer su ‘Política y Plataforma de Divulgación Responsable de Vulnerabilidades’.

Se trata de una iniciativa que representa “un paso significativo hacia una ciberseguridad



más sólida y colaborativa”, resaltó el director del CSIRT Nacional, **Carlos Leonardo**, poniendo en valor que permitirá contar con “un espacio y canal oficial dedicado a reportar y notificar vulnerabilidades y brechas de datos que afecten a instituciones públicas”.

A mediados de diciembre, por su parte, el **Congreso Nacional de Chile** aprobó la ‘Ley Marco de Ciberseguridad e Infraestructura Crítica’, faltando únicamente su promulgación por parte del presidente de la República. Gracias a ella se creará la **Agencia Nacional de Ciberseguridad (ANCI)**, además del CSIRT Nacional y el de Defensa.

Asimismo, la ley considera obligatorio que las empresas privadas tomen mayor responsabilidad sobre sus incidentes, reportando a la ANCI situaciones críticas para responder de forma coordinada, con capacidades público privadas.

Igualmente, **Brasil** también logró un hito importante en la materia tras aprobar la creación de su **Policía Nacional de Ciberseguridad (PN-Ciber)** y poner en marcha su **Comité Nacional de Ciberseguridad (CNCiber)**, encargado de monitorizar la implementación y evolución de la PNCiber, así como de formular propuestas para mejorar la prevención, detección, análisis y respuesta a incidentes cibernéticos.

Por otro lado, se ha continuado fortaleciendo la ciberseguridad nacional mediante notables acuerdos como el firmado entre **Paraguay** y **Estados Unidos** para colaborar y hacer frente, de forma conjunta, a las amenazas de actores estatales y no estatales en el ciberespacio.

HEARTBREAK PROTECTION

PROACTIVE MEASURES AGAINST ANY THREAT



#F*YOU CUPIDO**

RED TEAM | THREAT HUNTING | INCIDENT RESPONSE

www.tarlogic.com



Con 17 países como socios, será el asesor cibernético de Smart África, iniciativa gubernamental con 39 países, que representan a más de 1.000 millones de habitantes

Arranca la RED DE AUTORIDADES DE SEGURIDAD CIBERNÉTICA (ANCA)

Los países africanos se enfrentan habitualmente a una variedad de ataques, incluidas campañas distribuidas de denegación de servicio (DDoS) y, cada vez más, a *ransomware*, según un informe de **Positive Technologies**, de julio de 2023. Para evitar esta situación, África está dando pasos notables para alcanzar una rápida madurez cibernética. Según un reciente estudio de **SecurityScorecard**, el continente ha mejorado de forma importante en los últimos años, aunque “necesita invertir en reemplazar tecnología obsoleta y sistemas al final de su vida útil, y crear flujos de trabajo más sólidos para identificar amenazas y parchear sistemas”, ha destacado el vicepresidente senior de la compañía, **Ryan Sherstobitoff**, que recuerda que entre otros retos “no todos los países de África son iguales; algunos tienen economías más prósperas que otros, especialmente Sudáfrica, y lo mismo ocurre con el Medio Oriente”.

Entre las iniciativas más importantes de los últimos años, destaca la construcción de un **Centro Cibernético Virtual**, en Nigeria, y el refuerzo de la



Miembros de la junta de gobierno de ANCA (de dcha. a izq.): Thelma Quaye, Directora de Infraestructura Digital, Habilidades y Género; General Mostapha El Rabbi, Vicepresidente, Director General de la Autoridad de Seguridad Cibernética del Reino de Marruecos; Dr. Albert Antwi-Boasiako, Presidente y Director General de la Autoridad de Seguridad Cibernética de Ghana y Didier Nkurikyimfura, Director de Estrategia y Crecimiento, Smart África

inteligencia de amenazas transfronterizas, implementándose como proyectos importantes para abordar el déficit con la participación de varios países. Y de forma especial, destaca la puesta en marcha de la **Red Africana de Autoridades de Ciberseguridad (ANCA)** compuesta por agencias y autoridades nacionales de ciberprotección de 17 países –Benin, Burkina Faso, Camerún, Chad, República del Congo, Djibouti, Gabón, Ghana, Guinea, Kenia, Marruecos, Mozambique, Ruanda, Senegal,

Sierra Leona, Togo y Túnez–, que tendrá como presidente al director de la Autoridad de Seguridad Cibernética (CSA) de Ghana que, a través de una mesa de trabajo (en la imagen), se encargará de poner en marcha la Red.

Precisamente, aprovechando la celebración en el país de la primera Conferencia Global sobre Creación de Capacidad Cibernética (GC3B), con el lema ‘Ciberresiliencia para el desarrollo’, impulsada por la CSA, el **Foro Global sobre Experiencia Cibernética (GFCE)**, el **Instituto Cibernético para la Paz**, el **Banco Mundial** y el **Foro Económico Mundial**, se puso en valor la creación de



la ANCA como organismo asesor en este ámbito con **Smart África** –asociación

internacional puesta en marcha de la que forman parte 39 países representando a más de 1.000 millones de personas–, además de articular la voz del continente sobre cuestiones de ciberprotección en debates globales, entre otros aspectos.

Albert Antwi-Boasiako, presidente de la ANCA:

“Queremos crear una plataforma para el intercambio y la cooperación y hacer oír la voz de África en las relaciones con sus socios”

– ¿Cuál es el principal reto para poner en marcha esta iniciativa?

– El fin es crear una plataforma para el intercambio y la cooperación entre sus miembros y hacer oír la voz de África en sus relaciones con sus socios en todo el mundo en materia de ciberseguridad. Y mi principal reto, como responsable de la iniciativa, es trabajar con la Secretaría de Smart Africa y centrarme en brindar liderazgo en cuestiones de ciberprotección en el continente africano.

– En 2024, como primer año, ¿qué considera prioritario?

– Seis puntos muy concretos, que van desde el establecimiento de una estructura de gobernanza para la red para compromisos efectivos, hasta el crecimiento en el número de miembros de la red –actualmente, son 17 países– y la creación de una plataforma para los intercambios operativos y la cooperación práctica entre los miembros.

Además, se explorarán modelos de financiación y asociaciones para el desarrollo de la ciberseguridad en los países miembros y en todo el continente. También, se va a hacer un esfuerzo en la creación de capacidades y ver cómo se puede contribuir a las iniciativas emblemáticas de Smart Africa como organismo asesor continental en cuestiones de ciberseguridad, entre otros.

– ¿Qué le preocupa en este ámbito?

– Muchos países africanos también deben desarrollar mecanismos reguladores de ciberseguridad maduros y tienen una capacidad limitada para detectar y responder a ciberataques que podrían poner en peligro la seguridad nacional y el bienestar socioeconómico de sus ciudadanos.

– Las ciberamenazas más preocupantes para este año en África...

– El continente está expuesto a una serie de riesgos, incluidos posibles ataques a sistemas de infraestructura de información crítica, fraude de identidad/en línea, amenazas a la seguridad en línea de los niños y la desinformación, entre otras.



Albert Antwi-Boasiako

– ¿En la creación y evolución de la ANCA se prestó atención a las diferentes iniciativas que se están llevando a cabo en España en esta materia?

– La ANCA aprecia la naturaleza sin fronteras de las cuestiones relacionadas y ha estado monitorizando el desarrollo global de la ciberseguridad en todo el mundo, además, África está comprometida con el desarrollo de legislación, políticas y capacidades a través del intercambio de conocimientos y la colaboración.

España, como miembro de la UE, ha desarrollado sólidos sistemas de ciberprotección, contribuyendo a la ciberresiliencia, tanto europea como global. Además, al igual que Ghana, es parte en el Convenio sobre la Ciberdelincuencia, también conocido como Convenio de Budapest, y dichas relaciones son necesarias para garantizar la cooperación transfronteriza y mejorar la resiliencia cibernética.

La ANCA en colaboración con la Secretaría de Smart Africa, que dio origen a esta iniciativa, también aprenderá de las mejores prácticas globales para mejorar el estado de la ciberseguridad entre los países miembros y en todo el continente.

– ¿Cuáles serán los organismos de referencia que marcarán la ‘hoja de ruta’ de ANCA?

– Nos guiaremos por una serie de instrumentos, incluida la Convención de la Unión Africana sobre Seguridad Cibernética y Protección de Datos Personales (Convenio de Malabo), el Plan de África Inteligente sobre Ciberseguridad y el Llamado de Accra para el Desarrollo de la Resiliencia Cibernética, que se lanzó en Accra en noviembre de 2023 durante el Conferencia Mundial sobre Creación de Capacidad Cibernética (GC3B).



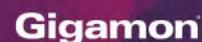
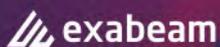
Somos Exclusive Networks.

Especialista global en ciberseguridad de confianza.

Somos líderes en tecnologías innovadoras de ciberseguridad y proporcionamos servicios para acelerar la venta de tecnologías disruptivas de ciberseguridad e infraestructura digital a escala global. Desde Exclusive Networks ayudamos a los proveedores de ciberseguridad a expandir sus negocios a nivel mundial, y ofrecemos a nuestros socios de canal experiencia, tecnologías disruptivas y servicios para satisfacer las necesidades de sus clientes.

ARISTA

BITSIGHT



www.exclusive-networks.com/es

CENTRO CRIPTOLÓGICO NACIONAL: 20 años dedicados a la protección y defensa de la ciberseguridad en España

El Centro Criptológico Nacional del Centro Nacional de Inteligencia celebra este año su **vigésimo aniversario**, conmemorando así la publicación del Real Decreto 421/2004 que establecía el ámbito de actuación y las funciones del **primer organismo español con competencias en materia de ciberseguridad**. Se plasmaba entonces la apuesta firme y decidida del CNI por la protección del ciberespacio español.

Los orígenes del CCN habría que buscarlos en el propio Centro. Allí, a principios de la década de los 80, se había formado un departamento con un grupo reducido de profesionales con un amplio conocimiento en materia de amenazas, vulnerabilidades y riesgos de los sistemas de información y comunicaciones. Su misión principal entonces era el desarrollo de material de cifra y algoritmos para la protección de la información clasificada, el desarrollo de requisitos de seguridad para estos sistemas y la acreditación de los mismos. Todo ello, siguiendo la línea trazada en materia de seguridad de las TIC por los países avanzados y por las organizaciones internacionales en las que nos integramos en aquellos años: OTAN y Unión Europea. Su vocación de servicio y su capacidad de vislumbrar estas amenazas los llevó a formar y capacitar al personal de la Administración Pública y compartir su conocimiento con todos ellos.

En el RD 421/2004 se estableció el ámbito de actuación y las funciones del CCN, primer organismo español con competencias en materia de ciberseguridad. Se plasmó entonces la apuesta firme y decidida del CNI por la protección del ciberespacio español.

A lo largo de estos 20 años, y gracias a la acción tanto de los hombres y mujeres que lo componen como de un grupo importante de expertos colaboradores, el CCN se ha convertido en un referente nacional e internacional en materia de ciberseguridad, volcado en **proteger, defender y fortalecer la ciberseguridad de España** ante las ciberamenazas que puedan atentar contra la seguridad nacional, el Estado de derecho, la prosperidad económica y el normal funcionamiento de nuestra sociedad y de las administraciones públicas españolas.

Hemos sido testigos de la evolución del panorama de las ciberamenazas hasta llegar al contexto geoestratégico actual, complejo y marcado, cada vez más, por la omnipresencia de la digitalización que ha llevado a un incremento preocupante en el número y sofisticación de los ciberataques. Una situación aprovechada por los agentes de la amenaza que no dudan en utilizar las técnicas de la ciberdelincuencia para alcanzar sus objetivos estratégicos. Así, los ataques complejos esponsorizados por Estados, el secuestro de sistemas y la extorsión (*ransomware*), la industrialización de las herramientas de ataque y el mercado negro de venta de credenciales o las campañas de desinformación, se han erigido como nuevas formas de desestabilización a las que es preciso hacer frente.

En esta evolución, la prioridad del CNI ha sido siempre proteger la información y el patrimonio tecnológico de nuestro país. Para ello, hemos participado en toda la legislación desarrollada en la materia como puede ser las dos **Estrategias Nacionales de Ciberseguridad**, el **Esquema Nacional de Seguridad** o la trasposición de la **Directivas NIS** al ordenamiento jurídico español.

Servicios, proyectos e iniciativas lideradas por el CCN

A lo largo de estas dos décadas, hemos potenciado las acciones de **prevención, detección y respuesta** a los ciberataques. En 2006 creamos el **CCN-CERT**, que como **CERT Gubernamental Nacional** tiene responsabilidad sobre sistemas clasificados, del sector público y de empresas de interés estratégico (ha gestionado más de **medio millón de incidentes**).

Tras el incidente de WannaCry, detectamos la necesidad de habilitar espacios donde compartir la información sobre ciberataques entre sector público y privado. Por ello, activamos el grupo **CSIRT.es** (que ahora mismo cuenta con más de 70 miembros) y, en 2022, potenciamos la **Red Nacional de SOC**, un proyecto pionero en Europa para coordinar la colaboración y el intercambio de información, con vistas a su futura integración con otros foros nacionales como el propio **CSIRT.es** o internacionales como la **Red Europea de SOC** (ENSOC).

Hemos sido los principales impulsores de la implantación del **ENS** en las administraciones públicas, en la **formación y capacitación de personal** especialista y hemos publicado centenares de normas, instrucciones y recomendaciones, con más de 550 guías CCN-STIC disponibles en nuestra web.

Capítulo destacado tiene todo lo relativo al fomento y certificación de productos y servicios seguros. Así, constituimos el **organismo de certificación** del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información y lideramos la promoción y desarrollo de productos TIC confiables, elaborando desde 2017 el **Catálogo de Productos y Servicios STIC**, en constante actualización.

Cabe destacar también el impulso al desarrollo de nuevas herramientas tecnológicas, con **25 soluciones de seguridad** (LUCIA, REYES, IRIS, microCLAUDIA, OLVIDO, INES, entre otras); el **Sistema de Alerta Temprana**, con más de 500 sondas desplegadas; o el desarrollo de la **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes** en coordinación con los otros CSIRT de referencia (Mando Conjunto del Ciberespacio e INCIBE) y que permite el intercambio ágil de información relacionada con ciberataques.

Este ánimo de colaboración nos ha llevado a organizar las que con el tiempo se han convertido en el principal encuentro de ciberseguridad celebrado en España: las **Jornadas STIC**, cuya próxima edición internacional será en el mes de abril en Panamá.

Son pues 20 años de intensa actividad en las que el CCN, como instrumento del CNI al servicio de la ciberseguridad nacional, ha alcanzado una experiencia clave para que nuestro país sea capaz de evolucionar, adaptarse y responder de forma eficiente a los retos que nos plantea este ciberespacio transversal y global.



ESPERANZA CASTELLEIRO
Secretaria de Estado Directora
Centro Criptológico Nacional-CCN
Centro Nacional de Inteligencia-CNI



EAGLESIGHT

MNEMO

*Tu nivel de salud en Ciberseguridad, medido,
accesible y accionable en todo momento*

Casi un **50%** de las vulnerabilidades de ciberseguridad se deben a errores de diseño o mantenimiento de tus sistemas. MNEMO te ayuda a reducir tu superficie vulnerable antes que los ciber criminales y a gestionar su remediación.



Solicita tu prueba gratuita ▶



info@memo.com
Mnemo
memo.com

Se presentó también un informe para proponer una hoja de ruta hacia un sistema financiero cuántico seguro

El WEF sitúa al cibercrimen y la inseguridad cibernética entre los principales retos a dos y 10 años, con un impacto incierto de las nuevas tecnologías

La inseguridad cibernética sigue ocupando un lugar destacado entre los principales problemas de los que alerta el 'Informe de Riesgos Globales 2024' del Foro Económico Mundial (WEF), tanto en el horizonte temporal a corto plazo (dos años), como a una década. En el documento, publicado a principios de enero, figuran casi los mismos riesgos —o muy similares— tanto a corto (dos años), como a largo plazo (una década), incluidos la “confrontación

geo-económica” y la “erosión de la cohesión social y polarización social”, junto con dos nuevos en los primeros puestos: el “cibercrimen generalizado y la inseguridad cibernética” y la “migración involuntaria a gran escala”. De hecho, según destaca el documento, la tecnología exacerbará las desigualdades —también se alerta de la incertidumbre que generará la IA—, mientras que los riesgos de la inseguridad cibernética seguirán siendo una preocupación constante.

“El mundo enfrenta una serie de riesgos que parecen completamente nuevos y al mismo tiempo inquietantemente familiares”, recuerda el documento que explica

RIESGOS GLOBALES 2024, A CORTO Y LARGO PLAZO



que, en su nuevo ranking, están el regreso de riesgos “antiguos” —como la inflación, la crisis del coste de la vida, guerras comerciales, salidas de capital de los mercados emergentes, malestar social generalizado, confrontación geopolítica y el espectro de una guerra nuclear—.

El informe recuerda que “el entrelazamiento cada vez mayor de las tecnologías con el funcionamiento crítico de las sociedades está exponiendo a las poblaciones a amenazas internas directas, incluidas aquellas que buscan destruir el funcionamiento social”. Así, alerta de que, junto con un aumento de los delitos cibernéticos,

“los intentos de alterar recursos y servicios críticos basados en la tecnología se volverán más comunes, y se prevén ataques contra la agricultura y el agua, los sistemas financieros, la seguridad pública, el transporte, la energía y la infraestructura de comunicaciones doméstica, espacial y submarina”.

También, destaca que “el análisis sofisticado de conjuntos de datos más grandes permitirá el uso indebido de información personal a través de mecanismos legales legítimos, debilitando la soberanía digital individual y el derecho a la privacidad, incluso en regímenes democráticos bien regulados”.

Tecnología cuántica y sector financiero

Por otro lado, el WEF también ha hecho público un informe, junto con la Autoridad de Conducta Financiera (FCA), con el que pretende trazar la hoja de ruta hacia un sistema financiero cuántico seguro —en el que se prevé una inversión global de 19.000 millones de dólares para 2030—. Además de las enormes oportunidades económicas, el informe advierte que la transición de lo digital a

lo cuántico también desatará nuevas ciberamenazas que podrían amenazar la seguridad y la infraestructura digital actuales e, incluso, erosionar la confianza y la estabilidad de las que depende el sistema financiero global.

“El sector financiero depende en gran medida del cifrado para proteger información confidencial, cuya exposición podría causar un daño significativo a los consumidores y los mercados”, ha destacado el jefe de Resiliencia Tecnológica y Cibernética de la FCA, **Suman Ziaullah**. “Abordar esto requiere un esfuerzo verdaderamente colaborativo para hacer la transición hacia un futuro cuántico seguro”.

Las tres AUTORIDADES EUROPEAS DE SUPERVISIÓN publican el primer conjunto de proyectos finales de normas técnicas dentro de la Ley DORA

Las tres **Autoridades Europeas de Supervisión (EBA, EIOPA y ESMA, las AES)** publicaron, a principios de año, el primer conjunto de proyectos finales de normas técnicas en el marco de la Ley de Resiliencia Operacional Digital (DORA).

Así, en ellos se incluyen desde Normas Técnicas Regulatorias (RTS) sobre el marco de gestión de riesgos de TIC y sobre el marco simplificado de gestión de riesgos de TIC, hasta RTS sobre criterios para la clasificación de incidentes relacionados con las TIC, especificaciones en cuanto a la política sobre servicios de TIC que respaldan funciones críticas o importantes proporcionadas por proveedores externos de servicios de TIC (TPP), así como la forma de implementar Normas Técnicas

(ITS) para establecer las plantillas para el registro de información, entre otros aspectos.

A través de este documento los profesionales pueden disponer de un borrador de RTS sobre el marco de gestión de riesgos de TIC, que identifica otros elementos relacionados con la gestión de dichos riesgos con miras a armonizar herramientas, métodos, procesos y política, además de los criterios específicos para la clasificación de incidentes importantes o los aspectos más destacados de los acuerdos de gobernanza, gestión de riesgos y marco de control interno que las entidades financieras deben tener en vigor



con respecto al uso de proveedores externos de servicios de TIC. Su objetivo es garantizar que las entidades financieras mantengan el control de sus riesgos operativos, la seguridad de la información y la continuidad del negocio durante todo el ciclo de vida de los acuerdos contractuales con dichos proveedores.

Tras su presentación a la **Comisión Europea**, ésta comenzará a trabajar en su revisión con el objetivo de adoptar estas primeras normas en los próximos meses.

**CUANDO LAS BARBAS DE TU
VECINO VEAS QUEMAR...**



**GESTIONAMOS LA SEGURIDAD
DE TUS THIRD PARTY**

www.zerolynx.com



INCIBE adjudica más de 150 millones de euros a 82 empresas en su iniciativa de Compra Pública de Innovación

El Instituto Nacional de Ciberseguridad (Incibe) ha adjudicado, a fecha de cierre de esta edición de SIC, 150,5 millones de euros a 82 empresas, dentro del ámbito de la denominada Compra Pública de Innovación (IECPI) —el organismo ha publicado un mapa con las empresas adjudicatarias—, para el desarrollo de 142 proyectos. Esta iniciativa estratégica “tiene como objetivos el desarrollo de soluciones y servicios de alto valor de innovación, en materia de ciberseguridad, el fortalecimiento de las capacidades y el impulso del talento”. La IECPI está dotada con un presupuesto de 224 millones de euros y, por ahora, ha realizado tres convocatorias activas. Desde el Incibe resaltan que, de momento, el 42% de las propuestas han finalizado de manera satisfactoria la primera fase.

UBICACION DE LAS EMPRESAS ADJUDICATARIAS DE FONDOS PARA COMPRA PÚBLICA INNOVADORA



dades del Centro de Coordinación Nacional (NCC-ES) —del que ha sido designado Incibe— por parte de España. La Comisión Europea ha impulsado este proyecto (lo cofinanciará al 50%) para fortalecer las capacidades de los 27 centros de dicha red, uno por cada estado miembro, para apoyar la transformación digital, aumentar la ciberresiliencia y conectar los ecosistemas nacionales con la propia red del Centro Europeo de Competencia en Ciberseguridad (ECCC).

Además, a finales de enero, Incibe celebró un ‘InfoDay’, en el que explicó las seis nuevas convocatorias en ciberseguridad del Digital Europe Programme (DEP), abiertas hasta el 26 de marzo, donde se movilizarán 84 millones de euros, con seis líneas de financiación —se aceptan propuestas hasta el 26 de marzo—. Estarán enfocadas a actividades de apoyo a los Centros de Operaciones de Seguridad (SOC) con aplicaciones novedosas de

IA y otras tecnologías facilitadoras; la aplicación de la legislación de la UE sobre ciberseguridad, como la Ley de Ciberresiliencia, y especialmente entre pymes; y la transición europea a la criptografía postcuántica. Además, Maite Boyero, de CDTI, avanzó que en junio el Cluster 3 de Horizonte Europa convocará cuatro proyectos, por 71,4 millones.

Sumando fuerzas con la OCC

También, es de resaltar la firma de un convenio entre la Secretaría de Estado de Digitalización e IA (SEDIA), y la de Estado de Seguridad (SES), a través del Incibe, el Centro Nacional

de Protección de Infraestructuras Críticas (CNPIC) y la Oficina de Coordinación de Ciberseguridad (OCC).

El acuerdo, entre otros aspectos, recoge la coordinación de todas las actuaciones en el ámbito de la protección de las infraestructuras críticas y de los servicios esenciales y destaca que Incibe-CERT será operado conjuntamente por el Instituto y la OCC en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.

Por último, el Instituto dio a cono-

cer que, a través de un acuerdo entre Castilla y León y Euskadi, en el ámbito del programa Retech financiará con 14,3 millones el Proyecto Red-Argos para impulsar y fortalecer el ecosistema nacional de ciberseguridad a través del trabajo en Red de Nodos de Ciberseguridad regionales coordinados y la generación de capacidades especializadas en ámbitos estratégicos como la movilidad, el sector aeroespacial, energía, industria inteligente, salud y ciudades inteligentes.



Además, el Incibe firmó en enero ocho convenios para reforzar la ciberprotección y ciberresiliencia de más de 840 empresas del sector privado de la automoción, pertenecientes a los principales clústeres de todo el territorio español.

Por otro lado, poco después de tomar posesión, el ministro de Transformación Digital, José Luis Escrivá, visitó la sede del Incibe, en la que conoció sus retos y proyectos, así como su servicio ‘Tu Ayuda en Ciberseguridad’.

Capacidades europeas

El Instituto también está ejecutando el proyecto europeo ‘National Coordination Centre-Spain’, dotado con 1,2 millones de euros, con el objetivo de aumentar las capaci-



CCN celebra su 20º aniversario: dos décadas dedicadas a la protección y defensa de la ciberseguridad de España

El Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI), celebra este año su 20º aniversario y conmemora la publicación, hace ahora dos décadas, del Real Decreto 421/2004 que establecía su ámbito de actuación y funciones como primer organismo español con competencias en materia de ciberseguridad. Desde entonces, ha desarrollado una labor incansable, siendo un referente europeo en este ámbito y con importantes hitos como su contribución al desarrollo de las dos Estrategias Nacionales de Ciberseguridad existentes hasta la fecha, su apuesta por la implementación del Esquema Nacional de Seguridad (ENS) y su trabajo en la trasposición de la Directiva NIS. Además, ha impulsado el desarrollo de 23 soluciones de seguridad (Lucía, Reyes Iris, microClaudia, Olvido, Inés y Ángeles, entre otras), así como del Sistema de Alerta Temprana para

la detección en tiempo real de amenazas, que cuenta con más de 500 sondas desplegadas en la Administración y la puesta en marcha de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

Entre sus últimas novedades, su Departamento de Productos y Tecnologías del Centro Criptológico Nacional (CCN-PYTEC) ha presentado metaOLVIDO, una solución pensada en la gestión y tratamiento de metadatos.

Capacidades de respuesta

Asimismo, el CCN potenció las acciones de prevención, detección y respuesta a los ciberataques a través de la puesta en marcha, en 2006, del



CCN-CERT, que en 2023 gestionó 107.777 incidentes, un 34% de ellos con una peligrosidad alta, muy alta o crítica. Esta experiencia le ha llevado a liderar la Red Nacional de SOC (RNS), que se integrará con otros foros nacionales como CSIRT.es o internacionales como la Red Europea de SOC (ENSOC).

También ha sido notable su actividad formativa con centenares de normas, instrucciones, informes y recomendaciones, y más de 550 Guías CCN-STIC publicadas —la última su ‘Aproximación a la IA y la Ciberseguridad’—. Además, el CCN es el organismo de certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las TI y, desde 2017, elabora el Catálogo de Productos y Servicios STIC.

Enfoque su escenario de ciber riesgos

Consiga una inversión en ciberseguridad más efectiva con NCC Group.

Soluciones gestionadas, de asesoramiento y evaluación de ciber riesgos centradas en cada sector para ayudarle a tener control sobre su horizonte de riesgos, aumentar la confianza con sus clientes e impulsar la transformación digital.



Experiencia avalada



Empresa global de ciberseguridad con más de 100 consultores tecnológicos y especialistas en España, y más de 800 en el mundo.

Pionero en la industria



Liderando el camino en la combinación de la mejora continua y la experiencia específica de la industria para abordar desafíos únicos y demandas regulatorias.

Adaptado a tus necesidades



A su lado 24/7 para identificar, proteger y responder a las nuevas amenazas, personalizado para su nivel de seguridad y requisitos.



¿Quiere descubrir qué y quién amenaza a su empresa?

Reciba toda la inteligencia de amenazas analizada por NCC Group cada mes en su correo. Escanee el código QR y suscríbese ya.

Contará con un presupuesto de 3,5 millones a dos años y formará parte del proyecto de Redes Territoriales de Especialización Tecnológica

NAVARRA CYBERSECURITY CENTER inicia su actividad enfocado a cinco aspectos que van desde la resiliencia, hasta la colaboración y la concienciación

Desde finales de 2023, el **Navarra Cybersecurity Center** ya es una realidad. Forma parte del proyecto 'CIBERREG', liderado por el Departamento de Universidad, Innovación y Transformación Digital del Gobierno de Navarra, que cuenta con la participación de otras siete regiones españolas y que es parte del programa Retech, impulsado por la Secretaría de Estado de Digitalización e IA. Con esta iniciativa, dotada con 3,5 millones de euros, hasta mediados de 2026 y una plantilla de tres personas en 2024, se pretende vertebrar diversos proyectos nacionales orientados a la transformación digital a través de la colaboración público-privada, permitiendo una mayor coordinación entre las comunidades autónomas y las empresas.

Así, el Navarra Cybersecurity Center nace como el centro de referencia en materia de ciberseguridad en la Comunidad y, también, como



una ventanilla única de respuesta a los servicios en esta área, que se integra en el Polo de Innovación Digital de Navarra, IRIS, iniciativas que cuentan con la coordinación de **Nasertic**. Su objetivo será impulsar iniciativas que permitan mejorar en la región la ciberresiliencia en todos los ámbitos de la Comunidad Foral (ciudadanía, tejido empresarial –con especial foco en pymes y autónomos– y administraciones públicas). Por eso, gran parte de su trabajo, al frente del que estará **Juan Ramón Aramendía** como coordinador, irá destinado a la dinamización del sector de la ciberseguridad

en la región, contribuyendo a la transformación socioeconómica sostenible de Navarra en un entorno digital, hiperconectado y ciberresiliente.

En este sentido, se han definido cinco líneas de actuación estratégicas. En primer lugar, ofrecer un servicio de atención y monitorización de amenazas, sirviendo como ven-

tanilla única de respuesta a incidentes y punto de referencia para acercar la ciberseguridad a la sociedad navarra, apoyándose para ello en los servicios que ofrece el **Incibe**. En segundo, fomentando el ecosistema empresarial: identificando los actores clave del sector en Navarra, creando un catálogo de productos y servicios, promoviendo e incentivando su consumo e impulsando la generación de nuevas empresas o líneas de negocio. También, pretende erigirse como centro demostrador para acercar las tecnologías de ciberseguridad a las empresas promoviendo su implantación, así como la integración de buenas prácticas y evaluaciones en los procesos de diseño y desarrollo de productos y servicios tecnológicos. Por último, el Centro buscará impulsar la creación de itinerarios formativos especializados, en colaboración con universidades y centros de formación profesional, con el objetivo de generar talento profesional altamente cualificado, así como la sensibilización en este ámbito través de campañas de concienciación para empresas y ciudadanía.

Juan Ramón Aramendía, Coordinador del Navarra Cybersecurity Center

“Esperamos ser un ejemplo y referente de cómo la colaboración público-privada puede dinamizar un sector como el de la ciberseguridad”

– **¿Qué ha sido lo más complicado para sacar adelante el Centro y cuáles serán objetivos prioritarios?**

– La creación del Centro ha sido un proceso laborioso que se lleva gestando desde hace más de dos años y que, finalmente, ha sido posible gracias a la persistencia del Gobierno de Navarra y la financiación del programa Retech. Personalmente, es un orgullo poder liderar este proyecto tan necesario para Navarra y cuya vocación es elevar el nivel de madurez en ciberseguridad y la ciberresiliencia de nuestra sociedad y su tejido empresarial.

– **De sus cinco retos planteados, ¿cuáles son críticos?**

– Todos son importantes, pero quizás el fomento del ecosistema empresarial tenga una especial relevancia por su interrelación con otro proyecto estratégico de reciente creación: el Polo IRIS de Innovación Digital de Navarra. Nuestro objetivo es doble,

por un lado, fomentar el crecimiento de empresas de ciberseguridad y, por otro, situar la ciberprotección en el centro de la cultura empresarial navarra.

– **¿Cómo va a trabajar junto al resto de Agencias de ciberseguridad y Centros autonómicos y de qué va a depender su éxito o fracaso?**

– El proyecto CIBERREG es un entorno colaborativo conformado por ocho comunidades autónomas. Fuera del marco del proyecto, tenemos claro que debemos apoyarnos en aquellos centros que ya tienen una experiencia contrastada, como es el caso de la Cyberzaintza en el País Vasco y otras agencias o centros autonómicos similares.

– **¿Qué marca la diferencia del Centro con otras entidades similares en España y qué espera aportar en concreto?**

– En Navarra contamos desde hace



Foto cedida por Diario de Navarra / J.C. Cordovilla

muchos años con un SOC altamente cualificado para atender a la infraestructura interna del Gobierno. La diferencia del Centro radica en su orientación hacia pymes y ciudadanía, que son colectivos vulnerables, poco concienciados y que no pueden costearse unos servicios de ciberseguridad como los de las grandes empresas o la administración.

– **Su objetivo principal para 2024...**

– Pensamos que el 'EU Cyber Resilience Act' va a tener un impacto significativo en la industria navarra y, por tanto, desde el Centro nos marcamos como objetivo ayudar a nuestras empresas a integrar la ciberseguridad en el proceso de diseño y desarrollo de productos con elementos digitales. Además, tendremos como prioridad la creación del centro de respuesta ante incidentes para ciudadanos y empresas.

– **¿Qué espera aportar el Centro al ecosistema de ciberseguridad en España?**

– Esperamos ser un ejemplo y referente de cómo la colaboración público-privada puede dinamizar un sector como el de la ciberseguridad en una comunidad pequeña pero inmersa en un ambicioso plan de transformación digital.

SIC



La Referencia en Seguridad de Endpoints **100% en la nube**



Inteligencia sobre amenazas

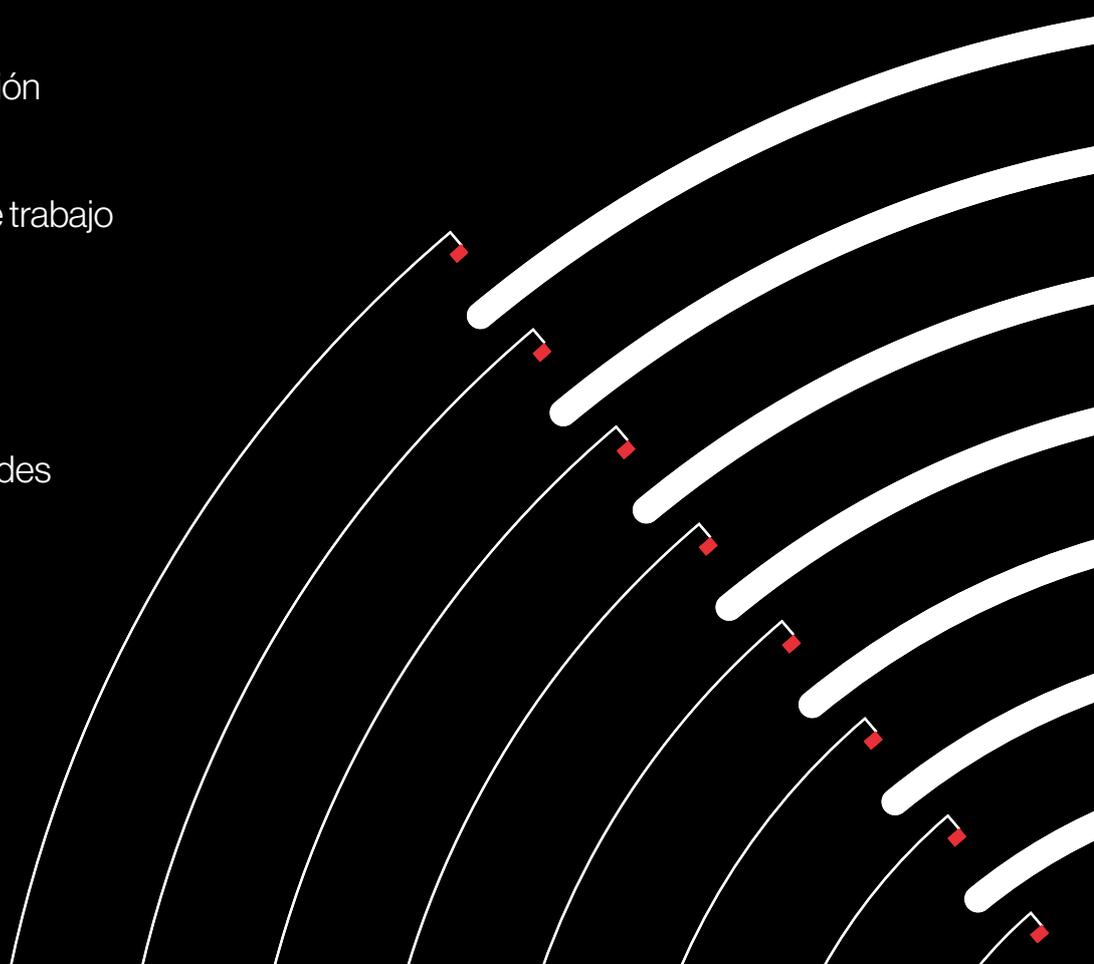
Protección de identidad

Antivirus de nueva generación

Protección de las cargas de trabajo

Control de dispositivos

Evaluación de vulnerabilidades



En un acto albergado en Bilbao en la Torre Iberdrola el pasado 20 de diciembre, la Agencia Vasca de Ciberseguridad inicia su singladura

CYBERZAINNTZA oficializa su puesta de largo con el lema de su propósito y los desafíos de ciberprotección que afronta: "Por ti hacemos red"

A finales de diciembre pasado el Vicelehen-dakari Primero y Consejero de Seguridad, **Josu Erkoreka**, presidió el acto oficial de presentación de *Cyberzaintza*, la **Agencia Vasca de Ciberseguridad**, conformada para afrontar de modo transversal e integral las amenazas derivadas del uso de internet y las nuevas tecnologías en Euskadi. Esta iniciativa, como recordarán los lectores, fue Premio SIC 2023.

En la puesta de largo, el Director General, **Javier Diéguez**, dio a conocer los retos que abordará la agencia, entre ellos la protección digital de instituciones públicas, empresas y ciudadanía, y, al tiempo, situar a Euskadi como un referente en ciberprotección dentro de una Europa digital, contribuir a romper con la dependencia tecnológica de otras economías, así como promover la formación en disciplinas de alto contenido tecnológico (*STEAM* –Ciencias, Tecnología, Ingeniería, Artes y Matemáticas–) de



las próximas generaciones, para asegurar el relevo generacional en el sector digital vasco, clave para asegurar el progreso y bienestar vascos de cara al futuro.

tiva, la cual, además de incorporar a representantes del Gobierno Vasco, las diputaciones forales, los ayuntamientos de las tres capitales y Eudel, cuenta con un Consejo Consultivo integrado por once expertos en distintas disciplinas –de ámbitos público y privado–, y con

Estado y de la Unión Europea en materia de ciberseguridad.

Como colofón a esta pretensión y ante una abarrotada audiencia en la torre Iberdrola bilbaína, aco-gedora del evento, Diéguez hizo público el lema de *Cyberzaintza*: "Por ti hacemos red", sin duda una explícita declaración de intenciones.

Como muestra de la decidida voluntad de colaboración, el resto de la jornada incluyó varios paneles que reunieron a distintos actores públicos y privados directamente concernidos con la ciberprotección (**Centro Criptológico Nacional-CCN, Gobierno Vasco, Agencia de Ciberseguridad de Cataluña, Comunidad Valenciana, Incibe, Cybasque, Grupo Santander, Iberdrola, Diputaciones**

forales vascas...), así como a **Lui-gi Rebuffi**, Secretario General de la **ECSO (European Cyber Security Organisation)**.



La puesta de largo congregó a una multitudinaria asistencia de expertos en ciberseguridad



Durante el evento se celebraron varios paneles en los que intervinieron agentes y entidades con foco en la ciberprotección

Es de reseñar que ambos intervinientes enfatizaron la singularidad orgánica de *Cyberzaintza* y su modelo de gobernanza colabora-

la firme voluntad de mantener una relación permanente con agentes relevantes del sistema, de forma alineada con las estrategias del

La biometría, principal apuesta para evitar el fraude de identidad por parte de los 'nómadas digitales'

Los llamados 'nómadas digitales', teletrabajadores internacionales, dieron pie, en 2023, a un acuerdo marco regulatorio de la UE para adaptarse a la nueva realidad laboral. Sin embargo, más allá de lo legal, según un estudio de la compañía **Regula**, también está suponiendo un quebradero de cabeza para los encargados de la gestión y control de la identidad. Y es que sólo en países como EE.UU. y Emiratos Árabes, el número de este tipo de profesionales se han incrementado en un 25% en el último año.

El problema es que los nómadas digitales deben someterse de forma rutinaria a diferentes pruebas de verificación de identidad (IDV) allí donde físicamente están y esto hace que muchas empresas incrementen el riesgo de fraude de este tipo de perfiles por no tener sistemas de gestión de la identidad adaptados a ellos. Según



un informe de la compañía, el 40% de los responsables de la toma de decisiones empresariales destacan el aumento del fraude como el principal desafío cuando se trata de la verificación de identidad de los nómadas digitales. De hecho, en países como Emiratos Árabes Unidos y México, los preguntados destacaron en un 51% y el 49% sentirse víctimas de fraude. Es significativo que el 80% de los responsables de la toma de deci-

siones asocien directamente el movimiento de los nómadas digitales con el fraude de identidad. Los sectores que más sufren este tipo de riesgo son los de seguros, seguidos de servicios financieros y bancarios.

Por ello, el 57% de las organizaciones ya ha implementado autenticación biométrica para detectar y prevenir este tipo de fraudes. Además, un 53% destacó que verifica documentos electrónicos a través del chip RFID que contienen –usados en un 61% de los casos–. También, se usan para permitir el acceso a productos y servicios corporativos con la seguridad adecuada. Sin embargo, el estudio recuerda que estas medidas no bastan y hay que apostar por un enfoque de "confianza cero en el móvil" y una tecnología de verificación NFC confiable para confirmar la autenticidad tanto del chip como de sus datos.

El enemigo ya conoce sus vulnerabilidades.

Conozca sus estrategias para protegerse de él.



Descubra por qué los CISOs eligen nuestro servicio de modelado de amenazas.

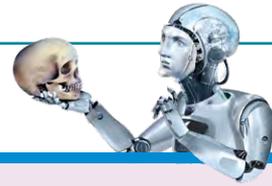
En un mundo donde los ciberataques están en constante evolución, y las responsabilidades asociadas al CISO aumentan, es crucial conocer los movimientos de los atacantes con antelación. Nuestro modelado de amenazas le brinda la información necesaria para que pueda prevenir y anticipar estos ataques y proteger la continuidad de su negocio.

Actúe ahora para fortalecer su ciberseguridad. Somos su mejor aliado para dar jaque mate a sus atacantes.

MITRE
ATT&CK



Síguenos en:      @s2grupo  s2grupo.es



2024: diario de un CISO

Ha sido un año muy intenso. Tengo ganas de pasar página, relajarme y plantearme nuevos paradigmas. Confío en que las decisiones que he tomado durante estos últimos doce meses me lleven a un mejor puerto del que partí. En el fondo, sigo siendo un ingenuo: aún me apasiona la ciberseguridad.

Desde enero reporto directamente, como CISO, al consejo de administración. No paso por el CIO ni por el COO. Impresionante, ni en mis mejores sueños hubiera imaginado semejante grado de responsabilidad en aquella flamante empresa del IBEX 35.

DIARIO DE UN CISO *En ciber no puedes convencer a nadie, sólo dejar una semilla de conocimiento y esperar que germine. Sobre todo, cuando hablas a los miembros del consejo.*

En ciber no puedes convencer a nadie. Sólo puedes dejar una semilla de conocimiento y esperar que germine. Sobre todo, cuando hablas a los miembros del consejo. Estas son algunas de las simientes que he intentado plantar en 2024.

Primero, no he mostrado necesidad, ni de recursos ni de aprobación. Simplemente, he ido proporcionando evidencias y formas de protegernos de cada uno de los ataques que hemos sufrido, desde los “deep fakes” de audio con la voz de nuestro CEO que convencieron a nuestro departamento de finanzas para pagar a una cuenta fuera de nuestro sistema una cifra millonaria, hasta la pieza de “malware” que, durante meses, estuvo filtrando información sobre nuestros clientes a una dirección IP fuera de Europa.

Segundo, he transformado el problema complejo de la ciberseguridad en una suma de elementos comprensibles dentro de un entorno de transparencia. Para cada uno de ellos, he seleccionado a un líder que ha construido un equipo multidisciplinar de protección y detección, involucrando también a nuestros proveedores. Todas las métricas de seguimiento, incluyendo nuestros objetivos, se publican en la Intranet. Todas nuestras reuniones están abiertas a toda la organización. Además, hemos acordado la definición de valor con nuestros auditores internos y externos. Las actividades que no proporcionan ese valor definido y esperado se eliminan rápido, en semanas.

Tercero, he construido alianzas con otros departamentos clave de la organización. Dos ejemplos: el primero, como en 2023 no fuimos capaces de atraer nuevo talento de ciber, apostamos por

enfocarnos en la diversidad de nuestros colegas. Hemos entrenado y formado, en sintonía con el departamento de recursos humanos, de forma divertida, compitiendo con otras formaciones online, a empleadas internas que querían dar un cambio a su vida profesional y sentirse valoradas. Hemos demostrado que podemos identificar y cultivar talento dentro de nuestra empresa. El segundo ejemplo, colaboramos día a día con nuestro departamento de comunicaciones: informamos a nuestros clientes sobre elementos de seguridad que implementamos día a día a través de los canales y redes sociales que prefieran.

Cuarto, me he rodeado de buenos profesionales y mejores personas, capaces de hacer suyos nuestros objetivos de desarrollo sostenible. Una mezcla heterogénea: desde psiquiatras, antropólogos, científicos de datos, y algún que otro ingeniero. Todas las evaluaciones, salarios y condiciones del departamento del CISO son conocidas por todos sus miembros. Mi apuesta personal para todos mis colaboradores es clara: su valor profesional aumenta en el mercado por el hecho de trabajar con nosotros.

Quinto y último, he creado un grupo de voluntarios que siguen los avances sociales que ya nos están impactando: las implementaciones de inteligencia artificial, la personalización que requieren los clientes en la provisión de los servicios que compran, los nuevos modelos de negocio que están apareciendo con una frecuencia cada vez mayor, las nuevas regulaciones europeas que entran en vigor en 2025 y, finalmente, las opciones reales de protección que ofrecen los ciberseguros.

Quién sabe, quizá haya sido este mi último año completamente dedicado a la ciber. Cada vez me atrae más la posibilidad de enseñar: cambiar la vida, a mejor, de profesionales, jóvenes o no, motivados para aprender de la experiencia de aquellos que comenzamos nuestra carrera profesional en el mundo de la seguridad hace ya algunas décadas. Estoy deseoso de contarles en primera persona todo lo que me hubiera encantado haber leído o escuchado cuando comencé mi andadura profesional.

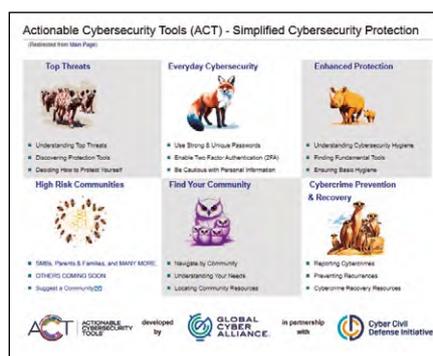


Dr. Alberto Partida

[linkedin.com/in/albertopartida](https://www.linkedin.com/in/albertopartida)

ACT, la wiki de ciberseguridad, impulsada por la GLOBAL CYBER ALLIANCE ya supera los 1.500 recursos gratuitos

La **Global Cyber Alliance** ha creado ‘Actionable Cybersecurity Tools (ACT)’, una wiki especializada en ciberprotección que ofrece más de 1.500 herramientas y recursos para ayudar a las personas y profesionales a encontrar soluciones en este ámbito a sus principales retos. Desarrollada para que cualquier, sin altos conocimientos, la pueda sacar partida y en colaboración con otras iniciativas como **CyberPeace Institute** y **Cyber Readiness Institute** gran parte de sus recursos están dirigidos para colectivos sobre lo que se centran gran parte de los ataques como ONGs, entidades educativas, periodistas, familias, pymes...



En definitiva, ACT busca “democratizar el acceso a las soluciones adecuadas que satisfagan las necesidades de la gente”, explica la Strategic Communications de la asociación, **Marina Calvo**. Por ello, entre otras, incluye desde soluciones comerciales, hasta gubernamentales, de código abierto y de comunidades. También ofrece información para identificar dónde hay vacíos o falta de recursos frente a determinados ciberriesgos. Tampoco falta un apartado para facilitar la colaboración entre los profesionales de la ciberseguridad, proveedores de servicios y herramientas. De momento, sólo está en inglés, aunque se ofrecerá en otros idiomas en un futuro.

25 años

Expertos en Cross-Domain

Tecnologías propias certificadas
PSTgateways y PSTdiode



CC Hasta EAL4+



Incluido en NIAPC

Autek Ingeniería, S.L.
info@auttek.es | www.auttek.es

auttek 

25
años

El mercado corporativo de ciberseguridad en España, en constante ascenso, superará los 2.300 millones de euros en 2024

Según estimaciones de **Revista SIC**, que lleva realizándolas desde el año 2000, referidas exclusivamente a la actividad del mercado corporativo de ciberseguridad –no directamente residencial– en España y algunas áreas de influencia, el sector facturó en 2023 la cifra de 2.106 millones de euros, experimentando un crecimiento promediado del 9% respecto del año anterior, en tanto que su proyección estimada para este 2024 experimentaría un incremento de entre el 10% y el 12% promediado, situando la facturación en órdenes de los 2.338 millones de euros previsto para este año. Con todo, esta previsión aún podría ir al alza derivada del agravamiento de los conflictos internacionales y el alboroto derivado por una Inteligencia Artificial sin embriidar.

La inestabilidad digital auspiciada por la eventual manipulación de elecciones a lomos de *fakes* nutridos por IA contaminantes, el acelerón legislativo europeo –marco regulatorio de IA incluido–, los conflictos y escaramuzas cibernéticas Rusia-Ucrania e Israel-Palestina, la intensa y continua amenaza de chantajes y extorsiones por la proliferación de *ransomware* crecientemente agresivo y muy evolucionado, así como unas administraciones públicas espoleadas por su precariedad defensiva y con el viento a favor de la eclosión de SOC's y exigencias de ENS, nuevas agencias y cen-



tros de ciberprotección territoriales y el ansiado arranque de los nodos Rethec autonómicos bajo el auspicio del maná de la UE encauzados por **Incibe**, podría disparar estas estimaciones.

Asimismo, el mercado laboral viene registrando en este periodo una importante convulsión propiciando un inusitado trasiego de profesionales en el sector oferente y demandante. De la misma manera, continúa causando serias distorsiones en el capítulo de salarios y remuneraciones ante la acusada falta de especialistas en algunas

funciones y, paradójicamente, el subidón salarial desproporcionado demandado por algunos técnicos de escueta trayectoria. A día de hoy, el efecto de la IA en este ámbito es una incógnita y los suministradores de provisiones en esto dan palos de ciego.

Por último, cabe precisar que estas estimaciones de SIC hacen referencia exclusivamente a las actividades mercantiles del sector con clientes empresariales (privados y públicos) que aglutinarían las actividades de consultoría/asesoría, prescripción, implantación de he-

rramientas y soluciones, licencias/mantenimiento/actualización, externalización de servicios (mayormente MSSPs) y en la nube, auditoría, personal externo, formación y seguros (en fase de encarecimiento e, incluso, de repliegue por acusados contratiempos en ciberpólizas mal confeccionadas y/o con cobertura inapropiada). De este conjunto de actividades quedan excluidas las referidas a la estrictamente jurídicas de protección de datos personales (que no las TIC) y a la I+D+i de laboratorios, centros de investigación y universidades.

El BCE analizará la capacidad para recuperarse de un ciberataque de 109 entidades, entre ellas BANCO SANTANDER, CAIXABANK y CAJAMAR

El **Banco Central Europeo (BCE)** llevará a cabo, en 2024, una prueba de resistencia cibernética a 109 bancos supervisados directamente, entre ellos tres españoles: **Banco Santander, CaixaBank y Cajamar**. El ejercicio evaluará cómo las entidades son capaces de responder y recuperarse de un ciberataque, más que su capacidad para prevenirlo. En concreto, se simulará, en una primera fase, un incidente que logra perturbar las operaciones comerciales diarias del banco para comprobar qué medidas de respuesta y recuperación ponen en marcha, incluida la activación de procedimientos de emergencia y planes de contingencia, y el restablecimiento de las operaciones normales. Posteriormente, los supervisores evaluarán hasta qué punto los bancos pueden hacer frente a tal escenario.

Además, 28 bancos se someterán a una 'evaluación mejorada' para la que deberán presentar información adicional sobre cómo afrontar esta prueba de estrés. Se trata de comprobar, mediante una muestra representativa, que existe una coordinación eficiente con otras actividades de supervisión.



Eso sí, este ejercicio será predominantemente cualitativo y no tendrá ningún impacto, ya que se trata de utilizar los conocimientos adquiridos para una evaluación supervisora más amplia. Por ello, la prueba servirá para que los supervisores discutan los hallazgos y las lecciones aprendidas con cada banco, como parte del Proceso de Revisión y Evaluación Supervisora de este año que busca evaluar el perfil de riesgo individual de un banco. Los principales hallazgos del ejercicio se comunicarán este verano.

Como es sabido, el BCE lleva a cabo pruebas de resistencia de supervisión anualmente, de conformidad con el artículo 100 de la Directiva sobre requisitos de capital, y cada dos años participa en una prueba de resistencia, a nivel de la Unión Europea, coordinada por la **Autoridad Bancaria Europea**.

Tu escudo infalible en la era digital

Asegura tu futuro digital con nuestro nuevo SOC



La Inteligencia Artificial y el aprendizaje automático desempeñarán un papel fundamental en las amenazas cibernéticas del futuro.

En un entorno geopolítico complejo, la adopción de tecnologías basadas en la nube avanzará significativamente, abriendo a su vez nuevas vías de ataque que la ciberdelincuencia aprovechará para infligir el máximo daño posible.

Tu seguridad no puede esperar, apóyate en el mejor partner para asegurar tu transformación digital.

Ponte en contacto con DXC Technology.

 www.dxc.com/us/en/contact-us

CONTACTA





Compras millonarias como la de VMWARE por BROADCOM y JUNIPER por HPE auguran un 2024 que continuará la efervescencia del año pasado

A pesar de los avances en ciberprotección, el cibercrimen continuó en 2023 obteniendo ingresos millonarios: sólo en EE.UU., según Statista, se calcula que causó unas pérdidas de 294.000 millones de euros el pasado año, lo que supone un incremento de 270.000 desde 2017. Frente a ello, el mercado de ciberseguridad no dejará de crecer y el analista Grandview Research predice que lo hará a una tasa anual de 12,3% hasta 2030, cuando alcance un valor estimado de casi 475.000 millones de euros. En lo que respecta a 2024, el informe 'Perspectivas de la industria de la ciberseguridad global 2024: una mirada hacia el futuro del panorama cibernético' de MarketsandMarkets, vaticina un incremento del 10%, pasando de los 175.400 millones en 2023 a los 191.500 este año.

Por volumen, es significativo que el grupo integrado por Palo Alto Networks, IBM, Microsoft, Cisco, Broadcom, Fortinet, AWS, Trellix, Check Point, Oracle, Trend Micro, Open Text, Akamai y Accenture consiguieron hacerse con un 25% del mercado en 2022, según MarketsandMarkets.

“A lo largo de 2023, los provee-

definitivo, por parte del gigante Broadcom, para adquirir VMware por casi 64.000 millones de euros, además de la adquisición por parte de HPE de Juniper Networks, por casi 13.000 millones. Una operación esta última que se espera esté cerrada a finales de 2024 o principios de 2025. Por su parte, la zarandeada

Okta cerró el acuerdo para adquirir a la israelí Spera Security, para mejorar su propuesta de monitorización de cuentas posiblemente maliciosas y detectar configuraciones incorrectas, ya que su tecnología, según destaca ella misma, “brinda a los equipos de seguridad visibilidad en tiempo real de toda su superficie de identidad”, y por su parte Delinea adquirió Authomize, pionero en la detección y eliminación de amenazas basadas en la identidad a través de la nube, para reforzar sus soluciones Extended PAM con

en la nube. Además, Branddocs Inc, un destacado proveedor de transacciones digitales seguras y servicios de verificación de vídeo, compró TrustCloud Inc, centrada en transacciones digitales seguras.

Mercado ibérico

En España, la incertidumbre del destino de Minsait, a instancias de la estrategia de su matriz, sigue dando que hablar. Así recientemente se dio a conocer que Indra podría estar estudiando la venta de su división tecnológica por un montante que podría rondar los 1.600 millones de euros, de la que forman algunas de sus empresas de ciberseguridad como la potente SIA y la recientemente adquirida ICA Sistemas, entre otras. Una operación que con alta probabilidad podría fraguarse a lo largo de este 2024. De momento, a través de Minsait Payments se consumió la compra de Pecunpay, con la que espera mejorar su posicionamiento ante fintechs y neobancos, con una oferta de pagos más amplia.

Rondas de financiación

En este ámbito, fue notable la operación de Lynx Financial Crime Tech, participada por Banco Santander, que anunció una ronda de financiación de 17 millones de euros liderada por Forgepoint Capital para combatir el fraude y los delitos financieros. Además, Risk Ledger, por su parte, recaudó 7,3 millones de euros para fortalecer su propuesta de ciberprotección en las cadenas de suministro, y Vicarius, consiguió 27 millones.



Broadcom compra VMware, HPE a Juniper, Airbus se interesa por Evidian, de Atos, Palo Alto Networks adquiere Talon, Cisco a Isovalent, SonicWall a Solutions Granted y Banyan Security, Okta a Spera; en España Indra estudia la venta de su división Minsait, de la que forman parte SIA e ICA, entre otras.

dores cambiaron su énfasis hacia la innovación de productos y la integración de la IA. Y en 2024, los proveedores de seguridad estarán posicionados para encabezar la innovación, reforzando las medidas defensivas e introduciendo iniciativas que señalen una era resiliente de protección, estrategias proactivas y resiliencia contra amenazas en continua evolución”, resalta en su informe, que predice un año marcado por “la adopción de soluciones XDR en entornos IT-OT, los esfuerzos de los gobiernos para combatir la amenaza de deepfakes, las estrategias de los CISO para mejorar la resiliencia cibernética y la transición hacia una seguridad sin contraseñas y sin perímetros”.

De cualquier forma, en 2023, según SecurityWeek, se registraron 413 acuerdos y fusiones, un 8% menos que en 2022.

Entre las operaciones más llamativas en este último trimestre destacaron el cierre del acuerdo

Atos anunció de forma oficial la recepción de una oferta indicativa de Airbus para un acuerdo estratégico y tecnológico a largo plazo y adquirir una participación minoritaria del 29,9% en Evidian, especializada en la gestión de identidades y accesos.

Por su parte, Palo Alto Networks compró Talon Cyber Security para mejorar su propuesta de SASE AI, a través de lo que se denomina ‘tecnología de navegadores empresariales’, de la que la compañía es una de las pioneras. Cisco anunció la adquisición de Isovalent para reforzar su propuesta de ciberprotección en la nube.

Además, SonicWall se ha hecho con Solutions Granted, especializada en servicios de detección y respuesta gestionados hechos a medida para los MSPs/MSSPs, así como con Banyan Security, un proveedor de soluciones de borde de servicios de seguridad (SSE).

En los ámbitos de identidad,

el objetivo de detectar y mitigar las amenazas a la identidad y el acceso en la nube. Así, a partir de ahora, las capacidades CIEM e ITDR de Authomize se entregarán a través de la Plataforma Delinea nativa de la nube, añadiendo profundidad a la ejecución de la visión de la compañía para extender PAM en las empresas modernas.

En cuanto a Accenture prosigue con su intensa actividad en adquisiciones y así completó la compra de la consultora tecnológica, con sede en Reino Unido, 6point6, especializada en nube, datos y ciberseguridad.

SentinelOne anunció que adquirirá PingSafe, conocida por su plataforma de protección de aplicaciones nativas en la nube (CNAPP), para combinarla con sus capacidades de seguridad de cargas de trabajo cloud y seguridad de datos, y ofrecer una plataforma totalmente integrada que impulse una mejor cobertura, higiene y automatización en toda su huella



Gestiona **tu futuro** con operaciones de seguridad **cloud-native**

CyberProof permite a las empresas globales anticiparse, adaptarse y responder a las ciberamenazas de forma eficiente en su transición a entornos cloud-native con servicios avanzados de detección y respuesta gestionada.

CyberProof[®]
A UST Company

 @CYBERPROOFINC

 @CYBERPROOF-INC.

 WWW.CYBERPROOF.ES

TELEFÓNICA: 100 años conectando la vida de las personas de forma segura

Telefónica ha llegado hasta aquí porque ha sabido transformarse, anti- cipándose siempre a su tiempo y con una misión clara: dar servicio y ser de utilidad a la sociedad, donde la seguridad de los clientes y las comunicaciones ha sido un elemento fundamental en esta misión.

Como dice nuestro Presidente Ejecutivo José María Álvarez-Pallete, “Telefónica es una historia apasionante de constante transformación”, y la transformación de la ciberseguridad en Telefónica también ha sido constante y especialmente apasionante.



En los inicios la seguridad física tenía casi todo el protagonismo, pero fue a mediados de los años 90 con el Internet comercial impulsado por Infovia

cuando la “seguridad informática” empieza a crecer en protagonismo, tanto en Telefónica como en muchas otras grandes empresas.

La función de seguridad informática interna estaba repartida en las áreas de sistemas y de red, así como en las áreas de seguridad corporativa dependientes de las áreas legales. Existían funciones globales que buscaban la coordinación de las áreas de seguridad de los países y lideraban la relación con otras empresas y organismos nacionales e internacionales.

Unificación

En 2017, se unificaron todas las funciones de seguridad, acorde a una nueva política global de seguridad, bajo el liderazgo de la Dirección Global de Seguridad e Inteligencia, con una sólida coordinación global, para funcionar como un equipo y estar mejor preparados frente a las nuevas ciber amenazas (como lo fue el WannaCry). Al CISO se le bautizó como responsable de la función de Seguridad Digital, con una dimensión más ambiciosa que unificara la seguridad de la información y la ciberdefensa, apostando por desarrollar las funciones de ciberinteligencia, la detección y la respuesta a incidentes.

En los últimos años se han desarrollado internamente capacidades de ciberdefensa propias, que han permitido a Telefónica ir más allá de lo que ofrece el mercado y ser más eficaces y eficientes en la anticipación, detección y respuesta. Durante este tiempo, también se ha reforzado el posicionamiento de la seguridad digital en la agenda de las Comisiones y de la Alta Dirección, existiendo un compromiso con aquella al máximo nivel. De igual manera, se han desarrollado capacidades de mando y con-

trol que refuerzan otras funciones de seguridad, como la gestión de crisis o la prevención del fraude.

Y desde siempre, Telefónica ha creído en la colaboración público-privada y privada-privada, participando en diversos foros tanto a nivel nacional como internacional.

Actualmente, la seguridad digital interna de Telefónica goza de madurez, pero si hemos podido ver más lejos es porque hemos estado subidos a hombros de gigantes, que son todos los “telefónicos” que durante años han dedicado su esfuerzo a que la seguridad digital interna de Telefónica haya mejorado día a día.

Paralelamente a esta transformación, Telefónica se ha consolidado como integrador de productos y servicios de ciberseguridad, cuya oferta hacia el cliente actualmente se canaliza a través de Telefónica Tech, que ha ganado por méritos propios convertirse en un proveedor de referencia y un socio de confianza en el mercado de ciberseguridad en los países en los que tiene presencia.

Durante cien años, Telefónica ha estado anticipándose y adaptándose a los nuevos retos de seguridad. Y los que hay por delante sin duda serán mayores, como el crecimiento y la sofisticación continua de las ciberamenazas, el uso y la protección de la IA, el despliegue seguro de 5G, la seguridad de la cadena de suministro, la regulación, el mercado asegurador, etc., por nombrar algunos. En este cambio de era, Telefónica está preparada y tiene el compromiso de afrontar la seguridad digital de las redes del futuro.

Para terminar, procede dar las gracias a todos los empleados, colaboradores, proveedores, socios y amigos que nos han acompañado en este camino de la seguridad en todos sus frentes y animar a las generaciones futuras de profesionales con el foco en la seguridad digital a conservar el espíritu de exigencia, compromiso y vocación de servicio a la sociedad que nos caracteriza.



JUAN CARLOS GÓMEZ CASTILLO
Global Chief Digital
Security Officer
TELEFÓNICA

La falta de comunicación y comprensión de los problemas entre CISOs y desarrolladores, origen de gran parte de los problemas en ciberseguridad en el software

La mayoría de los desarrolladores y CISO consideran la seguridad de la cadena de suministro de software como una máxima prioridad en sus funciones (70% y 52% respectivamente), según un estudio de **Chainguard**. En él, se alerta de que aún hay una gran brecha e, incluso, cierta desconfianza entre los CISO y los desarrolladores sobre quién es el responsable de prevenir y mitigar los problemas de seguridad en cada departamento, si los CISO realmente entienden las herramientas del día a día de los desarrolladores o el riesgo asociado que estos tienen en su trabajo y en las herramientas que utilizan.

Entre otros datos de interés, el 72% de los desarrolladores destacaron que son muy conscientes de la seguridad en sus funciones, mientras que

sólo el 50% de los CISO les consideran como muy conscientes de la seguridad. Sólo el 43% de los desarrolladores creen que los CISO están “muy familiarizados” con cómo las imágenes de contenedores encajan en su trabajo.

Además, el 92% de los desarrolladores participantes destacó que la seguridad de la cadena de suministro de software es, al menos, “muy importante” para su trabajo diario y sus procesos de desarrollo, y el 39% la considera “absolutamente esencial”.

Frente a ello, el 93% de los CISO explicaron que la protección del software eficaz es un componente crítico de la madurez organizacional



y de la estrategia de mitigación de amenazas/riesgos, y el 96% dice que las prácticas eficaces de seguridad del software son importantes para cumplir con los requisitos gubernamentales o regulatorios.

De cualquier forma, el trabajo de uno y de otros no es sencillo: el 36% de los CISO y el 34% de los desarrolladores informaron de una “abrumadora cantidad de alertas de vulnerabilidad de falsos positivos” en los escáneres y destacan este aspecto como uno de los mayores obstáculos a los que se enfrenta una organización para garantizar la seguridad de la cadena de suministro de software.



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

Murcia se convierte en una de las primeras comunidades que certifica sus infraestructuras digitales acordes al ENS

EL CENTRO DE INNOVACIÓN Y COMPETENCIA EN CIBERSEGURIDAD, financiado por INCIBE, Cataluña, Valencia y Galicia, comenzará a funcionar en 2024

Entre las principales novedades regionales en el arranque de este 2024 destaca la pretensión de poner en marcha en el primer trimestre del año la **Agencia de Ciberseguridad de Madrid**, de la que SIC dio cuenta informativa en su número 157, para "facilitar una visión centralizada y aumentar las facultades de gobierno mediante la configuración del Equipo de Respuesta a Incidentes



de Ciberseguridad para toda la **Comunidad de Madrid**. Esta estructura estará también enfocada a reforzar la protección informática de las infraestructuras más relevantes, con especial atención en el área de salud", destacan sus impulsores. Según lo indicado, quién la dirija deberá ser expresamente un profesional de reconocido prestigio en el ámbito de la ciberseguridad.

Además, esta comunidad también ha aprobado una inversión de 9,8 millones de euros hasta 2027, para reforzar la **Oficina de Seguridad de Sistemas de la Información (OSSI)**, organismo responsable de prevenir, detectar y responder a las amenazas y ataques cibernéticos que eventualmente sufra el **Servicio Madrileño de Salud (Sermas)**. Estos recursos también se destinarán a asegurar el cumplimiento normativo en materia de protección de datos en el ámbito sanitario. Así, la OSSI contará con el apoyo de la nueva Agencia de Ciberseguridad.

Galicia adjudica las obras para su centro de Ciberseguridad

Por su parte, la **Xunta de Galicia** adjudicó, antes de final de año y por más de 5,8 millones de euros, a **Oreco Balcón** las obras del **Centro**



de Ciberseguridad de Galicia, que se ubicará en el Parque Tecnológico ourensano, en San Cibrao das Viñas, cuya construcción comenzará en los primeros meses de este año, con el objetivo de inaugurarse en 2025. Con superficie útil de 2.100 m², las instalaciones acogerán los equipos de monitorización y gestión de ciberseguridad de la comunidad, además de contar con áreas de trabajo y de concienciación, así como locales de emprendimiento y de alquiler para empresas privadas, ya que también se quiere también que sea "un punto de encuentro entre la innovación en ciberseguridad y las necesidades de la sociedad".

Nuevo Centro de Innovación



Por su parte, la **Consejería de Hacienda, Economía y Administración Pública de la Comunidad Valenciana** también hizo un esfuerzo notable en este ámbito al autorizar un convenio por el que se pondrá en marcha el **Centro de Innovación y Competencia en Ciberseguridad**, en 2025, a través del programa Redes Territoriales de Especialización Tecnológica (Retech), en el que también participan **Cataluña** y **Galicia**, así como el **Instituto Nacional de Ciberseguridad (Incibe)**. Con una duración de dos años—hasta el 30 de diciembre de 2026—, el Centro se centrará en la creación de capital tecnológico y humano, y convertirá los territorios donde se implante en un

medio favorable para localizar inversiones. Para ello, hasta 2026, el Incibe aportará 43,2 millones, Cataluña cinco millones, mientras que Galicia y Valencia 4,7 millones cada una, esta última será la encargada de las líneas relacionadas con la industria conectada y la excelencia operativa.

La Rioja resuena su ciberseguridad

Asimismo, el gobierno de **La Rioja** ha dado luz verde a una inversión de más de 700.000 euros para el despliegue de un plan de renovación de sus infraestructuras tecnológicas esenciales, con la finalidad de mejorar su rendimiento y agilizar la respuesta de la administración regional a la ciudadanía. Además, destinará, 1,2 millones a reforzar la ciberseguridad hasta 2027, a través de un concurso para mejorar sus capacidades de detección y respuesta de ciberamenazas. "Aunque la solución existente ha demostrado ser altamente eficiente en la detección y respuesta en tiempo real, se han identificado áreas de mejora. Se trata de las relacionadas con la identidad digital, los dispositivos OT y las capacidades de análisis e investigaciones sobre eventos de ciberseguridad", destaca el pliego de la licitación.

Murcia, pionera en el ENS

Murcia se ha convertido "en la primera comunidad autónoma que ha certificado sus infraestructuras digitales conforme al Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad



(ENS)". "De esta manera, el ENS garantiza que en la Comunidad se aplican las medidas de seguridad adecuadas en la protección de la información gestionada por las infraestructuras digitales", des-

tafan sus responsables, que han contado con la **Entidad Nacional de Acreditación en España (Enac)** para lograrlo.

Entidades locales

En cuanto a ayuntamientos, ha sido especialmente llamativo el ataque de *ransomware* sufrido por el consistorio de **Calviá**, en Mallorca, al que se exigió 10 millones de euros de rescate, que el ayuntamiento se ha negado a pagar, tal y como marca el compromiso de España con la Iniciativa contra el *ransomware*, que acordó que los organismos públicos no abonarían este tipo de extorsiones a partir de este año. Además, el de **Paterna** ha reforzado su ciberprotección con la puesta en marcha de un Centro de Operaciones de Ciberseguridad que integra plenamente todas las medidas de protección para el cumplimiento del ENS, contratado con **Atos IT de Eviden**. Por su parte, **Huelva**, a través de la concejalía de Régimen Interior, Recursos Humanos y Modernización Digital, ha concluido su plan de ciberseguridad de cara a anticiparse y reforzar la detección de ataques informáticos, con una inversión de 500.000 euros.

Laboratorio de ciberseguridad

Junto a ello, cabe destacar también que **Linares (Jaén)** inauguró el primer laboratorio de ciberseguridad de Andalucía. En concreto, la **Cámara de Comercio, Industria y Servicios** de la ciudad impulsa este nuevo recurso, que viene a sumarse y fortalecer el resto de las infraestructuras destinadas a favorecer la innovación y el emprendimiento y que contará con una inversión de 400.000 euros, con financiación de la **Fundación Incyde** y de los fondos Feder.

Entre otras funciones, también será un lugar de formación y aprendizaje que enriquezca el campus tecnológico de Linares, adscrito a la **Universidad de Jaén**.



Akamai Connected Cloud

La plataforma cloud más distribuida del mundo, con soluciones líderes en:



**Content
Delivery**



**Cyber
Security**



**Cloud
Computing**

Forma parte de una inversión de la multinacional en España de 650 millones a cinco años

GOOGLE presenta en Málaga su centro de ciberseguridad mundial para investigación de amenazas y su punto europeo de referencia en este ámbito

“La seguridad ha sido siempre un elemento central de los productos de Google”. Así lo destacó el director de Ciberseguridad de **Google Cloud**, **Phil Venables**, quien recordó en la inauguración de la sede malacitana del denominado **Google Safety Engineering Center (GSEC)**, a finales de año, que está llamado a ser “uno de los buques insignia de la ciberseguridad en Europa”. “Trabajamos para ayudar a que internet sea mejor y más seguro”, añadió poniendo en valor la apertura de estas instalaciones. “Desde Málaga esperamos convertirnos en un *hub* referente en materia de ciberprotección con visibilidad internacional”.

El centro es un hito para España que se posiciona como uno de los referentes de la compañía, ya que desde él se compartirá inteligencia de amenazas, servirá para desarrollar nuevos productos y se erigirá en punto de encuentro entre los diferentes agentes del sector, además de impulsar el talento en este ámbito. Construido en el reformado edificio de lo que fue el antiguo Gobierno Militar de Málaga, cerca del **Centro de Ciberseguridad de Andalucía**

y del **Museo Pompidou**, ahora trabajará junto con los otros centros continentales con los que cuenta la compañía en Europa, el de Dublín y el de Munich.

Apuesta por España

Las nuevas instalaciones, con tres plantas, terraza y auditorio, cuya puesta en marcha forma parte de una inversión de la multinacional de 650 millones a cinco años para España, pretenden erigirse en la referencia mundial de la tecnológica. “Será un espacio de colaboración entre expertos, académicos, empresas y gobiernos europeos en el que discutir sobre buenas prácticas, compartir investigaciones y conocimientos y, en definitiva, conseguir avances en seguridad que sean beneficiosos para todos”, destacan sus impulsores. “En estos centros, el trabajo de los ingenieros de Google no se limita a hablar de seguridad digital, también la construyen”.

De momento, con una plantilla que ya ronda los 60 profesionales, el 80% de Málaga, la es-

tética y filosofía de la empresa se deja notar en cada rincón, con salas bautizadas como algunos de los virus informáticos más conocidos –Notpetya, Wannacry...– o conocidos videojuegos como ‘Wololo’, ‘Monkey Island’ o ‘Super Mario Bros’. Incluso, cuenta con el fútbolín original de **Virus Total**, la compañía española comprada por Google en 2012 y que, gracias al tesón de su actual Security Engineering director, **Bernardo Quintero** –presente en el evento– ha hecho que se apueste por el enclave andaluz como referente de Google para Europa y el mundo. Precisamente, su equipo trabajará ahora también en el GSEC. Así, la compañía se suma a otras muchas tecnológicas y consultoras que ya tienen instalaciones en la ciudad, como **EY**, **Fujitsu**, **Vodafone**, **Ericsson**, **NTT Data**, **Oracle** y **Capgemini**, entre otras.

En la inauguración, el presidente de Asuntos Globales, **Kent Walker**, explicó que el GSEC será parte importante en los tres pilares de la ciberprotección de la compañía: “velocidad de respuesta, código abierto e inteligencia artificial”.

Eric Doerr, Vicepresidente de Ingeniería de Seguridad en la Nube de Google Cloud

“El GSEC tendrá un papel importante en el desarrollo de soluciones innovadoras, la investigación de amenazas y el debate en ciberseguridad”

– ¿Qué le gusta (y qué no) de trabajar en ciberseguridad?

– La misión es asombrosa: te sientes bien al despertarte cada día y concentrarte en ayudar a las personas. A mí, que me gusta la arquitectura, creo que la ciberprotección se puede comparar con la Sagrada Familia de Barcelona: es hermosa, difícil... y queda mucho por hacer.

Lo complicado de la ciberseguridad es que a la industria a veces le resulta difícil unirse en pos de una causa compartida, aunque todos luchemos contra los mismos actores. Si bien hay excelentes ejemplos de colaboración, nosotros (los defensores) superamos en número a los malos actores 100:1 y, sin embargo, no siempre

trabajamos para unir los escudos.

– ¿Qué espera lograr con este Centro?

– Como centro de asociación con expertos, académicos, empresas y gobiernos europeos, GSEC Málaga encarnará el compromiso de Google de apoyar a Europa y a sus líderes en ciberseguridad en apoyo de nuestros valores compartidos. En concreto, esperamos lograr tres cosas: promover el conocimiento, combatir amenazas cada vez más sofisticadas mediante la creación y el desarrollo de investigaciones y herramientas de vanguardia y abordar la brecha de habilidades



Eric Doerr

en ciberseguridad en toda Europa ofreciendo capacitación y programas de formación.

– ¿Qué aportará a los expertos concernidos?

– GSEC Málaga se convertirá en un centro internacional de ciberseguridad, colaborando con expertos, académicos y empresas europeas. Además, nuestros equipos analizarán aquí todo tipo de archivos, dominios, IP y URL sospechosos para detectar *malware* y otras infracciones, y compartirlos con la comunidad de seguridad. Al compartir investigaciones, conocimientos y mejores prácticas, el GSEC de Málaga ayudará a empresas de todos los tamaños a prevenir, detectar y responder a estas

amenazas, entre otros aspectos. – Usted coordinará aquí a los equipos de **VirusTotal**, **Mandiant**, **Chronicle**, **Uppercase** y **Cloud Security**...

¿Por qué elegir a Westcon como tu distribuidor de confianza?

Entre otros motivos, porque Westcon dispone de las mejores herramientas del mercado para facilitar tu capacitación.

Westcon  | TechXpert

TechXperts

¿Qué es? Es una comunidad tecnológica de Westcon dirigida exclusivamente a perfiles técnicos de partners y fabricantes con contenido relevante e interesante para los mismos (boletines informativos, invitaciones a eventos exclusivos, canales de comunicación con expertos, descuentos en formaciones, acceso a material formativo, etc.).



Westcon  | Academy

Portal de e-learning (LMS)

¿Qué es? Portal de e-learning con contenidos formativos para partners. Hay contenidos oficiales de pago que se intercalan con muchos otros de carácter gratuito.



Westcon  | 3D Labs

3DLabs

¿Qué es? Es un entorno de múltiples laboratorios multi-fabricante perfectamente documentados y gratuitos. Iniciativa única en el sector.



Tech & Café

¿Qué es? Sesiones dirigidas a los comerciales de partners en donde se les dan herramientas de venta a través de sencillos y potentes "Elevator Pitch" o argumentos que les sirvan para descubrir oportunidades en los clientes. Cada edición va dedicada a un fabricante. Durante la ejecución de la sesión, hay networking y desayuno en grupo.



TechLab & Beers

¿Qué es? Workshops prácticos de soluciones del portfolio Westcon dirigidos a perfiles técnicos de partners y fabricantes (preventa, servicios, soporte, auditoría, etc.) A la finalización del workshop hay networking, con cervezas y tapas en grupo.



El acto de presentación contó, además, con destacados referentes de la compañía en este ámbito como son el director de Seguridad Informática, **Eric Doerr**, y la directora de Ingeniería de Seguridad del Grupo de Análisis de Amenazas, **Kate Morgan**. Por parte española, estuvo la directora general de la compañía en España, **Fuencisla Clemares**, y la general manager para EMEA de Google Cloud Security, **Cristina Pitarch**. No se quisieron perder la inauguración el actual ministro de Transformación Digital y Función Pública, **José Luis Escrivá**, y la secretaria general del **Incibe**, **Carla Redondo**, entre otras personalidades del sector público, así como directores de centros de ciberseguridad europeos, embajadores y expertos de *think tank*, como **Max Smeets**, director de la Iniciativa Europea de Investigación sobre Ciberconflictos. Además, estuvieron presentes numerosos periodistas especializados de los principales medios internacionales, entre ellos **Revista SIC**. A ellos se sumaron, para conocer el Centro, un nutrido grupo de CISO europeos, de la mano de **Jorge Blanco**, CISO de Google en España, entre ellos **Rosa Kariger**, de **Iberdrola**, y **Mario Andrés**, de **Mercadona**.



Investigación y formación

Durante una jornada maratónica, se expusieron los retos del centro, entre ellos, dar apoyo a toda clase de entidades para reforzar su protección y sus conocimientos sobre ciber-

protección, en línea con los planteamientos de los principios de seguridad abierta de la compañía. Para ello, contará con un espacio dedicado a la formación, en el que se impartirán seminarios a medida para empresas de todos los tamaños, instituciones, profesionales, ONG e, incluso, instituciones de enseñanza locales.

Además, presentó un programa que realizará a través de **Google.org**, con 10 millones

de dólares de presupuesto, en colaboración con la **Incubadora Europea de Investigación sobre Ciberconflictos (ECCRI CIC)**, para impulsar la formación y ayudar a ONG locales, y en el que participaran ocho universidades, también de España.

En esta cantidad también está incluida la aportación de Google a la **Academia de Competencias en Ciberseguridad** de la UE, una iniciativa de la **Comisión** para cerrar, de forma coordinada, la brecha de talento en el sector.

Además, poco antes de su inauguración, Google también anunció la creación de la **Cátedra de Ciberseguridad**, junto con la **Universidad de Málaga**, dependiente de la ETSI de Ingeniería Informática, que inicialmente dirigirá el catedrático del Departamento de Lenguajes y Ciencias de la Computación, **Javier López Muñoz**, **'Premio SIC'** en 2023.

Aprovechando el evento, se dio a conocer el informe de Virus Defenders: How AI is shaping malware analysis'. "Gracias a ella, se puede identificar código malicioso hasta un 300% más rápido, con un 70% más de precisión y con utilidad para más personas, en comparación con las herramientas tradicionales", destacó el estratega de Inteligencia de Amenazas de la empresa, **Vicente Díaz**.

– Sí, aquí se reunirán una amplia gama de equipos y expertos de Google (de VirusTotal, Mandiant, Chronicle, el Grupo de Análisis de Amenazas –TAG–, etc.), para hacer lo que mejor saben hacer: crear y desarrollar investigaciones y herramientas de vanguardia para combatir amenazas cada vez más sofisticadas, basadas en la velocidad, el código abierto y la IA. Continuarán trabajando con otros de toda Europa y del resto del mundo (tanto dentro, como fuera de Google) para compartir experiencias, conocimientos, mejores prácticas, herramientas e investigaciones para combatir las amenazas. Lo que me encanta de ellos es la diversidad de experiencia y trabajo. Por otro lado, el GSEC de Málaga también trabajará estrechamente con los GSEC de Dublín, que abrió en 2020 y está especializado en responsabilidad de contenidos, y de Munich, que abrió en 2019 y está

especializado en ingeniería de privacidad y seguridad. En estos centros, los ingenieros de Google no sólo hablan de seguridad digital, sino que realmente la construyen. Aunque los enfoques de los tres GSEC difieren, los equipos trabajarán y aprenderán unos de otros.

– **¿Se van a ofrecer también servicios gestionados de ciberprotección en los que el GSEC está muy presente? Y, ¿para los SOC?**

– Google Cloud es miembro de la Red Nacional de SOC (RNS) y, de hecho, es el primer proveedor de nube que se convierte en miembro de esta red, dando apoyo a la RNS mediante alerta temprana y respuesta a incidentes en las administraciones públicas, compartir conocimiento sobre amenazas y tecnologías emergentes. Además, proporcionaremos educación y formación a la próxima generación de ciberdefensores en España. Nos enorgullece haber desarrollado so-

luciones integrales de ciberseguridad, como Google CyberShield, para abordar las necesidades de operaciones de seguridad de los gobiernos de todo el mundo. Y el GSEC desempeñará un papel importante en nuestros esfuerzos, indirectamente, mediante el desarrollo de soluciones de seguridad innovadoras, la producción de investigaciones de amenazas de vanguardia y la información para el debate más amplio sobre la ciberseguridad.

– **¿Qué alianzas, desde el GSEC, realizarán?**

– Impulsaremos asociarnos con responsables políticos europeos, expertos en ciberseguridad, instituciones académicas y clientes de la nube, porque es una de las principales prioridades de este centro, así como acelerar el desarrollo de herramientas e investigaciones para combatir las amenazas. También apostaremos por nuestro enfoque

tradicional en la transparencia y el código abierto.

– **A cinco años vista, ¿de qué tres logros esperaría sentirse más satisfecho?**

– Gran pregunta. GSEC Málaga tiene que ver con la colaboración, por lo que el éxito para nosotros no significará sólo un Google más seguro, sino una Internet mejor y más segura que beneficie a todos (personas, empresas y gobiernos) en toda Europa. Parte de eso consistirá en promover el conocimiento: trabajar con gobiernos, instituciones e investigadores europeos para compartir las tendencias, amenazas y mejores prácticas. Si podemos continuar compartiendo informes, organizando talleres y analizando y exponiendo nuevas amenazas a la seguridad que ayuden a otros a protegerse y desarrollar mejores prácticas, eso será una señal de éxito.

José Manuel Vera

IV JORNADAS STIC & CONGRESO ROOTED CON

CAPÍTULO PANAMÁ

GOBERNAR Y COMPARTIR,
LAS CLAVES DEL ÉXITO EN
CIBERSEGURIDAD.

DEL 10 AL 12 DE ABRIL
DE 2024

#STICPANAMÁ



ORGANIZADO POR:



CON EL APOYO INSTITUCIONAL DE:



CON LA COLABORACIÓN DE:



El ministro de Interior, GRANDE-MARLASKA visita la OCC para conocer, entre otros aspectos, los retos que la competen en 2024

El ministro de Interior, **Fernando Grande-Marlaska**, visitó en enero las instalaciones del **Centro Nacional de Infraestructuras Críticas (CNPIC)** y de la **Oficina de Coordinación de Ciberseguridad (OCC)**, ubicadas en el **Centro Tecnológico de Seguridad (CETSE)**, en El Pardo (Madrid), donde mantuvo un encuentro con sus responsables.

Durante la visita, los jefes del CNPIC, **José Luis Pérez**, y de la OCC, el comisario **Álvaro de Lossada**, presentaron al ministro, acompañado por el director general de Coordinación y Estudios, **José Antonio Rodríguez**, un balance de



los trabajos realizados hasta la fecha por los diferentes servicios de estas unidades, así como de sus retos para este año, ya que la OCC, entre otros, participa de forma ac-

tiva en el grupo de trabajo que espera antes de final de año ofrecer el texto normativo de transposición

de primera mano, los principales proyectos que se llevan a cabo en organizaciones como la OCC para

hacer frente a los nuevos retos y amenazas que entraña el ámbito cibernético.

Una iniciativa en la que participa de forma activa **Alberto Francoso**, jefe del Servicio de Análisis de la Ciberseguridad y la Cibercriminalidad de la OCC, también presente en la visita.

Desde su creación en 2007, el CNPIC ha establecido una compleja comunidad de seguridad con más de 250 operadores críticos en la actualidad, que sitúa a España en una posición de referencia internacional en este ámbito”, destacan desde Interior.

Además de la puesta al día, el ministro aprovechó para conocer,

ROOTEDCON reconoce, durante la jornada X1RedMásSegura, el buen hacer de Ángel Pablo Avilés, 'Angelucho', en concienciación

Como es sabido, en 2023 falleció de forma inesperada el que es considerado uno de los grandes referentes españoles en ciberconcienciación, **Ángel Pablo Avilés**, conocido por su apodo 'Angelucho'. Precisamente, aprovechando la edición de este año de **X1RedMásSegura**, iniciativa de la que era uno de sus máximos

jornada, incluyendo a **Revista SIC** –de siempre muy comprometida con esta inspiradora iniciativa–, compartiendo con todos los asistentes momentos especiales en su labor de concienciación y forma-



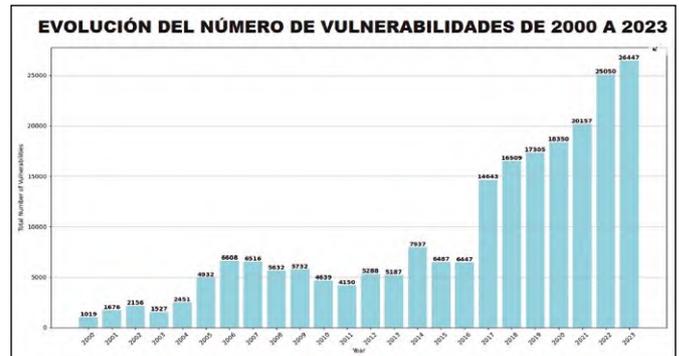
impulsores, el congreso **RootedCON** –a través de su presidenta **Arantxa Sanz**–, quiso honrarle entregando el Premio Raúl Jover a su mujer, **Virtu Saavedra** y a su hijo, **David Avilés**, 'Insonusvita', quien estrenó, como homenaje, el rap 'Guardianes de la Red'.

Angelucho fue homenajeado por diferentes expertos durante la

ción de padres y menores, así como también, rehabilitación de algunos jóvenes detenidos –durante su etapa de Guardia Civil en el entonces Grupo de Delitos Telemáticos–, a los que ayudó a reintegrarse como profesionales del sector.

De hecho, el **Congreso C1b3rWall 2024**, en la **Academia Nacional de Policía de Ávila**, del 18 al 20 de junio, que este año coincidirá con su 200 aniversario, pondrá precisamente en esta edición el nombre del agente a su sala principal como reconocimiento.

Una de cada cuatro vulnerabilidades son explotadas el mismo día que se conocen y, de media, tardan en descubrirse en torno a 44 días



En 2023, se contabilizaron a nivel global cerca de 26.500 vulnerabilidades, lo que significó un aumento del 6% respecto a 2022, manteniendo la tendencia anual de crecimiento constante. Así lo destaca el informe de **Qualys**, 'Panorama de Amenazas 2023', elaborado por su Unidad de Investigación de Amenazas. En él, desvela también que solo el 1% de las descubiertas supusieron un nivel de riesgo crítico para la seguridad de las organizaciones. Precisamente, sus responsables centraron gran parte de su análisis en este pequeño porcentaje, pero crítico, con datos

ilustrativos: cerca de la mitad no se hallaban en el catálogo de Vulnerabilidades Conocidas (KEV) de la CISA. "El uso de las vulnerabilidades como arma de ataque crece a un ritmo muy rápido, al mismo tiempo que aumenta la diversidad de actores que ejecutan estas amenazas", ha explicado el country manager de la compañía en España, **Sergio Pedroche**.

El tiempo medio para explotar las vulnerabilidades en 2023 fue, según el informe, de 44 días pero, sin embargo, muchas de ellas ya tenían un *exploit* el mismo día de su publicación.

kaspersky



¿Para ti la inteligencia contra amenazas representa una ayuda o un obstáculo?

Obtén inteligencia de amenazas personalizada para tu organización



Kaspersky
Threat Intelligence

kaspersky.es/enterprise-security/threat-intelligence

Centro de Análisis y Prospectiva: 25 años con una extraordinaria visión anticipatoria

En la Guardia Civil estamos de enhorabuena. Nuestro Centro de Análisis y Prospectiva cumple 25 años de existencia. Hace 25 años, con una extraordinaria visión anticipatoria y en el marco de una colaboración intensa que la Guardia Civil ha desarrollado siempre con el mundo de la Academia, un conjunto de mentes brillantes y de visión estratégica y anticipatoria determinaron la necesidad de adquirir capacidades en el diseño de escenarios de futuro, con el fin de mitigar riesgos y anticipar amenazas en materia de Seguridad Interior en España.

La prospectiva es una disciplina joven. Es en los años 60, el filósofo francés Berger introduce este término para referirse a un conjunto de técnicas y metodologías orientadas a ayudar en los procesos de toma de decisión informados, cada vez más complejos, a los que se enfrentan las sociedades humanas.

En estos 25 años hemos vivido varias revoluciones sociales, geopolíticas, tecnológicas y tenemos la misión de intentar anticiparnos a sus efectos indeseados en seguridad. Al tiempo, la prospectiva intenta, a través de la técnica de los “pequeños empujoncitos”, influir, de forma positiva, en ese futuro, con el fin de mejorar nuestra resiliencia como sociedad.

Y llegamos al momento de nuestra creación formal: El 9 de diciembre de 1998 se crea, en el seno del Gabinete Técnico de la Guardia Civil, el Centro de Análisis y Prospectiva de la Guardia Civil (CAP), como órgano encargado de estudiar, recopilar, difundir y colaborar en todas las tareas y misiones relacionadas con la adquisición y gestión de conocimiento de fuente abierta, de utilidad para la Seguridad Pública, así como en la elaboración de escenarios de futuro con impacto en Seguridad.

Durante estos años, nos hemos ido adaptando a esos momentos históricos que han pasado por nuestra vida adulta. Los ataques a las Torres Gemelas y su impacto posterior marcaron toda una época en la actividad del CAP que ha ido generando un conjunto de series documentales, muchas de ellas de acceso público desde nuestro servicio de biblioteca electrónica.

Tras el último cambio en su Dirección, se ha apostado por el uso intensivo de la tecnología, tanto para manejar de manera eficiente la información disponible, como para causar el mayor impacto social posible, ya que la generación de cultura de la seguridad, cultura de la inteligencia y cultura de la prospectiva en nuestra sociedad es una de nuestras misiones estratégicas.

Siguiendo esta directriz, hemos desplegado una IA (Casandra) para ayudar a nuestro personal en prácticas en la elaboración de informes de fuente abierta y generar píldoras formativas para formar a la ciudadanía en estos asuntos. También hemos desplegado servicios de Vigilancia Tecnológica para monitorizar nuestro entorno y servicios de extracción de entidades para poder mapear determinados asuntos de interés en materia de seguridad interior.

Participamos en el diseño de acciones de la Guardia Civil tan importantes como la National Cyber League, de la que somos elemento fundamental en la dirección de su metaverso, así como en otras acciones de nivel estratégico relacionadas con la prospectiva.

No podemos terminar sin ofrecer un mensaje importante: “Una ciudadanía formada e informada, en materia de seguridad, conforma siempre una sociedad más resiliente frente a las amenazas.”



ENRIQUE ÁVILA GÓMEZ
Director
Centro de Análisis y Prospectiva
Gabinete Técnico
DIRECCIÓN GENERAL
DE LA GUARDIA CIVIL

Hackers éticos españoles se hacen con el título oficioso de ‘Campeones del Mundo’ en la ‘Ambassadors World Cup 2023’ tras derrotar a Israel

A final de año, España se hizo con el título ‘oficioso’ de campeona del mundo en el disputado ‘Ambassadors World Cup’ (AWC 2023), de la empresa **HackerOne**, tras vencer a Israel en una final muy disputada con un centenar de participantes. Un hito por cuanto se trata de una competición con grandes referentes en ‘caza de vulnerabilidades’, de 29 equipos y casi 680 hackers éticos de 22 países, incluidas grandes potencias como EE.UU. e India.

En esta edición, el equipo español de *bug bounty*, seleccionado por **Diego Jurado** y **Carlos Rivero**, según criterios técnicos, fue superando fase tras fase hasta convertirse en una de las favoritas a pesar de ser debutante en este torneo.

En concreto, la edición de 2023, comenzó en



marzo y tuvo una duración de ocho meses, de forma virtual, excepto la final, en formato presencial. Para hacerse con el título, los integrantes

nacionales tuvieron que identificar vulnerabilidades importantes en los programas de los clientes participantes, entre ellos multinacionales como **Epic Games, OpenSea, Shopify, Stripe y Yahoo**.

El éxito conseguido fue tal que incluso el **Centro Criptológico Nacional (CCN)** quiso reconocer este mérito en sus XVII Jornadas STIC y V Jornadas de Ciberdefensa, felicitando en directo a la selección nacional ganadora de esta competición. **Luis Jiménez**, subdirector General del CCN, y **Javier Candau**, jefe del Departamento de Ciberseguridad, conversaron con dos de los representantes del equipo español, **Camilo Andrés** y **Bernardo Viqueira**, destacando el “enorme potencial de talento en ciberseguridad existente en nuestro país”.

Botech evoluciona

Un paso más allá de la ciberseguridad



+

Solver 

+



=



BOTECH



botech.info

España - México - EE.UU. - Chile

Contempla multas de hasta 35 millones de euros o el 7% de la facturación global

EUROPA, pionera en aprobar el primer marco regulatorio de Inteligencia Artificial, no exento de críticas

Tras muchos meses de negociación y tres días maratónicos de negociaciones entre expertos del **Consejo de Europa** y el **Parlamento Europeo**, a finales de año se llegó a un acuerdo del texto final que será aprobado de la llamada Ley de Inteligencia Artificial (AI Act), el marco regulatorio que busca garantizar que los sistemas de IA comercializados en el mercado europeo y utilizados en la UE sean seguros y respeten los derechos fundamentales y se preserven los valores del Viejo Continente. “Esta propuesta histórica también tiene como objetivo estimular la inversión y la innovación en IA en Europa”, según destacaron sus impulsores, que la consideran “un logro histórico y un gran hito hacia el futuro”. Además, al ser el primer texto legislativo de este tipo aprobado en el mundo, también aspira a convertirse en un estándar global para la regulación de la IA, tal como lo ha sido el RGPD.

Su idea principal es regular la IA en función de su capacidad de causar daño a la sociedad siguiendo un enfoque ‘basado en el riesgo’: cuanto mayor sea, más estrictos serán los requisitos que debe superar.

Evaluación de impacto

Entre otras novedades respecto al texto de partida, incluye reglas sobre modelos de IA de propósito general de alto impacto que pueden causar riesgo sistémico en el futuro, así como sobre sistemas de IA de alto riesgo, un sistema revisado de gobernanza con algunos poderes de ejecución a nivel de la UE y la ampliación de la lista de prohibiciones, pero con la posibilidad de utilizar la identificación biométrica remota por parte de las autoridades encargadas de hacer cumplir la ley en espacios públicos, sujeto a salvaguardias. También, supone una mejor protección de los derechos mediante la obligación de que quienes implementen sistemas de IA de alto riesgo realicen una evaluación del impacto en los derechos fundamentales antes de poner en uso un sistema de IA.

Exclusiones

Entre otros aspectos, el reglamento contiene una definición de un sistema de IA –alineada con la OCDE–, con los criterios suficientemente claros para distinguirla de los sistemas de *software* más simples. Además, destaca que esta ley no se aplica a áreas fuera del alcance de la legislación

faciales de Internet o imágenes de CCTV, el reconocimiento de emociones en el lugar de trabajo y en instituciones educativas, la puntuación social, la categorización biométrica para inferir datos sensibles, como la orientación sexual o la religión, creencias y algunos casos de vigilancia policial predictiva para individuos.

Además, a partir de las normas que afectan a los modelos GPAL (sistemas de IA de propósito general) y la evidente necesidad de su aplicación a nivel de la UE, la Ley aprueba la creación de una **Oficina de IA**, dentro de la Comisión, encargada de supervisar los modelos más avanzados, contribuir a fomentar estándares y prácticas

de prueba, y hacer cumplir las normas comunes en todos los estados miembros. A ella, se sumará un panel científico de expertos independientes que la asesorará (Junta de IA), compuesto por representantes de los estados miembros, así como un foro consultivo para las partes interesadas, como representantes de la industria, las pymes, las empresas emergentes, la sociedad civil y el mundo académico, para proporcionar conocimientos técnicos a la Junta de IA.

Multas y sanciones

El texto también aprueba multas por violaciones de la ley de IA, según un porcentaje de la facturación anual global de la empresa infractora en el año financiero anterior o una cantidad predeterminada, lo que sea mayor. Esto equivaldría a 35 millones de euros o el 7% por violaciones de las aplicaciones de IA

prohibidas, 15 millones de euros o el 3% por violaciones de las obligaciones de la ley de IA, y 7,5 millones de euros o el 1,5% por el suministro de información incorrecta.

A la espera de su aprobación, la ley sobre IA debería aplicarse dos años después de su entrada en vigor, con algunas excepciones para disposiciones específicas.



de la UE y no debería, en ningún caso, afectar las competencias de los estados miembros en materia de seguridad nacional o cualquier entidad a la que se

le hayan confiado tareas en esta área. Tampoco tendrá validez sobre sistemas que se utilicen exclusivamente con fines militares o de defensa, ni los usados en investigación e innovación, ni en usos personales.

Asimismo, contiene una clasificación de los sistemas de IA para evitar que causen violaciones graves de los derechos fundamentales u otros riesgos importantes. Por ejemplo, los que presenten un riesgo limitado estarán sujetos a obligaciones muy leves. Además, se permitirá una amplia gama de sistemas de IA de alto riesgo, pero sujetos a una serie de requisitos y obligaciones para acceder al mercado de la UE.

De cualquier forma, se destaca que “para algunos usos de la IA, el riesgo se considera inaceptable y, por lo tanto, estos sistemas serán prohibidos en la UE”. Entre otros, se prohíbe, por ejemplo, la manipulación cognitiva conductual, la eliminación no selectiva de imágenes



UN GRAN AVANCE EN DIGITALIZACIÓN



ASLAN ³¹ED ²⁰24

17 y 18 ABRIL > MADRID

congreso.aslan.es

Data Resilience

Cyber Security

Digital WorkSpace

Cloud DataCenter

Intelligent Networks

Todo cambia.

La irrupción de la IA está produciendo grandes cambios en la industria de la innovación digital. El Congreso ASLAN2024 es una oportunidad única para conocer cómo está evolucionando la ciberseguridad, el puesto de trabajo digital o la gestión del dato gracias a la inteligencia artificial y cómo afrontar los nuevos retos para redes, entornos multi-cloud, centros de datos y otras infraestructuras digitales.

Juntos aceleramos la transformación digital.



GLOBAL SPONSORS



EVENT SPONSORS



El gran evento anual en España organizado por la Asociación nacional de la industria tecnológica

@aslan/35 años

EN BREVE

18 agencias de ciberprotección acuerdan unas directrices globales para usar la IA con seguridad

El Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC), la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. (CISA) y otras 16 agencias nacionales -entre ellas, el Centro Canadiense de Seguridad Cibernética, la Agencia Francesa



de Ciberseguridad, la Oficina Federal de Seguridad de la Información de Alemania, la Agencia de Seguridad Cibernética de Singapur y el Centro Nacional de Incidentes de Japón-, no estando presente España, han publicado y apoyado las 'Directrices para el desarrollo seguro de sistemas de IA', presentadas por el NCSC, y pensadas para guiar el trabajo de los desarrolladores a través del diseño, desarrollo, implementación y operación de sistemas de IA y garantizar que la seguridad siga siendo un componente central durante todo su ciclo de vida, para que "funcionen según lo previsto, estén disponibles cuando sea necesario y operen sin revelar datos confidenciales a partes no autorizadas".

En total, el documento está dividido en cuatro secciones, que se identifican con las diferentes

etapas del ciclo de vida del desarrollo de un sistema de IA: diseño seguro, desarrollo seguro, implementación segura, y operación y mantenimiento seguros.

Mala solución

Por otro lado, investigadores del Instituto Nacional de Estándares y Tecnología (NIST), de EE.UU. han publicado una investigación en profundidad sobre la seguridad de los sistemas de IA en la que se alerta que los que dependen de grandes cantidades de datos para realizar tareas, puede funcionar mal cuando se expone a datos no confiables. Entre otros aspectos, sus responsables encontraron que los ciberdelincuentes pueden confundir o 'envenenar' deliberadamente los sistemas de IA para que funcionen mal al exponerlos a datos incorrectos. Y lo que es más preocupante: según el estudio, no existe una defensa única que los desarrolladores o expertos en ciberseguridad puedan implementar para proteger los sistemas de IA.

La inversión de las empresas en IA crece un 30%: así están innovando los negocios

En un mundo en el que las empresas buscan diferenciarse cada vez más y lograr estrategias únicas, la innovación es un componente clave, algo que se puede conseguir mediante tecnología digital. Un claro ejemplo es el caso de la IA. Y es que, un estudio llevado a cabo por el **Mobile World Capital**, concluye que la inversión que están haciendo las compañías en IA se ha duplicado desde 2017, año en el que sólo el 20% de las organizaciones la habían adoptado, mientras que ahora lo han hecho un 50%.

Asimismo, una investigación sobre Data&Analytics e IA en España, ha concluido que siete de cada 10 empresas han aumentado su inversión en análisis de datos durante este último año.

Junto a ello, **IBM** ha presentado un fondo, IBM Enterprise AI Venture Fund, de 500 millones de dólares, para invertir en empresas de IA, desde las más emergentes en etapas iniciales hasta aquellas en hipercrecimiento, para acelerar su implementación e investigación.



ESPAÑA impulsa la cooperación y la convergencia regulatoria de la IA entre EUROPA, LATINOAMÉRICA y EL CARIBE

La presidencia española del Consejo de la Unión Europea promovió, a finales de 2023, una declaración suscrita por Argentina, Colombia, Chile, México, Uruguay, Panamá, República Dominicana, Alemania, Eslovenia, Estonia, Bélgica y España.

La declaración, impulsada por la presidencia española, ha llegado en "un momento crucial para el desarrollo y la regulación de la IA a nivel mundial", según sus impulsores, que se han comprometido a avanzar en la cooperación, el refuerzo y la conver-



gencia de las políticas y los marcos regulatorios en esta área, durante los próximos meses, antes de la Cumbre de Colombia de 2025.

El acuerdo se ha alcanzado durante la 4ª Asamblea Europea de la Alianza de IA, en Madrid, en una sesión paralela a puerta cerrada, presidida por la entonces secretaria de Estado de Digitalización e Inteligencia Artificial, **Carme Artigas**, en la que también participaron la **Comisión Europea** y la **Unesco**.

EE.UU. da a conocer la primera hoja de ruta de IA para la ciberseguridad

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), dependiente del Departamento de Seguridad Nacional (DHS) ha presentado su hoja de ruta inaugural para la IA.

El documento contempla cinco líneas estratégicas en la que pide focalizarse: uso responsable de la IA para apoyar la misión de CISA, evaluación y garantía de estos sistemas, protección de la infraestructura crítica de su uso malicioso, colaboración y comunicación sobre esfuerzos clave de IA, así como la ampliación de la experiencia en IA en la fuerza laboral.



destacado el secretario de Seguridad Nacional, **Alejandro Mayorkas**.

"La hoja de ruta de CISA establece los pasos que la agencia tomará como parte de los esfuerzos más amplios de nuestro Departamento para aprovechar la IA y mitigar sus riesgos para nuestra infraestructura crítica y defensas cibernéticas", ha des-



**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.**

AKAMAI: 25 años a la vanguardia tecnológica, definiendo el futuro de Internet

Todos los días, miles de millones de personas acceden *online* a sus marcas favoritas para comprar, jugar, compartir ideas o administrar dinero, entre otras. Es posible que no lo sepan, pero Akamai está allí, impulsando y protegiendo la vida en línea.

Hace 25 años nos propusimos resolver el desafío más complicado de los inicios de Internet: la “World Wide Wait” Y, desde entonces, hemos resuelto los retos más complejos de Internet trabajando por nuestra visión de un mundo más seguro y conectado.

En la actualidad, Akamai Connected Cloud, nuestra plataforma de nube distribuida de forma masiva en el Edge, ayuda a las empresas a ejecutar aplicaciones y cargas de trabajo al tiempo que acercamos las experiencias a los usuarios y mantenemos alejadas las amenazas. Desde nuestros inicios, las empresas más innovadoras de todo el mundo han contado con nosotros para crear, proteger y ofrecer sus experiencias digitales.

Entre nuestros clientes se encuentran grandes compañías de atención sanitaria, las principales empresas de Retail y de Tecnología financiera. Los grandes operadores de telecomunicaciones y empresas de tecnología financiera. Las empresas farmacéuticas, de automoción y videojuegos de primera línea y las principales grandes entidades bancarias.

Nuestro conjunto de soluciones de *cloud computing*, seguridad y distribución de contenido ayuda a las empresas a mejorar la vida de miles de millones de personas miles de millones de veces al día.

Estas tres líneas de negocio muestran la evolución y el crecimiento de Akamai en estos 25 años, acompañando a la propia evolución del mercado que exige, más que nunca, ser inmediato, escalable, más seguro y flexible.

Es importante tener en cuenta que, desde el nacimiento de Akamai en 1998, Internet ha crecido de 70 millones a 5.000 millones de usuarios en 2023. Nuestro éxito siempre ha sido una distribución de contenido altamente escalable que hace posible retransmitir eventos masivos, como las grandes finales de fútbol, que hubieran estado limitados por la capacidad interna de cada empresa de escalar ante eventos no planificados.

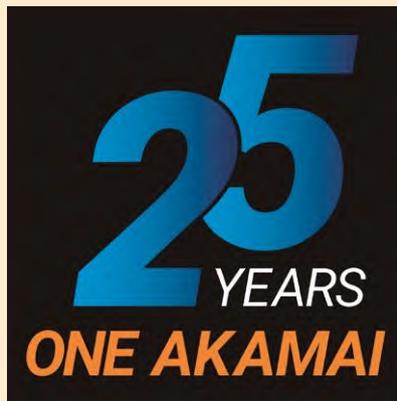
Akamai ofrece ahora una plataforma altamente escalable, con más de 1.000 TBPS de capacidad y totalmente distribuida que opera en más de 750 ciudades del mundo y con más de 1.200 redes.

Akamai ha sido el líder indiscutible en el mercado CDN desde su creación, entregando más contenido que la suma de todos nuestros competidores juntos, lo que además nos proporciona una visión única de lo que sucede en Internet que para nosotros es fundamental para poder ayudar a nuestros clientes a prevenir posibles ataques.

Por otro lado, cuando Akamai irrumpe en la Ciberseguridad mejora notablemente la vida de las empresas que antes dependían de sus *datacenter* con lo que esto suponía. Necesidad de personal extra, riesgo de caída ante los ataques DDoS, etc. Akamai apostó por WAF y lo implantó de forma global consiguiendo que las empresas estén protegidas automáticamente siempre con las últimas versiones y de una forma más económica al funcionar como servicio.

Nuestra visión es mantener a las empresas y sus aplicaciones, datos, empleados y clientes a salvo de ataques cibernéticos de todas las formas y para ello apostamos por la Seguridad en las infraestructuras, las aplicaciones y el Zero Trust.

Este es un momento emocionante para Akamai con inmensas oportunidades por delante. Quiero agradecer la confianza de todos aquellos que han estado a nuestro lado durante estos años. Especialmente a nuestros clientes y nuestro magnífico equipo.



FRANCISCO ARNAU
Vicepresidente Regional
para España y Portugal
AKAMAI

Alertan de que todavía demasiados portales y webs permiten usar contraseñas basadas en las recomendaciones de los años 80

Investigadores del **Instituto de Tecnología de Georgia** han alertado de que un número notable de webs, visitadas y usadas por millones de internautas, basan su gestión y utilización en un sistema de contraseña vulnerable ya sea por ser débiles e, incluso, simples al permitir claves de un sólo carácter. En su estudio, en el que emplearon un método automatizado para analizar más de 20.000 webs situadas en el ‘Top un millón’, del analista Tranco, constataron que 755 de las webs permiten contraseñas más cortas que los ocho caracteres reco-



mendados por los expertos –incluso un 12% de un sólo carácter–.

Además, un 40% de los sitios limitan la longitud de las contraseñas por debajo de los 64 caracteres recomendados. A ello se suma que el 72% permite usar palabras del diccionario como contraseña y el 88% no impide que se usen, incluso, las más hackeadas y conocidas. Y un tercio de las webs no admiten caracteres especiales en las contraseñas. El documento destaca, a modo de ejemplo, que el 39% de las webs acepta la contraseña más popular (“123456”),

mientras que casi la mitad acepta una de las cuatro contraseñas principales –‘123456’, ‘123456789’, ‘qwerty’ y ‘contraseña’–.

Además, un 42,1% todavía cumplen con las pautas de política de contraseñas del NIST de 2004, a pesar de que se actualizaron en 2017. En la investigación no faltan datos alarmantes como que un 16,7% aún no siguen las recomendaciones del NIST de 1985. Además, desvelaron que sólo el 5,5% de los sitios tienen políticas que satisfacen el nivel 2 del NIST 2004, en comparación con el 42,1% del nivel 1.



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

www.aenor.com



FRAUDFENSE, ambiciosa iniciativa para la lucha antifraude, inaugura su sede social con la asistencia de expertos de sus tres entidades

Recientemente tuvo lugar la inauguración de la sede social de **Fraudfense**, evento que reunió a muchos de los profesionales del **Santander**, **BBVA** y **CaixaBank** que han estado participando y trabajando durante meses en esta ambicioso y esperanzador proyecto. Como es sabido -SIC ya informó de ello en ediciones anteriores e incluso le concedió un Premio SIC en 2023-, esta iniciativa es la unión para hacer frente a uno de los grandes retos a los que se enfrenta el sector bancario, el fraude financiero. Las tres entidades españolas mencionadas están trabajando en herramientas para intercambiar información y datos relevantes que ayuden a prevenir el crimen financiero. A futuro es previsible la incorporación de más actores.

En este contexto, bajo la denominación de **Fraudfense**, se constituyó la compañía, aglutinadora de iniciativas antifraude de las tres entidades y ya presentada ante los diferentes

supervisores y reguladores competentes. **Carlos Requena**, con una dilatada y solvente trayectoria en el ámbito financiero y gran bagaje en temas de fraude, es su director general, en tanto que

Gobierno del Fraude, y **Lorenzo Malo**, CISO de CaixaBank. Ortega, de BBVA, es la precisamente la primera presidenta de **Fraudfense**, cargo que se irá renovando cada dos años entre los



membros de las tres entidades integrantes del proyecto.

El proyecto abarca la lucha contra diferentes prácticas fraudulentas, que pueden ser muy diversas y sofisticadas, como el fraude de admisión, en el que se compromete información de los clientes suplantándolos para la contratación de productos, y el fraude digital o de pagos con tarjeta.

en su consejo de administración, compuesto por dos representantes de cada entidad, figuran: **Carles Solé**, CISO de PagoNxt Payments, y **Daniel Barriuso**, Group CTO de Banco Santander; **Natalia Ortega**, responsable global de Prevención del Crimen Financiero, y **Sergio Fidalgo**, CSO Global y CISO Global, en representación de BBVA, y **Sofia Karapatsiou**, directora de

Esta ambiciosa colaboración, que comenzará en España, estará abierta a la incorporación de otras empresas y entidades, tanto financieras como de otros sectores, interesadas en poner en común información contra el fraude, con el fin de proporcionar una mayor protección a los clientes, a las entidades y a la sociedad en general.

ONUM arranca en España con su innovadora "plataforma de observabilidad de datos en tiempo real" y la vista en la internacionalización

La compañía **Onum**, nacida de la unión de profesionales de activos de **Signalit** y **Noister**, con una ronda de financiación inicial de 11 millones de euros -liderada por **Insight Partners** y **Kibo Ventures**-, ha comenzado a ofrecer sus servicios en España a través de una plataforma que aspira a convertirse en "la primera del

análisis de datos para comprender información crítica como latencia de la red, posibles amenazas en la seguridad y posibilidad de interrupciones. Sin embargo, la cantidad de datos generados por dispositivos en todo el mundo ha crecido exponencialmente en los últimos años, causando que estos datos sean cada vez más



mundo capacitada para observar y orquestar los datos en tiempo real: no se ha visto nada igual en el mercado hasta el momento", destacan sus fundadores, tres reconocidos profesionales como **Pedro Castillo**, **Lucas Varela** y **Pedro Tortosa**. En la presentación de la compañía señalaron que, de momento, ha tenido muy buena acogida.

"Durante más de 15 años, las empresas han utilizado plataformas de

inmanejables con los administradores de seguridad IT son incapaces de distinguir los datos valiosos del ruido", destacó

Castillo en la presentación, a la vez que recordó que muchas plataformas de orquestación de datos "no logran realizar observaciones en tiempo real, lo que desperdicia tiempo valioso que cualquier empresa necesita para tomar medidas decisivas, basadas en señales de advertencia en los datos". Un reto para el que Onum ofrece respuesta a través de su plataforma observabilidad de datos Edge "verdadamente agnóstica".

INTERPOL presenta el primer metaverso policial mundial con el que también espera luchar contra el cibercrimen en este entorno

"El metaverso no pertenece al futuro cercano. Ya está aquí". Así lo ha destacado **Interpol** en su 90ª reunión de la Asamblea General, en Nueva Delhi, en la que ha aprovechado

que tener permiso para conectarse a la 'Interpol Secure Cloud', la nube protegida de la organización, garantizando su neutralidad.

En una mesa redonda po-



para presentar el primer metaverso específicamente diseñado para los organismos encargados de la aplicación de la ley de todo el mundo. En él,

entre otros aspectos, los usuarios pueden desde recorrer la reproducción virtual de la sede de la Secretaría General de Interpol en Lyon (Francia), hasta interactuar con otros funcionarios por medio de sus avatares e, incluso, tomar cursos inmersivos en el ámbito de la investigación forense y otras capacidades policiales.

Eso sí, para acceder hay

posterior, la organización también anunció la creación de un grupo de especialistas en el metaverso para representar las preocupaciones de los organismos encargados de la aplicación de la ley en la escena mundial, a fin de garantizar la seguridad desde el diseño de este nuevo mundo virtual, en el que el cibercrimen cada vez actúa más.



GHENOVA

CIBERSEGURIDAD

Soluciones realistas a problemas reales.

- Consultoría
- Auditoría
- Concienciación
- Formación



Pretende desarrollar soluciones avanzadas para Salud, centradas en la protección de la información y los dispositivos médicos

SIA pone en marcha un Centro de Excelencia de Ciberseguridad para el sector sanitario con foco internacional

SIA, compañía de Indra, ha puesto en marcha un Centro de Excelencia de Ciberseguridad especializado en el sector sanitario con el fin de desarrollar y proporcionar soluciones avanzadas y adaptadas a las necesidades específicas de estos entornos. Enfocado tanto al ámbito público como privado, responderá con su labor a los principales desafíos de un sector tan crítico, donde proteger adecuadamente la información de los pacientes, las infraestructuras y los dispositivos médicos, así como la operación, puede llegar a salvar, también, vidas. Según un reciente informe de la Agencia de Ciberseguridad de la UE (Enisa), los ciberataques en este sector se duplicaron en el primer trimestre de 2023, en relación al mismo periodo de 2021 y 2022, siendo los objetivos no solo los hospitales, sino también los proveedores de servicios.

Ubicado en su sede de Alcobendas (Madrid), aunque con foco internacional, su equipo técnico está formado por expertos de SIA espe-

ponibilidad de las tecnologías y los equipamientos puede suponer una amenaza grave para la prestación del servicio y una atención adecuada y de calidad a los pacientes y ciudadanos”, destacó el CEO de la compañía, **Roberto Espina** (en la imagen).

En concreto, el llamado IoMT (Internet of Medical Things) se refiere a aquellos dispositivos médicos conectados a sistemas de tecnologías de la información a través de internet y/o entre sí –por ejemplo, grandes máquinas de diagnóstico o dispositivos de monitorización de soporte vital–; estos permiten a los profesionales de la salud mejorar y agilizar el tratamiento a los pacientes gracias a la posibilidad de acceder a la información de manera instantánea y monitorizarlos a distancia. Sin embargo, frente a estas ventajas, también surgen retos a los



Roberto Espina



cializados en este campo, y cuenta, además, con la colaboración y conocimiento sectorial y de gestión sanitaria de **Minsait**, la compañía de transformación digital de Indra.

Así, el Centro de Excelencia proyectará su actividad en varias líneas de actuación, principalmente, en la protección de la información y los dispositivos médicos (IoMT), la gestión de riesgos de terceros, y la aplicación de la Inteligencia Artificial contemplando sus beneficios y los riesgos que conlleva, para asegurar la continuidad de la actividad en estos entornos, “ya que la no dis-

que hay que dar una respuesta: garantizar que toda esta información sensible se almacene de forma totalmente segura y el incremento de la superficie de ataque, ante el creciente despliegue de unos dispositivos IoT obsoletos, poco visibles y protegidos, de múltiples fabricantes y protocolos, y con una no adecuada segmentación de las redes IT y OT a las que se conectan. Además, “los terceros también deben de formar parte de la estrategia de protección y monitorización, estableciéndose procesos y controles específicos”, añade Espina.

SOPHOS celebra su gran jornada anual alertando de la rapidez de los ataques y cómo los ciberdelincuentes, en el 82% de los casos, borran su rastro

La multinacional británica ha hecho público el informe ‘Active Adversary Report for Security Practitioners’, durante su Sophos Day 2023, celebrado a finales de año en el Museo Reina Sofía, en Madrid, con más de 400 asistentes. Durante la jornada, los participantes pudieron conocer las novedades en MDR, XDR, cortafuegos y ZTNA de Sophos. También, tuvo lugar una interesante mesa redonda, en la que **Carlos Rodríguez**, CISO de **Adolfo Domínguez**, **Alberto Corredera**, Director TI de **Room Mate Hoteles**, y **Alejandro Donoso**, Director TI de **Prinex Real State Software**, debatieron sobre las actuales amenazas y cómo hacerlas frente.

En la presentación del informe, basado en más de 230 casos reales investigados por el equipo de Respuesta a Incidente, se destacó cómo los atacantes están desactivando o borrando los registros de telemetría (todos los datos y registros de los movimientos llevados a cabo dentro de la red) para ocultar su rastro, ya que faltaban en casi el 42% de los ataques estudiados, mientras

que en el 82%, los atacantes los había eliminado a propósito para dificultar su captura.

Además, se alertó de la rapidez con la que actúan los atacantes –llegan, de media al Active Directory en 16 horas–, aunque se ha conseguido reducir el tiempo de permanencia desde el inicio de un ataque hasta que se detecta, situándose en ocho días en la primera mitad de 2023. “La única solución es avanzar hacia la



ciberprotección como servicio. Todas las organizaciones están evolucionando hacia servicios de ciberseguridad gestionada y creemos que ese es el camino, además de poder incorporar telemetría que garantice que las soluciones sean extensibles y completas”, comentó el Regional Vicepresident South EMEA & Emerging, **Ricardo Maté**.

Las empresas perdieron casi el 10% de sus ingresos debido a ciberataques en el último año, según FASTLY

Las organizaciones tardan una media de hasta ocho meses en recuperarse de los efectos negativos de las brechas de seguridad, que incluyen cuentas de clientes comprometidas y pérdida masiva de datos. Así lo destaca **Fastly** en la más reciente versión de su ‘Informe anual global de ciberseguridad’, en el que revela el notable impacto de los ciberataques en las principales empresas de todo el mundo, víctimas de un promedio de 46 ciberataques conocidos este año. Esta encuesta también se hace eco de los efectos financieros de las brechas de seguridad. Por ejemplo, las empresas han perdido el 9% de sus ingresos en los últimos 12 meses, como resultado

ATAQUES MÁS COMUNES

1	29%	Ransomware
2	28%	DDoS
3	25%	Con vulnerabilidades en software open source
4	22%	Ingeniería social
5	20%	APIs / ataques contra aplicaciones web

directo de los ciberataques sufridos (una cifra que en España alcanza el 8%). Junto a ellos, las empresas también destacan las interrupciones de la red (34%), la pérdida de datos (29%), la desconexión de aplicaciones web (24%) y el compromiso de cuentas de clientes (22%).

“Asimismo, el hecho de que sólo el 55% de las herramientas de seguridad se utilicen en su totalidad es representativo, suponiendo una importante cantidad de dinero infrutilizado en la lucha contra los ciberdelincuentes. En España esta cifra es algo superior, con un 63% de las herramientas de ciberprotección completamente desplegadas”, destaca el informe.

<TEHTRIS>

FACE THE UNPREDICTABLE

XDR

TEHTRIS XDR PLATFORM ERES EL PROTECTOR DEL CIBERESPACIO

HIPERAUTOMATIZA TU SEGURIDAD



TEHTRIS recognized as a Representative Vendor in the 2023 Gartner® Market Guide for Mobile Threat Defense.*

MADE IN
EUROPE

afaq
ISO 27001
Information
Security
AFIRM CERTIFICATION
2009/102155

CONTACTA
CON NOSOTROS

spain@tehtris.eu
tehtris.com

Gartner, Market Guide for Mobile Threat Defense, January 2023.
*GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation.
Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

La empleabilidad, eje diferenciador de la FUNDACIÓN GOODJOB y del foco de su multitudinaria convocatoria dentro de las Jornadas STIC

Dentro de las acciones de visibilidad de su propósito fundacional, y en el contexto de las XVII Jornadas STIC, organizadas por el **Centro Criptológico Nacional (CCN)** en conjunción con el **Mando Conjunto del Ciberespacio (MCCE)** —celebradas el pasado noviembre en las instalaciones madrileñas de Kinépolis—, tuvo lugar en su seno, el día 29, una multitudinaria sesión vespertina a instancias de la **Fundación GoodJob** en la cual se visibilizó el balance de su actividad. Dentro del alcance de sus diferentes áreas, sin duda el énfasis en esta ocasión se centró en los asuntos más próximos a la ciberprotección, dimensión tecnológica en la que la fundación viene haciendo foco intenso y con contrastado éxito, como es el **programa #include**, con ya ocho ediciones a sus espaldas.

La sesión, incorporada a la programación por deferencia y apoyo expreso de la principal entidad anfitriona, estuvo conformada por dos debates de gran interés y registró una multitudinaria asistencia. El primero de ellos, titulado “Ciberseguridad, la gran autopista a la integración laboral en la tecnología. Caso de éxito”, contó con **Dante Cacciatore**, **Joaquín Cidoncha** y **Kamil Svec**, todos del grupo Telefónica, quienes junto al Director General de la Fundación, **César López**,

y el Director Académico de los programas #Impact, **Román Ramírez**, profundizaron en la experiencia acumulada por la multinacional española de telecomunicaciones en tanto exitosa pionera en integración.

Por su parte, en el segundo debate, “Presente y futuro de las posiciones

Testa, participante de los Programas #Impact, **Arancha Jiménez**, VP Cybersecurity Services and Products para Iberia en **Eviden**, y con **César López**, como conductor.

nen inversiones por ello— en incentivar la impartición de conocimientos sin cerrar el círculo virtuoso.

GOODJOB, premiada en los Zero Project 2024

Por otro lado, a comienzos de diciembre se supo que la Fundación GoodJob fue una de las organizaciones premiadas en los **Zero Project 2024**, de entre



las 523 organizaciones presentadas. Este premio, uno de los más reconocidos en Europa, promovido por Zero Project, es una iniciativa de Essl Foundation, institución austriaca que busca la construcción de un mundo sin barreras para el ejercicio de los derechos de las personas con discapacidad, mediante la búsqueda y difusión de soluciones innovadoras para la inclusión.

Fueron los Programas #IMPACT de empleabilidad por los que la Fundación obtuvo el galardón. Estos programas de capacitación tienen como objetivo dar acceso al mercado de trabajo ordinario a Personas con Discapacidad en el sector de la tecnología. Hasta el momento han sido cerca de 800 las personas con discapacidad preparadas para ocupar puestos junior en empresas tecnológicas y más del 70% de ellas ya tiene un trabajo estable en alguna de estas empresas.



César López



Los diagnósticos de la situación, mayormente halagüeños, no fueron óbice para alertar del innegable impacto de la IA y al tiempo, saber servirse de ella para potenciar las capacidades de aprendizaje de cara a la inserción laboral y social de personas con discapacidad. En esa línea Fernández enfatizó la la-



Luis Fernández

junior en ciberseguridad”, participó **Luis Fernández**, editor de SIC —co-impulsora del programa #include desde sus inicios— junto con el ya citado Román Ramírez —cofundador de **RootedCON**—; **Luis Jiménez**, subdirector de **CCN-CERT** y también firme convencido de la iniciativa; **Mónica Espinosa**, directora del **Centro de Innovación y Competencias en Ciberseguridad de la Agencia Catalana de Ciberseguridad**, **Jorge Uyá**, COO de **Innotec Security Part of Accenture**, **Jorge**



bor de GoodJob, en tanto agente diferenciador en cuanto a empleabilidad respecto al resto de entidades que, con mayor o menor compromiso de formación genuina, exclusivamente promueven y/o se centran —y obtie-

EL CONSEJO DE LA UE reúne a más de 500 expertos en la ‘Conferencia Octopus 2023’, en Bucarest, para luchar con éxito contra el cibercrimen

El **Consejo de Europa** reunió, a finales de 2023, a más de 500 expertos en cibercrimen de todo el mundo en Bucarest (Rumania) para discutir las mejores prácticas para asegurar e intercambiar evidencia electrónica y fortalecer la cooperación internacional en la ‘XIV Octopus Conference’, analizando también los retos de la Oficina del **Programa de Cibercrimen del Consejo de Europa (C-PROC)**, que ha cumplido una década de vida. Durante los tres días que duró, se celebraron 14 apartados especializados en temas como a legislación sobre delitos cibernéticos, el intercambio de información, la explotación,

las investigaciones financieras o el uso seguro de la inteligencia artificial, entre otros.

Además, se puso en valor el incremento de paí-

ses que se adhiriendo al Convenio de Budapest del Consejo de Europa, suscrito por 69 estados —los últimos en sumarse han sido Brasil, Nigeria y Camerún—, además de otros 23 que estudian firmarlo y 130 que han alineado su legislación a lo emanado por este foro.

“El cibercrimen afecta los valores e instituciones fundamentales de nuestras sociedades democráticas: desde la interferencia electoral hasta los ataques contra infraestructura crítica. Necesitamos mantenernos al día, o incluso estar a la vanguardia, ya que las nuevas tecnologías se desarrollan a una velocidad asombrosa”, destacó en su clausura su secretario general adjunto, **Bjørn Berge**.



SECURMÁTICA²⁰²⁴

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

Manos a la obra...



... y bien acompañados

Organiza

Revista

SIC

www.securmatica.com

8 · 9 · 10 OCTUBRE

Para analizar sus retos, Leet Security celebró un foro de expertos

Certificaciones y automatización, claves para la protección de la cadena de suministro, según usuarios, proveedores y organismos

Leet Security (an Uptime Company) celebró una jornada, bajo el título 'Del caos a la eficiencia en la ciberseguridad de la cadena de suministro', para hablar de sus retos, la cual comenzó presentando su CEO, **Antonio Ramos**, actualmente *founding partner*, y contó con el *chief corporate development officer* de **Uptime Institute**, **Ali Moinuddin**, destacando los retos de las infraestructuras digitales en un mundo interconectado, "cuya superficie de ataque se ha ampliado con el uso intensivo de la nube, incrementando la complejidad de su protección".

Durante su intervención, Moinuddin resaltó el trabajo de la compañía, presente en 25 países, y conocida por su estándar de seguridad para centros de datos, el conocido Tier, además de avanzar todo lo que supondrá la llegada de normativas como DORA. Frente a ello, resaltó que hace falta "mejor visibilidad y planes adaptativos al riesgo", para evitar la "tormenta perfecta".

La jornada también contó con una mesa de debate para analizar la protección de la cadena de suministro desde el punto de vista del usuario, con **Damián Ruiz (Singular Bank)**, **Pedro Benítez (Amadeus)**, **Hermínio del Campo (CCI)** y **Luis Paredes (Ingesan OHLA)**.

En ella, se profundizó sobre la situación en ciberseguridad en diferentes entornos. "Las gran-

des compañías tienen más capacidades, pero también más problemas, y no hay una entidad financiera que tenga capacidad para auditar la ciberseguridad propia y la de sus proveedores y por eso nació Pinakes", comentó Del Campo. "Es fundamental la responsabilidad en una cadena de



suministro, apostar por modelos tempranos para que antes de la contratación se sepa de forma clara qué le vas a exigir, a través de homologaciones o certificaciones", explicó Ruiz. "Pero no es fácil, ya que, por ejemplo, nosotros trabajamos en un entorno internacional con los proveedores muy distribuidos", añadió Beneitez. De cualquier forma, todos los participantes, moderados por Ramos, estuvieron de acuerdo en la importancia de apostar por la homologación para mejorar en ciberprotección.

A continuación, se debatió la protección cibernética de la cadena de suministro bajo la mirada

del proveedor. Un debate, moderado por **Alfonso Pastor**, socio de Leet Security, en el que participaron **Eduardo Solís (Innotec Security)**, **Rodrigo Hornos (IBM)**, **Javier Palacios (Avvale)** y **Antonio Navas (Kyndryl)**. En él, se dio a conocer la perspectiva del proveedor destacando la mayor complejidad en ciberprotección que obliga a "industrializar y automatizar al máximo", para, también, suplir el déficit de profesionales que hay, así como la necesidad de contar con certificaciones, como el ENS, para trabajar en sector público o formar parte de organizaciones de respuesta a incidentes como **First** o **Csirt.es**, entre otras. **Revista SIC** ofrece en su web un cuadro actualizado, cada mes, con los equipos, con sede en España, en cada organización—. Igualmente, destacaron la necesidad de colaborar entre clientes y proveedores para optimizar al máximo el servicio y los mecanismos de resiliencia en situaciones críticas.

Por último, se celebró una mesa redonda para conocer el punto de vista institucional de la protección en la cadena de suministro, en la que estuvieron **Elena de la Calle (DSN)**, **Alberto Francoso (OCC)**, **Jesús Feliz (Incibe)**, y **Pedro M. Mosquera (CNPIC)**. Todos resaltaron la importancia que tendrán normativas como DORA y NIS2 y su armonización y cumplimiento sin resultar una carga excesiva para las empresas.

El área de Ciberseguridad de KPMG en España crece un 33% en el último ejercicio y pone en marcha una nueva unidad de servicios

Dentro de la estrategia del área de ciberseguridad para continuar dando servicios de valor a sus clientes, **KPMG** se reforzó a finales de 2023 con la incorporación de



De izq. a drcha, Alejandro Belón, Rubén Muñoz, Karen Gaines, Marc Martínez y Francisco Guirado

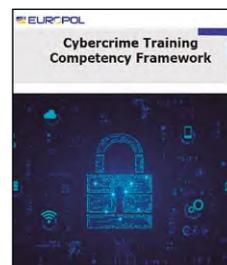
Karen Gaines en calidad de socia responsable de los servicios de Managed Detection and Response (MDR) y Threat Intelligence. Junto a ella, lo hicieron un equipo altamente cualificado formado por un director, **Rubén Muñoz**, y dos *senior managers*, **Alejandro Belón** y **Francisco Guirado**. Todos ellos ayudarán al desarrollo y crecimiento de esta área que lidera Gaines, cuyo objetivo para este ejercicio es alcanzar los 25 profesionales en MDR. Así, este equipo se ocupará de la nueva área de negocio de servicios gestionados de ciberseguridad en la protección, detección y respuesta 24x7 desde su SOC. Incluye servi-

cios como MDR, Threat Intelligence, Cloud Sec, Data Sec, así como Seguridad IT/OT basada en IA.

"Estamos muy orgullosos del trabajo que venimos haciendo para nuestros clientes, en un entorno ciber cada vez más complejo y, también, del crecimiento que nos ha acompañado en los últimos años", señala el socio responsable de ciberprotección de la consultora en España, **Marc Martínez**. "Pero no nos conformamos con lo conseguido y queremos ampliar el catálogo de servicios que ofrecemos y, por ello, la incorporación de este equipo que viene a desarrollar los servicios de MDR, es clave para el futuro". De hecho, el área de ciberseguridad de la consultora en España continúa creciendo, con un incremento de sus ingresos de un 33% en el último ejercicio

EUROPOL propone un marco de competencias de formación en materia de ciberdelincuencia

El organismo europeo policial ha publicado un documento en el que detalla cómo debería ser el 'Marco de Competencias para la Capacitación en Delitos Cibernéticos'. En él describe las habilidades y capacidades necesarias para los agentes del orden que trabajan en investigaciones de delitos cibernéticos, así como las habilidades necesarias para el manejo de evidencia digital para combatir las formas modernas de delincuencia. El documento, en el que



han trabajado desde el **Grupo de trabajo sobre ciberdelincuencia de la Unión Europea (EUCTF)**, hasta **la Agencia de la Unión**

Europea para la Formación Policial (CEPOL), el **Grupo Europeo de Formación y Educación en Ciberdelincuencia (ECTEG)**, **Eurojust** y la **Red Europea de Ciberdelincuencia Judicial (EJCN)**, pretende ayudar a los agentes que trabajan en la lucha contra el cibercrimen, sin importar el país, estableciendo un camino formativo común.



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

La ingeniería social y el *phishing* son las técnicas más empleadas para acceder a las redes de las empresas a través de la nube, según Netskope

El rápido crecimiento en la adopción de aplicaciones de IA generativa en entornos corporativos abre nuevas superficies para los ciberataques

Netskope ha dado a conocer las conclusiones de su 'Informe Anual sobre Nube y Amenazas, 2024', en el que alerta del rápido crecimiento en la adopción de aplicaciones de IA generativa en la empresa y los riesgos emergentes que se derivan de ello. Un ejemplo, es que, según la investigación, más del 10% de los empleados de las empresas acceden, al menos, a una aplicación de IA generativa –como ChatGPT–, cada mes, en comparación con solo el 2% de los usuarios corporativos que lo hacían hace un año. El informe destaca que se espera que el 25% de los usuarios más avanzados incrementen significativamente la actividad de la IA generativa este año, por cuanto cada vez más profesionales encuentran la forma de usar esta tecnología en su día a día.

Asimismo, la investigación también analiza el estado de la ciberprotección en la nube recordando que, en 2023, el número de aplicaciones en este entorno para usuarios empresariales creció un 19% pasando, en sólo dos años, de usar cada empleado de 14 a 20 aplicaciones. De media, se interactúa con entre 11 y 33 aplicacio-

nes *cloud* al mes, aunque un 1% llega a utilizar hasta 96 aplicaciones.

Como dato curioso, se calcula que los empleados 'cayeron' tres veces más en estafas de suplantación que en la descarga de software malicioso.

Por entornos, los más buscados por los ciberdelincuentes fueron aplicaciones en la nube y los sitios de compras en línea, seguidos de los portales bancarios, las redes sociales y gobiernos, que también experimentaron un notable aumento.

Por último, el informe recuerda que la mayoría de los ciberdelincuentes, gran parte desde suelo ruso, tuvieron motivaciones económicas, siendo los adversarios geopolíticos, con grupos desde China, los más activos contra los usuarios de Asia e Iberoamérica.

El documento finaliza con unas recomendaciones sobre cómo limitar el acceso solo a aquellas aplicaciones que se ajusten a los propósitos legítimos de las empresas, garantizar la habilitación y adopción de manera segura de aplicaciones de IA y continuar invirtiendo para reducir el riesgo de ingeniería social, incluida la formación para la concienciación de seguridad y la tecnología *antiphishing*.



Superficie de ataque

En cuanto a ciberamenazas, la forma más común en que los atacantes obtuvieron acceso inicial al pasado año fue a través de la ingeniería social. También, aprovecharon técnicas como el *phishing*, robo de credenciales y caballos de Troya para engañar a las víctimas para que descargasen e instalasen programas maliciosos.

S2 GRUPO trasladará su sede en Valencia a La Centrifugadora, uno de los edificios más singulares de la ciudad, unificando sus unidades

En las próximas semanas S2 Grupo prevé trasladar todos sus activos a la denominada 'La Centrifugadora', recinto en Valencia con más de 6.000 m² de oficinas y 700 m² de jardín, lo que permitirá unir, en un solo espacio, la dirección corporativa, su Centro de Desarrollo de I+D+i, su Laboratorio de Ciberseguridad Industrial, así como su Centro de Operaciones de Ciberseguridad y su CERT, "que es uno de los más seguros, avanzados y completos del mundo", destacan desde la compañía.

Como se sabe, La Centrifugadora, en la zona del Grao, es uno de los edificios más emblemáticos de la capital valenciana y se ubica en una antigua nave industrial de principios del siglo XX.

La compañía ha continuado su crecimiento marcado en su plan estratégico, con un 30% más de facturación y una plantilla que ya al-



canza los 650 personas –tiene previsto alcanzar el millar–, además de una amplia presencia internacional con clientes en los sectores de Distribución, Energía, Banca y Seguros, Sanidad, Industria y organismos de la Administración Pública. Asimismo, su presencia en Europa

se ve reforzada por su papel como uno de los miembros fundadores de la ECSO (Asociación Europea de Ciberseguridad) y por formar parte del 'Partnership Board' de esta asociación, que es el órgano encargado de colaborar con la Comisión Europea para la definición de la estrategia de I+D en ciberseguridad de los próximos años.

A su sede de Valencia, S2 Grupo suma sus oficinas en Madrid, Sevilla, Barcelona, San Sebastián, Bruselas, Bogotá, Brindisi, Santiago de Chile, México, Róterdam y Lisboa.

AKAMAI World Tour Madrid 2023 muestra nuevos enfoques de seguridad y nube en su 25 aniversario

Akamai Technologies celebró su evento anual, el World Tour, en el Real Casino de Madrid, aprovechando la ocasión para conmemorar los 25 años de la compañía.

Una jornada que contó con expertos de la industria, referentes y profesionales de la tecnología que asistieron a diferentes conferencias en las que sus especialistas mostraron nuevas formas de crear, escalar y proteger aplicaciones que garantizan la agilidad necesaria para innovar, impulsar el

valor para sus clientes y eliminar las brechas de su marco Zero Trust.



Entre otras intervenciones, el vicepresidente Regional de Akamai para España y Portugal, Francisco Arnau, repasó las contribuciones de la compañía al mundo digital, además de plantear sus retos y presentar sus últimas innovaciones en servicios para, entre otras, gestionar sus operaciones en línea.



illumio
The Zero Trust Segmentation Company

Zero Trust Segmentation:
Evite que los ataques se propaguen por su red



Habilite su estrategia Zero Trust

- Mantener una verificación continua y basada en riesgos
- Hacer cumplir el acceso con privilegios mínimos
- Obtenga un monitoreo integral de la seguridad

Contener ransomware en minutos

- Evite que el ransomware se propague
- Identificar áreas de alto riesgo
- Construir protección a largo plazo

Fortalecer la ciberresiliencia

- Poner en cuarentena rápidamente los sistemas comprometidos
- Implementar controles granulares para limitar el alcance de los ataques
- Acelere la respuesta con alertas automáticas

Seguridad en la nube simplificada

- Identifique el riesgo evaluando los patrones de tráfico actuales
- Refuerce los controles de seguridad con recomendaciones de reglas
- Proteja los datos durante los proyectos de migración a la nube



HORIZON3.ai
TRUST BUT VERIFY

Pentesting Autónomo: Encuentre, corrija y verifique continuamente su superficie de ataque explotable.



Internal Pentesting

Haga pruebas sobre “una posible brecha” y ejecute un pentest interno a su infraestructura para entender lo que un atacante podría hacer una vez dentro de su red.

External Pentesting

Con el sistema autónomo NodeZero External Pentesting, alojado completamente en el cloud de Horizon3 en Europa, puede evaluar de forma rápida y precisa la postura de seguridad de su organización desde la perspectiva de un atacante que intenta traspasar su perímetro.

N-Day Pentesting

Analiza rápidamente si una vulnerabilidad N-Day es explotable en su entorno. NodeZero proporciona exploits para esas Vulnerabilidades N-Day así como nuevas amenazas 0-Day que surgen.

AD Password Audit

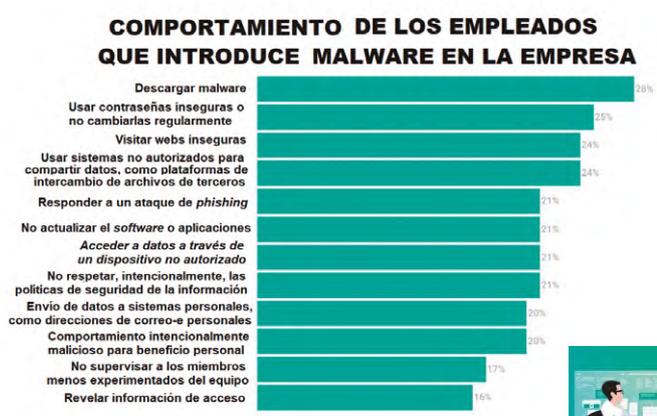
Los atacantes no piratean, inician una sesión. Las credenciales son las culpables de un alto porcentaje de ataques. Verifica continuamente la efectividad de sus políticas de credenciales para asegurarse de no dar la opción a acceder a actores no deseados.

En España, en los últimos dos años, el 12% de los incidentes corporativos se produjeron porque el personal se saltó el protocolo de seguridad

Según un reciente estudio de **Kaspersky** en España, más de tres cuartas partes (74%) de las empresas sufrieron al menos un ciberincidente en los últimos dos años, de los cuales el 70% se consideraron 'graves'. Y entre las principales razones de esta situación, los participantes apuntan la falta de personal cualificado. Por ello, el 34% reco-

nocieron que tienen previsto invertir en la externalización de la ciberseguridad en los próximos 12 o 18 meses. Asimismo, el 40% mostraron su interés en implantar, en el próximo año, un software que gestione automáticamente su ciberprotección, mientras que el 22% están debatiendo el tema.

Por otro lado, la multinacional presentó las conclusiones de otro interesante estudio sobre el



papel que juegan los empleados en las brechas de ciberseguridad. En él, se resalta que, en España, en los últimos dos años, el 12% de los incidentes corporativos se produjeron porque el personal se saltó el protocolo de seguridad. Esta cifra es casi igual a los daños causados por las brechas, un 36% de ellas por culpa de cibercriminales.



En cuanto a las razones de los problemas de ciberprotección por empleados, el informe explica que una cuarta parte (8%), en los dos últimos años, se produjeron por el uso de contraseñas débiles o por no cambiarlas a tiempo, seguidas (13%) por visitar webs no seguras y (16%) por no actualizar el software o las aplicaciones cuando es necesario. A ello se suma el empleo de dispositivos o servicios no autorizados (18%) e, incluso, un 8% por usar aplicaciones 'en la sombra', sin conocimiento del equipo de seguridad ni TI.

Centro de Transparencia en África

Kaspersky también ha anunciado la inauguración de su primer Centro de Transparencia en África. Ubicado en Kigali, Ruanda, se abre como parte de su Iniciativa Global de Transparencia, cuyo fin es demostrar que sus soluciones son de total confianza. Con esta nueva apertura, la multinacional amplía su red a once países de Europa, Asia-Pacífico, Norteamérica, Latinoamérica, Oriente Medio y África.

BEDISRUPTIVE amplía su sede en Madrid y ya es miembro 'Gold' de la RNS

La por entonces secretaria de Estado de Digitalización e IA del Gobierno de España, **Carme Artigas**, inauguró a finales del año pasado la



ampliación de las oficinas de **BeDisruptive**, acompañada por **José Ángel Delgado**, CEO de la empresa, **Xavier Mitxelena**, director general, y **Begoña Villacís**, directora global de Relaciones Institucionales. "Se trata de una buena demostración de la capacidad de nuestro país para convertirse en un polo de atracción de talento" y "la consolidación de un proyecto apasionante, la recompensa al trabajo bien hecho". Por su parte, Mitxelena consideró "imprescindible que las empresas, tanto las grandes como las pymes, entiendan que hay que invertir en seguridad", ya que "no es un gasto, es una inversión" y un "elemento de competitividad y resiliencia".

Desde que inaugurase su oficina en Madrid, en 2022, BeDisruptive no ha parado de reforzar todos sus departamentos con personas de elevada cualificación. Así, actualmente, aún

en sus filas a más de 250 empleados –34% mujeres–, de los cuales más de 140 trabajan en

nuestro país.

Reconocimiento de la RNS

Además, la empresa ha sido encuadrada en la **Red Nacional de SOC (RNS) del Centro Criptológico Nacional**, con el nivel 'Gold' y de la que ya forman parte 29 entidades proveedoras de un total de 151 miembros. Este hito reconoce el alto nivel de participación de la compañía como proveedor en la RNS y otorga acceso inmediato a toda la información compartida y consolidada en dicha red. También es miembro de pleno derecho en organizaciones como **FIRST** y **TF-CSIRT** y **CSIRT.es**, además de estar incluidos en el inventario de Enisa. Además, la compañía ha sido reconocida como primer **partner** estratégico de la asociación **Women4Cyber Spain**.

Se publica el 'Indicador de ciberseguridad', para analizar la madurez de cada compañía, y guías para implementar la IA de forma segura

A finales de año, se publicó el Código de Buen Gobierno de la Ciberseguridad, basado en 13 principios y con el objetivo de proponer un modelo que ayude a los órganos de gobierno de las organizaciones y, en especial, de la Administración, a tomar las decisiones adecuadas. De ahí que sea necesario su implementación desde el principio.

Aprovechando las 'XXV Jornadas Internacionales de ciberseguridad' del **ISMS Forum**, también se dio a conocer el primer estudio que refleja el coste para las empresas de no aplicar medidas de protección, bajo el título 'Indicador de ciberinseguridad'. Sus responsables destacaron, además, el impacto que tienen los ciberataques frente al PIB español –en torno a 110.000 millones de euros– subrayando que las pérdidas generadas por el cibercrimen son muy importantes en nuestro



país. El documento complementa a la cuarta edición del 'Indicador de madurez en ciberseguridad', de 2023.

Asimismo se han publicado cinco informes relacionados con la IA, que tratan desde su gobernanza en España, hasta de la importancia de los profesionales de seguridad utilizando la nueva herramienta, su ética y *compliance*, políticas de ciberseguridad en las empresas, así como los modelos de gobierno que ayuden a desarrollar nuevas estrategias.

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.



Casi uno de cada tres empleados no entiende el proceso para dejar de usarla, según Delinea

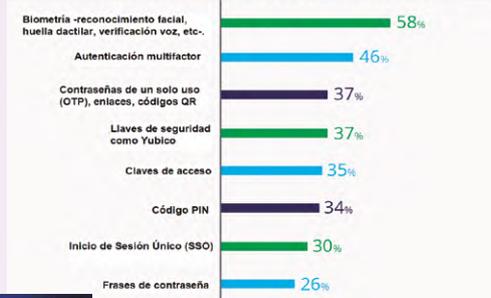
La tecnología heredada y el factor de doble autenticación frenan la evolución hacia una autenticación sin contraseña en el trabajo

Las contraseñas no están muertas... Sólo están evolucionando. Así lo destacan el 68% de los 300 expertos preguntados, responsables de la toma de decisiones de IT de EE.UU., en el informe 'El futuro de las contraseñas en el lugar de trabajo', de **Delinea**, en el que más de la mitad (53%) consideró que simplemente están evolucionando hacia algo nuevo.

El estudio, realizado junto a **Censuswide**, destaca que las soluciones con las que los usuarios ya están familiarizados en su vida personal, son también las que pueden sustituir a las contraseñas en el lugar de trabajo, como el caso de la biometría (58%), otras tecnologías de autenticación multifactor (46%), contraseñas de un sólo uso (37%) y *passkeys* (35%).

Además, ha evidenciado que la mayoría de las organizaciones aún están a años de distancia de una realidad sin contraseñas. Mientras que el 30% afirma que su organización ya ha iniciado esta transición, el 36% manifiesta que aún le faltan 1-2 años y el 21% admite que le faltan 3-4 años. Según los encuestados, en su camino se interponen varios obstáculos: para el 43%, el prin-

¿CON QUÉ SOLUCIONES TÉCNICAS, SI LA HAY, ESPERAN REEMPLAZAR SUS CONTRASEÑAS?



cipal obstáculo son las plataformas y aplicaciones heredadas que requieren contraseñas y MFA; para el 37% es la necesidad de métodos de autenticación coherentes en todas partes; y, para el 28%, el principal freno son los empleados que no entienden o no confían en los procesos sin contraseña. Asimismo, el 95% ha afirmado que sus empresas deben cumplir con al menos un conjunto de requisitos de conformidad, lo que exige a las organizaciones demostrar controles de acceso que pueden complicarse al adaptarse a nuevos

métodos de autenticación. A pesar de esta situación, el 35% espera que el acceso a los sistemas del lugar de trabajo requiera retos de MFA en el inicio de sesión, mientras que el 19% espera un futuro en el que no se necesite el nombre de usuario, ni contraseña. Cerca del 60% también han indicado que sus organizaciones utilizan una solución de gestión de acceso privilegiado (PAM) para gestionar las contraseñas. Por último, el informe también arroja luz sobre las perspectivas acerca de la Inteligencia Artificial (IA) y su papel en la ciberseguridad, por cuanto el 83% de los encuestados afirma que ve la IA como un 'defensor', aunque la mitad también admite que podría ser una amenaza.

"El término 'sin contraseña' suele suscitar una respuesta contundente, ya sea por parte de quienes afirman que las contraseñas nunca morirán o de quienes afirman que desaparecerán inevitablemente. Nuestros últimos estudios demuestran que no tiene por qué ser ni lo uno ni lo otro, y que hay nuevas opciones de autenticación que están llevándonos a un futuro en el que las contraseñas seguirán existiendo, pero en un segundo plano", ha explicado el CMO de la empresa, **Chris Smith**.

El 66% de los ataques DoS tienen motivaciones políticas, según ENISA

Se estima que el 66% de los ataques de denegación de servicio (DoS) están motivados por motivos políticos o agendas activistas. Así lo destaca uno de los últimos informes de la



Agencia de Ciberseguridad de la UE (Enisa), tras analizar más de 300 incidentes de enero del 2022, a agosto del 2023. El organismo resalta que este tipo de incidentes "se han vuelto más fáciles, más baratos y más agresivos que nunca. El surgimiento de nuevos conflictos armados en todo el mundo actuó como combustible para nuevas oleadas de ataques DoS en los que los actores de amenazas recién formados eligen objetivos sin temor a repercusiones".

Por ello, con este documento, Enisa espera "proporcionar una mejor comprensión de este tipo de amenazas analizando las motivaciones y su impacto, al mismo tiempo que busca crear conciencia sugiriendo recomendaciones de prevención y remediación". Además, el

informe destaca que en los últimos años los ataques DoS han aumentado en número, especialmente en la administración pública, y se han vuelto más fáciles y agresivos que antes, en gran parte debido a razones geopolíticas. A su vez, recuerda que el panorama actual de DoS está muy influenciado por el surgimiento de los recientes conflictos armados en todo el mundo y, especialmente, por el de Rusia-Ucrania.

Entre otros datos de interés también resalta que el sector más afectado por este tipo de incidentes es el de Administración Pública, que ha recibido el 46% de los ataques, así como que un 8% causaron un gran impacto. También plantea que los principales desafíos para hacerles frente pasan por mejorar la detección, descripción y análisis, por cuanto siguen siendo "muy complejas", pidiendo mejorar la información sobre este tipo de incidentes y sus responsables.

ALEMANIA gana el Reto Europeo de la Ciberseguridad, logrando ESPAÑA una meritoria décima posición



Alemania se alzó con el primer puesto del Desafío Europeo de Ciberseguridad 2023 (CECA), a finales de 2023, seguida de Suiza y Dinamarca. El campeonato, cuya novena edición tuvo lugar en la **Universidad Noruega de Ciencia y Tecnología (NTNU)**, reunió a 34 equipos de la UE, además de países asociados e invitados como Canadá, Georgia y Serbia. Se trata de un ejercicio anual, con desafíos relacionados con la seguridad, el hardware, la seguridad web y móvil y la ingeniería inversa, coordinado por la **Enisa**, para animar a los jóvenes a seguir una carrera en el sector desafiando sus habilidades. Y es que, "la experiencia técnica no es suficiente para tener éxito. Los participantes deben trabajar en equipo en un entorno complejo, de forma rápida y eficiente", explican sus impulsores. La próxima edición, a finales de 2024, será en Italia.

Enséñale los dientes al ransomware.

OBTÉN LA DEFENSA MÁS FERROZ
CONTRA AMENAZAS COMPLEJAS.



CYBERPROOF presenta su XDR administrado para GOOGLE CHRONICLE

CyberProof ha cerrado un acuerdo con Google para “mejorar y optimizar las defensas para los clientes empresariales de Google Chronicle”. Fruto de él y señalando que “las operaciones de seguridad deben trasladarse a arquitecturas nativas de la nube

CyberProof
A UST Company



para manejar datos de gran volumen y gran escala”, Google Chronicle ha destacado las capacidades avanzadas de Google Cloud Platform (GCP), así como la búsqueda de Google, para ofrecer lo que se considera ampliamente como capacidades de próxima generación. Por su parte, CyberProof ha explicado su apuesta por facilitar la monitorización para reducir costes y mejorar la detección y respuesta.

“La experiencia de CyberProof ayudando a grandes organizaciones multinacionales en industrias altamente reguladas a pasar del uso de infraestructura de seguridad local heredada

a la nube está alineada con la visión de Google para el futuro de la seguridad”, indican, a la vez que recuerdan que, “en el entorno empresarial y tecnológico actual, el cambio rápido es la nueva norma. Las arquitecturas de seguridad que estén preparadas para el futuro y que admitan tecnologías emergentes como GenAI son fundamentales”. Por ello, CyberProof ofrece un modelo de servicio de operaciones de seguridad cogestionado habilitado por su plataforma de servicio CyberProof Defense Center, que permite una transformación centrada en los resultados de seguridad.

“Es especialmente importante que los proveedores de servicios de seguridad ofrezcan capacidades de ingeniería profundas para ayudar a los clientes a implementar arquitecturas de protección de próxima generación. Hay infinitas oportunidades para reducir el riesgo y los costes cibernéticos, pero hay muchas incógnitas y los errores son costosos. Nuestra relación estratégica con Google nos ayuda a atender mejor las necesidades de nuestros clientes y a impulsar la innovación rápidamente”, ha explicado el director ejecutivo de CyberProof, **Tony Velleca**.

La AEPD publica una guía sobre el uso de datos biométricos para controles de presencia y acceso

La **Agencia Española de Protección de Datos (AEPD)** ha publicado la Guía ‘Tratamientos de



control de presencia mediante sistemas biométricos’, un documento que fija los criterios para la utilización de la biometría para el control de acceso, tanto con fines laborales como no laborales, estableciendo las medidas que deben tenerse en cuenta para que un tratamiento de datos personales que utilice esa tecnología cumpla con el RGPD, entre otras normativas. En el documento, el organismo considera el tratamiento de datos biométricos, tanto para identificación como para autenticación, como un tratamiento de alto riesgo que incluye categorías especiales de datos. Tal y como establece el RGPD, para poder

tratar esas categorías es necesario que exista una circunstancia que levante la prohibición de su tratamiento y, además, una condición que lo legitime.

Sistema de verificación para menores

Además, la AEPD, coincidiendo con su 30 aniversario, ha presentado un sistema de verificación de edad –plasmado en un decálogo– para proteger a los menores ante el acceso a contenidos de adultos en Internet.

Asimismo, ha presentado su ‘Estrategia Global sobre menores, salud digital y privacidad’, con 10 actuaciones prioritarias y 35 medidas agrupadas en tres ejes.

BREVES

■ Como es habitual, **Revista SIC** publica en su web la información actualizada de los equipos de respuesta a incidentes –conocidos como CERT/CSIRT– con sede en España. En su más reciente actualización, destacan dos cambios de denominación notables: **BCSC** pasa a ser **Cyberzaintza** en **FIRST** (no en los otros organismos), e **Entelgy Innotec CSIRT** pasa a ser Innotec Security CSIRT en FIRST, **Trusted Introducer** y **CSIRT.es**, pero sigue siendo Entelgy Innotec CSIRT en el listado de **Enisa**.

■ **María Nogales**, Global Head Cyber External Engagement & Governance de **Banco Santander**, ha sido distinguida por **FS-ISAC** con su galardón ‘Global Leader Award para EMEA 2023’, por su excelente labor y apuesta en pro de la colaboración en ciberseguridad. “Estamos increíblemente orgullosos de lo que podemos lograr como comunidad para realizar cambios significativos en la forma en que abordamos el panorama de amenazas”, destacó en el acto de entrega.

■ La **Cloud Security Alliance (CSA)** ha presentado su Certificado de Competencia en Confianza Cero (CCZT) y materiales de capacitación para permitir a los profesionales desarrollar el conocimiento que necesitarán para implementar y gestionar una estrategia Zero Trust. Con esta novedad, pretende proporcionar una comprensión profunda de esta arquitectura, sus componentes y su funcionamiento. También incluye las mejores prácticas publicadas por fuentes como la propia CISA o NIST, entre otros aspectos.

■ **Prosegur** ha reportado un crecimiento del 10% en su negocio de *security* durante 2023, además de celebrar el primer aniversario de su iSOC en Madrid, consolidando su compromiso con el modelo de seguridad híbrida, clave en su crecimiento. Actualmente, su red iSOC alcanza los 14 centros, con 10 nuevas aperturas en 2023. “El iSOC es fundamental en nuestra estrategia de Seguridad Híbrida, conectando a nivel mundial a más de 100.000 expertos y más de un millón de dispositivos”, destacó su CEO, **Fernando Abos**.

■ **IBM** y **Meta** han puesto en marcha la **AI Alliance** como una comunidad internacional de desarrolladores, investigadores y adoptantes de tecnología de referencia que colaboran juntos para promover una IA abierta, segura y responsable. De momento, cuenta con más de 50 miembros fundadores y colaboradores a nivel mundial. Por otro lado, IBM ha firmado un contrato con la **Agencia de Información y Comunicaciones de la OTAN** (Agencia NCI) para ayudar a fortalecer su postura de ciberprotección.

■ **Luis Pardo**, director general de **Ametic** y **Eduvigis Ortiz**, fundadora y presidenta de **Women4Cyber Spain**, sellaron un convenio de colaboración con el propósito de unir fuerzas en incrementar el posicionamiento de la mujer en campos como la ciberseguridad y la protección de datos, a fin de contar con una ecosistema social y empresarial más inclusivo, diverso y participativo en España. Cabe destacar, también, la celebración en Madrid, el pasado 14 de noviembre, de la primera Women4Cyber Conference, que convocó a 200 asistentes internacionales.

■ El **Instituto de Investigación Sanitaria La Fe (IIS La Fe)** se ha convertido en el primer instituto de investigación sanitaria de España en obtener la conformidad con las exigencias del Esquema Nacional de Seguridad (ENS), por parte del **Centro Criptológico Nacional (CCN)**.

¿Sabías que...

Fujitsu está celebrando 50 años en España?

Contando actualmente con 3 centros de servicios de ciberseguridad:

- Valencia: Endpoint Protection Center (EPC)
- Sevilla: Cybertrust Center (CTC) (*)
- Barcelona: Centro de servicios de Ciberseguridad para Sanidad

(*) ENS – Nivel alto, miembros de Red Nacional de SOCs, Trusted-Introducer, FIRST y CSIRT.es

A satellite night view of the Iberian Peninsula, showing the glowing lights of cities and towns across Spain and Portugal. The image is used as a background for the right half of the page.

50

50 años presentes en el futuro de España

La edición más multitudinaria e internacional, entre presenciales y remotos, convocó a más de 13.000 profesionales de 37 países

Las Jornadas STIC, broche de oro de la 'ciberpresidencia' europea española, anuncian nuevos retos para 2024, presentan herramientas y apuestan por la colaboración

Las **XVII Jornadas STIC CCN-CERT y V Jornadas de Ciberdefensa ESPDEF-CERT**, celebradas a finales de noviembre, volvieron a demostrar la madurez y capacidades del sector privado y público en ciberseguridad convocando una potente participación: 220 ponentes y la asistencia de 6.000 profesionales, de forma presencial, y de 7.000 conexiones en línea, de casi 40 países. Durante tres días, representantes del sector público español e iberoamericano, de la **Comisión Europea**, compañías estratégicas y de servicios esenciales, así como empresas especializadas y del ámbito universitario debatieron y analizaron los retos de este 2024 con normativas como NIS2, la amenaza de la IA en ataques más sofisticados y complejos, ciberprotección 5G, así como la creación de una Red Europea de SOC, la EN-SOC –con medio millón de euros de presupuesto para su puesta en marcha–, y que está inspirada en la Red Nacional de SOC (RNS) española. También, estuvieron presentes los referentes del **Departamento de Seguridad Nacional**, la **Oficina de Coordinación Cibernética (OCC)** de Interior, **Incibe**, **Guardia Civil**, **Policía Nacional**, la **Organización de Estados Americanos (OEA)**, **Rooted-CON**, **CCI** y la **Fundación GoodJob**, entre otros.

Organizadas por el **Centro Criptológico Nacional (CCN)**, del **Centro Nacional de Inteligencia (CNI)**, en conjunción con el **Mando Conjunto del Ciberespacio (MCCE)**, las jornadas, además de los encuentros de la red CyClone y del Grupo de Cooperación NIS, lograron un hito histórico bajo la presidencia española: la primera reunión conjunta del grupo de Cooperación NIS y del grupo de Resiliencia de Entidades Críticas. Un año más,

SIC contribuyó a la conducción y moderación de distintas sesiones.

Como es habitual, el jefe del Departamento de ciberseguridad, **Javier Candau**, repasó el trabajo del CCN durante 2023 y sus retos para 2024, pidiendo más colaboración y mostrando también el total ofrecimiento del organismo

Apoyo institucional

El congreso fue inaugurado al alimón por la ministra de **Defensa, Margarita Robles**, la secretaria de Estado directora del CNI y CCN, **Esperanza Casteleiro**, y la por entonces aún secretaria de Estado de Digitalización e IA, **Carne Artigas**. “Estas jornadas del CCN son un impulso representativo de la colaboración y el liderazgo internacional de España en el ámbito de la ciberseguridad”, comentó Robles.

En el transcurso del acto, se rindió homenaje a la trayectoria profesional de **Miguel Ángel Ballesteros**, director general del DSN hasta ese mismo día. Asimismo, la titular de defensa entregó el Premio a la Trayectoria Profesional en favor de la ciberseguridad a **David Barroso**, fundador de la empresa **CounterCraft**, todo un ejemplo de visión y triunfo real del emprendimiento. Igualmente, durante las jornadas se conocieron los nombramientos de la nueva responsable del DSN, la general de Brigada **Loreto Gutiérrez Hurtado** y del nuevo comandante del MCCE, el vicealmirante **Javier Roca**, que participó presentando sus ‘10 reglas del liderazgo’.

No faltaron ponencias técnicas, como la realizada por **Raúl Siles**, de **Dinosec** y **GuardedBox**, bajo el título “Ecosistema móvil: ¿qué hay de nuevo, viejo? ¿MdM (Más de (lo) Mismo)?”, en la que realizó una prueba práctica con las conexiones WiFi de los teléfonos de los asistentes aprovechando una vulnerabilidad conocida y no solucionada de Apple, no crítica, pero molesta.

No faltaron tampoco diversas sesiones de debate, entre las que destacó las organizadas por la **Fundación GoodJob** sobre el presente

y futuro de las posiciones junior en ciberseguridad en el contexto de la empleabilidad y la discapacidad, multitudinarios paneles en uno de los cuales participó **Luis Fernández**, editor de Revista SIC, decidida co-impulsora de este proyecto.



Autoridades participantes en el acto inaugural



Las XVII Jornadas registraron una masiva asistencia



Javier Candau, CCN



Miguel A. Ballesteros, DSN



David Barroso, CounterCraft



Un año más SIC condujo y moderó diversas sesiones. En la imagen, el editor Luis Fernández, departe con Miguel A. Amutio, y José de la Peña, director, hace lo propio con Javier Roca



CCN-PYTEC premia a REVISTA SIC por su actividad de Formación y Concienciación relacionadas con el Catálogo CPSTIC

El departamento de Productos y Tecnologías de Seguridad TIC (CCN-PYTEC) aprovechó el módulo que coordinaba para celebrar la segunda edición de premios a los que más han apoyado y hecho por la ciberprotección de los productos y servicios que se incluyen en el catálogo. “El CPSTIC es el resultado del esfuerzo de muchos y no es más que un medio para conseguir un listado de productos confiables que puedan ser desplegados en los sistemas del Sector Público para mejorar así sus niveles de seguridad”, destacó una de sus integrantes, **Estefanía** –en el CCN no se facilitan apellidos–. Además de explicar que “con el objetivo de poder enriquecer el CPSTIC y darle la visibilidad e importancia que el Esquema Nacional de Seguridad le otorga, decidimos crear esta entrega de premios y dar visibilidad al compromiso de fabricantes, sector público y otras entidades con el proyecto del Catálogo”.

En la categoría de ‘Actividades de Formación y Concienciación relacionadas con el Catálogo de Productos y Servicios de Seguridad TIC’ los premiados fueron “unos viejos conocidos de todos nosotros, ya que ejercen con su trabajo una encomiable labor, no solo de información, sino también de formación y concienciación en el mundo de la ciberseguridad”, comenzó anunciando el galardón para **Revista SIC**, que recogió el editor de la publicación, **Luis Fernández**, en nombre también del director **José de la Peña**. “Con este premio, todo el equipo del CPSTIC



Los representantes de SIC posan con el galardón concedido



La imagen recoge a todos los galardonados en la 2ª edición de los premios y el equipo gestor de CCN-PYTEC relativo al catálogo CPSTIC

pretende agradecer el apoyo e interés demostrado por nuestro proyecto desde su primera publicación, allá por el año 2018 y el haber constituido en muchas ocasiones y por iniciativa propia de un canal de comunicación efectivo entre el equipo del Catálogo y el usuario final, al hacerse eco de su evolución”, destacaron desde CCN-PYTEC. Fernández agradeció la distinción poniendo en valor el solvente y concienzudo trabajo que se hace para mejorar el catálogo.

También fueron premiados en esta segunda edición **Google Cloud**, por su “cualificación de servicios de seguridad cloud y, sobre todo, por su planteamiento y estrategia de cualificación puesta en marcha en 2023, recogiendo el galardón **Héctor Sánchez Montenegro**, así como la tecnológica **Cisco**, a quién le fue entregada el premio a su director general, **Andreu**

Vilamitjana, en la categoría de ‘Productos de seguridad’, la **Dirección General de Racionalización y Centralización de la Contratación del Ministerio de Hacienda y Función Pública**, en el apartado de ‘Organismos públicos’, recogido por su subdirector general adjunto, **Alberto Ramallo** y, por último, en la categoría de pymes, el galardón fue para **Dinosec**, cuya socia fundadora, **Mónica Salas** recogió el galardón, junto a todo el equipo de la empresa, también propietaria de **GuardedBox**.

Notables novedades

Junto a todo ello, se presentaron herramientas que utilizará el CCN, como **ELSA** (Exposición Local y Superficie de Ataque), en una ponencia de **Carlos Abad** y **Jaime Sánchez**, de **Delta 90**, así como nuevas compañías como **Tamiza**, de origen malagueño y centrada en protección DNS.

En el acto de clausura, **Luis Jiménez**, subdirector del CCN, y **Javier Candau**, entregaron los premios a los ganadores de la competición **Atenea Jornadas**: **Gonzalo Jiménez**, **Román Medina** y **Jorge Belmonte**. Finalizaron las jornadas con la intervención del secretario General de Administración Digital, **Juan Jesús Torres** quien recordó que “la transformación digital no puede ser entendida sin ciberseguridad”. Asimismo, se dio a conocer que, como novedad, en la edición de 2024 se dedicará un nuevo módulo a identidad y biometría, emplazando a los asistentes a las que organizará el CCN en Panamá, con **RootedCON**, en abril.

INCIBE reconoce con un premio a su ‘destacada trayectoria profesional’ a uno de los especialistas españoles de referencia: Carlos Manuel Fernández

En el contexto de las Jornadas STIC, el **Instituto Nacional de Ciberseguridad (Incibe)**, que coordinó las ponencias dedicadas a emprendimiento e innovación en ciberseguridad, también quiso

entregar un premio a su ‘destacada trayectoria profesional’ a **Carlos Manuel Fernández**, asesor estratégico de TI de **Aenor**. Un galardón que recogió de manos del director general del organismo, **Félix Barrio**, poniendo en valor sus 40 años de trayectoria en este ámbito, además de su contribución como docente de las TIC (ciberseguridad, control interno y auditoría informática) y su sobresaliente contribución a la



El premiado posa en compañía del director general de INCIBE, Félix Barrio, y algunos integrantes del FNC

sociedad española en este ámbito.

Durante el módulo se repasaron diferentes iniciativas acometidas por el Incibe, como el Proyecto **Re-tech**, las cátedras de ciberseguridad, así

como diferentes actuaciones para mejorar la colaboración público privada, como la **Iniciativa Estratégica de Compra Pública Innovadora (IECPI)**, puesta en marcha en 2021. Además, se aprovechó para presentar los resultados –distintas piezas informativas con foco expreso en cinco dimensiones de la ciberprotección– de varios grupos de trabajo del **Foro Nacional de Ciberseguridad**.

La JUNTA DE ANDALUCÍA opta por FUJITSU para hacking ético en dispositivos, en entornos IoMT

La Junta de Andalucía ha firmado un Protocolo General de Actuación con la filial española de Fujitsu para reforzar la ciberseguridad en Internet Of Medical Things (IoMT).

En concreto, este paso permitirá poner en marcha diferentes actuaciones en el ámbito de ciberseguridad ofensiva y del hacking ético en dispositivos usados en centros sanitarios. "Se trata de establecer un equipo específico para testeo de la ciberseguridad de dispositivos médicos, contribuyendo de esta forma a conseguir unos servicios socio-sanitarios más seguros para los pacientes y profesionales del sector sanitario", explica el responsable de Ciberseguridad de Fujitsu en España, **Javier Pérez**.



El consejero, Antonio Sanz, en la firma del protocolo junto a la presidenta de Fujitsu España, Ángeles Delgado

El acuerdo también contempla establecer una colaboración y cooperación institucional que contribuya a que Málaga se convierta

en el polo de conocimiento sobre ciberseguridad en el ámbito socio-sanitario y, en especial, del IoMT, tanto aquí como fuera de nuestras fronteras.

En el último año, el área de ciberseguridad de la compañía en España ha experimentado un fuerte crecimiento, con una facturación que ya ronda los 20 millones, y una presencia notable tanto en compañías del Ibex, como en organismos y, también, en el sector sanitario. De hecho, la empresa cuenta con un Centro de Excelencia de Ciberseguridad Sociosanitaria.

V-VALLEY incrementa su oferta en protección de las comunicaciones, a través de MITEL, y de virtualización del puesto de trabajo con VIRTUAL CABLE

V-Valley distribuirá soluciones UCC tras firmar una alianza con Mitel Iberia y soluciones de virtualización del puesto de trabajo tras una alianza con Virtual Cable. Así, en el primer caso, el mayorista aportará a Mitel su estructura y orientación para proporcionar

soluciones de valor, incrementando sus oportunidades de negocio a empresas que están en el sector de las comunicaciones unificadas, que podrán disponer a partir de ahora de su gama de soluciones de Plataforma de Comunicaciones Unificadas, incluyendo servidores de comunicación, aplicaciones de colaboración,



soluciones de Contact Center, teléfonos empresariales y soluciones de movilidad. Como se sabe, Mitel es un referente en dicho mercado, reforzando su posición con la compra reciente de Unify.

Propuesta personalizada

Por otro, lado el mayorista también ha firmado con acuerdo estratégico con **Virtual Cable** para distribuir en Iberia e Italia su portafolio de virtualización del puesto de trabajo, compuesto por Uds Enterprise, la solución segura de virtualización de escritorios, aplicaciones virtuales y acceso remoto a equipos.

NOMBRAMIENTOS



● **Iberdrola** ha apostado por **Rafael Ceres** promocionándole a CISO Global del Grupo, y fichado a **Ana de la Higuera López-Frías** para su área de Ciberseguridad Global Protección de Datos. En la multinacional desde 2001, donde comenzó como analista, Ceres también ha trabajado en Indra y Grupo Arion. Es ingeniero en Informática por la Universidad de Sevilla. De la Higuera ha trabajado para la International Association of Privacy Professionals y KPMG España, donde estuvo casi una década. Es vocal de la junta directiva de la Asociación Profesional Española de Privacidad.



● **Unicaja** ha ascendido a **Manuel Portolés** a Director de Gobierno y Estrategia de Ciberseguridad y Control de Terceros. Con una destacada trayectoria, ha contribuido con su trabajo en empresas como Ingenia, Deloitte España y Finamatrix. Es graduado en Ingeniería Informática por la Politécnica de Valencia.



● **Eduardo Cunha** ha sido fichado por **Consentino Group** en calidad de Global CISO. Con amplia trayectoria en el sector, ha ocupado puestos de responsabilidad previos en Deloitte, Andbank, Morabanc y Reale seguros, entre otras. Es ingeniero de Telecomunicaciones por la Universidad de Vigo.



● **CaixaBank** ha contratado a **Jordi Recio** como Cyber Security Risks Manager. Hasta ahora en Fujitsu, donde fue eCISO para el sector financiero, ha desarrollado su trayectoria en EY, S21sec e Internet Security Auditors.



● **Washington Gómez** se ha sumado a **Grupo Global Exchange** como CISO, cargo que ha ocupado hasta ahora en Bit2Me. Ha trabajado para Deloitte, dLocal e ISA, entre otras. Es graduado en Informática por la Universidad de la Empresa (UDE), además de contar con un máster en ciberseguridad por la UCLM.



● **Plenitude España** contará con **Jesús R. Abascal** como CISO. Además, de ser profesor en este ámbito en la Universidad de Cantabria, es CEO y Fundador de Next Security y ha trabajado para ClarkeModet, Inlog Consultoría y Prodware, entre otras.



● **W2M World2meet** ha contratado como CISO a **Jorge Félix Iglesias**, rol que desempeñó hasta el año pasado en FacePhi Biometría. Con anterioridad trabajó para TICs&Fi, Miniland New Concepts y Phillips. Es licenciado en Telecomunicaciones por la Politécnica de Valencia.



● **Ignacio Ortiz** ha sido fichado por **Ufinet** como CISO. Con más de 15 años de experiencia, ha trabajado en roles de responsabilidad en Vodafone, Deloitte y Accenture, entre otras. Es ingeniero de Telecomunicaciones por la Universidad Europea.



FACTUM

Cybersecurity Services

Tu tranquilidad,
nuestra razón de ser.



cyberex_
Cyber Security Exercises

hackrøcks | FACTUM
1º RANKING ESPAÑA

+200 clientes en el mundo +120 especialistas +15 años de experiencia

No te pierdas nada
Síguenos en LinkedIn



SOPHOS y VEEAM suman fuerzas para mejorar la protección de las copias de seguridad críticas

Sophos y Veeam Software han firmado un acuerdo a través del que Veeam Data Platform se integrará con Sophos Managed Detection and Response (MDR), agregando una capa crítica de detección y respuesta liderada por personas para avanzar en la protección de las copias de seguridad críticas para el negocio.



Para ello, Veeam Data Platform supervisa el entorno de una organización para detectar posibles amenazas contra las cargas de trabajo de producción de los clientes y su entorno de copia de seguridad.

Si se identifica una amenaza,

como un atacante que intenta manipular las copias de seguridad, Veeam envía una alerta a Sophos MDR, un servicio gestionado de caza, detección y respuesta ante amenazas que proporciona un equipo de seguridad dedicado 24x7, que identifica y neutraliza rápidamente ataques complejos, como *ransomware*, brechas en la red, etc. El equipo de operaciones de seguridad de Sophos MDR puede determinar si se está produciendo un ataque y tomar medidas para interrumpirlo y neutralizarlo.

“La necesidad de copias de seguridad seguras es primordial, y las operaciones de protección siempre activas son imprescindibles para fortificar estos datos críticos para el negocio”, ha explicado el vicepresidente de Operaciones Tecnológicas de Sophos, **Marty Ward**.

ELECNOR se blinda con la última tecnología EDR y Zero Trust de CROWDSTRIKE y NETSKOPE

El proveedor de servicios de tecnología e ingeniería, **Ayesa**, ha construido una nueva capa de ciberseguridad en **Elecnor** para mantener su actividad a salvo de las últimas amenazas avanzadas. Para ello, ha utilizado las soluciones EDR (Endpoint Detection and Response) de **CrowdStrike** y la tecnología



ZTNA (Zero Trust Network Access) de **Netskope**.

Con ello, la compañía busca disponer de una “mayor anticipación a los ataques dirigidos, menor tiempo de exposición a incidentes y visibilidad completa de las amenazas. Y es que, las técnicas empleadas por los cibercriminales son cada vez más

dirigidas y sofisticadas y ya no es suficiente con proteger los dispositivos conectados y el perímetro de la red”. Así con esta solución EDR “nos podemos enfocar en amenazas avanzadas, las diseñadas para evadir la primera capa de defensa que logran penetrar en la red. Detectamos esa actividad y contenemos a los atacantes antes de que puedan moverse lateralmente. Con ello hacemos que la empresa esté protegida frente a cualquier posible incidente de seguridad, tanto si es una amenaza tradicional, desconocida o una aplicación vulnerable”, ha explicado el director de Ciberseguridad, **Álvaro Fraile**, destacando también, el enfoque de Confianza Cero, con la solución Zero Trust Network Access, que permite “medir la fortaleza del acceso a la red, verificando quién, qué, cuándo, dónde, por qué y cómo se conectan a los recursos empresariales”.

NOMBRAMIENTOS



Nebrija.

● **SegurCaixa Adeslas** ha apostado por **Miguel Huertas** como Coordinador de Seguridad Digital y Continuidad. Ha desempeñado roles de responsabilidad en S2 Grupo, S21sec, Técnicas Reunidas y Meta4, entre otras. Es ingeniero técnico en Informática por la Universidad de



i2CAT Foundation, entre otras.

● **Xavier Galcerán** se ha incorporado a **Barcelona Activa** como Responsable de Ciberseguridad, donde ya fue DevOps Project Manager Technical. Ingeniero en Telecomunicaciones por la Universidad Pompey Fabra, ha trabajado para Digital Catalonia Alliance (DCA), Giesecke+Devrient e



la Oberta de Catalunya.

● **NH Hotel Group** ha promocionado a **Nuria Lago**, por su buena labor en este ámbito, a Vicepresidenta de Seguridad de la Información. Con más de 15 años de trayectoria, ha desarrollado su labor en PwC, Tissat y itSMF España, entre otras. Es graduada en ingeniería informática por la



la Universidad de Chile.

● **Active Business & Technology** ha apostado por **Edgar Carrillo** como CISO. Con una amplia trayectoria, ha trabajado para la Agència de Ciberseguretat de Catalunya, Plexus Tech y Untronics, entre otras. Es diplomado en Gobernanza, Gestión y Auditoría a la Ciberseguridad por



con una amplia trayectoria como CISO, ha trabajado para Ibermática, Jazztel y Avaya España, entre otras. Solanas ha estado, entre otras, en Valorista, Global Technology4E, Bitdefender, GE Capital y Asseco Spain.

● **Integración Tecnológica Empresarial (ITE)** ha contratado a **Juan Carlos Chamizo** como Director de la Unidad de Ciberseguridad y a **Carlos Solanas** como Gerente de Desarrollo de Negocio. Chamizo,



Forensic & Incident Response. Con una amplia trayectoria, Núñez-Vilabeiran ha trabajado en puestos de responsabilidad en EY, Everis, SIA y Ecija, entre otras. Es abogada por la Complutense de Madrid. Hernández, tiene una dilatada trayectoria en Entelgy Innotec Security, Cipher e Indra.

● **Mapfre** ha reconocido la buena labor de **María Luisa Núñez-Vilabeiran** ascendéndola a Vicedirectora en Privacidad y Protección de Datos, además de incorporar a **José Manuel Hernández** para su área de Digital



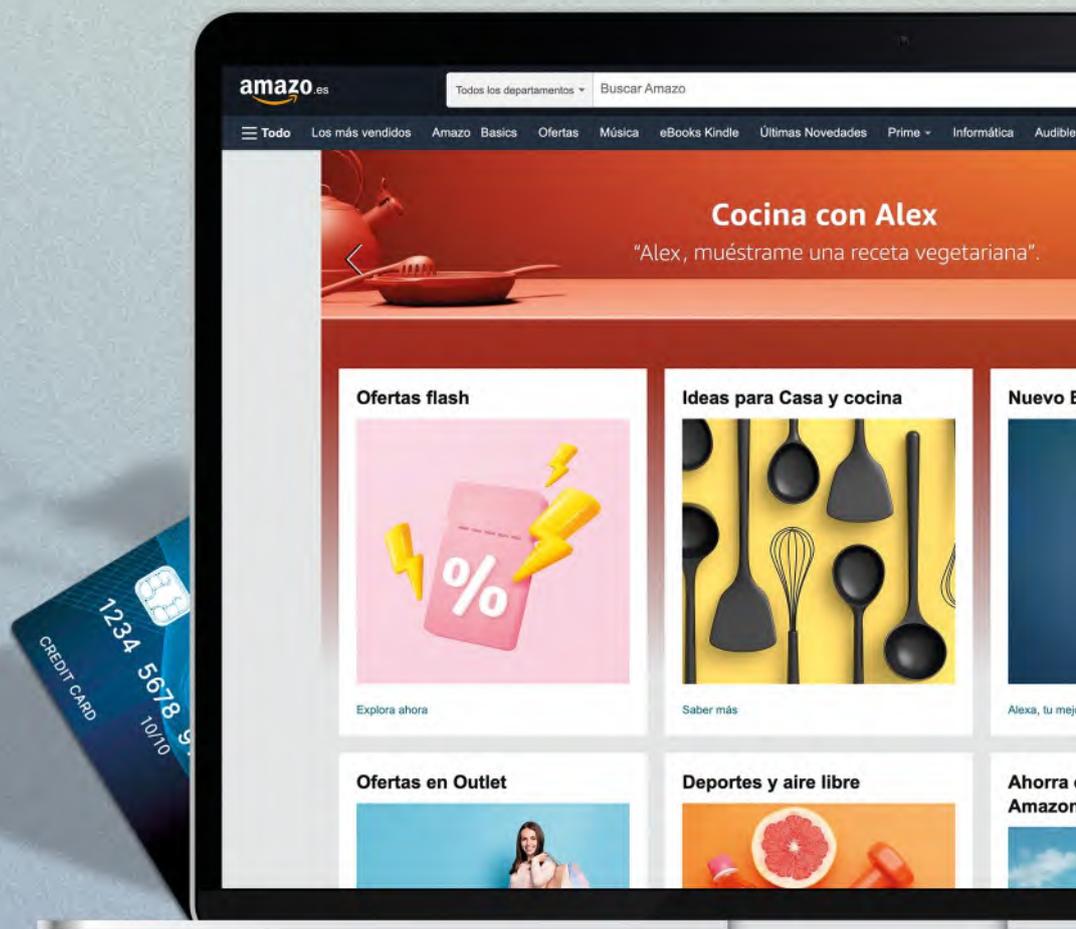
como DLTCode.

● **LaLiga** se ha reforzado con la incorporación de **Alex Barreiros** como Senior CyberSecurity Engineer. Ha trabajado para la Agència de Ciberseguretat de Catalunya, la Guardia Civil, así como



cia de Salamanca.

● **Mastercard** ha designado a **Juan Rodríguez** como Regional Director, Spain & Portugal. Con una amplia trayectoria profesional, ha ocupado roles de responsabilidad en F5, Citrix y Elium Advanced Technology Education, entre otras. Es graduado en ciencias por la Universidad Pontificia de Salamanca.



¿Crees que puedes reconocer un sitio web falso?

Antes de proporcionar tus datos sensibles, verifica siempre la confiabilidad del sitio. Es mejor dedicar unos minutos más, que arriesgarse a perderlo todo. Transformar los comportamientos digitales de tus empleados es fundamental, pero para hacerlo necesitas una plataforma de capacitación completa, diseñada para maximizar la efectividad de los procesos de aprendizaje. Tres rutas de formación para desarrollar las tres principales características defensivas de cada individuo: el conocimiento, la percepción del peligro y la prontitud.



SECURITY AWARENESS TRAINING THAT WORKS!

www.cyberguru.io



ESTE ES UN QR CODE SEGURO

HORNETSECURITY publica 'Microsoft 365: Guía Esencial', un recurso de referencia para las empresas que utilizan M365

Hornetsecurity ha dado a conocer su 'Microsoft 365: Guía Esencial', creada para administradores de



IT que gestionan un entorno de Microsoft 365, así como para tomadores de decisiones que buscan obtener una descripción general de qué esperar al migrar a la nube y las formas en que pueden adoptar los servicios en Microsoft 365.

Escrita por el respetado autor de tecnología y Certified Trainer de Microsoft, **Paul Schnackenburg**, "es un recurso integral que proporciona un análisis en profundidad de Microsoft 365 para ayudar a los usuarios a maximizar sus esfuerzos al usar esta plataforma. Esta guía también

proporciona enlaces a recursos adicionales para profundizar en las aplicaciones más relevantes para las necesidades específicas de cada empresa", destacan desde la empresa, poniendo en valor la información que ofrecen sus tres apartados principales dedicados desde a conceptos básicos de Office y Microsoft 365, hasta a su gestión, mantenimiento y asistencia técnica y, por supuesto, a la ciberseguridad, copia de protección y cumplimiento. Con ella, la empresa quiere complementar su propuesta a través de su recientemente publicado 'Plan 4 Compliance & Awareness', de su solución insignia, 365 Total Protection.

ACRONIS ayuda a crecer a los proveedores de servicios gestionados con su plataforma de aprendizaje 'MSP Academy'

Acronis ha puesto en marcha, en todo el mundo, su 'MSP Academy', una iniciativa educativa destinada a proporcionar a los proveedores de servicios gestionados (MSP) el conocimiento empresarial y tecnológico, las habilidades y las herramientas necesarias para destacar y crecer. MSP Academy es una plataforma de aprendizaje creada para abordar los desafíos clave a los que se enfrentan los proveedores de servicios gestionados (MSP).



En la plataforma se cubren varios temas, desde cómo empezar a ser un MSP, cómo dirigir una empresa de MSP exitosa y cómo llevar a cabo el marketing de la misma, hasta cómo optimi-

zar la eficiencia y productividad de los técnicos de MSP. Por ello, "representa una expansión significativa de la oferta educativa de Acronis, y le permite también cumplir con su compromiso de brindar apoyo al desarrollo del mercado global de proveedores de servicios gestionados", resaltan desde la empresa.

Entre las próximas iniciativas de Acronis figura el desarrollo de talleres intensivos híbridos en colaboración con distribuidores de la nube, así como el lanzamiento de nuevas opciones de formación multilingüe *online*, híbridas u *offline*, lo que garantizará que los MSP de todo el mundo puedan beneficiarse del programa.

NOMBRAMIENTOS



● **Mayte Ledo Turiel** ha sido nombrada Secretaria de Estado de **Digitalización e Inteligencia Artificial** dependiente del ministro para la Transformación Digital y de la Función Pública, José Luis Escrivá, tras haber sido, hasta ahora, su Directora de Gabinete. Licenciada en Económicas por la Universidad de Valladolid, fue nombrada Economista Jefe de escenarios económicos y financieros en el BBVA en 1999, entidad en la que ha ejercido notables roles de responsabilidad. En 2021 pasó a formar parte del actual gobierno, donde comenzó como Jefa de Gabinete del Ministerio de Inclusión, Seguridad Social y Migraciones para, el año pasado, pasar al actual Ministerio del que es Secretaria de Estado.



● La general del Ejército del Aire **Loreto Gutiérrez Hurtado** ha sido designada directora del **Departamento de Seguridad Nacional**, sucediendo al general Miguel Ángel Ballesteros, en el cargo desde 2018. Nacida en Madrid en 1970 e ingeniera Aeronáutica por la Politécnica de Madrid, ingresó en la Academia General en 1996 habiendo sido, entre otros destinos, directora técnica de los programas A400M y MRTT en la Dirección de Armamento y Material. Hasta su nombramiento como general, en agosto, ejercía la jefatura de la sección de aviones de transporte y patrulla marítima del Mando de Apoyo Logístico.



● **José Miguel Corvinos Lafuente** fue designado, a finales de año, **Embajador en Misión Especial para la Transformación Digital y Amenazas Híbridas** -incluyendo ciberseguridad-. Sucede así a Nicolás Pascual de la Parte, que sí incluía en su denominación formalmente apartado de ciberprotección. Licenciado en Derecho y diplomático desde 1993, ha sido embajador en Cabo Verde y Malasia, además de Cónsul General Adjunto en Moscú y Consejero en la Embajada de España en Francia. En **Asuntos Exteriores**, ha ejercido de Director Adjunto del Gabinete del ministro, además de haber sido Director General de Recursos Pesqueros y Acuicultura en el de Agricultura, Alimentación y Medio Ambiente.



● **Hans de Vries**, anterior Director del Centro Nacional de Ciberseguridad de los Países Bajos, se incorporará en abril a la **Agencia de la Unión Europea (Enisa)** como Director de Ciberseguridad, apoyando al organismo en la coordinación de asuntos estratégicos y operativos clave. Licenciado en Derecho por la Universidad de Leiden, ha ocupado cargos de responsabilidad en el Ministerio de Interior de Países Bajos.



● **Juan Ramón Aramendía** ha sido designado Coordinador del **Navarra Cybersecurity Center**. Ingeniero de Telecomunicaciones por la Universidad de Navarra, cuenta con más de 15 años de experiencia forjada en empresas como Lookwise, S21sec y Auriga, entre otras.



● La **Agència de Ciberseguretat de Catalunya** ha promocionado a **Helena Rodríguez Pérez** a Directora de Certificaciones, habiendo sido hasta ahora Responsable de Seguridad de la Información. Ha desarrollado su carrera profesional en PwC y Mutua Terrassa, entre otras. Es graduada en ingeniería de Sistemas Audiovisuales y Telecomunicaciones por la UPC.



● **Red.es** ha nombrado a **Jesús Herrero** Director General. Es licenciado en Ciencias Políticas por la Carlos III y ha sido asesor en Hacienda, en la Dirección General de Asuntos Públicos de Presidencia del Gobierno, y Director de Gabinete de la Secretaría de Estado de Digitalización. Además, ha participado en los grupos de trabajo que han diseñado y lanzado los principales programas de la entidad, entre ellos Kit Digital.

a3Sec

<SHIELDING DIGITAL ASSETS GLOBALLY>

¿Por qué adaptarte a servicios de ciberseguridad estandarizados?

En A3Sec te ofrecemos la flexibilidad y personalización que estás buscando.

www.a3sec.com

> /
Prevención
Detección
Respuesta

MAPFRE y CYBERWRITE suman fuerzas para impulsar la ciberprotección para pymes con Inteligencia Artificial

Mapfre ha sumado fuerzas con Cyberwrite, centrado en tecnología para el ámbito de los ciberseguros, con Inteligencia Artificial (IA).

Cyberwrite proporcionará a la compañía española una plataforma de análisis del ciberriesgo en pymes, con el objeto de disponer de un conocimiento más preciso del riesgo en el momento de suscripción y renovación del ciberseguro.

En concreto, su propuesta emplea la IA para ofrecer análisis de ciberriesgos a la carta y en tiempo real a través de su algoritmo 4SEEN. Ello le permite generar, casi en tiempo real, informes multilingües con datos contextuales, comparando empresas de

todo el mundo con sus homólogos del sector y proporcionando análisis de deficiencias en el marco normativo y cuantificación financiera de las potenciales pérdidas.

A través de ellos, Mapfre puede conocer el nivel de riesgo de cada pyme y ayudarla a tomar medidas para remediar sus vulnerabilidades o ajustar las condiciones del ciberseguro para conseguir la mejor protección posible, ya que, entre otros factores, su tecnología permite analizar puertos abiertos, tecnologías o versiones de software obsoletas con debilidades conocidas, malas prácticas en cifrado y certificados, etc.

Además, la solución facilita la asociación de estos riesgos a las coberturas más típicas como fraude y robo financiero, ciberextorsión, pérdida de datos, violación de la privacidad, interrupción de operaciones, respuesta ante incidentes, defensa jurídica o responsabilidad civil.



LYNX lleva a cabo con éxito una nueva ronda de financiación, por 17 millones de euros, sumándose a su junta Leo Casusol, de FORGEPOINT

Lynx ha llevado a cabo una ronda de

financiación de 17 millones de euros liderada por Forgepoint Capital, con la participación de Banco Santander, accionista de Lynx. Ello también supondrá que el director general de Forgepoint, Leo Casusol (en la imagen), se unirá a la junta directiva de la compañía, además nombrar director ejecutivo a Dan Dica.

Creada hace 20 años por Carlos Santa Cruz, un científico informático y experto en IA que ahora es director de tecnología, Lynx aplica IA avanzada y aprendizaje automático para prevenir el fraude digital



y combatir el lavado de dinero.



Leo Casusol

En la actualidad, Lynx ayuda a instituciones financieras de referencia en Europa, el Reino Unido, EE.UU. e Iberoamérica, incluido Cielo, el mayor operador de tarjetas de crédito y débito de Brasil.

La compañía ofrece prevención de fraude para tarjetas, banca digital, comercio electrónico, telefonía, sucursales y cajeros automáticos. En 2022, Forgepoint Capital y Banco Santander anunciaron una alianza estratégica para impulsar la inversión y la innovación en ciberseguridad a nivel mundial y esta es su primera inversión conjunta.

NOMBRAMIENTOS



● **Incode Technologies** ha incorporado a **Raúl Tapias** como Director Regional. Ha trabajado para ThreatMark, FacePhi Biometría y Ecertic Digital Solutions. Es graduado en ADE por la Carlos III de Madrid.



● **Lynx** ha nombrado como Director Ejecutivo a **Dan Dica**, quien aprovechará su amplia experiencia en el crecimiento de empresas de software para ayudar a la empresa a escalar. Con una destacada trayectoria, ha ocupado cargos de responsabilidad en compañías como Agnostic Intelligence, OneSpan, Vasco Data Security y WhiteStone, entre otras.

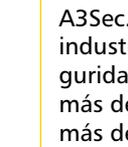


● **Ricardo Escriba** ha sido ascendido por **Comforte AG** a Senior Vice President para Reino Unido, Irlanda e Iberia. Ha trabajado para el Colegio de Abogados de Valencia, One Trust y Crayon, entre otras.

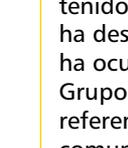


● **BeDisruptive** prosigue su intenso refuerzo de plantilla con la incorporación de **Nacho García Egea** como Global CISO, **David Marco** como Global Industrial Cybersecurity Director, a **Alexandre Gaspar** como Security Business Executive, a **Susana Sánchez** como Global Industrial Cybersecurity Head y ha promocionado a **Iván Portillo** a CTI Leader.

García tiene más de 20 años de experiencia, con roles de responsabilidad en EY, Orange, Hewlett Packard Enterprise España, PwC, Innotec o Entelgy, además de haber sido hasta ahora Director de Operaciones y CTO en A3Sec. Marco ha sido responsable de ciberseguridad industrial en Técnicas Reunidas y Gerente de Ciberseguridad Industrial en Entelgy Innotec Security, además de haber trabajado para Accenture. Gaspar, con más de 25 años en el sector, también como CISO, ha tenido roles de responsabilidad en Telefónica, donde ha desempeñado gran parte de su trabajo. Sánchez ha ocupado roles de responsabilidad en Accenture, Grupo CMC y Sampol. Portillo, es uno de los grandes referentes en Inteligencia, siendo cofundador de la comunidad Ginseg y del congreso IntelCON, muy activo en la docencia en universidades, además de haber trabajado para EY casi una década en este ámbito.



● **Cyberbit** ha apostado por **Francesco Mancini** como Regional Director, Italia y Sureste de Europa. Hasta ahora Country Manager de Skybox Security para Iberia e Italia, ha ocupado roles de responsabilidad en Symantec, CyberArk y Fortinet.



● **Kyndryl** ha incorporado a **Aitor Herrero** como Consultor de Ciberseguridad. Grado en criminalidad por la Universidad de Alicante, con anterioridad ha trabajado en test de intrusión durante toda su trayectoria profesional en Inetum, Viewnext y TryHackMe, entre otras.





HORNETSECURITY

**PROTECCIÓN
TODO EN UNO
PARA MICROSOFT 365**

SEGURIDAD EMAIL

BACKUP Y RECUPERACIÓN

CUMPLIMIENTO Y GESTIÓN DE PERMISOS

CONCIENCIACIÓN EN SEGURIDAD

VALIDACIÓN DE DESTINATARIOS IA

PRUEBA AHORA

www.hornetsecurity.com



GOOGLE CLOUD y el CCN firman un convenio en seguridad en la nube

Google Cloud y el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI)



han firmado un convenio de colaboración para fortalecer la cooperación en seguridad en la nube en áreas como el cumplimiento regulatorio, innovación e Inteligencia Artificial. El acuerdo busca crear un nuevo marco de colaboración para el desarrollo de iniciativas conjuntas tales como talleres técnicos, intercambio de información sobre ciberamenazas, así como colaboración para eventos y campañas conjuntas para promover la capacitación y conocimiento en seguridad *cloud* por parte de las organizaciones españolas.

Además, gracias a él, Google Cloud también apoyará al CCN en la definición de la evolución y el

cumplimiento del ENS (Esquema Nacional de Seguridad) y otras acreditaciones requeridas, y contribuirá a la Red Nacional de SOC.

Esta iniciativa se lleva a cabo tras la inclusión de la solución de cifrado y soberanía del dato de Google Cloud, de gestión externa de claves de cifrado (External Key Manager en su denominación en inglés) en el catálogo de productos y servicios del CCN, anunciado a principios de este año. EKM es la primera solución que permite la gestión de claves de cifrado tanto del lado del cliente como de terceros, que ha sido acreditada por el CCN. Google Cloud está trabajando para incluir otros productos de seguridad en el catálogo en los próximos meses.

GMV inaugura una réplica de la sala de operaciones de Galileo, el GPS europeo, para entrenarse en situaciones críticas

GMV ha inaugurado, en su sede central de NTN en Madrid, una réplica de la sala de operaciones del programa Galileo, el sistema de navegación por satélite de la Unión Europea, en cuyo desarrollo tiene un papel relevante.

La nueva sala permitirá simular todas las operaciones de los satélites en un entorno equivalente al de los centros de control del sis-

tema, permitiendo así mantener y desplegar versiones operacionales del segmento terreno, desarrollar servicios y probar nuevas tecnologías que mejoren los servicios existentes, incrementar la robustez del sistema, mejorar la seguridad

de la red y la gestión de las claves, así como reducir los costes de mantenimiento del sistema. GMV es el contratista principal del segmento terreno de control de Galileo, tanto para la primera como para la segunda generación, como resultado de los contratos que la ESA la otorgó en 2018 y 2023, respectivamente.

La nueva sala se usará tanto para el segmento terreno de control de la primera generación de Galileo (G1G), como para la evolución del mismo actualmente en desarrollo para la validación en órbita (IOV) de estos satélites de segunda generación (G2G) siendo también un componente crítico de la ciberseguridad.

Además, la compañía también ha destacado su apuesta pionera, en el sector espacial, por el SAFE Agile, una nueva forma de trabajar en este sector que mejora la productividad y la calidad.



tema, permitiendo así mantener y desplegar versiones operacionales del segmento terreno, desarrollar servicios y probar nuevas tecnologías que mejoren los servicios existentes, incrementar la robustez del sistema, mejorar la seguridad

NOMBRAMIENTOS



● **Raquel Hernández González** ha sido fichada por Microsoft como Directora de Soluciones de Seguridad para España. Durante los últimos dos años, fue Directora General de la región Iberia de Zscaler, además de haber ocupado puestos de responsabilidad en el mercado nacional como internacional, en organizaciones como Hewlett-Packard, Gartner o Repsol. Es ingeniera Industrial por la Universidad de Las Palmas de Gran Canaria.



● **Marta Olbes** ha entrado a formar parte de Cyber Guardian como Responsable de Producto. Física por la Complutense de Madrid, ha desempeñado cargos de responsabilidad en Panda Security, Canon, Santander y Factum, entre otras.



● **Almudena Justo** se ha incorporado a Fujitsu España para dirigir el Centro Internacional de Cuántica que la compañía acaba de inaugurar en nuestro país, apoyado por la Xunta de Galicia y el Centro de Supercomputación de Galicia. Es ingeniera Química y cuenta, entre otros títulos, con un Máster en Energía y Sostenibilidad y otro en Ingeniería Ambiental y Bioprocesos. Por su conocimiento tecnológico, de negocio y su amplia experiencia en financiación pública a la I+D+i, ha sido experta externa de la Comisión Europea y el Instituto Europeo de Innovación y Tecnología.



● **Sothis** ha contratado a **Pedro García Villacañas** como ICS/OT Cybersecurity Consultant y a **Mario Trigueros** como SOC Manager. García ha trabajado para Sabada Security, Kaspersky, Pragsis Technologies y McAfee, entre otras. Trigueros, con más de 15 años de trayectoria, ha estado en Nunsys, Agedos Business Datacenter, Inforges y una década en KPMG.



● **Zerolynx** contará con **Eduardo Martínez Mendizábal** como Director of Business Development para Soluciones de Ciberseguridad y con **Héctor Sainz** como Technical Lead. Martínez, con más de 30 años en experiencia, ha dirigido equipos de negocio, marketing y ventas en entidades como Telefónica, Indra Minsait/SIA y Siemens, donde ha ocupado posiciones de Vicepresidente y de Head of Business Development en diferentes países. Sainz, ingeniero en Informática por la Pontificia de Salamanca, ha trabajado para Nec, EY, Inetum y The Bridge.



● **Fastly** ha fichado a **Kip Compton** como Chief Product Officer (CPO), reportando al CEO de la compañía Todd Nightingale. Aporta más de 25 años de experiencia impulsando la innovación en *cloud*, vídeo, Internet de las Cosas (IoT) y redes, habiendo ocupado, entre otros puestos de responsabilidad, la vicepresidencia de Estrategia de Cisco.



● **ControlPlane** ha fichado como Principal Cloud Native Security Consultant a **Miguel Ángel Hernández Ruiz**. Ingeniero en Tecnología de la Información por la Universidad de Murcia ha trabajado para Sopra Steria, IBM y Kevin.



● **Víctor Arroyo** se ha incorporado a **Cefiros** como socio y Director del Área Técnica. Cuenta con más de 20 años de experiencia y ha trabajado para Bexiqo, Atrys Health, Vivo diagnóstico y Pallex Medical, entre otras. Ha recibido numerosos reconocimientos como el 'Premio Incibe' y el 'Premio Feindef'.

Predecir lo que importa

La Alianza Líder que garantiza
la **gestión de vulnerabilidades**
y **compliance técnico**



www.mdtel.es
marketing@mdtel.es

BT y NETSKOPE firman un acuerdo para ofrecer servicios gestionados seguros para la empresa híbrida actual

BT y **Netskope** han sumado fuerzas para llevar las capacidades de Security Service Edge (SSE) de Netskope a los clientes globales de la compañía de telecomunicaciones. Esta asociación se produce tras una serie de implementaciones



de grandes clientes en las que las dos empresas ya han colaborado para satisfacer con éxito las necesidades de seguridad y acceso de las grandes organizaciones.

El acuerdo aprovechará las capacidades de Netskope en SSE y la presencia de la nube privada de seguridad global NewEdge, junto con la huella global de BT y las relaciones

sólidas y establecidas con algunas de las organizaciones más grandes del mundo. BT procura servicios gestionados de telecomunicaciones, seguridad, redes

e infraestructuras de TI a clientes de 180 países. Netskope Intelligent SSE proporciona visibilidad granular y protección de datos y amenazas en tiempo real para servicios en la nube, sitios web y aplicaciones privadas a las que se accede desde cualquier lugar y dispositivo.

Netskope Intelligent SSE, además, ya se integra con muchos de los proveedores estratégicos y socios de integración tecnológica de BT, incluidos **Microsoft, AWS y CrowdStrike.**

CLAROTY y ROCKWELL AUTOMATION amplían su oferta e incluyen la solución de seguridad OT xDome basada en SaaS

Claroty ha ampliado de sus capacidades con **Rockwell Automation** con la incorporación de la plataforma de ciberprotección industrial Claroty xDome -impulsada por SaaS-, a la cartera de servicios globales de la segunda, cuyos clientes también



podrán acceder a sus capacidades de seguridad OT basadas en la nube. En concreto, Claroty xDome buscará ofrecer una cobertura de seguridad completa, interoperabilidad integrada y profundas alianzas tecnológicas bidireccionales. La ampliación de la asociación pone de relieve la postura pionera de Rockwell

en seguridad OT al ofrecer una solución alojada en la nube a sus clientes.

Así, con la incorporación de xDome, la cartera global de

Rockwell Automation ahora cuenta con el conjunto completo de ofertas de ciberseguridad industrial de Claroty, junto con la Detección Continua de Amenazas (CTD) y el Acceso Remoto Seguro (SRA). Juntas, estas soluciones ofrecen controles específicos que identifican, protegen, supervisan y optimizan todos los activos, sistemas y procesos OT, IoT y BMS en entornos industriales.

NOMBRAMIENTOS



● **aDvens** ha incorporado a **Antonio Martínez** como Regional Sales Director, quien venía siendo Vicepresidente de Ventas en Kroll para todo el territorio de Iberia, como responsable del desarrollo de negocio de la división de ciberseguridad. Previamente, trabajó en Telefónica y Banco Santander. Es doble graduado en Ciencias Empresariales y Relaciones Laborales por la Universidad de Zaragoza.



● **Jordi Lorenzo** ha sido contratado por **Ackcent Cybersecurity** como Chief Product Officer. Con más de 20 años de experiencia, este ingeniero técnico en Informática de Sistemas por la Universidad de Giroña y Máster en Redes y Telecomunicaciones por la Ramon LLull, ha trabajado para Telefónica, Orange, Ricoch y Evolutio.



● **Tokio Marine HCC** ha contratado a **César Andrés Vásquez** como Senior Cyber Underwriter para Iberia e Italia. Estuvo más de un lustro en Zurich, además de haber trabajado para Novaecuador y Tecniseguros. Es licenciado en ADE por la Universidad San Francisco de Quito.



● **Christian Barral** se ha incorporado a **Tarlogic** como Cybersecurity Senior Consultant. Ha desempeñado diferentes roles en Azertium IT, EY y Citi, el Centro de Investigación, Transición e Innovación de Ourense.



● **Symantec** ha apostado por **Julio Valpuesta** como EMEA Security Transformation Architect. Ha desarrollado su carrera en Imgram Micro y DXC Technology, comenzando hace casi una década en la propia Symantec. Es ingeniero de Telecomunicaciones por la Universidad de Sevilla.



● **Netskope** contará con **Frantz Tourette** como Regional Marketing Manager. Graduado en Marketing y Relaciones Internacionales por la Novancia Business School de París, ha trabajado para Zscaler, Cosentino, Bull e Informática, entre otras.



● **Onum** contará con **Vicente de la Morena** y con **Fernando Lalanda** como Vicepresidentes de Ventas. De la Morena, con una notable trayectoria, ha ocupado puestos de responsabilidad siendo Country Leader en RiskRecon y Security Sales en IBM España, entre otros. Lalanda ha trabajado como CCO de Foreworth, además de ocupar cargos de responsabilidad, entre otras, en Devo, ASPgems, Genasys y Bytemobile. Es licenciado en Económicas por la Complutense.



● **Cato Networks** se ha reforzado con la incorporación de **José Muniz** como Solutions Engineer. Ha desarrollado su labor profesional en Sadinia at home, Ermetic, SentinelOne, Netskope, Palo Alto Networks y Juniper Networks.



● La asociación **@aslan** ha elegido como presidente a **Alberto Pascual**, actual Executive Director de Ingram Micro, en la que lleva más de una década. Emprendedor y fundador de varias empresas del sector TI, ha ocupado puestos de responsabilidad en ArkeNova y PGR Marketing y Tecnología, entre otras.

“El 44% de los directivos españoles no prioriza la ciberseguridad porque el lenguaje empleado en el sector es confuso”

europa **press** 30 de Mayo de 2023



¿Le parece confuso?

Si puede entender esta imagen, no tiene excusa.

Dele a la ciberseguridad la prioridad que se merece

- ✓ para su **organización**
- ✓ para gestionar los **riesgos de proveedores**

Descubra los servicios de calificación de ciberseguridad de **LEET Security**.

Las empresas con ciberseguro podrían tener más probabilidades de verse afectadas por ransomware, según BARRACUDA

El ransomware continúa siendo una amenaza crítica en el campo de batalla de las



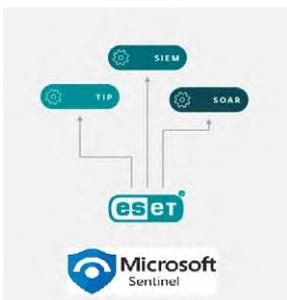
organizaciones en todo el mundo, con el 73% de las empresas afectadas con al menos un ataque exitoso de este tipo en el último año. Así se desprende del informe '2023 Ransomware Insights', de Barracuda, en el que han participado 1.350 responsables de la toma de decisiones en TI. El documento resalta que el 63% de los encuestados ha invertido en seguros de ciberseguridad para ayudarles a minimizar los costes asociados con cualquier tipo de violación de datos. "Pero podría hacerlos más propensos a ser atacados por atacantes", se afirma en el informe. Y es que, el 77% de las organizaciones con seguro cibernético se vieron afectadas por un ataque de ransomware exitoso,

en comparación con el 65% sin seguro cibernético. "Esto podría significar que es más probable que los ciberdelincuentes apunten a organizaciones con seguros, con la creencia de que las aseguradoras estarán dispuestas a cubrir el coste del rescate para acelerar la recuperación". Junto a ello, indica que casi la mitad de las organizaciones (42%) que sufrieron tres o más ataques pagaron el rescate para restaurar los datos cifrados. En comparación, solo el 31% de las que lo sufrieron una vez, lo pagaron.

Cabe destacar también, entre otros datos de interés, que el correo-e es el punto de partida más común, según el informe. Y es que, para el 69% de los encuestados, este tipo de ataques comenzaron con un correo-e malicioso.

ESET integra los datos de su threat intelligence con MICROSOFT Sentinel

Dentro de su sólida colaboración con Microsoft, Eset ha anunciado que ahora incluye la integración de seis de sus fuentes de datos de inteligencia sobre amenazas con Microsoft



Sentinel, una solución escalable y nativa de la nube que proporciona capacidades SIEM y SOAR.

En concreto, las fuentes de datos incluyen fuentes APT, fuentes de archivos maliciosos, fuentes de botnets, fuentes de dominios, fuentes de URL y fuentes de IP. "Los flujos de datos sobre amenazas que se incluyen en esta integración comprenden únicamente datos pertinentes y seleccionados que ya han sido objeto de evaluación, selección, clasificación, puntuación y procesamiento internos", explican sus responsables, "los

usuarios de Microsoft Sentinel ahora pueden beneficiarse de feeds únicos, diversos y procesables de Eset".

Además, la compañía repasó, a finales de año, a través de su director del Investigación y Concienciación de Eset España, Josep Albers, las ciberamenazas de 2023 en las que "los datos corporativos han sido el objetivo principal de los ciberdelincuentes", en ocasiones, acompañados de "solicitud de rescate" a través de grupos ciberdelincuenciales "muy activos como Lockbit". Por otro lado, la compañía entregó los galardones de la séptima edición de sus Premios Periodísticos y Divulgación en Seguridad Informática a profesionales de todos los ámbitos de la comunicación.

NOMBRAMIENTOS



● Palo Alto Networks ha apostado por Jordi Botifoll para la vicepresidencia para el Sur de EMEA y áreas emergentes, así como por Carlos Pueyo y Javier Rodríguez, como Regional Sales Manager y Cloud Security Sales Specialist para España, respectivamente. Además, ha promocionado a Roberto Ramírez a Cortex Area Sales Executive para el Sur de Europa. Botifoll, con más de 30 años de experiencia, ha ocupado puestos de responsabilidad en NetApp, Cisco, Grupo Auna e IBM. Pueyo



ha contribuido con su labor, entre otras, a Telefónica, Sirt, Fujitsu Global y Nissan Motor Ibérica. Rodríguez ha desempeñado cargos de responsabilidad en Check Point, F5, Dimension Data y Cisco Systems, entre otros. Ramírez ha trabajado para S&P Capital IQ, Eims, entre otras. Es economista por la Rey Juan Carlos.



● CrowdStrike ha reconocido la solvencia y fructíferos resultados de Joan Taulé ascendéndole a Vicepresidente de Ventas para Europa y ha contratado como Sales Engineer a Roberto Clavero. Taulé, con más de 20 años de experiencia, ha ocupado puestos de responsabilidad en Symantec, Wavilon, Veritas y CA Technologies. Clavero ha trabajado para Netskope, Symantec y Activision Blizzard King.



● Ricardo Martínez Sancho se ha sumado a Teldat como Sales Manager Cybersecurity. Con una amplia experiencia comercial de más de 20 años dedicados a la venta y explotación de productos de ciberseguridad, ha trabajado en proyectos y con clientes pertenecientes tanto al sector privado, como al público, en compañías como Entelgy Innotec Security, Grupo SIA y S2 Grupo.



● S2 Grupo ha reforzado su área de Marketing con la incorporación de María Duart en calidad de Subdirectora del área. Cuenta con una doble licenciatura en Administración de Empresas y Derecho por la Universitat de València y tiene más de 12 años de experiencia en planificación estratégica, gestión de equipos en entornos complejos, innovación y comunicación.



● Qualys contará con Enrique Serrano como Enterprise Account Executive. Con una amplia trayectoria, ha trabajado para Delinea, Palo Alto Networks, Veritas Technologies y Symantec, entre otras. Es graduado en Informática por la Universidad Nebrija.



● Outpost24 ha fichado a David García Marín como Account Executive. Fundador y Director de Sec2Crime, es colaborador de uno de los equipos técnicos de la OTAN, además de haber trabajado para Global Security Boulders, Bidaidea y Logista, entre otras.



● jtsec Beyond IT Security ha reconocido la buena labor de Antonio Checa promocionándole a Business Development Key Account Manager. Cuenta con una destacada trayectoria en Otero Group, Agencia SIDN y Stanton Fischer, entre otras. Es graduado en Psicología por la Uned y en Comunicación Audiovisual por la Universidad de Málaga.



● David Arroyo ha sido contratado por el Grupo Cybentia como Director de Desarrollo e Innovación. Cuenta con más de 40 años de experiencia en periodismo en el sector de la automoción, así como en la gestión de medios. Ha trabajado para Marca, Marca Motor, El Mundo y Nius, entre otros medios.



WISERTHANEVER

+CyberTrust +CyberSecurity

A Var Group company

wsg127.com



CEFIROS incorpora a HORIZON3 e ILLUMIO a su portafolio para remediar vulnerabilidades de forma autónoma y contar con zero trust

El mayorista **Cefiros** ha potenciado su portafolio de soluciones de ciberseguridad a través de los acuerdos de distribución recientemente firmados con **Horizon3** e **illumio**. Se trata de un paso más en su estrategia de crecimiento por cuanto, Horizon3, le permitirá reforzar su propuesta de soluciones de testeo y simulación, incluyendo ahora *pentesting* autónomo. Para ello, la empresa dispone de su plataforma NodeZero, que ayuda a las organizaciones a mejorar la productividad de SecOps y ahorrar en costes de test de intrusión y escáner de vulnerabilidades de terceros, detectando así debilidades explotables en su red y brindándole orientación detallada sobre cómo priorizarlas y solucionarlas, pudiendo verificar que sus correcciones sean efectivas. “Esto permitirá a nuestros *partners* y *MSSP* ofre-

Cefiros



HORIZON3.ai

illumio

cer todo tipo de *pentesting* internos y externos, detectar vulnerabilidades 0-Day reales o realizar auditorías de *password* en los AD”, destacan desde Cefiros, recordando que, “sin duda, será de una gran ayuda a la hora de cumplir con NIS2”.

A esta novedad se suma su alianza con **illumio**, especializada en soluciones de segmentación *zero trust*, que le permitirá ofrecer su plataforma *Zero Trust* Segmentation (ZTS), para evitar que las infecciones se propaguen a través de *endpoints*, nubes y *datacenters* visualizando continuamente cómo se comunican las cargas de trabajo y los dispositivos, creando políticas que sólo permiten la comunicación deseada y necesaria, y aislando de forma automática las infracciones restringiendo el movimiento lateral de forma proactiva.

MANPOWERGROUP obtiene, con AENOR, la certificación ENS nivel medio

ManpowerGroup España ha logrado la certificación en el Esquema Nacional de Seguridad (ENS), en categoría media, convirtiéndose así en la única empresa de gestión del talento en conseguir el grado medio hasta el momento.



Con este certificado otorgado por Aenor, ManpowerGroup España y todas sus empresas (**Manpower**, **Talent Solutions** **Right Management** y **Experis**) garantizan el cumplimiento de los requisitos de seguridad establecidos por el **Centro Criptológico Nacional (CCN-CERT)** para implementar un sistema de seguridad robusto y

eficaz que protege la información y los datos de sus clientes y empleados de forma integral.

Este sello se suma a la certificación ISO 27001, con la que también cuenta la empresa en España y sus entidades.

“Contar con estas certificaciones nos ayuda a compartir con nuestro talento y con todas las organizaciones con las que trabajamos, públicas o privadas, que nos tomamos muy en serio un aspecto clave en el mundo digital en el que vivimos, como es la ciberseguridad. También refleja la apuesta decidida de la compañía por explotar todas las ventajas de la digitalización con una gestión responsable, conscientes de que proteger nuestra información, es cuidar de equipos y clientes”, ha destacado el *country manager* de la empresa en nuestro país, **Franco Ribero**.

NOMBRAMIENTOS



● **Barracuda Networks** ha incorporado a **Patrick O'Donnell** como SVP, Worldwide MSP Sales, para acelerar las ventas del proveedor de servicios gestionados. Con una gran trayectoria internacional en compañías como IBM y GE, ha ocupado el cargo de Vicepresidente de Ventas de Norteamérica en Datto.



● **Pablo Nebreda** se ha sumado como Director de Marketing a **Factum**, que también ha sumado a **Cristina López** como Directora de Recursos Humanos, además de fichar a **Raquel de Navas** como Senior Account Manager. Nebreda, con más de 15 años de experiencia cuenta con una reciente incursión en ciberseguridad, de la mano de Alice Biometrics y ha trabajado en PayPal, Sage y UniversalPay. López tiene más de 25 años de trayectoria en compañías como Banco Santander y Prohuban, entre otras. De Navas, con más de 25 años en el sector ha desempeñado roles de responsabilidad



en Grupo Open, IT Deusto/Oesía, CGI, HR Access y Grupo IMCS, además de haber sido Business Development Manager en Grupo Davinci, Scassi y BeDisruptive



● **Leet Security** ha reforzado su plantilla con la incorporación de **María Eugenia Iglesias** y **Carlos Tello** como Directora de Grandes Cuentas, y Auditor y Responsable de Desarrollo de Producto, respectivamente. Iglesias, con formación en administración y Marketing y Publicidad, y tiene más de 20 años de experiencia en el ámbito comercial y desarrollo de negocio en TI. Tello ha alternado su labor formativa con su trabajo de Country Manager de Veeva Solution, ambas en EE.UU.



● **SailPoint** contará con **David Sánchez** como Enterprise Account Executive. Graduado en ADE en la Oberta de Catalunya, ha ocupado roles de responsabilidad en Transmit Security, Akamai Technologies, Azlan y Marconi Iberia, entre otras.



● **TRC** ha fichado a **Patricia Sáenz** como Account Manager. Licenciada en ADE, ha desarrollado su carrera en AbbVie, Grupo Adra360 y CH Carolina Herrera, entre otras.



● **Silvia López Sánchez-Polain** ha sido contratada como Directora Comercial en **Global Technology**. Con más de 20 años en TIC, ha desempeñado puestos de responsabilidad en Babel, Accenture, Abast y GlobalSuite Solutions. Además, ha sido responsable hasta 2023 del programa de *mentoring* de Women4Cyber Spain (W4C Spain).



● **S21sec** ha promocionado a **Asterio Fernández** a Bid Manager para el departamento de Presales. Ha desarrollado su labor en Telefónica Tech, Westcon Comstor, A3Sec y Amazon, entre otras. Es ingeniero en Informática por la UPM.



● **Julio Tejedor** ha sido fichado por **Cisco** como Especialista en Ventas de Ciberseguridad en el equipo de Proveedores de Servicios. Hasta ahora responsable de Ingeniería Preventa de Ciberseguridad de Telefónica Tech, también estuvo en Swisscom y Accenture.



● **SentinelOne** ha apostado por **Sergio Bravo** como Enterprise Sales Manager. Ha ocupado roles de responsabilidad en Bitdefender, Kaspersky Lab, HPE y MicroStrategy. Es graduado en Telecomunicaciones por la Politécnica de Madrid.

Podría encargarse de la ciberseguridad de su empresa por su cuenta, pero... ¿por qué debería hacerlo?

El servicio SOPHOS MDR garantiza resultados excepcionales de seguridad para que usted pueda liberar a su personal de TI.



**Sophos Managed
Detection and Response**

Nuestro equipo dedicado y altamente especializado detecta y neutraliza las amenazas más rápido que nadie.

SOPHOS

CAIXABANK, TECNALIA y OPENNEBULA participarán en un consorcio europeo para definir un marco de evaluación y certificación de servicios en nube

CaixaBank ha anunciado su participación en un consorcio europeo enfocado en proporcionar herramientas para automatizar y unificar la gestión de controles de seguridad para servicios *cloud*. Con este proyecto, los integrantes del consorcio pretenden definir un marco europeo homogéneo de evaluación y certificación continua de servicios en la nube.

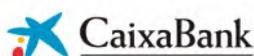
El proyecto de investigación, denominado Emerald (*Evidence Management for Continuous Certification as a Service in the Cloud*), estará financiado por la Comisión en el marco del programa Horizonte Europa, con una inversión de 4,7 millones de euros, y tendrá una duración de tres años. En total, estará integrado por 11 entidades **Fabasoft, Nixu, Fraunhofer, scch, Know Center,**

Consiglio Nazionale delle Ricerche y IONOS, Cloud Ferro, además de tres españolas: **CaixaBank, Tecnalía** (coordinador de esta iniciativa) y **OpenNebula Systems.**

Emerald pretende mejorar la interoperabilidad a nivel tecnológico de las soluciones actuales de moni-

torización e incorporar regulaciones específicas, así como desarrollar herramientas y modelos inteligentes para facilitar la aplicación e implementación ágil de una certificación

de servicios de *cloud* reduciendo la complejidad en toda la cadena de valor. El rol principal de CaixaBank en el proyecto será liderar un caso de uso de certificación continua de servicios *multi cloud* automatizando el proceso de recogida y *reporting* de los controles de seguridad.



ZIUR consolida el espacio creado para que las empresas compartan experiencias sobre protección cibernética

El Centro de Ciberseguridad Industrial de Gipuzkoa (Ziur), ha consolidado el espacio creado hace un año para que las empresas industriales del territorio compartan experiencias en torno a la ciberseguridad. El grupo de colaboración impulsado por la organización cuenta actualmente con 43 CIOs (responsables de sistemas), que han tejido una red de



presencia de 35 CIOs y CISOs de 30 empresas guipuzcoanas. En el encuentro, también participaron referentes como **Igor Navascues, de Mytra,** quien mostró las conclusiones de un proyecto que lleva a cabo para evaluar la seguridad en los

entornos ICS (Sistema de Control Industrial, por sus siglas en inglés) de 18 empresas de diversos sectores industriales. **Amor Domínguez, de TÜViT,** también presentó el panorama de normativas que se está desarrollando a nivel europeo y que se aplicarán a la industria con notables cambios a través de regulaciones como NIS2, CRA e IEC 62443.

confianza para compartir información útil y para apoyarse ante los ataques informáticos, que se han multiplicado en el último año.

Precisamente, entre sus últimas iniciativas, antes de final de año celebró una jornada dedicada a ciberseguridad industrial, con la

NOMBRAMIENTOS



● **Botech** ha comenzado una nueva etapa, tras reorganizar y reunificar sus negocios, en la que **Alberto España** ocupará el cargo de CEO, que compartirá con el fundador de la empresa, **Miguel Ángel Rojo**, mientras que **Fernando Carrazón** será CTO y responsable del VSOC 4.0 de la empresa y **Raúl Mejía** COO. España cuenta con una trayectoria de 30 años con puestos de responsabilidad en Visa Internacional, American Express, Citibank y Banco Santander. Rojo, fundador de la empresa hace casi 15 años, cuenta con tres décadas de trayectoria en los que ha destacado por su profundo conocimiento técnico y su experiencia en el mundo del fraude y la ciberseguridad. Carrazón ha trabajado para Radware, Gonet y ha sido confundador de Solver4. Mejía tiene una trayectoria de 15 años, destacando, entre otras, por su experiencia en evaluaciones de cumplimiento, riesgo y controles en grandes organizaciones en Iberoamérica.



● **Veeam Software** ha promocionado a **Tim Pfaelzer** a Director General y Vicepresidente Senior de Europa, Oriente Medio y África (EMEA). Pfaelzer, que lleva en la compañía desde 2021, cuenta con más de 20 años en el sector TI, incluyendo puestos de dirección en Dell y varios cargos de responsabilidad en Adobe, Autodesk y Salesforce.



● **Sofistic**, del Grupo Cuatroochenta, ha contratado como Country Manager para España a **Fernando Denis Ramirez**. Hasta ahora CEO de Hispasec, con una amplia trayectoria, ha trabajado en Koodous, Iron Gate y fue confundador de TheCircurs, entre otras.



● **José Ramón Palanco** ha puesto en marcha una compañía bajo el nombre de **Plexicus**, que gestionará como CEO, centrada en la gestión automatizada de vulnerabilidades con LLM. Con una amplia experiencia, ha ocupado cargos de responsabilidad y fundado empresas como Epic Bounties, Dinoflux y Puffin Security, además de haber trabajado para Telefónica. Es ingeniero de Telecomunicaciones por la Universidad de Alcalá.



● **Hispasec** ha reconocido la buena labor de **Miguel Manteca**, hasta ahora Director Comercial, ascendéndole a CEO, además de promocionar a **Benigno Cantero** a Director Técnico Comercial.

Manteca, que lleva más de un lustro en la empresa, ha trabajado para Simply Blet y El Corte Inglés, entre otras. Cantero ha desarrollado casi toda su trayectoria en la organización y en El Corte Inglés.



● **Arrow ECS** ha ascendido a **Iñaki López Monje** a Vicepresidente para el Sur de EMEA. Con una dilatada trayectoria profesional, lleva en el Grupo desde hace más de una década, además de haber trabajado en roles de responsabilidad en compañías como Altimate, Mambo Technology y Sofecom, entre otras.



All4Sec | All4Sec
CiberSeguridad

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**



www.all4sec.es | info@all4sec.es
916 366 544



STORMSHIELD integra el 'Estado de URL' de BITDEFENDER, como servicio de filtrado

Stormshield ha ampliado su asociación con Bitdefender para incluir el 'Estado de URL' como



servicio de filtrado, tras integrar el año pasado su herramienta *antimalware* en sus soluciones Stormshield Network Security y Breach Fighter. "Con tantas normativas que controlan el uso de la web, las empresas tienen la responsabilidad de regular su utilización en el ámbito profesional, por motivos legales, de productividad y -lo más importante- de seguridad. La funcionalidad de filtrado de URL incorporada en los cortafuegos Stormshield hace más sencillo cumplir con dicha regulación", recuerdan desde la compañía gala, a la vez que subrayan que los clientes tienen la opción de contratar el servicio de Estado de URL como suscripción.

En paralelo, Stormshield ha anunciado que su gama de soluciones de Seguridad de Infraestructuras TI (Stormshield Network Security), ha obtenido la Certificación Common Criteria (CC) EAL 4+, uno de los certificados internacionales más importante en el ámbito de la seguridad y que reconoce el valor y la excelencia de productos TI.

Esta nueva certificación representa un nuevo e importante voto de confianza de la **Agencia Nacional de Seguridad de los Sistemas de Información (ANSI)** francesa, y una nueva etapa en el proceso de certificación y cualificación de las soluciones de la compañía.

SUPERCOMPUTACIÓN DE CASTILLA Y LEÓN potencia su ciberseguridad de la mano de ALTIA

Altia ha sido adjudicataria de un contrato con el **Centro de Supercomputación de Castilla y León**, financiado con fondos REACT-EU, para potenciar su ciberseguridad. La consultora española suministrará e implementará herramientas avanzadas y brindará soporte desde su SOC.



El Centro de Supercomputación de Castilla y León (SCAyLE) es una entidad pública creada por la **Junta y la Universidad de León**, que pertenece a la **Red Española de Supercomputación (RES)**, y tiene por objeto la mejora de las tareas de investigación de la Universidad, los centros de investigación y las empresas de la Comunidad. Con el fin de contar con soluciones avan-

zadas que le permitan proteger toda su organización, ha decidido confiar en Altia en un proyecto que tendrá una duración de 60 meses.

En dicho proyecto destacan la implementación de soluciones avanzadas para proteger los diferentes entornos de SCAyLE y una infraestructura de nueva generación que salvaguarde el perímetro completo de la organización, con un cortafuegos perimetral en alta disponibilidad.

Además, dispondrá de un sistema de protección del correo-e y de vigilancia y monitorización de sus redes internas basados en IA para la detección de patrones, actividades y tráfico potencialmente peligrosos. El sistema de análisis y monitorización de la red IP corporativa implantado permitirá conocer las amenazas, gestionar los riesgos de la red y articular la adecuada capacidad de prevención, defensa, análisis, investigación, recuperación y respuesta.

NOMBRAMIENTOS



● **Jaime Ron** ha sido nombrado CEO de **Prosegur Tech**, bajo cuya responsabilidad estará la unidad de ciberseguridad Cipher y con cuya puesta en marcha la empresa "reafirma su compromiso con la innovación tecnológica, presentando una propuesta única y diferencial para abordar las necesidades del mercado". Hasta ahora Director de Estrategia, ha trabajado para Telefónica, Movistar, Nomura y Barclays, entre otras. Es graduado en ADE por la Autónoma de Madrid.



● **Zscaler** ha reforzado su equipo en España y Portugal con la incorporación de **Pablo Vera** como Regional Director. Cuenta con una solventa experiencia de más de 16 años en ciberseguridad y anteriormente había sido Director de Soluciones de Ciberseguridad de Microsoft, Director Comercial en Symantec, además de trabajar en FireEye/Mandiant y McAfee. Es Ingeniero Superior de Telecomunicación por la Universidad Politécnica de Madrid y PDD por IESE Business School.



● **Alejandro Ramos** se ha reincorporado a **Telefonica Tech**, en calidad de Country Manager de Brasil, en tanto que el equivalente de la multinacional española para México es **Rafael González Barboza**.

Con más de 20 años de experiencia, venía siendo CISO en El Corte Inglés y con anterioridad Director Global de Operaciones de Ciberseguridad en la recién creada T-Tech. Por su parte, González Barboza cuenta con más de 25 años de trayectoria, diez de ellos en Telefónica Movistar México donde fue responsable de establecer el *go to market* de todas las soluciones digitales en el país.



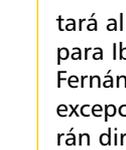
● **KPMG España**, de cara a su oferta de servicios, contará con **Rubén Muñoz** como Cybersecurity Director, con **Fernando Guirado** como Cybersecurity Senior Manager y con **Alejandro Belón** como



Cybersecurity Senior Sales Manager. Muñoz ha ocupado puestos de responsabilidad en DXC Technology, Microsoft y HPE, entre otras. Es ingeniero Informático por la Autónoma de Madrid. Guirado, ingeniero de Telecomunicaciones por la Universidad de Granada, ha realizado su trayectoria en Siemens, BBVA y GMV, entre otras. Belón, con una amplia trayectoria, ha trabajado en Accenture, DXC Technology, Vodafone Global Enterprise y Econocom, entre otras.



● El mayorista **V-Valley** ha cambiado su estructura organizativa, nombrando a **Alberto López** y **Hugo Fernández** responsables del negocio en España, Portugal y norte de África. En concreto, López estará al frente del área de ciberseguridad de la compañía para Iberia, además de asumir la dirección de **Lidera**.



Fernández dirigirá el negocio para Iberia y Marruecos, a excepción del área de ciberprotección. Ambos reportarán directamente al Director General del Grupo Espinnet, **Giovanni Testa**. Estos movimientos también han supuesto la salida de Javier Bilbao-Goyoaga del Grupo.

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

La fusión de SOLVER4, HYDRAPAYMENT y BOTECH da lugar a una nueva organización con una cartera de soluciones y servicios integrada y global

Botech ha acometido una reorganización uniéndose tanto la propia Botech como **Hydrapayment** y **Solver4**, dando lugar a una nueva entidad, “donde se encuentran todas nuestras soluciones y servicios de ciberseguridad, normativa y pagos”.

Casi 15 años de historia y presencia en España, México y Estados Unidos, la empresa ha destacado



este movimiento que también supone la renovación de su identidad corporativa “para seguir innovando, creciendo y dando el mejor servicio a nuestros clientes, a nuestros *partners* y al mercado”.

Así, en su cartera de servicios y soluciones destaca desde su

propuesta de prevención contra el fraude, hasta de Inteligencia, PCI, orquestación de pagos, virtual SOC y certificación para comercios, entre otros. Asimismo ha puesto en marcha una nueva plataforma web que busca “reflejar esta nueva marca y nuestros valores: globalidad, cercanía,

personalización y orquestación de pago”.

En paralelo, ha organizado su equipo ejecutivo, pasando **Alberto España** a ser, desde diciembre, CEO de Botech, cargo que compartirá con **Miguel Ángel Rojo**, fundador de la compañía. A ellos se sumará **Fernando Carrazón**, como CTO de BOTECH y **Raúl Mejía** como CCO.

TELEFÓNICA gana la adjudicación, por 9,1 millones, del equipamiento del LABORATORIO NACIONAL DE CIBERSEGURIDAD 5G

Telefónica ha sido adjudicataria por 9,1 millones de euros (IVA incluido) del contrato público financiado con fondos europeos para el suministro de equipamiento destinado al lanzamiento, despliegue y operación del **Laboratorio Nacional de**



Ciberseguridad 5G y Nuevas Tecnologías (Incibe-Lab), así como los servicios conexos, según figura en el portal de contratación del Estado y recoge **Europa Press**.

“Se trata de un contrato mixto con un presupuesto máximo en el cual el contratista se obliga a ejecutar el objeto (del contrato) de forma sucesiva y por precio unitario, sin que el número total de entregas o prestaciones estimadas en el objeto del contrato se defina con exactitud al tiempo de celebrar este por estar subordinadas las mismas

a las necesidades de Incibe”, detalla la adjudicación.

La duración del contrato es de 36 meses, con fecha límite del 30 de junio de 2026, y los pedidos de suministro a lo largo de la vigencia del mismo distintos del primer pedido estarán “sujetos a las necesidades” del **Instituto Nacional de Ciberseguridad** (Incibe).

El contrato ha sido adjudicado por la dirección general del Incibe y se ha negociado sin publicidad “por exigirlo la protección de intereses esenciales para la seguridad del Estado”, añaden los documentos publicados en el portal de contratación.

Telefónica se ha impuesto a la unión temporal de empresas (UTE) compuesta por **Fujitsu** y **Vodafone**, que también había presentado una oferta para este contrato.

NOMBRAMIENTOS



● **Joaquín Castellón** ha sido contratado por **Izertis** –adquiriente de **Sidertia**– como Director de Defensa y Ciberseguridad. Hasta ahora CSO de **Navantia**, fue anteriormente Director Operativo del Departamento de Seguridad Nacional cuando el organismo se puso en marcha en 2012. Es oficial de la Armada en la reserva.



● **Oriol Torruella** ha sido contratado como Director de Ciberseguridad e Identidad Digital de **Inetum** para Cataluña, a la vez que la compañía ha ascendido a **David Santafé** a Director para Iberia y Latam. Torruella ha desarrollado su amplia carrera profesional como abogado en despachos privados y en el Centro de la Seguridad de la Información de Cataluña (CESICAT) y, en 2019, fue nombrado Director de la Agencia de Ciberseguridad de Cataluña. Por su parte, Santafé ha trabajado para **Iecisa**, **Kio Networks** y **El Corte Inglés**, entre otras.



● **Logalty** ha promocionado a **Sergio Barbero** a CISO. Cuenta con una dilatada trayectoria donde ha ejercido diferentes roles en compañías como **Datia Technologic**s e **Entelgy Innotec Security**. Es graduado superior en Administración de Sistemas.



● **NTT Data Reino Unido e Irlanda** ha fichado a **Enrique Martín Pascual** como Deputy CISO y Regional CISO para Iberia y Benelux. Cuenta con una dilatada trayectoria con roles de responsabilidad en **Everis**, **Mnemo** e **Ingenico**, entre otras. Es licenciado en Filosofía por la **Uned** y cuenta con dos postgrados por la Autónoma en Ciberseguridad e Inteligencia.



● **Diego Fernández González** ha sido promocionado por **Centum Digital** a Director DTI (Defensa Transporte Industria) y Ciberseguridad. Ha desarrollado gran parte de su trayectoria en el Ministerio de Defensa, donde fue supervisor de SOC durante un lustro.



● **myCloudDoor** ha incorporado a **Catalina Jiménez** para su área de Security & Innovation. Ingeniera de Telecomunicaciones por la Politécnica de Valencia, con anterioridad ha ocupado roles de responsabilidad con foco en ciberprotección en **Sothis**, **Everis** y **EADS**, entre otras.



● **Applus+ Laboratories** ha reconocido la buena labor de **José Francisco Ruiz**, hasta ahora CTO de **jtsec** -perteneciente a la compañía-, encomendándole la dirección de la Unidad de Negocio de Ciberseguridad, con un equipo de casi 200 profesionales. Ingeniero en Informática por la Universidad de Granada, es Cofundador de **jtsec**.



● **Evolutio** ha reconocido la buena labor de **Ricardo Sanz**, ascendéndole a Cybersecurity Director, además de designar como CISO a **Alfonso Minaya** y a Cybersecurity Sales Manager a **Daniel López Rojo**. Sanz ha desarrollado gran parte de su trayectoria en la compañía y en **BT**, en la que comenzó hace más de dos décadas. Minaya, con más de 25 años de experiencia, ha trabajado para **LagoSolar**, **DF Digital Security**, **Entelgy Innotec Security** y **Mnemo**, entre otras.



López es ingeniero en Organización Industrial por la Universidad de Valladolid y ha trabajado para **HPE**, **DXC** y **BT**, entre otras.

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



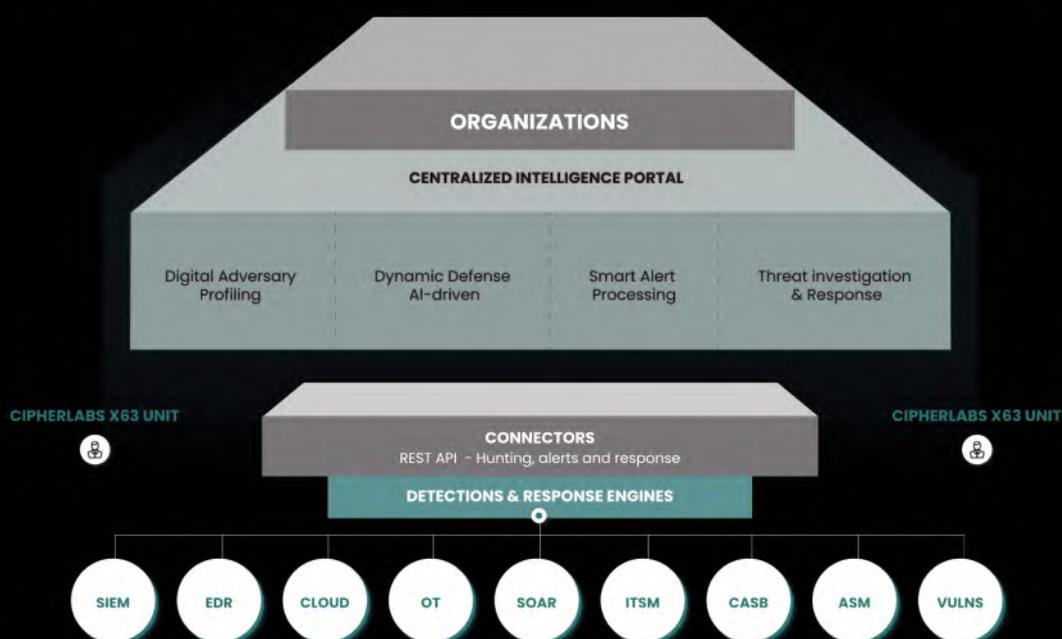
MODELADO DEL
ADVERSARIO +
COGNITIVE



CIPHER
PLATFORM



SISTEMA DE
DETECCIÓN SIN
PRECEDENTES



Hable con nosotros: contacto@cipher.com



ABANCA: sintetización de todos los datos sobre riesgo humano en un solo indicador para mejorar el Gobierno de la Concienciación en Seguridad

Los CISOs de las empresas se enfrentan al desafío desproporcionado de reclutar a todos los empleados de la compañía para proporcionar un frente común de defensa contra los intentos cada vez más numerosos y sofisticados de los ciberdelincuentes, de utilizarles como vector de entrada. Si bien el mercado de la Ciberseguridad produce nuevas y mejores soluciones para ayudar con este problema, el responsable de Seguridad se encuentra con la dificultad añadida de tener que orquestar todos estos elementos de forma integrada y que permita obtener las sinergias que resultan de combinarlos de manera optimizada. En este contexto, en las siguientes líneas se describe el proyecto que Abanca, en conjunción con Áudea, lleva a cabo con foco expreso en la operación (y constante rediseño) de una Oficina de Concienciación de Seguridad. Dicha experiencia fue expuesta en primicia en la última edición de Securmática.



CARLOS PÉREZ SALDAÑA / JAVIER RUIZ DE OJEDA

El problema de la concienciación de Seguridad a los empleados de cualquier organización (y especialmente en el sector bancario, el más regulado de todos) no es nuevo, pero tampoco ha dejado de evolucionar, impulsado por el aumento incesante de nuestra relación con la tecnología.

Aunque las defensas tecnológicas siguen siendo las más relevantes y fiables en una compañía, los atacantes recurren constantemente al error humano como vector de entrada, precisamente porque a veces permite un atajo a la hora de sobrepasar estas medidas defensivas.

Adicionalmente, pocas son las organizaciones que pueden permitirse disponer de personal interno dedicado exclusivamente a la concienciación de sus empleados, por lo que se hace necesario recurrir a servicios externos que puedan aportar la especialización y la experiencia necesarias para hacer frente a un enemigo que dedica todo su tiempo a la creación y difusión de nuevos ataques de ingeniería social y extorsión. Esto ha permitido a lo largo de las últimas décadas evolucionar las herramientas defensivas desde las píldoras y los coloquios con los empleados (que siguen manteniendo cierta eficacia) para pasar a simular ataques para que puedan entrenar sus capacidades defensivas, o incluso emplear funciones de inteligencia artificial para diseñar itinerarios formativos personalizados que impacten a los empleados de forma optimizada en función de su experiencia, capacidades, puesto, herramientas tecnológicas, etc.

Las ventajas que presenta este ecosistema defensivo diverso y especializado de colaboración tienen un coste, que es la gestión e integración de cada elemento participante. No solo eso, la concienciación de los empleados no deja de ser una pieza más en la estrategia de ciberseguri-

dad, que debe encontrar su lugar entre el resto de los elementos que componen la protección contra los vectores de entrada más comunes.

Para **Abanca** y para **Áudea**, que colaboran desde hace tiempo en la operación (y constante rediseño) de una Oficina de Concienciación de Seguridad, algunas de las claves para el éxito son precisamente:

- La combinación de servicios y herramientas aprovechando las fortalezas de cada uno.
- La obtención y el uso de datos de todas las iniciativas independientemente de su origen y canal, y el diseño de un cuadro de mandos que condense todos estos datos de distintos orígenes en unos pocos indicadores agregados que tengan significado propio y que ayuden a gobernar la toma de decisiones y a reportar una situación compleja de forma simple a las distintas partes interesadas.
- La aproximación combinada ha consistido desde el inicio en la segmentación de las

acciones de concienciación en tres dominios diferenciados que detallaremos a continuación. En este sentido, es indispensable el uso de la herramienta **Kymatio** que aplica tecnología IA, siendo la única forma de conseguir ese nivel de granularidad en la formación con su capacidad para medir de forma continua tanto los conocimientos como el cambio de comportamiento. Estos dominios son: [ver **Figura 1**].

• Los que aumentan el **conocimiento** del empleado a nivel teórico sobre los tipos de ataques que pueden sufrir, las estrategias defensivas que pueden seguir y los organismos a los que pueden solicitar ayuda dentro del banco. Aquí se hace especialmente relevante segmentar todos los conocimientos que se espera que adquieran los empleados, definiendo las acciones y conocimientos exactos que se esperan de ellos. También es necesario contar con capacidades de producción de

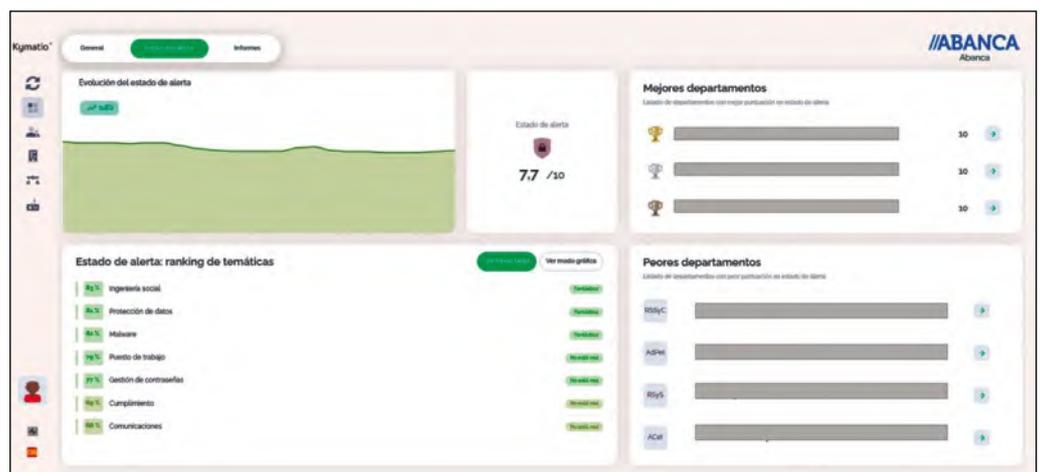


Figura 1

La aproximación combinada ha consistido desde el inicio en la segmentación de las acciones de concienciación en tres dominios diferenciados: Los que aumentan el conocimiento del empleado, los que lo entrenan y los que aumentan su compromiso con la misión de ciberseguridad del banco.



MDR OT

CIBERSEGURIDAD INDUSTRIAL

25
MILL

En 2030 habrá 25 mill. de dispositivos OT/IoT conectados en infraestructuras IT. (Gartner)

641

Nuevas vulnerabilidades específicamente industriales descubiertas en el primer semestre de 2023 (Nozomi Networks)

34%

De las vulnerabilidades carecen de un método de parcheo o de remediación, poniendo en riesgo la disponibilidad del entorno productivo (CISA)

80%

De las organizaciones con entornos industriales, carecen de mecanismos de visibilidad, lo que impide una correcta detección, triaje y respuesta (Dragos)

Servicios de monitorización prestados por un equipo ICS con experiencia acreditada:

Monitorización de entornos OT, considerando los movimientos laterales IT	Detección OT basada en las TTPs de Mitre Att&ck for ICS y los patrones comunes de ataque de CAPEC	Inteligencia y procedimientos propios del grupo de competencias globales de ciberseguridad de Thales	Más de 20 años ofreciendo servicios de detección y respuesta 24x7x365
---	--	---	--

Contacta con nosotros para más información:



+34 900 840 730



www.s21sec.com



marketing@s21sec.com

S21
SEC
Cyber Solutions by Thales

contenidos en distintos formatos para poder aprovechar los distintos canales en una estrategia unificada de comunicación. Por último, deberá diferenciarse entre los distintos roles del banco a partir de sus perfiles de riesgo.

- Los que entrenan el **comportamiento** seguro del empleado proponiéndole situaciones prácticas y simulando ataques realistas para mejorar y medir su respuesta ante ellas. En este caso debe contarse con la capacidad de simular tecnológicamente estos ataques y de medir los resultados de su ciclo de vida para observar qué dificultades encuentran los empleados y cómo orientar la formación a futuro. Adicionalmente, se debe poner énfasis en que el empleado no solo evite las conductas peligrosas, sino que además reporte cualquier sospecha inmediatamente, ayudando a “vacunar” a sus compañeros de ataques similares. Finalmente, se deben complementar los datos obtenidos de los ataques simulados con los obtenidos por otros medios que puedan ser reflejo de conductas de riesgo o indicios de otros ataques que puedan ocurrir contra los empleados (contraseñas filtradas, webs copiadas, información exfiltrada, dispositivos robados o extraviados, etc.)

- Los que aumentan el **compromiso** del empleado con la misión de ciberseguridad del banco, consiguiendo que éste comprenda la importancia de ayudar en su defensa. Este componente suele dejarse de lado, pero es fundamental para entender por qué ciertos empleados a pesar de conocer las conductas que deben seguir aun así pueden no hacerlo, ya que puede tratarse de un problema motivacional. Para ello es fundamental contar con la capacidad de establecer itinerarios personalizados que refuercen los temas que cada empleado requiere.

Adicionalmente, es importante recordar que una estrategia de comunicación exitosa no puede ser iniciativa de un solo departamento, sino que requiere de la participación de áreas como Recursos Humanos, Capacitación, Gestión del Cambio o Comunicación. En ABANCA estas áreas no se limitan a encajarlos en el calendario formativo de los empleados, sino que son miembros activos, multidisciplinares e implicados de la Oficina proponiendo iniciativas, liderando la interlocución con el resto de áreas, y tomando decisiones para la mejora de los indicadores. Convirtiéndose así en una pieza clave del éxito del proyecto.



Figura 2

Una estrategia de comunicación exitosa requiere de la participación de áreas como RRHH, Capacitación, Gestión del Cambio o Comunicación. Son miembros activos, multidisciplinares e implicados de la Oficina proponiendo iniciativas, liderando la interlocución con el resto de áreas, y tomando decisiones para la mejora de los indicadores, convirtiéndose así en una pieza clave del éxito del proyecto.

¿Cómo medir toda esta actividad?

La última cuestión es: ¿Cómo medir toda esta actividad? ¿Cómo puede agregarse toda la información recopilada de cada iniciativa y fuente de datos para crear un único cuadro de mandos que permita al banco guiar su toma de decisiones y a su vez transmitir a la Alta Dirección un indicador agregado de riesgo y rendimiento para reflejar los avances de esta Oficina de Concienciación?

Para responder a estas preguntas debe comenzarse recordando los factores que debe incluir un indicador relevante:

- Transmitir el estado actual de la variable medida, pero también su evolución desde situaciones pasadas y su tendencia y proyección futuras.

- Reflejar el impacto que distintas iniciativas tengan sobre las variables medidas, de manera que pueda observarse su utilidad y decidirse cómo enfocar futuras iniciativas para optimizar su impacto.

- Ser comprensibles y aportar valor a nivel directivo.

- Permitir su desglose en indicadores de mayor profundidad para su aplicación ejecutiva y táctica en el día a día.

- Guiar, en última instancia, la toma de decisiones de la Oficina de Concienciación para seguir reduciendo la exposición al riesgo cibernético basado en el error humano.

Una vez contemplados los requisitos para los indicadores, deben empezar a construirse desde la capa inferior, incluyendo los datos de todas las iniciativas efectuadas y separándolos en los dominios de conocimiento, comportamiento y compromiso. Aquí es donde se sitúa la definición de una estrategia de medición que integre todos los indicadores para que se pueda medir el cambio de comportamiento de los empleados.

Una vez establecido el piso inferior, pueden empezar a definirse indicadores agregados, que serán los que nos permitan conocer el estado de cumplimiento actual y previsto. Para ello, debemos contar con objetivos numéricos y concretos que perseguir y también con umbrales que reflejen los estados tolerables y deseables para

cada indicador agregado. El último nivel se compondrá de uno o unos pocos indicadores finales que reflejen el nivel de exposición al ciberriesgo humano para el banco.

Una vez creados, solo queda trasladarlos a un cuadro de mandos que disponga de vistas especializadas para cada parte interesada, y mantener la relación y el reporte con dichas partes interesadas para proporcionar el mayor valor posible. [Ver **Figura 2**].

En definitiva, nuestra metodología está fundamentada en una estrategia basada en una medición eficaz combinando distintos dominios, servicios y tecnologías que facilitan esa mejora continua necesaria en cualquier proceso. ■

CARLOS PÉREZ SALDAÑA
CISO
Grupo ABANCA

JAVIER RUIZ DE OJEDA
Consultor Senior GRC
ÁUDEA Seguridad de la Información

Seguridad que está lista para



Cualquier situación

Cualquier nube

Transformación empresarial

Fusiones y adquisiciones

Cambios empresariales

Trabajadores híbridos

Automatización

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 \[netskope.com/es\]\(https://www.netskope.com/es\)](https://www.netskope.com/es)

“La adquisición, gestada en España, da forma a un proveedor global de servicios de ciberseguridad capaz de operar simultáneamente en más de 120 países”

Félix Muñoz
 Director General
 de Innotec Security,
 part of Accenture

**Agustín
 Muñoz-Grandes**
 Responsable de Accenture
 Security Iberia

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

La reciente operación por la que Accenture ha adquirido a la compañía española de ciberseguridad Innotec Security, es una de las más importantes realizadas en nuestro país en este sector de actividad, que viene a sumar al enorme catálogo de servicios Tech de la multinacional de origen americano, el *expertise* y la buena cartera de clientes de la española. Accenture Security, que ya disponía de un destacable potencial

de capacidades, logra una posición fuerte también en el segmento de la operación en el mercado ibérico. SIC ha tenido la oportunidad de hablar con los dos ejecutivos clave de ambas organizaciones, antes competidores, hoy compañeros y siempre colegas. Ellos nos cuentan la experiencia en los primeros pasos de la integración.

– **Son conscientes de que la operación que han llevado a cabo sus organizaciones ha conmovido los cimientos del sector de la ciberseguridad en España y en algunos otros mercados?**

– **Agustín Muñoz-Grandes (AM-G).** Es una fórmula ganadora, que va a permitirnos ofrecer a los clientes el máximo valor, combinando nuestras capacidades globales con un excelente equipo al integrar los aproximadamente 400 especialistas que teníamos aquí en Accenture Security con los 450 de Innotec Security.

– **Félix Muñoz (FM).** Integrar Innotec Security, un jugador puro en ciberseguridad, en una multinacional, eleva hasta el infinito nuestra capacidad de llegar a muchos mercados y de incorporar la ciberseguridad en todos los escenarios Tech. Estamos en un mercado muy competitivo. Evidentemente nosotros ya tenemos un histórico significativo en España y llevábamos tiempo abriendo mercados en Iberoamérica, pero

nos faltaba la fortaleza para hacer proyectos globales, que es lo que exigen las grandes empresas de nuestro país para seleccionar socios que les acompañen en sus proyectos estratégicos. Ahora no tenemos ese límite. Se nos abre, además, un mundo nuevo a la hora de desarrollar competencias a nivel nacional, y también de internacionalizar esas excepcionales competencias de factura española apoyándonos en el Centro del que dispone Accenture en Málaga.

– **Accenture es una compañía muy exigente con la verificación de las capacidades de sus empleados y colaboradores. ¿Está generando disfunciones este particular en el proceso de integración de Innotec, ahora que tan importante es contar con expertos?**

– **AM-G.** En absoluto. Las políticas de ambas empresas casan bien. En este tipo de operaciones siempre existe el reto de la integración de culturas, la integración de personas, de formas de trabajo. En Accenture

tenemos en la más alta consideración a las personas, sus capacidades y la formación de los equipos que formamos. Y en ciberseguridad casi más que en ningún otro campo. Eso es clave. La carestía de talento va a seguir manifestándose. Nuestro proyecto de ciberseguridad conjunta está basado en las personas que tenemos y en nuestra capacidad de seguir desarrollando y atraer el mejor talento Tech y no Tech del mercado, combinando lo mejor de los estilos de ambas organizaciones.

Esta fórmula, particularmente en España y Portugal, refuerza lo que queremos que sea el nuevo Accenture Security. Ahora mismo estamos en pleno proceso de integración, haciendo numerosas sesiones de trabajo en todo frente: cultura, procesos, innovación... Y por ahora la respuesta de los equipos está siendo excelente. Hay mucha motivación. Es verdad que siempre habrá que integrar plataformas, procesos y que Accenture como multinacional es muy exigente.

– **FM.** Hemos acordado un modelo de integración en el que no vamos a tocar las operaciones que tenemos con nuestros clientes. Tenemos claro que lo que sí podemos es potenciarnos combinando competencias de ambas compañías. Y ese es el nudo gordiano del asunto. La cultura depende de las personas, sea en una compañía grande, mediana o pequeña. En el caso que nos ocupa, a pesar de que pueda parecer que Accenture tiene una cultura muy diferente a Innotec Security, en el trato a la gente, en la forma de actuar y en la forma de hacer las cosas, hay sintonía. Por ejemplo, valoran mucho nuestro estilo de atraer talento en las capas digamos muy “frikis” en el mercado. En nuestro mundo de la ciberseguridad no hace falta decir más.

– **¿Cuándo tienen previsto que Innotec Security, part of Accenture, deje de serlo y se convierta en Accenture Security? En los mentideros se habla del año 2025.**

– **FM.** Todavía no lo tenemos fijado, porque la primera y fundamental tarea es generar valor en los clientes. Además, la madurez en todos los procesos de Accenture es



“El objetivo marcado es tener un cuerpo de ciberseguridad en Accenture Security, integrado por los dos equipos trabajando conjuntamente como una única organización para prestar más y mejores servicios y liderar el mercado. Hasta cuándo se va a utilizar la diferenciación de marcas va a depender mucho de las dinámicas de mercado”. AM-G

incuestionable, y todos los que trabajamos en Innotec Security estamos, como quien dice, haciendo un máster.

– **AM-G.** Evidentemente hay un plan de integración. Y como dice Félix, en él la prioridad son los clientes y las personas. El objetivo que nos hemos marcado es tener un cuerpo de ciberseguridad en Accenture Security, integrado por los dos equipos trabajando conjuntamente como una única organización para prestar más y mejores servicios y liderar el mercado. Hasta cuándo se va a utilizar la diferenciación de marcas va a depender mucho de las dinámicas de mercado. Con todo, el objetivo es que haya una transferencia de valor y una integración completa.

– **FM.** Vamos a seguir trabajando con la misma cercanía con los clientes que nos caracteriza. Evidentemente ahora nuestras capacidades técnicas se multiplican por cinco con Accenture, que tiene además un número de clientes muy respetable y conocimientos enciclopédicos de la industria. Por eso uno de los retos es la suma de competencias para que el *go to market* sea conjunto desde ya.

El centro de Accenture en Málaga, que es de alcance mundial, tiene tal nivel de competencias que podemos sumar en muchos clientes. Dicho de otro modo: proyectos que yo nunca me hubiera imaginado emprender, ahora se muestran factibles y los podemos ejecutar con todas las capacidades globales de Accenture Security, porque ellos sí que tienen una capacidad global donde toda la ciberseguridad está conectada y hay un modelo de cooperación y de poder incluir en proyectos competencias de otros países fácilmente. Es apasionante.

– **No es la de Innotec Security la única adquisición que ha realizado Accenture en materia de ciberseguridad. En Colombia y en México también ha movido ficha últimamente. Se ve que hay en la firma un especial interés en fortalecer Accenture Security.**

– **AM-G.** Uno de los elementos diferenciales de Accenture es que realmente somos una compañía global gestionada globalmente. Tenemos presencia en 67 países y ofrecemos a nuestros clientes los servicios de manera global. De forma que si un banco español multinacional o una empresa de *utilities* de energía en España con presencia también en muchísimos países, demandan servicios globales, podemos ofrecérselos diseñados aquí en España por el equipo de Accenture Security y Tech, y garantizar que se ejecuta con los parámetros, sea cual sea el país en el que operamos, coordinando todas las divi-



“Accenture tiene una red de 27 centros especializados de ciberseguridad y SOC a escala global. En España y Portugal, Accenture Security no tenía una presencia muy potente en este ámbito. Éramos parte de la red global, que está muy bien para dar servicio a clientes multinacionales y grandes clientes, pero nos faltaba capacidad de ejecución local. Con Innotec Security damos vida a uno de los líderes de nuestro mercado dentro de esa red global”. AM-G

siones de Accenture o todas las marcas de Accenture. Porque no somos un conjunto de empresas operando bajo la misma marca. Somos una única empresa cotizada, que opera con una estructura de gestión única, y eso aporta calidad de servicios, uniformidad de procesos, agilidad de respuesta (por ejemplo, referida a incidentes de ciberseguridad). Como es bien sabido, el equipo de Innotec Security dedicado a respuesta ante incidentes es muy reputado. Por tanto, tenemos hoy un equipo de más de 40 personas dedicado solo a respuesta con capacidad operativa a nivel global.

– **FM.** Los clientes nos estaban exigiendo capacidades globales en países, por ejemplo, europeos, en los que no teníamos implantación. Con Accenture, tal cual comenta Agustín, este escollo desaparece.

– **Es evidente que Accenture Security Iberia ha tenido mucho que ver con la adquisición de Innotec Security.**

– **AM-G.** Era importante para Accenture alcanzar una elevada posición en el mercado de ciberseguridad que se gesta en España y Portugal. A futuro, en Accenture siempre

estamos considerando la opción de llevar a cabo más adquisiciones. Pero, como digo, en este caso, el enfoque de crecimiento y de desarrollo se ha centrado en los mercados español y portugués, incardinado, por supuesto, en la estrategia global de crecimiento de Accenture.

Aclaro: nosotros colaboramos y trabajamos con el resto de *market units*, pero no entran dentro de nuestro ámbito de responsabilidad.

– **FM.** Innotec Security se debe a las empresas españolas. Los recursos no los vamos a utilizar para proyectos internacionales sin vinculación directa con España. La idea es crecer, generar un *hub* aquí que nos permita dar trabajo de calidad en ciberseguridad, crear y consolidar capacidades locales y lanzarlas al mundo gracias a Accenture.

– **¿Qué les han comentado los clientes al conocer la noticia de la adquisición?**

– **AM-G.** La respuesta ha sido excelente en todos los casos. Lo decía antes Félix: hay clientes que llevan más de 20 años confiando en Innotec Security, están contentos con sus capacidades técnicas y ahora ven que la



“Hemos acordado un modelo de integración en el que no vamos a tocar las operaciones que tenemos con nuestros clientes. Tenemos claro que lo que sí podemos es potenciarnos combinando las capacidades de ambas compañías”. FM

pueden proyectar a toda su operación en los países donde operan.

Accenture es una multinacional puntera en transformación y está abordando la transformación del *core* tecnológico y de los modelos de negocio de muchas de las grandes empresas con las que trabaja. Y los expertos en ciberseguridad sabemos que esta, la ciberseguridad, tiene que ir formando parte e ir acompañando ese proceso de transformación. Ese es el camino trazado por el buen gobierno, las legislaciones y el ánimo permanente de mejora. Por ser más concreto: hay que abordar los riesgos de ciberseguridad integrados con las actividades y negocios, no como un cuerpo extraño.

– Innotec Security está muy vinculada con áreas muy significativas de la “ciberseguridad nacional”. ¿Qué implicaciones va a tener su adquisición por Accenture en esta parcela del mercado?

– FM. No vamos a dejar de tener la bandera de España en el corazón. Accenture es una empresa implantada en nuestro país, que crea y quiere seguir creando riqueza y trabajo aquí. El objetivo es seguir aportando nuestro valor a la seguridad nacional, pero ampliándolo. Accenture a escala global participa en proyectos de valor para las seguridades nacionales de países, y puede aportar mucho conocimiento para fortale-

cer la nuestra. Eso sí, vaya por delante que en la materia somos muy buenos en nuestro país.

– AM-G. Trabajamos en Accenture Iberia más de 18.000 personas, la inmensa mayoría españoles. Y comprometidos con la seguridad nacional de nuestro país. ¿Qué podemos aportar Accenture y Accenture Security? Capacidades en áreas de innovación e investigación. Por ejemplo, en Quantum Computing Security y en aplicaciones de metaverso. Pero hay muchas más que existen; otras están por descubrir.

– FM. Tras la operación con Accenture, hemos tenido en Innotec Security oportunidad de conocer un impresionante laboratorio dedicado a 5G que la compañía tiene en Alemania. Nos va a permitir crecer en competencias en este campo a nivel nacional, generar dinámicas y actividad de mercado, que redundarán en mejores condiciones para la seguridad nacional y la ciberseguridad en general.

– AM-G. Además, trabajamos con las áreas de seguridad nacional de muchos países del entorno OTAN, en proyectos clasificados con los niveles de acreditación y certificación de seguridad necesarias, siempre respetando la confidencialidad y la relación local. Y los asuntos en los que dichos países están de acuerdo podemos compartirlos, y ayudar a poner en común capacidades y

visión global, cosa que cuando solo operas en un estado no puedes hacer por falta de información, análisis y medios humanos y materiales.

– La propia organización de las actividades y el mercado en verticales con una fuerte personalidad en tecnologías específicas y cada vez más conectadas, demanda ya una sectorización más o menos extremada de la gestión de la ciberseguridad. Uno de los sectores más avanzados en este camino, incluso en el terreno legal específico, es el financiero. ¿Se plantean, por ejemplo, normalizar un modelo de gobierno y gestión en todas las líneas de defensa?

– AM-G. La tendencia es esa. Es el modo de irse transformando, alcanzar eficiencia y estar preparado para el siguiente paso. No obstante, la complejidad es elevada, el punto de partida de las entidades es diferente, su madurez organizativa y en el uso de TIC también. La forma en que acontece el hecho de la gestión de la ciberseguridad depende de, entre otros, estos factores.

– FM. Se está trabajando en la materia, porque DORA, a efectos de resiliencia operativa, implica a entidades financieras y proveedores. Este es uno de los terrenos en los que se muestra la complementariedad de Accenture en su enfoque global en la gestión tecnológica orientada al negocio y la gestión de riesgos tecnológicos con las reconocidas capacidades específicas de Innotec Security enfocadas al Red Team y al Blue Team.

– AM-G. Efectivamente, hemos empezado a trabajar conjuntamente en el terreno de la resiliencia y la continuidad de negocio, incluyendo la problemática de la cadena de suministro de los clientes, de sus procesos de negocio y combinando esas capacidades de Red Team y Blue Team que menciona Félix. Pero también estamos colaborando con nuestros equipos de infraestructura, el área de gestión de riesgos, de procesos y las de nuestros clientes para estudiar cómo adaptar sus procesos, su tecnología, su infraestructura para que, tras la realización de test de estrés, sean capaces de recuperar la infraestructura crítica, aunque el punto de fallo no sea el de ciberseguridad. Este enfoque holístico de Accenture es de valor para los CISOs y CIOs, porque les ayuda a abordar el problema en todas sus dimensiones.

– ¿Qué sinergias tienen en el entorno concreto de la operación de la ciberseguridad?

– AM-G. Accenture tiene una red de 27 centros especializados de ciberseguridad y SOC a escala global. Como antes comentaba, en



/Rooted^o CON XIV

Congreso de ciberseguridad

7, 8 y 9 de marzo / KINEPOLIS Madrid

Escanea si te atreves



www.rootedcon.com

España y Portugal, Accenture Security no tenía una presencia muy potente en este ámbito. Éramos parte de la red global, que está muy bien para dar servicio a clientes multinacionales y grandes clientes, pero nos faltaba capacidad de ejecución local. Con Innotec Security damos vida a uno de los líderes de mercado dentro de esa red global y a los grandes clientes con las que ya trabajaba. Disponemos entonces de dos centros, el de Innotec Security y el centro de red europeo de Accenture de Málaga. Desde este último damos servicio a 70 clientes europeos de fuera de España. Se ve la sinergia. Queremos ser la compañía de referencia de ciberseguridad en España y Portugal, y, al tiempo, crear riqueza aquí para el resto del mundo. Esa era la idea.



“Accenture es una compañía implantada en nuestro país, que crea y quiere seguir creando riqueza y trabajo aquí. El objetivo es seguir aportando nuestro valor a la seguridad nacional y la ciberseguridad, pero ampliándolo”. FM

– **¿Cuánto llevaban ustedes hablando de la operación?**

– **AM-G.** Las incertidumbres surgen en las estrategias de adquisición de empresas. En los últimos años, los procesos de decisión suelen durar entre seis meses y un año de media.

– **FM.** Ha sido, yo creo, un proceso muy meditado para no perder nada por el camino.

– **Se conocen ustedes desde hace años. En el ramo de la ciberseguridad han sido competidores, colaboradores y ahora digamos que compañeros. ¿Cómo se ven ante esta inédita situación?**

– **FM.** Estoy francamente contento de trabajar con Agustín, a quien aprecio. Nos compenetramos bien. Yo soy una persona a la que le gustan los modelos de gestión cercanos a las personas, poco jerarquizados. Estoy trabajando muy a gusto.

– **AM-G.** Es un lujo colaborar con Félix, su equipo directivo y con el equipo que ya teníamos en Accenture. En el escenario del sector de la ciberseguridad en España, en los últimos diez años, ambos hemos liderado empresas y teníamos cierta voz y reconocimiento en el mercado. Lo digo con humildad. Encajamos en personalidad

y estilo y trabajamos para engrandecer a los dos súper equipos que hemos logrado aglutinar para construir el nuevo Accenture Security.

– **Pero, ¿les están dejando trabajar?**

– **FM.** Se nos está dejando trabajar. Y he de decir que se nota que Accenture sabe guiar con éxito este tipo de operaciones: no en vano tienen experiencia en más de 1.500 integraciones. Te apoyan y te escuchan. Lo digo yo y lo dice mi gente.

– **Antes les he preguntado, en el contexto de la sectorización, por el ramo financiero. Pero es solo uno más –si bien que destacado– en el que las especificidades tienen un peso importante a la hora de prestar servicios de ciberseguridad. Muchos otros tienen también experiencia regulatoria en ciberprotección. Otros no tanta.**

– **AM-G.** La estrategia de Accenture Security, en el marco de la de Accenture, ya desde hace años, pasa por la verticalización. Capacitamos a los equipos de trabajo, brindamos proximidad al cliente, conocemos su negocio, sus procesos, tecnologías, hitos y retos sectoriales, y adaptamos nuestra ofer-

ta y nuestras capacidades para ofrecer, por ejemplo, un *renting* a los sectores con sus particularidades, sus necesidades tecnológicas, regulatorias...

A efectos globales, Accenture tiene bien establecidos verticales como el sector público, financiero, *utilities*, energía, distribución, sanidad, hostelería, por citar algunos relevantes. Y trabajamos en portafolios y ofertas específicas. Y queremos profundizar más.

– **FM.** Este enfoque nos abre caminos. Ahora mismo estamos trabajando en una oferta específica de ciberseguridad para el sector del turismo. Es potente y extenso, y ya se están viendo muchos incidentes de ciberseguridad ligados a este sector.

– **Una última cuestión: ¿cómo van a captar y retener a gente con talento en la cantidad necesaria?**

– **AM-G y FM.** Nuestro proyecto, enraizado en España y lanzado al mundo, afecta a todas las especialidades, capacidades y disciplinas asociadas con la ciberseguridad. Creemos que tiene atractivo para el mejor talento joven de cualquier género que sale de las universidades. ■

CIBERATAQUES 2024

La ciberdelincuencia se afila los dientes

SUMARIO

- Unión Europea
- Ucrania
- Actores internacionales relevantes
- Naciones Unidas
- Autoridades públicas competentes y Departamentos de la AGE
- Fiscalía General del Estado
- Fuerzas y Cuerpos de Seguridad del Estado
- Policías autonómicas
- Entidades autonómicas y locales
- Asociaciones y analistas
- Asociaciones de mujeres
- Aseguradoras y mediadores
- Centros y Laboratorios de Investigación y Evaluación
- Industria y servicios
- IAs
- Congresos
- Hackers
- Bug bounty
- El canto de la Sibila en la ciberseguridad de 2024, por JORGE DÁVILA





LA CIBERDELINCUENCIA

Cual arúspices, es momento de escrudiñar qué puede sobrevenir a la sociedad digital de las incontenibles incursiones de la ciberdelincuencia –ya la tercera economía del mundo–, en su objetivo de seguir desplumándola con artimañas, más o menos sofisticadas, más o menos pícaras, más o menos severas, pero en última instancia jugosamente rentables.

¿Es posible escrutar la bola de cristal de este 2024? ¿Todo son brumas o sí se pueden vislumbrar ya algunos vaticinios con fundamento? ¿Sobrevienen sorpresas o solo persistirán las usuales? La bipolaridad de la IA ya asoma la patita y el crimen cibernético saliva por su pingüe alianza con su nueva y flamante arma ciberdelincuencial.

De cara a atisbar qué amenazas y ciberataques harán padecer a buen seguro en este año que



SE AFILA LOS DIENTES

arranca a quienes conforman este planeta sustentado en lo ciber, Revista SIC, como suele, ha llevado a cabo una consulta de alcance sin precedentes –la más amplia y representativa hecha hasta la fecha– a más de 230 actores de referencia internacionales y supranacionales y de la industria y los servicios para pulsar sus intuiciones en este asunto tan crucial para el devenir confiable. Como no podía ser de otra manera, a estos expertos también se han sumado los pronósticos de algunas IAs en el candelero.

En las siguientes páginas del especial los respondedores se retratan, a través de sus respuestas, comentarios y enfoques, desvelándose sus preocupaciones y predicciones en lo que nos sobreviene. Es hora de su ingesta y valoración, y por supuesto, de estar alerta y no bajar la guardia.

 “Los cibercriminales se han vuelto extremadamente sofisticados y más organizados en sus operaciones, siendo habitual el movimiento de activos y despliegue de infraestructura en varias partes del mundo. El *malware*, como los *infostealers*, y las *botnets* seguirán siendo eficaces para el robo de credenciales, así como el auge de las comunidades o foros ilegales de servicios y activos cibercriminales”.

 “Se comenzarán a ver debilidades en ciertas pruebas de autenticación biométricas, en las que se ha venido confiando hasta ahora, lo que impulsará una nueva generación de factores de autenticación”.

 “Poco se habla de seguridad a nivel de infraestructura. En este contexto, ataques como ‘Route Hijacking’, ‘IP Address Spoofing’, ‘DNS Spoofing’ o ‘DDoS’, entre otros, afectan cada día a la seguridad de las redes”.

 “La vulnerabilidad latente en algoritmos criptográficos obsoletos podría ser explotada para comprometer comunicaciones y transacciones financieras, especialmente en organizaciones que no siguen el paradigma de agilidad criptográfica”.

 “Los ciberataques a los procesos electorales que se desarrollarán en este 2024 (Estados Unidos, India, Taiwán, etc) mediante denegación de servicio u otros y con el objetivo de debilitar la confianza de la población respecto a fiabilidad de dichos procesos”.

 “En el ámbito de la seguridad *cloud* enfrentará desafíos significativos debido a la complejidad de los entornos de nube híbridos y multiplataforma”.

 “Aumentarán las estafas relacionadas con VPN, los sistemas de pago directo y un incremento de los paquetes de código abierto con puertas traseras”.

 “Los de mayor impacto tratarán de afectar a la disponibilidad mediante ataques de DDoS a través de *botnets* empleando código dañino orientado a IoT”.

 “La mayor amenaza somos nosotros. Personal sin la experiencia adecuada ha sido incorporado en la industria y no recibe la formación continua necesaria. La industria aún exhibe inmadurez. Esto conduce a una cultura viciada definida por un alto grado de imitación y tendencia a acumular méritos aparentes”.

 “Los vehículos conectados que requieren de actualizaciones de software ‘Over The Air’ –OTA/SOTA/FOTA– están expuestos a riesgos que afectan, sobre todo, a la integridad física de los pasajeros y los peatones”.

 “Un ataque realmente crítico a esta sociedad protodigital sería la corrupción intencionada y controlada (por el atacante) de las bases de datos sobre las que se desarrollan las actividades de la sociedad analógica en la que nosotros existimos”.

 “Las tácticas actuales de ciberseguridad se apoyan en tecnologías avanzadas como SIEM, SOAR, IPS, EDR y NGFW. Estas soluciones implementan Indicadores de Compromiso (IoC) y Playbooks que, paradójicamente, podrían transformarse en amenazas serias en 2024”.

 “Los ataques más complejos técnicamente vendrán protagonizados por actores APT. Los grupos de ciberespionaje continuarán explotando vulnerabilidades *0-days* como vector de acceso que, en muchos casos, se centran en el compromiso de *appliances* de red propietarios”.

 “Podría llegar un cisne negro real utilizando los últimos avances de la Inteligencia Artificial, pudiendo ser un caso único, tipo el incidente de IFX Networks, o como un ataque de efectos masivos y globales en el mundo, como WannaCry”.

 “Los ámbitos ‘Phygital’, habilitados por tecnologías como el 5G, VR, AR, AI, IOT..., abre un escenario de nuevas ciberamenazas de alta complejidad en entornos multidimensionales. Retos para una NG-CTI buscando una combinación armoniosa entre los dos mundos”.

 “El IoT seguirá siendo vulnerable y activamente explotado, se realizará *spoofing* sobre los sistemas GPS y 5G con altos impactos en puntos calientes del planeta”.

 “Los atacantes contratan servicios legítimos de la Nube a nombre de identidades reales que han robado o que suplantan. Estos servicios son inicialmente indistinguibles de un nuevo usuario legítimo de la Nube, y sólo se pueden cualificar correctamente iniciar actividades hostiles”.

 “Los defectos de diseño de OS facilitarán más despliegues de controladores vulnerables BYOVD. MaaS sigue en aumento. Los *Pods* de Kubernetes con privilegios altos agravarán la seguridad de contenedor”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024

UNIÓN EUROPEA



DG CONNECT, COMISIÓN EUROPEA

Lorena Boix Alonso

Directora para la Sociedad Digital, la Confianza y la Ciberseguridad

“Veo tres grandes tendencias a tener en cuenta en 2024:

Primera, será el año en el que veremos la centralidad de la ciberseguridad para defender nuestros valores democráticos.

Más de 400 millones de europeos, así como la mitad de la población mundial, votarán en elecciones, y habrá intentos de actores estatales hostiles de socavar las democracias a través de ciberataques, desinformación y manipulación. Los mecanismos de cooperación y gestión de crisis de Europa estarán listos para enfrentar este desafío. Más específicamente, la Unión Europea y las autoridades cibernéticas y electorales de los Estados miembros llevaron a cabo un ejercicio conjunto en noviembre de 2023, y están actualizando sus directrices sobre cómo salvaguardar las elecciones, a tiempo para las elecciones al Parlamento Europeo en mayo.

Segunda, las tecnologías emergentes pasarán al centro del escenario tanto en defensa cibernética como en ofensiva cibernética. La UE está construyendo un escudo cibernético y 2024 será el año en el que, por primera vez, habrá dos –y pronto esperamos tres– redes regionales de SOCs habilitados para IA para detectar mejor las amenazas de ataque. España está a la vanguardia de esta iniciativa. Pero la IA y los LLM también pueden aumentar las campañas de *phishing* y otro contenido engañoso. Por lo tanto, NIS2 y CRA ya incluyen reglas sobre servicios y productos que utilizan IA, pero también esperamos una adopción rápida de la Ley de IA de la UE, que proporcionará salvaguardias para productos riesgosos antes de que se pongan en el mercado. Mientras tanto, debemos acelerar nuestra preparación para un futuro cuántico: implementando un pilar clave de la estrategia de ciberseguridad de la UE, en 2024 la UE trabajará para garantizar una transición coordinada a la criptografía post cuántica resistente a la computación cuántica, priorizando los sistemas más críticos.

Tercera: finalmente, el *ransomware* seguirá siendo la mayor amenaza para las empresas y los servicios esenciales. Según las tendencias actuales, para 2025 esta forma de delincuencia tendrá un coste mundial de 10 billones de dólares al año.

El nuevo marco regulatorio único de la UE, especialmente la Directiva NIS 2 y la Ley de Resiliencia Cibernética (CRA), ayudará a asegurar la infraestructura crítica y los productos conectados. También será esencial seguir el dinero, con Europol y los organismos nacionales de aplicación de la ley buscando aprovechar los éxitos recientes en la desarticulación de bandas de cibercriminales”.



PARLAMENTO EUROPEO

Dita Charanzová

Vicepresidenta

–encargada de Ciberseguridad–

“La ciberseguridad es más importante que nunca. Como vicepresidenta del Parlamento y como responsable de ciberprotección, he sido testigo de que las ciberamenazas han ido creciendo en los últimos años. Incidentes causados por *ransomware*, contra instituciones europeas, contra oleoductos... Algunos se han hecho públicos, pero muchos otros no verán la luz en las noticias.

Estas amenazas no hacen más que aumentar: se detectan 230.000 nuevas infecciones de *malware* cada día. Y los cibercriminales no sólo actúan por motivos económicos sino también para socavar la democracia: no me cabe duda de que las próximas elecciones europeas serán un blanco.

El Foro Económico Mundial sitúa a la cibercriminalidad entre los principales riesgos a corto y largo plazo. La digitalización ha creado nuevas oportunidades para ciberataques y sectores claves dependen de sistemas de redes en formación, cada vez más interconectados. Las nuevas tecnologías también están ofreciendo nuevas oportunidades a estafadores de todo tipo. Y la IA es una amenaza emergente a nuestra seguridad. También, la guerra de Ucrania ha supuesto ciberataques masivos. Por ello, nos enfrentamos a estos retos como Unión Europea y debemos reaccionar para corresponder a esto, con iniciativas como un marco normativo reforzado o la Ley de Ciberresiliencia. Vamos a seguir trabajando hacia un marco normativo que garantice que los productos conectados y servicios asociados y las cadenas de suministros son seguros por diseño y resistentes a incidentes cibernéticos. Pero, aunque la UE está actuando, lo cierto es que los gobiernos no serán capaces por sí mismos de proteger por completo a instituciones, empresas y ciudadanos. Por eso hay que desarrollar asociaciones público-privadas, trabajar con verdaderos expertos de las empresas, que sean capaces de parar las ciberamenazas antes de su impacto en el sector público y encontrar el origen de esas amenazas. Además, es importante que el sector privado haga de ‘buen samaritano’ y proteja a los usuarios cuando lo pidan. La apertura del GSEC de Google, en Málaga, es una señal de que las tecnológicas mundiales entienden que Europa es un lugar donde invertir en talento y donde los expertos en ciberseguridad son valorados, aunque necesitamos más profesionales. Somos conscientes de ello en Europa y haremos todo lo que esté en nuestras manos para conseguirlo. La ciberseguridad es un reto importante para Europa: sin ella la UE no puede existir y este centro nos ayudará a garantizar que ciudadanos y empresas estén protegidos”.

*Declaraciones en la apertura del GSEC de Google en Málaga



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



COMISIÓN EUROPEA

Thierry Breton

Comisario Europeo de Mercado Interior

"A medida que Europa se ha convertido en un actor político, económico y de seguridad global, también es un objetivo cada vez mayor para los ciberataques destinados a desestabilizar nuestros sistemas y alterar nuestras infraestructuras críticas. Europa se está equipando con cortafuegos en el ciberespacio para proteger a sus ciudadanos, sus empresas y sus intereses estratégicos.

Por eso, en los últimos cuatro años, hemos revisado por completo el marco de ciberseguridad en Europa. En un mercado único interconectado, somos tan fuertes como el eslabón más débil, ya sea un Estado miembro vulnerable, un producto inseguro o una coordinación ineficaz.

Aumentamos la ciberresiliencia de nuestros principales operadores económicos críticos y, ahora, de todos los productos comercializados en el mercado único, imponiendo características 'cibernéticamente por diseño'.

Estamos construyendo el embrión de un escudo cibernético europeo (una red de centros de operaciones de seguridad, impulsados por IA, para apoyar la detección y la concienciación sobre las amenazas a la ciberseguridad) y creando la primera reserva cibernética europea de proveedores privados de ciberseguridad de confianza que apoyan a los Estados miembros bajo ataque. El mensaje es claro: Europa está unida contra las ciberamenazas. También hemos impuesto estrictos requisitos de seguridad en las redes 5G para excluir a los proveedores de alto riesgo. (...) Varios Estados miembros ya han decidido excluir completamente a Huawei y ZTE de sus redes 5G, de acuerdo con la caja de herramientas europea.

Hago un llamamiento a todos los Estados miembros para que tomen las decisiones necesarias para garantizar la resiliencia de Europa y evitar dependencias en una infraestructura crítica".

* Discurso de apertura en la Cumbre Digital de Tallin. 5 de septiembre 2023



BANCO CENTRAL EUROPEO

Anneli Tuominen

Miembro del Consejo de Supervisión

"El número de ciberataques es mayor que antes de la pandemia. Los ataques distribuidos de denegación de servicio, en los que los perpetradores interrumpen los servicios bancarios inundando y obstruyendo los servidores bancarios con solicitudes falsas, son los que más han aumentado. También, observamos más ataques a proveedores ex-

ternos y más ataques de *ransomware*, en los que a un objetivo se le niega el acceso a los datos en sus propios dispositivos a menos que se pague un rescate. Pero los bancos de la zona del euro han demostrado hasta ahora ser resistentes. Los ataques no fueron tan graves como para desestabilizar a los bancos de forma individual o al sistema bancario. Sin embargo, tenemos que estar preparados: un ataque exitoso podría ocurrir en cualquier momento".



EUROPOL

Catherine De Bolle

Directora Ejecutiva

"En nuestro mundo globalizado, el comercio, la tecnología y el transporte nos acercan y crean oportunidades económicas y prosperidad. Sin embargo, hay otra cara de la moneda: nuestro mundo intercon-

nectado es mal utilizado y objeto de abuso por actores criminales involucrados en delitos económicos y financieros. De hecho, el crimen organizado ha construido un sistema económico y financiero criminal global paralelo en torno al lavado de dinero, las transferencias financieras ilícitas y la corrupción. Los delincuentes aprovechan estas tres prácticas para ocultar, moverse y, en última instancia, beneficiarse de sus ganancias criminales. La capacidad de lavar ganancias ilícitas a escala industrial, moverlas a través de una red de intermediarios financieros criminales y corromper a los actores relevantes se ha vuelto indispensable para el crimen organizado moderno.

Los actores criminales involucrados en delitos económicos y financieros aprovechan las vulnerabilidades de los sistemas económicos y sociales para generar miles de millones en ganancias ilícitas. Mientras tanto, con la tecnología moderna a su disposición, los delincuentes han innovado y diversificado sus *modus operandi* para evadir la detección.

Gracias a los crecientes esfuerzos realizados por los legisladores nacionales y de la UE, las investigaciones sobre delitos financieros y económicos están aumentando en número y teniendo más éxito. Aun así, en la actualidad, la cantidad de activos que las fuerzas del orden logran arrebatar de las manos de las redes criminales sigue estando por debajo del 2% de los ingresos anuales estimados del crimen organizado, una gota en el océano de los inmensos ingresos ilícitos (y no gravados) obtenidos por redes criminales. Esto no es algo que una fuerza policial o un país pueda cambiar por sí solo; debemos fortalecer la cooperación y las asociaciones existentes y desarrollar nuevos enfoques. Las asociaciones público-privadas en particular desempeñarán un papel fundamental, ya que juntos podemos evitar que las ganancias delictivas entren en el sistema financiero legal".

* *The Other side of the coin. An Analysis of Financial and Economic Crime*



UNIÓN EUROPEA



ECCC – CENTRO EUROPEO DE COMPETENCIA EN CIBERSEGURIDAD
Miguel González Sancho
Director interino

“Las grandes amenazas actuales probablemente se amplificarán: ataques mediante inteligencia artificial e ingeniería social, a través de la cadena de valor y de dispositivos móviles. Esto se produce en

un contexto de dependencia digital generalizada donde persisten grandes vulnerabilidades como una situación geopolítica volátil sin reglas de ciberseguridad, y unas arquitecturas informáticas plagadas de vulnerabilidades de software, que continuarán favoreciendo un sinfín de manipulaciones más o menos ilegales en el ámbito económico, político y social.

Ante este panorama, la Unión Europea ha desarrollado recientemente una ingente labor en materia de ciberseguridad, con medidas de coordinación, financiación y legislativas, cuyo impacto se hará sentir con más fuerza en este 2024”.



ENISA
Vicente González Pedrós
Research and Innovation Team

“El informe de ENISA de amenazas de 2023 (*2023 ENISA Threat Landscape report*) identifica los ataques de Denegación de Servicio Distribuido (DDoS) y el *ransomware* como las principales amenazas, seguidos de la ingeniería social, las amenazas relacionadas con datos, la manipulación de la información, la cadena de suministro y el *malware*. Los ataques de Denegación

de Servicio (DoS) han sido una preocupación de seguridad constante para las organizaciones. En los últimos años, los ataques DoS se han vuelto más fáciles, más baratos y más agresivos que nunca. Por otra parte, el surgimiento de nuevos conflictos armados en todo el mundo actuó como combustible para nuevas oleadas de ataques DoS en los que grupos de amenazas recién formados eligen varios objetivos. ENISA ha publicado un informe (*DoS Threat Landscape*) que tiene como objetivo aportar nuevos conocimientos sobre el panorama de amenazas DoS para apoyar a las organizaciones”.

de Servicio (DoS) han sido una preocupación de seguridad constante para las organizaciones. En los últimos años, los ataques DoS se han vuelto más fáciles, más baratos y más agresivos que nunca. Por otra parte, el surgimiento de nuevos conflictos armados en todo el mundo actuó como combustible para nuevas oleadas de ataques DoS en los que grupos de amenazas recién formados eligen varios objetivos. ENISA ha publicado un informe (*DoS Threat Landscape*) que tiene como objetivo aportar nuevos conocimientos sobre el panorama de amenazas DoS para apoyar a las organizaciones”.



ESA SECURITY AUTHORITY
Massimo Mercatti
Head of ESA Security Office
Director General's Service

“Los desafíos cibernéticos probablemente permanecerán al menos en el nivel de años anteriores. Se espera que el aumento continuo de los desafíos se vincule con el empeoramiento de los factores geopolíticos y la introducción de tecnologías disruptivas.

Se espera que los ataques patrocinados por estados aumenten. El espacio es tradicionalmente un sector altamente expuesto con respecto a la resistencia cibernética y continuará siendo una opción atractiva para la explotación digital.

Se espera una introducción gradual de ciberamenazas impulsadas por la Inteligencia Artificial. De hecho, el aumento de la tecnología impulsada por la IA introducida en el flujo de trabajo corporativo aumentará los desafíos de seguridad en términos de expandir rápidamente la huella de explotación cibernética. Los ataques cibernéticos dirigidos por vulnerabilidades identificados con IA, diseñados o ayudados por IA también pueden comenzar a ser vistos”.

sino también a las empresas privadas que pueden ser contratadas por compañías o instituciones públicas que posean o administren dicha infraestructura.

Los vectores de compromiso inicial más comunes incluyen:

- Vulnerabilidades conocidas (PHP, MS Exchange, FortiGate, Zimbra).
- Cuentas comprometidas (->VPN -> LAN)
- Spearphishing.
- Autoinfección (a través de sistemas operativos, paquetes de software descargados de rastreadores).

Tampoco cesan nunca los intentos de encontrar personas que puedan tener acceso a determinadas instalaciones y explotar-

las para ataques posteriores. Por lo tanto, instamos a todos los ucranianos a que tengan cuidado y sigan las reglas básicas de higiene cibernética, y a todas las instituciones u organizaciones a que sigan trabajando para mejorar sus sistemas de seguridad y recuperación.

La reciente actividad en los canales rusos de Telegram sugiere que el agresor está involucrando activamente a los jóvenes, proporcionándoles materiales de capacitación para fomentar una nueva generación de hackers motivados que se convertirán en futuros actores del cibercrimen.

Nosotros, a su vez, los estamos estudiando y diseñando nuestras



ACTORES INTERNACIONALES RELEVANTES



ANC-AD – AGENCIA NACIONAL DE CIBERSEGURIDAD DE ANDORRA
Jordi Ubach
Líder de Proyecto

“Al mirar hacia el horizonte digital de 2024 nos enfrentamos a una realidad ineludible: el cibercrimen no tiene fronteras, su coste es más que solo dinero, amenaza los cimientos mismos de nuestras empresas y el tejido de la sociedad. Dado que se prevé que las pérdidas globales alcancen los 9,5 billones de dólares para este 2024, la necesidad de fortalecer nuestras defensas cibernéticas está fuera de debate. En este contexto, las dinámicas de liderazgo como la relación entre el CISO y el CIO deben fortalecerse a través de políticas consistentes y colaborativas. La realidad es que la ciberseguridad no es sólo una inversión, es una garantía importante de nuestra continuidad y prosperidad en el mundo digital”.



ANCA – RED AFRICANA DE AUTORIDADES DE CIBERSEGURIDAD
Dr. Albert Antwi-Boasiako
Presidente

“Los ataques a la infraestructura de información crítica (CII) siguen siendo una preocupación debido a la falta de regulaciones y la capacidad limitada para detectar, responder y gestionar estos ataques. Se espera que los principales vectores de ataque sean el *ransomware*, el *phishing* (incluido el compromiso del correo electrónico empresarial), las filtraciones de datos y la denegación de servicio distribuido (DDoS).

También se espera que las estafas en línea dirigidas a ciudadanos con estilos de vida cada vez más digitales y, sin embargo, prácticas deficientes de higiene cibernética, como estafas en compras,

estafas laborales y suplantación de identidad, sean un problema importante este año.

Además, también se considera que el mayor uso de herramientas habilitadas con Inteligencia Artificial (IA) impulse manifestaciones más sofisticadas y de mayor impacto de las amenazas descritas anteriormente, por ejemplo, mediante el despliegue de *bots* en plataformas de redes sociales para difundir noticias falsas, la generación de *deep fakes*, volúmenes de tráfico malicioso para DDoS y más difícil de detectar correos electrónicos de *phishing*”.



ANSSI – AGENCIA NACIONAL FRANCESA PARA LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
Vincent Strubel
Director General

“Estas Olimpiadas son la ilustración de un desafío más amplio: la industrialización del cibercrimen que, en los últimos tres años, afecta a todos de manera muy visible, a nuestros hospitales y a nuestras comunidades. Nos estamos preparando para gestionar crisis importantes. La formación marca la diferencia”.



CCB – CENTRO DE CIBERSEGURIDAD DE BÉLGICA
Miguel De Bruycker
Director General

“Percibimos una evolución de las ciberamenazas y los ataques en 2024 en tres dominios: el crecimiento de los ataques de filtración de datos y *ransomware*, el aumento de los ataques a los sistemas IoT y OT y los ataques de espionaje impulsados por Estados.

estrategias de defensa para ayudar a los operadores a mejorar el nivel de seguridad de los objetivos potenciales. Todavía enfrentamos muchos desafíos y problemas, con un enfoque especial en la protección de infraestructura crítica, ya que el SSSCIP está a cargo de coordinar la protección de los CIF en su conjunto. Somos muy conscientes de toda la gama de posibles amenazas, incluidas las del dominio cibernético.

La guerra en Ucrania ha demostrado que la agresión basada en el ciberespacio es un componente esencial de la doctrina militar rusa. Esta amenaza sólo se expandirá en el futuro. Tanto para Ucrania como para sus socios”.

UCRANIA



SSSCIP, SERVICIO ESTATAL DE COMUNICACIONES ESPECIALES Y PROTECCIÓN DE LA INFORMACIÓN DE UCRANIA
Oleksandr Potii
General de Brigada
Subdirector

“No hay duda de que los hackers rusos no dejarán de intentar atacar a Ucrania en el ciberespacio. No sólo se atacará la infraestructura crítica,



ACTORES INTERNACIONALES RELEVANTES

Los ataques de fuga de datos y *ransomware* seguirán causando una cantidad récord de daños y pérdidas. Gracias a las nuevas tecnologías como la IA, la sofisticación y el nivel de ingeniería social podrían aumentar significativamente. Debido a los deficientes estándares de seguridad de los sistemas IoT y OT, la proporción de ataques OT podría crecer considerablemente. Finalmente, las tensiones geopolíticas globales aumentarán la importancia del espionaje y de los esfuerzos para detectarlo, lo que se traducirá en un aumento del número de casos denunciados”.



CCDCOE – CENTRO DE EXCELENCIA DE CIBERDEFENSA COOPERATIVA DE LA OTAN

Sergio Pastor
Teniente Coronel
Operations Branch Head

“Es previsible que sean los siguientes:

1. Los ciberataques a infraestructuras críticas (transporte, ISP y principalmente energía), porque un ataque exitoso a estos sistemas puede tener consecuencias devastadoras.
2. Los ciberataques a los procesos electorales que se desarrollarán en este 2024 (Estados Unidos, India, Taiwán, etc) mediante denegación de servicio u otros y con el objetivo de debilitar la confianza de la población respecto a la fiabilidad de dichos procesos.
3. No podemos olvidarnos del IoT y de los dispositivos móviles, ya que la gran cantidad de datos que están almacenados en ellos no son únicamente una amenaza para la privacidad de las personas (datos clasificados del puesto de trabajo, metadatos de las fotos, etc.)
4. Por último, aunque menos complejo, los ciberataques a dispositivos IP, ubicados en lugares públicos, se convertirán en una parte importante de los conflictos (por ejemplo, hackear las cámaras web de las ciudades para obtener información de inteligencia o para “corregir” los ataques de misiles o drones contra objetivos). De hecho, NATO CCDCOE, siguiendo la máxima “*train as you fight, fight as you train*” pone en práctica, en un escenario totalmente ficticio, muchos de estos ciberataques en su ejercicio anual ‘Crossed Swords’.



FIRST

Olivier Caleff
Board Member

“Aunque las técnicas de ataque están evolucionando, la gran mayoría de ellas explotan vulnerabilidades conocidas (CVE), dirigidas a sistemas sin parches, a menudo engañando a los usuarios para que ejecuten *malware*. Abordar el problema de las vulnerabilidades es una prioridad absoluta, pero 2023 fue un año récord

con casi 29.000 nuevos CVE (es decir, alrededor de 80 por día) [1][2]. Las organizaciones primero deben priorizar las actividades de gestión de parches y pueden hacerlo aprovechando dos estándares que se actualizaron en 2023; el Sistema de puntuación de vulnerabilidad común (CVSS) [3] para evaluar la gravedad de la vulnerabilidad y el Sistema de puntuación de predicción de explotación (EPSS) [4] para estimar la probabilidad de que una vulnerabilidad de software sea explotada en ‘estado salvaje’. El conocimiento de la situación y la automatización también pueden resultar beneficiosos. Luego viene la IA.

Ya es hora de prepararse para los ciberataques basados en IA, que se han convertido en una realidad y representan una amenaza existencial para las organizaciones en manos de actores de amenazas. Los equipos de TI y ciberseguridad también pueden beneficiarse de la IA, comenzando con la automatización e incluyendo progresivamente el conocimiento en las plataformas para lograr una detección más temprana, una reacción más rápida y reducir el tiempo para gestionar los incidentes. Por último, pero no menos importante, comprender que los ataques (exitosos) son parte del juego, prepararse para la sostenibilidad y la resiliencia cibernética es de gran ayuda cuando la situación se vuelve mala. La anticipación aquí es clave”.



ITU – UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

Dr. Cosmas Luckyson Zavazava
Director, Oficina de Desarrollo de las Telecomunicaciones

“Los Estados miembros han informado de un aumento en la frecuencia y complejidad de los ciberataques. Mejorar la coordinación interna y el intercambio de información son cruciales para una respuesta eficaz a incidentes y desarrollar resiliencia. El Índice Global de Ciberseguridad 2020 muestra que el 54% de los países no tienen una Estrategia Nacional de Ciberseguridad y el 52% no se prepara periódicamente para responder a incidentes de ciberseguridad. Para colmar esta brecha, la ITU lleva a cabo periódicamente cibernsimulacros regionales y nacionales en los que participan equipos nacionales de respuesta a incidentes informáticos para dotar a los participantes de los últimos conocimientos y capacidades prácticas en materia de ciberseguridad. El énfasis en el desarrollo de capacidades es esencial para garantizar que los profesionales de la ciberseguridad estén bien preparados para enfrentar los desafíos futuros”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



NSA – AGENCIA DE SEGURIDAD NACIONAL DE EE.UU.

Paul Nakasone, General Director

“La República Popular China (RPC) se ha convertido en el desafío para los Estados Unidos, como competidor, con la intención y la capacidad de remodelar el sistema internacional para adaptarse a sus

propios diseños. La RPC es un adversario único en el alcance, escala y sofisticación de la amenaza. Y ha planteado y manifestado su deseo de convertirse en uno de los poderes gobernantes. Además, Rusia sigue siendo una amenaza grave y continúa amenazando la seguridad regional y la estabilidad global a través de su desprecio de las normas internacionales y su voluntad de utilizar sus armas contra civiles e infraestructuras críticas.

Fuimos testigos de un ejemplo revelador de esto durante la crisis de Rusia y la invasión ilegal de Ucrania. También ha desplegado operaciones de información destinadas a debilitar la democracia e instituciones alrededor del mundo. Necesitamos poder responder a las amenazas de la República Popular China, Rusia y otros adversarios globales hoy y en el futuro. Debemos mantenernos por delante de nuestros competidores globales que constantemente buscan remodelar la información global el medio ambiente y el orden mundial tal como lo conocemos”.

* *Cybersecurity Year in Review report de la NSA*



OEA – ORGANIZACIÓN DE ESTADOS AMERICANOS

Alison August Treppel
Executive Secretary, Inter-American Committee against Terrorism (CICTE)

“Es bien sabido que cada nueva tecnología trae consigo nuevos riesgos. Así, vemos el uso malicioso de la Inteligencia Artificial como la amenaza más compleja.

Después de la ola de *ransomware* que azotó nuestra región en 2023, creemos que los actores maliciosos emplearán IA para poner en práctica ataques aún más frecuentes y complejos contra infraestructura crítica para obtener ganancias financieras. En términos de alto impacto y reconociendo la gran cantidad de países a nivel mundial que participarán en procesos democráticos en 2024, creemos que los malos actores buscarán utilizar tecnologías emergentes, incluida la inteligencia artificial, para llevar a cabo campañas de *phishing* y desinformación a gran escala. En la OEA estamos dispuestos a trabajar con nuestros socios en todo el mundo para ayudar a los países a enfrentar este problema”.



SISTEMA NACIONAL DE CIBERSEGURIDAD DE CHILE

Daniel Álvarez Valenzuela
Coordinador Nacional de Ciberseguridad

“En América Latina y el Caribe experimentamos un incremento tanto en la cantidad como en la sofisticación de los ciberataques, destacándose varios incidentes que afectaron a organismos públicos

como empresas, incluyendo cadenas de suministros claves. El panorama para el año 2024 no parece ser diferente. América Latina se está convirtiendo en un objetivo atractivo para cibertacantes, quienes están desplegando incursiones avanzadas con *ransomware* novedosos o algunas APTs. Por ello, es interesante cómo varios países están trabajando en fortalecer sus capacidades de seguridad digital, tanto en la dimensión técnica como política. En el caso de Chile, el Congreso Nacional despachó, de manera unánime, una ley marco sobre ciberprotección, donde se crea la Agencia Nacional de Ciberseguridad, siendo el primer país de América Latina y el Caribe en contar con este tipo de capacidades institucionales”.



WEF – FORO ECONÓMICO MUNDIAL

Filipe Beato
Lead, Cyber Resilience, Centre for Cybersecurity

“Los riesgos de los ecosistemas están aumentando según la ‘Perspectiva de Ciberseguridad Global 2024’ del Foro Económico Mundial

recientemente presentada, donde el 41% de todas las organizaciones que experimentaron un incidente cibernético importante en el último año afirmaron que fue causado por un tercero. La mayor conectividad en las cadenas de suministro, la creciente desigualdad cibernética, los rápidos avances en las tecnologías transformadoras y la falta de talento disponible en ciberseguridad aumentan la complejidad de la gestión de los riesgos cibernéticos. Necesitamos desbloquear acciones colaborativas público-privadas a escala para adelantarnos a estos riesgos en evolución. El Centro para la Ciberseguridad lidera múltiples iniciativas y reúne a los actores del ecosistema para fortalecer la ciberresiliencia colaborativa en las industrias y cerrar la brecha cibernética”.



NACIONES UNIDAS



ONU – NACIONES UNIDAS

Dra. Camino Kavanagh

Investigadora Visitante Senior, King's College London / Consultora Naciones Unidas y otras entidades internacionales

“No hay descanso a nivel internacional respecto al tema ciber. Como el año pasado, la ciberdelincuencia figura en la agenda de enero, con la última ronda de negociaciones del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las TIC con Fines Delictivos. El borrador de la Convención que hay sobre la mesa es, como poco, controvertido. Esto era de esperar, en particular, dada la polémica que se había generado por la mera idea de concebir un tratado global, antes de que las negociaciones comenzaran en 2019. No obstante, el borrador actual, distribuido en diciembre de 2023, será la base de las negociaciones en la sesión final del proceso, programada para finales de enero de este 2024. El documento ha sido criticado por varias razones, entre ellas, por su título y alcance. Además, tanto actores públicos como privados están preocupados por que el tratado criminalice la expresión y el disenso, expanda los poderes de vigilancia de los gobiernos y facilite la represión a través de las fronteras. No está claro cómo se resolverán estas cuestiones, sobre todo, en el contexto actual. Por ello, es un proceso para seguir en los próximos meses, entre otros aspectos, porque su resultado nos afectará a todos.

Más allá del cibercrimen, las negociaciones dentro del Grupo de Trabajo Abierto de la ONU (UN OEWG) sobre TIC y seguridad internacional seguirán avanzando en 2024. Como el año pasado, hay dos sesiones formales programadas: una en marzo y otra en julio. Se puede esperar ciertos avances en la identificación de nuevas amenazas, incluyendo problemas relacionados con la ciberseguridad derivados de la IA generativa. También, continuarán los intercambios de opiniones sobre la implementación de las normas existentes. Sin embargo, la no adhesión a las normas de restricción acordadas en 2015 sigue siendo un problema, como lo demuestran las operaciones cibernéticas ofensivas que han sido dirigidas a infraestructuras críticas en numerosos países. Que los cables submarinos, esenciales para el funcionamiento del sistema financiero global y muchas otras infraestructuras esenciales, ahora sean percibidos como posibles objetivos de acciones ofensivas, no disipa las preocupaciones. Varios gobiernos, principalmente occidentales, continúan impulsando la cuestión de la responsabilidad por tales acciones en la ONU, sin mucho éxito. La cuestión del diálogo institucional regular sobre las TIC y seguridad internacional seguirá siendo un tema espinoso, a pesar de que la resolución sobre el Programa de Acción recibió un apoyo significativo en la sesión del Primer Comité de la Asamblea General, en octubre del 2023. Como sugieren los patrones de votación del año pasado, las resoluciones paralelas pueden recibir igualmente mucho apoyo.”

AUTORIDADES PUBLICAS COMPETENTES Y DEPARTAMENTOS DE LA AGE



CCN – CENTRO CRIPTOLÓGICO NACIONAL

Carlos Abad

Jefe del Área de Sistemas de Alerta y Respuesta a Incidentes

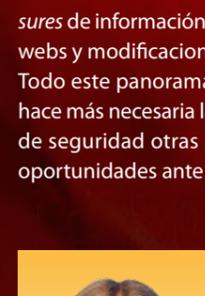
“Los ataques más complejos técnicamente vendrán protagonizados por actores APT. En este sentido, los grupos de ciberespionaje continuarán explotando vulnerabilidades 0-days como vector de acceso que, en muchos casos, se centran en el compromiso de *appliances* de red propietarios, donde las posibilidades de detección y forense son muy reducidas. Asimismo, los ataques contra dispositivos móviles serán cada vez más avanzados y extendidos, pudiendo incluir *smart devices* y *wearables* entre sus objetivos, por sus crecientes capacidades y potencial información sensible que brindan. Además, los grupos APT continuarán perfeccionando su OPSEC con el empleo de medios desvinculados encadenados para la realización de ataques, a través del compromiso a gran escala de dispositivos conectados a Internet (IoT, routers domésticos, etc) y el empleo de VPN comerciales que dificultan la trazabilidad del ataque y, por tanto, su atribución.

Por otra parte, en líneas generales, y especialmente en grupos de cibercrimen, se mantendrá la tendencia actual de acceso inicial a la red mediante la compra de credenciales en el mercado negro, dada la limitada implantación del MFA en muchos sistemas. Este mundo va a continuar profesionalizándose con nuevos mercados de compra-venta de credenciales en foros, grupos de Telegram y webs más exclusivas. En este sentido, el desarrollo de *stealers* seguirá creciendo para alimentar a dichos mercados. A esto cabe añadir que las campañas de *phishing* y *smishing* aumentarán en escala, calidad y sofisticación por las posibilidades que ofrece la IA generativa (genAI) en general, y los algoritmos de *Deep Learning* para procesamiento del lenguaje natural (NLP) basados en modelos extendidos (Large Language Models) en particular.

Tras la intrusión, para el movimiento lateral por la red se seguirá abusando de herramientas legítimas, con un uso de *malware* cada vez más reducido para minimizar las oportunidades de detección. Esto unido al hecho de la hiperconectividad existente de nuestras redes, con excesiva confianza entre ellas muchas veces o potencialmente debilitadas por una cadena de proveedores compleja de controlar, dificultará a los responsables de seguridad su labor.

Por último, se incrementará la actividad ofensiva vinculada a fines ideológicos (hacktivismo) derivada de los actuales conflictos internacionales en forma de ataques DDoS a entidades gubernamentales y empresas –aunque de escaso impacto–, y ataques a la confidencialidad de la información (*public disclosure*

de información sensible) o a su integridad (*defacements* de webs y modificaciones de cuentas en redes sociales). Todo este panorama, y como ya se pronosticó el pasado año, hace más necesaria la incorporación a las tradicionales medidas de seguridad otras de Ciberdefensa Activa que nos den más oportunidades ante los atacantes.”



DSN – DEPARTAMENTO DE SEGURIDAD NACIONAL

Marina Rodríguez Díaz

Jefa de la Unidad de Ciberseguridad y lucha contra la desinformación

“2023 se caracterizó por una incesante sucesión de ciberataques cuyo número, frecuencia, sofisticación, capacidad expansiva y severidad en el impacto se prevé creciente en este 2024. Esta tendencia preocupa al DSN, especialmente cuando van dirigidos contra la Administración Pública, muy digitalizada y conectada, en la que radican datos críticos-país, tanto de ciudadanos como de empresas.

La guerra de agresión de Rusia sobre Ucrania marcó 2023, otro año más, en términos de ciberataques, expandiendo sus objetivos a Israel por el conflicto de Hamas, en el formato habitual de DDoS de páginas web y suplantación de estas, con fines propagandísticos y consiguiente daño reputacional.

Respecto a los retos ciber para 2024, desde el punto de vista de seguridad nacional, se destaca:

– La ciberprotección de información y datos sensibles, públicos y privados, frente a APTs procedentes de actores hostiles clásicos como Rusia y significativamente China, cada vez más sofisticadas y efectivas y no atribuibles.

– Migración a los servicios en nube, como parte de un proceso de optimización, no exento de riesgos: ubicación del dato en términos de legislación aplicable, disponibilidad y dependencia tecnológica de actores extranjeros, en detrimento de las capacidades nacionales y europeas.

– La trasposición de la Directiva NIS2, a cargo del Ministerio del Interior, en colaboración con Defensa, Transformación Digital y Presidencia, cuyo plazo expira el próximo 17 de octubre de este 2024. Este proceso requiere, además de comunicación y coordinación entre los distintos actores ciber nacionales, avanzar y definir un nuevo sistema de gobernanza en ciberseguridad para nuestro país.

– La definición de un Esquema Nacional de redes y servicios 5G, en desarrollo del RD 7/22 de 29 de marzo. En términos de seguridad nacional resulta clave asegurar la protección estratégica del despliegue 5G en España, teniendo muy en cuenta la posible exposición a espionaje e injerencias extranjeras de equipos, productos y servicios.”



INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

Marcos Gómez

Subdirector INCIBE-CERT. CISO de INCIBE

“2023 se caracterizó por ciberamenazas y ciberincidentes que podemos considerar como viejos conocidos en el mundo digital, como el *phishing*, la detección de sistemas vulnerables, que deberían protegerse y actualizarse mejor, los *ransomware* que ponen en riesgo nuestra disponibilidad, pero, también, la fuga o robo de datos sensibles, daños reputacionales, y finalmente los ataques dirigidos. Además y derivados de los conflictos bélicos llevados a la Red, tenemos la incansable actividad de grupos organizados y polarizados, como Noname o Killnet, o amenazas en sí mismas como DDoS Project, BlackEnergy, NotPetya o Colonial Pipeline.

Un año en el que también tuvimos muchas novedades legislativas de relevancia, como la NIS2, la Cyberresilience Act, la Digital Services Act, etc., que son claramente el desafío para todos los Estados miembro, especialmente para países como España, con un enorme crecimiento en su transformación digital, o por su posición avanzada en ciberseguridad, en un muy meritorio cuarto puesto a nivel mundial y tercero en Europa en el ranking de la ITU, y que habrá que seguir manteniendo. Los mecanismos de detección de las diferentes entidades de referencia en ciberseguridad siguen aumentando, y como contrapartida, se detectan y previenen o mitigan con mayor efectividad las ciberamenazas y ciberataques, pero solo cabe seguir reforzando dichas iniciativas, servicios y capacidades, para afrontar los retos técnicos y legislativos. Con fronteras cada vez más grises y difíciles de delimitar, como los grupos cibercriminales y ciberterroristas, el hacktivismo, los intereses económicos, políticos, sociales e incluso estatales, este 2024 será aún más exigente, para cubrir las nuevas complejidades e incertidumbres. El año pasado nos hacíamos algunas preguntas en esta línea, como: ¿será el 2023 de nuevo un año marcado por este tipo de ciberataques? ¿veremos más hacktivismo relacionado con conflictos vigentes? Ya podemos confirmar que parte de esas cuestiones se cristalizaron en ataques e incidentes de impacto significativo en empresas y administraciones.

Por eso es tan importante que cualquier entidad y organización fortifique sus políticas, procedimientos, tecnologías y capacidades en seguridad, que siga formando a sus empleados y clientela, pero que no deje fuera de esta necesidad las otras relativas a los requisitos y obligaciones que se derivan de todas las normas y legislaciones que están apareciendo, y que cuenten siempre con la ayuda que el Estado les presta a través de servicios de referencia como el 017, e INCIBE-CERT, o incluso la importante labor que se está haciendo en la dinamización e impulso de la industria de ciberseguridad, la innovación y el emprendimiento o la formación y captación del talento. Todo ello, se ofrece como apoyo desde INCIBE, porque, todo ello, está muy interconectado.”



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024

AUTORIDADES PÚBLICAS COMPETENTES Y DEPARTAMENTOS DE LA AGE



MCCE – MANDO CONJUNTO DEL CIBERESPACIO

Javier Roca, Vicealmirante Comandante

“Todo indica que en 2024 el *hacktivismo* híbrido seguirá desempeñando un papel relevante, intensificando el ciberespionaje combinado con nuevas capacidades de *malware* destructivo. Respecto a la Inteligencia Artificial (IA) la proliferación de soluciones de *jailbreaking* para eliminar restricciones de uso y desarrollar contenido malicioso generará vectores de ataque potenciados, mientras que la consolidación del *deepfake as a service* ofrecerá capacidades avanzadas a actores menos experimentados. La celebración de importantes eventos como procesos electorales y los Juegos Olímpicos de París incrementará los ciberataques y las campañas desinformativas, planteando importantes desafíos de seguridad agravados por la vulnerabilidad de los sistemas de comunicación por satélite.”

La proliferación de soluciones de *jailbreaking* para eliminar restricciones de uso y desarrollar contenido malicioso generará vectores de ataque potenciados, mientras que la consolidación del *deepfake as a service* ofrecerá capacidades avanzadas a actores menos experimentados. La celebración de importantes eventos como procesos electorales y los Juegos Olímpicos de París incrementará los ciberataques y las campañas desinformativas, planteando importantes desafíos de seguridad agravados por la vulnerabilidad de los sistemas de comunicación por satélite.”



Mº PARA LA TRANSFORMACIÓN DIGITAL Y FUNCIÓN PÚBLICA

José Luis Bezares
Subdirector General de Ciberseguridad

“Es previsible que en el año 2024 sigamos siendo testigos de un aumento de la repercusión mediática de los ciberataques, debido al incremento en volumen de las amenazas y su impacto en la economía española. La mejora en las tácticas y las técnicas utilizadas en los ataques, especialmente debida al uso de la inteligencia artificial, les permitirán una mayor eficacia y sofisticación. Entre estos ataques destacarán los patrocinados por naciones-estado en el contexto de las crecientes tensiones geopolíticas. Para contrarrestar estas amenazas se observará también un refuerzo en la inversión de ciberseguridad de las organizaciones públicas y privadas, como el que ya se viene realizando a través de iniciativas públicas como el Kit Digital que ayuda a las pymes y autónomos en su digitalización.”



Mº DE ASUNTOS EXTERIORES

José Miguel Corvinos Lafuente
Embajador en Misión Especial para la Transformación Digital y Amenazas Híbridas

“El continuo deterioro de la seguridad internacional seguirá siendo el telón de fondo de los debates multilaterales sobre ciberseguridad. Además de la posible aprobación de la Convención de la ONU sobre

Ciberdelincuencia, este es el último año de mandato del Grupo de Composición Abierta de la ONU sobre la seguridad de las TIC. Se augura difícil alcanzar un consenso sobre la aplicación al ciberespacio del derecho internacional vigente, así como sobre la creación del Programa de Acción, un mecanismo permanente de discusión sobre la seguridad de las TIC impulsado por Francia y Egipto. La incertidumbre respecto a la inteligencia artificial dominará también el debate en un año en que el elector será clave para orientar la gobernanza tecnológica mundial.”



OCC – OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

Álvaro de Lossada
Jefe de la OCC. Secretaría de Estado de Seguridad Mº del Interior

“El dato seguirá siendo el activo más valioso dentro de la economía ilícita derivada de la actividad criminal en el ámbito ciber. Su indiscutible importancia, como fuente de información, como vector de ataque o como medio de extorsión, asegura el auge de todos los tipos de ataques relacionados con su obtención ilegítima, como los IAB. Debemos mencionar la IA y el abuso de aplicaciones NLP y modelos LLM legítimos o su creación con fines criminales, que ponen sistemas de ataque más eficientes al servicio de actores sin alta cualificación. La rápida implantación de dispositivos IoT en todos los ámbitos supone también un reto. El Mº del Interior, junto con Deloitte, acaba de publicar una guía de ciberseguridad para este tipo de dispositivos.”

FISCALÍA



FISCALÍA GENERAL DEL ESTADO

Elvira Tejada de la Fuente
Fiscal de Sala contra la criminalidad informática

“El imparable traslado de la actividad de los ciudadanos al entorno digital sigue provocando un desplazamiento progresivo de la delincuencia al ciberespacio. Los ataques informáticos para exfiltración de datos y/o sabotaje, ponen en riesgo los intereses generales y también los de empresas y ciudadanos que ven amenazada seriamente su privacidad por el robo y posterior utilización ilícita de sus datos personales. Las agresiones contra bienes personalísimos en especial contra los

menores y, en particular, el peligroso incremento de las que afectan a su libertad sexual está determinando importantes iniciativas normativas en la UE. Con todo, los ilícitos que generan más investigaciones policiales y judiciales siguen siendo las defraudaciones en sus distintas variantes, de las que se están derivando graves perjuicios económicos. En esta realidad criminológica empezamos a percibir los efectos del uso irregular de la IA que ofrece nuevas posibilidades de actuación a los ciberdelincuentes y plantea nuevos desafíos al Estado de Derecho. Una adecuada respuesta, protegiendo al tiempo los derechos y libertades de todos, es el gran reto al que nos enfrentamos y que exige de todos los poderes del Estado un esfuerzo serio y responsable de reflexión y acción coordinada, tanto en el ámbito nacional e internacional como con el sector privado, para adecuar nuestra legislación y organización interna a la consecución efectiva de dichos objetivos.”

menores y, en particular, el peligroso incremento de las que afectan a su libertad sexual está determinando importantes iniciativas normativas en la UE. Con todo, los ilícitos que generan más investigaciones policiales y judiciales siguen siendo las defraudaciones en sus distintas variantes, de las que se están derivando graves perjuicios económicos. En esta realidad criminológica empezamos a percibir los efectos del uso irregular de la IA que ofrece nuevas posibilidades de actuación a los ciberdelincuentes y plantea nuevos desafíos al Estado de Derecho. Una adecuada respuesta, protegiendo al tiempo los derechos y libertades de todos, es el gran reto al que nos enfrentamos y que exige de todos los poderes del Estado un esfuerzo serio y responsable de reflexión y acción coordinada, tanto en el ámbito nacional e internacional como con el sector privado, para adecuar nuestra legislación y organización interna a la consecución efectiva de dichos objetivos.”



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024

FCSE – FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO (INVESTIGACIÓN)



POLICÍA NACIONAL

M^a Piedad Álvarez de Arriba
Comisaria Principal
Jefa de la Unidad Central
de Ciberdelincuencia
Comisaría General
de Policía Judicial

“Desde Policía Nacional (PN) hacemos un balance muy positivo de las operaciones que hemos realizado en 2023 y no esperamos menos de 2024, año en el que celebramos nuestro 200 aniversario.

El año pasado junto con fuerzas policiales de otros países, como Estados Unidos, Alemania, Dinamarca, Canadá, Australia, Suiza, Reino Unido, etc., participamos en el desmantelamiento de las infraestructuras utilizadas por dos de los principales grupos criminales, Hive y Blackcat, autores de miles de ataques tipo *ransomware* en todo el mundo, recuperando y poniendo a disposición de las víctimas las claves de descifrado, evitando de esta manera que cientos de empresas tuviesen que pagar los rescates para recuperar la información que les habían cifrado.

También, bajo la coordinación de Europol, se clausuró el mayor mercado de venta de credenciales conocido hasta la fecha, Genesis Market, con 119 detenidos a nivel internacional, 11 de ellos en España, obteniéndose numerosa información que Policía Nacional continúa analizando.

Esta colaboración internacional y colaboración público-privada, con sectores estratégicos de nuestro país, en la que está volcada PN, no se ciñe a actividades operativas, sino que va más allá, propiciando intercambios de buenas prácticas. Así en la actualidad desde la UCC se está impulsando la constitución de un grupo de trabajo multidisciplinar, para implementar la solución al problema del *spoofing*, en la línea de lo realizado por Finlandia, y que consiguió una reducción del 97% al 3%.

Continuaremos concienciando a la sociedad, informando sin alarmar, sobre los riesgos asociados a las nuevas tecnologías, utilizando entre otros las redes sociales, donde PN es líder indiscutible a nivel mundial. Y seguiremos diseñando campañas de prevención dirigidas a los ciberdelincuentes, en la línea del exitoso Proyecto de 2023, ‘Intercop’, liderado por Europol, en el que hemos participado en representación de España. En resumen, continuaremos trabajando, a nivel nacional e internacional, en el plano operativo y estratégico, con la vista puesta en las amenazas asociadas a la IA, el metaverso o la computación cuántica, con el objetivo de garantizar la máxima protección de nuestros ciudadanos”.



GUARDIA CIVIL

Juan Antonio Rodríguez Álvarez de Sotomayor
Teniente Coronel.
Jefe del Departamento contra el Ciberdelincuencia
UCO – Unidad Central Operativa
Policía Judicial

“Cuando los malos pueden suplantar un teléfono, cuando han conseguido la información bancaria de la mayoría de las entidades financieras, cuando tienen la información necesaria para suplantar la identidad de los ciudadanos, cuando hackearon el DNI, el Punto Neutro Judicial, Hacienda, DGT, Ayuntamientos, Diputaciones, etc., cuando suplantaron a los Bancos, a las empresas, a las administraciones, cuando no tienen problemas de engañar los procesos de *onboarding* de los sistemas financieros, cuando navegan anónimamente sin limitaciones por internet, cuando usan correos electrónicos anónimos, cuando mueven criptomonedas impunemente, cuando crean sistemas inteligentes de información con todos los datos robados a instituciones y particulares y los usan para estafar..., algunos lo llaman seguridad nacional ¡pero la realidad es que asistimos al mayor reto a la seguridad de los ciudadanos y el orden público!

El aumento del ciberdelincuencia en todos los países de nuestro entorno es la tónica general, como lamentablemente viene siendo ya costumbre. Del mismo modo, seguiremos viendo un aumento significativo de la operativa criminal con motivación económica, con la seguridad de que sufriremos momentos donde se alcancen situaciones de grave riesgo para la integridad y seguridad de las personas.

Los cibercriminales se han vuelto extremadamente sofisticados y más organizados en sus operaciones, siendo habitual el movimiento de activos y despliegue de infraestructura en varias partes del mundo. El *malware*, como los *infostealers*, y las *botnets* seguirán siendo eficaces para el robo de credenciales, así como el auge de las comunidades o foros ilegales de servicios y activos cibercriminales.

El aumento de las campañas de ciberestafas viene siendo otro clásico del ciberdelincuencia, dado que nuestros datos personales no dejan de comercializarse en canales ilícitos, abusando de la suplantación de todo tipo de entidades financieras y servicios *online* para obtener nuestra información personal.

Continuaremos apreciando operativas criminales de mayor gravedad, en forma de ciberextorsiones, ya sea con la aparición de estructuras complejas detrás de nuevas formas extorsivas mediante cibersecuestros de personas, o las ya habituales con ataques mediante *ransomware*, apreciando últimamente un aumento de los ataques del tipo DDoS.

Solo mediante el intercambio eficaz de información sobre la operativa del ciberdelincuencia, mediante la asociación público-privada entre la industria, el mundo académico y las fuerzas de seguridad, se podrán desarrollar estrategias proactivas conjuntas para identificar, mitigar y, en última instancia, detener a los autores de las ciberamenazas”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024

POLICÍAS AUTONÓMICAS



ERTZAINTZA

Iskander Segurola

Unidad de Investigación Criminal y Policía Judicial
Jefe Sección Delitos en Tecnologías
de la Información

“Los ataques más complejos serán llevados a cabo principalmente por dos actores: organizaciones criminales internacionales y grupos estado-nación. El principal objetivo de los primeros será la obtención de capital mediante robo y venta de información o extorsiones utilizando la exfiltración de datos, entre otras. Los segundos, además de dinero, buscarán llevar a cabo acciones de espionaje contra infraestructuras críticas, empresas tecnológicas y objetivos políticos. Se experimentará una mayor sofisticación en las técnicas empleadas, elementos como el *Cybercrime as a Service* (CaaS) o la Inteligencia Artificial, no harán sino facilitar aquellos elementos necesarios para la comisión del delito”.



MOSSOS D'ESQUADRA

Josep Antoni López Garzón

Inspector. Jefe del Área Central de Cibercrimen

“2023 fue un año de consolidación de ciertas modalidades delictivas, donde lo más relevante fue el incremento en el número de denuncias asociadas a este ámbito. En el caso de las usurpaciones de identidad, se cuadruplicó el número de hechos delictivos desde el 2019. Tras la pandemia, la exposición personal a la red se incrementó y no ha cesado de hacerlo. Fruto de esto y de las fugas de información provenientes de ataques informáticos, se incrementó el comercio y uso de datos personales para fines delictivos. En el caso de Mossos d'Esquadra, se ha observado el incremento de esta tendencia. Como ejemplo destacado, el ataque que sufrió un importante centro sanitario de Barcelona donde se vieron afectadas multitud de víctimas, provocando cancelaciones de servicios y la filtración de datos personales”.



POLICÍA FORAL DE NAVARRA

Miguel Ruiz Marfany

Jefe de la Brigada de Delitos Económicos
y Contra el Patrimonio

“Parece claro que, en 2024, los ciberdelincuentes volverán a atacar al eslabón más débil de la cadena de la ciberseguridad y se centrarán cada vez más en explotar las vulnerabilidades humanas a través de la ingeniería social, con el uso de técnicas de OSINT para obtener la máxima información personal disponible de sus víctimas y de técnicas de *phishing* con el uso innovador de la inteligencia artificial generativa. La conciencia y educación en ciberseguridad se volverán, por lo tanto, esenciales, ya que cualquiera podemos ser el vector de entrada de un ciberataque. Los gobiernos deben impulsar las regulaciones que, garantizando la protección de datos, promuevan prácticas de seguridad robustas. La ciberseguridad se centrará en la prevención proactiva mediante la detección temprana y la respuesta rápida. Nuevamente, debemos insistir en la colaboración entre gobiernos, empresas y organismos de seguridad para compartir amenazas y desarrollar soluciones y estrategias conjuntas”.

ENTIDADES AUTONÓMICAS Y LOCALES



AGENCIA DE CIBERSEGURIDAD DE CATALUÑA

Pedro Lendínez Zaragoza

Director de Operacions (SOC-CERT)

“La actividad cibercriminal continuará creciendo derivada del contexto social, económico y político global. Por ello, continuarán produciéndose ataques de *ransomware* en infraestructuras públicas clave, así como en empresas de la cadena de suministro. Estos ataques serán en su mayoría poco sofisticados y de ejecución rápida, para maximizar el beneficio e impacto de los mismos. A su vez, aparecerán nuevas amenazas que utilizarán herramientas asistentes IA en entornos empresariales que dificultarán el control de acceso a la información para realizar fugas de datos sensibles mediante LLM”.



AGENCIA DIGITAL DE ANDALUCÍA

Enrique Rando González

Consejero Técnico para el Centro de Ciberseguridad de Andalucía

“Habrá ataques a infraestructuras críticas y servicios esenciales, de alto impacto, pero no necesariamente complejos, como alguno sufrido en España en enero. Otros ganarán en complejidad, quizá gracias a una IA que ofrecerá a los adversarios mayor eficacia y un alto grado de automatización. Dos escenarios que nos exigirán una mejora continua de nuestras capacidades si no queremos quedarnos atrás”.



CYBERZAINZA – AGENCIA VASCA DE CIBERSEGURIDAD

Asier Martínez

Director de Operaciones

“Los cibercriminales continuarán implementando tecnologías que, según el “hype” que generan muchos “expertos”, vienen a resolver todos nuestros problemas y que en realidad en la mayoría de los casos nos los provocan porque la sociedad las adopta sin conocer los riesgos, ni hacer un uso responsable de las mismas. Si bien es cierto que mayormente no es necesario que implementen demasiada complejidad porque continuamos fallando en aspectos básicos como contraseñas robustas, 2FA, actualizaciones, *backups*, etc.”



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



GENERALITAT VALENCIANA

Carmen Serrano Durbá
Subdirectora General
de Ciberseguridad

“El uso de la inteligencia artificial acortará los tiempos de aparición de ataques explotando nuevas vulnerabilidades críticas, reduciendo así el tiempo de reacción. En el contexto de la guerra, las infraestructuras críticas seguirán siendo objetivo prioritario de los grupos prorrusos. Se intensificará y sofisticará el compromiso de cuentas y robo de sesiones de usuario de accesos remotos y Cloud”.

infraestructuras críticas seguirán siendo objetivo prioritario de los grupos prorrusos. Se intensificará y sofisticará el compromiso de cuentas y robo de sesiones de usuario de accesos remotos y Cloud”.



XUNTA DE GALICIA – AMTEGA

Gustavo Herva
Jefe Subárea de Seguridad
de la Agencia para
la Modernización Tecnológica
de Galicia

“La conectividad a Internet se va incorporando a todo tipo de activos. Esa creciente superficie de ataque y la enorme dependencia que tenemos de todos los servicios a los que da soporte esa infraestructura, es carne de cañón para ser objeto de ataques de gran impacto. En este sentido, será conveniente avanzar con rapidez en la aprobación e implantación del Reglamento europeo de ciberresiliencia.”

tenemos de todos los servicios a los que da soporte esa infraestructura, es carne de cañón para ser objeto de ataques de gran impacto. En este sentido, será conveniente avanzar con rapidez en la aprobación e implantación del Reglamento europeo de ciberresiliencia.”



CENTRO DE CIBERSEGURIDAD DE NAVARRA (NCC)

Juan Ramón Aramendía
Coordinador

“La industria del cibercrimen va a seguir creciendo de forma imparable este año, priorizando sus objetivos entre los sectores más vulnerables como son los ciudadanos, que cada vez hacen un mayor uso

de canales digitales sin recibir formación acerca de los riesgos que estos entrañan: las pymes, inmersas en un proceso de transformación digital y que siguen viendo la ciberseguridad como un gasto y no como una parte inherente de ese proceso de transformación, el sector industrial, por la convergencia IT-OT y la cadena de suministro, y los fabricantes de electrónica que no hayan interiorizado que la ciberseguridad debe ser parte nuclear de sus procesos de diseño y desarrollo de producto.”



CENTRO DE CIBERSEGURIDAD DEL AYUNTAMIENTO DE MADRID – CCMAD

José Ángel Álvarez
Director del Centro de Ciberseguridad

“En 2024 no se reducirá el volumen ni la complejidad de los ciberataques. Los cibercriminales seguirán beneficiándose de la transformación digital global, con una alta especialización (*phishing as a service, ransomware as a service*), obteniendo enormes beneficios debido a la falta de capacidades de ciberseguridad de las víctimas.

Como parte de los conflictos geopolíticos presentes y futuros, habrá grupos avanzados que usarán todas las TTPs a su alcance para atacar infraestructuras críticas. En este sentido, las ciudades deberán poner el foco en la protección, no solo de los entornos IT, sino de los millones de dispositivos inteligentes que se están desplegando y que, sin control, son un riesgo evidente para la sociedad en su conjunto”.





ASOCIACIONES Y ANALISTAS



AENOR
Boris Delgado
Director de Industria
y TIC

“He conversado con una IA generativa. Su respuesta ha sido convincente y me ha hecho reflexionar. Efectivamente los ciberataques a las infraestructuras críticas, a la cadena de suministro, jun-

to con el *ransomware* e ingeniería social seguirán impactando en 2024. Sin embargo, la mayor amenaza será el propio uso inadecuado de la IA, que perfecciona y complica los ciberataques. Una vez más, la aplicación de estándares abiertos, como ISO 27001/27002/27701, o la reciente ISO 42001 de IA podrán gestionar y mitigar el impacto de nuevas amenazas y riesgos en ciberseguridad y privacidad”.



ALIANZA DIGI AMÉRICAS
Belisario Contreras
Coordinador

“El impacto de un ciberataque depende de la importancia de su objetivo. En 2024, uno de los más importantes para los actores de amenazas será la infraestructura electoral. A lo largo del año, está previsto que 76 países

celebren elecciones a nivel nacional, incluidas algunas de las democracias más grandes del mundo, como EE.UU., India, Brasil, Indonesia y la Unión Europea, que celebrará elecciones para su parlamento en los 27 Estados miembros en junio. Esto significa que podríamos ver un aumento de los ciberataques por parte de actores de amenazas con motivación política que apuntan a alterar una pieza crucial de la infraestructura electoral o simplemente causar dudas sobre su funcionalidad. De hecho, estos actores de amenazas tienen a su disposición varias herramientas tecnológicamente simples, pero impactantes, para lograr este objetivo. Por ejemplo, podrían utilizar un ataque de denegación de servicio distribuido (DDoS) a la infraestructura electoral para impedir que los votantes accedan a información confiable sobre su lugar de votación. De manera similar, podrían usar *phishing* para atacar una campaña o un partido y filtrarlo al público. De hecho, esto ocurrió durante las elecciones presidenciales estadounidenses de 2016, cuando piratas informáticos vinculados al gobierno ruso obtuvieron acceso a los sistemas del Comité Nacional Demócrata (DNC) y filtraron correos-e para dañar la campaña de Clinton.

Los sistemas de infraestructura crítica, especialmente aquellos utilizados para operar los sectores de energía, comunicaciones, agua y transporte, también seguirán siendo un objetivo importante para los actores de amenazas. Desafortunadamente, muchas de las tecnologías operativas (OT) tienen numerosas vulnerabilidades no mitigadas y podrían explotarse. Veremos ataques a infraestructuras críticas, que pueden tener un impacto aún más grave. Que un ciberataque sea complejo depende de la sofisticación de los métodos del actor de la amenaza. En 2024, los actores de amenazas aprovecharán tecnologías novedosas y emergentes, especialmente la IA, con la cual pueden aumentar drásticamente la eficacia de las estrategias de ciberataque existentes”.



ISACA
Vanesa Gil
Presidenta de ISACA Madrid Chapter

“En 2024 continuaremos asistiendo a un aumento en la sofisticación de los ciberataques, propiciado por la evolución en las técnicas de ataque derivada del empleo de tecnologías emergentes. Junto con *malware*, in-

geniería social y ataques dirigidos a entornos *cloud*, los ataques más complejos serán los perpetrados aprovechando los riesgos asociados a proveedores de servicios y cadena de suministro”.



CCI – CENTRO DE CIBERSEGURIDAD INDUSTRIAL
José Valiente
Director

“Las tácticas actuales de ciberseguridad se apoyan en tecnologías avanzadas como SIEM, SOAR, IPS, EDR y NGFW. Estas soluciones implementan Indicadores de Compromiso (IoC)

y *Playbooks* que, paradójicamente, podrían transformarse en amenazas serias en 2024. Con los ciberdelincuentes innovando continuamente en sus técnicas y métodos, la manipulación de IoC y *Playbooks* podría permitirles no solo evadir la detección sino también causar interrupciones significativas o, más preocupante aún, utilizando los mismos sistemas de defensa como herramientas para perpetrar ataques. Esta reflexión subraya la idea de que la ciberseguridad no es un fin, sino un proceso constante de adaptación y aprendizaje”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



CENTRO DE ANÁLISIS E INTERCAMBIO DE INFORMACIÓN DE SERVICIOS FINANCIEROS (FS-ISAC)

Teresa Walsh
Chief Intelligence Officer
and Managing Director, EMEA

“Los ataques distribuidos de denegación de servicio (DDoS), que antes se consideraban un ‘problema resuelto’, han resurgido como una amenaza principal para las empresas financieras, especialmente en la UE. Nuevas tácticas y más sofisticadas dieron como resultado los ataques DDoS más grandes jamás registrados en 2023. Esperamos que esta tendencia continúe, lo que podría afectar la disponibilidad de los sitios web orientados al cliente. Los ataques a terceros serán un vector de amenaza clave para las empresas financieras, particularmente difícil de gestionar dada la complejidad de la cadena de suministro del sector financiero y la dependencia de unos pocos proveedores clave. El fraude será, también, aún más complicado de detectar a medida que proliferen la IA y los actores de amenazas mejoren sus tácticas de ingeniería social para engañar a los clientes para que entreguen sus credenciales o envíen dinero”.



CLOUD SECURITY ALLIANCE (CSA) ESPAÑA

Mariano J. Benito
Vicepresidente

“Consideramos que el acceso a servicios en la nube desde cualquier geografía expone estos servicios a la evolución de los conflictos geopolíticos, tanto los que están en curso como otros futuros. No obstante, los actores de amenaza están adoptando un *modus operandi* con un gran impacto potencial para dificultar las operaciones necesarias para detección y respuesta. Crecientemente, los atacantes contratan servicios legítimos de la nube a nombre de identidades reales que han robado o que suplantan. Estos servicios son inicialmente indistinguibles de un nuevo usuario legítimo de la nube, y sólo se pueden cualificar correctamente iniciar actividades hostiles. La posición que adopten los proveedores de la nube ante estos *fake users* será decisiva”.



CYBERMADRID

Damián Ruiz
Presidente

“Incremento de ataques a pymes, en déficit continuo de Ciberseguridad y atractivas (*per se* o como vector de entrada a empresas grandes aprovechando sus debilidades en la cadena de suministro). Aumento del Fraude Digital en banca y *retail* como consecuencia de: 1) el robo constante de datos en terceros y en venta para su explotación y 2) las mejoras en ingeniería social del cibercrimen. Para todos, nuevo foco: dispositivos móviles”.



CYBERSECURITY INNOVATION HUB

Tomás Castro
Presidente de la AEI de Ciberseguridad
y Tecnologías Avanzadas

“En este 2024 afrontamos un panorama de ciberseguridad cada vez más desafiante. Los ataques a infraestructuras críticas representan una amenaza creciente. La evolución del *ransomware*, ahora más sofisticado, se centra en extorsionar con técnicas de doble amenaza. Los ataques a las cadenas de suministro emergen como un peligro clave. Además, la inteligencia artificial es aprovechada por los ciberdelincuentes para lanzar ataques más dirigidos. Mientras tanto, la proliferación de desinformación mediante *deepfakes* amenaza con desestabilizar sociedades. La creciente conectividad de los dispositivos IoT expande la superficie de ataque. Finalmente, el ciberespionaje y la guerra cibernética plantean riesgos de conflictos a gran escala”.



FORRESTER

Tope Olufon
Senior Analyst

“Se culpará de múltiples infracciones al código generado por IA. Además, una gran cantidad de brechas se derivarán de errores relacionados con las aplicaciones a medida que las organizaciones intenten (y fracasen) reemplazar completamente las pruebas humanas con IA. Las herramientas de mitigación de riesgos de terceros también se convertirán en un elemento básico y las organizaciones intentarán (y fracasarán) automatizar la diligencia debida. Desde una perspectiva de herramientas, XDR se volverá dominante y reemplazará a EDR en el mercado y los clientes europeos estarán más interesados en automatizar los procesos de respuesta básicos y desinvertir de los servicios MSSP heredados en favor de MDR. Por último, las empresas de confianza digitales también posicionarán sus ofertas como herramientas de mitigación de riesgos en lugar de simplemente mejoras en la eficiencia a medida que el mundo se preocupe más por la IA”.



ASOCIACIONES Y ANALISTAS



GLOBAL CYBER ALLIANCE

Pablo López-Aguilar
Operations and Business Associate
Director, Internet Integrity
Program

“Las cada vez más omnipresentes TIC están remodelando el mundo. Los servicios basados en inteligencia artificial (IA) y

capacidades de comunicación sin precedentes en términos de velocidad, confiabilidad, densidad y latencia, abrirán sin duda un sinfín de posibilidades a los ciberatacantes. Si bien nuestro tejido social es cada vez más consciente de la necesidad de aplicar medidas adecuadas de ciberseguridad desde una perspectiva técnica pero también educacional, poco se habla de seguridad a nivel de infraestructura. En este contexto, ataques como ‘Route Hijacking’, ‘IP Address Spoofing’, ‘DNS Spoofing’ o ‘DDoS’, entre otros, afectan cada día a la seguridad de las redes. Así pues, es fundamental que las organizaciones que operan a nivel de red inviertan tiempo y recursos en aplicar medidas de seguridad que protejan y mejoren la calidad de la información que llega a los consumidores”.



INICIATIVA EUROPEA DE INVESTIGACIÓN SOBRE CIBERCONFLICTOS (ECCRI- CIC)

Max Smeets
Director

“Creo que habrá mucho *ransomware*, ya que cada vez es más fácil hacer *emails de phishing* creíbles por parte de los cibercriminales. Algo que

está cambiando mucho por el uso de la IA y los modelos de lenguaje (ML) que permiten llegar con sus ataques a compañías de más lugares, sin importar la lengua que usan y esto va a pasar en 2024. Lógicamente existe la posibilidad de un ‘cyberarmagedon’, es una pesadilla que está ahí. Por ejemplo, impactando contra la salud de las personas, afectando a hospitales o a datos de pacientes, que se puedan dar a conocer y que sean críticos, como los informes de psiquiatría de menores o imágenes de personas con cáncer. Pueden ser terribles, incluso, causando pérdidas humanas y ese escenario donde afecta de forma sensible a las personas es una verdadera pesadilla que está ahí...”



(ISC)² ESPAÑA

Alejandro Cadarso
Presidente

“En 2023 los *chatbots* (Bard, ChatGPT, etc.) con LLM (Modelos de Lenguaje de Gran Escala) fueron la innovación más destacada en todos los ámbitos. Por lo tanto, para 2024, estoy seguro de que los ataques más complejos utilizarán LLMs para crear *malware* y *phishing*, combinándolos con suplantaciones mediante la simulación de voz a través de la tecnología *deepfake* ya que es indetectable para las personas, lo que hará que sea muy difícil evitar ataques de *Business email compromise*. Pero los ataques con mayor impacto serán aquellos que, con la disponibilidad de computación cuántica en AWS, Azure y GCP, permitirán romper los actuales algoritmos de cifrado comprometiendo la seguridad de datos”.

de *Business email compromise*. Pero los ataques con mayor impacto serán aquellos que, con la disponibilidad de computación cuántica en AWS, Azure y GCP, permitirán romper los actuales algoritmos de cifrado comprometiendo la seguridad de datos”.



KUPPINGERCOLE

Marina Iantorno
Research Analyst

“Una encuesta reciente realizada por Kuppinger-Cole Analysts muestra que el 48,2% de las organizaciones informaron hasta 50 ciberataques este año, pero solo el 18,2% planea aumentar sus presupuestos destinados ciberseguridad. La automatización de los ataques usando inteligencia artificial va en aumento y, por lo tanto, las empresas deberán anticipar y responder a las nuevas amenazas. Nuestra investigación indica que, en los próximos dos años, las empresas buscarán profesionales de ciberprotección especializados en autenticación de usuarios, seguridad en la nube y análisis de datos. Esto será necesario para superar la batalla de la IA para atacantes *versus* defensores”.

de las empresas deberán anticipar y responder a las nuevas amenazas. Nuestra investigación indica que, en los próximos dos años, las empresas buscarán profesionales de ciberprotección especializados en autenticación de usuarios, seguridad en la nube y análisis de datos. Esto será necesario para superar la batalla de la IA para atacantes *versus* defensores”.



MITRE ENGENUITY

Jon Baker
Gerente General del Centro
para la Defensa Informada sobre Amenazas

“Los adversarios seguirán usando lo que funciona. Innovarán para ponerse más eficientes y desarrollarán nuevas capacidades cuando sea necesario. Utilizarán modelos establecidos de *phishing* y *ransomware* en tanto que sigan funcionando. Al mismo

tiempo, los adversarios aprovecharán cada vez más la IA para automatizar. A medida que los entornos de TI evolucionan, desarrollarán nuevas tácticas. Así pues, adoptar un enfoque basado en amenazas para comprender los TTPs específicos de adversarios con MITRE ATT&CK ayudará a optimizar sus defensas frente a las amenazas más relevantes”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



OWASP ESPAÑA

Vicente Aguilera
Presidente del Capítulo

“Se incrementará el uso de la inteligencia artificial generativa para llevar a cabo ataques más elaborados y difíciles de detectar. Probablemente veamos un incremento en el uso de plataformas de mensajería populares como medio para organizar ataques orquestados, así como un incremento en ataques a dispositivos móviles o *gadgets* ampliamente extendidos, quizás formando parte de *botnets*”.



RAND CORPORATION

Sasha Romanosky
Senior Policy Researcher

“Una de las mayores preocupaciones siguen siendo los ataques contra infraestructuras y servicios públicos críticos (por ejemplo, electricidad, agua, gas natural, etc.). Si bien solo ha habido unos pocos ataques notables, la magnitud del impacto –así como la incertidumbre en torno a los efectos directos y colaterales– sigue siendo muy alta. Para enfatizar aún más este punto, dado que tenemos tanta incertidumbre sobre los efectos agregados (en cascada) de un solo ataque (incluso, de algo tan simple o prevenible como el *ransomware*), nuestra capacidad para priorizar de manera efectiva la mitigación sigue siendo una preocupación. Además, hay mucho revuelo en torno a la IA y su capacidad para generar o ejecutar ciberataques. Si bien la capacidad final no está clara, el potencial de este tipo de ataques cibernéticos asistidos por IA debe ser una de las principales preocupaciones”.



RENIC – RED DE EXCELENCIA NACIONAL EN INVESTIGACION DE CIBERSEGURIDAD

Ana Ayerbe
Presidenta

“Los cibercriminales explotarán la IA Generativa aprovechando su capacidad multimodal para generar imágenes, vídeos, texto y audio falsos, crear identidades falsas convincentes o generar *malware*. Todo ello lo aprovecharán para obtener más información, generar contenido de *phishing*, facilitar convincentes ataques de tipo BEC, manipular la opinión pública o sortear medidas de seguridad. Observaremos creativos ciberataques difíciles de imaginar en estos momentos.”



SANS INSTITUTE

Jess García
Senior Instructor

“2024 supondrá el despegue de la IA tanto en ataques de Ingeniería Social como en la automatización y sofisticación de técnicas ofensivas. Veremos una evolución creativa en *ransomware* y extorsión, un aumento de ataques a la infraestructura *cloud*, y cómo la actividad de los Actores de Espionaje (‘Nation-State’) se multiplicará, debido a la creciente complejidad geopolítica actual”.



THIBER

Adolfo Hernández
Cofundador

“A lo largo de 2024, presenciaremos un crecimiento de ataques más automatizados, más variados, con un enfoque en el usuario y sus diversos atributos de identidad. La inteligencia artificial facilitará la creación de *malware* y *ransomware* más ágil en cuanto a esfuerzo de desarrollo, capaces de aprender y ‘baipasear’ las defensas de seguridad. Las amenazas de cadena de suministro seguirán siendo comunes y difíciles de detectar. En el ámbito de la seguridad *cloud* enfrentará desafíos significativos debido a la complejidad de los entornos de nube híbridos y multiplataforma. Por último, la creciente tensión geopolítica podría traducirse en ciberataques estatales, dirigidos a infraestructuras nacionales clave y espionaje industrial”.





ASOCIACIONES DE MUJERES



GIRLS CAN HACK
Soledad Antelada
Presidenta y Fundadora

“La mayor amenaza somos nosotros. Personal sin la experiencia adecuada ha sido incorporado en la industria y no recibe la formación continua necesaria. La industria aún exhibe inmadurez. Esto conduce a una cultura viciada definida por un alto grado de imitación y tendencia a acumular méritos aparentes.

“Mi principal preocupación en ciberataques se centra en las infraestructuras críticas. Aunque a nivel gubernamental la seguridad se aborda como una necesidad imperativa todavía nos enfrentamos a sistemas excesivamente vulnerables.

Los ‘nuevos’ esfuerzos en diversidad dentro del sector a menudo son liderados por quienes, paradójicamente, representan el problema, destacando la necesidad de un enfoque más auténtico en esta área”.

Los ‘nuevos’ esfuerzos en diversidad dentro del sector a menudo son liderados por quienes, paradójicamente, representan el problema, destacando la necesidad de un enfoque más auténtico en esta área”.



WOMCY, LATAM WOMEN IN CYBERSECURITY
Leticia Gammill
Presidenta y Fundadora

“Se espera que la IA ayude a las organizaciones a adoptar métodos de seguridad más sólidos y sencillos. La IA aportará información y ayudará en la gestión de incidentes mediante la automatización de tareas rutinarias. El talento en ciberseguridad se beneficiará, reduciendo la curva de aprendizaje y aliviando la brecha de talento. La creación de una fuerza de trabajo diversa en ciberseguridad pasará de ser un mantra a una acción y formará parte de la ciberestrategia general. Las organizaciones aplicarán prácticas creativas de reclutamiento, contratación, retención y formación que irán más allá de los enfoques tradicionales para crear equipos más diversos que se ajusten a las necesidades futuras de las empresas y las misiones”.

información y ayudará en la gestión de incidentes mediante la automatización de tareas rutinarias. El talento en ciberseguridad se beneficiará, reduciendo la curva de aprendizaje y aliviando la brecha de talento. La creación de una fuerza de trabajo diversa en ciberseguridad pasará de ser un mantra a una acción y formará parte de la ciberestrategia general. Las organizaciones aplicarán prácticas creativas de reclutamiento, contratación, retención y formación que irán más allá de los enfoques tradicionales para crear equipos más diversos que se ajusten a las necesidades futuras de las empresas y las misiones”.

ASEGURADORAS Y MEDIADORES



AON
Verónica Jiménez
Director Cyber Solutions

“En base al estudio ‘Aon’s 2023 Global Risk Management Survey’, los ciberataques son la principal preocupación para las organizaciones. Los ataques *ransomware* crecieron en un 200% durante 2023 y se espera que sigan subiendo este año con mayor sofisticación y con un crecimiento de los ataques basados en IA. En este sentido, la creación de *malware* inteligente que logre evadir cualquier tipo de sistema de detección irá en aumento y se prevé que se ejecuten ataques bastante autónomos, dirigidos principalmente por *bots* y con la mínima participación humana. Por sectores, se espera que los de educación y sanitario sean los principales afectados: las cadenas de suministro serán una vía de entrada de ataques con objetivo final en una gran corporación”.

“En base al estudio ‘Aon’s 2023 Global Risk Management Survey’, los ciberataques son la principal preocupación para las organizaciones. Los ataques *ransomware* crecieron en un 200% durante 2023 y se espera que sigan subiendo este año con mayor sofisticación y con un crecimiento de los ataques basados en IA. En este sentido, la creación de *malware* inteligente que logre evadir cualquier tipo de sistema de detección irá en aumento y se prevé que se ejecuten ataques bastante autónomos, dirigidos principalmente por *bots* y con la mínima participación humana. Por sectores, se espera que los de educación y sanitario sean los principales afectados: las cadenas de suministro serán una vía de entrada de ataques con objetivo final en una gran corporación”.



MAPFRE
Andrés Peral
Director de Seguridad en Sistemas de Información

“2024 se presenta como un año aún más complejo que 2023. El escenario geopolítico seguirá complicándose, impactando claramente en una ciberamenaza, que no parará de crecer. Los ataques a la cadena de suministro y el impacto que ataques a grandes proveedores de servicios tecnológicos sobre los servicios que las empresas prestamos a nuestros clientes, serán portada en 2024”.

“2024 se presenta como un año aún más complejo que 2023. El escenario geopolítico seguirá complicándose, impactando claramente en una ciberamenaza, que no parará de crecer. Los ataques a la cadena de suministro y el impacto que ataques a grandes proveedores de servicios tecnológicos sobre los servicios que las empresas prestamos a nuestros clientes, serán portada en 2024”.



CENTROS Y LABORATORIOS DE INVESTIGACIÓN Y EVALUACIÓN



LABORATORIO DE CRIPTOGRAFÍA – LIIS
Jorge Dávila
Director
Facultad de Informática
UNIVERSIDAD POLITÉCNICA DE MADRID

“Hablar sobre lo que va a ocurrir es tarea difícil y siempre pone de

manifiesto los temores subconscientes de los que se expresan. Como este año nos dejan gozar de la libertad de que nuestros vaticinios sean esperables o no, podemos ponernos a pensar en qué haría realmente daño a la actual y futura sociedad digital.

Está claro que en la fuerza/esencia de cualquier ataque esperable y probable siempre va a estar el dinero, los rescates, las ventajas tácticas; en definitiva, la gestión del poder. Por ello en 2024 lo esperable es lo que de más dinero/poder a cualquiera de los agentes involucrados, ya sean los denominados ciberdelincuentes o los autodenominados ciberguerreros/defensores (o ‘ciberseguratas’ en terminología más coloquial) que representa toda la industria de la ciberseguridad actual. En este año, los incidentes de todo tipo aumentarán en beneficios gracias a la industrialización (*Tailorizacion*) de los ataques rentables y a la mayor inversión por parte de la amedrentada sociedad protodigital a la que se le regala miedo para venderle ‘seguridad’.

En cuanto a los tipos de ataques que harían mas daño, imagino que serán aquellos que socaven o eliminen la misma digitalización y sus beneficios colaterales, que son muchos. La digitalización se da como fenómeno por causas de su eficiencia, abaratamiento y globalización, pero socialmente se la tolera porque se confía en ella, porque la gente sigue creyendo que lo que circula en esa realidad paralela es la verdad y es la misma esencia de la sociedad (identidades, propiedad, transacciones e intercambios documentados, etc.). Además de la confianza o no de la gente, también está en la capacidad de prueba que tenga el escenario digital ante los sistemas judiciales de las distintas sociedades.

Puestos a pensar en un ataque realmente crítico a esta sociedad protodigital, se me ocurre la corrupción intencionada y controlada (por el atacante) de las bases de datos sobre las que se desarrollan las actividades de la sociedad analógica en la que nosotros existimos. ¿Cuánto valdría recuperar la integridad del catastro, de los protocolos notariales, de las bases de datos de ciudadanía, los censos electorales, de los registros de todo tipo, etc.?”



TOKIO MARINE HCC
Isaac Guasch
Cyber Security Leader

“Esperamos un auge en severidad y frecuencia de ataques de *supply chain* que afecten especialmente al sector de fabricación y distribución, y proveedores de TI. Estos ataques llegaron incluso a parar a reguladores de industrias debido a la dependencia de las partes en la cadena de suministro. Este año preveo un mayor impacto debido a la acumulación de riesgo que se traducirá en un entorno de alto riesgo sistémico”.

“Esperamos un auge en severidad y frecuencia de ataques de *supply chain* que afecten especialmente al sector de fabricación y distribución, y proveedores de TI. Estos ataques llegaron incluso a parar a reguladores de industrias debido a la dependencia de las partes en la cadena de suministro. Este año preveo un mayor impacto debido a la acumulación de riesgo que se traducirá en un entorno de alto riesgo sistémico”.



WTW
Carmen Segovia
Directora de Ciber Riesgos

“El mercado asegurador ve con preocupación: 1) Avances en IA que abren nuevas vías para ataques más efectivos; 2) El contexto geopolítico sugiere un aumento de los ataques patrocinados por los estados por lo que la cláusula de exclusión de guerra seguirá dando guerra; 3) Explotación de vulnerabilidades de día cero para instalar *malware*, robar datos, interrumpir operaciones y exigir rescates”.

“El mercado asegurador ve con preocupación: 1) Avances en IA que abren nuevas vías para ataques más efectivos; 2) El contexto geopolítico sugiere un aumento de los ataques patrocinados por los estados por lo que la cláusula de exclusión de guerra seguirá dando guerra; 3) Explotación de vulnerabilidades de día cero para instalar *malware*, robar datos, interrumpir operaciones y exigir rescates”.





CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024

CENTROS Y LABORATORIOS DE INVESTIGACIÓN Y EVALUACIÓN



APPLUS+ LABORATORIES

Nuria Carrió
Certification Technical Director

“En 2024, se anticipan ciberataques avanzados y de gran impacto utilizando inteligencia artificial (IA). Las amenazas incluyen “IA ofensiva” para desarrollar *malware* sigiloso y descubrir vulnerabilidades, ingeniería social con IA para engaños personalizados, y ataques DDoS automatizados. Por eso, se requiere inversión en ciberseguridad en IA, con preparación y vigilancia continua”.



EURECAT

Juan Caubet
Director de Ciberseguridad

“En 2024 habrá un crecimiento importante de ataques de suplantación de identidad ayudados por Inteligencia Artificial y llevados a cabo para conseguir ambiciosos objetivos (fraude financiero, robo de información sensible, acceso ilegítimo a infraestructuras...), ya que suelen ser ataques muy difíciles de detectar. Los atacantes consiguen que nuestros sistemas los vean como usuarios legítimos”.



FUNDACION i2CAT

Jordi Guijarro Olivares
Cybersecurity Innovator Director

“La tendencia de unir la realidad con el mundo virtual es un concepto conocido como ‘Phygital’. Potenciada por la última pandemia y con una muy rápida proliferación de escenarios que ya van más allá del *retail* y que empieza a calar en sectores críticos, habilitada por tecnologías como el 5G, VR, AR, AI, IOT... abre un escenario de nuevas ciberamenazas de alta complejidad en entornos multidimensionales. Retos para una NG-CTI buscando una combinación armoniosa entre los dos mundos”.



FUNDITEC

Miguel Rego
Director General

“La IA generativa ayuda a reducir la capacitación necesaria para escribir señuelos creíbles y para incrementar la automatización, ya que permite encadenar tareas, proporcionar recetas e integrarse con recursos externos para

lograr tareas de nivel superior. La IA es capaz de generar nuevos tipos de ataques o provocar cambios profundos sobre ciberataques ya existentes, facilitando que las arquitecturas de ciberseguridad existentes nos sean capaces de actuar sobre los ataques generados de esta manera. Otro de los efectos de su uso es la de la suplantación. Hemos visto ya algunos ejemplos de cómo crear imágenes, voz o vídeo humanos de forma muy realista, lo que deriva en campañas de desinformación o a socavar la verificación de la identidad y la biometría de voz. Es evidente que la IA y la ciberseguridad, cuando trabajan juntos nos hacen más fuertes y resilientes. Por ello, ante la vorágine de ciberamenazas reforzadas por la IA, la solución es conjugar regulación y las buenas prácticas con la mejora de las tecnologías ciberseguridad, usando para ello las capacidades que, esta vez a nuestro favor, nos aporta la IA”.



GRADIANT

Juan González Martínez
Director Área de Seguridad y Privacidad

“Los potenciales ciberataques dirigidos a servicios esenciales, con un enfoque específico en los sistemas financieros y sus interconexiones estarían sin duda entre los más complejos y con consecuencias devastadoras. La vulnerabilidad latente en algoritmos criptográficos obsoletos podría ser explotada para comprometer comunicaciones y transacciones financieras, especialmente en organizaciones que no siguen el paradigma de agilidad criptográfica”.



GRUPO DE INVESTIGACIÓN REDES Y SISTEMAS

Javier Areitio
Director, Facultad de Ingeniería
UNIVERSIDAD DE DEUSTO

“Nos vamos a encontrar con afecciones debidas a: IA/GenIA, creación de *ng-malware*, *Fake-datos*/biométricos, *honey-traps* en *chatbot-genIA* contaminados; *SEO-poisoning* (técnicas *Search Engine Optimization* legítimas para poner los sitios web maliciosos a la cabeza de los resultados del *search-engine*); computación cuántica contra la criptografía existente; crecimiento de vulnerabilidades en todo (APPs/APIs/*Blockchain*/*Criptomoney*, Contratos-inteligentes/nubes); No actualizaciones/falta-parches; *Middlemen*; No: DevSecOp/DevPrivacyOp, Zero-Trust, ZK/fragmentación-secretos, SMPC, OT, C-Faraday; Implicando todas las áreas: Privacidad/confidencialidad (robo de identidades, datos, secretos, vigilancias-escuchas clandestinas), disponibilidad (*ng-DDoS-IA*, *ng-ransomware*, interferencias), integridad (*Mis-Mal-Dis-Information*, modificar configuraciones/códigos, *deep-fake-all*)”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



JTSEC
Javier Tallón
Director Técnico

“Los ataques de mayor impacto vendrán a través de la cadena de suministro, especialmente por el uso de componentes de terceros cuyo código no es controlado ni supervisado. Estos ataques, que causan graves problemas año tras año, seguirán intensificándose debido al crecimiento exponencial de la complejidad del software. Es urgente que se exija el uso de herramientas como SBOM para controlar y vigilar la composición del software”.



NETWORK INFORMATION AND COMPUTER SECURITY LABORATORI (NICs Lab)
Javier López Muñoz
Director
Universidad de Málaga

“Las amenazas del futuro combinarán técnicas tradicionales con Inteligencia Artificial, permitiendo la automatización de ataques o el desarrollo de *malware*. La IA también permitirá mejorar los ataques de ingeniería social y las campañas de desinformación. Asimismo, aumentarán los ataques a la IA para manipular sectores críticos como Industria 4.0/5.0 y los gemelos digitales”.



SGS BRIGHTSIGHT
Lucio González Jiménez
General Manager CyberLab Madrid

“Este nuevo año se presenta con avances en términos de prevención y protección con nueva regulación europea en productos (CRA, CSA – EUCC) y con la realidad de la IA que se nos antoja un tanto impredecible. Es decir, se inicia un periodo de transición en el que se espera aumento del número de fabricantes que van a reforzar la seguridad en el diseño de sus productos lo que contribuirá a disminuir el nivel de exposición. Sin embargo, el nuevo escenario junto a los indudables avances que conllevará la IA nos indica que sólo se acaba de empezar y todo está por hacer. Respecto a amenazas ‘tradicionales’ la ingeniería social seguirá siendo una de las principales actividades teniendo en cuenta, además, la proliferación de bases de datos en el mercado negro. Cabe señalar que la rápida absorción de tecnología, productos y servicios destinados a los servicios de seguridad gestionados precisan de mayor protección (alta frecuencia de actualizaciones) precisa de mayor énfasis en la capacitación del personal con el fin de poder maximizar la vigilancia y respuesta. El contexto de la guerra en Ucrania y en Oriente Medio ya ha aportado nuevas modalidades de ataque, añadiendo la facilidad con la que las redes sociales pueden ser utilizadas sigue creciendo cuando se abren periodos electorales de relevancia (Europa, EE.UU., en nuestro caso las regionales). Por lo tanto, se abren nuevos escenarios que van a permitir avances significativos

en términos de protección, respuesta y diseño de dispositivos, software y servicios que no necesariamente irán progresando al mismo ritmo. Generalmente, las amenazas han sido siempre han aparecido con mayor prontitud que la respuesta o solución, esperemos que se cambie la tendencia”.



TECNALIA
Óscar Lage
Responsable de Ciberseguridad

“La creciente popularidad de los LLM plantea nuevos desafíos de seguridad y privacidad. Estos modelos, desarrollados a contrarreloj sin considerar su seguridad, serán un gran riesgo en este 2024. Permitirán, entre otros, el acceso a datos de entrenamiento e histórico de consultas a través de técnicas de *Prompt Hacking*, generarán código vulnerable, y se usarán para perfeccionar los ataques de *phishing*”.



VICOMTECH
Raúl Orduña
Director de Seguridad Digital

“En 2024 destacarán tres fuentes de amenaza: la búsqueda e identificación automática de vulnerabilidades utilizando sistemas de inteligencia artificial, la generación de contenidos fraudulentos realistas, bien para suplantar la identidad de los usuarios de aplicaciones, o bien la de los servicios que utilizan dichos usuarios y el uso sobre entidades críticas de uso civil de parte del ciberarsenal desarrollado y probado en los conflictos en curso”.



ZIUR – CENTRO DE CIBERSEGURIDAD INDUSTRIAL DE GUIPÚZCOA
María Penilla
Directora General

“Para 2024 no se esperan grandes cambios en las estrategias de ataques y explotación, lo que sí esperamos es una irrupción clara de la IA y herramientas, como ChatGPT, que les permiten a los ciberdelicuentes reducir los tiempos en la elaboración de su ciberarmamento. También estamos viendo cambios en el proceso de extorsión por parte de los ciberdelincuentes, empezamos a ver casos en los que a las amenazas de: no descifrar los datos; publicar los datos más críticos en foros; informar del compromiso de los datos a clientes y/o inversores; se suma una nueva y última extorsión de informar a las autoridades locales sobre el incidente, para así, provocar el pago de una multa. Todo con el único objetivo de conseguir el beneficio económico”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024

INDUSTRIA Y SERVICIOS



ABAI GROUP

Alberto Arbizu

Director Comercial Iberia

“La superficie de ataque se ha extendido desde la típica venta al por menor hasta la fabricación, que implica actividades operativas (OT) y la influencia de la economía digital. El asumir que tarde o temprano vamos

a ser atacados es un punto crítico y de asunción dentro de las organizaciones. Desde Abai Group vemos que la GenAI, junto con el uso de Redes Generativas Adversativas (GAN), alteren el mercado del *phishing* en 2024. Esta transformación permitirá la creación rentable de contenidos de audio y vídeo súper realistas, lo que impulsará una nueva oleada de fraudes de *business email compromise* (BEC), secuestros virtuales, entre otros”.



ACCENTURE

Agustín Muñoz-Grandes

Accenture Security Lead in Iberia
Managing Director

“Se espera un incremento y sofisticación del cibercrimen debido al uso de GenAI para la explotación de Zero-days, el desarrollo de *malware* más difícil de detectar y eliminar, así como

la construcción de campañas de ingeniería social, extorsión, desinformación y suplantación con *Deep Fake*. Aumentarán también los ataques estados-nación y hacktivistas, debido a los conflictos geoestratégicos”.



ADVENS

José Luis Díaz

CEO Iberia

“En 2024 habrá un aumento generalizado en todos los tipos de ataques que conllevan el uso de IA. También tendremos que seguir hablando de *ransomware*, que se volverán aún más sofisticados y dirigidos. Nuestra

apuesta: *Ransomware* dirigido (al igual que en años anteriores, estos ataques seguirán creciendo y serán más sofisticados, apuntando a objetivos específicos para maximizar el impacto), ataques basados en IA y usándola para identificar y explotar vulnerabilidades, ingeniería social avanzada y automatizada (uso personalizado de datos *online* para engañar a usuarios y obtener acceso), ataques sobre la cadena de suministro y terceras partes, y aumento de los ataques basados en *Zero days*”.



AIUKEN CYBERSECURITY

Juan Miguel Velasco

CEO

“Según el observatorio de Ciberseguridad de Aiuken, 2023 se ha cerrado con un aumento de más de un 27% de ataques con respecto a 2022, especialmente en *phishing*, *ransomware* y se mantienen DDoS y otras infec-

ciones. Todos esperamos que en 2024 los ataques aumenten. Como los sistemas, gobiernos y la sociedad están mejor preparados, el impacto será mayor para los ataques dirigidos esponsorizados por crimen organizado y estados. La difícil situación socio-política en el norte de Europa y en Medio Oeste mantendrá el aumento de ataque a infraestructuras y sistemas vinculados a los gobiernos, en España todas la infraestructuras críticas y grandes empresas serán objetos de ataques especialmente del bloque soviético. En Medio Oeste debido a la tensión seguirán los DDoS, los ataques de *ransomware* y el robo de datos. El lucro con los datos y los ataques dirigidos pagados serán el foco de la explotación de *Zero days* y vulnerabilidades”.



AJOOAL ASOCIADOS

Carlos Serra

CTO

“Sin duda alguna, 2024 es el año de la consolidación de las amenazas asociadas a la IA. No hablamos solo de nuevas técnicas o formas de explotación, sino de un paso más allá en cuanto a la creación de nuevas herramientas de

ingeniería social tan necesarias para poder acceder a entornos más seguros de una manera totalmente silenciosa, pieza clave en las ciberamenazas de cualquier índole”.



AKAMAI TECHNOLOGIES

Francisco Arnau

Vicepresidente Regional para España y Portugal

“El panorama de ciberseguridad es desafiante, con EMEA persistiendo como epicentro de ataques, vulnerable a ataques DDoS, web y de *bots*. La evolución de estos vectores, fusionando vulnerabilidades de día cero con tácticas de *ransomware*,

indica una amenaza extorsionadora. Es urgente reforzar la ciberdefensa con planes de contingencia proactivos. En 2024, la anticipación y la acción concertada serán clave ante la creciente sofisticación de amenazas”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



ALL4SEC

Alfonso Franco
CEO & Managing Director

“La ingente información que circula por la *Dark Web* servirá para alimentar las soluciones de Inteligencia Artificial en la identificación de nuevas aproximaciones técnicas para completar ciberataques desconocidos. Nada impedirá que surjan soluciones IAaaS para elaborar ataques

dirigidos a partir de la extensa información que posean sobre la posible víctima. El *phishing* personalizado será el ejemplo más evidente de este tipo de ataques”.



ALVAREZ & MARSAL SPAIN

Julio San José
Managing Director

“Asistiremos a un crecimiento de los ciberataques tanto en amplitud como en complejidad. Serán IA *centric* o dirigidos por la IA, permitiendo un rápido desarrollo automatizado de variantes de *ransomware*, *deepfakes*, etc., abaratando coste y maximizando *targets*. El nivel geopolítico es

muy complejo (Ucrania, Gaza, etc.) que conlleva un incremento de la actividad de los actores Estados-nación, veremos ataques en los sistemas electorales completos y colectivos personales. En las amenazas, veremos ataques selectivos a colectivos de personas y desarrollos de IA de con modelos de lenguaje malicioso que llamaremos *IA criminal*”.



ARMIS

Axel Pérez García
Solution Architect – Iberia Region

“Debido a la proliferación de la IA generativa, los ataques en entornos IoT, IoMT y OT serán cada vez más frecuentes y de mayor alcance al aprovechar las vulnerabilidades de dispositivos que están expuestos a los riesgos de Internet. Estos ataques serán cada vez más sofisticados, emulando patrones de comportamiento que dificultarán la detección, al intentar eludir las defensas en la red”.

“Debido a la proliferación de la IA generativa, los ataques en entornos IoT, IoMT y OT serán cada vez más frecuentes y de mayor alcance al aprovechar las vulnerabilidades de dispositivos que están expuestos a los riesgos de Internet. Estos ataques serán cada vez más sofisticados, emulando patrones de comportamiento que dificultarán la detección, al intentar eludir las defensas en la red”.



ARROW ECS

Ignacio López Monge
Vice Presidente, Sales ECS, South EMEA

“El incremento de las capacidades de las IAs y el ML se aprovechará para desarrollar programas maliciosos de manera mucho más rápida y difícil de detectar. El *digital blackmail* seguirá incrementando los ataques a infraestructuras y los nuevos dispositivos de IoT sufrirán un

mayor número de ataques y más sofisticados. Además, se desarrollarán nuevas aplicaciones móviles señuelo cuyo principal objetivo será espiar y obtener información sensible de los usuarios”.



ATALANTA

Isaac Gutiérrez
CEO

“2023 terminó marcado por las diferentes guerras y tensiones geopolíticas que provocaron mucho ciberespionaje, aumento de actividad hacktivista, ataques a infraestructuras críticas y campañas de desinformación, *phishing* y *ransomware*. En este 2024 veremos cómo la

IA puede dar lugar a ciberamenazas mejoradas; el uso de redes generativas adversarias (GANs) a fin de crear identidades falsas realistas para ataques de ingeniería social, el desarrollo de *malware* impulsado por IA que puede mutar para evitar la detección o la creación de *exploits* cada vez más creativos para dispositivos móviles. Por lo que el *ransomware* estará muy presente durante 2024. No podemos olvidar los ataques a los servicios en la nube, que conllevan importantes desafíos, como, por ejemplo, la gestión de identidades, el uso de APIs y seguridad en las aplicaciones, la arquitectura y estrategia de seguridad en la nube o el tratamiento de datos, entre otros”.



A3SEC

Alejandro de la Peña
Director de A3Sec España

“En 2024 seguirá creciendo el volumen de dispositivos digitales por lo que aumentarán las amenazas a dispositivos IoT, así como a la cadena de suministro, la banca y las infraestructuras críticas, que serán objeto de mayores ataques provenientes del ánimo de lucro

y de los intereses de los estados. Los atacantes harán evolucionar sus procedimientos basados en la IA, que deberá competir con la IA de los servicios de defensa. ¡Tenemos que tener nuestras defensas cada vez más activas y preparadas!”.



ÁUDEA

Antonio Martínez
Socio y Desarrollo de Negocio

“En los tiempos actuales en los que los datos son el nuevo petróleo, impulsor de toda economía e industria, la seguridad es un problema, dicho de otra forma, nos enfrentamos a riesgos de diversa índole, unos viejos conocidos, otros actuales y otros por venir, pero creo

que, como todo en la vida, hay que afrontarlo como una verdadera oportunidad de profesionalización, y mejorar las capacidades para afrontar todos estos retos, todo en un entorno regulado y bajo control. Un aspecto central de estos esfuerzos será la necesidad de disponer de inteligencia sobre ciberamenazas tanto externa como interna que sea relevante y contextual para cada organización. La IA ha llegado para quedarse, y va a revolucionar todo, con ciberataques más afectivos gracias a la GenAI, aumento de las falsificaciones cada vez más sofisticadas de correos, suplantaciones de voz y vídeo, de identidad y atención de credenciales”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



AUTEK INGENIERÍA

Miguel Ángel Martín
Product Manager

“Aunque la tendencia de amenazas y ciberataques va a seguir la misma línea de los últimos años, últimamente hemos visto un cambio en la manera de afrontar la ciberseguridad. Como vimos en las pasadas jornadas STIC CCN el concepto *Zero Trust* ganó impulso en 2023 y seguirá desarrollándose este año. Del nicho de las redes clasificadas ha pasado a ser un aspecto fundamental en la ciberseguridad de cualquier organización”.



AUTHUSB

María Cobas
CMO

“Por supuesto que los ciberataques utilizando la IA generativa serán una tendencia al alza que habrá que vigilar muy de cerca, pero con esto no estoy descubriendo la pólvora. Mas o menos todos lo tenemos claro, pero es algo con lo que tendremos que lidiar. Nosotros creemos que el foco tiene que seguir siendo el mismo. Por una parte, las personas y su educación en ciberseguridad, en todos los ámbitos público y privado. Cada vez los ciberdelincuentes lo hacen mejor y más difícil de detectar. El *phishing*, *smishing* y muchos otros seguirán siendo un problema muy importante que deberemos afrontar. Por otra parte, hay que hacer un *Back to the basics*. A veces nos dejamos llevar por las últimas ‘modas’ y novedades y nos olvidamos de que las organizaciones son muy vulnerables en sus lugares más básicos, allí donde nadie se espera que nunca vaya a surgir un problema”.



BABEL

Mario Casado
Global Head of Cybersecurity

“En 2024, prevemos un aumento en ciberamenazas de IA manipulada, ataques de *ransomware* más sofisticados y riesgo creciente de ataques a infraestructura crítica, apuntando a sectores clave como salud y energía. Además, hay que prestar especial atención a los ataques en entornos nube y kubernetes. Es imprescindible que cambiemos nuestro modelo de protección aprovechando los avances en IA”.



BARRACUDA

Antonio Anchustegui
Iberia Channel Manager

“La IA hará imposible distinguir realidad de ficción. Nuevos ataques evadirán la protección basada en MFA y las estrategias de *backup* tradicionales serán cada vez más vulnerables ante la extorsión y el *ransomware*. Pero todo no serán malas noticias. La adopción de la IA por la industria permitirá hacer frente a estos ataques con eficacia y pondrá de relieve el abismo tecnológico entre las soluciones tradicionales y las que utilizan IA como motor de análisis”.



BOTECH

Fernando Carrazón
CTO

“En 2024, el ciberataque de moda será el *Deepfake Data Breach*. Los atacantes utilizarán IA avanzada para crear videos y audio falsificados convincentes de figuras públicas y empresarios, difamando, extorsionando o propagando desinformación. Estos *deepfakes* se emplearán como señuelos para robar datos confidenciales y desestabilizar organizaciones y gobiernos. Para evitar fraudes masivos a las organizaciones, será necesario implantar defensas avanzadas contra este tipo de ataque”.



BROADCOM

Nur Pulad
Head of Cybersecurity Iberia

“En este 2024 nos encontraremos nuevas amenazas y tipologías de estafas relacionadas con la incorporación y adopción imparable de herramientas de inteligencia artificial en tareas convencionales, monedas digitales y metaverso. Hablaremos con nuestro CRM, con nuestro navegador, con nuestra TV, con nuestras hojas de calculo... La pregunta es ¿Quién será el encargado de velar por el control y fuga de la información?”



BEDISRUPTIVE

Xabier Mitxelena
Director General

“Al enorme debate sobre los riesgos que conlleva el auge de la inteligencia artificial, junto a la masificación de la tecnología *Deepfake*, se suma también el hacktivismo como una de las principales ciberamenazas en 2024. Asimismo, la proliferación de tecnologías emergentes, como las redes 5G y el IoT, ampliará la superficie de ataque aumentando las amenazas a la cadena de suministro”.



BITDEFENDER

Martin Zugec
Technical Solutions Director
at Bitdefender

“El cibercrimen sigue evolucionando en la misma dirección que tomó hace más de un año. Los ciberdelincuentes motivados por ganancias, por *ransomware*, au-



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024

mentarán sus habilidades, reflejando ciberataques sofisticados patrocinados por el estado. Es fundamental equiparse con soluciones de seguridad avanzadas, como detección y respuesta extendidas (XDR), y modelos de seguridad gestionados como MDR”.



CASTROALONSO
Miguel García-Menéndez
CEO

“El vigente ‘desorden mundial’ (tensiones políticas, económicas y militares) marcará la agenda de las principales amenazas a las que prestar atención en el nuevo año. Las numerosas citas electorales, domésticas y

foráneas, así como otros grandes eventos –los deportivos, en pleno año olímpico, no serán una excepción– serán objetivo prioritario para quienes deseen obtener el mayor impacto”.



CEFIROS
Ángel Carreras
Director

“En 2024, sin lugar a dudas, serán los que tengan que ver con ataques a infraestructuras críticas, y no ataques a ellas directamente, sino a través de proveedores o a sus cadenas de suministro, y teniendo como principal vector de ataque e infección el correo electrónico”.



CHECK POINT
Eusebio Nieva
Director SE para Iberia

“Entre todos los ataques que se producirán este año cabe destacar el previsible aumento, tanto en número como en efectividad y perjuicio económico global, de los que involucren *deepfakes*, tanto de vídeo como de voz. Crecerá de forma importante el apoyo tecnológico a la consecución del éxito del ataque por la popularización y disponibilidad de estas técnicas y su evidente adecuación. Respecto a ataques como el timo de CEO o similares, la previsión es que estos se multipliquen en un orden de magnitud hasta que las empresas desarrollen y actualicen sus protocolos y mecanismos para luchar contra este problema. Por supuesto, no puede descartarse un incidente importante que afecte a múltiples empresas basado en ataques a la cadena de suministro y, seguro que en los próximos años veremos algún caso con un impacto muy extenso que implique riesgos para un número muy elevado de organizaciones de forma similar al caso Solarwinds del año 20 del siglo en curso”.



CIPHER (A PROSEGUR COMPANY)
Santiago Anaya
Global CTO of xMDR

“Desde la Unidad de Inteligencia X63 de xMDR by Cipher, observamos con creciente preocupación una tendencia alarmante: la seguridad en el uso de la IA, ya sea con modelos LLM propios o mediante plataformas como OpenAI, ChatGPT y LLaMa, se ha convertido en un asunto de suma importancia. Es esencial garantizar que nuestras soluciones

de IA no sean vulneradas, una medida clave para prevenir potenciales catástrofes. El hecho de que la IA esté tan integrada en los procesos críticos de las empresas nos pone en alerta. Además, nos enfrentamos a un incremento de tácticas de extorsión por parte de grupos malintencionados, lo que nos impulsa a estar constantemente actualizados en cuanto a las últimas Técnicas, Tácticas y Procedimientos (TTP)”.



CISCO
Ángel Ortiz
Director de Ciberseguridad en Cisco Iberia

“*Ransomware*, *commodity loaders* y APTs seguirán dominando el panorama de amenazas aunque con cambios significativos (incorporación de *exploits* de día cero, eliminación del pasado troyano en los *commodity loaders*...). Aumentarán también los ataques a dispositivos de red que explotan credenciales débiles o comprometidas y vulnerabilidades conocidas. Los ataques nativos a plataformas en la(s) nube(s) se aprovecharán de las brechas de seguridad en estos entornos. Finalmente, cabe destacar las dos caras de la IA: por un lado permitirá simplificar la labor del analista automatizando múltiples tareas; pero por otro lado, abrirá la puerta a nuevos problemas de seguridad y privacidad permitiendo, por ejemplo, a los atacantes mejorar sus señuelos de ingeniería social en ataques dirigidos”.



COMFORTE
Ricardo Escrivà Ferrer
Iberian Country Manager

“Se anticipa un aumento en la complejidad de las amenazas de ciberseguridad, especialmente con la llegada de la IA generativa. El mal uso de estas tecnologías permitirá crear ataques más sofisticados y generará un riesgo interno en la manipulación de datos. La clave para mitigar estos riesgos radica en proteger y *tokenizar* los datos, preservando así su integridad frente a estas complejas amenazas”.



COMMVAULT
Maite Ramos
Country Manager

“Los ciberdelincuentes utilizarán la IA para atacar. Lo que antes exigía un esfuerzo humano, unos conocimientos y una experiencia técnica considerables, ahora puede hacerse de forma más eficiente con IA. Por eso desde Commvault hemos incorporado IA para ayudar a las empresas a adaptarse a este nuevo panorama y combatir las amenazas utilizando las mismas herramientas que los atacantes”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



CONSIST

Francisco Rosado

Gerente de Productos de Ciberseguridad

“Si bien resulta complejo prever las que más impacto tendrán en 2024, se vislumbra un marcado aumento en el empleo de la Inteligencia Artificial para orquestrar ataques más sofisticados, capaces incluso de evadir los sistemas de seguridad actuales. Este uso de la IA se focalizará principalmente en áreas como la ingeniería social, *phishing*, robo de datos y amenazas a la privacidad. Asimismo, creo que habrá un incremento significativo de los ciberataques dirigidos a la nube, aprovechando tecnologías y plataformas *cloud*-nativas. Por supuesto, persistirán y posiblemente se intensificarán amenazas ya existentes, tales como ataques de *ransomware* a niveles más avanzados, ataques DDoS, entre otros”.

escala. El reto será potenciar el factor humano, utilizando también la IA y las técnicas más avanzadas disponibles”.



CYBERPROOF

Nathaniel Ribco

Cyber Threat Intelligence Leader

virtual. La adición de IA agilizará el adelanto y disponibilidad de estas técnicas exponencialmente”.

“Los conflictos globales actuales influyen en el desarrollo acelerado de técnicas de Guerra cibernética avanzadas, como el uso de *malware* Wiper. Estas técnicas son utilizadas para atacar infraestructura civil crítica con el fin de causar daño a la población, mas allá que en el plano virtual. La adición de IA agilizará el adelanto y disponibilidad de estas técnicas exponencialmente”.



CROWDSTRIKE

Juan Luis Garijo

Director Regional para España y Portugal

“Los puntos ciegos de la Inteligencia Artificial están abriendo la puerta a nuevos riesgos dentro de las empresas y en la sociedad en general. En 2024, CrowdStrike espera que los ciberdelincuentes trasladen sus objetivos hacia los sistemas de IA, con el propósito de atacar a las organizaciones, por un lado, a través de vulnerabilidades en sistemas legítimos y, por otro, aprovechando la falta de gobernanza en el uso de herramientas de IA por parte de los empleados de la organización”.



CYMLULATE

Neftalí Mañes

Lead Solutions Architect Southern Europe

entornos cada vez más amplios”.

“Esperamos una evolución en ataques personalizados que, mediante técnicas de industrialización y herramientas como las IA, puedan implementarse y realizarse a nivel de escala. Estas amenazas parece que se extienden a nuevas áreas, como IoT o cadenas de suministro, obligándonos a enfocarnos en la previsión de las mismas en entornos cada vez más amplios”.



COUNTERCRAFT

David Barroso

Fundador

“Debido a las cada vez más graves tensiones geopolíticas y guerras que existen por el mundo, es posible que empecemos a ver repercusiones directas como daño colateral sobre la sociedad civil. Las infraestructuras críticas de una nación son un objetivo claramente muy atractivo dentro de la escalada de violencia propia de un conflicto. Hasta ahora ha sido una línea roja muy pocas veces cruzada, pero sin duda las probabilidades de que ocurra son ahora mayores”.



DEDGE SECURITY

Rubén Jiménez

Co-Founder & CEO

en este nuevo ecosistema”.

“En 2024, los ataques tradicionales se potenciarán con el uso de IA y se expandirán a entornos emergentes como Web3. Prevemos un notable aumento de amenazas y ciberataques, con un enfoque particular en la cadena de suministro. La gestión del riesgo en el código e infraestructura *blockchain* será esencial para cultivar confianza en este nuevo ecosistema”.



CYBER GURU

Mar Sánchez Caro

Business Development Manager

“Con las herramientas de IA disponibles en el mercado, en 2024 los ataques de *phishing*, *smishing*, *quishing* e ingeniería social serán aún más fáciles, baratos y eficaces para los ciberdelincuentes, por lo que lamentablemente los incidentes aumentarán o serán de mayor



DELINEA

Roger Gallego

Iberia Sales Manager

La ciberresiliencia de las organizaciones será la característica más valiosa”.

“Los ciberdelincuentes utilizarán de forma creativa e intensiva capacidades de Inteligencia Artificial para mejorar ataques de Ingeniería Social. Debemos priorizar una ciber-defensa proactiva con foco en el acceso autorizado a infraestructuras críticas. *Zero Trust* debe integrarse en la estrategia corporativa. La ciberresiliencia de las organizaciones será la característica más valiosa”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



DELOITTE

Nicola Esposito

Socio responsable de Detect and Response

“Esperamos una mayor sofisticación y volumen de ciberataques por el avance de la IA. La situación geopolítica incrementará la actividad de grupos APT haciendo uso de *Zero days* y con infiltraciones y desinformación mediante *deepfakes*. Persisten

los DDoS hacktivistas y suben los ataques a librerías y componentes de la cadena de suministro con impacto en OT/IoT y procesos críticos de negocio”.



DEVO

Emmanuel Roeseler

Director Strategic Accounts EMEA

“La democratización de la IA aumentará el uso malicioso, intensificando ataques sofisticados, rápidos y dirigidos. La presión sobre la ciberseguridad crecerá, exacerbada por limitaciones económicas que dificultarán la modernización de controles.

La geopolítica podría impulsar el cibercrimen en 2024, por ello la colaboración y automatización en ciberseguridad serán vitales ante estos desafíos”.



DIGITEL TS

Ricardo Rodríguez Martín

CISO

“Amenazas muy sofisticadas: evolución de *ransomware* hacia exfiltración de datos previa a cifrado; ingeniería social muy personalizada; IA para suplantación de imágenes y voces; vulnerabilidades *zero-day* y *exploits* de terceros. Hay que seguir fortaleciendo la seguridad. Adopción de SSDLC, metodología de desarrollo, separación de elementos, utilización de MFA, revisión continua con auditorías. Es esencial ir a ecosistemas seguros con estándares europeos, tecnologías descentralizadas y la EUID”.



DXC TECHNOLOGY

Mikel Salazar Peña

Iberia Cybersecurity Country Lead

“La inteligencia artificial y el ML jugarán un papel crucial en los ciberataques en 2024. Prevemos que los ciberdelincuentes utilicen estas tecnologías para automatizar y mejorar sus capacidades, creando cada vez más ataques tanto en sofisticación como en volumen. En un contexto geopolítico complicado la transformación digital no parará de avanzar y las organizaciones abrazarán la IA en sus negocios (*chatbots*...) y darán más pasos a la adopción de la nube que supondrán nuevos vectores de ataque que los ciberdelincuentes aprovecharán para hacer el mayor daño posible y monetizar”.



ELASTIC

María Campos

Regional VP Sales

“La evasión de la defensa y la manipulación (vs. ocultación) ganarán terreno. Los defectos de diseño de OS facilitarán más despliegues de controladores vulnerables BYOVD. MaaS sigue en aumento. Los *pods* de Kubernetes con privilegios altos agravarán la seguridad de contenedor. GAI

mejorará la productividad de los atacantes y ayudará a los más noveles, por ejemplo creando *malware* polimórfico”.



ENTHEC

María Rojo Rivas

CEO

“En 2024 el uso de IA para el diseño de ataques basados en ingeniería social será un factor determinante. Se adoptará y popularizará para elaborar ataques masivos a las pymes, donde el factor humano continuará siendo crítico en este aspecto. Además, se prevé el crecimiento agresivo de

chantajes y ataques a profesionales de empresa *C-Levels* y personas relevantes con uso de IA generativa y de imágenes entrenadas por toda la información filtrada y expuesta de los mismos. La reputación personal comenzará a emerger como un activo a proteger de ataques, de similar importancia a la reputación de marca. Por otro lado, seguirá creciendo el mercado de venta de información sensible en la *Dark Web* y en aplicaciones de chat como Telegram. Un mercado que servirá para alimentar esos ataques elaborados con IA”.



ENTRUST

Rocío Martínez

Regional Director Digital Security

“Aunque la criptografía post-cuántica puede no parecer una prioridad inmediata, su amenaza no debe ser ignorada. En 2024, las organizaciones, especialmente las que manejan datos sensibles, deberán prepararse para los ataques cuánticos ‘*Harvest Now, Decrypt Later*’ y tenerlos en cuenta

para mejorar sus estrategias de ciberseguridad y el impacto en su organización y sus clientes”.



ESET

Josep Albors

Responsable de Investigación y Concienciación

“Por mucho que se hable de ella, salvo excepciones, la inteligencia artificial usada de forma maliciosa está lejos de compararse con amenazas más tradicionales que nos tienen tomada la medida. En 2024, es preferible centrar nuestros esfuerzos en detectar amenazas que usen TTPs conocidos, aunque refinados, e implementar, de una vez por todas, las medidas de seguridad necesarias que tantas veces se han mencionado pero que pocos se preocupan de aplicar en su totalidad”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



EUROCYBCAR
Azucena Hernández
CEO

“Los vehículos conectados que requieren de actualizaciones de software ‘Over The Air’ –OTA/SOTA/FOTA– están expuestos a riesgos que afectan, sobre todo, a la integridad física de los pasajeros y los peatones; es decir que, si el proceso de actualización no es lo suficientemente ciberseguro –como exige por ley la UNECE/R156–, un *cracker* podría interferir dicha comunicación e introducir paquetes con software malicioso con el objetivo de atacar al fabricante, ‘secuestrando’ de forma remota la flota de uno de sus modelos y solicitándole una recompensa para poder liberarlos”.



EVIDEN
Arancha Jiménez
VP - Ciberseguridad Servicios y Productos en Iberia

“Se prevé que los ciberataques se basen en IA generativa, para aumentar la velocidad, principalmente en ataques *spear phishing*, y la capacidad de evasión ante las medidas de detección. Se incrementarán en conflictos geopolíticos con ataques a sectores como telco, energía o defensa. Y también se centrarán en la cadena de suministro, por la falta de visibilidad y alineamiento entre sus integrantes”.



EVOLUTIO
Ricardo Sanz
Director de Ciberseguridad

“2024 se prevé que sea un año electoral sin precedentes a nivel mundial, por lo que se anticipa un aumento de ciberataques relacionados con IA en procesos electorales, ejecutados por actores estatales, grupos extremistas y hacktivistas, empleando tácticas de desinformación y *deepfakes* para manipular opiniones, distorsionando el discurso público e influyendo en los procesos democráticos”.



EXCLUSIVE NETWORKS
José Manuel Medina
Director de Desarrollo de Negocio para Iberia

“2024 se presenta como un año emocionante en términos de ciberseguridad, con la IA en el centro como solución y problema a todos los temas de ciberataques. Ante ‘una nueva era’ del cibercrimen avanzado, la IA se sitúa como una de las grandes transformadoras de las reglas del juego. Se prevé que aumente la sofisticación de los ataques, y estos serán más selectivos, sigilosos, y diseñados para eludir los controles de seguridad más estrictos. Conectividad, ciberseguridad y *cloud* son claves para que las empresas mejoren su competitividad y lo hagan con todas las garantías”.



EY
Jordi Juan Guillem
Socio. Ciberseguridad.
Consultoría Tecnológica

“La creciente dependencia en la tecnología augura ciberataques cada vez más numerosos, sofisticados y con mayor impacto. La inteligencia artificial se utilizará para ataques dirigidos, creando *deepfakes* cada vez más realistas para manipular la opinión pública o robar identidades. Del mismo modo, la expansión del internet de las cosas (IoT) supone un creciente número de dispositivos vulnerables a ataques, con posibles impactos devastadores. Las criptomonedas seguirán siendo el medio de pago preferente para los ciberdelincuentes debido a la dificultad para rastrear su procedencia. Por último, se espera un aumento en la explotación de vulnerabilidades de la cadena de suministro, similar al caso de SolarWinds, que podría llevar el cibercrimen a un nuevo nivel de complejidad y alcance. A pesar de los avances en seguridad, la amenaza siempre está evolucionando, requiriendo una respuesta constante y adaptativa”.



F5 NETWORKS
Francisco Lahoz
Systems Engineer Iberia

“Para 2024 esperamos que las IA generativas (y LLMs) actúen como multiplicador de amenazas: conversaciones con víctimas de *phishing*, *fake accounts*, campañas desinformativas o ataques web con datos “*real-time*”. Veremos arquitecturas complejas, mayor superficie de exposición (asociados al auge del *edge computing*) y una mayor necesidad tecnológica de convergencia de seguridad y observabilidad”.



FACTUM
Patricia Gallo
Sales Director

“En 2024, la suplantación de identidad y el *ransomware* seguirán siendo grandes amenazas para cualquier organización. Los ciberdelincuentes desplegarán tácticas más sofisticadas causando, principalmente, pérdidas económicas inmediatas, exfiltración de datos sensibles, y paradas operativas. Por ello, será más necesario que nunca, implementar una estrategia global de ciberseguridad adaptada a la realidad de cada organización. Esta estrategia debe cubrir el Gobierno de la seguridad, la Identificación y resolución de posibles brechas, la Protección de activos, y dar Respuesta 24x7”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



FASTLY
Daniel Howe
Senior Presales

“Según nuestro reciente Informe Global de Ciberseguridad la preocupación se centra en el *ransomware*, experimentado por el 29% de las empresas, DDoS (28%) y ataques relacionados con software de código abierto (25%), la ingeniería social (22%) y aplicaciones web/API (20%). Además, en 2024 les preocupará especialmente la IA Generativa con fines maliciosos y la brecha en competencias digitales para enfrentar esta amenaza”.



FORCEPOINT
José Bavaresco
Channel Sales Engineer EMEA

“Se prevé *malware* con módulos de Inteligencia Artificial. Los *malwares* incluirán internamente modelos de IA que hará que al infiltrarse puedan cambiar, mutar y adaptarse localmente y, lo mejor, en tiempo real... Esto desafiará a todos los métodos actuales de detección. *Malware* y IA es el nuevo vector de ataque, la resiliencia y la innovación en la ciberseguridad son primordiales para la integridad de los datos de las empresas”.



FORGEROCK (PING IDENTITY)
Alex Laurie
SVP Global Sales Engineering
Ping Identity

“Seremos desafiados como nunca antes, ya que los nombres, rostros y voces de las personas más cercanas se utilizarán para engañarnos. La tecnología *Deepfake* que suplanta la imagen de una persona va a ser una realidad y más difícil de detectar por el consumidor medio. Debemos permanecer vigilantes ante estos fraudes avanzados, que desafiarán nuestro umbral estándar de confianza”.



FORENSIC & SECURITY
Pilar Vila
CEO

“Existen ataques de gran impacto que no son nada complejos y viceversa. La capacidad de resiliencia de una organización determina esto, pero algunos muy básicos pueden generar un nivel de caos total. Como indica el creciente número de CVE publicados cada año, las organizaciones se enfrentan cada vez más a más puntos de falla, esto acompañado de lo que suelen tardar en actualizar/ parchear no ayuda. Una gran amenaza desde hace años es el incremento de los CVEs que ya se reflejó muy claramente en los tipos de ciberataques de 2023. Por otro lado, cada vez son más agresivas las campañas de grupos de *ransomware*. La caída de Blackcat podría ge-

nerar actividades más indiscriminadas ya anunciadas por este grupo y en paralelo, otras organizaciones como LockBit están usando la situación para ampliar su negocio de *ransom as a service*”.



FORTINET
Acacio Martín
VP Sales Iberia

“El CaaS y la IA generativa siguen en auge, potenciando a los actores de amenazas con herramientas más fuertes. Las tácticas antiguas evolucionan y los ciberdelincuentes diversifican objetivos y estrategias, enfocándose en ataques sofisticados, denegación de servicio y extorsión. El *ransomware* se intensifica y se dirige a sectores críticos como salud, finanzas, transporte y servicios públicos para maximizar el impacto y beneficio de sus acciones. Se prevé un aumento de ataques *Zero days*, con la aparición de los *brokers* en la *Dark Web*. Los eventos geopolíticos de 2024 también traerán ciber-sorpresa”.



FRAUDFENSE
Carlos Requena
Director General

“Creo que una amenaza importante es la capacidad de los ciberdelincuentes de adaptar su *Business plan*, reorientando sus objetivos de mercado. Ahora pondrán más foco en suplantación de identidad y gestión de cuentas mulas ya que supera en rentabilidad a los ataques de *ransomware*, con un ROI



FUJITSU ESPAÑA
Javier Pérez García
Head of Cybersecurity

“La IA será el *trending topic*, por mejorar las capacidades de detección y análisis de amenazas, por sus riesgos inherentes, y por los usos fraudulentos de la misma. Además, una tendencia que se consolidará en el 2024 es la hiper-especialización en ciberseguridad alcanzando todos los ámbitos de la ciberseguridad. Desde la amenaza, mercado laboral y por supuesto toda la oferta de servicios”.



GHENOVA
Enrique Cubeiro
Director de Ciberseguridad

“La explosión de las IA, algunas especializadas en la creación de *malware*, pone al alcance de cualquiera herramientas y conocimientos que posibilitan ciberataques sofisticados, lo que a buen seguro va a animar a muchísimas personas (¿millones?) a hacer del uso malicioso del ciberespacio su actividad profesional, convirtiendo a individuos insignificantes en actores relevantes y peligrosos”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



GMV

Javier Osuna

Director de la División de Consultoría y Servicios de Ciberseguridad

“Las tensiones geopolíticas provocarán represalias mediante ataques de DDoS contra la Administración Pública, Infraestructuras Críticas y colaboradores. Los malos optimizarán el uso de la IA en su beneficio mientras los buenos debatirán sobre su moralidad. El *ransomware*, *malware low-cost*, infectará los eslabones más débiles de la cadena de suministro enriqueciendo más al crimen organizado”.



GOOGLE CLOUD

José Carlos Cerezo

Responsable del Área de Seguridad y Cumplimiento de EMEA South

“Prevedemos un aumento en número y sofisticación de las vulnerabilidades de día cero en dispositivos perimetrales y arquitecturas de virtualización; crecimiento de *wiper malware* en el contexto de ataques destructivos asociados a los conflictos globales; tecnologías espaciales (Starlink y otros) como nuevo objetivo para comprometer las infraestructuras; intensificación de ataques a entornos *multi-cloud* e híbridos a través de técnicas que permitan cruzar las fronteras; aprovechamiento de las tecnologías *cloud serverless* que ofrecen mayor escalabilidad; resurgimiento de técnicas ‘antiguas’ que no están documentadas y dificultan su detección; adopción de nuevos lenguajes de programación (Go, Rust, Swift) que facilitan el desarrollo rápido de *malware* de difícil detección; sofisticación de ataques de ingeniería social y operaciones de información utilizando modelos de inteligencia artificial generativa. El uso de la Inteligencia Artificial Generativa como un arma de doble filo; por un lado un potenciador y acelerador de los ataques, aportando una mayor sofisticación y personalización; y por otro, un elemento que ayudará a evolucionar las defensas de las organizaciones, impulsando la forma en que sintetizan grandes cantidades de datos y contextualizan inteligencia, reduciendo la carga de trabajo, abordando la saturación de amenazas y cerrando la brecha de talento”.



GRUPO TRC

Emilio Rico

Security Advisor

“Nuestra dependencia de la tecnología es tan grande, que lo peor que nos puede pasar es perder nuestra identidad digital. Un escenario distópico de enorme impacto sería un ataque donde se alteren los registros de nuestros datos y se asignen a otras personas, donde los sanos enfermen y los enfermos parezcan curados, los drones sean gente honrada y los demás criminales, donde perdamos los lazos familiares o cambie la titularidad de nuestros bienes y propiedades”.



HISPASEC

Miguel Manteca

CEO

“En 2024 observaremos resultados avanzados de los entrenamientos donde la IA será un agente catalizador en ataque y defensa ante *deep fakes*, *phishings* e ingeniería social. Asistiremos a ataques a infraestructuras 5G, *cloud*, *software* CI/CD y dispositivos IoT, con gran impacto, especialmente en procesos electorales y Juegos Olímpicos. Y quizás presenciemos cibersecuestros de vehículos inteligentes”.



HORNETSECURITY

Félix de la Fuente

Country Manager

“Como cualquier otro negocio, los grupos detrás de los ataques de ciberseguridad buscan el máximo beneficio posible de cada evento. Tienen además nuevas herramientas para mejorar y elaborar sus intentos: la IA es un ejemplo. Las empresas nos tenemos que preocupar en adecuar las soluciones que protegen nuestro perímetro con herramientas equivalentes a aquellas que usan los atacantes. Los intentos de romper el perímetro seguirán existiendo, y cada vez serán más sofisticados. A pesar de todas las medidas implantadas, el ataque puede ser exitoso en algún momento, es imprescindible tener copias de seguridad de los datos de forma que la recuperación ante un posible *ransomware*, no afecte o afecte lo menos posible al negocio de la compañía”.



IC CONSULTING

Óscar González

Regional Director Iberia

“Si hace dos o tres años el foco estuvo en los ciberataques contra la identidad y el año pasado fue el de la IA, para 2024 esperamos un aumento del riesgo de amenazas contra la identidad impulsadas por la IA, especialmente ataques selectivos contra individuos o grupos de individuos. La disponibilidad de una cantidad ingente de datos comprometidos y la potencia de la IA generativa junto con el uso de *large language models* (LLM) solo hacen que aumentar dicho riesgo”.



IMMERSIVE LABS

James Hadley

CEO

“En 2024 disminuirá el miedo a la GenAI a medida que las organizaciones comprendan mejor sus riesgos y beneficios siendo capaces de probar y justificar el nivel de ciberresiliencia. Los *ransomware* seguirán siendo una amenaza y se utilizarán nuevas técnicas para evadir la



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024

detección y explotar las vulnerabilidades. Por eso mismo, se prevé un foco en la capacitación de las personas, y en crear y testear estrategias de respuesta eficaces en lugar de limitarnos a la detección”.



INETUM
Alberto Martín de los Santos
Director de Ciberseguridad

“2024 seguirá siendo un año con foco en la cadena de suministro, centrado en el software y código de terceros. Desde un punto de vista de impacto, las principales amenazas se centrarán en los sectores más sensibles como son salud, AAPP e infraestructuras críticas. Además, la IA ayudará a los cibercriminales a sofisticar sus ataques con campañas más potentes pero más sencillas de realizar”.

Además, la IA ayudará a los cibercriminales a sofisticar sus ataques con campañas más potentes pero más sencillas de realizar”.



INNOTECH SECURITY, part of ACCENTURE
Félix Muñoz
CEO

“Habrà que prestar atención a la inteligencia artificial (IA) y sus primeras amenazas de suplantación de identidad; al mantenimiento de los ataques de *ransomware* (y la doble y triple extorsión), los ataques de denegación de servicio (DDoS) y a la cadena de suministro. La escasez de profesionales de ciberseguridad será otro de los riesgos a tener en cuenta. En defensa, deberemos enfocarnos en la automatización”.

La escasez de profesionales de ciberseguridad será otro de los riesgos a tener en cuenta. En defensa, deberemos enfocarnos en la automatización”.



INTEGRITY360
Manuel Fernández
Director para España, Portugal y Latam

“Percibimos una concentración de foco en la explotación de vulnerabilidades en los APIs, así como en los *scripts* de las páginas web. Posiblemente comenzaremos a ver

debilidades en ciertas pruebas de autenticación biométricas, en las que hemos confiado hasta ahora, lo que impulsará una nueva generación de factores de autenticación. Seguimos viendo todo tipo de infraestructuras críticas como una prioridad en defensa, tanto lógica como físicamente. Resaltaríamos que la falta de madurez generalizada en la pronta respuesta a incidentes de muchas de las empresas provoca que los daños tras un ataque se agraven”.



INTERNET SECURITY AUDITORS
Daniel Fernández Bleda
Director Comercial

“Durante este año, en el que más de la mitad de la población del planeta pasará por procesos electorales, unos de los mayores riesgos globales será la de la desinformación mediante IA en las múltiples vertientes de su aplicación y usos para modificar, alterar o generar tendencias de opinión. Combinando las amenazas regionales, producto del creciente belicismo, hará que pescadores voraces saquen provecho de esta situación”.



IPM, A RICOH COMPANY
David López Pacheco
Cybersecurity Product Specialist

“En 2023 vimos como la IA estuvo siendo utilizada con fines maliciosos, como ejemplo WormGPT. En este 2024 se espera que proliferen este tipo de IA, que aunque sabemos que todavía son un ‘bebé’ ya hemos visto de lo que son capaces. Las empresas que basen su estrategia de ciberseguridad en modelos *Zero Trust* con mejoras en la gestión de identidades, gestión de vulnerabilidades y de Ciberresiliencia, estarán mejor preparadas para combatir este tipo de amenazas”.



ISDEFE
José Antonio Pérez Rodríguez
Gerente de Seguridad de la Información

“Los ataques más complejos y de gran impacto tendrán como origen el contexto geopolítico y social actual. Sus objetivos seguirán siendo los organismos de Estados que han proporcionado ayuda al bando contrario, y en especial los principales eventos de 2024 (elecciones al Parlamento Europeo en junio, Eurocopa en Alemania en julio, Juegos Olímpicos de París en agosto y, sobre todo, las elecciones presidenciales en Estados Unidos de noviembre). Es probable que los de mayor impacto tratarán de afectar a la disponibilidad mediante ataques de DDoS a través de *botnets* empleando código dañino orientado a IoT, y se verá una orientación del *ransomware* hacia sectores más críticos. En lo que respecta a los ataques más complejos, podrían ser los que se orienten hacia la cadena de suministro para afectar a los sectores críticos y a los procesos electorales mencionados”.



KASPERSKY
Alfonso Ramírez
Director General de Kaspersky Iberia

“La Inteligencia Artificial tendrá un papel fundamental, especialmente en ataques de suplantación de identidad y *deepfake*. Además, prevemos un aumento en estafas relacionadas con VPN, los sistemas de pago directo y un incremento de los paquetes de código abierto con *backdoors*. También habrá que prestar atención a la vulnerabilidad de *smartphones* y los riesgos en la cadena de suministro”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



KPMG

Guillermo González

Director en el Área de Technology Risk y Ciberseguridad

“Habrá un incremento significativo de ataques dirigidos mediante nuevas variantes de *malware* y *ransomware*, que aprovecharán la IA y el aprendizaje automático como herramientas para potenciar sus capacidades de infección y evasión. Los

atacantes dispondrán de herramientas cada vez más sofisticadas para ejecutar enfoques inteligentes y personalizados en la ingeniería social, incluyendo ataques como *BEC*, *vishing*, *smishing*, *deepfake*, entre otros. Se requerirá una atención especial al aumento de ataques a la cadena de suministro. Siguiendo la tendencia observada en 2023, se anticipa un crecimiento continuo en el número de vulnerabilidades *zero-day*, *one-day* y publicación de CVEs. Asimismo, se prevé un aumento en la presencia de grupos conocidos como ‘zero-day brokers’, quienes comercializarán estos *exploits* al mejor postor”.



LEET SECURITY

Antonio Ramos

Executive Manager

“Los ataques siempre persiguen las iniciativas de éxito por lo que en 2024 cabría esperar: un incremento de los ataques a infraestructuras virtualizadas sin importar que estén gestionadas por terceros (SaaS, APIs e hipervisores). Además, la IA seguirá dominando las conversaciones y veremos mejores *phishings* y estafas, así como un mayor foco en los *end points* y resto de *gadgets* con potencial de rentabilidad”.



LIDERA / V-VALLEY

Dámaso Ramos

Business Unit Manager Cybersecurity Services

“En 2024 seguiremos hablando de Inteligencia Artificial de manera predominante. Será clave evolucionar el uso de la IA en las contramedidas de seguridad a la misma velocidad que la evolucionan los cibercriminales. Además, será importante estar atentos al uso de la IA y el perfeccionamiento del

deepfake como herramientas de ingeniería social. Los ataques a la cadena de suministro y el *ransomware* seguirán teniendo relevancia en este año”.



LIVEACTION

Carlos Ferro

SVP & GM International Region

“Aumentará en la sofisticación de los ataques de suplantación de identidad, *phishing* y *ransomware*, destacando el papel de las herramientas de IA, que se está utilizando para automatizar el proceso de recolección de datos de la víctima

y localizar mensajes en diversos idiomas, elevando la complejidad de los ciberataques. La migración hacia la nube y la transformación digital han ampliado tanto la cantidad como la sofisticación de estos ataques. Particularmente preocupante es el fenómeno conocido como ‘fatiga de alerta de ciberseguridad’. A pesar de la abundancia de datos recopilados, enfrentamos un desafío considerable al procesarlos y convertirlos en información accionable. En este contexto, la adopción de herramientas de observabilidad y la aplicación de IA para analizar patrones de actividad en la red y detectar comportamientos anómalos se tornan cruciales para fortalecer nuestra postura de seguridad”.



LOGICALIS SPAIN

Miguel Ángel Cano

Security Presales Consultant

“Con el auge de la IA, habrá un incremento de las *deepfakes* y las campañas de *phishing*, que permitirá a los delincuentes hacerse con credenciales y acceso a entornos críticos e información confidencial. Mediante soluciones

creadas a partir de IA Generativa, los ciberdelincuentes encontrarán vulnerabilidades con mayor efectividad y velocidad en los sistemas de las compañías”.



LOGALTY GROUP

Sergio Barbero

CISO

“Sin duda, 2024 va a ser un año marcado por las cada vez más omnipresentes soluciones de IA en todos los ámbitos de las empresas, lo cual supone un gran reto para los equipos de ciberseguridad. Además, la falta

de profesionales especializados seguirá siendo una necesidad inherente a un sector en continua evolución, que precisará unos mayores niveles de capacitación y conocimiento”.



MANAGEENGINE

Mathivanan Venkatachalam

Vice Presidente

“Los grandes modelos de lenguaje han facilitado la elaboración de campañas de ingeniería social. Las amenazas avanzadas a menudo eluden las medidas de seguridad tradicionales y sirven como puerta de entrada a las

filtraciones de datos. En 2024 se producirá un aumento en la frecuencia y gravedad de este tipo de ataques, lo que los convertirá en un gran desafío para las organizaciones”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



MASTERCARD

Rigo van den Broeck

Vicepresidente ejecutivo de Innovación de Productos de Ciberseguridad

“La ciberseguridad sigue siendo un tema crítico para cualquier negocio en 2024. A medida que las amenazas evolucionan, los líderes empresariales están dispuestos a explorar nuevas tecnologías para proteger su reputación y la de sus clientes.

Es vital que las empresas continúen invirtiendo y estimulando la innovación en este campo para mitigar los riesgos en sus cadenas de suministro y colaborar para proteger nuestro futuro digital”.



MYCLOUDDOOR

Miguel Monedero

Global Information Security Director

“Las nuevas tácticas de *ransomware* seguirán asolando a las empresas. El avance de las tecnologías de IA permitirá a los atacantes crear audio, vídeo e imágenes falsas más convincentes, para llevar a cabo campañas de ingeniería social y desinformación a gran escala. Los actores se dirigirán a entornos cloud para ganar persistencia y moverse lateralmente entre los entornos de las víctimas”.



MDTEL TELECOMUNICACIONES

Francisco Cuesta

Director General Adjunto / CISO MD Securit

“De la inestabilidad vírica a la generada por los conflictos bélicos y la guerra fría tecnológica entre naciones o grupos de países afines. Lo único constante es el cambio y la complejidad que nosotros mismos generamos. Las amenazas más complejas y de mayor impacto harán uso de la IA aplicada al *phishing*, generación de información falsa y código dañino entre otras posibilidades. Serán relevantes las amenazas sobre la miríada de dispositivos IoT que nos rodean, así como las que se ciernen sobre redes industriales, todavía lejos de encontrarse gestionadas correctamente. Siendo por lo tanto muy necesaria la gestión continua del riesgo de estas superficies de ataque cada vez más difíciles de controlar”.



NETSKOPE

Miguel Ángel Martos

Country Manager para Iberia

“A medida que la IA se vuelva más sofisticada, los ciberdelincuentes la explotan para lanzar ataques más complejos y efectivos como son generación de *phishing* realista y *deepfakes* para desinformar, abuso de *chatbots* de IA generativa para distribuir *malware*, así como la fuga de datos e información confidencial. La tecnología SSE/SASE será sin duda una de las más demandadas en este 2024”.



MICROSOFT

Raquel Hernández

Directora de Soluciones de Seguridad de Microsoft España

“El uso del cibercrimen como servicio sigue y seguirá creciendo. Los ataques de *ransomware* aumentaron de 3.000 millones en 2022 a 30.000 millones en 2023. La IA es un componente crítico para crear soluciones efectivas de ciberdefensa y ello requiere cantidades inmensas de datos. Microsoft analiza 65 billones de señales al día en nuestra plataforma que nos permite proteger el 99% de los ciberataques”.



NOVARED

José Miguel Lavín

Director Comercial

“Para 2024, se espera un mayor uso de IA y ML en ciberseguridad, más seguridad en IoT, evolución de ataques de *phishing*, relevancia de la seguridad móvil, expansión del trabajo remoto, y el auge de la computación cuántica. También se prevé un enfoque en la seguridad *Zero Trust* y el uso de *blockchain*. Como siempre, las soluciones de seguridad avanzada en múltiples capas, así como la formación y concienciación de usuarios, seguirán siendo fundamentales”.



MNEMO

Eva Moya Losada

Directora de Inteligencia

“Los avances legislativos sobre ciberseguridad en la UE se vuelven más estrictos a partir de 2024, señalando como últimos responsables de las medidas adoptadas a los Consejos de Administración y la Dirección General. Se potencian los automatismos y el uso de la IA abriendo escenarios para nuevas vulnerabilidades Oday. Las IA generativas intensificarán el peligro de la ingeniería social”.



OKTA

Vitali Siciliano

Director Técnico Iberia

“Los problemas relacionados con la identidad siguen siendo la causa principal de brechas de seguridad en las empresas. Tenemos que ir al peldaño más básico: los seres humanos. Con el crecimiento de la IA, las técnicas de Ingeniería social, los ataques de *phishing*, *Account Takeover* y AITM van a ser más reales y exitosos en 2024. Otra dirección de ataques va a ser por la explotación de las APIs corporativas”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



OMADA

Jorge Sendra
Country Manager para Iberia

“En 2024 la Identidad Digital va a volver a ser la clave para la ciberseguridad. Más del 80% de los ciberataques en sus diferentes formas (*ransomware*, *malware*, *spoofing*, etc.) estarán basados en dos factores clave de riesgo; el robo de credenciales y el exceso de privilegios. Los paradigmas como *Zero Trust* sólo serán efectivos teniendo visibilidad, control y gestión del riesgo de la identidad”.



ONESEQ (by Alhambra)

José María Ochoa
Cybersecurity Manager

“Creemos que vamos a encontrar mayor capacitación y mejora sustancial en las campañas volumétricas de *phishing*, con sus variantes en voz y SMS, acercándose la calidad de los actuales ataques dirigidos. Sin olvidar que esperamos métodos y ataques más sofisticados sobre la usurpación de identidad, incluyendo técnicas para doblegar el 2FA, MFA, etc.”



ONUM

Pedro Castillo
Fundador y CEO

“El problema es que ahora tenemos muchos datos, pero no necesariamente mucha información y entre tanto ruido, ser capaces de buscar las señales se convierte en complicado. Más aun tener un mínimo control sobre qué datos generamos y dónde terminan esos datos. La irrupción en nuestras vidas de la IA, hace que tengamos un nuevo chico en el bloque jugando dos roles: Un (otro) gran generador de datos y un tamizador de datos. Sobra decir que ambas cosas las pueden (las van) a usar los malos para comprometer nuestros sistemas de una forma más automática que nunca”.



ONE eSECURITY

Toño Díaz
Responsable de Respuesta a Incidentes y Forense Digital

“Para 2024, se prevén ataques de *ransomware* más complejos y personalizados, explotando vulnerabilidades en software corporativo común. La ingeniería social, potenciada por IA, presentará retos únicos en *phishing* y manipulación de datos. Además, el aumento en el uso indebido de la IA para generar *malware* y la resurgencia de dispositivos USB como vectores de ataque destacan la necesidad de enfoques proactivos en ciberseguridad”.



OPENTEXT SECURITY

Ramsés Gallego
Chief Technology Officer

“La ‘revolución IA’ se va a aplicar de manera masiva. Nuestras herramientas de inteligencia de amenazas perciben un aumento generalizado en ataques desatendidos y automatizados, incluso con variantes en función del entorno. Esa ‘IA en todas partes’ se aplicará también a la facilidad para suplantar identidades y realizar ataques más efectivos, eficientes y ¿definitivos?”.



OUTPOST24

Víctor Acín
Labs Manager

“Los grupos de *ransomware* exploran nuevas formas de distribuir datos robados, el uso de servicios *peer-to-peer*, además ganan prevalencia las herramientas maliciosas impulsadas por inteligencia artificial. Por último, los ataques a cadenas de suministro seguirán aumentando, aprovechando la externalización de soluciones empresariales y la consolidación de proveedores.”



PALO ALTO NETWORKS

Marc Sarriás
Director General para España y Portugal

“La AI seguirá estando en primera línea como área disruptiva y transformadora, tanto para las empresas como para los actores de amenazas. Los atacantes están respondiendo con técnicas más sofisticadas, aprovechando los modelos de grandes lenguajes (LLM) y la IA generativa para mejorar los correos-e de *phishing* selectivo, combinándolos con *deepfake* y otros ataques habilitados por IA para aumentar las tasas de clic. Además, la proliferación de la IA generativa aplicada a la ingeniería de software conducirá a un pico de software autodesarrollado con errores y a una aceleración de los ataques contra esas aplicaciones. Los CISO tendrán que aprovechar las plataformas habilitadas por IA para reducir la complejidad y aumentar la eficacia de la seguridad para ir un paso por delante de los actores de amenazas”.



PwC ESPAÑA

César Tascón
Socio en Business Security Solutions

“Para este año, nuestras previsiones se centran en dos aspectos: Por un lado, ataques enfocados a dispositivos ‘inteligentes’ dada la gran proliferación y distribución de estos, en muchos casos sin las medidas de seguridad necesarias. Por otro, escenarios de abuso de herramientas de Inteligencia Artificial para fraude y ataques de ingeniería social más sofisticados”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



QUALYS

Sergio Pedroche

Country Manager España y Portugal

“En 2024, la IA seguirá madurando y abriéndose camino como una potente herramienta tanto para la protección y prevención, así como para acelerar la creación de *malware* y la diversificación de los ataques. También gracias a la IA, los atacantes contarán con mayor automatización y velocidad

para el desarrollo, generalizando aún más la creación de software malicioso. El fraude y la suplantación de identidad con el apoyo de estas herramientas serán más difíciles de detectar y prevenir. La explotación de vulnerabilidades cada vez es más rápida y agresiva, así como la continua expansión de la superficie de ataque, lo que propiciará que la gestión del riesgo sea la clave para cualquier negocio, aunque para ello lo primero es poder medir y contextualizar en tiempo real dicho riesgo”.



SIA Icasys An Indra Company

Roberto Pérez García

Head of Cybersecurity Services & Solutions Business

“Este año estará marcado por: el incremento de ciberataques y *phishings* potenciados con IA generativa, y a la cadena de suministro; el aumento de los incidentes y brechas de seguridad en entornos cloud, sistemas de control industrial, dispositivos IoT y redes 5G, con una motivación política o social mayor; las tácticas y técnicas cada vez más complejas: IA y computación cuántica. Todo ello en un contexto con compañías con más capacidades de inteligencia de amenazas, automatización y orquestación”.



RECORDED FUTURE

Pablo Valenzuela

Principal Sales Engineer

“Los actores han estado probando las IAs para diversos procesos, dando paso a una tendencia para este 2024: Podremos ver que tácticas como *ishing*, creación de videos y shorts de desinformación, o la mejora en la creación de *malware* para una exfiltración más rápida partiendo del robo de credenciales. Este año debemos hacer foco en la automatización y monitorización de presencia *online*”.



SIEMENS

Pedro Martín Giral

Head of Cyber Defense Center

“Los ataques más complejos serán los que afecten a las tecnologías IT de infraestructuras críticas, como agua, energía, etc. Tampoco nos podemos olvidar de los ataques que sean capaces de parar líneas de producción de componentes de fabricación de gran impacto, como pueden ser los semiconductores. La detección y respuesta de incidentes en entornos industriales será clave para evitarlos”.



SAILPOINT

Elena Cerrada

Country Manager Spain & Portugal

“Ya estamos empezando a ver un aumento en los ciberataques altamente dirigidos, basados en investigaciones detalladas sobre individuos y empresas, con herramientas más sofisticadas que exigirán a las empresas este 2024 elevar la robustez de su seguridad y mantenerla en constante evolución, con la identidad como gran protagonista”.



S21SEC

Igor Unanue

CTO

“La continuidad de los conflictos geopolíticos, así como la sofisticación de los ataques, la evolución de la IA y el auge de los *infostealers* incrementará el riesgo de los ciberataques a nivel global en 2024. Para hacer frente a estos riesgos, implementaremos soluciones de seguridad más eficaces como las tecnologías SSE y SASE, que marcarán un antes y un después en la detección y respuesta de las amenazas”.



S2 GRUPO

Óscar Navarro

Director del Área de Industrial

“Durante el último cuatrimestre de 2023 observamos un incremento en el número de ataques contra sistemas ciberfísicos. Si bien en algunos casos estas acciones fueron sido reivindicadas por grupos hacktivistas, siendo ataques de oportunidad y con impacto limitado, en otros casos hay detrás

organizaciones con un nivel de conocimiento y recursos. Es previsible que esta tendencia se mantenga durante 2024”.



SECURITY SCORECARD

Jose Ferreira da Costa

Vicepresidente Iberia y Latam

“En 2024, se prevé la consolidación de las regulaciones de ciberseguridad DORA y NIS2 en la UE. Buscarán reforzar la resiliencia financiera digital, imponiendo altos estándares de seguridad, resguardando infraestructuras críticas y fomentando la notificación de incidentes. La complejidad creciente en la gestión de riesgos en la cadena de suministro digital será un desafío clave”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



SMART HC
Ignacio Arrese
CEO

“Para este 2024 marcarán el curso dos aspectos muy relevantes. Por un lado, debido a los conflictos bélicos en el mundo y la proliferación de los estados nación, prevemos un aumento de ataques tipo DDoS y sobre todo de

desinformación. Y por otro, con la espectacular proliferación de la IA, veremos un aumento de la capacidad de ataque, tanto por grupos de ciberdelincuencia conocidos usando y aprovechando los agujeros que irán dejando nuevos aspectos como el lenguaje LLM, como por gente sin experiencia para ataques más pequeños que querrán aprovechar las capacidades de generación de herramientas de *hacking*. Esto nos lleva a tener en cuenta la lucha contra la desinformación, ya que veremos una proliferación de técnicas orientadas al engaño, no solo phishing, con el uso de IA en métodos ya conocidos como el *vishing* o el mayor uso de *deep fakes*”.



SOFISTIC CYBERSECURITY
Fernando Ramírez
Country Manager

“En los últimos cuatro años, hemos hablado sobre la importancia de la seguridad en dispositivos móviles, el riesgo del *ransomware* bajo el amparo de las criptomonedas, la necesidad de una correcta gestión de la ciber-

seguridad ante las vulnerabilidades *0-day* y de lo que trae consigo la IA, como arma en la fase de infección de un *malware*, para los ciberdelincuentes. Si unimos todas ellas, con la potencia de la IA, los atacantes podrían diseñar un *malware* que explote una vulnerabilidad no parcheada, permitiendo la exfiltración de información personal de nuestros móviles. Viendo que, cada vez, los ataques informáticos tienen mayor importancia y sofisticación tampoco habría que descartar uno a gran escala que exponga la información personal de millones de usuarios”.



SONICWALL
Sergio Martínez
Iberia Regional Manager

“Los ataques serán más virulentos y focalizados, con una secuencia parecida a ésta: robo de credenciales, movimientos laterales, consecución de cuentas privilegiadas, desactivación de copias de seguridad, robo de da-

tos sensibles y, finalmente, cifrado de servidores críticos. Y la guinda: el chantaje final, con los tres vectores del secuestro: cuentas, datos y cifrado”.



SOPHOS
Ricardo Maté
Regional Vicepresident South EMEA

“El robo de credenciales, por la proliferación/profesionalización de los IAB's (*Initial Access Brokers*) y la explotación de vulnerabilidades en equipos conectados a internet. Esto no es nuevo, pero probablemente seguirán siendo las dos razones principales por las que una

organización se vea comprometida. Vemos que los delincuentes se centran en formas de eludir la autenticación de doble factor a medida que aumenta su adopción. Esto incluye una mezcla de servidores proxy maliciosos, ataques de ingeniería social, robo de *cookies* y ataques de fuerza bruta”.



STORMSHIELD
Borja Pérez
Country Manager

“Esperamos una continuidad en el tipo de ataques, con un incremento de aquellos promovidos por Estados debido a la compleja situación geopolítica. Como novedades, más allá de los ataques generados por IAs, creo que veremos ataques dirigidos contra IAs. Ataques

que “envenenen” los conjuntos de datos utilizados por una IA con el objetivo de inutilizarla o de que dé resultados que aporten algún beneficio al atacante”.



SUSE
Gustavo Varela
Solutions Architect

“La extorsión con *ransomware*, *cryptojacking*, robo de datos o la interrupción del servicio seguirán siendo utilizados contra los entornos virtualizados basados en contenedores, tanto en nubes privadas como públicas. La reciente vulnerabilidad de *man in the middle* en Kuber-

netes es solo un ejemplo de los posibles *exploits* basados en tecnología de contenedores que se espera proliferen en los próximos meses y años”.



TARLOGIC
Jessica Cohen
Directora de Ciberinteligencia

“Se perpetuarán los ciberataques tradicionales, como son los basados en técnicas de ingeniería social con fines de fraude, que seguirán evidenciando una alta capacidad de éxito apoyados, entre otros, en los avances en IA generativa y en la arrolladora entrada, en el

terreno de juego, de actores con conocimientos técnicos limitados de la mano de soluciones *as a Service*”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



TD-SYNNEX

Nicanor Pulido

Technical Presales Consultant Security

“2024 será el año en que veremos ciberataques asistidos por Inteligencia Artificial a gran escala. La productividad de los *hackers* maliciosos se incrementará con el uso de estas herramientas y las compañías deben prepararse para ello, poniendo al día sus políticas de ciberseguridad e invirtiendo en las áreas de mayor riesgo”.



TEHTRIS

Pedro Morcillo

Country Manager Spain

“Como dice Tehtris, ‘*Face to unpredictable*’ (contra lo impredecible). Aún así nuestra inteligencia detecta posibles ataques contra infraestructuras críticas y la explotación inmediata de vulnerabilidades mediante inteligencia artificial. El ataque a servicios básicos del ciudadano va a sufrir un incremento. Además, la velocidad de remediación, cuenta. Sin IA en tu protección eres vulnerable”.



TELDAT

Ricardo Martínez Sancho

Sales Manager Cybersecurity

“Las amenazas cibernéticas en 2024 incluirán ataques avanzados de *ransomware*, *exploits* de vulnerabilidades críticas y el aumento de la inteligencia artificial en ciberataques. Se incrementarán los ataques a infraestructuras críticas y la IoT será un punto de vulnerabilidad importante y su protección podrá impulsar innovaciones en respuesta, prevención y colaboración global”.



TELFÓNICA TECH

Sergio de los Santos

Director del Área de Innovación y Laboratorio

“El *ransomware* sigue siendo lucrativo, y continuará como la piedra angular del cibercrimen. Existirán menos bandas, mejor organizadas, perpetrando menos robos a todo tipo de empresas, pero más dañinos tanto económica como socialmente (infraestructuras críticas, OT...). Veo un empate: la IA les ayudará a crear mejor código, pero a los analistas también a analizarlo más eficientemente”.



THALES DATA SECURITY

Alfonso Martínez

Responsable para España y Portugal

“La soberanía digital va a plantear nuevas preguntas a los CIOs sobre su estrategia de nube, gobierno y gestión de riesgos. Garantizar que los datos confidenciales no caigan en manos de una entidad extranjera sin permiso expreso, será el principal reto. Mantener el control sobre el cifrado y el acceso a sus datos será el caballo de batalla para las administraciones y empresas”.



TRANXFER

Eli Bernal

Global Sales Director & Innovation

“En 2024, los ciberataques serán más sofisticados. La inteligencia artificial se usará para crear engaños convincentes, y los delincuentes aprovecharán herramientas de IA asequibles, focalizándose en productos desactualizados. Proteger los canales de entrada y salida de archivos y contenidos y concienciar al usuario seguirá siendo el foco de los CISOs”.



TRELLIX

David Baldomero

Senior Systems Engineer

“La IA generativa avanzada y el regreso de *Script Kiddies*: la creciente disponibilidad de herramientas avanzadas de IA generativa y su potencial para ser utilizadas de forma maliciosa no tiene precedentes. Si bien muchos se utilizan para hacernos la vida más fácil, los que se están desarrollando para la web oscura no cuentan con mecanismos de seguridad, lo que, más que nunca, que actores sin capacitación creen ataques sofisticados”.



VARONIS

Julián Domínguez

Iberia Sales Team Lead

“En 2024 veremos como el teletrabajo, la IA y ChatGPT cambiarán el uso de los datos. La situación geopolítica mundial asentará cierta incertidumbre económica e incluso cierta recesión. Esto generará el aumento de ciberamenazas. El reto de las empresas será garantizar la continuidad de negocio. La automatización y la precisión en la detección de amenazas será más importante que nunca”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



VECTRA
Eutimio Fernández
Country Manager

“Los ciberataques en 2024 van a seguir una estela parecida a la del año pasado, aunque con más intensidad. Hoy tenemos más guerras y los ataques entre estados y el espionaje se están incrementando, así como los dirigidos a la cadena de suministro. El uso masivo de la IA en todas partes va a permitir automatizar aún más este tipo de actividad, digamos que el ‘copilot’ está también en el lado de los atacantes. Las tácticas y técnicas no van a variar mucho, pero serán más creativas para ser capaces de evadir las capas de seguridad actuales (más avanzadas)”.



VEEAM
Santiago Campuzano
Country Manager

“Los ataques de *ransomware* son cada vez más graves. Para 2024 se prevé un aumento en el valor de los rescates; pero cada vez menos organizaciones accederán a pagar por ellos, por lo que veremos una disminución en el número de ataques. El gran desafío para las empresas es la anticipación ante las amenazas, por lo que la capacidad de adaptación y actualización tecnológica serán claves para combatirlos. A día de hoy es importante la seguridad proactiva, pero con el riesgo que un ataque cause daño, lo realmente relevante es tener la capacidad de mantener la Continuidad de Negocio”.



V-VALLEY
David Gasca
Sales & Marketing Manager Cybersecurity

“Vemos que la incertidumbre global que hay está afectando a inversión que hacen las empresas, incluyendo la ciberseguridad. Con mayor rotación de personal, una mala gestión de identidades de manera corporativa es la puerta de entrada a ataques indiscriminados o dirigidos. También la inteligencia conversacional mejorará ataques que hasta ahora podían ser fáciles de detectar”.



WATCHGUARD
Miguel Carrero
Vicepresidente Security Service Providers & Strategic Accounts

“Veremos sofisticados trucos de ingeniería maliciosos dirigidos a grandes modelos de lenguaje (LLM), *vishers* que escalan sus operaciones maliciosas con *chatbots* de voz basados en IA, *hacks* en modernos auriculares VR/MR y otros relacionados con el uso de códigos QR. Entre los ci-

berataques de más impacto, nuevos *ransomware* con gran impacto operacional y reputacional, ejecutados principalmente mediante el robo de credenciales. De ahí que la gestión de la identidad con soluciones MFA sea crítica. En este contexto, las amenazas emergentes dirigidas a empresas y particulares serán aún más intensas, complicadas y difíciles de gestionar. Con la feroz competencia por el talento en ciberseguridad, la necesidad de MSP, seguridad unificada y plataformas automatizadas para reforzar la ciberseguridad y proteger a las organizaciones del panorama de amenazas en constante evolución nunca ha sido mayor”.



WESTCON
Iván Rodrigo
Director de Preventa España

“Este año, se espera un aumento en los ataques impulsados por inteligencia artificial. Estas tecnologías intentarán evadir sistemas biométricos y crear contenido fraudulento, lo que llevará a campañas de *phishing* más sofisticadas. El uso de la IA plantea desafíos para la seguridad digital, haciendo necesaria la implementación de medidas proactivas y educación en materia de ciberseguridad”.



WISE SECURITY GLOBAL
Domingo Cardona
Senior Managing Director

“En 2024 la identidad digital enfrenta serios riesgos por ciberataques. *Ransomware* sofisticado y la ingeniería social amenazan la integridad personal y empresarial. La creciente red IoT y el uso de IA en ataques agravan peligros para la autenticación y la confidencialidad. Es vital implementar robustas medidas de seguridad para con la mejora continua de la gestión de identidades”.



XAUEN.io
Santiago Moral
Consejero Delegado

“Apostamos por un *Black Swan* real utilizando los últimos avances de la Inteligencia Artificial. Puede ser caso único tipo el incidente de IFX Networks, o como un ataque de efectos masivos y globales en el mundo, como WannaCry. Posiblemente ni los delincuentes que están ya invirtiendo en estos *Black Swan* sepan si van a poder conseguirlo este año, o tendremos que esperar algo más para verlo”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



XM CYBER

Raúl Pérez
Director Técnico

“La ciberseguridad va a seguir en constante cambio. Las empresas punteras se centrarán en lograr más con menos herramientas y priorizan medidas de seguridad impactantes, en lugar de métricas superficiales. Los ataques a la nube (basados en la identidad) exigirán una

vigilancia cada vez mayor, y la IA se utilizará cada vez más para imitar a los individuos mediante la ingeniería social. Se ampliará la formación en habilidades cibernéticas, mientras que la consolidación de herramientas fomentará la colaboración”.



XYGENY

Luis Rodríguez
CTO

“Vamos a asistir a intrusiones de gran impacto en las infraestructuras para construcción de fabricantes de software. Se popularizará el uso de IA para reconocimiento, *phishing* convincente, y creación de *malware*. Por el lado del bien, se desarrollarán iniciativas para

soportar el principio de ‘seguridad por diseño’, y contemplaremos una mayor carga normativa sobre los hombros de los fabricantes del software”.



ZEROLYNX

Juan Antonio Calles
Chief Executive Officer

“En 2024, la ciberseguridad estará ligada a la palabra IA. Malos y buenos comenzaremos a hacer uso de ellas de forma más activa. Es obvio que continuarán las amenazas avanzadas, los ataques a la nube y a la identidad digital, pero solo podremos afrontarlos de forma efectiva si logramos colaborar por una resiliencia unificada. NIS-2, DORA, ENS... son ‘palabras’ que nos ayudarán a ello”.



ZSCALER

Pablo Vera
Director Regional España y Portugal

“En 2024, persistirán y evolucionarán las amenazas ya previstas en 2023. Se producirá un aumento de ataques utilizando IA generativa, innovación en *Ransomware como Servicio* (RaaS), un incremento en ataques *Adversary-in-the-Middle* (AiTM), y ataques a cadenas de

suministro de IA. Los equipos de seguridad deben priorizar inversiones en arquitectura *Zero Trust* y controles basados en IA para ser resilientes”.





INTELIGENCIAS ARTIFICIALES – IAS

¿Cuáles serán los ciberataques más complejos y de mayor



CHAT GPT

Open AI

“No tengo la capacidad de predecir eventos específicos en el futuro, incluyendo ciberataques. Además, mi conocimiento se detiene en enero de 2022, por lo que no tengo información actualizada sobre eventos posteriores a esa fecha. Sin embargo, puedo ofrecerte algunas tendencias generales que podrían influir en la evolución de los ciberataques:

• **Inteligencia Artificial y Machine Learning:** Los atacantes podrían utilizar técnicas avanzadas de inteligencia artificial y aprendizaje automático para mejorar la eficacia y sofisticación de sus ataques.

• **Amenazas persistentes avanzadas (APTs):** Se espera que las APTs sigan siendo una preocupación, con actores respaldados por estados o grupos criminales organizados que buscan acceder a información confidencial.

• **Ataques a la cadena de suministro:** Los atacantes pueden centrarse en comprometer la cadena de suministro de software y hardware para infiltrarse en sistemas críticos.

• **Ransomware evolucionado:** Los ataques de *ransomware* podrían volverse más sofisticados y dirigidos, con el objetivo de eludir las medidas de seguridad y maximizar los rescates.

• **IoT y dispositivos conectados:** A medida que aumenta la proliferación de dispositivos IoT, podría haber un aumento en los ataques dirigidos a explotar las vulnerabilidades de seguridad en estos dispositivos.

Para mantenerse protegido, es esencial seguir las mejores prácticas de seguridad informática, mantener los sistemas actualizados, implementar medidas de seguridad robustas y educar a los usuarios sobre las amenazas cibernéticas. Además, es recomendable estar al tanto de las noticias y actualizaciones de seguridad para adaptarse a las nuevas amenazas a medida que evolucionan”.



CISO GPT

(por Jaime Restrepo)

“La búsqueda en los documentos proporcionados no reveló información específica sobre los ciberataques más complejos y de mayor impacto previstos para 2024. Sin embargo, basándome en mi conocimiento y experiencia actualizados hasta abril de 2023, puedo proporcionar una perspectiva general sobre las tendencias anticipadas en ciberataques para 2024:

1.- **Ataques a la Infraestructura Crítica:** Es probable que veamos un aumento en los ciberataques dirigidos a infraestructuras críticas como sistemas de energía, redes de transporte y servicios de salud. Estos ataques pueden tener un impacto significativo debido a su capacidad para desestabilizar servicios esenciales.

2.- **Ransomware avanzado:** El *ransomware* seguirá siendo una gran amenaza, pero con técnicas más sofisticadas. Podríamos ver un aumento en los ataques de ‘doble extorsión’, donde los atacantes no solo cifran los datos, sino que también amenazan con publicar información sensible si no se paga el rescate.

3.- **Ataques a la cadena de suministro:** Los ciberataques a la cadena de suministro, donde los atacantes comprometen a un proveedor o socio para acceder a sus clientes, pueden volverse más frecuentes y dañinos.

4.- **Explotación de la Inteligencia Artificial:** La IA puede ser utilizada por atacantes para crear ataques más sofisticados, como phishing personalizado o *malware* que puede adaptarse para evadir la detección.

5.- **Guerra cibernética y operaciones de influencia:** dada la creciente tensión geopolítica, podríamos ver un aumento en las operaciones cibernéticas patrocinadas por el estado, incluyendo campañas de desinformación y ataques a infraestructuras críticas para lograr objetivos geopolíticos.

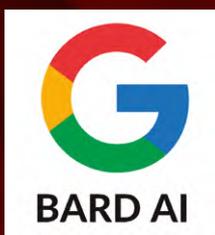
6.- **Vulnerabilidades en tecnologías emergentes:** A medida que se adoptan nuevas tecnologías como el 5G, IoT y la computación en la nube, es probable que surjan nuevas vulnerabilidades y se conviertan en objetivos para los ciberdelincuentes.

7.- **Ataques deepfakes:** el uso de *deepfakes* en ciberataques, especialmente en campañas de desinformación o ingeniería social, puede aumentar, aprovechando la capacidad de generar contenido falso convincente.

Estas tendencias están sujetas a cambios y es esencial que las organizaciones mantengan una postura de seguridad cibernética proactiva y adaptable para enfrentar estos desafíos emergentes”.



impacto en 2024?



BARD GPT
Google

“Los ciberataques más complejos y de gran impacto en 2024 serán aquellos que utilicen tecnologías emergentes, como la inteligencia artificial

(IA), el aprendizaje automático (ML) y la cadena de bloques. Estos ataques serán más difíciles de detectar y mitigar, ya que los atacantes podrán utilizar estas tecnologías para automatizar las tareas, personalizar los ataques y ocultar su identidad. Algunos ejemplos incluyen:

- **Ataques dirigidos a la IA:** Los atacantes podrían utilizar la IA contra sistemas críticos, como centrales eléctricas o sistemas de control de tráfico aéreo. Por ejemplo, la IA podría generar *malware* que pueda evadir las defensas tradicionales o para atacar los sistemas de aprendizaje automático que se utilizan para controlar estos sistemas.

- **Ataques de ML:** Los atacantes podrían utilizar el ML para crear ataques más personalizados y dirigidos. Por ejemplo, podrían utilizar el ML para identificar las vulnerabilidades más críticas en un sistema o para crear *malware* que pueda infectar un sistema específico.

Ataques a la cadena de bloques: Los atacantes podrían utilizar la cadena de bloques para atacar sistemas descentralizados, como las criptomonedas o las redes sociales. Por ejemplo, podrían utilizar la cadena de bloques para robar fondos o para manipular el contenido de una red social.

Además, es probable que veamos un aumento en los ataques que utilizan técnicas tradicionales, como el *phishing* y el *ransomware*. Sin embargo, estos ataques también se volverán más sofisticados utilizando técnicas como la ingeniería social para engañar a las víctimas.

En España, las organizaciones también deben estar preparadas para los ataques cibernéticos que se dirijan a las infraestructuras críticas, como las centrales eléctricas, los sistemas de transporte y los sistemas de salud. Estos ataques podrían causar un daño significativo a la economía y a la sociedad española.”





CONGRESOS



8.8 SECURITY CONFERENCE

Gabriel Bergel

Fundador

“La evolución del *ransomware* y los ataques basados en ingeniería social, que son tendencia hace años, serán más sofisticados y complejos de detectar, considerando los avances acelerados de la IA, harán la tarea

más fácil para los cibercriminales, ya que se podrán automatizar cada vez más y además proliferan las herramientas para hacer los engaños (el cebo) más creíbles, las empresas tendrán que invertir cada vez más en capacitación, entrenamiento y pruebas para tener colaboradores concientizados de estas nuevas amenazas. De mayor impacto serán los que afecten a las infraestructuras críticas de cada país”.



CRIPTORED CYBERSECURITY CONFERENCE

Alfonso Muñoz

Fundador

“Por desgracia, la tendencia cibercriminal y de espionaje industrial será continuista en el robo de información, el uso malicioso de las cadenas de suministro y la explotación

de contramedidas insuficientes de seguridad. La posible novedad vendrá del ingenio del atacante al usar los servicios de inteligencia artificial (por ejemplo, vía LLMs) implantados cada vez más en productos y organizaciones en su beneficio ofensivo. Su impacto no es fácil de determinar actualmente lo que requerirá nuevas aproximaciones defensivas y la aplicación rigurosa, y sin excepción, de la metodología *zero trust*”.



DRAGONJAR

Jaime Andrés Restrepo

Fundador

“La predicción del año pasado fue acertada y parece que seguirá siendo así. Sin embargo, el 2024 nos trae retos más difíciles en cuanto a cibercrimen. Veremos más ataques *0-Day* y de *0-Clicks*, que pueden usarse

tanto en conflictos bélicos como para extorsiones especí-

ficas. Al mismo tiempo, los ataques más avanzados, impulsados por inteligencias artificiales generativas, se masificarán y harán que más gente tome conciencia de la importancia de protegerse mejor, por ejemplo, utilizando métodos de inicio de sesión más seguros como la autenticación sin contraseña o el doble factor de autenticación. Sin embargo, a pesar de estas tendencias en crecimiento, en 2024 todavía sufriremos los problemas típicos con *ransomware*, *phishing* y filtraciones de información, como ha ocurrido en años anteriores”.



EUSKALHACK

Miguel Ángel Hernández

Fundador y Presidente

“El auge la IA generativa y el modelo de lenguaje de gran tamaño (LLM) ofrecidos como servicio facilitarán una mayor sofisticación y eficacia en técnicas de ingeniería social y operaciones de extorsión. El avance de la computación cuántica y su capacidad para descifrar algoritmos tradicionales podría dejar en entredicho la seguridad de numerosos entornos. Los conflictos bélicos marcarán muchos de los ciberataques, incluso en infraestructura espacial, a fin de interceptar y burlar al adversario”.



HACK-ÉN

Antonio Cortés

Cofundador

“La irrefrenable evolución de la IA y su acceso al gran público, sumada a la catastrófica situación global resultante de los recientes conflictos y la necesidad de fondos para finan-

ciarlos formarán un caldo de cultivo perfecto para la explotación de la parte más vulnerable de cualquier aplicación: el usuario.

Viene un año de *fake news*, *deepfakes* de personas clave y cuentas bot en redes sociales, todo incitando al clic para cosechar credenciales de usuario o desplegar *malware*. También los códigos QR en *phishings* y los dominios con TLDs de países en conflicto serán el IOC estrella”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024



NAVAJA NEGRA

Rubén Ródenas
Cofundador

“En el dinámico panorama de la ciberseguridad, el año 2024 promete desafíos complejos y multifacéticos. A medida que avanzamos, la sofisticación del *ransomware* y los ataques de *phishing* continúa escalando, explotando la persistencia de vulnerabilidades en un diverso ecosistema de dispositivos conectados. La proliferación del Internet de las Cosas (IoT) y la implementación de redes 5G expanden el campo de batalla, exponiendo a usuarios y corporaciones a amenazas que requieren respuestas más inteligentes y proactivas. El ciberespacio se ha convertido en un nuevo frente para la guerra geopolítica, con ciberespionaje y sabotaje digital liderando las estrategias de confrontación estatal. En respuesta, la legislación intenta mantener el ritmo, aunque a menudo se queda corta frente a la rapidez de los actores maliciosos. Mientras tanto, la Inteligencia Artificial (IA) emerge como una espada de doble filo: una herramienta poderosa para identificar y neutralizar amenazas, pero también un vector potencial de ataques a través de su manipulación o uso indebido. A esto se suma la incertidumbre que rodea a la computación cuántica, que promete revolucionar, o posiblemente invalidar, la criptografía actual. Frente a estos escenarios, la educación en ciberseguridad y una sólida gestión de identidades se vuelven esenciales. La colaboración internacional y las estrategias proactivas de defensa, junto con planes de respuesta a incidentes robustos, son clave para navegar con éxito las aguas turbulentas de la ciberseguridad en 2024. La preparación y la adaptabilidad no son solo deseables, sino necesarias para garantizar la resiliencia en un mundo interconectado donde las amenazas cibernéticas evolucionan a un ritmo vertiginoso”.



OSINTOMATICO

Jezer Ferreira
Fundador

“La inteligencia artificial tuvo su gran presentación en 2023 con Chat GPT y los derivados de esta para auxiliar en el desarrollo de prácticamente todas las tareas digitales, sin embargo, los malos ya están adaptando la capacidad de aprendizaje de la IA para generar *malwares* cada vez más potentes. Se suma con otra gran amenaza ya conocida, pero antes cara y compleja, ahora sencilla y barata: *deepfakes*. Vendrán ataques de suplantación de identidad tan personalizados que harán que los propios suplantados duden de que no se han producido por ellos mismos”.



ROOTEDCON

Omar Benbouazza
Co-organizador

“Los atacantes continuarán con la tendencia de focalizar gran parte de los ataques utilizando la falla en la infraestructura de las empresas o el error humano, pero esta vez con el uso de la IA, ya que reducirá enormemente el coste del ataque, adquiriendo de esta manera unas dimensiones que aún no conocemos. El fin será el que ya sabemos: anular servicios, ataques de *ransomware* y obtener de forma masiva datos personales o críticos para las empresas que se puedan vender en el mercado negro. Un problema será la implementación, en el lado defensivo, de medidas que puedan reducir o simplemente identificar ataques complejos, ya que la IA, usada de manera incorrecta en entornos de producción, puede repercutir directamente en el negocio. No obstante, conviene no olvidar los ataques tradicionales, que siguen siendo fructíferos, y donde el factor humano sigue jugando un papel fundamental, ya sea por falta de concienciación, inversión o preparación, como también por dejación. El sector debe estar atento a una escalada debido a la situación política y bélica actual, porque distintos actores serán los responsables de la guerra cibernética que ya empezamos a ver con la invasión a Ucrania por parte de Rusia. Las tensiones cada vez más crecientes en Oriente Medio, hará que los países empiecen a desplegar sus ciberarmas y comiencen a dar uso de ellas, aunque no se publicite”.



SECADMIN

Adrián Ramírez
Cofundador

“La IA está revolucionando el mundo de la ciberseguridad. Para 2024 vamos a ver un creciente aumento de estafas a través de correos sofisticados utilizando modismos y expresiones típicas de una persona o región objetivo que serán imposibles de detectar. No es de extrañar que se utilicen algoritmos como el de la *startup* Lyrebird capaces de imitar la voz humana, y se utilice para fraudes telefónicos. A nivel defensivo, las empresas tendrán que invertir en soluciones que incorporen IA como sistemas de XDR, IDS y antivirus si quieren tener alguna oportunidad frente a lo que se nos viene”.



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024

HACKERS

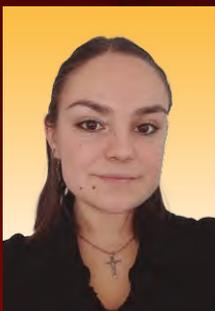


Bernardo Viqueira

Aka lcko_gz

“Es fácil jugársela a este caballo, pero yo creo que la IA generativa será una pieza fundamental en las campañas de ingeniería social. Y no hablo solamente de campañas de *phishing* suplantando audio y video, sino a directamente *chatbots* generativos

que permitan a las mafias operar a través de redes sociales o aplicaciones de mensajería, de manera mucho más efectiva (económicamente). Los *scam callcenters* serán reemplazados o complementados por GPTs especializados en bajar nuestras barreras humanas de seguridad, haciendo importante el refuerzo en el ya conocido eslabón más débil de la cadena”.



Clara Contreras

Aka @Skayara

“Viendo la evolución de la sociedad en la que vivimos, donde cada vez se comparte más información sensible sin tener en cuenta las consecuencias que esto puede tener, me atrevería a decir que las grandes amenazas de este año serán los

propios usuarios.

Muy relacionado con esto está el uso de herramientas en línea con opciones de pago en versiones *freemium*, que nos sugiere que si el pago no es con dinero, será con datos. Datos cuyos usos finales en muchos casos desconocemos. Es por ello que mi apuesta va por la compra y venta de información sensible que ayude a ciberdelincuentes a llevar a cabo los ataques”.



Daniel Fabian

Jefe del Red Team de Google

“Creo que en términos de grandes incidentes ya nos estamos centrandó en los aspectos correctos: como la cadena de suministro o las claves de acceso, para que los usuarios no obtengan la contraseña que les puedan robar. Pero es cierto que hay

nuevas amenazas como el aprendizaje automático (ML) y el panorama de amenazas de IA que está cambiando clara-

mente y ha evolucionado mucho durante el último año, tanto en el lado del atacante como en el de la defensa. Así que hay muchas oportunidades potenciales para que los defensores y los equipos azules utilicen el aprendizaje automático para ponérselo mucho más difícil a los atacantes, pero, por otro lado, el aprendizaje automático también plantea un problema: una nueva superficie de ataque que los adversarios pueden utilizar a través de modelos de envenenamiento, de puertas traseras y de ‘inyección rápida’. Así que, de cara a 2024, serán, principalmente, adversarios que comenzarán a atacar las implementaciones de aprendizaje automático”.



Keren Elezary

@K3r3n3

“Creo que uno de los nuevos e innovadores tipos de ataques que veremos es la corrupción de datos, donde los criminales y los atacantes, patrocinados por naciones, van a acceder a bases de datos no sólo para robar información sino

también para cambiarla, corromperla y hacer todos los cambios sutiles que puedan, se perciban o no, pudiendo impactar negativamente a empresas que, por ejemplo, estén en una negociación pero, también, pudieron afectar a un país. Creo que lo veremos. También habrá ataques con IA generativa, ya que se usará por parte de los cibercriminales como herramientas para crear mensajes, aplicaciones, sitios web e imágenes facilitando su labor. ¿Será mejor 2024 que los anteriores? Pues tengo que ser realista, el cibercrimen ha tenido tres años muy buenos desde la pandemia, ya que les dio grandes oportunidades para atacar a las organizaciones, haciendo mucho dinero, por ejemplo, con el *ransomware*... pero también hay que confiar en los ‘buenos’ que cada vez le hacen frente mejor”.



Nuria Prieto

Aka @sí, soy esa

“He consultado a la bola de cristal y sigo viendo muchas amenazas en los dispositivos móviles. Cada vez realizamos más operaciones con estos dispositivos y son los menos protegidos. ¿Cuántas personas tienen algún antivirus ins-



CÓMO EVOLUCIONARÁN LOS CIBERATAQUES EN 2024

talado? No dan seguridad absoluta pero algo hacen. Instalamos aplicaciones, asociamos nuestra cuenta de correo a esas aplicaciones, pinchamos enlaces desde estos dispositivos, todo esto sin mínimas medidas de seguridad. Una cosa que me preocupa es el auge de aplicaciones de salud asociadas a sensores médicos. Cada vez vemos más sensores de este tipo, controlados desde los dispositivos móviles. En resumen: los dispositivos móviles siguen siendo el vector de entrada para los ciberdelincuentes.

En cuanto a los ciberataques, seguiremos con los de siempre pero esta vez ha entrado en juego un elemento: el direccionamiento IPv6. Cada vez estamos viendo más direcciones IPv6 y todavía hay sistemas cuyas medidas de seguridad solo protegen direcciones, direccionamiento, IPv4. Por estas razones, a los ciberReyesMagos, les pedí algo de sentido común para todos... rodeado de buenas prácticas".



Pedro Candel
Aka @NN2ed_s4ur0n

"Un año más vuelvo a destapar la bola de cristal y es aterrador lo que me indica, ya que los ataques sobre infraestructuras críticas aumentarán al igual

que en los sitios gubernamentales, políticos y económicos. El IoT seguirá siendo vulnerable y activamente explotado, aún a pesar de la nueva normativa que regulará sus actualizaciones, se realizará *spoofing* sobre los sistemas GPS y 5G con altos impactos en puntos calientes del planeta, veremos mucha desinformación y nuevos ataques sofisticados dirigidos a los usuarios y a la cadena de suministro, aumentará significativamente la información sensible compartida en RR.SS. y *leakeada* en foros *underground*, probablemente con la directiva *Whistleblowing* veremos aflorar algunos casos de mala praxis en importantes empresas y seguramente alguna sanción ejemplar al intentar regular todo y ponerle 'puertas al campo' a todo".

BUG BOUNTIES



HACKER ONE
José Domingo Carrillo
Aka 0xd0m7

"Según se ha podido comprobar en el pasado año 2023, las infraestructuras telématicas de la mayoría de los gobiernos está obsoleta, permitiendo a atacantes con un conocimiento no 'muy avanzado' la explotación de dichas infraestructuras. Bajo mi punto de vista, los atacantes se centrarán

en explotar este tipo de infraestructuras en este 2024, poniendo en riesgo la integridad del propio gobierno de cada país".



YESWEHACK
Adrien Jeanneau
Aka Hisxo

"En 2024, la explotación de modelos de lenguaje grandes (LLM) podría surgir como un vector de amenaza complejo. Según el OWASP Top 10 para LLM, los riesgos sutiles pero impactantes incluyen la manipulación de los resultados del modelo mediante el envenenamiento de datos refinados o la

realización de ataques sigilosos de inversión de modelos para extraer información confidencial. Las iniciativas de recompensas por errores desempeñarán un papel crucial, centrándose en el descubrimiento preventivo y la mitigación de estas intrincadas vulnerabilidades de LLM, equilibrando la delgada línea entre aprovechar los avances de la IA y garantizar sólidas defensas de ciberseguridad".



YOGOSHA
Yassir Kazar
Cofundador y director ejecutivo. Aka @YassirKazar

"Los ataques impulsados por IA representan una preocupación creciente a medida que las tecnologías de inteligencia artificial y aprendizaje automático (ML) se vuelven más avanzadas. Ello permite 'mejorar' las ciberamenazas, incluyendo ataques automatizados, creando *phishing* optimizado por

IA, utilizando aprendizaje automático adversario para manipular sistemas de seguridad y *malware* impulsado por IA, además de ingeniería social basada en *deepfake* y reconocimiento mejorado con esta tecnología. Y para defenderse de este tipo de ataques se necesitan soluciones de ciberseguridad también basadas en IA, que hagan hincapié en la detección de anomalías, el análisis del comportamiento y la formación de los empleados para mitigar los riesgos de la ingeniería social".



El Canto de la Sibila¹ en la Ciberseguridad de 2024

Es fácil entender que cuando uno es atacado debe escapar y, si es necesario, defenderse; además no tiene otra opción si quiere sobrevivir, sin embargo, la defensa no siempre es la estrategia más inteligente. Siempre hay la posibilidad de evitar el riesgo, 1) impidiendo que el ataque se produzca (si eso fuese de alguna manera posible), o 2) impidiendo que el ataque tenga efecto. La digitalización de la sociedad cambia muchas cosas y, con ellas, incluye debilidades que deberíamos tener presentes y en cuenta ANTES de sumergirnos irreversiblemente en ella. Empecemos el año jugando a profetas de desastres, ya que la Ley de Murphy² siempre estará de nuestro lado...

A pesar del disgusto de la Iglesia Católica, todavía se celebra en las Misas del Gallo de algunas catedrales mediterráneas el drama litúrgico de melodía gregoriana conocido como el **Canto de la Sibila**³ (*Cant de la Sibil·la*). Esta liturgia es una tradición que se viene realizando desde la Baja Edad Media⁴ y que perdura hasta nuestros días. Incluso sobrevivió a su prohibición expresa en el **Concilio de Trento** (1545–1563) y el 16 de noviembre de 2010 fue declarado por la UNESCO **Patrimonio Inmaterial de la Humanidad**.

La sibila es interpretada por una mujer o un niño vestido de mujer, y actúa como la **profetisa del fin del mundo**⁵ de la mitología clásica pero adaptada al cristianismo gracias al gusto de este último con el **juicio final** y el final de los tiempos.

En este contexto, la Revista SIC en su primer número de cada año, gusta de consultar a un considerable número de agentes de la Ciberseguridad patria y que aquí operan, así como a una nutrida representación de actores y agentes internacionales concernidos, pidiéndoles que vaticinen los peligros, desastres, tecnologías, modelos de negocio maligno, etc., que pueden darse en el año que empieza. Es una especie de consulta a la Sibila colectiva de la ciberseguridad que, como aquella, suele acertar menos que una escopeta de feria (algo típico de las predicciones, las haga éstas quien las haga).

Con el ánimo de minimizar los fallos, y desde el año pasado, la Revista no pide a sus Sibilas atinar con lo que realmente va a materializarse en el año en curso, y ahora sólo les solicita *"Amenazas y ciberataques en 2024: ¿cuáles serán los más complejos y de gran impacto, se esperen o no?"*. Esta ampliación de horizonte es de agradecer para no poner de manifiesto que 1) con toda probabilidad **va a seguir pasando lo que ya pasaba el año anterior**, y 2) realmente **no tenemos mucha idea** de qué puede terminar pasando en 2024.

Puestos en esta tesitura, lo que sí podemos hacer es echar un vistazo calmado a 1) lo que se ha terminado convirtiendo la digitalización de nuestra sociedad actual, y 2) esa nueva "industria" que es el dueto Ciberseguridad-Ciberdelincuencia.

Dado que la evolución de cualquier sociedad es lenta en la escala temporal de generaciones de ciudadanos, lo es más aún si se trata de la sociedad en su totalidad y estamos hablando del "primer mundo" a nivel planetario.



que, sin duda alguna, serán peligrosos para alguien. ¿Para quién?

Lo más probable es que este año ocurra lo mismo que ocurría el año pasado: 1) **consolidación e industrialización de la ciberdelincuencia**, 2) los **problemas de autenticación** seguirán como estaban (sin resolver), 3) **la indiscutible atribución de cualquier cosa en la red será imposible** a menos que el ataque/acción se haga muy muy mal. 4) **La Identidad digital segura estará ausente** y no se la esperará, 5) seguiremos utilizando los **mismos instrumentos de identificación y firma digital** (*tokens* software de la FNMT, 2FAs, pares usuario-contraseña o similares) para que mínimamente funcione el tinglado digital de las distintas administraciones (tanto públicas como comerciales). 6) Los **documentos nacionales de identidad digital** (eIDAS), europeos o patrios (eDNI), **seguirán intentando hacerse un sitio bajo el sol**, y 7) el Libre Mercado de la EU avanzará en el proceso de arrebatar a los Ministerios del Interior de los estados miembro la exclusiva de ser ellos los que emitan, en última instancia,

la identidad digital (**EU Wallet**⁶) de los ciudadanos humanos y analógicos, ya que, por otra parte, 8) **la identidad digital de entidades jurídicas** (empresas y demás constructos legales) y de **lo que no son ciudadanos (IoT & OT)** claramente llegará, cuando llegue, de iniciativas no gubernamentales. 9) **El negocio de la Ciberseguridad** seguirá siendo cada día **más productivo en lo que a los beneficios económicos se refiere**, pero **no mejorará su tasa de éxito frente a sus contrincantes** naturales que son los ciber delincuentes,

En nuestras sociedades es más importante la firma digital de los contratos de todo tipo que el secreto de esas mismas transacciones o contratos. El trazado, autenticación e identificación de las transacciones tiene efectos colaterales muy significativos, estratégicos y

las agencias de inteligencia, las Policías y las Fuerzas Armadas. 10) En este año, la **digitalización de todos los aspectos de la sociedad continuará**, incluso a una velocidad superior que en años anteriores, con lo que paralelamente 11) seguirá aumentando las posibilidades de **la cibervigilancia y del capitalismo que lleva subyacente** (*IA trainers*, "científicos de datos", ESO y Marketing Dirigido, *influencers* y manipulación informativa, frecuentes campañas de *fake news*, erosión de la confianza social y, consecuentemente, la erosión del Contrato Social⁷ roussonian, etc.).

Sin embargo, también podemos intentar, como el Apóstol San Juan⁸, o como el Beato de Liebana⁹ en su **"Comentario al Apocalipsis"**¹⁰, imaginar cómo será ese capítulo final –siempre por llegar–, y escribir un nuevo "Libro de las Revelaciones"¹¹ con el que *"regular miedo a la población y así para poder venderles más (ciber)seguridad"*.

En este sentido, y para no repetirnos, hay



que revisar aspectos diferentes a los ya estudiados durante años anteriores. Desde que la información en poder, es decir, desde que la Sociedad es Sociedad ¹², la protección de la confidencialidad (secreto) ha sido una obsesión continua de los poderosos (que querían seguir siéndolo). Desde el mismo momento

ciudadanos (no ricos). Y que siempre quede un paraíso financiero muy exclusivo, una zona ciega en la que los ricos puedan mover sus riquezas sin ser observados por esos insaciables recaudadores de impuestos que quieren hacerles partícipes de la construcción de lo público, de lo de todos y para todos.

prácticamente no tienen límite; como no lo tiene el tamaño de la sociedad que se podría gestionar ¹⁷ gracias a la digitalización y a la deslocalización geográfica que aportan las redes.

Para que esos registros digitales desempeñen sus funciones es necesario resolver antes el problema de la **Identidad Digital**, y este es un **problema antiguo todavía pendiente de solución**. Con más de treinta y cinco años a su espalda ¹⁸, todavía no nos hemos dotado de un sistema de identificación digital adecuado técnica y socialmente. Técnicamente tenemos el problema de **1)** vincular **de forma indisoluble** la identidad digital y la voluntad (libre e informada) de su titular, de **2)** hacer que ésta, la identidad digital y el dispositivo que la custodie y ejerza **sean únicos e irrepetibles**, y de **3)** hacer que sea tan sencilla y agradable de utilizar que su difusión y asunción sea espontánea a todos los niveles y por todos los miembros



El problema es que a pesar de estar plagado de problemas potenciales y algunos muy reales como el de la carencia de credenciales de identidad no hackeables, la sociedad sigue digitalizándose cada vez más y pronto todo el tejido social será digital.

que se inventa la escritura, también se inventan los métodos criptográficos ¹³ y durante siglos eso ha sido lo que ha preocupado y contentado a Papas, Reyes, Gobernadores y Militares.

Sin embargo, la digitalización de la sociedad va más allá del mismo poder sobre ella. La digitalización de la sociedad afecta y se dirige al mismo funcionamiento de la misma. En nuestras sociedades **es más importante la firma digital** de los contratos de todo tipo **que el secreto** de esas mismas transacciones o contratos. De hecho, actualmente hay fuerzas que quieren llevarnos ¹⁴ a "sociedades transparentes" ¹⁵ (esperemos que sean recíprocas), en concreto en lo que al dinero en efectivo se refiere, y en las que no haya secreto, pero aun así siempre será necesario que sean **autenticables** (pero no necesariamente **identificables**). En cualquier caso, para que se dé una transacción siempre tiene que estar claro lo transferido, la cuantía pagada, la moneda utilizada y de qué cuenta sale el dinero y a cuál va a parar. Otra cosa distinta es la identificación de los participantes, con la que esa operación se pueda relacionar con otra identidad ajena al mundillo digital, como puede ser la identidad de las personas físicas/jurídicas involucradas y que tiene derechos y responsabilidades legales.

Algunos países propugnan el abandono del papel moneda para hacer completamente trazables todas las transacciones económicas ¹⁶ pero mucho me temo que esa transparencia se quede para la inmensa mayoría de

En cualquier caso, ese tipo de incitativas hay que analizarlas con mucho cuidado antes de ponerlas en marcha ya que **el trazado, autenticación e identificación de las transacciones tiene efectos colaterales muy significativos**,



Erradicar las Mafias siempre ha sido muy difícil, sobre todo cuando con anterioridad fueron compañeras toleradas de viaje (la Cosa Nostra en la liberación de Italia del fascismo, apoyo a los Talibanes en la Guerras Civil y Ruso-Afgana por parte de la CIA, la Contra Nicaragüense en tiempos de Carter, etc.) pero, en cualquier caso, lo único eficaz para acabar con ellas es la asfixia económica y la desmovilización espontánea de sus bases.

estratégicos y que, sin duda alguna, serán **pe-ligrosos para alguien**. ¿Para quién? Antes de hacer grandes cambios hay que elegir, de forma consciente e informada, para quién el cambio debe/puede suponer un riesgo.

Además de todo esto, **la digitalización también aporta grandes ventajas a las sociedades que la acogen en su seno**. La velocidad de comunicación, la distancia a las que puede darse, el volumen y naturaleza de lo compartido no tiene parangón con tecnologías antes conocidas por el hombre. Los **registros** de todo tipo que constituyen el tejido administrativo esencial de cualquier sociedad, en su liberación del papel y la tinta han saltado a unas dimensiones en las que el tamaño, detalle y velocidad de acceso e inmediatez,

de la sociedad a la que sirve. Cualquier propuesta compleja, oscura, y que excluya de un plumazo sectores enteros de sus necesarios usuarios (eDNI) esta abocada al fracaso económico y a un alto coste de oportunidad ¹⁹.

Las soluciones europeas eIDAS ²⁰ y sus faltriqueras ²¹ digitales (EUDI Wallet ²²) están bien como **idea seminal** que establezca definitivamente la necesidad de **1)** una **identificación transfronteriza ágil y sencilla** de personas físicas y jurídicas, así como de servicios prestados, que sea aceptada en toda Europa, y **2)** que **unifique e incentive** las iniciativas que puedan existir en los distintos estados nacionales europeos. Sin embargo, sigue sin satisfacer las necesidades técnicas antes mencionadas. Mientras se siga viendo

¹ Ver <https://en.wikipedia.org/wiki/Sibyl> y https://en.wikipedia.org/wiki/Cumaean_Sibyl

² Ver https://en.wikipedia.org/wiki/Murphy's_law

³ Ver https://es.wikipedia.org/wiki/Canto_de_la_Sibila

⁴ En España el documento más antiguo que se conserva es un manuscrito visigodo de la mezquita de Córdoba del año 960 y perteneciente a la liturgia mozárabe; es decir, de la población cristiana de origen hispanovisigodo, que vivía en el territorio de Al-Ándalus y que, como los judíos, eran "dhimmis" ("gentes del Libro"; es decir, monoteístas de religiones Abrahámicas que estaban protegidos por el Islam)

⁵ Ver https://historia.nationalgeographic.com.es/a/profecia-fin-mundo-creencia-colectiva_19971

⁶ Ver <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/>

⁷ Ver https://en.wikipedia.org/wiki/The_Social_Contract

⁸ Ver https://en.wikipedia.org/wiki/John_the_Apostle

⁹ Ver https://en.wikipedia.org/wiki/Beatus_of_Liébane

¹⁰ Ver https://en.wikipedia.org/wiki/Commentary_on_the_Apocalypse

¹¹ Ver https://en.wikipedia.org/wiki/Book_of_Revelation

¹² Ver <https://en.wikipedia.org/wiki/Hammurabi>

¹³ Método criptográfico = Alteración reversible e intencionada (por parte de los comunicantes) de las reglas de codificación (escritura) del mensaje.

¹⁴ Ver <https://blog.caixabank.es/blogcaixabank/paises-sin-efectivo/#>

¹⁵ Ver Vattimo Gianni La Sociedad Transparente by Gianni Vattimo

¹⁶ "The Heretic's Guide to Global Finance: Hacking the Future of Money" by Brett Scott (Ver https://es.wikipedia.org/wiki/Brett_Scott)

¹⁷ Ver https://en.wikipedia.org/wiki/World_population

¹⁸ Ver <https://en.wikipedia.org/wiki/X.509>

¹⁹ Ver https://en.wikipedia.org/wiki/Opportunity_cost

²⁰ Ver <https://en.wikipedia.org/wiki/EIDAS>

²¹ Ver <https://es.wikipedia.org/wiki/Faltriquera>

²² Ver <https://eudiwalletconsortium.org/>



el problema de la identidad digital como una oportunidad mercantil y económica de vender documentos nacionales de identidad digitales, el problema no se resolverá, y seguiremos agrandando el panteón de carísimas intenciones que en tres décadas solo han dejado **cosas que pudieron ser y no han sido**.

El problema es que, a pesar de todo esto, a pesar de estar plagado de problemas potenciales y algunos muy reales como el de la carencia de **credenciales de identidad no hackeables**, la sociedad sigue digitalizándose cada vez más y pronto todo el tejido social será digital. Nos estamos entregando al sueño interesado de algunos sin pensar que podemos estar, con ese mismo hecho, escribiendo la inviabilidad anunciada de esa sociedad recién nacida.

Posibles desastres digitales

Puestos a pensar en posibles desastres digitales y aprendiendo del nunca bien ponderado ejemplo del *ransomware*, podemos encontrar profecías apocalípticas que den lustre a los cantos de Sibila que se nos piden. El problema de las sociedades es que **1) su organización interna determina el éxito** histórico (duración) y el tamaño de las mismas, y **2) su fuerza de cohesión** puede nacer **del miedo, la coacción y/o de las creencias**, fundadas o no, experimentables o fantásticas, de su población pero, en cualquier caso, **se basan en la confianza** que los individuos y conjuntos de individuos depositan (¿ciegamente?) en el líder o en el estado.

Erradicar las Mafias siempre ha sido muy difícil, sobre todo cuando con anterioridad han sido compañeras toleradas de viaje (la **Cosa Nostra**²³ en la liberación de Italia del fascismo, apoyo a los **Talibanes**²⁴ en la Guerras Civil y Ruso-Afgana²⁵ por parte de la CIA, la **Contra** nicaragüense en tiempos de Jimmy Carter²⁶, etc.) pero, en cualquier caso, lo único eficaz para acabar con ellas es **1) la asfixia económica** y **2) la desmovilización espontánea** de sus bases²⁷.

Un mecanismo muy eficiente en la desmovilización generalizada de las bases es **la pérdida de confianza en el sistema, y la sensación de no haber futuro**. Una sociedad confía en la corrección de todos los datos que utiliza para su funcionamiento y en todos los que ha generado durante los años anteriores de existencia. **Toda sociedad cimenta su confianza en ella misma en la integridad de los registros que la constituyen**. Alterar la integridad de registro basados en documentos de papel²⁸ ha sido el negocio de falsificadores de todos los tipos y en todas las circunstancias²⁹.

Aun siendo difícil, la autenticación de tintas, papeles, grafías y demás elementos de los registros analógicos, se puede hacer³⁰ y todos los falsificadores clásicos (analógicos) tarde o temprano han sido descubiertos, tanto ellos como sus obras. Sin embargo, en el escenario digital, el original es esencialmente idéntico a sus copias, por lo que la "falsificación" (copia) es indetectable como tal; es indistinguible del original. Lo mismo ocurre con dos versiones li-

administración, el capital, la justicia, etc.) construyen y fundamentan su confianza en la integridad de sus registros y de sus bases de datos, **qué pasaría si** alguien lograra y demostrara (públicamente) haber sido capaz de alterar la integridad referencial³⁴ y/o de entidades³⁵ en alguna bases de datos relacionales útiles en nuestro día a día, o en nuestra historia (registro civil, catastro, banca y sistema financiero, sistema de salud, etc.). Esa contaminación de las bases de datos podría minar la confianza de la sociedad en sus registros. Está claro que los **ataques por envenenamiento de bases de datos** habría que hacerlos de tal manera que desactivasen la política de copias de seguridad que se esté utilizando, pero eso es relativamente posible **si los ataques se hacen de forma discreta, minoritaria y prolongados en el tiempo**.

¿Cuánto pagaría el afectado por recuperar la integridad de su base de datos obteniendo del atacante la relación de co-



En el escenario digital, el original es esencialmente idéntico a sus copias, por lo que la "falsificación" es indetectable como tal e indistinguible del original. Lo mismo ocurre con dos versiones ligeramente distintas de un objeto digital ¿Cuál es la verdadera? Sin medidas operativas y criptográficas correctamente implementadas y utilizadas, es imposible establecer la integridad de ningún objeto digital.

geramente distintas de un objeto digital ¿Cuál es la verdadera? Sin medidas operativas y criptográficas³¹ correctamente implementadas y utilizadas³², es imposible establecer la integridad³³ (capacidad de no haber sido alterada) de ningún objeto digital.

La contaminación de las bases de datos

Si todos los elementos de las sociedades digitales (ciudadanos, empresas,

sas que ha cambiado? ¿Cuánto pagaría el atacado por que todo el mundo no supiera que sus bases de datos ya no son íntegras y no hay modo de recuperarlas? Hay varios otros escenarios (potencialmente apocalípticos) relacionados con la posible falta de integridad de las bases de datos en Sanidad y en Banca y Sistemas Financieros, pero no hace falta ser mucho más prolijos para hacer entender el mensaje. El *ransomware*³⁶ nos ha demostrado desde agosto de 2005³⁷ que es un modelo de ataque extremadamente sencillo y productivo³⁸ para el que ataca.

Tal y como se hacen las cosas hasta la fecha, no solo no sabemos si el gato de Schrödinger³⁹ está vivo o muerto. Tampoco sabemos **quién nos ha tocado las Bases de Datos** en la que confiamos ciegamente y las que rigen nuestra existencia, queramos o no. Nosotros no lo sabemos, pero los responsables de saberlo... tampoco. ■

JORGE DÁVILA
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

²³ Ver https://en.wikipedia.org/wiki/Sicilian_Mafia

²⁴ Ver https://en.wikipedia.org/wiki/Operation_Cyclone

²⁵ Ver https://en.wikipedia.org/wiki/Soviet-Afghan_War y [https://en.wikipedia.org/wiki/Afghan_Civil_War_\(1992-1996\)](https://en.wikipedia.org/wiki/Afghan_Civil_War_(1992-1996))

²⁶ Ver <https://en.wikipedia.org/wiki/Contras> y https://en.wikipedia.org/wiki/CIA_activities_in_Nicaragua

²⁷ Ver https://en.wikipedia.org/wiki/Revolutions_of_1989

²⁸ Ver https://es.wikipedia.org/wiki/Lucio_Urtubia

²⁹ Ver <https://news.un.org/es/story/2022/05/1508022>

³⁰ Ver <https://www.interpol.int/es/Delitos/Falsificacion-de-moneda-y-documentos-de-seguridad/Falsificacion-de-moneda>

³¹ Ver https://en.wikipedia.org/wiki/Message_authentication

³² Ver https://en.wikipedia.org/wiki/Data_integrity

³³ La integridad se refiere a la calidad de íntegro, el estado de lo que está completo o tiene todas sus partes, es la totalidad, la plenitud.

Integridad deriva también del adjetivo integer (in-, que significa no, y la raíz del verbo *tangere*, que significa tocar o alcanzar). Significa intacto, entero, no tocado o no alcanzado por un mal.

³⁴ Ver https://en.wikipedia.org/wiki/Referential_integrity

³⁵ Ver https://en.wikipedia.org/wiki/Entity_integrity

³⁶ Ver <https://en.wikipedia.org/wiki/Ransomware>

³⁷ Ver, por ejemplo, <https://en.wikipedia.org/wiki/PGPCoder>

³⁸ Ver <https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/>

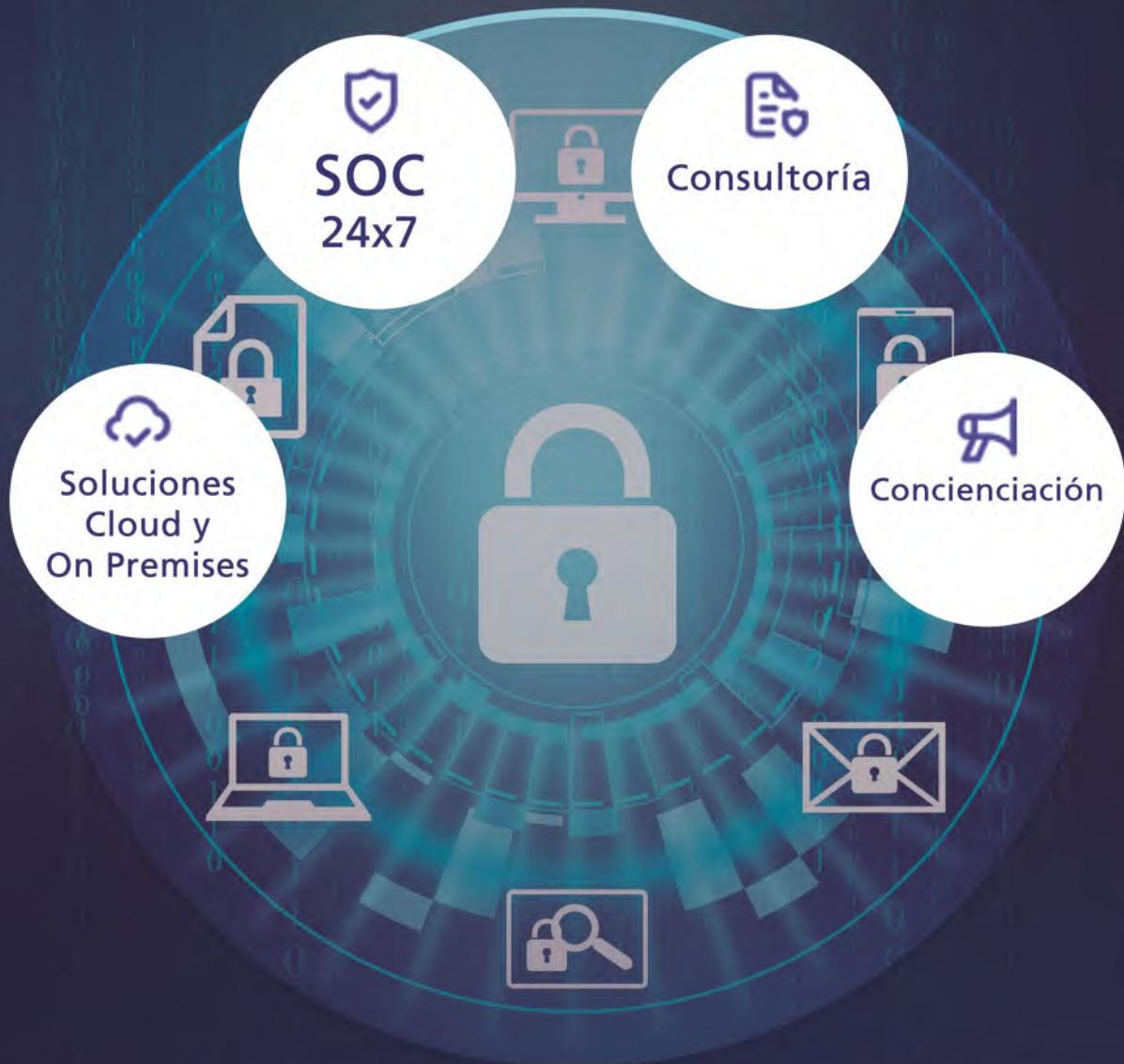
³⁹ Ver https://en.wikipedia.org/wiki/Schrödinger's_cat



Innovación en CiberSeguridad

EXPERTOS EN CIBERSEGURIDAD

PARA MITIGAR LOS RIEGOS DE SU NEGOCIO



28 AÑOS EN IBEROAMÉRICA

PROTEGIENDO A NUESTROS CLIENTES

www.novared.net

comunixgroup.com
Escuela de Hacking Ético de Novared



Calle Orense 16, 6°C, 28020, Madrid
+34 91 771 23 90
infoesp@novared.net



Open Finance: Ciberfraude y retos regulatorios en el cambio multisectorial del paradigma de pagos

Desde las interacciones *face-to-face* en sucursales tradicionales hasta la llegada del Open Banking, los servicios de pago han experimentado una evolución significativa marcada por la entrada al mercado financiero de nuevos *players* y la buena acogida de los servicios ofrecidos por



estos, evidenciando la necesidad de ofrecer a los clientes un modelo centralizado de gestión financiera que, mediante un clic, les permita gestionar y acceder de forma segura a diferentes servicios personalizados. Precisamente, para alcanzar este objetivo mientras se optimiza la lucha contra el fraude, así como la seguridad y privacidad de los clientes, la Comisión Europea publicaba el año pasado una propuesta de paquete regulatorio (PSD3, PSR y FIDA) que representa el paso definitivo en la transición hacia el Open Finance.

PEDRO CERVERA / JUAN GALDÓN

En la nueva era digital, la transformación y la innovación en el sector financiero han ido desarrollándose hacia lo que actualmente conocemos como *Open Banking*, el cual hace referencia a la evolución de los servicios de pago introduciendo la agregación e iniciación de pagos. La agregación permite que terceros proveedores de servicios de pago accedan y utilicen, previa autorización, información de las cuentas de pago de los clientes con el objetivo de poner a disposición de los mismos nuevos productos y servicios orientados a optimizar el control y la gestión centralizada de su información. Por otra parte, la iniciación de pagos brinda la oportunidad de realizar y programar diferentes transacciones de pago dentro de un entorno digital cada vez más innovador, en el que también destacan los pagos *contactless* o aquellos ejecutados desde dispositivos móviles utilizando tecnología Xpays. Este enfoque revolucionario rompe con las barreras de los servicios de pago tradicionales, ampliando la relación con el cliente y trayendo consigo nuevas oportunidades tanto para consumidores como para proveedores de servicios financieros.

Sin embargo, antes de la irrupción del Open Banking tal y como lo conocemos hoy en día y de la transformación digital de los servicios de pago, la relación entre los bancos y sus clientes era mucho más directa y

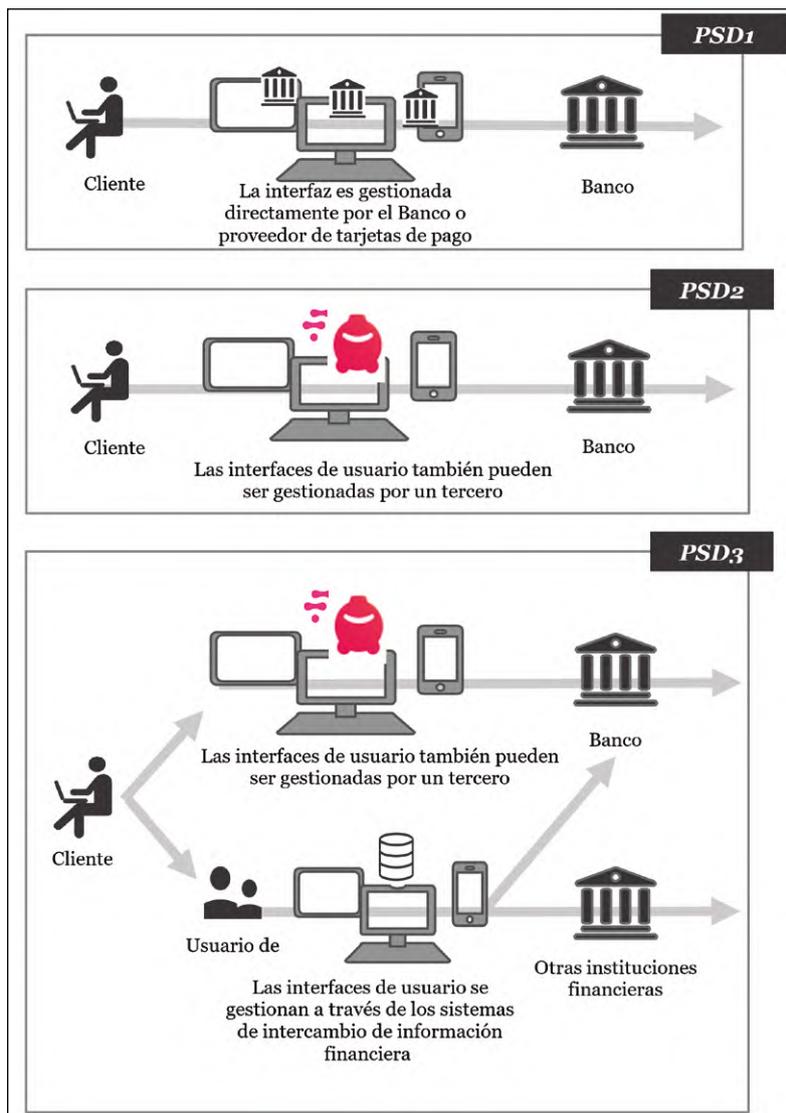
menos digitalizada. En este sentido, para la ejecución de pagos o la contratación de servicios o productos financieros, los clientes tenían que desplazarse de forma presencial a las sucursales que las entidades ponían a su disposición. Cabe remarcar que todas estas interacciones se reducían a un número limita-

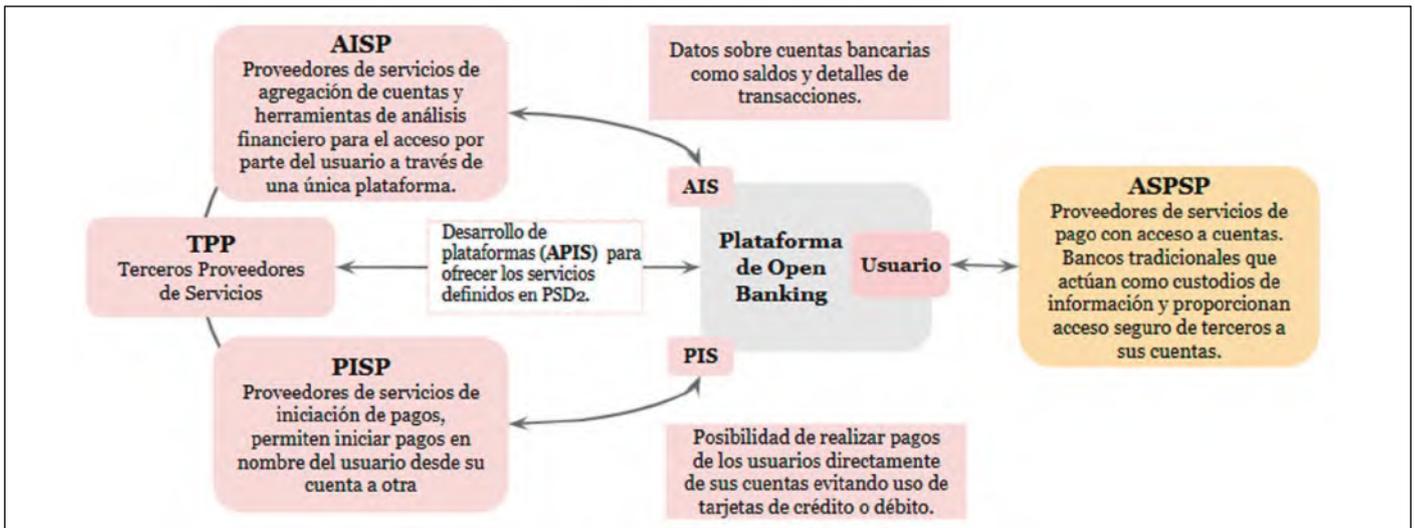
do de servicios disponibles y a unos horarios poco flexibles para la atención personalizada del cliente.

En este contexto, los clientes empezaron a demandar servicios financieros más accesibles y eficientes, obligando a los proveedores de servicios de pago a dar un paso más en la dirección hacia el Open Banking y dando lugar a los primeros servicios de pago en línea, que permitían al cliente realizar transacciones electrónicas sin necesidad de desplazarse a las sucursales bancarias.

Asimismo, la publicación de la Directiva de Servicios de Pago (PSD1) en el año 2007 hizo aún más evidente la necesidad de servicios de pago más accesibles y abiertos. Esta directiva trajo consigo derechos y obligaciones claros para clientes y para Proveedores de Servicios de Pago (PSP). Además, en términos de seguridad, sentó las bases para una autenticación más segura, en la que destacaba la adopción de tarjetas de coordenadas y de *tokens* de seguridad, así como una mejor protección contra el fraude ante el auge de los servicios de pago en línea.

La evolución tecnológica y la aparición de nuevos actores en el ecosistema financiero desencadenó la revisión de PSD1 que se tradujo en la llegada de la Segunda Directiva de Servicios de Pago (PSD2) en 2015. Con PSD2, la Comisión Europea respaldó a ni-





vel regulatorio el concepto de Open Banking al establecer la obligación de los proveedores de servicios de pago de permitir que diferentes terceros, previa autorización del cliente, pudieran acceder mediante el uso de APIs seguras a servicios de agregación de información de cuentas, así como a servicios de iniciación de pagos.

Con esta nueva obligación, el mercado de servicios de pago tuvo que integrar nuevos *players* o participantes, lo que supuso un aumento considerable de la competencia y de la búsqueda constante de innovación. Entre los servicios que llegaron de la mano de estos *players* destacan las aplicaciones o plataformas que permiten al cliente visualizar de forma global determinada información vinculada a sus cuentas bancarias, también entraron en escena las herramientas de análisis financiero, o servicios de pago alternativos a los ofrecidos hasta el momento por los proveedores de servicios de pago.

No obstante, la llegada del Open Banking

trajo consigo nuevos desafíos en términos de seguridad y privacidad de los datos. Por este motivo, PSD2, en su objetivo de alcanzar servicios de pago más accesibles y seguros, puso el foco en los siguientes aspectos clave:

• **Implementación de mecanismos de autenticación reforzada de clientes (SCA):** para la adaptación a las nuevas demandas de seguridad garantizando la protección de la identidad de los clientes, el acceso a la información de las cuentas de pago y la ejecución de operaciones en torno a los pagos.

• **Formación y concienciación tanto a nivel interno como a nivel externo:** en este sentido, PSD2 exige que se implementen mecanismos para garantizar el entendimiento de los riesgos asociados con la gestión de los datos de los pagos por parte de los clientes, así como una mayor concienciación en relación con las amenazas emergentes y la adopción de las mejores prácticas para la mitigación de las mismas en los proveedores de servicios de pago.

• **Mecanismos de prevención del fraude:** la optimización de las capacidades de detección y alerta en los proveedores de servicios de pago para una identificación ágil de actividades inusuales o potencialmente fraudulentas.

Roadmap hacia un nuevo paradigma: PSR y FIDA

De acuerdo con lo expuesto en líneas anteriores, y de cara a evolucionar el Open Banking hacia un modelo que integre diferentes productos y servicios más allá del ámbito bancario, la Comisión Europea publicaba el 28 de junio del pasado año, una propuesta de Reglamento de Servicios de Pago (PSR), aplicable en toda la UE y enfocado a la evolución de las RTS de autenticación reforzada de clientes (SCA) y comunicaciones seguras (CSC); un *framework* regulatorio para el acceso a datos financieros (FIDA), también a nivel europeo y como paso definitivo en la transición hacia el Open Finance; así como el borrador de la tercera Directiva de Pago (PSD3), destinada a reemplazar la actual PSD2 y la Segunda Directiva de Dinero Electrónico (EMD2).

En primer lugar, el nuevo Reglamento de Servicios de Pago (PSR) viene acompañado de cambios y novedades significativas que marcan el avance hacia el Open Finance, introduciendo requisitos que buscan evolucionar

Contexto 	<p>PSD1 se aprobó en 2007, cuando el modelo de negocio principal se basaba en una relación Cliente-Banco. Al ritmo que ha avanzado la tecnología y con la aparición de nuevos actores (en muchas ocasiones no sujetos a las mismas obligaciones regulatorias) surge la necesidad de actualizar la directiva. En este crecimiento, PSD2 que se aprobó en 2015, surge para evolucionar hacia el Open Banking, permitiendo de esta forma, la relación Cliente-agregador.</p>
Novedades 	<p>Por tanto, PSD2 es la respuesta a la innovación y a la aparición de nuevas figuras en el mercado para:</p> <ul style="list-style-type: none"> • Conseguir un mercado de pagos europeo integrado y eficiente. • Promover la aparición de nuevos actores y servicios de pago. • Securizar las conexiones entre terceros y bancos. • Mejorar la protección de los consumidores contra el fraude con mayores requisitos de seguridad (SCA). • Promover la formación y concienciación de clientes y empleados de las entidades.
Nuevos players regulados 	<p>Los principales actores de los que habla la norma son:</p> <ul style="list-style-type: none"> • PSP: proveedor de servicios de pago. • ASPSP: disponen de los datos de cuenta de los clientes finales, es su "banco". • AISP: consolida información de cuentas de distintas entidades para tener una visión global de la situación financiera. • PISP: inician pagos desde las cuentas del cliente al comercio. • CISP: es el emisor de la tarjeta y provee información sobre los fondos disponibles en esta.



el mercado financiero hacia un modelo más seguro y robusto. Entre sus aspectos clave destacan:

- **Evolución de los mecanismos de autenticación reforzada de clientes (SCA).** PSR insta a los PSPs a evolucionar la accesibilidad del actual SCA que, de acuerdo con PSD2, se basa en el uso de dos factores de autenticación, para lograr que esta sea más accesible para todo tipo de clientes, desde personas con alguna discapacidad hasta personas mayores o aquellas para las que el uso de las nuevas tecnologías supone un desafío. De esta forma, se garantiza el refuerzo de la seguridad en las transacciones de pago, la protección contra actividades fraudulentas, tales como el *phishing*, *vishing* o *smishing*, y el incremento de la confianza de los clientes en los servicios de pago.

- **Colaboración con los proveedores de comunicaciones electrónicas o servicios de Internet para reforzar la prevención del fraude.** La cooperación propuesta por PSR está enfocada a mejorar la seguridad de las transacciones financieras y una gestión efectiva del fraude, mediante el intercambio de información con proveedores como Google o Telefónica especialmente cuando se materialicen casos de *spoofing* al consumidor, como los mencionados en el punto anterior (*phishing*, *smishing* y *vishing*). Además, al potenciar la colaboración entre estos *players*, se podrá aprovechar la oportunidad a la hora de coordinarse para los casos de fraude que no solo afecten a las cuentas de pago de los clientes, sino que además puedan estar vinculados a casos de fraude interno, como es el caso del *whaling* o fraude al CEO. Del mismo modo, el acceso a mayor información de los clientes resultante de esta colaboración permitirá aumentar el conocimiento que se tiene del cliente y del contexto de uso habitual de los servicios financieros (como información biométrica), lo que, analizado de la manera adecuada, podrá aumentar las capacidades de la entidad en la prevención y detección del fraude, con el consecuente beneficio que esto conlleva tanto para

el cliente como para la organización.

- **Matching services.** Este concepto ha redefinido la manera en que se realizan las transacciones electrónicas, mediante la implementación de un mecanismo que verifica la correspondencia entre los detalles de una



cuenta que, de acuerdo con lo que propone PSR, sería el nombre del cliente y el identificador único (IBAN) proporcionado durante una transacción. Este servicio tiene como objetivo reducir el riesgo de fraude y los errores en las transferencias electrónicas, asegurando que los fondos se envíen a la cuenta correcta al requerir que el cliente introduzca datos que concuerden acerca del beneficiario.

- **Interfaz de acceso a datos (APIs).** Siguiendo la línea marcada por PSD2, PSR apuesta por evolucionar las interfaces de acceso a datos e iniciación de operaciones de pago para facilitar la interconexión entre los diversos participantes del sistema financie-

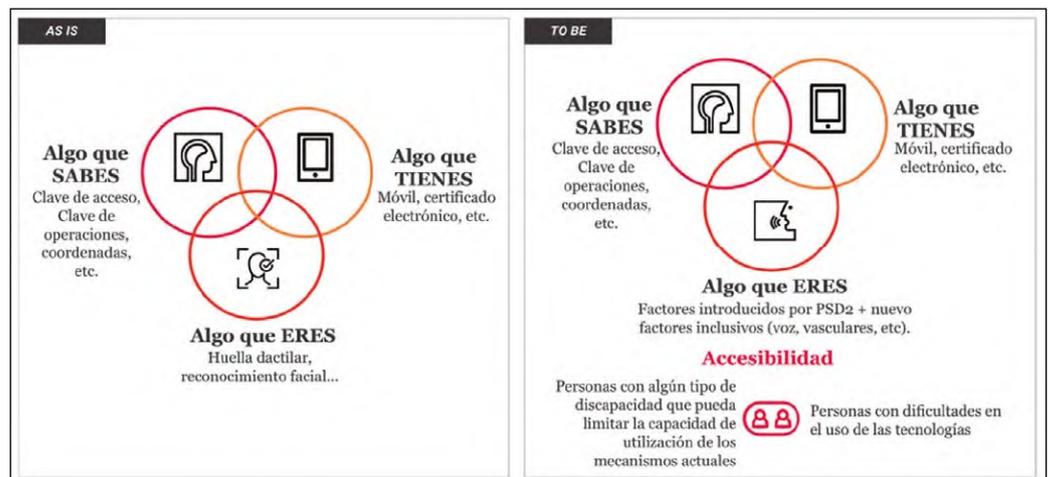
ción y la mejora continua.

- **Creación de un panel de control de gestión de los permisos otorgados por el cliente a los diferentes proveedores de servicios de pago.** En consonancia con las interfaces nombradas en el punto anterior, PSR establece la creación de un panel de control que permita ser empleado tanto por los servicios de información de cuentas como de iniciación de pagos. Además, alineado con la información en el alcance de FIDA, se establece la creación de un panel de control que muestre al cliente los distintos productos financieros para que pueda gestionar los permisos que conceda a terceros.

Por otro lado, el segundo reglamento propuesto por la Comisión Europea es el **Framework de Acceso a Datos Financieros (FIDA)** que, tal y como se describe en líneas anteriores, es el paso definitivo hacia el Open Finance. Su objetivo principal es garantizar el acceso regulado y seguro a la información de los clientes, vinculada a productos y servicios contratados por estos, extendiéndose más allá de los ofrecidos por los bancos. Esta evolución del ecosistema financiero introduce tres roles o actores clave que participarán en dicho acceso e intercambio de información:

- **Propietario de los datos.** Entidades dentro del alcance de la norma que son capaces de obtener, procesar y almacenar la información de los clientes.

- **Usuario de los datos.** Entidades que,





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.

previa autorización del cliente, soliciten acceso a la información del propietario de los datos.

• **Ciente.** Todas las personas físicas o jurídicas cuyos datos serán tratados por el propietario de los datos.

Además de expandir el alcance de la información accesible vinculada a productos y servicios prestados por organizaciones que no sean entidades bancarias, tales como empresas de seguros y pensiones, FIDA también amplía los límites de acceso a la información

financiera, más allá de la información vinculada a los servicios de iniciación de pagos e información de cuentas regulados por PSD2.

La participación de las entidades en el nuevo ecosistema financiero asumiendo el rol de usuario de datos en el contexto de FIDA incrementa las oportunidades de negocio de aquellas organizaciones que deseen ofrecer a sus clientes nuevos servicios personalizados y más orientados a las demandas del mercado a partir de la información que de ellos tengan otras entidades, previa autorización del cliente.

Por último, para complementar el nuevo paquete regulatorio, la Comisión Europea también ha presentado la tercera Directiva de Servicios de Pago (PSD3). Esta Directiva, desarrollada sobre las bases establecidas por la actual PSD2 y la Directiva de Dinero Electrónico (EMD2), es clave en la evolución de los servicios de pago. Entre otros aspectos, PSD3 amplía su alcance incluyendo en el mismo a las entidades de dinero electrónico (EMIs), y redefine el proceso de solicitud que han de seguir las diferentes entidades que pretendan incorporarse a este mercado. Además, PSD3 no queda indiferente ante la revolución a nivel regulatorio en la que se encuentra inmersa Europa y busca alinearse con otras regulaciones como DORA o GDPR.

Con este nuevo paquete regulatorio la Unión Europea emprende el camino hacia un nuevo paradigma orientado al intercambio de datos financieros dentro del espacio europeo. En definitiva, estas nuevas regulaciones serán los elementos fundamentales para homogeneizar un entorno financiero más abierto, competitivo e innovador en toda la Unión Europea.

	SERVICIOS	TIPO DE PRODUCTO	INSTITUCIONES AFECTADAS	
SERVICIOS FINANCIEROS	Préstamos	Préstamos	Instituciones de crédito	
	Cuentas	Cuentas corrientes, excepto las de pago		
	Hipotecas	Contratos de crédito hipotecario		
	Inversiones	Inversiones	Productos de ahorro	Entidades de dinero electrónico
			Inversiones en instrumentos financieros	Proveedores de servicios de criptoactivos
			Productos de inversión basados en seguros	Emisores de tokens referenciados en activos
			Criptoactivos	Empresas de inversión
			Bienes inmuebles	Gestores de fondos de inversión alternativos
Otros activos financieros conexos			Proveedores de servicios de crowdfunding	
Solvencia empresarial	Solvencia empresarial, no incluye los datos personales	Agencias de calificación de crédito		
SEGUROS	Seguros	Productos de seguros no relacionados con la salud o la vida	Empresas de seguros y reaseguros Intermediarios de seguros y complementarios	
PENSIONES	Pensiones individuales y ocupacionales	Planes de pensión de empleo	Proveedores de PEPP	
		Productos paneuropeos de pensiones individuales		

La apertura a otros sectores más allá del sector bancario

De acuerdo con lo comentado en el punto anterior, la llegada de FIDA representa un paso significativo en la expansión del Open Finance más allá del sector bancario. En este sentido, el acceso e intercambio de información financiera ha dejado de ser exclusivo de las entidades bancarias abarcando, al mismo tiempo, un espectro mayor de productos y servicios, y promoviendo las sinergias entre diversas organizaciones, tales como empresas de seguros y de pensiones.

Con todo esto, la principal novedad de FIDA es la implementación de un sistema de intercambio de información financiera del que surge un esquema en el que sus principales interlocutores son el propietario de los datos, el usuario de los datos y el cliente. Este sistema de intercambio de información financiera permite compartir la información relativa a los productos financieros en el alcance de la norma. De esta forma, y mediante la adhesión a uno de estos sistemas de intercambio de información financiera, tanto propietarios de los datos como usuarios de datos serán capaces de comunicarse y obtener la información que hayan solicitado siempre y cuando hayan obtenido los permisos oportunos por parte del cliente. Al mismo tiempo, el usuario de datos podrá presentar al cliente toda la información a la que ha accedido a través de un único panel de control.

Todo el proceso de intercambio de datos, reflejado en la figura anterior, supone una gran inversión y reestructuración a nivel tecnológico por parte de las organizaciones en el alcance de FIDA. Dicha inversión ha de

contemplar desde el desarrollo de nuevas interfaces dedicadas, o la evolución de las actuales, hasta la implementación de nuevos requisitos técnicos para el total alineamiento con los esquemas de acceso a datos financieros. En esta línea, el esquema SPAA elaborado por el *European Payment Council* (EPC) introduce diferentes flujos de servicios de iniciación de pagos e intercambio de información con el fin de facilitar a las entidades el cumplimiento normati-

vo desde un punto de vista técnico, y que previsiblemente serán requeridos para posibilitar la adhesión a los sistemas de intercambio de información financiera que surjan como respuesta a las exigencias de FIDA.

En relación con la adhesión a los sistemas de intercambio de información, surgen desafíos adicionales como la estandarización de sistemas y datos vinculados a los productos y servicios que entidades financieras, como empresas de seguros y de pensiones, deban poner a disposición de sus clientes, así como la evolución o implementación de una infraestructura tecnológica segura, robusta y capaz de soportar el intercambio de información cumpliendo con los requisitos de FIDA para disponibilizar la información requerida por el cliente de forma continua y en tiempo real.

Más allá de las figuras o actores intervinientes en el intercambio de información financiera, otra pieza clave para la adecuada evolución hacia el Open Finance, es la colaboración entre todas las instituciones participantes en el ecosistema financiero, esto incluye autoridades de control y supervisoras como el BCE, la DGS o AESPJ (estas dos últimas introducidas dentro del marco de FIDA), así como la EBA o la EIOPA. La comunicación entre dichas entidades y organismos supervisores será clave tanto para el reporte de incidentes como para el desarrollo de medidas de control que deban aplicarse sobre las instituciones. Asimismo, el desarrollo de las RTS cuya publicación se espera en el marco del nuevo paquete regulatorio estará a cargo de la EBA en colaboración con la EIOPA que desarrollará directrices que completarán las RTS.



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

Riesgos en el horizonte del Open Finance

Aunque el nuevo paradigma financiero trae consigo múltiples beneficios y oportunidades no se puede pasar por alto que este también viene acompañado de nuevos riesgos, por lo que conviene que, de forma temprana, todas las organizaciones en el alcance del nuevo paquete regulatorio propuesto analicen y valoren el impacto de, al menos, los siguientes **riesgos en materia de privacidad, fraude y seguridad de la información**:

- **Exposición de datos sensibles:** en paralelo al incremento sobre el volumen de los datos sensibles accedidos y compartidos a través de las interfaces y plataformas que proponen tanto FIDA como PSR, aumenta también el riesgo de que esta información quede expuesta como resultado de vulnerabilidades o errores de seguridad en la implementación de dichas interfaces y plataformas. En este sentido, la aplicación del principio de limitación del tratamiento será clave para evitar riesgos derivados de los datos considerados sensibles.

- **Incumplimiento de regulaciones aplicables en materia de privacidad:** el procesamiento y uso de datos sensibles debe estar alineado con el GDPR aplicable en la UE. Si no se garantiza que el uso de los datos asociados a FIDA y PSR se lleva en consonancia con el mismo, las organizaciones en el alcance de FIDA y PSR podrían tener que afrontar multas o sanciones vinculadas al incumplimiento de estas regulaciones.

- **Transacciones fraudulentas:** los productos y servicios que se pretende poner a disposición de los clientes como resultado de la aplicación de FIDA como PSR, abre la puerta a que los ciberatacantes evolucionen sus tácticas de *spoofing* (*phishing*, *smishing*, *vishing* o *whaling*, entre otros) logrando acceder a la información necesaria de los clientes para ejecutar transacciones fraudulentas.

- **Acceso no autorizado:** las organizaciones deberán revisar y optimizar sus controles de acceso y autorización, con especial relevancia a la gestión de consentimientos concedidos por los clientes para el acceso a sus datos. Actualmente, prácticas como el *screen scraping* implican un importante riesgo en este sentido ya que se pierde gran parte



del control sobre los datos que se exponen independientemente de la autorización que el cliente haya concedido.

- **Autenticación:** FIDA y PSR deben garantizar una autenticación reforzada del cliente para evitar el acceso no autorizado, siendo necesaria la evolución de los mecanismos de autenticación a la situación y las tecnologías actuales (como es el caso de la ciberbiometría y los patrones de comportamiento en la prevención del fraude).

- **Errores en la implementación TIC:** la necesidad de integrar diferentes sistemas y plataformas incrementa el riesgo de incompatibilidades que podrían ser explotadas para

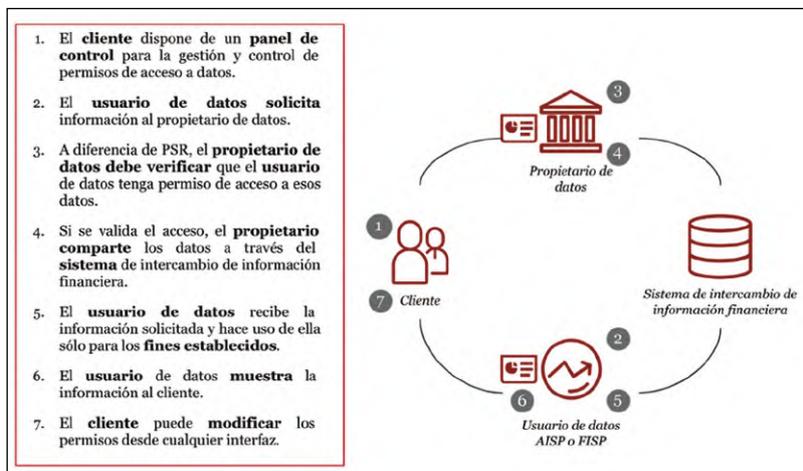
como el impacto de las mismas, sobre los servicios que prestan y sobre su infraestructura TIC a corto, medio y largo plazo.

Cabe mencionar que aquellas organizaciones que cuenten con el conocimiento y los recursos necesarios para llevar a cabo dicho análisis y, a partir de este, diseñar una hoja de ruta que trace los hitos y objetivos a alcanzar para adaptarse a las exigencias aplicables, podrán anticipar los riesgos que vienen de la mano del nuevo paquete regulatorio, establecer de forma temprana las medidas y mecanismos de seguridad, privacidad y prevención del fraude necesarios para abordarlos, y posicionarse como referentes en la evolución

hacia el Open Finance, sorteando adecuadamente la complejidad tecnológica que tiene asociada.

Una temprana adecuación a este nuevo paquete regulatorio permitirá identificar y aprovechar las ventajas competitivas derivadas del mismo, como puede ser la prestación de nuevos servicios financieros o el incremento en la seguridad y la fiabilidad de las organizaciones de cara a los clientes. Otro de los aspectos clave es la evolución en las capacidades

de gestión del fraude gracias al refuerzo en la formación y concienciación de clientes y empleados en esta materia, la coordinación intra e intersectorial (con mecanismos como los *matching services* o el nuevo rol de los proveedores de comunicaciones electrónicas) y el mejor conocimiento de los clientes y su contexto de uso de los servicios financieros para alimentar las herramientas de monitorización de transacciones y detección de fraude. ■



comprometer la seguridad de la infraestructura tecnológica de las entidades en el alcance del paquete regulatorio propuesto.

Por otro lado, las diferentes organizaciones en el alcance de FIDA y PSR deben permanecer vigilantes a la evolución del borrador de propuesta de paquete regulatorio, así como a la publicación de las RTS por parte de los organismos supervisores, y que podrían incluir nuevas medidas orientadas a la gestión de los riesgos mencionados.

Conclusiones: Aspectos a tener en cuenta para hacer frente al nuevo paradigma

Las entidades financieras, con especial mención a las empresas de seguros y pensio-

PEDRO CERVERA RUIZ
Director de Organización y Operaciones
IBERCAJA

JUAN GALDÓN
Director en Business Security Solutions
PWC

kartos[®]

#AlwaysWatching

XTI watchbots

Plataforma de cibervigilancia e inteligencia

XTI Extended CTI Watchbots Platform

- EASM (External Attack Surface Management) •
- DRPS (Digital Risk Protection Services) •
- SRS (Security Rating Services) •



www.enthec.com

Kartos es una marca registrada de **ENTHEC**

Sí a la Inteligencia Artificial, pero con garantías

El mundo sigue en constante avance. Las distintas crisis que estamos viviendo junto a nuevos escenarios tecnológicos hacen las organizaciones innoven y se transformen constantemente. La tecnología es la palanca, donde ha irrumpido con gran vehemencia la Inteligencia Artificial. Consecuencia de esto, ISO publicó en el pasado diciembre la nueva ISO/IEC 42001 de Sistema de Gestión de Inteligencia Artificial. Desde AENOR, damos las principales claves para entender y aplicar con garantías, este nuevo estándar, y su estrecha relación con la ciberseguridad, la privacidad y los nuevos reglamentos europeos.



BORIS DELGADO / CARLOS MANUEL FERNÁNDEZ

Covid-19, Transformación Digital e Inteligencia Artificial

Se cumplen cuatro años de aquel 2020, marcado para siempre en la historia por la pandemia del Covid-19. Aquella crisis mundial realizó una transformación social que precipitó la digital, por tres razones:

- 1. La necesidad de mantener la actividad económica y social**, que nos llevó a una rápida adopción de soluciones digitales, como el teletrabajo, la telemedicina y la enseñanza virtual.
- 2. La inversión de las AAPP en tecnología**, que hizo que los gobiernos de todo el mundo destinaran importantes recursos a la digitalización de sus servicios públicos y dar apoyo a las empresas en la transformación digital, como son los Fondos NextGeneration.
- 3. La concienciación sobre la importancia de la tecnología**, como elemento fundamental para hacer frente a las crisis. Esto despertó un mayor interés por la digitalización a ciudadanos y organizaciones.

Estas razones, avalan los datos aportados por diferentes analistas, que indican que el 70% de las empresas españolas impulsaron su proceso de digitalización durante la pandemia.

Este impulso hacia lo digital en las organizaciones ha propiciado la innovación y la adopción de tecnologías habilitadoras. Sin duda, la que ha irrumpido con mayor relevancia es la inteligencia artificial – IA.

En la reunión anual de enero 2024 en Davos, del World Economic Forum se afirmó: “La inteligencia artificial es la fuerza impulsora de la economía y la sociedad”, donde los avances en tecnología tienen el potencial de ayudarnos a resolver desafíos globales.

Como resultado han puesto en marcha la **AI Governance Alliance**, que une a líderes de la industria, gobiernos, instituciones académicas y organizaciones para defender el diseño global responsable y la **provisión de sistemas de inteligencia artificial transparentes, inclusivos y seguros**.

Efectivamente la IA puede tener el potencial de transformar radicalmente la forma en que vivimos, trabajamos y nos relacionamos. Sin embargo, también plantea una serie de riesgos a los que atender, como pueden ser la discriminación, los sesgos o aquellos relacionados con la ciberseguridad y la privacidad. Es decir, su uso y aplicación tiene muchos beneficios, si bien el uso inadecuado de esta tecnología o la falta de control se perciben como riesgos que requieren una gestión con todas las garantías.

IA con garantías: ISO/IEC 42001

Tras lo comentado anteriormente, después de varios años de trabajo, ISO publicó en diciembre del año pasado el estándar **ISO 42001 - Sistema de Gestión de Inteligencia Artificial (SGIA)**. No es el primer estándar que trata la IA, pero sí es

el primero que propone un sistema de gestión certificable.

La ISO/IEC 42001 es un estándar o *best-practices* consensuada a nivel internacional por más de 155 países y expertos, que ayudan a las organizaciones a desarrollar e implementar un SGIA que permita garantizar que los sistemas y productos de IA se desarrollan y utilizan de forma responsable. Para ello:

1. Promueve el desarrollo y la utilización de sistemas de IA:

- **Fiables:** los sistemas de IA deben ser capaces de realizar sus tareas de forma precisa y consistente. Por este motivo, las IA generativas deben ser coherentes e íntegras.
- **Transparentes:** los sistemas de IA deben ser comprensibles y explicables para los usuarios y las partes interesadas. Lo que se denomina IA explicativa.

La ISO/IEC 42001 mantiene la estructura documental en sus apartados del 4 al 10 según la estructura de alto nivel basado en la gestión de riesgos, aplicación de controles para su mitigación y ciclo de Demming (PDCA o mejora continua).

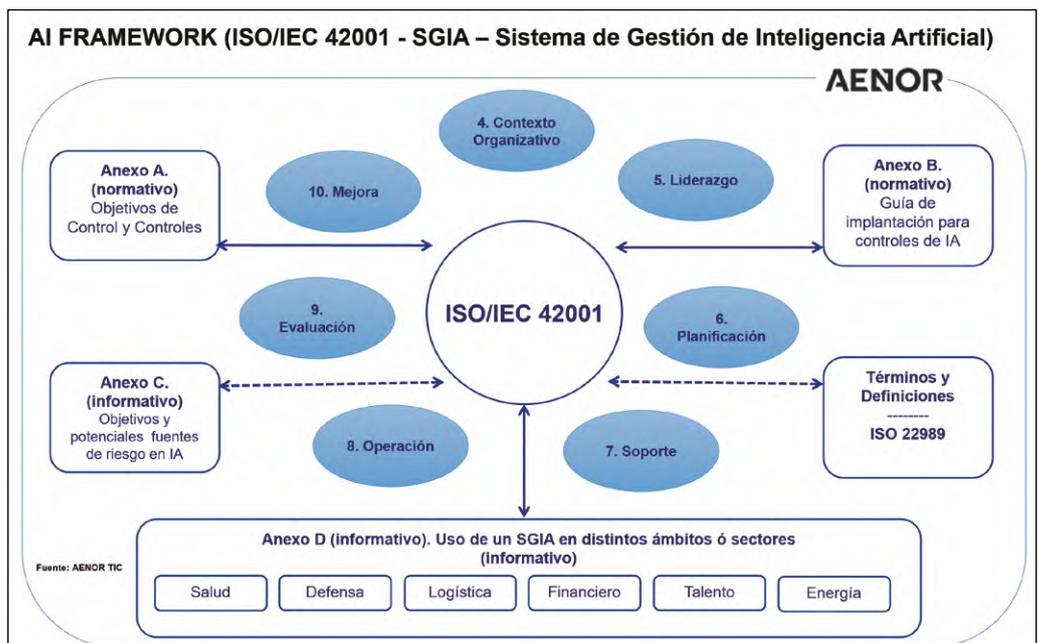


Figura 1.- AI Framework según ISO/IEC 42001.



Ayudándote a aprovechar todo el potencial de la tecnología, para construir un futuro en el que todos podemos confiar.

• **Responsables:** los sistemas de IA deben ser utilizados de forma que se minimice el riesgo de daños o perjuicios a las personas o al medio ambiente.

2. Apela a los principios y valores éticos a la hora de desplegar sistemas de IA, como la equidad, la no discriminación y el respeto a la seguridad y privacidad de los datos.

3. Facilita un proceso para la evaluación y gestión de riesgos y controles, relacionados con la implantación de la IA.

4. Prioriza el bienestar de las personas, la seguridad y la experiencia del usuario en el diseño y despliegue de la IA.

5. Ayudar a las organizaciones a gestionar el cumplimiento de las regulaciones en esta materia. En este sentido es compatible con los principios del reglamento europeo de IA, considerando que uno de los pilares es la clasificación de los sistemas de IA en función de su nivel de riesgo, poniendo especial atención en aquellos de alto riesgo para garantizar la seguridad y la privacidad.

La ISO/IEC 42001, mantiene la estructura documental en sus apartados del 4 al 10 según la estructura de alto nivel (HLS), basado en la gestión de riesgos, aplicación de controles para su mitigación y ciclo de Demming (PDCA o mejora continua). Esto permite su integración con otros sistemas de gestión como la veterana ISO 27001 de sistemas de gestión de seguridad de la información o la ISO 27701 de sistemas de gestión de privacidad de la información.

Además, se completa con cuatro anexos que facilitan y ayudan a la comprensión de los posibles riesgos e implantación de controles, además de los principales ámbitos o sectores que pueden verse afectado (ver **Figura 1**).

Entre estos anexos cabe destacar el anexo A. Objetivos de control y controles, donde podemos identificar 10 objetivos de control y 38 controles (ver **Figura 2**).

A1. General, que proporciona una referencia (declaración de aplicabilidad) de controles para cumplir los objetivos organizativos y gestionar los riesgos relacionados con el diseño y el funcionamiento de los sistemas de IA.

A2. Políticas relacionadas con la IA: proporcionar las directrices de gestión y soporte a los sistemas de IA de acuerdo con los requisitos de la organización

A3. Organización interna: establecer el compromiso firme dentro de la organización para mantener su enfoque adecuado de la implantación, el funcionamiento y la gestión de los sistemas de IA.

A4. Recursos para Sistemas de IA: asegurar

Estructura de ISO/IEC 42001 – Sistema de Gestión de IA

0. INTRODUCCION	
1. ALCANCE	
2. REFERENCIAS NORMATIVAS	
3. TERMINOS Y DEFINICIONES	
4. CONTEXTO DE LA ORGANIZACIÓN	
5. LIDERAZGO	
6. PLANIFICACION	
7. SOPORTE	
8. OPERACIÓN	
9. EVALUACION	
10. MEJORA	
ANEXO A. OBJETIVOS DE CONTROL Y CONTROLES	
A1. GENERAL	
A2. POLITICAS RELACIONADAS CON LA IA	
A3. ORGANIZACIÓN INTERNA	
A4. RECURSOS PARA SISTEMAS DE IA	
A5. EVALUACION DE IMPACTO EN SISTEMAS IA	
A6. CICLO DE VIDA DE UN SISTEMA IA	
A7. DATOS PARA SISTEMAS IA	
A8. INFORMACION PARA LAS PARTES INTERESADA DE SISTEMAS IA	
A9. USO DE SISTEMAS IA	
A10. RELACION DE TERCERAS PARTES Y CLIENTES	
ANEXO B. GUIA DE IMPLANTACION PARA CONTROLES DE IA	
ANEXO C. OBJETIVOS Y POTENCIALES FUENTES DE RIESGO EN IA	
ANEXO D. USO DE UN SGIA EN DISTINTOS AMBITOS O SECTORES	

Figura 2.- Estructura de ISO/IEC 42001 – Sistema de Gestión de IA.

La estructura documental de la ISO/IEC 42001 permite su integración con otros sistemas de gestión como la veterana ISO 27001 de sistemas de gestión de seguridad de la información o la ISO 27701 de sistemas de gestión de privacidad de la información.

que la organización identifica los recursos (incluidos los procesos/servicios/productos y activos del sistema de IA) para comprender y abordar consecuentemente posibles riesgos e impactos.

A5. Evaluación de impacto en sistemas IA: asegurar que se determinan los impactos del sistema de IA sobre los individuos o colectivos por el sistema de IA a lo largo de su ciclo de vida.

A6. Ciclo de Vida de un sistema IA: asegurar que la organización identifique y documente los objetivos y aplique procesos para el diseño y desarrollo responsables de sistemas de IA.

A7. Datos para Sistemas IA: asegurar que la organización comprende el papel y las repercusiones de los datos en los sistemas de IA en la aplicación y el desarrollo, la provisión o el uso de los sistemas de IA a lo largo de sus ciclos de vida.

A8. Información para las partes interesadas de sistemas IA: asegurar que las partes interesadas pertinentes dispongan de la información necesaria para comprender y evaluar los riesgos y sus repercusiones (tanto positivas como negativas).

A9. Uso de Sistemas IA: asegurar que la organización utiliza los sistemas de IA de forma

responsable y conforme a las políticas de la organización.

A10. Relaciones de terceras partes y clientes: asegurar que la organización comprende sus responsabilidades, y que los riesgos se reparten de forma transparente cuando intervienen terceros en cualquier fase del ciclo de vida del sistema de IA.

La incorporación de la IA plantea la gestión de nuevos riesgos que requieren la aplicación de controles. Por ejemplo, los sistemas de IA, en el análisis y uso de datos, realizan un aprendizaje automático y continuo, los cuales permiten cambiar su comportamiento durante su uso. Esto requiere una consideración especial para garantizar que su uso responsable continúe a pesar de este tipo de comportamiento.

GarantIA a través de las normas y estándares

AENOR, fiel a su propósito de aportar soluciones que crean confianza entre organizaciones y personas, y ante los escenarios y desafíos como lo es la inteligencia artificial, consideramos que esta nueva ISO/IEC 42001 permitirá disponer de una herramienta muy potente para la gestión de los

sistemas y productos de IA, donde AENOR ya está trabajando con organizaciones que lo están implantando para su próxima certificación.

En definitiva, las organizaciones que ya están incorporando en su estrategia la IA, deben:

- Considerar a sus *stakeholders*, sus objetivos, y el difícil equilibrio entre los riesgos y los beneficios.

- Concienciar y capacitar a los empleados, determinando posibles nuevas habilidades y conocimientos. Valorar la inversión en la formación de los empleados para que puedan aprovechar el potencial de esta tecnología para que no sea una amenaza sino una oportunidad.

- Adoptar un enfoque responsable, ético, con garantías de (ciber)seguridad y privacidad. ■

BORIS DELGADO
Director de Industria y TIC
bdelgado@aenor.com

CARLOS MANUEL FERNÁNDEZ
Asesor Estratégico de TI
cmfernandez@fidesol.org

AENOR

“En el mundo empresarial,
el verdadero progreso es estar atento
a cómo la evolución de la tecnología
abre nuevas puertas”
Steven Johnson, escritor y experto en innovación



Cuando la tecnología permite el progreso,
ESET está aquí para protegerlo.

www.eset.es

eset[®]

Digital Security
Progress. Protected.

BSAM: Creando un ecosistema Bluetooth seguro y confiable



En la actualidad existen más de 6.000 millones de dispositivos Bluetooth en el mundo. Esta tecnología inalámbrica es ideal para su uso en IoT y en IIoT. Con el objetivo de ayudar a mejorar la seguridad en Bluetooth, la compañía española Tarlogic ha desarrollado durante el último año BSAM (Bluetooth Security Assessment Methodology), una metodología abierta con la que evaluar las implementaciones de los fabricantes y la seguridad de las comunicaciones en todas sus etapas.

MIGUEL TARASCÓ / ANTONIO VÁZQUEZ

Bluetooth es una tecnología inalámbrica de corto alcance diseñada para la transmisión de datos y voz entre dispositivos. Se caracteriza por su bajo consumo de energía y su capacidad para conectar una gran variedad de dispositivos, lo que la hace ideal para aplicaciones en el Internet de las Cosas (IoT) y el Internet Industrial de las Cosas (IIoT).

En el mercado del IoT e IIoT, Bluetooth se ha posicionado como una opción económica debido a su amplia disponibilidad en dispositivos de consumo y su facilidad de implementación. Además, su enfoque en la usabilidad se refleja en la facilidad con la que los usuarios finales pueden emparejar y administrar dispositivos Bluetooth.

Con el desarrollo de diferentes versiones, como Bluetooth Low Energy (BLE), la tecnología ha evolucionado para satisfacer las necesidades de aplicaciones que requieren bajo consumo de energía, como sensores inalámbricos y dispositivos portátiles. En la actualidad existen más de 6.000 millones de dispositivos Bluetooth en el mundo.

Si bien es una tecnología ampliamente extendida, se trata de un estándar complejo y con muchas funcionalidades, que se han ido extendiendo año a año, y están implementadas en hardware y *firmware*. Estos factores, y la ausencia de fuentes de información centradas en la seguridad, ha provocado que no haya sido analizado con tanto detalle, como sí ha sucedido con otras tecnologías inalámbricas como Wi-Fi (802.11).

La ubicuidad de Bluetooth requiere que como sector tomemos conciencia de la importancia de la seguridad de esta tecnología y de su impacto en los dispositivos que lo implementan.

La Bluetooth Security Assessment Methodology (BSAM) se presenta como una metodología colaborativa y abierta para la evaluación de seguridad en dispositivos con capacidades Bluetooth. Diseñada para estandarizar la evaluación de seguridad de dispositivos que hacen uso de la tecnología bluetooth y para guiar a fabricantes, investigadores y profesionales de ciberseguridad durante el proceso de diseño e implementación, la etapa de auditoría y verificación de su seguridad.

BSAM aborda la complejidad y variabilidad del estándar Bluetooth, proporcionando un marco integral de controles de seguridad. Su aplicación se extiende a dispositivos IoT en diversos sectores, desde dispositivos personales y de transporte hasta dispositivos domésticos, de salud o industriales.

En constante desarrollo, el proyecto BSAM busca crear una guía completa, expandiendo secciones de documentación y recursos, y vinculando controles con estándares de seguridad reconocidos, como GSMA IoT Security Assessment e IEC 62443 para ciberseguridad industrial.

BSAM es un estándar con el que evaluar y mejorar la seguridad en dispositivos Bluetooth, y contribuye significativamente en la protección de la privacidad y la integridad en el entorno de comunicaciones inalámbricas.

Objetivos de BSAM

Con el objetivo de ayudar a mejorar la seguridad en Bluetooth, Tarlogic ha desarrollado durante

el último año BSAM, una metodología abierta con la que evaluar las implementaciones de los fabricantes y la seguridad de las comunicaciones en todas sus etapas.

De este modo se reduce la barrera de entrada para evaluar la seguridad de dispositivos que hacen uso de tecnología Bluetooth, ya que BSAM



define los controles a analizar durante un proceso de auditoría, prestando especial atención a aquellos aspectos en los que pueden existir problemas de seguridad o privacidad debido a diferencias en la implementación de las comunicaciones por parte del fabricante.

BSAM pone su foco en aspectos relevantes del estándar, reduciendo el tiempo necesario para un análisis de seguridad Bluetooth. El establecimiento de un marco de referencia abierto y común permite realizar auditorías de manera metódica garantizando su rigor, y posibilita la comparación de la seguridad entre dispositivos Bluetooth diferentes y medir la evolución de la seguridad en el tiempo.

Para facilitar su uso por parte de profesionales

BSAM aborda la complejidad y variabilidad del estándar Bluetooth, proporcionando un marco integral de controles de seguridad. Su aplicación se extiende a dispositivos IoT en diversos sectores, desde los personales y de transporte hasta domésticos, de salud o industriales.

VULNERABILIDADES Y PORCENTAJES



El 50% de gadgets como ratones inalámbricos o mandos de videoconsola son emparejables por defecto. Lo que implica que actores maliciosos puedan capturar datos específicos de los dispositivos y llegar a suplantarlos para acceder a otros aparatos como ordenadores.

El 80% de los dispositivos IoT analizados son descubribles y trazables. Esto supone un gran riesgo para la privacidad de las personas, al permitir monitorizar sus movimientos y acciones.

El 20% de dispositivos como televisiones o manos libres emplean códigos PIN por defecto para emparejarse con otros aparatos, tales como 0000 o 1111.

El 90% de los aparatos permiten acceder a información confidencial para lanzar ataques más avanzados.

CentOS & RHEL support for years to come



How to Face Linux Distro End-of-Life Challenges

Navigating the evolving open source landscape



- Enjoy proven enterprise support from a partner who understands Linux.
- Keep your current operating system with SUSE Liberty Linux.
- Get predictable releases and support RHEL/CentOS.
- Expand your IT lifecycle, without migrations.
- Embrace an open Linux with no restrictions.

End of life doesn't mean
end of the road



With SUSE, choice
happens

y compañías de todo el mundo, se ha diseñado BSAM partiendo de una estructura sencilla, clara e intuitiva, en la que se sintetiza el conocimiento sobre Bluetooth y sus riesgos.

– **Documentación** sobre el estándar Bluetooth y su funcionamiento.

– **Controles**, con las verificaciones técnicas que se han de realizar para analizar la seguridad de los dispositivos desde la óptica del protocolo Bluetooth.

– **Recursos** y herramientas para facilitar la ejecución y evaluación de los controles.

BSAM se estructura en torno a 36 controles, que se deben evaluar individualmente para asegurar la seguridad en las comunicaciones Bluetooth. Estos controles se organizan en siete categorías principales:

- 1. Recolección de Datos de Componentes Bluetooth.** Para una evaluación efectiva de la seguridad Bluetooth, es crucial recabar información pública del dispositivo y sus componentes Bluetooth para tener un punto de partida del estado del arte de la seguridad de ese dispositivo.
- 2. Seguridad en la Fase de Descubrimiento Bluetooth.** Los controles en esta sección están enfocados en asegurar que las configuraciones durante el descubrimiento Bluetooth no son vulnerables ni revelan información sensible.
- 3. Seguridad en el Emparejamiento Bluetooth.** Analizar las configuraciones y los métodos de emparejamiento es vital para asegurarse de que no se permiten emparejamientos de dispositivos no autorizados o sin supervisión del usuario. El emparejamiento es un aspecto crítico en la seguridad Bluetooth, razón por la cual se incluyen hasta 10 controles específicos en este ámbito.
- 4. Seguridad en la Autenticación Bluetooth.** Estos controles están diseñados para verificar que no se pueden autenticar dispositivos desconocidos, lo que podría resultar en la fuga de información privada.
- 5. Seguridad en el Cifrado de Comunicaciones Bluetooth.** En esta categoría, los controles evalúan la seguridad en el cifrado de las comunicaciones Bluetooth para asegurarse de que no se transmitan datos sensibles sin proteger, evitando así la posible filtración de información confidencial.
- 6. Seguridad en servicios Bluetooth.** Al emplear la metodología de evaluación de seguridad Bluetooth, los evaluadores deben comprobar que no es posible acceder a servicios sin los permisos adecuados.
- 7. Seguridad en la capa de aplicación Bluetooth.** Los últimos controles de BSAM analizan la seguridad de las aplicaciones de un dispositivo expuestas a través de servicios Bluetooth.



En constante desarrollo, el proyecto BSAM busca crear una guía completa, expandiendo secciones de documentación y recursos, y vinculando controles con estándares de seguridad reconocidos, como GSMA IoT Security Assessment e IEC 62443 para ciberseguridad industrial.

A lo largo del desarrollo de BSAM, el equipo de Innovación de Tarlogic empleó esta metodología para **auditar múltiples dispositivos de consumo masivo** que emplean la tecnología Bluetooth para comunicarse. Esta investigación permitió constatar que:

- El 50% de *gadgets*, como ratones inalámbricos o mandos de videoconsola, son **emparejables por defecto**. Lo que implica que actores maliciosos puedan capturar datos específicos de los dispositivos y llegar a suplantarlos para acceder a otros aparatos como ordenadores.
- El 80% de los dispositivos IoT analizados son “descubribles” y trazables. Esto supone un gran **riesgo para la privacidad de las personas**, al permitir monitorizar sus movimientos y acciones.
- El 90% de los aparatos permiten acceder a información confidencial, necesaria para realizar **ataques más avanzados**.
- El 20% de dispositivos, como televisiones o manos libres, emplean **códigos PIN por defecto para emparejarse con otros aparatos**, tales como 0000 o 1111.

Estas vulnerabilidades de los dispositivos Bluetooth pueden explotarse para:

- Suplantar teclados y ratones inalámbricos para **atacar ordenadores corporativos y personales**, tomar el control y sustraer información crítica.
- Obtener **datos médicos** a partir de dispositivos, como equipos de apnea del sueño o pulsioximetría.
- Escuchar **conversaciones privadas** vulneran-

do *gadgets* de nuestro día a día, como mandos de videoconsolas, altavoces inteligentes o auriculares Bluetooth.

- Emplear toda clase de dispositivos IoT para lanzar **ataques más sofisticados** contra instituciones, empresas, directivos y ciudadanos.

Un número importante de riesgos que sólo estamos empezando a vislumbrar.

El futuro de BSAM

El trabajo realizado hasta la fecha es el germen que permitirá una progresiva adopción de BSAM como estándar por parte de la industria y, de la mano a las directivas comunitarias, reducir el riesgo de los dispositivos IoT.

La evolución de la tecnología Bluetooth requerirá que BSAM se adapte para contemplar nuevos riesgos. Pero este trabajo debe estar acompañado de un importante esfuerzo de divulgación desde la industria y de la elaboración de productos de seguridad que automaticen y amplíen la profundidad de las pruebas técnicas de seguridad Bluetooth. ■

* BSAM puede ser consultado en: <https://www.tarlogic.com/bsam/>

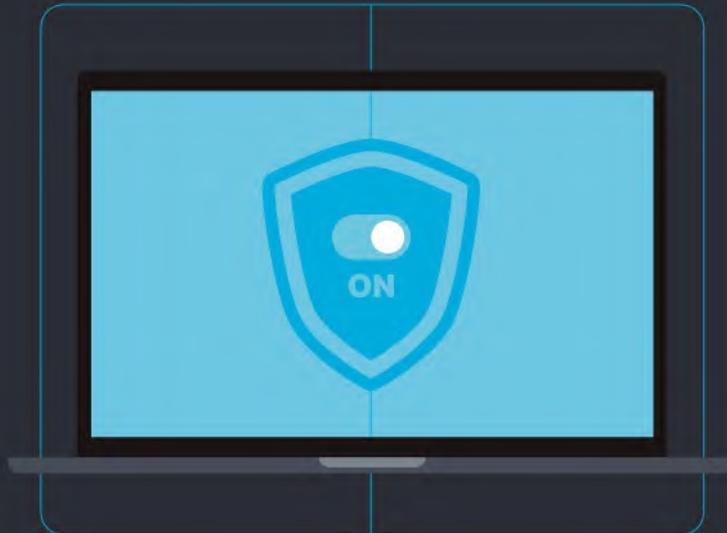
MIGUEL TARASCÓ
R&D Director and Co-founder

ANTONIO VÁZQUEZ
Cyber Security Researcher

TARLOGIC

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



Con más de 250 asistentes, en su novena edición se evidenciaron los grandes desafíos, novedades e innovaciones en este frente digital

IdentiSIC 2023: La protección de la identidad digital y el marco específico europeo deben blindarse frente a la delincuencia y el mal uso de los sistemas de IA



IdentiSIC, el congreso de referencia sobre la protección de la identidad, puso en valor en su IX edición la madurez de la industria en sus enfoques, la innovación a través de conceptos como ITDR, de detección y respuesta a incidentes en este ámbito, así como el debate aún muy abierto sobre cómo se aplicará el nuevo marco europeo de identidad y las carteras digitales. Además, en su marco se profundizó en la evolución de la IA, las tecnologías passwordless de FIDO y la especialización en la seguridad de la identidad en entornos OT e IoT. Tampoco faltaron debates sobre los grandes retos en este ámbito de la mano de referentes de la prescripción y consultoría, como PwC España y Telefónica, y del desarrollo de tecnologías con foco expreso, como Delinea, ForgeRock, Okta, Omada, SailPoint y WatchGuard.

IdentiSIC es uno de los congresos más esperados por el creciente ramo de la protección de la identidad. Y es que, ya hay en el mundo más de 2.000 empresas que trabajan en esta área. Se calcula –según publicó SIC 157– que este año se invertirá en protección de la identidad tanto como en nube, por considerarla un pilar estratégico de cualquier plan de seguridad digital, una situación que propició que esta edición del congreso reuniera a grandes referentes y más de 250 asistentes, en presencial y en remoto.

La primera jornada, que comenzó condu-

ciendo el director de **Revista SIC**, **José de la Peña**, contó con la 'puesta al día' del nuevo marco europeo de identidad digital, eIDAS2, y las carteras digitales que se esperan desplegar, a cargo de la reconocida abogada, **Paloma Llana**, CEO de **Razona Legaltech** y directora técnica del Esquema eIDAS&eIDE en **CerteIDAS**. En su conferencia 'eIDAS2, carteras de identidad digital y PSC cualificados ante la encrucija-

da de su certificación y supervisión en la UE', destacó el reto de las certificaciones nacio-



Paloma Llana

nales de las carteras digitales, entre las iniciativas más notables, así como la evolución de la estandarización eID (*electronic IDentification*), apoyada por la Comisión Europea.

Además, puso en valor el acuerdo que alcanzaron en noviembre en este ámbito tanto el Consejo, como la Comisión y el Parlamento, que



EVOLUCIÓN DE FIDO EN DETALLE...



permitirá que, a finales del primer trimestre de 2024, el texto final del eIDAS2 sea publicado en el Diario Oficial de la UE, con “más de 20 actos de implantación, además del Reglamento”, entre ellos, los de estandarización.

No faltó en su intervención la denuncia en torno a cómo algunas multinacionales tecnológicas, como Google o Mozilla, están planteando una campaña amparada en la privacidad de los usuarios para no perder peso. “La realidad es que es estamos ante una disputa” que es “cuestión de poder”. Pero también resaltó que es “radicalmente falso que haya una ‘persona interpuesta’ en todas las operaciones, porque esto no funciona así”. Terminó su intervención recordando que España es uno de los referentes en identidad digital con 47 prestadores cualificados, siendo



Jorge Arrufat

el mercado más grande de Europa, frente a países como el Reino Unido donde sólo hay uno. Además, alertó de que “el periodo del salvaje oeste de las corporaciones, en este entorno, está acabando para entrar en el camino de las regulaciones”. Eso sí, también auguró que las carteras digitales darán pie a un “mercado negro de atributos”, contra el que habrá que luchar.

Mundo sin contraseñas

A continuación, el CISO de BBVA Next Technologies, Jorge Arrufat, destacó “los logros y el futuro de la estandarización de tecnologías para la autenticación de usuarios en un mercado global”, a través de iniciativas como FIDO (*Fast Identity Online*), que nació para reforzar los “mecanismos de seguridad tradicionales, como *password*, 2FA,

etc.” y puso en valor el foco que se ha puesto “en la experiencia del usuario (UX) para garantizar que las credenciales criptográficas no abandonen su dispositivo”, además de incrementarse los mecanismos de identificación biométrica, que ya se usa más “que el segundo factor”. Eso sí, también planteó que “queda mucho por hacer, ya que es un camino muy largo, porque sólo el 30% usa el 2FA para acceder a servicios financieros”.

Arrufat mostró cómo ha evolucionado el estándar FIDO, adoptado por grandes tecnológicas como **Microsoft**, **Google** o **Amazon**, desde su primera especificación en 2013, con notables “bondades” y “claros beneficios, como el uso de medios que sólo tiene el usuario, como la biometría o la clave criptográfica, que refuerza la seguridad ante ataques de *phishing*, *replay*... que son los más habituales”.

Finalizó poniendo en valor grandes retos, como reducir el uso de contraseñas, el fortalecimiento de 2FA y MFA, y recordó que, seguramente, las “*passkey* serán el futuro, aunque su implementación es compleja, sobre todo, para las medianas empresas”.

En definitiva, para mejorar es clave “remar todos en la misma dirección, sector privado y público”, señaló, “contando más que nunca con marcos y estándares comunes”.

En detalle

Acto seguido, el editor de Revista SIC, Luis Fernández, presentó a Julio Castilla, director de Identity & Data Governance en **Business Security Solutions (BSS)** en **PwC España**, junto con Daniel Álvarez, senior manager de la consultora, que mostraron uno de los enfoques más novedosos en protección de la identidad conocido por sus siglas ITDR (*Identity Threat Detection and Response*).

PwC España apuesta por ITDR como evolución lógica en protección de la identidad

Julio Castilla y Daniel Álvarez, de PwC España, mostraron en *Identidad SIC* el estado, evolución y retos de ‘ITDR: evolucionado la gestión de amenazas IAM’, una ponencia en la que recordaron que esta sofisticada propuesta de ciberprotección no “sustituye al mundo IAM, PAM, etc., sino que viene a complementarlo, porque permite proteger la infraestructura de IAM y optimizar la detección y respuesta de ataques basados en compromisos de identidad”, explicó Castilla, quien resumió este concepto como un buen ejemplo de un enfoque de confianza cero y capacidades proactivas. “Que haya sido necesario desarrollar ITDR da una idea de la complejidad y sofisticación de las amenazas”, añadió Álvarez. Así, entre otros aspectos de interés, destacaron las “seis etapas en la que actual ITDR: prevención, monitorización, detección, análisis de

amenazas, probabilidad e impacto, con una capacidad de respuesta en base a unas reglas de actuación preestablecidas, además de contar con mejora continua del sistema ITDR con revisiones de las políticas y tecnologías”.

Asimismo, ambos resaltaron que las tecnologías y procesos que forman parte de ITDR están “adaptándose a las nuevas amenazas”, con especial foco en el “robo de cuentas, para detectar actividades sospechosas, amenazas internas, además de parar ataques de *phishing* e ingeniería social”, comentó Álvarez a la vez que Castilla destacó que la necesidad de contar con un ITDR que se centre, de forma especial, en la protección del Active Directory (AD). Finalizaron aconsejando por apostar por una “solución ITDR que dé respuesta a las necesidades de cada empresa”.



Julio Castilla



Daniel Álvarez



Comenzó después el módulo dedicado a una muestra amplia y exhaustiva de las propuestas más interesantes del mercado a cargo de destacados referentes de **Delinea**, **ForgeRock** y **Okta**, tras las que se celebró un animado debate, conducido por **José Manuel Vera**, redactor de SIC, sobre los grandes retos en este ámbito que puso fin a la primera jornada.

La protección de la identidad digital, bajo lupa

Comenzó la segunda jornada con una ponencia del profesor de la **Universidad Politécnica de Madrid (UPM)**, **Jorge Dávila**, quien abordó 'La Identidad digital ante el requisito de la ciberseguridad y la privacidad por diseño y los sistemas de IA'. En ella, el habitual colaborador de Revista SIC y experto en criptografía, planteó que la identidad digital puede existir como tal, "pero no bajo las condiciones del mercado, sino basada en un secreto único e intransferible", con el reto de interrelacionarla con otras identidades (biométricas, legales,



Jorge Dávila

etc.). Y el gran problema, según destacó, es que "el ser humano y el ser analógico no pueden entrar en el mundo digital si no lo hacen a través de un representante". Además, profundizó en el concepto de anonimato como "ausencia de identidad" y, del pseudoanonimato para proteger la privacidad a través del uso de alias, como se hace habitualmente, aunque recordó que "si se usa siempre el mismo pseudónimo te vas definiendo, aunque también se puede usar una identidad falsa con información falsa". Además, alertó de lo que puede suponer dos colapsos digitales –el denominado 'gran apa-

gón' y la corrupción de los registros públicos digitales– que supondría un caos global, recordando que frente al riesgo está "la ciberseguridad que trabaja en reducirlo y generar confianza". Lamentó, en este sentido, que

algunos agentes del mercado trabajen en que las cosas "sean más productivas que seguras". Finalizó destacando, entre otros aspectos de



Ignacio Alamillo

interés, que la IA es "algo mal definido, ya que es inmanejable, porque evoluciona", por lo que explicó que "la identidad digital es incompatible con la naturaleza de la IA porque si no sé quién eres en cada momento no te puedo asignar una identidad en cada momento". Como conclusión, resaltó "que las identidades digitales se le están resistiendo a la tecnología y a la sociedad conectada" ya que, en determinados casos, "la prevalencia del negocio y del coste dificultan que la digitalización sea resiliente y cibersegura", aunque sí consideró que "lo mejor está por venir".

Carteras digitales federadas

A continuación, **Ignacio Alamillo**, advisor de **Logalty** y referente español en los foros continentales sobre identidad y temas concernidos, disertó sobre las "consideraciones ante una eventual futura ley española de identificación digital", planteando los retos y lo que supondrá el nuevo marco de identidad europeo. Precisamente, puso en valor el gran paso que supone el eIDAS2, "una normativa que no

DEBATE DÍA 15

Los peligros y complejidades de la IA en la seguridad de las identidades y los espacios de mejora, a examen

La primera jornada concluyó con un debate, moderado por **José Manuel Vera**, redactor de **Revista SIC**, en el que se reflexionó sobre diferentes cuestiones, a través de las preguntas de los presentes. Entre ellas, hubo un especial interés por profundizar en los retos para evitar las falsas alarmas de ataques, sobre todo, cuando la IA cobre más protagonismo creando identidades *fake*. **Julio Castilla (PwC España)**

empezó opinando que, desde el área de la consultoría, "somos conscientes del contexto retador de los incidentes sofisticados, pero las organizaciones más maduras y más grandes están avanzando para mitigarlos. Sí que es verdad que falta camino por recorrer, por ejemplo, en el espectro de las pymes, pero en este contexto también vemos avances y dedicación". "La cuestión también es qué tipo de

identidades se están robando y cómo se utilizan", añadía **Roger Gallego (Delinea)** destacando que "estamos en el negocio de la seguridad para aumentar la resiliencia de las compañías, por lo que si la alarma existe hay que trabajar en analizarla". **Nuno Silveiro (Okta)** matizó que, de momento, "las falsas alarmas son una ínfima minoría de los ataques", una opinión que compartía **Guillermo Arias (ForgeRock)** quien indicó que "el impacto económico de un falso positivo está muy por debajo de un impacto real. Y la verdad es que la innovación en la que está sumergida esta industria es gigante", apuntó.

Entonces, ¿qué hacemos mal?, se preguntaba la audiencia. Scott señaló que "lo que más falla es la parte humana, la toma de decisiones, ya que se sigue asumiendo que el riesgo no tiene un

coste hasta que sucede algo". Para Silveiro es que "el negocio sigue estando por encima de la seguridad". A lo que Castilla agregó que, en su caso, "el problema que nos encontramos es que las bases y el gobierno se dan como superado, pero a veces no es así". Gallego, optimista, destacó que "las capacidades tecnológicas de las compañías han mejorado muchísimo", aunque "los cibercriminales también hacen todo lo que pueden". Así que, "estamos en una carrera de competencias apasionante", afirmó.

Otras de las cuestiones que generaron más interés fue cómo van a afectar las normativas que se están aprobando, como el eIDAS2, y si en España existen compañías que lleven la protección y gestión de las identidades, a último término, con tecnologías sofisticadas. Para todos,

la respuesta fue afirmativa, aunque se mostraron algunos matices, ya que explicaron que es difícil mantenerse al día con la innovación, las tecnologías y otros requisitos que se demandan, como las certificaciones, lo que requiere un gran esfuerzo por parte de las compañías.

Para concluir se pidió a los ponentes que resumieran en pocas palabras de qué va a depender el éxito o fracaso de la protección de la identidad en 2024. Para Castilla recae en "la gestión integral del riesgo". Gallego abogó por "incrementar la resiliencia". Silveiro indicó la necesidad de "agarrar los riesgos como un toro y pensar dónde hay que actuar". Y Scott cerró la ronda destacando la importancia de "cuantificar el riesgo".



Debate de la 1ª jornada



VISION Y PROPUESTAS DE LA INDUSTRIA



DELINIA / Roger Gallego, Iberia Sales Manager

“Apostar por un PAM Extended para contar con visibilidad punto a punto y una gestión fácil y ágil del acceso privilegiado, de forma intuitiva y de forma proactiva”

Destacó en su ponencia el valor de su propuesta “Extended PAM” como “viaje a la gestión de los privilegios”. “Todo tiene una identidad y las humanas y máquinas siguen multiplicándose y precisan de estar protegidas”. El problema es que “el PAM tradicional solo cubre algunos de los sistemas y cuentas privilegiadas”. “La superficie de ataque es cada vez más grande, lo que ha obligado a pasar de ‘Traditional PAM a Extended PAM que permite defender *on premise*, nube, identidad humanas y máquinas”, comentó detallando en profundidad la propuesta de la compañía, apostando por “prevenir el robo de identidades y credenciales a través de la visibilidad y el descubrimiento”. En este sentido, destacó el valor en su enfoque de dos conceptos: el Least Privilege y el Just in Time Access, que permiten tener la capacidad de hacer lo que necesitas hacer cuando lo necesitas y solo durante el tiempo necesario. Así, el primero pretende que los usuarios e identidades puedan acceder solo a los recursos y aplicaciones que requieren y, el segundo, eliminar los privilegios existentes definiendo cuándo el acceso debe ser autorizado y durante cuánto tiempo”, dando lugar al ‘Zero Standing Privilege’ (ZSP), ejemplificado en el ‘PAM Maturity Model’ de la compañía.



FORGEROCK / Carlos Scott, Consultor de Riesgo Digital

“La facilidad de tomar la decisión adecuada en cada momento, con IA y enfoque heurístico, para reducir el fraude a través del ‘ciclo de la identidad’”

El experto de la multinacional estadounidense explicó que ITDR (**Identity Threat Detection and Response**) ya va “por una segunda ola, con mayor digitalización y mayor adopción de la nube” y puso en valor la fusión de Ping Identity y ForgeRock, a principios de enero, dando lugar a la nueva Ping Identity “que busca el acceso de forma conectada y segura”, apostando por la “prevención del fraude con la identidad digital”, un objetivo que centra gran parte de los esfuerzos de la empresa recordando que, actualmente, está enfocada en los principales vectores de fraude, apostando también por “la necesidad de analizar el comportamiento de los usuarios para combinar, como propone ForgeRock, tres diferentes modelos de ciberprotección basados en el contexto, en tiempo real, durante la autenticación, con fuentes externas de credenciales comprometidas, con detección de *bots* e, incluso, validando el dispositivo, de forma criptográfica para evitar su suplantación, entre otros aspectos. En este sentido, mostró cuál es su aproximación implementando todos los controles que se precisan para contar con una gestión y protección de la identidad adecuada, también con el uso de IA y un enfoque heurístico, para “tomar la acción indicada según el riesgo”, bajo lo que la compañía denomina ‘Intelligent Journey’.



OKTA / Nuno Silveiro, Large Enterprise Account Executive

“IA aplicada a capacidades de ciberseguridad ante ataques a la identidad, con información estructurada y fácil de usar”

“Hace tiempo que se decía que si no estabas en Internet no existías como empresa. Y eso va a ocurrir en IA. Si no cuentas con ella, no vas a existir”, comenzó destacando el reconocido experto en la materia, que recordó que “la identidad digital de cada uno es el nuevo perímetro porque es lo único que nos hace diferentes de los demás, con las oportunidades de negocio que supone, en cuanto a soluciones que estén bien implementadas para protegerla”. Por ello, repasó el panorama de amenazas avanzadas, por ejemplo, con IA. “Estamos abrumados por la información de todo tipo de sistemas de ciberseguridad (*firewalls*, SIEMs, IAM, EDR, etc.) y sus datos desagregados pueden generar huecos y puntos grises”. Frente a ello, mostró las capacidades de la denominada ‘Workfoce Identity con Okta IA’, además de Okta Customer Identity Cloud, que “permite contar con información sobre amenazas” y capacidades, también, ante ataques con IA. “En cierto modo es una especie de Alexa o Siri aplicado a los *logs*, al que puedes preguntar por un usuario o fallos de identidad y es capaz de ofrecerte información estructurada”. Finalizó mostrando su apuesta por una “solución moderna para las necesidades de cada empresa, con una buena experiencia de usuario e innovación”.



VISIÓN Y PROPUESTAS DE LA INDUSTRIA



OMADA / Jorge Sendra, Country Manager

“Centrados en el gobierno de la identidad con un foco disruptivo, una solución SaaS de rápido despliegue y la garantía de muchos clientes satisfechos”

Especialista en protección de la identidad, dio a conocer la propuesta de la compañía danesa, que este año ha abierto oficinas en España -aunque cuenta con un laboratorio en Alicante desde 2021-. “Apostamos por un enfoque centrado en el gobierno de las identidades, de forma disruptiva, siendo un referente contrastado en este ámbito y con muchos clientes satisfechos”, destacó entre otros aspectos de interés, a la vez que recordó que su portafolio, a través de su Omada Identity Cloud, está pensado para casos de uso complejos porque “nuestra solución funciona muy bien en lo difícil”. Así, puso en valor su solución SaaS “con las mismas capacidades que *on premise*, basada en una arquitectura nativa del *cloud*, ofreciendo lo que realmente necesita cada empresa y un *roadmap* real y preciso en cada despliegue que logra un producto mínimo viable en poco más de 12 semanas”, para disponer de la solución “llave en mano”. En definitiva, frente a los retos que supone la protección de la identidad “queremos ofrecer la tranquilidad de que nuestros clientes están en el nivel de ciberseguridad que se busca”, recordando que, por supuesto, también cuentan con capacidades de Identity Analytics e IA.



SAILPOINT / Alejandro Fernández, Solutions Engineer

“Comenzar a gobernar la identidad desde el primer momento, a través de una sola plataforma para gestionar su ciclo de vida”

En su conferencia ‘Redefinir cómo abordar un programa de identidad’, destacó que, actualmente, “el 84% de las empresas tiene brechas de seguridad asociadas a la identidad”. Frente a este riesgo, la empresa propone contar, a través de SailPoint Atlas, con una “plataforma flexible, que permite disponer de los ‘satélites’ que necesita el cliente para la gestión y protección de la identidad”, partiendo de contar con visibilidad, a través de los más de 120 conectores de los que se dispone, contando con las mejores prácticas, con redescubrimiento de roles y con un cuadro de mandos fácil de usar, ofreciendo indicadores (KPI) para dar respuesta a la organización en todo tipo de aspectos, incluso, respecto a la gestión de la identidad de terceros, para reducir los riesgos de la cadena de suministro. “En definitiva nuestra apuesta pasa por gestionar, de forma eficaz, el ciclo de vida de la identidad” a través de un programa, paso a paso, automatizando, con IA y con políticas basadas en el acceso”, teniendo claro cuáles son críticos. “Todo ello permite a nuestros clientes, desde el primer momento, comenzar a gobernar la identidad, con una apuesta por la seguridad de la identidad autónoma para disponer de aceleradores en cualquier proyecto”.



WATCHGUARD / Miguel Carrero, VP Strategic Account

“Apostar por una estrategia basada en la simplicidad, la confianza cero, con la protección de la identidad como pilar, y capacidades de detección y respuesta (ITDR)”

El ejecutivo de la multinacional estadounidense mostró su apuesta por “habilitar Zero Trust con Identity Security, que ha venido para quedarse y que va a jugar un papel fundamental”. En su ponencia, mostró las capacidades y la apuesta de la empresa por una plataforma unificada de seguridad para controlar “la fuerza centrífuga de esta industria donde los clientes tienen una estrategia unificada”. Así mostró cómo aplicar el concepto de confianza cero a la identidad a través del WatchGuard Identity Framework, a través de soluciones como XDR, con ThreatSync XDR, AuthPoint Total Identity Security -para proteger los accesos-, además de integrar más capas de protección, automatizar y contar con ITDR -para contar con protección en el “mapa de los sectores de identidad”-, y poner en valor su ciberseguridad “centrada en el usuario”. Todo ello ilustrándolo con un ejemplo práctico de cómo protegerse frente a ataques a través de terceros o de fallos, como la reutilización de contraseñas, el uso de credenciales comprometidas, etc. Terminó recordando que la identidad debe ser “la piedra angular de la estrategia de confianza cero, acompañada de un modelo de detección y remediación de ataques que se aprovechen de ella”.



DEBATE DÍA 16

Visibilidad, confianza cero y tener sentido común para mitigar riesgos, claves para disponer de una identidad robusta frente a amenazas

El evento terminó con un debate en el que, al igual que en la jornada anterior, se mostraron los interesantes puntos de vista de los especialistas que habían intervenido. Una de las primeras preguntas de los presentes en la sala giró en torno a los errores que se están cometiendo a la hora de aplicar la IA a la protección y gestión de identidades. El primero en responder fue **Jorge Dávila**, que de manera categórica destacó que “el primer error técnico es confiar en ella. Las IA son mediocres, cuesta mucho producirlas, son poco flexibles, nada auditables, y lo peor es cargarles de una responsabilidad que no pueden tener, no están capacitadas”. **Alejandro Fernández (SailPoint)** estuvo de acuerdo, añadiendo que “su regulación también va a ser un gran reto”.

De igual forma, **Elena García (WatchGuard)** indicó que “el principal error es entender que la IA solo va a ser usada para un bien común”. “Son herramientas que, efectivamente, pueden ser muy potentes en ambos sentidos, pero aún tienen sesgos y son inmaduras, así que tenemos que intentar que el marco regulatorio y ético permitan ser usadas para el bien”. “Nosotros preferimos hablar más que de IA, de algoritmos de análisis y, obviamente, dejar el modelado de los roles a la IA es peligroso”, dijo **Jorge Sendra (Omada)**.

Ante este escenario, se preguntó cuál sería la ‘piedra filosofal’ para la protección de las identidades digitales. “Pues es tener visibilidad y control”, comentó Sendra. García señaló “la confianza cero, aunque prefiero utilizar más el término sentido común y el hecho de

ser conscientes de nuestra identidad, los derechos y obligaciones que conlleva, y sus consecuencias”. Fernández, por su parte, subrayó el “poder conocer en todo momento qué es lo que necesita cualquier tipo de identidad en la organización”.

La audiencia también se interesó por si es suficiente o no la cantidad de integradores especializados que hay en España en identidad, a lo que los representantes de las empresas participantes contestaron que existe un ecosistema “aceptable” y “saludable”, aunque se están focalizando en este sentido para que haya más y trabajar juntos. Al respecto, se preguntó por la relación con los llamados ‘hiperescales’ (como son Amazon, Microsoft y Google), una cuestión que García

resumió afirmando que “convivimos y coexistimos en un entorno de competitividad”. Así que, “lo que hacemos es como ‘el yin y el yang’, lo que no ofrece el hiperescalar lo aportamos las empresas que colaboramos y competimos con ellos proporcionando soluciones complementarias”.

Para concluir, se pidió a los participantes un consejo para los CISO, para afrontar 2024 de la mejor manera posible el gran reto de la protección de la identidad. Fernández apostó por “acercarte a los mejores fabricantes y partners”. García destacó “tener sentido común e identificar personas, procesos y tecnologías para mitigar el riesgo”. Sendra destacó una frase: “no te preocupes, ocúpate”. Y Dávila finalizó con un mensaje más mordaz “búscate a otro y que corra con el mono”.



Debate de la 2ª jornada

tiene que ver con la ciberseguridad sino con el mercado interior y eso explica muchas decisiones que se están adoptando” y que terminará con la entrada en vigor del nuevo Reglamento de identidad digital europea en torno al “tercer trimestre de 2026, con un plazo razonable para que la Comisión elabore los condicionantes técnicos”; Recordó que, en definitiva “la UE busca que haya una entidad digital fiable y controlada por el usuario, para 2030”.

En este sentido, apostó por la identidad digital descentralizada sobre la que trabaja en un grupo que apuesta por este enfoque “porque es la persona la que tiene siempre el control de su información”. Puntualizó que, por ejemplo, las carteras tienen que tener “unos niveles de seguridad, aunque no se va a poder impedir que le dejes tu wallet a un tercero, como no se puede hacer en el mundo físico. Pero la alternativa es peor, así que se están dando pasos correctos”, consideró añadiendo que el wallet europeo es más “un medio de identificación electrónica, no un contenedor”. “Sí, hay cierta oposición a algunas medidas, pero hay que darle una oportunidad y pelear a nivel

técnico para que el resultado sea muy bueno”.

Durante su presentación, en la que se mostró a favor de una ley de identificación digital en España –como la tienen Bélgica, Francia, Italia o Alemania, entre otros– destacó diferentes aspectos del marco de identidad digital y cómo se aterrizará con las carteras, dando a conocer algunos de los textos filtrados del documento final. Incluso, planteó la posibilidad de que, por ejemplo, en España pudiera haber “un sistema federativo de wallets, porque hay hueco para ello constitucionalmente”.

La ‘IoTización’

Le siguió una interesante conferencia de **Vicente Segura**, gerente de Producto de Ciberseguridad OT&IoT, en **Telefónica Tech**, sobre la ‘Gestión segura de identidades y accesos de cosas en entornos OT/IoT’, ironizando con lo que supone ‘IoTizar’ estos ámbitos.

Repasó los problemas de ciberseguridad planteados en las arquitecturas de referencia en servicios o sistemas IoT, también en lo que a su identidad se refiere, y cómo acometerlas para evitar las principales ciberamenazas como, por

ejemplo, creando un “certificado digital único para cada dispositivo y almacenarlo en un lugar seguro”, destacando el valor que suponen las garantías de seguridad para cada tipo de Base de Computación Confiable (TCB).

Así mostró cuatro casos concretos recordando, entre otras conclusiones, que la TCB es clave en lo que debe ser “computación confiable” y contar con un ‘ancla de confianza’ como elemento fundamental para la seguridad del dispositivo, que almacena y procesa los secretos criptográficos. En definitiva, apostó por soluciones “basadas en claves públicas personalizadas por dispositivos”, y aunque en la “práctica no se pueda hacer siempre –lo que obliga a entender cada caso–, sí hay que ver qué mecanismo de identidad usa y cómo se complementa con una seguridad de extremo a extremo”.

Finalizó la segunda jornada con el módulo dedicado a la innovación y las propuestas de la industria para la protección y gestión de la identidad a cargo de especialistas de **Omada**, **SailPoint** y **WatchGuard**. No faltó en **IdentiSIC** el recuerdo a uno de los grandes especialistas mundiales en identidad, recientemente fallecido, **Vittorio Luigi Bertocci**, Arquitecto Principal de Auth0, de Okta, a quien se rindió un cálido aplauso de homenaje. ■



Vicente Segura

EY 2023 Global Cybersecurity Leadership Insights: Ciberseguridad, un aliado necesario en un año complejo

El estudio *EY 2023 Global Cybersecurity Leadership Insights* revela que solo el 20% de CISOs cree que la estrategia de su organización es eficaz frente a las amenazas presentes y futuras. Las compañías experimentan en promedio 44 incidentes de ciberseguridad al año, pese al incremento de la inversión en ciberseguridad. No obstante, la detección y respuesta a estas amenazas sigue siendo lenta, superando los seis meses en más del 75% de los casos. El estudio categoriza a las organizaciones en dos tipos: “empresas seguras”, con prácticas de ciberseguridad eficientes, y “empresas vulnerables”, con deficiencias notables. Las primeras, destacan por adoptar rápidamente tecnologías emergentes, incluyendo la inteligencia artificial. Sin embargo, la incorporación de estas nuevas tecnologías supone desafíos significativos, incluyendo la necesidad de una regulación efectiva y la perspectiva de un déficit de profesionales capacitados en ciberseguridad.

La encuesta realizada a 500 responsables de ciberseguridad de todo el mundo, entre los que se encuentra una muestra de empresas españolas, revela que sólo uno de cada cinco considera que el enfoque de su organización es eficaz frente a las amenazas actuales y futuras.

Las empresas consultadas declaran recibir una media de 44 incidentes de ciberseguridad al año. Al mismo tiempo, los encuestados revelan un aumento de inversión en ciberprotección: a nivel global, la media anual se sitúa en 35 millones de dólares, mientras que el coste medio de una brecha de seguridad para las organizaciones ha aumentado un 12% hasta los 2,5 millones de dólares en 2023.

A pesar de los altos niveles de inversión, los tiempos de detección y respuesta siguen siendo lentos. Más de tres cuartas partes de los encuestados (76%) afirman que sus organizaciones tardan una media de seis meses o más en detectar y responder a un incidente.

Las métricas de ciberseguridad, novedad de este año

Como novedad en el estudio de este año, se han evaluado las organizaciones en función de una serie de métricas de ciberseguridad con el objetivo de identificar aquellas empresas con mejores prácticas de ciberprotección. A partir de los resultados, se han identificado dos tipos de organizaciones (**Figura 1**): las “empresas seguras”, aquellas con la ciberseguridad más desarrollada y eficiente (42% del total) y las “empresas vulnerables”, organizaciones con una ciberseguridad menos eficiente (58%).

En este contexto, la mayoría de las “empresas seguras” (70%) se consideran pioneras

en la adopción de tecnologías emergentes en lugar de esperar a que la tecnología esté probada y comprobada, una cifra que desciende a menos del 50% en las “empresas vulnerables” (**Figura 2**).

A todas luces, parece que la inteligencia artificial (IA) se antoja como el cambio más novedoso en la economía para los próximos años y, además, será una tecnología muy útil para mejorar las capacidades de detección y prevención de amenazas de ciberseguridad. El gran desafío será conseguir que el despliegue de la IA sea seguro y confiable para intentar

evitar los problemas que un mal uso puede causar. En este sentido, la gran apuesta para el año 2024 es la regulación sobre el uso de la IA. La Unión Europea, que a principios de diciembre de 2023 aprobó la primera regulación del mundo sobre IA, va encaminada a definir el uso autorizado de esta tecnología y los usos prohibidos, además de definir los aspectos de gestión de sus riesgos para dar garantías a los ciudadanos. La supervisión de estos aspectos será crucial para asegurar el cumplimiento en todas las organizaciones y será determinante de cara al desarrollo de la IA tanto en Europa como en el resto del mundo.

En esta línea, el incremento y adopción de nuevas tecnologías aumenta la superficie de ataque, lo cual supone el principal desafío al que se enfrenta la mayoría de los encuestados (**Figura 3**). Por otro lado, el presupuesto para ciberseguridad, que históricamente había sido citado en la encuesta como el principal obstáculo al que se enfrentan las organizaciones, se sitúa en el puesto 6 de 7, tanto en la muestra global como en la española.

La dificultad para equilibrar el ritmo de la innovación y el de la seguridad se posicionan como el segundo desafío más nombrado a nivel global y el primero en la muestra española.

Esto se ve agravado por el riesgo que plantea el despliegue de tecnologías en la nube a gran escala y la seguridad en entornos industriales (OT) o en el Internet de las cosas (IoT): más de siete de cada 10 consideran que son los dos principales riesgos tecnológicos para los próximos cinco años.

Otro aspecto relevante para los próximos meses (por lo menos) es la creciente inestabilidad geopolítica a la que se enfrentan tanto en Europa como en el resto del mundo, presentándose como



Figura 1

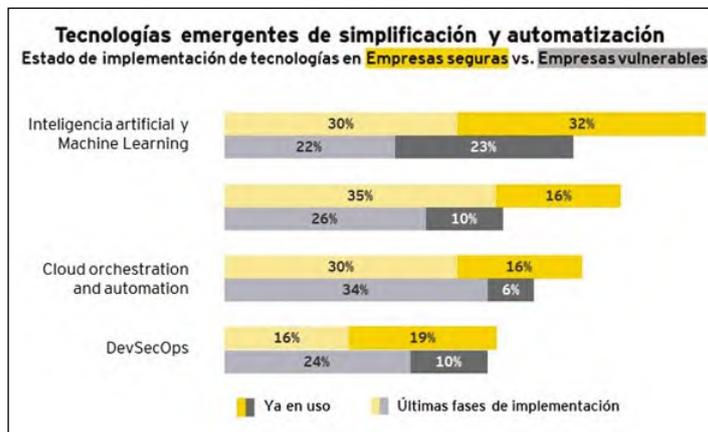


Figura 2

un escenario de amenaza especialmente para aquellas empresas que poseen presencia global o tienen intereses internacionales.

Este entorno volátil, a menudo cargado de conflictos sociopolíticos, altercados económicos y tensión estratégica, viene de la mano con un incremento notable de riesgos de ciberseguridad, los cuales pueden materializarse en forma de ataques maliciosos, espionaje o interrupciones intencionadas de servicios que afecten las operaciones de las empresas. Frente a este panorama, las organizaciones están tomando medidas preventivas y proactivas, incrementando notablemente el consumo de servicios de ciberinteligencia. Los más conscientes del entorno emergente de ciberamenazas están recurriendo a estas soluciones, no solo para securizar su infraestructura tecnológica e información crítica, sino también para mantenerse un paso adelante en un terreno cada vez más minado con riesgos, operando así dentro de una lógica de anticipación y respuesta veloz al cibercrimen.

Además de este contexto novedoso, prevalecen situaciones sobre las que es necesario seguir prestando atención: Todas las organizaciones están vinculadas operacional y digitalmente a las empresas que participan en su cadena de suministro. Sin embargo, a pesar del peligro, son pocos los que declaran estar muy preocupados por los ciberriesgos de la cadena de suministro y existe una brecha entre la percepción de las “empresas seguras” y las “empresas vulnerables” en este sentido (38% frente al 20% de las “empresas vulnerables”) (Figura 4). Esto supone un reto para las organizaciones puesto que el estudio revela que las cadenas de suministro han sido responsables del 62% de los incidentes de ciberseguridad en los últimos años.

Por otro lado, el año 2024 promete marcar un punto de inflexión en el terreno de la ciberseguridad y la resiliencia dentro del contexto europeo, paradigma que será redefinido a través del desarrollo de distintas directivas comunitarias. Estas directivas nacen con el objetivo de unificar y armonizar las medidas de seguridad que las empresas, intrínsecamente digitales, han de implementar en sus procesos operativos. Hasta ahora, las regulaciones se manejaban de manera predominantemente local o estatal, generando obstáculos para las empresas que operan en un entorno internacional. Actualmente, el desafío es alcanzar un consenso mínimo a nivel europeo en el entorno regulatorio de la ciberseguridad, y así facilitar una globalización más fluida de las organizaciones y promover su presencia internacional.

Estas regulaciones europeas, que aspiran a una supervisión rigurosa para garantizar su implementación, proyectan unas ambiciones elevadas. Todo indica que será su capacidad sancionadora la que catalizará su adopción y

el futuro lejano, sino en el panorama tecnológico inmediato y en la supervivencia empresarial.

El estudio aflora que, en general, la ciberseguridad ya forma parte de la agenda de los Comités de Dirección y en los Consejos de Administración de las grandes corporaciones. La creciente presencia de la tecnología, así como el incremento de los riesgos hace imprescindible una correcta identificación y gestión de los mismos. Por ello, en 2004 asistiremos a una mejora de la formación de los equipos directivos, así como a un aumento de la presencia de los asuntos relacionados con la ciberseguridad en los órganos de gobierno de las empresas.

Sin embargo, los resultados de la encuesta revelan que sigue habiendo una desconexión entre los CISOs y el resto de la dirección ejecutiva (C-suite). Los CISOs están menos satisfechos con el enfoque de ciberseguridad de su organización (36% frente a 58%). Entre las “empresas vulnerables”, esta brecha es aún más pronunciada. Cerrar estas brechas es clave: las organizaciones que tienen las operaciones de ciberseguridad integradas en las prioridades y estrategias empresariales básicas tienen menos probabilidades de sufrir incidentes de seguridad.

Finalmente, se pone de manifiesto que las “empresas seguras” trabajan para crear valor, no sólo para defenderlo. Su estrategia de ciberseguridad busca tener una repercusión positiva en su capacidad para transformarse a un ritmo adecuado, responder a las oportunidades del mercado y centrarse en la creación de valor. Esta creación de valor puede adoptar diversas formas, desde incrementar la confianza por parte de clientes o proveedores, hasta facilitar el aprovechamiento de distintos ecosistemas de colaboración sin incurrir en nuevos riesgos. ■

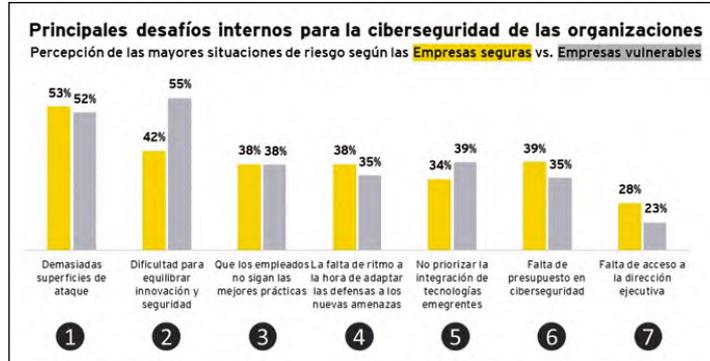


Figura 3



Figura 4

aplicación efectiva dentro del ecosistema de las organizaciones, dando un empuje decisivo hacia una gestión de la ciberseguridad cada vez más centralizada, coherente y homogénea en el tablero europeo.

En cuanto a la dimensión humana de las compañías, el mayor desafío al que tendrán que enfrentarse en el horizonte próximo es la notoria deficiencia de profesionales capacitados en el campo de la ciberseguridad. Este talento técnico resulta imprescindible para desarrollar y poner en marcha los protocolos de defensa necesarios en un entorno cada vez más propicio y vulnerable a ciberataques. Como se viene advirtiendo, los ciberincidentes son cada vez más frecuentes y, dado el ritmo acelerado de la digitalización, esta tendencia tiene todas las papeletas para incrementarse en vez de disminuir.

Las proyecciones apuntan a que para el 2024 será absolutamente imperativo para las organizaciones contar en sus filas con especialistas en ciberseguridad. Estos profesionales deben estar integrados de lleno en la gestión de riesgos de la compañía y ser pieza clave en la planificación estratégica. Deben poder anticiparse a los ataques, neutralizarlos de manera eficiente y minimizar el impacto en caso de que se produzcan. En resumen, el talento en ciberseguridad será un componente esencial no en



ELENA MAESTRE
Socia responsable servicios Ciberseguridad
elena.maestre@es.ey.com

JORDI JUAN GUILLEM
Socio, Ciberseguridad
jordi.juan.guillem@es.ey.com

EY

España, tras Japón, el país donde más se incrementaron en 2023, un 18,9%, hasta los 182.000

Los profesionales del sector rozan los 5,5 millones en todo el mundo, pero también crece el déficit hasta los 3,4 millones de puestos sin cubrir

La fuerza laboral global de ciberseguridad ha alcanzado niveles récord incluso cuando la demanda de habilidades aún supera con creces la oferta de trabajadores disponibles, según el Estudio de la fuerza laboral de ciberseguridad 2023 de (ISC)². Así lo destaca la asociación en su último estudio anual, publicado a final de año en el que recuerda que, en esta industria, “cada vez más identificada con tecnologías emergentes como la IA, aún se lucha por encontrar suficientes trabajadores con las habilidades y competencias adecuadas para satisfacer la creciente demanda de los empleadores”. En este sentido, el informe constata que la brecha entre oferta y demanda continúa agrandándose por el déficit de profesionales “con habilidades en áreas como seguridad en la nube, inteligencia artificial y aprendizaje automático, arquitecturas de confianza cero, así como la capacidad de resolver problemas y comunicarse”.

Entre otras novedades, el documento amplía el estudio de profesionales en cuatro países más: Emiratos Árabes Unidos, Arabia Saudita, Nigeria y Sudáfrica, y también se ha contemplado la estimación de analistas de ciberseguridad de la OCDE y la Oficina de Estadísticas Laborales de EE.UU., así como tendencias extrapoladas de otros estudios al respecto.

Cara y cruz

Aterrizando sus conclusiones, el informe destaca que, el año pasado, la fuerza laboral de ciberseguridad mundial alcanzó su máximo histórico con casi 5,5 millones de profesionales, un 87% más que el año anterior –unos 440.000 especialistas–. Un número bastante



notable teniendo en cuenta que en 2019 rondaba los 2,8 millones.

Sin embargo, y pesar de su incremento, el documento también destaca que, mientras que, en 2022, la brecha fue de

3,4 millones de puestos sin cubrir, un año más tarde esta cifra había superado los cuatro millones. “Esto deja a la profesión luchando con la aparente paradoja de que está empleando a un número cada vez mayor de personas en funciones de ciberseguridad, pero a un ritmo que nunca alcanza la necesidad subyacente en términos de números o habilidades específicas”, destacan desde (ISC)². “Si bien celebramos el número récord de nuevos profesionales que ingresan al campo, la realidad apremiante es

que debemos duplicar esta fuerza laboral para proteger adecuadamente a las organizaciones y sus activos críticos”, ha resaltado la CEO de la asociación, **Clar Rosso**.

Impacto mundial

En 2023, las geografías donde más creció la demanda de profesionales fueron Asia-Pacífico (un aumento interanual del 11,8%, hasta 960.000), Oriente Medio y África (un 11,7% más, hasta los 402.000) y América del Norte (un 11,3%, con hasta 1,5 millones), seguidas de Europa (con un aumento del 7,2%, hasta 1,3 millones) e Iberoamérica (que creció un 4,5% hasta casi 1,3 millones).

España, en segundo lugar

En la mayoría de los países, el estudio confirmó que las habi-

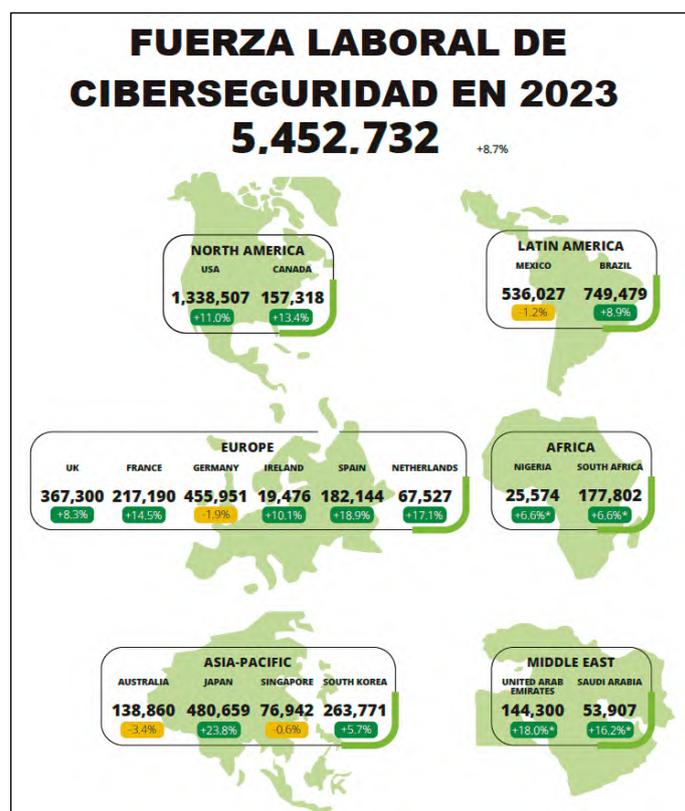
lidades en ciberseguridad siguen teniendo una gran demanda, lo que sugiere que los profesionales no deberían tener problemas para encontrar trabajo o pasar a un puesto nuevo o mejor con el tiempo. Así, por naciones con mayor crecimiento de profesionales, lidera el ranking Japón (hasta un 23,8% interanual y 480.000 más de profesionales), seguida de España (hasta un 18,9% interanual con hasta 182.000 más), Holanda (hasta un 17,1% y 68.000), Francia (un 14,5% más y hasta 217.000) y Reino Unido (con un crecimiento del 8,3% y 367.000 nuevos profesionales) que retrocede mucho en demanda a causa del Brexit, ganando mucha fuerza en este ámbito Alemania.

La investigación también destaca el fuerte incremento de demanda de profesionales en Oriente Medio a través de Emiratos Árabes Unidos (con un aumento interanual del 18% con hasta 144.000) y Arabia Saudí (que creció un 16,2%, con 54.000 profesionales). Como dato curioso, sólo cuatro países experimentaron una disminución en el tamaño de la fuerza laboral: Australia (-3,4%), Alemania (-1,9%, pero sigue siendo el mayor empleador de ciberseguridad en Europa continental), México (-1,2%) y Singapur (0,6%).

Déficits globales

En cuanto a déficit de profesionales, la región más penalizada es Asia y el Pacífico, con casi 2,7 millones, con un aumento del 23,4% respecto al último año, seguida de Norteamérica, con 522.000 personas y un incremento del 19,7% y Europa con 348.000 y 9,7%. En positivo, las que consiguieron reducir esta diferencia fueron Iberoamérica, donde el déficit cayó un 32,5%, a 348.000, y Oriente Medio y África, donde disminuyó un 7,1%, a 112.000.

El informe destaca que, por países, el que más ha sufrido esta



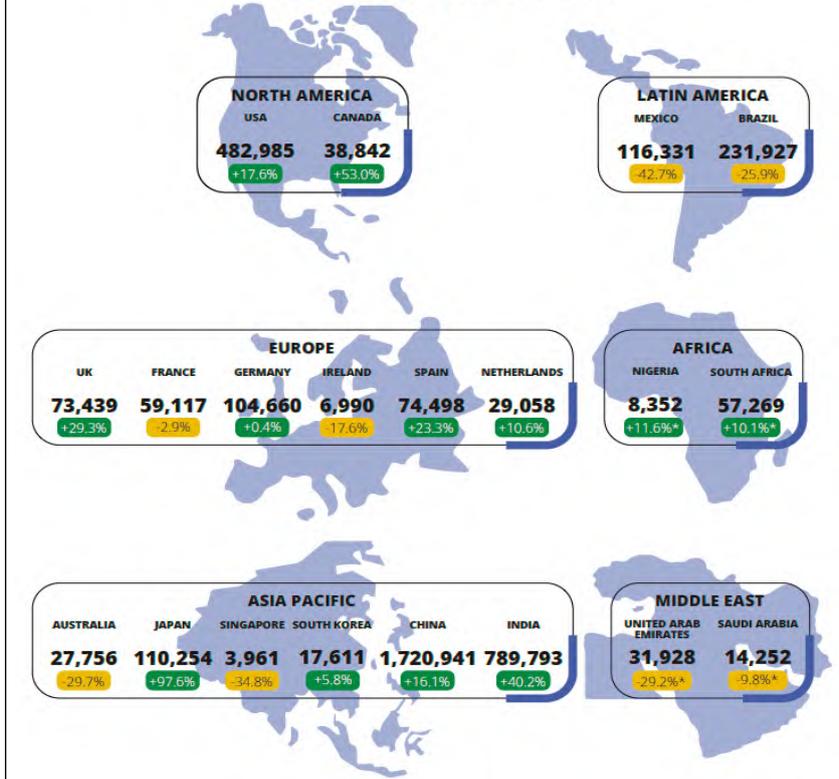
falta de profesionales es Japón, ya que, en sólo un año, la brecha de la fuerza laboral casi se duplicó a 110.000 (un aumento del 97,6%), seguido de Canadá (un incremento del 53% a 39.000), India (un 40,2% más a 790.000) y el Reino Unido (que creció un 29,3% a 73.000). Lo que más han reducido este déficit han sido Singapur (un 34,8% menos, hasta 4.000), Australia (un 29,7% menos, hasta 28.000), Emiratos Árabes Unidos (un 29,2% menos, hasta 32.000), Irlanda (un 17,6% menos, hasta 7.000), Arabia Saudita (un descenso del 9,8% a 14.000) y Francia (con un descenso del 2,9% a 59.000).

Frustración

Respecto a las razones para este déficit, el documento destaca que están “una variedad de factores, incluida la creciente necesidad de proteger a las organizaciones a medida que se digitalizan, la velocidad a la que la industria puede capacitar a nuevos trabajadores para satisfacer esta brecha. la demanda y la disposición de las organizaciones para contratarlos”, además de “factores macroeconómicos que tienen una influencia importante: el 47% de los encuestados informaron recortes (despidos, recortes presupuestarios, congelaciones de contrataciones o ascensos)”. De hecho, el 21% de los participantes destacó que su empresa tiene escasez de personal de ciberseguridad como para solucionar los problemas que sufren y otro 46% lo consideró “una ligera escasez”. El 41% destacó que la razón podría ser “la falta de talento calificado, el 34% restricciones presupuestarias y el 27% mencionó desafíos

DÉFICIT EN LA FUERZA LABORAL DE CIBERSEGURIDAD EN 2023

3.999.964 +12.6%



relacionados con la rotación y el desgaste del personal”. En este sentido, desde (ISC)² también destacan la necesaria inversión

que hay que acometer en profesionales de ciberprotección en “aspectos críticos”. De hecho, el documento considera “frustrante

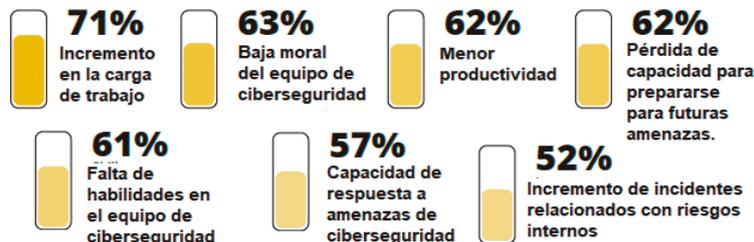
que las mayores brechas de habilidades mencionadas por los encuestados se encontraran en áreas que a menudo se ‘promocionan’ como muy demandadas e importantes, como la seguridad en la nube (35%), la IA/aprendizaje automático (32%), la confianza cero (29%) y las pruebas de penetración (27%)”.

Por ello, destaca que para hacer frente a este déficit “la profesión debe encontrar una manera de volver a capacitar y desarrollar constantemente a las personas que ya tiene en sus filas”. En este sentido, la edición de este año del informe sugiere que “todavía se está luchando por lograr el cambio” a través de, por ejemplo, la puesta en marcha de “nuevas vías hacia carreras cibernéticas, atrayendo a una mayor diversidad de personas y al mismo tiempo ofreciendo una ruta clara para que los profesionales amplíen sus calificaciones y conocimientos”.

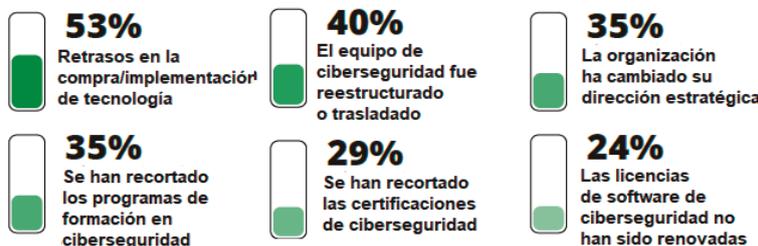
Diversidad

¿QUÉ IMPACTO HAN TENIDO LOS RECORTES EN LA EMPRESA Y EN CIBERSEGURIDAD?

IMPACTO DE LOS RECORTES EN CIBERSEGURIDAD Y SUS EQUIPOS



IMPACTO DE LOS RECORTES EN LA EMPRESA



Base: 8,598-8,907 global cybersecurity professionals. Note: "Don't know/not apply" responses were removed from the sample base. ISC2 Cybersecurity Workforce Study, 2023

En cuanto a la diversidad de la fuerza laboral de ciberseguridad el informe de (ISC)² el documento recuerda que “se está diversificando más rápidamente entre razas y etnias que entre géneros”, así como el, poco a poco, crecimiento de la presencia femenina en el sector, aunque, por ejemplo, de menos de 30 años, sólo el 26% son mujeres, dos veces más que las presentes en el tramo por encima de los 60 años. En este sentido, destaca que las empresas que han apostado por una selección de habilidades tienen un promedio de 25,5% de mujeres en su plantilla, frente al 22,2% de los que no adoptado este enfoque. ■

Por sectores, Telecomunicaciones, Banca y Energía lideran el ranking de transparencia realizado por Watch&Act Protection Services

AENA, ENAGÁS, INDITEX y TELEFÓNICA, empresas del IBEX 35 que mejor información proporcionan sobre sus prácticas de ciberseguridad

2023 fue un año especialmente ‘productivo’ en lo que a ciberataques y amenazas cibernéticas se refiere. De enero a septiembre, la cibercriminalidad registró en España 337.251 infracciones penales (el 18,5% del total de todas las formas de criminalidad), representando un incremento del 21,5% respecto a 2022, según los últimos datos del Balance de Criminalidad, correspondiente al tercer trimestre de 2023, del **Ministerio del Interior**.

Se trata de un hecho que vuelve a poner de manifiesto que la ciberseguridad es un factor crítico para todo tipo de organizaciones, aunque, algunas estén especialmente expuestas a las ciberamenazas, como es el caso de las empresas del **IBEX 35**, como parte fundamental de la economía española y global. Prueba de ello, fue el ciberataque ocurrido en diciembre pasado, *ransomware* mediante, a uno de los mayores bufetes de abogados que trabaja para el IBEX 35, **MS Albiñana y Suárez de Lezo**, del que se responsabilizó el grupo LockBit, que se apoderó de 500Gb de información, según El Confidencial.

A pesar de ello, las grandes empresas son las más conscientes de la importancia de una buena preparación y la inclusión de la ciberprotección como un componente fundamental de la estrategia empresarial. Y así lo refleja el ‘III Ranking de transparencia en ciberseguridad de las empresas del IBEX 35’, realizado por la correduría especializada en seguros de ciberriesgo, **Watch&Act Protection Services (W&APS)**, que, en su análisis, destaca una “mejora en general con respecto al año anterior”, en lo referente a la información en ciberprotección que publican en sus memorias no financieras, en este caso, del ejercicio 2022.

Así, para su elaboración, en el informe –con carácter anual e independiente– se consideraron los diversos aspectos publicados que van desde el marco legal y normativo, hasta las prácticas operativas cotidianas, con el objetivo identi-

POSICIÓN	EMPRESA	POSICIÓN	EMPRESA
1	AENA	11	FLUIDRA
	ENAGÁS	12	SACYR
	INDITEX	13	CELLNEX
	TELEFÓNICA	14	UNICAJA
2	INDRA	15	BANKINTER
3	NATURGY	16	ACC. ENERGÍA
4	MAPFRE	17	RED ELÉCTRICA
	BBVA	18	ACCIONA
	FERROVIAL	19	BANCO DE SABADELL
5	BANCO DE SANTANDER	20	ACS
	CAIXABANK	21	SOLARIA
6	IAG	22	COLONIAL
7	MELIÁ	23	GRIFOLS
8	IBERDROLA	24	LOGISTA
9	ENDESA	25	MERLIN PROPERTIES
10	AMADEUS	26	ACERINOX
	REPSOL		LABORATORIOS ROVI
			ARCELORMITTAL

dell y Bankinter, “si bien es de sobra conocida la tecnología innovadora de estos bancos especialmente en el caso de Bankinter”. Por su parte, Energía se mantiene en el tercer puesto. En este sentido, se indica que las empresas del IBEX 35 que conforman este sector “demuestran un interés por informar y manifestar que son empresas de servicios esenciales para la población y por lo tanto muy sensibles a cualquier comportamiento reputacional que implique un perjuicio para sus compañías”.

Participación de la alta dirección

El documento subraya, además, la involucración de la alta dirección de las empresas en los asuntos de ciberseguridad. Y es que, “todas ellas señalan una clara implicación de los miembros de los Consejos de Administración y de los Comités de Dirección para un conocimiento y

cumplimiento de la normativa en ciberseguridad”. De igual forma, destaca que “han trasladado la innegable necesidad de proporcionar formación en esta materia a todo el personal de la empresa, empezando por ellos mismos”.

Asimismo, el informe recoge entre sus conclusiones la mención que realizan estas empresas en cuanto al aumento de sus presupuestos en la innovación y tecnología, “haciendo especial énfasis muchas de ellas la parte específica en ciberseguridad”.

Además, cabe destacar que la información referida a las medidas de control en ciberprotección de terceras partes y en la cadena de suministro empieza a ser más relevante. Y es que, dicho dato es una muestra que indica que “todavía queda mucho camino por recorrer en la transparencia de la información en ciberseguridad puesto que la innovación y tecnología continúa evolucionando de forma acelerada obligándonos a tomar nuevas medidas de ciberprotección que deberemos informar”. ■

RESULTADO POR SECTORES 2022		RESULTADO POR SECTORES 2021		RESULTADO POR SECTORES 2020	
POSICIÓN	SECTOR	POSICIÓN	SECTOR	POSICIÓN	SECTOR
1	Telecomunicaciones	1	Finanzas Seguros	1	Telecomunicaciones
2	Finanzas y Seguros	2	Servicios de Consumo	2	Servicios de Consumo
3	Energía	3	Energía	3	Finanzas Seguros
4	Servicios de Consumo	4	Telecomunicaciones	4	Bienes de Consumo
5	Construcción	5	Construcción	5	Energía
6	Bienes de Consumo	6	Bienes de Consumo	6	Construcción
7	Inmobiliario	7	Inmobiliario	7	Inmobiliario

ficar a las empresas que mejor informan a sus accionistas clientes y proveedores. Este año, además, se incorporaron dos indicadores: la mención a los ataques recibidos a lo largo del año y a las medidas de control en materia de ciberprotección a los proveedores de la cadena de suministro de la empresa.

Cuatro empresas en primera posición

El documento destaca entre sus conclusiones “la mejora significativa en la información proporcionada por empresas como **Aena, Enagás, Inditex** o **Telefónica**, que alcanzaron las mayores puntuaciones”, situándolas en lo más alto del ranking. Asimismo, resalta que, con carácter general, las empresas que mantenían buenas posiciones en año anterior, como **Banco Santander, Mapfre** e **Iberdrola** entre otras, siguen situadas en la parte alta de la tabla, dentro de las ‘Top 10’ de cumplimiento con los nuevos criterios incorporados”. Además, empre-

sas como **Indra, IAG, Meliá** y **BBVA**, han dado un salto significativo para también situarse en la cabeza de la clasificación.

Del lado contrario, **Arcelor Mittal** junto con **Rovi** y **Acerinox** presentan un nivel de transparencia escaso o nulo”, se destaca.

En general, el informe resalta la mejora en la transparencia con respecto a los indicadores de Auditorías/Certificaciones y la existencia de Centros de Seguridad Operativos Internos (SOC/CERT) en estas organizaciones.

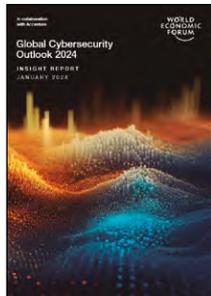
Telecomunicaciones, liderando el ranking

En cuanto a sectores, el de Telecomunicaciones se sitúa en primera posición, reflejando que “hay un claro interés en informar de las medidas que están tomando de la importancia que tienen en su actividad y de cómo puede repercutir en la sociedad”, explica el documento.

Por su parte, Finanzas baja posiciones, lastrado por Banco de Saba-

El WEF alerta de la cada vez mayor brecha en ciberresiliencia entre pymes y grandes empresas, y la incapacidad para reducirla

A medida que aumentan la escala y la diversidad de las amenazas, la resiliencia es primordial. Pocas organizaciones son lo suficientemente sólidas como para llamarse a sí mismas ciberresilientes con confianza, según explica el **Foro**



Económico Mundial (WEF) en su informe 'Perspectiva de ciberseguridad global 2024', publicado en enero. En él aborda los "desafíos multifacéticos que enfrentan los líderes cuando buscan desarrollar ciberresiliencia en sus organizaciones" entre los que están desde la escasez de habilidades hasta el auge de la IA generativa, además de identificar las oportunidades y obstáculos que suponen las nuevas tecnologías. "A medida que el ámbito cibernético evoluciona, acompañado a las tecnologías emergentes y a las cambiantes tendencias geopolíticas y económicas, también lo hacen los desafíos que amenazan nuestro mundo digital", se destaca al tiempo que se recuerda que la situación crítica que se vive hace imperiosa para las empresas la "resiliencia y permitir la colaboración global sistémica".

Y es que, entre otros aspectos, el informe constata como uno de los grandes retos globales, el crecimiento de la brecha entre las organizaciones ciberresilientes y aquellas que aún no han implementado medidas adecuadas para serlo.

El documento destaca lo que

denomina un "aumento de la ciberinequidad": la división entre las organizaciones ciber resistentes y las que no lo son se destaca, con la falta importante de un "grupo intermedio", formado por los que cuentan con protocolos básicos de ciberseguridad implementados. Precisamente, esta falta de ciberprotección en un notable número de organizaciones, identificadas con las pymes, es uno de los aspectos más preocupantes. Sin embargo, también explica que hay "motivos para el optimismo, ya que la ciberresiliencia está cada vez más presente en las agendas de los responsables ejecutivos".

Pólizas cibernéticas

De cualquier forma, el 90% de los 120 ejecutivos encuestados en la 'Reunión Anual sobre Ciberseguridad del Foro Económico Mundial', en la que se basa el documento, destacaron que se precisan medidas urgentes para abordar esta brecha, además de ser significativo que, según su investigación, sólo una de cada cuatro empresas cuenta con una póliza cibernética. A ello se suma que, desde 2022, se ha reducido al 31% el número de organizaciones que considera que cuenta con una ciberresiliencia mínima.

El documento, además, señala que el auge de las nuevas y emer-

gentes tecnologías exacerbará los desafíos existentes. "Las organizaciones deben desarrollar una mejor comprensión del impacto que suponen cuando se adoptan, por ejemplo, la IA generativa, desde la perspectiva de la ciberresiliencia", advierte. Es llamativo que el 56% de los preguntados consideran que la IA dará ventaja a los ciberatacantes sobre los defensores en los próximos dos años, sobre todo a través de técnicas como *phishing*, *malware* y *deepfakes*. Además, se cifra en un 7% el impacto previsto de la 'Generación IA' en el PIB mundial a 10 años.

Asimismo, es notable que el 60% de los ejecutivos preguntados coincidió en que las regulaciones cibernéticas y de privacidad reducen efectivamente el riesgo en su ecosistema de la organización: hasta un 21% más desde 2022.

Déficit crítico de profesionales

También se llama la atención sobre la creciente escasez de talento y habilidades cibernéticas y considera que "las tecnologías emergentes no harán sino aumentar la demanda de profesionales" y, prueba de ello, es que los preguntados informan que la escasez de personal capacitado para responder a ciberincidentes no deja de aumentar año tras año, pasando del 6% en 2022, al 20% este año. El 52% de los participantes reconoció que contar con habilidades y recursos es su mayor desafío en

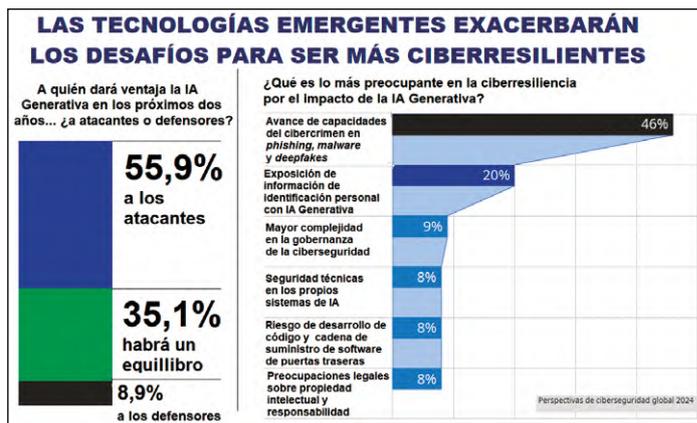
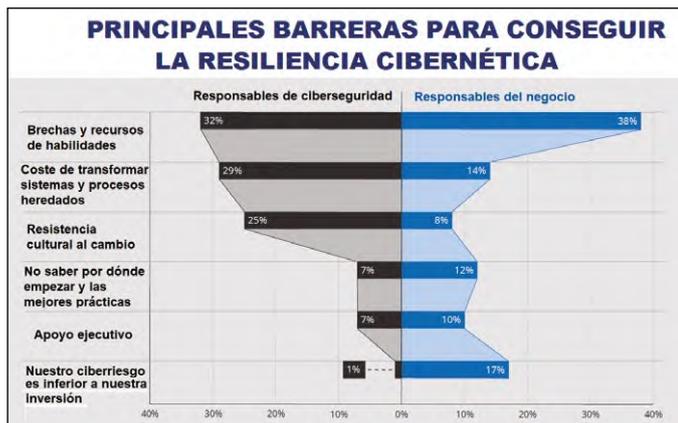
materia de resiliencia cibernética. Sólo el 15% de todas las organizaciones son optimistas en cuanto a que las habilidades y la educación en esta área mejorarán significativamente en los próximos dos años.

Junto a ello, los ejecutivos preguntados expresaron una creciente preocupación por el cada vez mayor riesgo cibernético que se asume en el negocio. En concreto, el 45% consideró su principal preocupación en este sentido las posibles interrupciones operativas y uno de cada tres (29%) informó que sufrió, en el último año, un ciberincidente con impacto material.

Más colaboración

En este sentido, el informe pone en valor la colaboración entre las empresas y su cadena de suministro para "crear oportunidades para desarrollar resiliencia". Son "a la vez el mayor activo y el mayor obstáculo de una organización para un futuro digital seguro, resiliente y digno de confianza", destaca el documento que alerta de la "necesidad imperiosa de comprender los riesgos de la cadena de suministro y los de las relaciones con terceros para mejorar en protección".

Un dato revelador es que un 51% de los ejecutivos preguntados destacaron que los socios de la cadena de suministro no les han pedido pruebas de su postura en materia de ciberseguridad y eso que un 41% reconoció haber sufrido un ciberataque, con un impacto material, a través de un tercero. ■



Una de cada cuatro admite no tener control alguno sobre esta tecnología, según Zscaler

Las empresas y organizaciones, presionadas, se lanzan a usar herramientas de IA generativa, a pesar de las dudas que provocan en materia de seguridad

La Inteligencia Artificial ha dado, en poco tiempo, un salto cuantitativo y cualitativo. Pero aún hay muchas dudas de

su impacto futuro real. De hecho, en uno de sus últimos informes, **Zscaler** alerta de que “las compañías se están viendo presionadas para utilizar herramientas de Inteligencia Artificial Generativa (GenAI), a pesar de las importantes dudas y preocupaciones que ello plantea en materia de seguridad”. El estudio titulado ‘All eyes on securing GenAI’ (Todos los ojos puestos en proteger la GenAI), con la participación de 900 responsables de TI de todo el mundo, recoge un dato que, por ser compartidos entre todos los participantes, llama poderosamente la atención: el 89% de las organizaciones tienen la certeza de que las herramientas GenAI, como ChatGPT, son un riesgo potencial para su seguridad y el 95% ya las están utilizando en sus empresas.

Principales riesgos

Entre las principales preocupaciones de los que aún no han apostado por usar esta tecnología destacan la posible pérdida de datos confidenciales, la falta de comprensión de sus peligros y beneficios, y la falta de recursos para supervisar su uso. Algo especialmente preocupante por cuanto el 23% de los que sí la utilizan reconocen no supervisar en absoluto su uso y, además, el 33% afirman no tener todavía implementada ninguna medida de seguridad asociada a GenAI, aunque



Organizations rush to use generative AI tools, despite significant security concerns

New All Eyes on Securing GenAI research from Zscaler explores how today's organizations are approaching GenAI tool usage and the security implications this might have.

muchas ya lo han planificado.

De hecho, esta situación es especialmente grave entre las empresas de menor tamaño (entre 500 y 999 empleados), según el informe, donde el 95% de las organizaciones reconocen estar utilizando herramientas GenAI y hasta un 94% es consciente del gran riesgo que ello implica. Incluso, en lo que atañe al uso de datos, sorprende que el sólo el 46% de los encuestados se han mostrado confiados en que su organización hubiera clasificado todos sus datos en función de su importancia, aunque un 44% sí han comenzado a clasificar algunos de sus datos como requisito previo para implementar medidas de seguridad.

De cualquier forma, un 57% de los responsables permiten su uso sin restricciones y un poco más de un tercio (38%) lo permite emplear, pero de forma cautelo-

sa. Sólo un 5% de los participantes respondió que o bien se están conteniendo para ver a dónde va la tecnología o han prohibido por completo su uso.

“Las herramientas de GenAI, incluyendo ChatGPT y otras, son una gran esperanza para las empresas en términos de velocidad, innovación y eficiencia”, explica la vicepresidenta de Gestión de Producto de la compañía, **Sanjay Kalra**. “A pesar de ello, con la preocupación existente en torno a sus medidas de seguridad, apenas un 39% de las organizaciones percibe su adopción como una oportunidad y no como una amenaza. Esto no solo pone en peligro su negocio y actividad, así como la integridad de los datos de sus clientes, sino que también desaprovecha su enorme potencial”.

Bajo control de TI

Curiosamente, los usuarios no son los que tienen el control –o descontrol– del uso de la IA en el ámbito corporativo. Sólo el 5% de los preguntados contestaron

que el riesgo viene de ellos. Por el contrario, el 59% destacaron que esta tecnología está siendo adoptada y desplegada desde los departamentos de TI. “Lo que supone que debería tranquilizar a los responsables empresariales”, destaca Kalra, que evidencia que “la dirección de las empresas dispone de autoridad para poder controlar estratégicamente el ritmo de adopción de GenAI y establecer un control firme sobre sus medidas de seguridad, antes de que su implantación dentro de su organización avance aún más. Eso sí, el estudio también denota que la ventana para lograr una buena gobernanza está disminuyendo rápidamente”.

Por ello, el informe finaliza destacando que, según el 51% de los participantes, está produciéndose un “aumento significativo en el interés por el uso de las herramientas GenAI”, lo que debe hacer que las empresas tengan claro qué medidas adoptar para cerrar la brecha entre su uso y su seguridad. Un riesgo para el que el estudio recomienda implementar una arquitectura integral de confian-

za cero para autorizar únicamente las aplicaciones y usuarios de IA aprobados, realizar análisis exhaustivos de los riesgos de seguridad de las nuevas aplicaciones de IA para comprender claramente las vulnerabilidades y responder a ellas, así como implantar un sistema de registro detallado para hacer un seguimiento de todas las solicitudes y respuestas de IA, y habilitar medidas de prevención de pérdida de datos (DLP) con confianza cero para todas las actividades de IA con el fin de evitar la extracción de datos. ■

A PESAR DE SU FALTA DE CIBERSEGURIDAD CONTRASTADA LA ADOPCIÓN DE HERRAMIENTAS CON GEN IA ESTÁ SIENDO IMPORTANTE

89% de las empresas consideran las herramientas de Gen IA como un riesgo potencial

48% ven las herramientas de Gen IA más como una amenaza que como una oportunidad

Y todavía...

95% están utilizando herramientas GenAI de alguna forma:

57% permite su uso completamente

38% están adoptándolas con precaución...

Sólo dos de los cinco riesgos principales son asegurables y cinco del 'Top10' tampoco lo son, destaca un informe de Aon

Los riesgos de ciberataques, fallos en la cadena de suministro y el déficit de profesionales serán los grandes protagonistas en 2024



La incapacidad para atraer y mantener el talento en ciberseguridad alcanza su posición más alta en el ranking que elabora cada dos años la compañía Aon. En su 'Encuesta de Gestión Riesgos Globales de Aon 2023', eleva "el capital humano como un riesgo empresarial clave". Y es que, "atraer y retener a los mejores talentos" ya ocupa el cuarto puesto de riesgos previstos a nivel mundial, después de no figurar siquiera en el 'Top10' desde 2021, lo que muestra un cambio en la forma en que los gerentes de riesgos ven el capital humano hoy en día. Aun así, sólo el 11% de los encuestados han cuantificado estos riesgos como una brecha significativa entre concienciación y preparación.

Esta novena edición de su informe, que recoge las opiniones de casi 3.000 gerentes de riesgos, directivos de alto nivel y otros ejecutivos de 61 países y territorios para identificar sus retos empresariales más relevantes, pone de manifiesto que las cuestiones de capital humano ya no son simplemente un "problema de personas", sino un riesgo empresarial clave que es alimentado por el aumento de los costes de atención médica, la competencia por el talento, la escasez de mano de obra y la falta de preparación frente a las jubilaciones.

"El mundo es más volátil, lo que refleja una serie de profundas transiciones a través del comercio, la tecnología, el clima y las cuestiones laborales que han alertado a los líderes empresariales sobre la naturaleza cada vez más interconectada de los retos relacionados con riesgos y personas", ha destacado el CEO de Aon, **Greg Case**.

Preocupación global

Entre los datos más relevantes, los ciberataques y las violaciones de datos continúan ocupando el primer lugar en la encuesta de este año,

tanto en el resultado global como el específico para EE.UU., ascendiendo también a la primera posición en Europa y Asia-Pacífico. La inversión y mejora de la preparación frente a ellos también figura entre las principales apuestas de las empresas y, en consonancia, presenta una de las menores pérdidas de ingresos declaradas y uno de los porcentajes más altos de acciones de mitigación de riesgos.

De cualquier forma, la interrupción del negocio sigue siendo el riesgo número dos desde la encuesta de Aon de 2021, lo que refleja la realidad de que estos eventos están aumentando y pueden afectar a múltiples sectores y empresas a la vez. Le siguen en el ranking global la desaceleración económica o recuperación lenta, la incapacidad para atraer o retener a los mejores talentos y los cambios normativos y legislativos, conformando los cinco primeros puestos.

Además, es notable que a medida que los conflictos, los cambios geopolíticos y las condiciones macroeconómicas siguen teniendo repercusiones de gran alcance, la alta dirección destacó en esta edición el riesgo de fallos en la cadena de suministro y distribución en su nivel más alto en 14 años, ocupando la sexta posición.

De cualquier forma, Aon también alerta, según el último estudio realizado en este aspecto, que menos del 40% de las organizaciones han llevado a cabo evaluaciones de resistencia de los proveedores y menos del 20% han diversificado su base de proveedores para mitigar el riesgo de fallos en la cadena de suministro o distribución. Por tanto, los esfuerzos

insuficientes de mitigación parecen estar estrechamente correlacionados con un aumento de la percepción de la exposición al riesgo de la cadena de suministro/distribución.

También es llamativo que, a pesar de los titulares que protagonizan, tanto el clima (nº 17) como la inteligencia artificial-IA (nº49) están muy alejadas del 'Top10' mundial de posibles riesgos, "lo que sugiere una

debido principalmente a un aumento en el precio que afecta a la rentabilidad de las empresas. Pero sí es interesante que los tres principales riesgos globales ocupan posiciones diferentes en España: ciberataques (2º en España), interrupción de negocio (4º) y ralentización económica (8º). También, figuran en este ranking la preocupación por los cambios normativos, la incapacidad por atraer y retener talento, la falta de innovación y de dar respuesta al mercado, así como el incremento de la competencia y los posibles fallos en la cadena de suministro.

Conclusiones

"El contexto global ha cambiado significativamente con respecto a la anterior edición de la Encuesta. Las empresas se enfrentan a una mayor volatilidad derivada de la dificultad para retener y atraer talento, la inflación, la subida de tipos de interés, el mayor impacto del cambio climático y los conflictos geopolíticos", ha comentado el

Managing Director de Aon España, **Erlantz Urbietta** que resalta que, en nuestro país, el precio y escasez de las materias primas son el primer riesgo, reflejando la dependencia exterior y la criticidad de las cadenas de suministros. Además, el ciberriesgo sigue siendo una de las mayores preocupaciones para las empresas, al ser uno de los que sufre

mayor número de ataques, cada vez más sofisticados. "En este entorno, la prevención, mitigación y transferencia de riesgos, junto con el desarrollo de modelos de gestión avanzados es cada vez más estratégico para todas las organizaciones y deben ser una prioridad para los Consejos de Administración", añade. ■



falta de concienciación sobre el impacto potencial de estas cuestiones en el perfil de riesgo de las empresas", destacan los responsables del informe, a la vez que recuerdan que, curiosamente, "sólo dos de los cinco riesgos principales son asegurables y cinco del 'Top10' tampoco lo son".



Resultados en España

El informe ofrece una estadística específica para nuestro país. En ella, destaca, en primer lugar, el riesgo relacionado con el precio y la escasez de las materias primas, que se mantiene en la primera posición, al igual que en la encuesta de 2021,

Los incidentes supusieron cambios de proveedor, repensar la estrategia de ciberprotección e, incluso, la creación de nuevos roles dentro del equipo de seguridad cibernética, según Trellix

Los ciberataques con éxito ya no suponen motivo de despido: incluso conllevan más apoyo a los CISO y más presupuesto por parte del Consejo

Sufrir un incidente grave de ciberseguridad ya no es causa de despido. Así lo constata una investigación de Trellix, realizada por Vanson Bourne, bajo el título 'La mente del CISO: detrás de la brecha', con la opinión de más de 500 CISO globales de todo tipo de sectores –desde Energía, hasta Sanidad– de EE.UU., México, Brasil, Reino Unido, Francia, Alemania, Australia, India, Singapur, Emiratos Árabes Unidos, Sudáfrica, Japón y Corea del Sur que, al menos, hayan sufrido un ataque de gravedad en los últimos cinco años.

Entre otros datos de interés, destaca que, en el último año, el 63% de las organizaciones fueron víctimas de ataques repetidos. Y esta situación está dando pie a que los Consejos de Administración cambien de un enfoque reactivo a uno proactivo. El documento constata que, según los participantes, el 95% de los CISO ya recibe más apoyo de la Junta Directiva después de un ataque.

Si bien más de una quinta parte de los encuestados (22%) informaron de la pérdida del empleo o el despido como una de las respuestas de su organización a una infracción, el documento señala que el porcentaje ha disminuido en los últimos años. En concreto, se pone como ejemplo que los despidos ocurrieron casi un tercio de las veces (31%) a causa de incidentes que se produjeron hace tres o más años, mientras que solo el 13% de las violaciones en el último año llevaron a las organizaciones a desprenderse de sus especialistas en ciberprotección.

Consecuencias positivas

Eso sí, sufrir una crisis cibernética también supuso, en la mayor parte de los casos, el cambio de proveedor de ciberseguridad y una mayor automatización. De aquellos que optaron por seguir con el suyo actual, el 51% destacó que se debe a su buen precio, el 51% a su experiencia. También, resaltaron su capacidad de respuesta a incidentes (45%), así como el coste y el esfuerzo. En concreto, el 46% destacó que el coste y el esfuerzo de la transición a un nuevo proveedor serían demasiado grandes.

De cualquier forma, la respuesta a incidentes también conllevó, en el 46 % de los



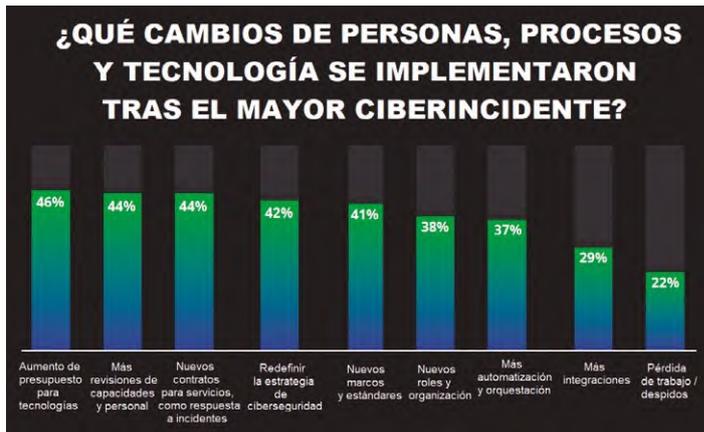
casos, incrementar el presupuesto para tecnología, en el 42% la revisión de la su estrategia general de ciberprotección buscando elementos de mejora y en el 41% la implementación de nuevos marcos y estándares.

Enfoque proactivo

“El mayor aprendizaje es que había que generar conciencia a nivel de la junta directiva... desafortunadamente, tuvo que haber un incidente para lograrlo”, comentó uno de los CISO encuestados, responsable de una agen-

importa qué tan seguros creamos que tenemos las cosas, ni cuántas herramientas tengamos implementadas, es una batalla constante”, añadió otro participante de una compañía manufacturera de Estados Unidos.

Además, el estudio destacó que los principales ataques a los que se enfrentan los CISO son el robo de datos (48%), a través de malware (43%) y de interrupción del negocio con incidentes DDoS (37%). Asimismo, los participantes destacaron como principales impactos tras un ciberataque desde la pérdida de datos (42%), hasta un estrés significativo para sus equipos de SecOps (41%) y una reputación en declive (39%).



Talón de Aquiles

También, resaltaron que la tecnología configurada incorrectamente (45%), las brechas en la capacidad de seguridad de la tecnología (42%) y las tecnologías aisladas (42%) jugaron un papel protagonista en muchos de los incidentes, además de destacar (53%) que un exceso de procesos manuales retrasaba la detección o mitigación de las amenazas cibernéticas. Por ello, el 92% de los encuestados se mostró de acuerdo en que es necesario

mejorar en personas, procesos y tecnología después de experimentar un incidente cibernético importante. ■

El ex CISO de UBER analiza los grandes retos de la profesión, tras ser condenado en 2022, con gran repercusión mediática



Especialmente relevante han sido, en este ámbito, las declaraciones del exCISO de Uber, Joe Sullivan, en Black Hat Europe 2023, tras ser condenado hace dos años por cargos

federales relacionados con el encubrimiento del robo de información personal de los conductores y clientes de Uber de 2016. En su intervención resaltó que la tendencia de responsabilizar al CISO hace que este “no piense en el panorama general, sino en sí mismo”, habiendo incluso muchos que consideren cambiar de trabajo. “El CISO libra una batalla cuesta arriba todos los días en su trabajo. Están rogando por recursos, están tratando de que el resto de la empresa baje el ritmo y piense en las cosas que les importan”, destacó. “Cuando eres

el ejecutivo responsable de la seguridad, eres el único ejecutivo que tiene adversarios activos fuera de tu organización que intentan destruirte”, dijo.

Sin embargo, también consideró que “no hay que huir de esta situación”: “si lo hacemos, perderemos una gran oportunidad”. Terminó indicando que se avecina un panorama muy diferente, con muchísima regulación y dando cuatro consejos a los CISO: desarrollar un plan personal de respuesta a incidentes, potenciar sus relaciones internas, crear equipos de absoluta confianza y contar con una ‘estación de bomberos’, preparada para ‘emergencias’. “¿Vamos a convertirnos en el equipo que está metido en la maleza lidiando con los controles técnicos y no invitado a la sala ejecutiva, o vamos a ser un equipo muy respetado y confiable en los niveles más altos del gobierno y entre las grandes corporaciones?”, preguntó a los asistentes.

Cómo alcanzar la seguridad Zero-Trust en Kubernetes con SUSE NeuVector

Kubernetes es una tecnología basada en el paradigma de los micro-servicios. Dada la cantidad de objetos que estas tecnologías gestionan, esto puede tornarse en un tema abrumador, convirtiendo en un verdadero reto el conseguir una seguridad Zero-Trust, protegiendo de manera eficiente y sin un autoconsumo elevado. SUSE NeuVector soluciona todos estos problemas con un enfoque Kubernetes nativo.

La Importancia de asegurar despliegues de contenedores

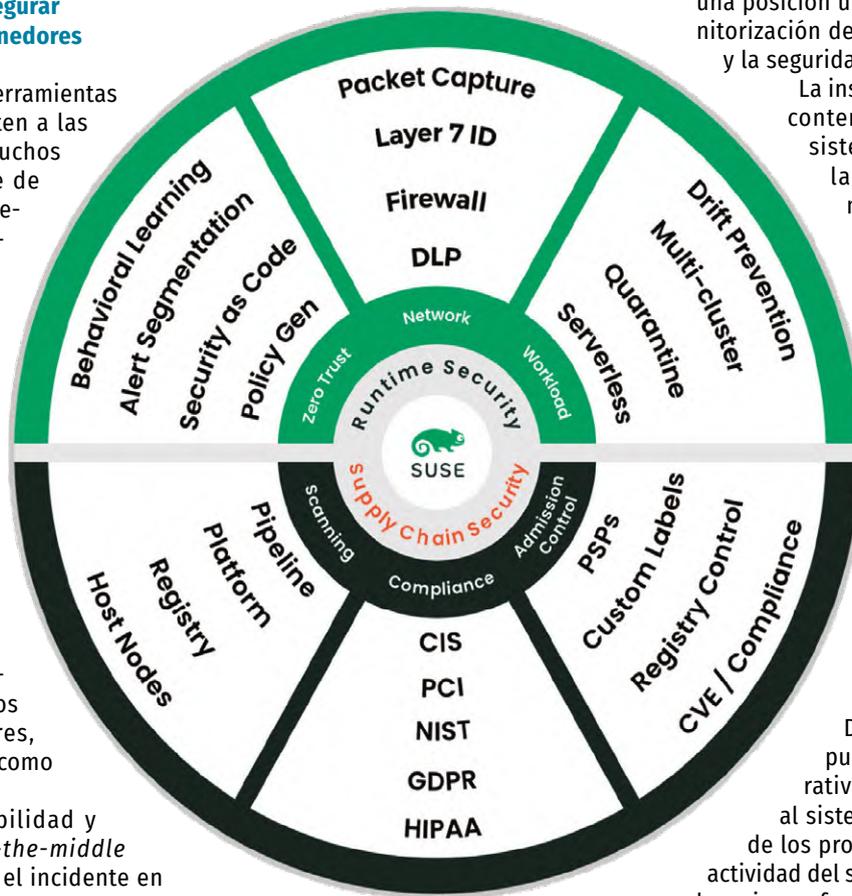
Los contenedores y herramientas como Kubernetes permiten a las empresas automatizar muchos aspectos del despliegue de aplicaciones, brindando beneficios comerciales significativos. Sin embargo, estos nuevos despliegues son igualmente vulnerables a ataques y explotaciones por parte de hackers e *insiders*, al igual que los entornos tradicionales.

La extorsión con *ransomware*, el *crypto-jacking*, el robo de datos y la interrupción del servicio seguirán siendo utilizados contra los nuevos entornos virtualizados basados en contenedores, tanto en nubes privadas como públicas.

La reciente vulnerabilidad y explotación de *man-in-the-middle* en Kubernetes, así como el incidente en Tesla, son solo los primeros de muchos posibles *exploits* basados en tecnología de contenedores que se espera proliferen en los próximos meses y años.

Seguridad de Contenedores en la cadena de suministro

SUSE NeuVector habilita a organizaciones globales para asegurar de manera integral sus aplicaciones nativas de Kubernetes sin comprometer la velocidad del negocio. La plataforma unificada de seguridad y cumplimiento de SUSE NeuVector simplifica y automatiza la seguridad, al tiempo que ofrece seguridad Zero-Trust para aplicacio-



nes nativas de Kubernetes desde la fase de desarrollo hasta la producción a través de escaneo de vulnerabilidades y cumplimiento en el *pipeline*.

Como última barrera antes de entrar en producción, un *admission controller* permite controlar la entrada de contenedores vulnerables o accesos no autorizados.

Seguridad de Contenedores en tiempo de ejecución en Kubernetes

Una vez que los contenedores están en ejecución en producción, un avanzado

sistema de *Deep Packet Inspection* y un algoritmo de aprendizaje de comportamiento automático de aplicaciones, permiten a SUSE NeuVector garantizar una seguridad Zero-Trust facilitando el escaneo de contenedores y cumplimiento de políticas también en tiempo de ejecución.

El *firewall* de SUSE NeuVector nativo de Kubernetes aprende del comportamiento de la aplicación para la creación automática de reglas de *firewall*. A las reglas de *firewall* de capa 7 de este-oeste y entrada-salida, se le añade la detección de ataques a aplicaciones basadas en red, como DDoS, DNS e inyección SQL.

El cortafuegos también se encuentra en una posición única para incorporar la monitorización de procesos de contenedores y la seguridad del *host*.

La inspección de los procesos en contenedores y la actividad del sistema de archivos, así como la detección de comportamientos sospechosos, nos proporcionan una herramienta adicional de seguridad que nos permitirá bloquear incluso vulnerabilidades *Zero-day*. El comportamiento aprendido de nuestra aplicación de manera automática nos permite defendernos de cualquier comportamiento anómalo.

Al igual que con los contenedores, es necesario monitorizar el sistema *host* en busca de actividades sospechosas.

Dado que los contenedores pueden ejecutar sistemas operativos y aplicaciones similares al sistema *host*, la monitorización de los procesos de contenedores y la actividad del sistema de archivos requiere las mismas funciones de seguridad que la monitorización de los sistemas *host*.

Todo lo mencionado anteriormente se puede exportar como seguridad como código en un formato YAML nativo de Kubernetes que nos permitirá automatizar nuestras políticas de seguridad.

SUSE NeuVector está disponible en cualquier distribución de Kubernetes, como SUSE Rancher, OpenShift, EKS, AKS, GKE, etc. ■

GUSTAVO VARELA
Solutions Architect
SUSE
gvarela@suse.com

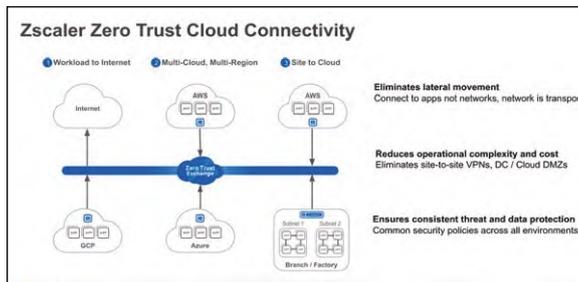


ZSCALER ANUNCIA AVANCES PIONEROS EN ZERO TRUST PARA SALVAGUARDAR LAS CARGAS DE TRABAJO Y LA INFRAESTRUCTURA DE ESCRITORIOS VIRTUALES (VDI) EN LA NUBE

Para 2025, más del 95% de las nuevas cargas de trabajo digitales se implementarán en plataformas nativas de la nube, frente al 30% en 2021, según Gartner.

Por ello, **Zscaler** ha desarrollado **Zero Trust Exchange**, en la que aúna numerosas innovaciones para aumentar y mejorar la seguridad de las cargas de trabajo y de infraestructura de escritorios virtuales (VDI) en la nube, con avances pioneros en Confianza Cero para esta labor.

Así, entre sus características destacan desarrollos en **Zscaler Workload Communications** que permiten, por un lado, una segmentación de la carga de trabajo mediante etiquetas definidas por el usuario. Y es que, la firma dispone de integración nativa con AWS Workload Tagging para proporcionar granulari-



dad de segmentación por políticas. “En AWS, Zscaler permite la creación exclusiva de grupos de seguridad personalizados basados en etiquetas definidas por el usuario y características nativas”, detallan desde la compañía.

También, proporciona detección de recursos en

tiempo real. Habilitando grupos personalizados, la integración nativa de Zscaler con AWS detecta automáticamente VPCs, subredes y recursos EC2, incluyendo sus etiquetas y atributos asociados en tiempo real. Junto a ello, ofrece, según la compañía, “una primicia en la industria”: Seguridad VDI multisesión, donde Zscaler inspecciona todos los puertos y protocolos para implementaciones VDI multisesión y no permanentes en la nube pública.

Además, Workload Communications ahora es compatible con Google Cloud Platform (GCP), además de Azure China Regions y AWS GovCloud con certificación FedRAMP.

ZSCALER
www.zscaler.com

CROWDSTRIKE PRESENTA FALCON DATA PROTECTION Y UNA VERSIÓN DE FALCON GO PARA PYMES

CrowdStrike ha actualizado su portafolio con dos nuevas soluciones: **Falcon Data Protection**, para evitar la exfiltración y las fugas accidentales de información; y una nueva versión de **Falcon Go**, para ayudar a las pymes a detener los ataques de ransomware y prevenir brechas de datos.



Con la primera de ellas, la compañía busca liberar a las empresas de sus productos DLP heredados “complicados de instalar y difíciles de gestionar, además de que hacen imposible el análisis

de datos en un entorno *cloud* y de IA”, para evolucionar a una solución con un enfoque innovador y sin fricciones, a través de “un agente único y muy ligero”, explican sus responsables.

Así pues, la solución, que se incluye en su plataforma Falcon XDR, permite “proteger los datos de forma inmediata desde el agente Falcon para consolidar los productos DLP existentes, reduciendo la complejidad”, destacan. Además, amplía la visibilidad de los flujos de datos en la empresa para identificar de forma rápida –y detener– cualquier exfiltración o fuga accidental. Con ello, es capaz de acelerar la detección y la respuesta desde una consola única y con un flujo de trabajo unificado que ahorra tiempo a los analistas de seguridad que investigan potenciales robos de datos.

Protección avanzada para pymes

Por otro lado, la más reciente versión de Falcon Go, basada en IA, refuerza la seguridad de las pymes a través de una protección preconfigurada que “permite una puesta en marcha inmediata para proteger y gestionar dispositivos”, según sus responsables.

Ofrece, además, protección verificada desde una consola simple y unificada que muestra qué dispositivos están protegidos y que resume la actividad relacionada con amenazas y la eficacia del producto a la hora de detener ataques.

CROWDSTRIKE
www.crowdstrike.com/sites/es

NEXT GEN SASE BRANCH, DE NETSKOPE, LA NUEVA GENERACIÓN DE SASE IMPULSADA POR BORDERLESS SD-WAN, PARA RESPONDER A LOS RETOS DE LAS SUCURSALES

Netskope ha presentado **Next Gen SASE Branch**, con la finalidad de ofrecer una solución a los retos que rodean a la infraestructura actual de las sucursales, que dependen de SD-WAN heredadas y de múltiples tecnologías de seguridad de red disgregadas, y que no pueden abarcar la gran cantidad de aplicaciones en la nube y dispositivos IoT que ahora se utilizan, entre otros problemas.

Se trata de una solución que está impulsada por su reconocido Borderless SD-WAN, combinando un dispositivo SD-WAN y de seguridad unificado (Netskope SASE Gateway), con un SASE Fabric adaptado al entorno, una protección basada en Confianza Cero y con un orquestador de nube respaldado por SkopeAI.

Entre sus características destaca que dicho SASE Fabric adaptable al entorno admite más de 75.000 aplicaciones y valores predeterminados de QoS (calidad de servicio) inteligentes fundamenta-



dos en el índice de confianza de la nube (CCI), inteligencia de dispositivos IoT basada en AI/ML para ingeniería de tráfico, y segmentación consciente de VRF (reenvío de ruta virtual), así como enrutamiento avanzado entregado de extremo a extremo a través de centros de datos y nubes.

Proporciona también una seguridad híbrida de Confianza Cero, integrando las funciones de Secure

Web Gateway (SWG) y Cloud Access Security Broker (CASB) distribuidas en la nube, junto con las capacidades locales de Cortafuegos de Aplicación, sistemas de prevención y detección de intrusiones (IPS/IDS) y Device Intelligence, entre otros.

Cabe destacar también su Cloud Orchestrator impulsado por SkopeAI, que agiliza la gestión de la red y la seguridad mediante una consola unificada y la aplicación de políticas coherentes con el entorno en sucursales, ubicaciones remotas y diversos entornos en la nube. Además, proporciona visibilidad de la ruta de extremo a extremo y rendimiento de aplicaciones con su Proactive Digital Experience Management (P-DEM).

NETSKOPE
www.netskope.com/es

PALO ALTO NETWORKS PRESENTA SU STRATA CLOUD MANAGER DE GESTIÓN Y OPERACIONES ZERO TRUST IMPULSADA POR INTELIGENCIA ARTIFICIAL

Strata Cloud Manager es el nombre de la más última solución de gestión y operaciones Zero Trust impulsada por IA de Palo Alto Networks. La compañía, además, ha anunciado un conjunto de capacidades de seguridad avanzadas y cinco *firewalls* de nueva generación.

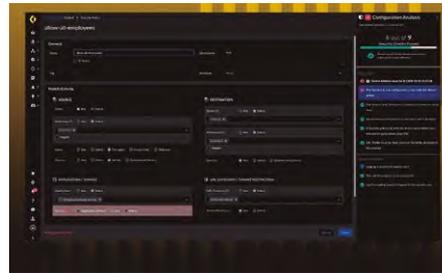
Con Strata Cloud Manager, la firma busca redefinir la seguridad de la red. Para ello, los equipos de seguridad pueden conseguir un tiempo de actividad de la red continuo, gracias a su análisis predictivo. Además, refuerza la seguridad de la red aprovechando el análisis de políticas basado en IA y las comprobaciones de cumplimiento en tiempo real. También, permite supervisar "sin esfuerzo" la configuración y las políticas de seguridad en todos los factores de forma, incluidos SASE y *firewalls*, tanto de hardware como de software.

Como parte de sus servicios de seguridad en la nube, la compañía también ha incorporado capacidades como **Advanced WildFire**, que bloquea los

ataques iniciales en mediante la integración del *machine learning* directamente en sus motores de detección basados en la nube. A ello se suman capacidades de detección frente a ataques *meddler-in-the-middle* y de *phishing*, alojados en plataformas SaaS, así como prevención avanzada frente a ataques de mando y control (C2).

Nueva generación de cortafuegos

Palo Alto Networks ha anunciado también cinco nuevos firewalls: **PA-7500** para un rendimiento "ultrarrápido", **PA-415-5G** para redes 5G, **PA-450R** para los entornos OT. Palo Alto Networks también



presentó el **PA-5445** para proteger centros de datos y grandes instalaciones, y el **PA-455** para proteger sucursales que necesitan alimentación a través de Ethernet. Asimismo, ha presentado **Cortex XSIAM 2.0**, que incluye un nuevo marco de *machine learning*

(BYOML), que permite que los vastos datos de seguridad almacenados en XSIAM estén disponibles para que los equipos de seguridad puedan crear e integrar sus propios modelos de ML. Además, mejora en visibilidad y priorización de amenazas con el nuevo **XSIAM Command Center**.

PALO ALTO NETWORKS
www.paloaltonetworks.com

STORMSHIELD EVOLUCIONA SU TECNOLOGÍA EDR HACIA UNA SOLUCIÓN XDR DE DETECCIÓN, ORQUESTACIÓN Y RESPUESTA

Como una versión evolucionada de las herramientas de detección y respuesta como EDR, **Stormshield** ha desarrollado **Stormshield eXtended Detection & Response (XDR)** que detecta, gestiona y responde a los incidentes cibernéticos.



En ella, combina las capacidades de Stormshield Network Security (SNS), para proteger la red, y de Stormshield Endpoint Security (SES), para salvaguardar los *endpoints*, respaldado por la experiencia de la compañía en ciberinteligencia (CTI) para anticiparse a las amenazas. Todo ello orquestado por Stormshield Log Supervisor (SLS) para alertar en tiempo real y ofrecer una respuesta rápida y sostenible tanto para la red, como para los puestos de trabajo.

Cabe destacar también, el análisis en profundidad del comportamiento que abarca las tramas de la red, el comportamiento del sistema operativo, los procesos o los archivos que reciben los empleados, así como la correlación de todos los eventos para identificar señales débiles, ofreciendo una visión de los ciberataques más sofisticados y capacidad para responder a ellos.

En definitiva, Stormshield XDR consigue reducir los riesgos y puntos ciegos, recibir alertas en tiempo real, correlacionar los eventos notificados por las distintas soluciones de ciberseguridad y gestionar incidentes a través de escenarios de respuesta y remediación.

STORMSHIELD
www.stormshield.com

COMMVAULT AÚNA SUS SOLUCIONES SAAS Y SOFTWARE EN SU PLATAFORMA CLOUD

Commvault ha unificado todas las ofertas de SaaS y software de la compañía en una sola plataforma, **Commvault Cloud** con la tecnología de **Metallic IA**, donde la visibilidad y el control se pueden gestionar de forma holística a través de un único panel.

Se trata de una solución que "está especialmente diseñada para la resiliencia cibernética, con el fin de permitir a los usuarios predecir las amenazas con mayor rapidez, realizar recuperaciones limpias y acelerar los tiempos de respuesta ante las amenazas",



destacan sus responsables.

En ella, aprovecha los beneficios de la IA, por ejemplo, a través de **Arlic** (abreviatura de 'Autonomous Resilience'), un nuevo copiloto de IA disponible 24x7 que puede responder a las preguntas en un lenguaje claro y sencillo. Entre sus características, destaca su capaci-

dad para proporcionar respuestas personalizadas y procesables.

Junto a ello, ha presentado **Cleanroom Recovery**, un servicio que, en colaboración con Microsoft Azure, los clientes pueden utilizar para "recuperar a una sala limpia en la nube siempre preparada". Además, ha puesto en marcha **Platinum Resilience**, un servicio gestionado que proporciona una protección, compromiso y capacidad de respuesta ante amenazas y situaciones de desastre.

Alianzas con referentes del sector

Sin duda, Commvault Cloud es una de las grandes apuestas de la compañía para la que está impulsado integraciones con referentes de la industria. A principios de este año, anunció integraciones con **Microsoft Sentinel** y **Palo Alto Networks**. Y, a día de hoy, entre los *partners* de seguridad e IA que se están integrando con Commvault Cloud se encuentran **Avira (parte de Gen)**, **Darktrace**, **Databricks**, **Entrust**, **Netskope** y **Trellix**.

COMMVAULT
www.commvault.com

BREVE

■ **Telefónica Tech** ha presentado un servicio integral de ciberinteligencia para grandes empresas que proporciona orientación experta e inteligencia en tiempo real abarcando todos los niveles del análisis de ciberamenazas. Forma parte de los servicios gestionados de NextDefense y la compañía presta el servicio desde su Centro de Operaciones Digitales (DOC), que opera con dos ubicaciones en España y Colombia.



NOVEDADES

KASPERSKY APUESTA POR XDR CON UNA PLATAFORMA UNIFICADA PARA PROTEGER ARCHIVOS Y PROCESOS

Kaspersky ha desarrollado una nueva solución integral de seguridad de Detección y Respuesta Extendidas (XDR) para proteger archivos y procesos frente a amenazas avanzadas, APT y ataques dirigidos, además de incluir análisis de registros, casos de éxito, investigación y guías de respuesta.

Kaspersky XDR, que se gestiona de forma sencilla desde una plataforma abierta y de administración única, dispone de seguridad local integral, permitiendo que los datos confidenciales

de los clientes permanezcan dentro de la propia infraestructura, al tiempo que “se cumple con los requisitos de soberanía de los datos”, aseguran desde la compañía.

La solución proporciona capacidades de detección y respuesta contra amenazas mediante una amplia gama de fuentes de datos, incluidos registros de terminales, redes y distintos sistemas operativos y apps. Realiza

análisis avanzados relacionando y analizando automáticamente datos de múltiples fuentes y, también, puede ejecutar respuestas automatizadas para contener posibles riesgos. Además, posee capacidades de búsqueda para detectar de forma proactiva amenazas avanzadas. Junto a ello, ofrece un área de

gráficos de análisis para facilitar el proceso de inicio de la investigación de alertas e incidentes. Y, permite la creación de guías para personalizar los flujos de trabajo, y generar escenarios

de respuesta personalizados. Cabe destacar, además, que la herramienta puede integrarse con otras soluciones de Kaspersky, así como con productos de terceros, como sistemas de protección de puntos finales y servicios de Inteligencia de Amenazas.

KASPERSKY
www.kaspersky.es



EXCLUSIVE NETWORKS INCLUYE EN SU PROPUESTA X-OD EL SERVICIO DE ALMACENAMIENTO CLOUD DE CUBBIT

La plataforma digital X-OD de **Exclusive Networks** ahora cuenta con el servicio de almacenamiento *cloud* geo-distribuido de **Cubbit**. La solución es compatible con S3 de Amazon Web Services (AWS) y permite a las empresas contar con “la máxima protección y cumplimiento normativo para sus copias de seguridad, a la vez que ahorra un 80% en precio frente a los hiperescalares”, destacan sus responsables.

Entre sus características, destaca el hecho de que, en lugar de adoptar el método tradicional de almacenamiento en *cloud* centralizada, Cubbit dispersa tus datos en diversas ubicaciones.

Los *buckets* S3 están cifrados, fragmentados y replicados en redes geográficamente dispersas, proporcionando una protección ante *ransomware* y otros posibles desastres inesperados.

Este sistema de distribución avanzado abarca diversas ciudades dentro de un país,

cumpliendo con las regulaciones específicas sobre protección de datos de dicho país.

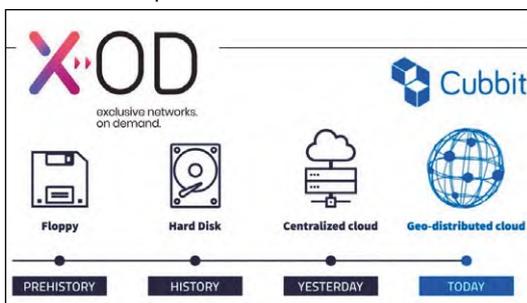
A diferencia del almacenamiento en la nube tradicional, Cubbit no guarda datos en unos pocos centros de datos centralizados. En cambio, los archivos están cifrados,

fragmentados y replicados en redes geodistribuidas, protegidos contra desastres, *ransomware* y violaciones de datos.

Este mecanismo avanzado

de distribución se extiende por varias ciudades dentro de un solo país, adecuándose al cumplimiento de las leyes específicas de soberanía de datos de la nación. De hecho, Cubbit permite a los usuarios geolocalizar el área donde se almacenan los datos cumpliendo totalmente con el GDPR, CCPA, ACN (anteriormente AgID) e ISO.

EXCLUSIVE NETWORKS
www.exclusive-networks.com/es



SUSE ACTUALIZA SU PORTAFOLIO CLOUD NATIVE PARA GESTIONAR DICHOS ENTORNOS A ESCALA

SUSE ha llevado a cabo una serie de actualizaciones en su portafolio entre las que destacan la **versión 2.0 de Rancher Prime**, además de la edición comunitaria de **Rancher 2.8**, **SLE Micro 5.5** y los planes de futuro para **SUSE Edge**. En general, las nuevas características continúan estando enfocadas en resolver las necesidades de los desarrolladores, al mismo tiempo que promueven la misión de SUSE dotar de mayor capacidad de elección a sus clientes.

En concreto, Rancher Prime 2.0, incluye una mayor integración con el portafolio de SUSE y nuevas extensiones de la interfaz de usuario (UIE).

Además, la compañía ha presentado Rancher Prime Application Collection, una biblioteca de aplicaciones seleccionadas para infraestructura y desarrolladores que, entre otros aspectos, están respaldadas por los principios de Zero Trust de SUSE y las garantías de seguridad de la cadena de suministro de software. A ello, se le une un asistente virtual, basado en IA generativa, que mejora la experiencia del usuario, así como capacidades de evaluación de rendimiento y asistencia técnica a largo plazo.



Por su parte, Rancher 2.8 ya está disponible con nuevas características que incluyen: compatibilidad mejorada con Kubernetes, personalización mejorada de la plataforma con la nueva API pública segura de autoservicio, además de flujos de trabajo GitOps mejorados.

SLE Micro 5.5, el sistema operativo “ligero y ultrafiable” está diseñado específicamente para cargas de trabajo virtualizadas o contenerizadas y ahora permite a los usuarios descargar imágenes y contenedores desde registros de confianza. También, permite transferir e integrar imágenes para su uso en entornos desconectados. Gracias a ello, es posible seguir lanzando procesos cuando no se desea o no se puede acceder directamente a los registros.

En paralelo, SUSE realizó la primera demostración de la integración de SUSE Edge con entornos Industrial Internet of Things (IIoT), que estará disponible en 2024. Gracias a Edge IIoT, las organizaciones pueden evolucionar sin problemas desde sus tecnologías *legacy* hacia el uso de cargas de trabajo modernas en el Edge basadas en contenedores, Kubernetes y estándares abiertos. Además, A principios de 2024, SUSE ampliará sus alianzas para soluciones Edge con **Buoyant** y **Synadia**.

SUSE
www.suse.com

CHECK POINT AMPLÍA EL CATÁLOGO DE INFINITY GLOBAL SERVICES PARA AUMENTAR LA PROTECCIÓN DE LA RED Y LA NUBE, ENRIQUECIDO CON LA INTELIGENCIA DE AMENAZAS DE THREATCLOUD AI

Fruto de la adquisición del proveedor de servicios norteamericano, **rmsource**, **Check Point** ha ampliado su catálogo **Infinity Global Services**, el cual, opera sobre cuatro pilares centrales: evaluar, optimizar, dominar y responder, además de estar 'enriquecido' con la inteligencia de amenazas, en tiempo real, de ThreatCloud AI.



En concreto, las mejoras se han destinado a aumentar la seguridad de red, donde la compañía

ofrece las capacidades del Centro de Operaciones de Red (NOC) y el Centro de Operaciones de Seguridad (SOC) como servicio, con herramientas y procesos para optimizar la protección y la infraestructura de red.

También, ha incrementado la seguridad en la nube, poniendo a disposición de los clientes expertos en *cloud* para facilitar una migración confiable, mejorar la postura de protección en esta plataforma y ofrecer

servicios de gestión de la seguridad en la nube (CSPM) y plataformas de protección de aplicaciones nativas (CNAPP). Junto a ello, Check Point ha ampliado **Horizon MDR/MPR** con las funcionalidades de la plataforma **Microsoft Sentinel** para el análisis de seguridad, detección de incidentes y respuesta a los mismos.

En total, desde su lanzamiento hace cinco meses, con Infinity Global Services la compañía ofrece más de 30 servicios a medida a más de 2.400 empresas de todo el mundo con el respaldo de 400 consultores especializados y 150 investigadores globales.

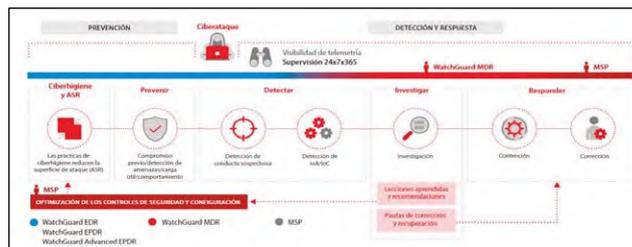
CHECK POINT
www.checkpoint.com/es

ACELERAR LA PRESTACIÓN DE SERVICIOS PARA QUE LOS MSP OFREZCAN LAS CAPACIDADES DE UN SOC MODERNO, OBJETIVO DE WATCHGUARD MDR

WatchGuard ha desarrollado un servicio 24x7, gestionado por un equipo de expertos en ciberprotección e impulsado por IA, diseñado especialmente para que los proveedores de servicios gestionados (MSP), puedan ofrecer detección y respuesta de amenazas a sus clientes, sin tener la carga de construir y gestionar un SOC interno.

Bajo el nombre de **WatchGuard MDR**, la compañía aborda con esta propuesta la escasez de profesionales y financiación a las que se enfrentan los MSP.

Para ayudarles, con esta solución proporciona una alta capacidad de personalización, además de ser muy escalable. Además, esta propuesta viene a reforzar la arquitectura Unified Security Platform de WatchGuard, proporcionando capacidades avan-



zadas de detección y respuesta a amenazas sobre WatchGuard EDR, EPDR y Advanced EPDR, que permiten a los MSP construir ofertas muy completas para sus clientes.

Incluye, también, soporte del servicio automatizado Zero-Trust Application Service, Threat Hunting Service, analíticas de seguridad avanzadas, inteligencia de amenazas y un equipo dedicado de analistas cualificados que monitorizan, de-

tectan y responden a las amenazas 24x7. Así pues, entre sus características más destacadas se encuentran la monitorización continua de la actividad de los *endpoints* y recopilación de datos, identificación y detección proactiva, investigación y validación, notificación rápida de incidentes con información clave (como los equipos afectados y las tácticas utilizadas), opciones para la mitigación y directrices para la remediación con el fin, según la compañía, de dar a los MSP la flexibilidad de elegir la estrategia que mejor funcione para su negocio, así como informes cada semana del estado de la seguridad y, cada mes, sobre su actividad.

WATCHGUARD TECHNOLOGIES
www.watchguard.com/es

DELINEA DESARROLLA INTELLIGENT AUTOMATED AUDITING PARA REDUCIR EL RIESGO, SIMPLIFICAR PROCESOS Y MEJORAR LA SEGURIDAD CON IA

Bajo el nombre de **Intelligent Automated Auditing (IAA)**, **Delinea** ha desarrollado una solución con Inteligencia Artificial (IA) que acelera la detección y la respuesta ante el abuso de privilegios. Se trata de la primera de varias herramientas de gestión de accesos privilegiados con innovaciones de IA en la Plataforma Delinea.

Con ellas, la compañía busca mejorar la detección de anomalías, el desarrollo de políticas y la visualización de alertas, "con el objetivo de ser las soluciones PAM más inteligentes", destacan sus responsables.

Así los clientes de la plataforma de Delinea que aprovechen IAA podrán, por ejemplo, utilizar una combinación de reconocimiento de la actividad del usuario y de aprendizaje de IA para supervisar grabaciones privilegiadas de la sesión y detectar actividades potencialmente peligrosas, como agregar a un nuevo usuario del administrador. El uso

de la IA ayudará a los administradores también a reducir la necesidad de revisar, de forma manual, horas de grabaciones de sesiones tras un incidente de seguridad.

Futuras innovaciones basadas en IA

Según destaca la compañía, sus equipos de innovación y producto están diseñando y probando funcionalidades adicionales aumentadas por IA. Entre ellas, destacan la funcionalidad **Delinea Copilot**, que ayudará a los administradores PAM con las tareas y solicitudes rutinarias del día a día, reduciendo su esfuerzo y estrés. Además, en el futuro, la aplicación contextual de la autenticación multifactor (MFA) "podrá aumentar o reducir el umbral de los desafíos de la MFA en función de los factores de riesgo que afecten al perfil de seguridad de una identidad", explican desde Delinea. Asimismo,



mo, resalta que las políticas de acceso privilegiado serán más dinámicas, recomendando políticas que estén alineadas con las mejores prácticas de mínimo privilegio y proporcionando recomendaciones para ajustes de políticas que puedan mejorar la seguridad y la productividad basadas en el perfil de riesgo de un cliente.

DELINEA
https://delinea.com



QUALYS PRESENTA ENTERPRISE TRURISK PARA LA MEDICIÓN, COMUNICACIÓN Y REDUCCIÓN DE LOS CIBERRIESGOS

Ayudar a las organizaciones a medir de manera integral el ciberriesgo, comunicarlo de la forma más efectiva posible y eliminarlo proactivamente. Estos son los principales objetivos para los que **Qualys** ha desarrollado la plataforma **Enterprise TruRisk**. Se trata de una herramienta fruto de su compromiso de “ofrecer soluciones más potentes de seguridad para la gestión de la superficie de ataque, la gestión de vulnerabilidades y la remediación, además de proporcionar un mayor nivel de orquestación”, señalan sus responsables.

Así pues, Enterprise TruRisk permite a los usuarios medir el ciberriesgo a través de todas las herramientas de seguridad y TI, sean o no de Qualys, dentro de una organización. Y es que, además de los datos de la Qualys Threat Library y más de 25 fuentes de inteligencia de amenazas, la plataforma incorpora datos de otras soluciones de terceros.



Además, facilita la, en numerosas ocasiones, complicada misión de comunicar el ciberriesgo, transformando datos dispares en conocimientos prácticos y métricas de impacto, para que el negocio lo comprenda mejor.

La solución también elimina el ciberriesgo con acciones precisas de remediación y mitigación, yendo más allá de la aplicación de parches para introducir métodos dinámicos para la reducción de riesgos.

Soluciones para pymes

En paralelo, Qualys ha anunciado la disponibilidad de las reconocidas capacidades de sus soluciones **VMDR TruRisk**, **FixIT** y **ProtectIT** en **AWS Marketplace**, con precios y paquetes dirigidos a pequeñas y medianas empresas. El paquete incluye protección frente a vulnerabilidades, gestión de parches, así como capacidades de EDR.

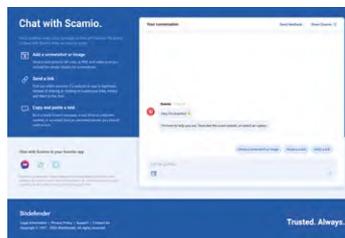
QUALYS
www.qualys.com

BITDEFENDER SUMA A SU CARTERA SERVICIOS DE CIBERPROTECCIÓN OFENSIVA Y DETECCIÓN DE ESTAFAS

Bitdefender ha sumado a su portafolio una oferta de servicios denominada **Offensive Services**, diseñada para evaluar, identificar y remediar, de forma proactiva, las brechas de seguridad en una organización (en la nube, local e híbrida), a través de pruebas de intrusión y ataques simulados de *red teaming*. Además, ha presentado **Scamio**, una solución gratuita de detección de estafas en línea.

Por un lado, los servicios de ciberprotección ofensiva están dirigidos por un equipo exclusivo de analistas, investigadores, cazadores de amenazas y hackers éticos de ciberseguridad acreditados por CREST y respaldados por la Red de Protección Global de Bitdefender, compuesta por “cientos de millones de sensores”, que recopila continuamente datos de amenazas en todo el mundo.

En concreto, en esta propuesta destaca su **Bitdefender penetration testing**, un servicio donde un equipo de hacking ético realiza una evaluación de vulnerabilidades en los sistemas



que cubren redes, aplicaciones y dispositivos móviles, entre otros, de una empresa. Las debilidades encontradas se utilizan para llevar a cabo ciberataques simulados autorizados que ponen a prueba sus defensas y controles de ciberprotección.

Además, su servicio **Bitdefender red teaming** ofrece un simulacro para demostrar cómo los atacantes intentarían comprometer las funciones críticas y los sistemas estratégicos de una empresa.

Detección de estafas

Bitdefender, también ha dado a conocer **Scamio**, un servicio gratuito de detección de estafas diseñado para identificar intentos de fraude en línea recibidos por correo-e, enlaces integrados, SMS y mensajería instantánea, gracias a la colaboración de un *chatbot* impulsado por IA.

BITDEFENDER
www.bitdefender.es

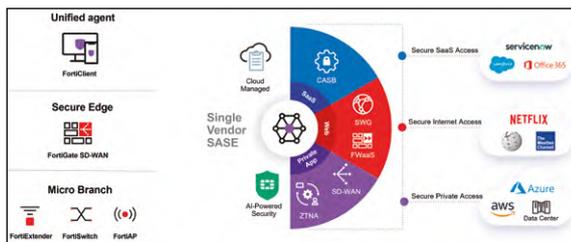
FORTINET EXTIENDE SU OFERTA SASE Y ACTUALIZA SU PLATAFORMA DE SEGURIDAD PARA ENTORNOS OT

Fortinet ha llevado a cabo una importante inversión en **Universal SASE** expandiendo el alcance de su oferta de **Secure Access Service Edge (SASE)** en tres áreas clave de su catálogo. Junto a ello, ha actualizado su portafolio de soluciones y servicios para entornos industriales.

En primer lugar, Fortinet ofrece ahora más de 100 localizaciones **cloud FortiSASE**. La compañía, además, lleva la pila completa SASE a los campus y sedes con el nuevo **FortiGate 120G SASE**. Junto a ello, el programa **FortiFlex** se amplía también a las soluciones de Universal SASE, tanto si los clientes quieren usarlo en sus instalaciones como para servicios *cloud*.

Soluciones y servicios OT

La firma, también ha actualizado su **Plataforma de Seguridad OT**, un conjunto integrado de productos, soluciones, y servicios para redes industriales. En concreto, para el área de redes seguras, ha ampliado su cartera con el nuevo **FortiSwitch Rugged 424F**, el punto de acceso



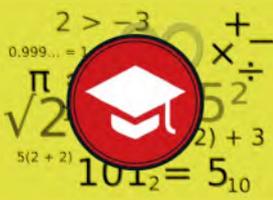
FortiAP 432F, **FortiExtender Vehicle 211F** inalámbrico, además de actualizar su sistema operativo FortiOS con el panel

OT View, que correlaciona y muestra datos OT importantes.

Fortinet ha mejorado, asimismo, **FortiAnalyzer**, que ahora incluye informes de análisis, riesgos y cumplimiento específicos para OT; **FortiNDR**, que ya puede analizar más de 15 protocolos de red OT diferentes e incluye análisis de comportamiento de redes basados en IA; **FortiDeceptor**, su tecnología para el aislamiento temprano de ataques y violaciones es ahora compatible con 30 protocolos y señuelos OT adicionales.

Además, el servicio **FortiGuard**, que cuenta con una de las bases de datos más completas de inteligencia sobre amenazas OT, ahora también cubre más de 70 protocolos y más de 4.000 firmas de vulnerabilidad de aplicaciones y dispositivos en entornos industriales.

FORTINET
www.fortinet.com



Del 7 al 9 de marzo, con el aforo ampliado a cinco salas

RootedCON convoca una potente XIV edición en Madrid y se expande a Portugal e Iberoamérica

Considerado el congreso español técnico de referencia, **RootedCON** está creciendo, tanto nacional como internacionalmente, y este año, celebrará ediciones en Málaga (enero), Madrid (marzo), Panamá (abril), Lisboa (junio) y Valencia (septiembre). Una efervescencia fruto de su buen hacer en pro de la comunidad técnica. Por supuesto, su evento en Madrid, en los cines Kínepolis, será su gran cita anual en el que este año se espera superar los 5.000 asistentes, ya que se ampliará el aforo de tres a cinco salas. “Hemos prestado atención más que nunca a ofrecer unas ponencias que tanto por su calidad técnica, como por su novedad, no dejarán indiferentes a nadie”, destaca su presidenta, **Arantxa Sanz**, que, entre otras, resalta la “que impartirán, sobre ciberseguridad en trenes,

los conocidos **David Meléndez** y **Gabriela García**, y la de los **Mossos d'Escuadra**, que presentarán una investigación que ha durado cinco años, junto al trabajo de diferentes actores europeos”.

También, estará el equipo español campeón del mundo en 2023, del ‘HackerOne AWC’.

Además de la sala plenaria, habrá otra dedicada a la ‘**Criptored Cybersecurity Conference**’, coordinada por **Alfonso Muñoz**, otra con foco en la Administración Pública, con la **Asociación ProtApp**, otra para la iniciativa **Securiters**, que gestionarán **Marta Barrio**, **Carolina Gómez** y **Mercedes Muñoz**, además

de otra a cargo de la asociación **Isaca**. En total, más de un centenar de expertos presentarán investigaciones novedosas sobre todo tipo de temas, desde la popular IA hasta hardware *hacking*,

forensia, vulnerabilidades, etc. También, se celebrará una ‘Hacker Night’, patrocinada por **Yogosha**, en la que medio centenar de especialistas en *bug bounty* pondrán a prueba su habilidad. A ello se sumarán, del 4 al 6 de marzo, sus talleres técnicos, los **BootCamp** y **RootedLab**, de 24 y ocho horas de duración, respectivamente, y que este año impartirán **E. Arriols**, **D. Meléndez**, **A. Sanz**, **R. Amado** y **J. M. Holguin**, y **C. Polop** y **P. Borda**.

Esta edición también acogerá un curioso concurso de composición musical, bajo el nombre ‘#hackthemusic’, apoyado por **Jorge Martínez**, con temas conocidos bajo su alias ‘@XTSK’, además de ser un reconocido hacker ético.

Por supuesto, el congreso volverá a contar con patrocinadores como **Tarlogic**, **CCN-Cert**, **Cipher** a **Prosegr company**, **S2 Grupo**, **ZeroLynx**, **S21sec**, **Palo Alto Networks**, **CrowdStrike**, **Telefónica Tech**, **Innotec Security (part of Accenture)**, **Outpost24**, **Factum** y **Synk**, entre otros.



Del 10 al 12 de abril, junto al MCCE, Incibe y Autoridad Nacional para la Innovación Gubernamental, sumándose RootedCON

Panamá, nueva cita de las jornadas anuales de las STIC en Iberoamérica

Las **IV Jornadas STIC** y el Congreso **RootedCON** Capítulo Panamá, bajo el lema ‘Gobernar y compartir, las claves del éxito en ciberseguridad’, sumarán fuerzas para ofrecer una nueva edición de esta cita iberoamericana, convertida ya en referencia. Este año se celebrará en el Centro de Convenciones de la capital, del 10 al 12 de abril. Y estará coordinada tanto por el **Centro Criptológico Nacional (CCN)**, como por el **Mando Conjunto del Ciberespacio (MCCE)**, el **Instituto Nacional de Ciberseguridad (Incibe)**, y

RootedCON, como representantes de España, y por la **Autoridad Nacional para la Innovación Gubernamental** de Panamá. Además, contarán con el apoyo institucional de la **Organización de Estados Americanos (OEA)**, la red **CSIRT Americas** y el **Banco Interamericano de Desarrollo**.

Se espera reunir a más de 4.000 profesionales de forma presencial y en línea, de más de 35 países, con el

fin de fortalecer las alianzas, promover el intercambio de conocimientos y afianzar la necesaria cooperación para una mejor defensa y protección del ciberespacio. A lo largo de tres días, los asistentes podrán asistir a conferencias magistrales, mesas redondas y ponencias centradas en aspectos como las ciberamenazas y tendencias, la gobernanza, el cibercrimen, la IA o las tecnologías emergentes.



El 17 y 18 de abril, en Madrid

@ASLAN 2024 hará foco en los retos y oportunidades de la IA aplicada a ciberprotección, nube y transformación digital

La **Asociación @aslan**, cuyo presidente es **Alberto Pascual** (Ingram Micro) que agrupa a 188 fabricantes y proveedores especializados en innovación digital y ciberprotección, organizará los 17 y 18 de abril, en el Palacio de Congresos de Madrid, la 31ª edición de su cita anual Congreso & EXPO ASLAN2024 bajo el lema ‘IA. Un gran avance en digitalización. Todo cambia’. “La irrupción de la IA está produciendo

grandes cambios en la industria de la innovación digital”, destacan los impulsores de esta cita que se centrará en seis temas claves: Retos y oportunidades en la aplicación de la IA a las infraestructuras digitales y ciberseguridad, empresas y servicios más competitivos apoyados en innovación digital, el canal de distribución TIC como palanca para avanzar en la



digitalización de la pyme, así como el reto de la modernización y digitalización de la AGE y la Administración Pública Territorial, la oportunidad de desarrollar la industria nacional de servicios gestionados de ciberseguridad y los centros de datos y conectividad, como oportunidad para consolidar Madrid y España como un *hub* digital para el sur de Europa.

Del 18 al 20 de junio, en Ávila

C1br3rWall 2024 homenajeará a Ángel Pablo Avilés ‘Angelucho’, bautizando con su nombre el auditorio principal de esta edición

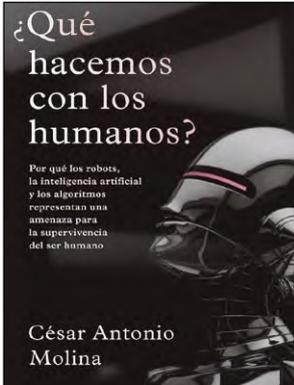
La IV edición del Congreso **C1br3rWall** con el lema ‘Inteligencia Segura’, organizado desde 2018 por la Policía Nacional, en las instalaciones de su Academia



de Ávila, rendirá un homenaje al guardia civil fallecido en 2023, Ángel Pablo Avilés, ‘Angelucho’, considerado uno de los grandes referentes en concienciación a familias y menores. Espera batir su récord de asistentes y ponentes –en la última edición contó con 230– que mostrarán investigaciones y formaciones de calidad en sus aulas y auditorio.

¿QUÉ HACEMOS CON LOS HUMANOS?

Por qué los robots, la IA y los algoritmos representan una amenaza para la supervivencia del ser humano



Autor: César Antonio Molina
Editorial: Deusto
Año: 2023 – 384 páginas
ISBN: 978-84-23436-32-3
www.planetadelibros.com

los cuales ya no podremos vivir?”. El polifacético y solvente **César Antonio Molina**, poeta, ensayista, periodista y, en su momento, ministro de Cultura, presenta una obra de obligada lectura en la que reflexiona sobre cómo los mayores desafíos contemporáneos no provienen únicamente de las graves crisis ambientales, las amenazas de las guerras nucleares o las olas de renovados autoritarismos, sino –y muy especialmente– de “la soberbia científica y el, hasta ahora, incontrolable desarrollo tecnológico en manos privadas desaprensivas”. Por ello, se pregunta y responde, con profundidad y calidad intelectual, si realmente estamos preparados para sobrevivir a la mayor revolución tecnológica de la historia, así como las diferentes opciones que podemos poner en marcha para preservar nuestra civilización, nuestra cultura, nuestras democracias, nuestras libertades y nuestro espíritu crítico. Absolutamente recomendable.

“¿Estamos a las puertas de un apocalipsis digital? ¿Perderá sentido o será sustituida o abolida definitivamente nuestra herencia espiritual acumulada a lo largo de milenios? ¿Estamos al final de nuestra civilización y desconocemos cómo será la que venga, así como el papel que tendremos en ella? ¿Nos conducen las nuevas tecnologías, los algoritmos y la inteligencia artificial a una especie de estado policial donde todos formaremos parte de una gran mente colectiva? ¿Dejaremos de actuar como individuos responsables y libres, esclavizados y vigilados por aparatos sin

HACKEA TU MENTE

Estrategias de crecimiento personal a partir de la filosofía hacker



Autor: Deepak Daswani
Editorial: Samarcanda
(Grupo Lantia Publishing)
Año: 2023 – 248 páginas
ISBN: 978-84-18720-58-1
editorialsamarcanda.com

encarar los desafíos de una vida donde la línea entre lo personal y lo profesional se desdibuja con cada clic, hasta acabar acercándonos a nuestras metas más deseadas de una manera tan eficaz como honesta y comprobable”.

Para ello, el libro se ofrece a modo de guía con consejos prácticos y ejemplos que permitan ir paso a paso a través de un viaje hacia “la superación personal, explorando la mejora de nuestras relaciones humanas, la humana aceptación de nuestras limitaciones y la maestría en el manejo de nuestras emociones”.

El conocido experto en ciberseguridad canario, **Deepak Daswani**, se atreve con un nuevo y original reto por la mirada con el que se aborda: “romper las barreras convencionales y proponer una odisea de autodescubrimiento inspirada en la filosofía hacker, tejida con los hilos de su brillante carrera”. Aunque la obra, según explica, no es “un elixir mágico para el éxito, la fama o la felicidad instantánea”, sí brinda “un compendio de estrategias y recursos para profundizar en el conocimiento de uno mismo y

Un conocimiento que se basa tanto en su experiencia personal y vital, como en un exhaustivo trabajo de investigación que confiere a este libro de “una autenticidad y credibilidad que te empujarán a alcanzar tus objetivos de una forma que nunca imaginaste”, resalta Daswani.

LA CIBERSEGURIDAD EN LA ERA DE LA INTELIGENCIA ARTIFICIAL



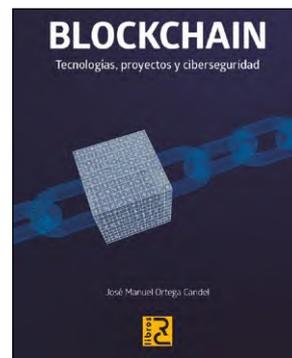
Coordinador: Basilio Ramírez Pascual
Editorial: La Ley
Año: 2023 – 504 páginas
ISBN: 978-84-19905-03-1
anayamultimedia.es

Ramírez, muestran el impacto y los cambios que está experimentando la ciberprotección mediante el uso intensivo de la IA en todo tipo de campos: desde la detección de amenazas avanzadas, hasta la automatización de la respuesta a incidentes. Por supuesto, también dedica varios apartados a los desafíos que plantea, entre otros, la amenaza de ataques con IA y la necesidad de abordar cuestiones éticas y de privacidad. Por ello, sus autores consideran que “la colaboración entre humanos y sistemas de IA es esencial para mantener seguros los entornos digitales en esta era”. En definitiva, una obra plural que recopila la visión, para legos y aficionados a las nuevas tecnologías, del impacto de la IA en la protección cibernética con un enfoque holístico.

“La IA comienza a tener un impacto significativo en la forma en que las organizaciones abordan la seguridad de la información y la protección contra amenazas cibernéticas”, destacan los autores de este volumen coral, que busca presentar la realidad actual del tejido empresarial frente a los retos de la ciberseguridad, con una mirada práctica y real. A través de sus diferentes aportaciones, reconocidos expertos como **Ana Isabel Corral García**, **Claudio Chifa**, **Nicolás Franco**, **Juan Carlos Galindo**, **Raúl Guillen**, **Manuel Huerta**, **Fernando Mairata** y **Javier Martín**, bajo la coordinación de **Basilio**

BLOCKCHAIN

Tecnologías, proyectos y ciberseguridad



Autor: José Manuel Ortega Candell
Editorial: Packt Publishing
Año: 2024 – 326 páginas
ISBN: 978-84-12546-76-7
<https://rclibros.es>

en este ámbito, incluido el de los diferentes algoritmos de consenso y qué aplicaciones prácticas tienen a través de los proyectos más notables que “están transformando la forma en que los usuarios interactúan y se relacionan con gobiernos y organizaciones”, destaca su autor.

Este libro nos sumerge en el fascinante mundo de la cadena de bloques, explorando sus aspectos técnicos fundamentales al mismo tiempo que examina los principales proyectos que tienen como base esta revolucionaria tecnología que está cambiando la manera en que las personas interactúan y se relacionan entre sí. A través de su contenido, el lector podrá comprender los aspectos esenciales de *blockchain*, desde sus conceptos básicos hasta su aplicación en diversos sectores, incluyendo las finanzas y las criptomonedas, alcanzando un conocimiento notable

Así, **José Manuel Ortega**, uno de los escritores técnicos españoles más prolíficos, explora también diversas aplicaciones de esta opción tecnológica, abarcando desde sistemas de votación hasta la automatización de acuerdos mediante contratos inteligentes, principales proyectos que se pueden encontrar dentro del ecosistema *crypto*. Finalmente, se estudia la ciberseguridad, analizando las amenazas que pueden producirse en estos entornos y cómo se podrían proteger los activos digitales de ellas.

AMAZON WEB SERVICES

Hardening de Infraestructuras Cloud Computing



Autor: Abraham Romero
Editorial: OxWord
Año: 2024 - 230 páginas
ISBN: 978-84-09539-84-0
www.oxword.com

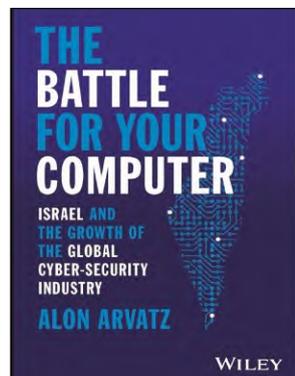
que se ofrecen a través de AWS, en computación, redes, almacenamiento y bases de datos. Por supuesto, incluye un capítulo muy extenso donde se analizan, de forma minuciosa, los diferentes mecanismos de protección frente a ataques, control de accesos, monitorización, conformidad...

Por ello se convierte en una obra imprescindible para los que quieran usar herramientas de AWS, en sus primeros pasos, creando infraestructura y aplicaciones en la nube, con alta escalabilidad, disponibilidad y seguridad. Y máxime cuando hay, en español, pocos libros tan especializados al respecto.

Con la profundidad habitual de su autor, ingeniero informático y máster en ciberseguridad por la Uned, este libro ofrece una visión técnica útil y de calidad como punto de partida para los que quieran adentrarse en la tecnología *cloud* o pretendan certificarse en la nube. A lo largo de sus capítulos se muestran desde conceptos básicos y ventajas de la nube frente al modelo tradicional, hasta los principales servicios

THE BATTLE FOR YOUR COMPUTER

Israel and the growth of the global cyber-security industry



Autor: Alon Arvatz
Editorial: Wiley
Año: 2023 - 378 páginas
ISBN: 978-13-94174-15-7
www.wiley.com

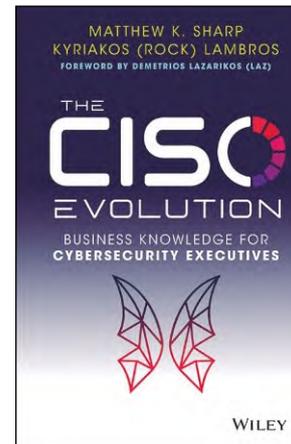
litar de referencia en este ámbito en una 'incubadora de tecnología' que ha permeado el mercado, con empresas como Palo Alto Networks o Check Point, entre otras muchas. No hay que olvidar, recuerda el libro, que, de los miles de millones de euros de capital riesgo que se invierten en ciberseguridad, el 40% son por parte de compañías de Israel.

Así, en este volumen, el lector encontrará desde interesantes curiosidades de qué tecnologías cibernéticas usadas en los hogares han partido del mundo militar, hasta cómo es el trabajo de los comandos cibernéticos del país o respuestas a preguntas como ¿qué criterios sigue una compañía cibernética ofensiva para decidir a quién vender su tecnología? Por ello, esta obra, según destaca su autor, es perfecta para "profesionales de la ciberseguridad que busquen comprender el mundo de riesgos, amenazas, oportunidades y trampas que definen el mundo de la ciberseguridad ofensiva y defensiva".

Interesante y original obra a cargo de uno de los grandes especialistas en guerra cibernética y ciberdefensa, **Alon Arvatz**. En ella, analiza el 'por qué' y el 'cómo' de la gran conexión que existe en Israel entre la unidad militar cibernética de élite del Ejército, la conocida como 'Unidad 8200' y la industria de ciberprotección ofensiva que cada vez cobra más protagonismo en el mercado. Para ello, no sólo repasa algunos de sus hitos, sino que además ofrece interesantes opiniones de los grandes expertos del sector nacional a través de entrevistas con profesionales y emprendedores que muestran el camino seguido por el país para convertir su unidad mi-

THE CISO EVOLUTION

Business Knowledge for Cybersecurity Executives



Autores: Matthew K. Sharp, Kyriakos Lambros
Editorial: Wiley
Año: 2024 - 415 páginas
ISBN: 978-11-19782-48-3
www.wiley.com

que experimentan los expertos en tecnología al hablar y hacer presentaciones ante ejecutivos, destacando que la ciberprotección siempre debe estar alineada con el negocio, por lo que debe generar "resultados comerciales significativos".

En definitiva, se trata de una obra para un perfil ejecutivo, cuya pretensión es contribuir a mejorar las habilidades 'blandas' para generar confianza entre la junta directiva, por parte de los CISO, "estableciendo adecuadamente las expectativas en torno al apetito por el riesgo y la asignación de capital". Por ello, es una buena novedad bibliográfica para profesionales de seguridad y riesgos, auditores de TI y administradores de riesgos que busquen cómo mejorar su comunicación interna, en los ámbitos que les conciernen.

Dos reconocidos expertos, Sharp y Lambros ofrecen en este libro un recurso práctico y revelador para ayudar a los profesionales de la ciberseguridad implicados a desarrollar las habilidades que necesitan para comunicarse de manera efectiva con la alta dirección y las juntas directivas. Para ello, emplean historias ilustrativas para mostrar a los profesionales cómo establecer una presencia ejecutiva y evitar los errores más comunes

TECNOLOGÍAS DISRUPTIVAS

Comprende las herramientas de la sociedad digital



Autores: Jorge S. Nolasco, Javier Gamboa, Jimmy S. Dextre, Luz E. Nolasco y Julio Palacios
Editorial: Ra-Ma
Año: 2024 - 400 páginas
ISBN: 978-84-19857-50-7
www.ra-ma.es

casos prácticos, cómo están impactando tecnologías como el *big data*, el *deep learning* -a través del procesamiento de Lenguaje Natural (NLP) y del *web scraping*, utilizado para extraer información de sitios web-, junto a la visión Artificial y procesamiento de imágenes, así como la criptografía, el *blockchain* y la ciberseguridad, aportando numerosos datos, enfoques y técnicas que se están utilizando para innovar en cada campo.

Además, el libro incluye un anexo que explica cómo usar el lenguaje de programación Python, a modo de guía, en entornos Windows, para aplicar, a través de proyectos sencillos, buena parte de los ejemplos descritos en el libro.

Las tecnologías disruptivas son aquellas que generan cambios significativos en la forma en que se realizan las actividades cotidianas, los procesos industriales o los modelos de negocio establecidos. Estas tecnologías tienen el potencial de transformar industrias enteras, alterar la forma en que interactuamos con el mundo y crear nuevas oportunidades y desafíos.

Por ello, los autores de esta obra coral, eminentemente técnica, se han centrado en explicar en profundidad, con abundantes

MorterueloCON X Edición

Organiza: Asociación MorterueloCon
 Fechas: 22/24-2-2024
 Lugar: Paraninfo Universidad de Castilla-La Mancha. Campus de Cuenca.
 Correo-e: contacto@morteruelo.net
 Sitio: morteruelo.net

Actividades CCI. Centro de Ciberseguridad Industrial

- **Máster profesional online en Ciberseguridad Industrial**, inicio 26 de febrero 2024.
- **Responsable de Ciberseguridad en IACS**, 4/7-3-2024
- **Ciberseguridad en el diseño, operación y mantenimiento industrial del sector agua**, 8/11-4-2024
- **Ciberseguridad en el diseño, operación y mantenimiento industrial del sector eléctrico**, 7/16-5-2024
 Organiza: Centro de Ciberseguridad Industrial-CCI.
 Tel.: 910 910 751
 Correo-e: info@cci-es.org
 Sitio: cci-es.org

RootedCON

Organiza: Asociación RootedCON
 Fechas: 7/9-3-2024
 Lugar: Kinépolis. Pozuelo de Alarcón. Madrid
 Correo-e: info@rootedcon.com
 Sitio: https://rootedcon.com

Espacio TISEC

- **A pleno SOC Centro de operaciones de ciberseguridad**
 Organiza: Revista SIC
 Fechas: 12/13-3-2024
 Lugar: Hotel Novotel Campo de las Naciones. Madrid.
 Tel.: 91 575 83 24
 Correo-e: info@codasic.com
 Sitio: revistasic.com/tisec

Ignite on tour

- **Cybersecurity for the AI Era**
 Organiza: Palo Alto Networks
 Fecha: 9-4-2024
 Lugar: Espacio Ventas. Madrid.
 Correo: igniteontour-emea@paloaltonetworks.com
 Sitio: register.paloaltonetworks.com/igniteontourmadrid24

IV Jornadas STIC & Congreso RootedCON

- **Capítulo Panamá**
 Organizan: CCN-CERT, Incibe, AIG-Panamá, RootedCon y ESPDEF-CERT
 Fechas: 10/12-4-2024
 Lugar: Ciudad de Panamá.
 Sitio: jornadas.ccn-cert.cni.es/es/ivjornada-panama

Congreso ASLAN 2024

Organiza: Asociación @ASLAN
 Fechas: 17/18-4-2024
 Lugar: Palacio de Congresos IFEMA. Madrid.
 Sitio: aslan.es

Barcelona Cybersecurity Congress

Organiza: Fira de Barcelona
 Fechas: 21/23-5-2024

Lugar: Fira de Barcelona-Gran Vía.
 Sitio: barcelonacybersecuritycongress.com

IV Congreso C1b3rWall Inteligencia Segura

Organiza: Policía Nacional
 Fechas: 18/20-6-2024
 Lugar: Escuela CNP. Avila.
 Sitio: c1b3rwall.policia.es

Espacio TISEC

- **Los ciberriesgos, en la encrucijada. El Ransomware tiene un precio.**
 Organiza: Revista SIC
 Fechas: 19/20-6-2024
 Lugar: Hotel Novotel Campo de las Naciones. Madrid.
 Tel.: 91 575 83 24
 Correo-e: info@codasic.com
 Sitio: revistasic.com/tisec

SECURMÁTICA 2024

Organiza: Revista SIC
 Fechas: 8/10-10-2024
 Lugar: Hotel Novotel Campo de las Naciones. Madrid.
 Tel.: 91 575 83 24
 Correo-e: info@securmatica.com
 Sitio: securmatica.com

Identi::SIC

- **Identidad digital: cebo y salvoconducto**
 Organiza: Revista SIC
 Fechas: 20/21-11-2024
 Lugar: Hotel Novotel Campo de las Naciones. Madrid.
 Tel.: 91 575 83 24
 Correo-e: info@codasic.com
 Sitio: revistasic.com/identisic

FORMACIÓN CONTINUA

AENOR

Tel.: 91 432 61 25
 Sitio: aenorciberseguridad.com

ES-CIBER, Escuela Superior de Ciberseguridad

Correo-e: info@es-ciber.com
 Sitio: es-ciber.com

Exclusive Networks

Tel.: 91 197 66 01
 Sitio: training.exclusive-networks.com/es-ES

M2i

Tel.: 91 578 23 57
 Correo-e: info@m2iformacion.com
 Sitio: m2iformacion.com

SANS INSTITUTE

Organiza: One eSecurity
 Lugar: Madrid
 Tel.: 911 011 000
 Correo-e: sans@one-esecurity.com
 Sitio: one-esecurity.com/events_training.html

Westcon-Comstor

Tel.: 91 419 61 00
 Correo-e: academy.es@westcon.com
 Sitio: https://academy.westconcomstor.com/es

INDICE DE ANUNCIANTES

EMPRESA	PAG.	EMPRESA	PAG.	EMPRESA	PAG.
A3SEC	83	EY	19	PWC	15
ADVENS	21	FACTUM	79	RECORDED FUTURE	67
AENOR	59	FASTLY	177	ROOTED CON	109
AIUKEN	57	FUJITSU	75	S2 GRUPO	35
AKAMAI	45	GHENOVA	61	S21SEC	101
ALL4SEC	95	GMV	43	SECURMÁTICA	CONTRAPORTADA
ASLAN	55	HORNETSECURITY	85	SOPHOS	93
AUTEK	37	IDENTISIC	11	STORMSHIELD	97
BARRACUDA	73	INNOTECH SECURITY, PART OF ACCENTURE	13	SUSE	175
BOTECH	53	JORNADAS STIC CCN	49	TARLOGIC	23
CEFIROS	69	KASPERSKY	51	TEHTRIS	63
CHECK POINT	6	LEET SECURITY	89	THALES	171
CIPHER	99	SECURMÁTICA	65	TISEC A PLENO SOC	4
CISCO	165	MDTEL	87	TISEC RANSOMWARE	9
CROWDSTRIKE	33	MNEMO	27	V-VALLEY	2-3
CYBER GURU	81	NCC GROUP	31	WESTCON	47
CYBERPROOF-UST	41	NETSKOPE	103	WISE SECURITY	91
DXC	39	NOVARED	161	ZEROLYNX	29
ENTHEC	169	ONE ESECURITY	203	ZSCALER	167
ES-CIBER	17	ONESEQ	71		
EXCLUSIVE NETWORKS	25	ONTINET ESET	173		



Readiness · Detection · Response



¿Preparado para afrontar un ciberataque?
Confía en los mejores expertos

Readiness



Cyber Consulting (CyCon)



Cyber Exercises (CybEx)



Cyber Insurance (Cybins)



Cyber Threat Intelligence

Detection Response



Deception



Threat Hunting (TH)



Emergency Incident Response (EIR)



Compromise Assessment



Managed Threat Hunting (MTH)



Digital Forensics (DFIR)

Detection & Response



Managed Detection and Response

SECURMÁTICA²⁰²⁴

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

Manos a la obra...



... y bien acompañados

Organiza

Revista **SIC**

8 · 9 · 10 OCTUBRE

www.securmatica.com