Nº 156 Septiembre 2023 – Año XXXII

SiC

www.revistasic.com

Revista
Ciberseguridad, seguridad de la información y privacidad

¡Ya llega!

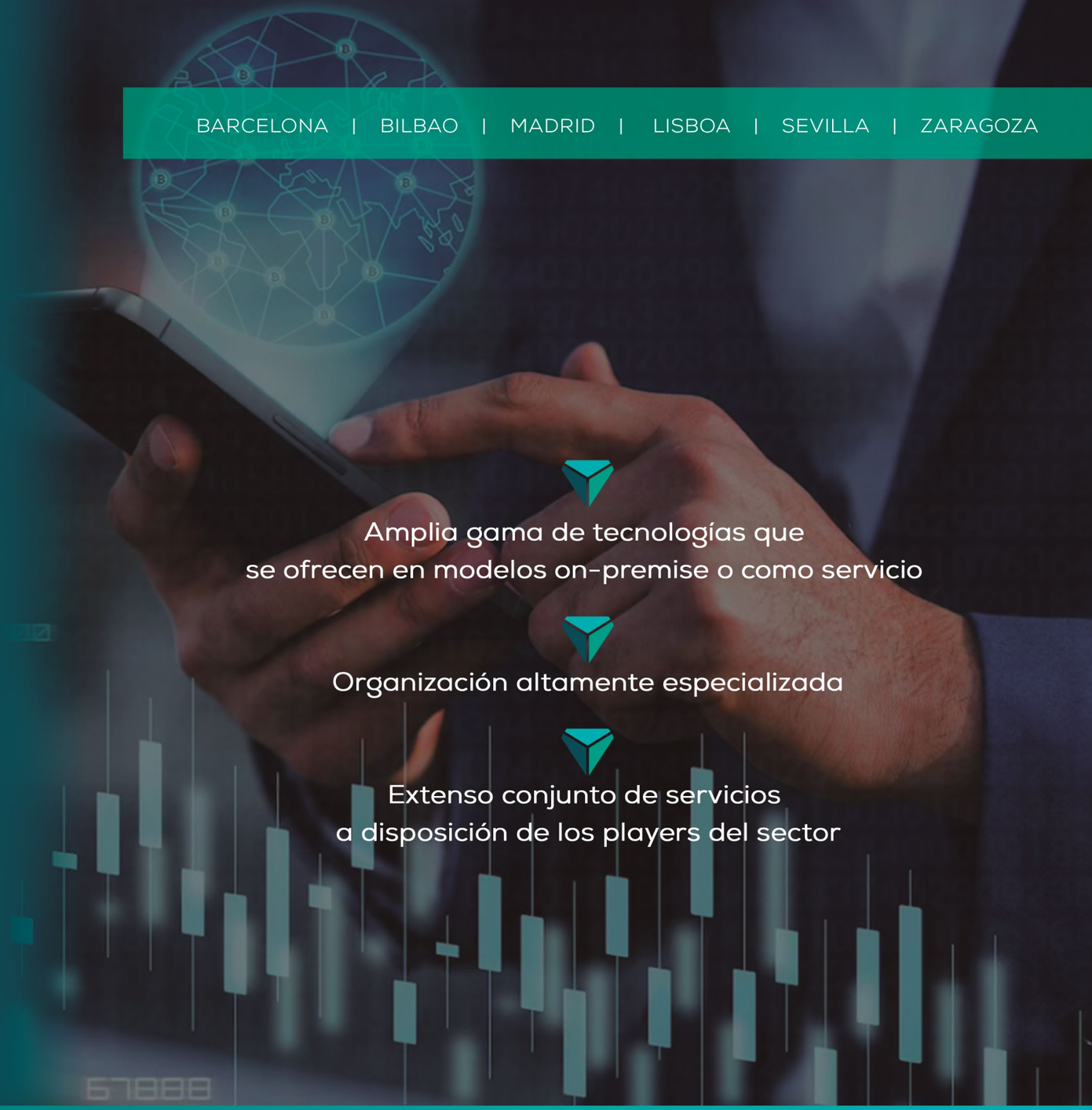
SECURMÁTICA 2023

V-Valley
enhancing your business

ESPECIALISTAS EN ADVANCED SOLUTIONS

Mayor rentabilidad y valor en tus proyectos de Ciberseguridad Corporativa

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



BARCELONA | BILBAO | MADRID | LISBOA | SEVILLA | ZARAGOZA

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 | Workplace | Aplicación | Dato | Gestión

A10 · BACKBOX · CVU · BROADCOM · CHECK POINT · CLOUDFLARE · CounterCraft · CyberRes · ENTRUST · ravenloop · kaspersky · McAfee · SONICWALL · MICRO FOCUS is now opentext · Trellix · Skyhigh Security · TREND MICRO · WatchGuard · XM Cyber

www.v-valley.es

seguridad@v-valley.com

Identi::SiC

Organiza:

Revista SiC

www.revistasic.com/identisic

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

Nº 156 Septiembre 2023 – Año XXXII

SiC

DOCUMENTOS

www.revistasic.com

Revista

Ciberseguridad, seguridad de la información y privacidad

ENTREVISTA

Iván Sánchez
CISO Global
BUPA

ENTREVISTA

Enrique Cubeiro
Director
GHENOVA
CIBERSEGURIDAD

PROYECTOS
SEC2GRID

INTERCAMBIO
Red Nacional de SOC

EN CONSTRUCCIÓN
European Fashion Victims

INFRAESTRUCTURAS
Profundizando en DevSecOps

¡Ya llega!

SECURMÁTICA 2023

YOU DESERVE THE BEST SECURITY

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

Quantum
Secure the Network

Harmony
Secure Users & Access

CloudGuard
Secure the Cloud

CHECK POINT™

MÁS INFORMACIÓN: www.checkpoint.com/es

info_iberia@checkpoint.com

SiC
Nº 156
Septiembre 2023

>> Sumario

>> en este número

DOCUMENTOS

SiC

• Securmática 2023, a punto. Las mañanas de los días 3, 4 y 5 de octubre tendrá lugar en Madrid la XXXIII edición de este congreso, en el que los responsables de seguridad de la información y otros directivos de grandes compañías y entidades públicas, conjuntamente con sus colaboradores externos, van a presentar iniciativas y proyectos de valor en diversas áreas de la gestión de la ciberseguridad.

El enfoque dado por DORA a la ciberseguridad en el sector financiero, enmarcado en el objetivo de este Reglamento, que no es otro que el de la resiliencia operativa, está potenciando tanto las actividades de operación como las de revisión de controles, al tiempo que ayudando a afinar en la calidad y eficacia de la ciberseguridad como servicio, de los programas de concienciación, una mayor atención corporativa para minimizar la posibilidad de fugas de información, la potenciación de la respuesta ante incidentes, el fortalecimiento de los sistemas de gestión de identidades, la consolidación en un solo SOC de varios SOC tras la realización de absorciones y fusiones empresariales, la protección de plataformas de datos y sistemas de IA corporativos, la incorporación de ciberseguridad en áreas no TIC, el incremento de inteligencia frente al fraude, los primeros esquemas de protección conjunta de empresas y sus cadenas de suministro…

La realidad de NIS2 (directiva todavía no traspuesta a la legislación española), también se verá reflejada en los proyectos que se presentarán fuera del entorno del ámbito financiero (especialmente bancario), puesto que Securmática es una cita profesional intersectorial.

En páginas interiores de esta edición encontrará el lector un avance del programa para que pueda mensurar las temáticas, alcance y organizaciones que este año han considerado procedente realizar aportaciones.

• AESIA. En el BOE de 2 de septiembre del presente vio la luz el Real Decreto 729/2023, de 22 de agosto, de aprobación del Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial. Esta Agencia Estatal, adscrita al ministerio de Asuntos Económicos y Transformación Digital, tendrá su sede institucional en A Coruña, y su "efectiva puesta en funcionamiento… se producirá con la constitución del Consejo Rector en el plazo máximo de tres meses desde la entrada en vigor…" del mencionado Real Decreto. Como la pieza legal entró en vigor el 3 de septiembre, ya puede ponerle el lector fecha al acontecimiento, si las cosas van según lo previsto.

Esta entidad de derecho público se estructura en base a dos órganos de gobierno: la Presidencia (la ostentará la persona titular de la SEDIA) y el Consejo Rector (del que dependerá la Comisión de Control); y cuatro órganos ejecutivos: la Dirección, la Secretaría General, la Subdirección de Informes e Infraestructuras de Prueba, y la Subdirección de Certificación, Evaluación de Tendencias, Coordinación y Formación en inteligencia artificial.

Las competencias de AESIA se incardinan con el ecosistema IA de la UE. Y en el caso específico de la supervisión de los sistemas de IA, a los efectos de garantizar el cumplimiento de la normativa española y europea en la materia, tendrá capacidades sancionadoras.

Será interesante ver cómo AESIA enfoca la gestión de la ciberseguridad de los sistemas de IA y la protección de datos personales, y qué sinergias pudieran aparecer con la AEPD y con las estructuras de la ciberseguridad españolas, incluidas, claro está, las propias del ministerio de Defensa. Además, el desarrollo y puesta en operación de sistemas de IA o la entrada de sistemas de IA en tratamientos implantados en servicios TIC, sujetos a DORA y NIS2, seguramente abrirá un fecundo espacio de discusión al que no será ajeno el mundo del cumplimiento y la siempre atenta delincuencia.

Edita: Ediciones CODA, S.L. Goya, 39. 28001 Madrid (España) Tels.: 91 575 83 24 / 25 Fax: 91 577 70 47 **Correo-e:** info@revistasic.com www.revistasic.com **Editor:** Luis Fernández Delgado **Director:** José de la Peña Muñoz **Redacción:** Ana Adeva, José Manuel Vera **Sección Laboratorio SIC:** Javier Areitio Bertolín **Colaboran en este número:** Manuel Achaques, Javier Blanco, Carlos Córdoba, Jorge Dávila, Ricardo escrivá, Gonzalo Gómez-Abad, Lola Miravet, Ángel Ortiz, Álejandro Pérez, Javier Pérez, Adrián Sanz, César Tascón **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

Soluciones de Seguridad de Negocio

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

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

Juntos, podemos construir una sociedad digital más segura.

www.pwc.es/bss

pwc

CISOs y DPOs: el abrazo de la IA

José de la Peña Muñoz
Director
jpm@codasic.com

Hay que desterrar de nuestras vidas la tentación de dejarnos vencer por la vorágine digital transformadora con la que la degenerada mercadotecnia, dirigida por recolectores banales de parné está incrustándose en el devenir de todos los sectores productivos, particularmente el de TIC y aledaños.

Los tópicos o confusiones con los que habilísimos enterados están tratando asuntos de ciberseguridad causan sonrojo. Y lo más preocupante es que algunos profesionales del mundillo empiezan a no saber (o no querer) distinguir el polvo de la paja, hecho que achacaremos al tremendo desgaste neuronal que lleva asociada la gestión de riesgos, y que conduce a estados agudos de sisifismo.

> Gestionar la ciberseguridad de los sistemas de IA y garantizar el derecho a la protección de datos y la privacidad van a requerir la estrechísima colaboración de CISOs y DPOs

"Bien, De la Peña", dirá usted, lector; "sea más concreto, porque en sus dos párrafos anteriores cabe casi todo". Vamos a ello.

Hay parcelas del asesoramiento externo en las que lo dicho acontece de forma notoria. DORA es un ejemplo. Ciertas conferencias sobre este Reglamento que he escuchado en tales o cuales foros, me llevaron a la náusea. Se notaba que los conferenciantes charlatanes, ni sabían los precedentes de la norma, ni lo que es la resiliencia operativa, ni el papel de la ciberseguridad en el contexto, ni la visión sectorial (clientes y proveedores).

Y algo así pasa con la todavía no traspuesta NIS2. Hay especialistas, empeñados en llevarnos por la senda del cumplimiento, que tienen una empanada mental con lo que hay que entender por una infraestructura crítica y por un servicio esencial. Creen que son lo mismo. Incluso cuando les he preguntado sobre posibles conflictos entre DORA, NIS2 y CER, han salido por peteneras: que si la NIST, que si la ISO 27001... ¡Alucinante! Si me hubieran contestado que era demasiado pronto para identificar posibles escenarios de tensión en la aplicación de estas piezas, les hubiera reconocido un punto estándar de picardía. Pero no cayó esa breva. Lo más descorazonador es que este es el nivel de competencia técnica al que tiende hoy ese pequeño rebaño de neoconsultores tóxicos. Como crecerá, los que conformamos el creciente gremio de la ciberseguridad tendremos que extremar la exigencia, más todavía cuando los consejos de administración y los órganos de dirección empiezan a entender de la cosa.

Imparable

Pero la palma en la degeneración mercadotécnica, informativa y formativa, ya en los terrenos específicos ya en los generales, se la lleva la inteligencia artificial, ganando incluso a la computación cuántica. Todo el mundo habla de algoritmos, de IA generativa... Y en algunas secciones de medios de comunicación se nos da noticia de Robots casi antropomorfos en los que supuestamente se han integrado algoritmos de IA y que sirven copas mejor que un camarero humano. Por este orden.

Cierto es que el momento que viven la Informática y las Telecomunicaciones permite vislumbrar el papel creciente de la IA en todo lo que se menea. Y por eso hemos criado estructuras de promoción, ordenación, supervisión y sanción en la UE sobre sistemas de IA. En España ya tenemos la Agencia Española de Supervisión de Inteligencia Artificial, AESIA. Y va a tener trabajo, porque los nuevos sistemas de IA, juntos o acompañados, incorporados en servicios públicos, privados o a la vez, trabajando con tecnologías de analítica de datos y reconocimiento, luchando contra el fraude,... deberán desarrollarse, implantarse y usarse en base a ciertos requisitos legales y éticos, porque van a afectar, entre otros, a los derechos a la protección de datos personales y a la privacidad, como bien ha manifestado recientemente **Leonardo Cervera-Navas**, flamante Secretario General del Supervisor Europeo de Protección de Datos, EDPS.

Y que no se nos olvide, aunque sea obvio: habrá que gestionar la ciberseguridad de los sistemas de IA. Un buen escenario para que DPOs y CISOs se entiendan bien. ●

¿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

Luis Fernández Delgado
Editor
lfernandez@codasic.com

13, RUE DEL CIBERCEBE

Qué le vamos a hacer. De siempre me gustaron las historias ilustradas: desde los tebeos infantiles a las revistas de superhazañas pasando por los cómics de autor. Me dejaron un poso muy potente y por ello, al conocer que en este verano nos había dejado el creador de tanto personaje mítico, mi admirado **Francisco Ibáñez**, no he podido por menos que desear rendirle en esta tribuna un respetuoso –y, si se me permite, pelín desenfadado– homenaje.

En su babeliano edificio deambularían febrilmente los expertos de la T.I.A. (Técnicos de Investigación Aerociberespacial), C.C.N. (Clan Criptocuántico Nacional), CE.CI.NA. (Centinela de Ciberprotección Nativa), M.C.C.E. (Movimiento Coordinado de Ciberserviolas Estelares), D.S.N. (Departamento de Sincronización Neointegral), USMS (Uotroesemese), RootedKONG, IsaKA, ZZI y demás actores de peso en incansable actitud de cumplimiento del deber.

Como decía, del noveno arte me gusta todo, destacando singularmente los superhéroes. Especialmente quienes tienen el superpoder de crearlos. Y sí, uno de mis preferidos es el mentado: tenía gafotas, era calvo y, de siempre, me pareció un señor mayor. Y encima, en lugar de ser un exótico gringo, era de por aquí, un españolito de a pie. En julio murió y con él muchos de mis sueños de infancia se sumieron en la tristeza por la pérdida irreparable de un mayúsculo ser talentoso.

Para los leídos (mayormente analógicos), desde hace seis décadas su herencia gráfica ha sido sencillamente colosal. Sus escenarios gráficos desternillantes, sus ocurrentes guiones y, cómo no, una retahíla antológica de personajes inolvidables (Mortadelo y Filemón, Pepe Gotera y Otilio, Rompetechos…) conforman un legado deslumbrante.

Por ello, parafraseando ejemplos de su universo creativo, deseo desenfadadamente trasladarlos a ese otro que nos es tan familiar, en el que cohabitamos no pocos venturosos y paranoicos: Ciberseguridandia, y que para el caso lo vamos a rebautizar, parafraseándolo, como su obra coral más mítica: **13, Rue del Cibercebe**.

En su babeliano edificio (pisos, terrazas, balcones, azotea, portal, ascensor, alcantarillas, aledaños…) el maestro Ibáñez lo poblaría de inquilinos de la farándula actoral pública y privada, febrilmente atareados en dotar de resiliencia digital a sus ciberurbanitas. Por el inmueble deambularían los expertos de la **T.I.A.** (Técnicos de Investigación Aerociberespacial), **C.C.N.** (Clan Criptocuántico Nacional), **CE.CI.NA.** (Centinela de Ciberprotección Nativa), **M.C.C.E.** (Movimiento Coordinado de Ciberserviolas Estelares), **D.S.N.** (Departamento de Sincronización Neointegral), **USMS** (Uotroesemese), **RootedKONG, IsaKA**, **ZZI** y demás actores de peso en incansable actitud de cumplimiento del deber.

También habría dependencias y jocosas viñetas para reflejar las andanzas y avatares heroicos del tándem estelar del ecosistema ciber: nuestros flamantes CISOs y hackers, los cuales, aún a dia de hoy, batallan por ser reconocidos en sus respectivos frentes, tan ásperos ellos: la renuente alta dirección y la tierra de nadie digital. Quizá hasta uno de los pisos alojaría toda suerte de caricaturizadas estrellas de la longeva Securmática, primerísimas calidades entre tanta cursilería y tertulianez vacua.

Lógicamente, en varios de sus otros pisos también se asentaría una abundante retahíla de provedores de megalofareguoles y demás artefactos, no pocos de ellos con IApacidades repeledoras *next generation*. Y por supuesto andaríamos por ahí los de **S.I.C.** (Sindicadura para la Información Cibernética).

Como empecé, termino. Trato de imaginar cómo Ibáñez inventaría hoy, ya en su paradero celestial, un nuevo personaje y me viene a la cabeza que a buen seguro dibujaría un ser fofete de atuendo con mucha 'pegada': capa y calzón toronchados y malla enfundada de rabioso verde guardia civil, blandiendo una superarma letal: el sulfato cibernético, siempre pulverizando el ciberespacio con concienciación virtual y disuadiendo a la chusma de la comisión de fechorías a indefensos. Su apodo sería **Súper Lucho**. Y tendría alas. ●

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

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

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

EY
Building a better working world

Europa

Buscará mejorar la protección de los organismos e instituciones europeas estableciendo una dirección estratégica

La UE pondrá en marcha nuevas medidas reforzando su CERT y creando el Consejo Interinstitucional de Ciberseguridad

La presidencia del **Consejo** y los negociadores del **Parlamento Europeo** llegaron a un acuerdo provisional sobre un reglamento destinado a establecer un alto nivel común de ciberseguridad en todas las instituciones, órganos, oficinas y agencias de la UE. La Comisión propuso las medidas en marzo de 2022 en el contexto de un aumento significativo en el número de ciberataques sofisticados, que afectaron a la administración pública de la UE en los últimos años. El nuevo reglamento creará por ello un marco común y mejorará su resiliencia y capacidades de respuesta ante incidentes.

En concreto, en todas las instituciones, organismos, oficinas y agencias de la UE, las nuevas reglas les exigen establecer un marco de gobernanza, gestión de riesgos y control en el área de la ciberprotección.

Todas las entidades de la UE también deberán implementar medidas que aborden los riesgos identificados, realizar evaluaciones regulares de madurez y poner en marcha un plan de ciberseguridad.

Más peso del CERT

Además, en virtud del nuevo reglamento, se reforzará el mandato del Equipo de Respuesta a Emergencias Informáticas de la UE (**CERT-EU**), que pasará a llamarse '**Servicio de Ciberseguridad para las instituciones, órganos, oficinas y agencias de la Unión**', manteniendo el acrónimo actual. Asímismo, CERT-EU asesorará a todas las instituciones, órganos, oficinas y agencias de la UE y les ayudará a prevenir, detectar y responder a incidentes. También, actuará como un centro para el intercambio de información y la coordinación sobre ciberseguridad y respuesta a incidentes. Todas las entidades de la UE deberán compartir información no clasificada relacionada con incidentes con CERT-EU sin demora indebida.

Consejo Interinstitucional

La nueva regulación establecerá, asimismo, el **Consejo Interinstitucional de Ciberseguridad** (IICB) para impulsar y monitorizar la implementación de la regulación. Este órgano también supervisará la implementación de las prioridades y objetivos generales del CERT-EU y le proporcionará una dirección estratégica. Estará compuesto por representantes de todas las instituciones y órganos consultivos de la UE, el **Banco Europeo de Inversiones**, el **Centro Europeo de Competencia en Ciberseguridad**, la **Agencia de Ciberseguridad de la Unión Europea** (Enisa), el **Supervisor Europeo de Protección de Datos,** la **Agencia de la UE para el Programa Espacial**, así como representantes de la **Red de Agencias de la UE**.

Tras este acuerdo, se enviará el texto a los embajadores de la UE de los estados miembro para su confirmación y una vez hecha, el Parlamento y el Consejo lo aprobarán.

EN BREVE

El CENTRO DE POLÍTICA EUROPEA pide a la UE más esfuerzos para hacer frente a las amenazas cuánticas

El **Centro de Política Europea** (EPC), un grupo de expertos con sede en Bruselas, ha publicado un documento en el que propone una estrategia de ciberseguridad y alerta de que la UE debe incrementar sus esfuerzos para anticiparse a los posibles ataques cuánticos contra el cifrado que puedan realizarse en el futuro. Se trata de un informe fruto de la reflexión diferentes expertos de la industria y el mundo de la investigación que "ofrece recomendaciones para poner en marcha políticas que permitan mitigar el impacto de las amenazas cibernéticas creadas por la llegada de una computadora cuántica criptográficamente significativa", ha destacado la autora del documento, **Andrea Rodríguez,** analista jefe en EPC. Además, ha subrayado que la UE puede desempeñar un papel fundamental "al compartir información y mejores prácticas y alcanzar un enfoque común para la transición cuántica", entre los estados miembros.

También, recuerda que la estrategia del cibercrimen y los ataques patrocinados por los estados pasan por el enfoque 'descargar ahora, descifrar más tarde', con la idea de que, en un plazo estimado de siete años, la información robada podrá leerse gracias a la tecnología cuántica.

Frente a ello, el documento plantea seis recomendaciones: establecer un plan de acción coordinado de la UE sobre la transición cuántica, crear un nuevo grupo de expertos dentro de Enisa, con expertos nacionales adscritos, para intercambiar buenas prácticas e identificar obstáculos para la transición al cifrado poscuántico, marcar prioridades para la transición a él e impulsar la agilidad criptográfica para responder a las vulnerabilidades emergentes, facilitar la coordinación política entre la Comisión, los países, las agencias de seguridad nacional y Enisa, así como impulsar la coordinación técnica en la UE en este ámbito, para abordar las lagunas de investigación en tecnologías cuánticas seguras y explorar el uso de *sandboxes* para acelerar el desarrollo de aplicaciones a corto plazo de tecnologías de información cuántica.

nccgroup

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 suscríbase ya.

+34 663 967 328 www.nccgroup.com/es

Europa

EN BREVE

La COMISIÓN presenta su estrategia para liderar la Web 4.0 y los mundos virtuales

Las perspectivas de la economía de la UE más allá de 2030, publicadas en marzo, destacan la digitalización como uno de sus impulsores clave y la Web 4.0 como una transición tecnológica importante que brinda un mundo inmersivo, inteligente e interconectado. Se estima que el tamaño del mercado global de mundos virtuales crecerá de 27.000 millones de euros, en 2022, a más de 800.000 millones, en 2030. Los mundos virtuales afectarán la forma en que las personas viven juntas, brindando tanto oportunidades como riesgos que deben abordarse.

Por ello, durante el verano, la Comisión adoptó una nueva estrategia sobre la Web 4.0 y los mundos virtuales para dirigir la próxima transición tecnológica y salvaguardar un entorno digital abierto, seguro, fiable, justo e inclusivo para los ciudadanos, las empresas y las entidades públicas de la UE.

Pilares clave

La estrategia está en línea con los objetivos para 2030 del programa de políticas de la Década Digital y tres de sus pilares clave de digitalización: habilidades, negocios y servicios públicos. El cuarto pilar, las infraestructuras, se aborda en el paquete de conectividad de la Comisión y sus esfuerzos más amplios en capacidades informáticas, en la nube y de borde (*edge*). También, aborda la apertura y la gobernanza global de los mundos virtuales y la Web 4.0 como líneas de acción específicas.

De hecho, la UE ya está invirtiendo en importantes iniciativas en este ámbito como **Destination Earth** (DestinE), **Local Digital Twins,** para comunidades inteligentes, o **European Digital Twin of the Ocean**.

Aprobada, tras muchos meses de negociaciones, la nueva normativa para el intercambio de datos UE-EE.UU.

La **Comisión Europea** ha adoptado oficialmente el marco de privacidad de datos transatlánticos UE-EE.UU., que permitirá el libre flujo de datos comerciales entre Europa y los Estados Unidos. El órgano ejecutivo de Europa aprobó en diciembre un proyecto de decisión sobre el marco y el lunes, la Comisión anunció la adopción formal del marco, allanando el camino para su implementación.

Con él, las empresas estadounidenses que operan en Europa podrán transferir y procesar datos de ciudadanos de la UE en los EE.UU. Este acuerdo es el resultado de casi dos años de negociaciones entre Bruselas y Washington, y cuenta con varios compromisos clave de los EE.UU., incluida la promesa de mantener la recopilación de inteligencia sobre los europeos proporcional a la seguridad nacional. El **Departamento de Justicia** de los EE.UU. también acordó revisar las afirmaciones europeas de que las agencias de inteligencia estadounidenses habían recopilado información personal de manera incorrecta.

A pesar de las garantías de privacidad, el marco ha sido criticado por la **Junta Europea de Protección de Datos** por falta de claridad sobre los aspectos clave que rigen su implementación. Entrará en vigor en diciembre y estará sujeto a una revisión anual.

La UE y COREA DEL SUR firman un acuerdo para semiconductores y redes 5G y 6G

La **Unión Europea** y la **República de Corea del Sur** celebraron en verano la primera reunión del consejo de la Asociación Digital en Seúl (República de Corea). Fue copresidido por el comisario de Mercado Interior europeo, **Thierry Breton**, y el ministro coreano de Ciencia y TIC, **Lee Jong-Ho.**

Con ocasión de la reunión ministerial, la UE y la República de Corea han acordado colaborar en materia de semiconductores, informática de alto rendimiento y tecnología cuántica, redes 5G y posteriores, economía de plataformas, inteligencia artificial (IA) y ciberseguridad.

Además, se han comprometido a cooperar en materia de nuevas tecnologías recientemente presentadas que son fundamentales en la estrategia de seguridad económica de la UE. También, se ha aprobado crear un Foro UE-República de Corea del Sur de Investigadores en Semiconductores, que tendrá por objeto la investigación en ámbitos complementarios.

Ambos socios definirán una visión común sobre las redes 6G, aprovechando su liderazgo en las tecnologías 5G. También intensificarán la cooperación en torno a la IA y entablarán un diálogo permanente para facilitar una actualización periódica por cada parte de las iniciativas en pro de una IA fiable, concretamente sobre grandes modelos de IA generativa, y apoyarán planteamientos comunes en los organismos internacionales de normalización relacionados con la IA.

Además, acordaron intercambiar información sobre la cadena de suministro de semiconductores y ampliar su cooperación en el futuro en lo que respecta a las conexiones de infraestructura de conectividad digital segura, incluidos los cables submarinos, las capacidades digitales y el desarrollo de capacidades, y el intercambio de mejores prácticas en materia de empresas emergentes del sector digital. La próxima reunión del consejo de la Asociación Digital está prevista para principios de 2024, en Bruselas.

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

230720 ES [PC]

EE.UU.

También se han publicado sus prioridades de inversión y se ha aprobado el borrador de su 'Ley de ciberconcienciación'

La 'Administración Biden' pone en marcha un plan de implementación de su estrategia para "un ciberespacio más resistente, equitativo y defendible"

El presidente de EE.UU. **Joe Biden** ha dejado en claro, en numerosas ocasiones, que "todos los estadounidenses merecen todos los beneficios y el potencial de nuestro futuro digital". Fruto de ello, su Estrategia Nacional de Ciberseguridad publicada a mediados de año exige dos cambios fundamentales en la forma en que EE.UU. asigna funciones, responsabilidades y recursos en el ciberespacio: por un lado, garantizar que las entidades más grandes, más capaces y mejor posicionadas en los sectores público y privado, asuman una mayor parte de la carga para mitigar el riesgo cibernético. Por otro, aumentar los incentivos para favorecer las inversiones a largo plazo en ciberseguridad.

Así, en su afán de fortalecer las capacidades cibernéticas nacionales, la Casa Blanca presentó en verano el **Plan Nacional de Implementación de la Estrategia de Ciberseguridad** (NCSIP). Entre sus aspectos más destacados, intentará poner en marcha estándares mínimos de seguridad, sobre todo para las infraestructuras críticas, y, también, para mejorar la protección de las empresas y entidades con menos recursos, por ejemplo, apostando por la nube.

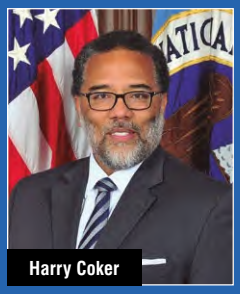
El Plan se basa en los principios marcados por la Estrategia: la defensa de la infraestructura crítica, actualizando el Plan Nacional de Respuesta a ciberincidentes; una apuesta firme por la interrupción y desmantelamiento de actores de amenazas combatiendo, especialmente, el *ransomware;* dar forma a las 'fuerzas del mercado' impulsando la seguridad y la resiliencia; disponer de mayor transparencia de la seguridad del software para "comprender mejor el riesgo de su cadena de suministro y responsabilizar a sus proveedores por las prácticas de desarrollo seguras"; invertir en un futuro más resiliente a través del impulso de estándares; e impulsar una Estrategia Internacional de Política Digital y Ciberespacio, en la que ya trabaja el **Departamento de Estado** y que publicará lo antes posible.

65 medidas

Todo ello se plasma en más de 65 iniciativas federales de alto impacto, desde la protección de los empleos estadounidenses

mediante la lucha contra los delitos cibernéticos, hasta la creación de una fuerza laboral capacitada, equipada para sobresalir en una economía cada vez más digital.

"Cada iniciativa del NCSIP se asigna a una agencia responsable y tiene un cronograma para su finalización. Algunas, como la emisión de las Prioridades de seguridad cibernética de la Administración para el presupuesto del año fiscal 2025, se completaron antes de lo previsto. Otras actividades completadas, como la transmisión al Congreso de la 'Estrategia Cibernética 2023', del **Departamento de Defensa,** el 26 de mayo, y la creación el 20 de junio de una 'Sección Cibernética de Seguridad Nacional' por parte del **Departamento de Justicia,** son hitos clave para completar las iniciativas.



Harry Coker

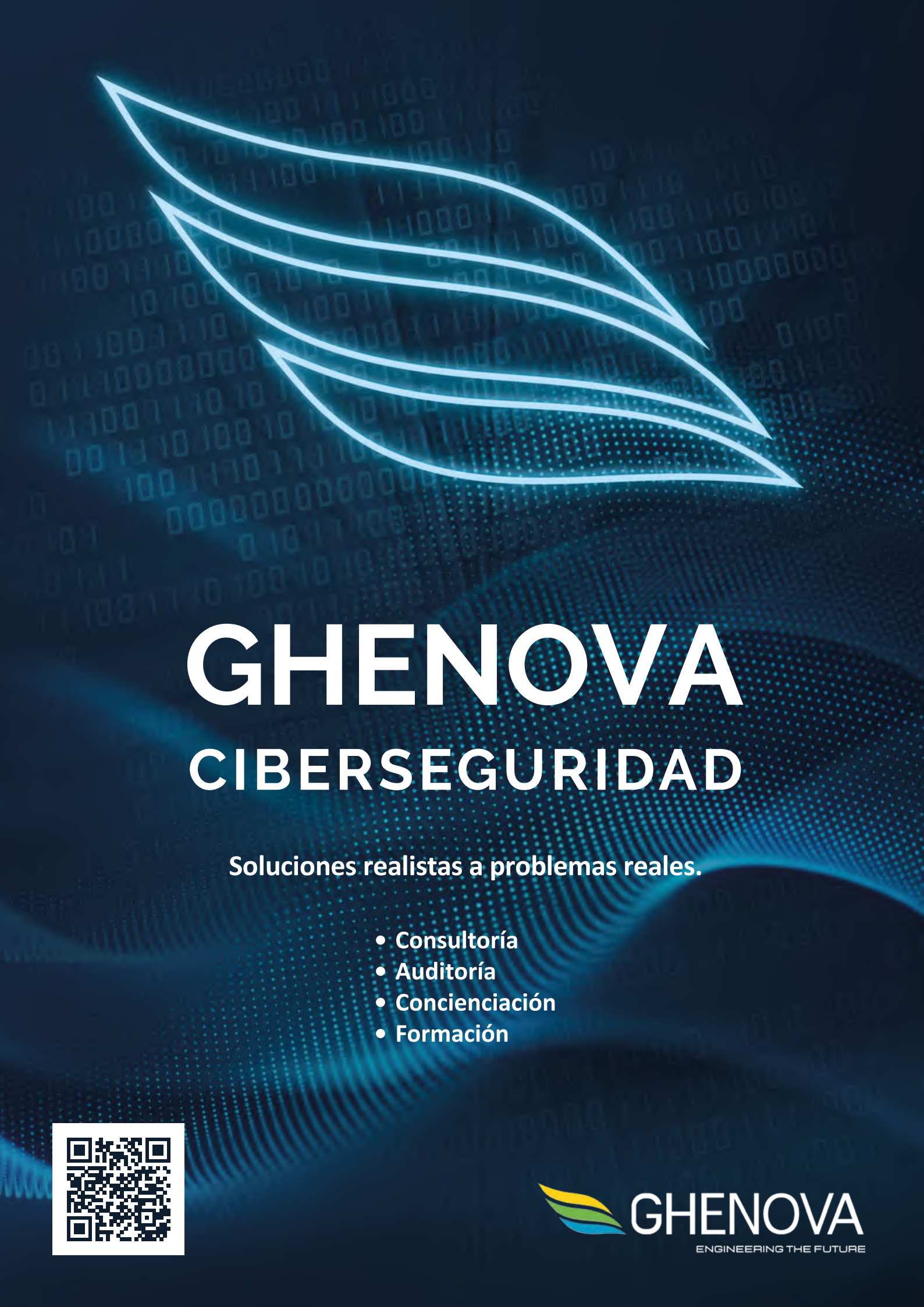
Coordinación y seguimiento

La **Oficina del Director Nacional Cibernético** (**ONCD**) coordinará las actividades bajo el plan, incluido un informe anual para el presidente y el Congreso sobre el estado de implementación, y se asociará con la **Oficina de Administración y Presupuesto** (**OMB**) para garantizar que las propuestas de financiamiento en la solicitud de presupuesto del presidente está alineada con las iniciativas del NCSIP. A pesar de todo, también han surgido críticas sobre cómo se están haciendo las cosas. Un ejemplo es la propuesta de la **Environmental Protection Agency** (**EPA**) de principios de 2023, en la que pedía a las empresas del sector de suministro de agua analizar su grado de madurez en este ámbito a través de una encuesta, algo que muchos consideraron poco eficaz por la complejidad para empresas para analizar, de verdad, su estado en este ámbito. El debate terminó cuando un tribunal determinó que esta exigencia podría no ser legal.

Prioridades de inversión

Por otro lado, la **Casa Blanca** ha dado a conocer sus prioridades de inversión para el año fiscal 2025, focalizándose en el fortalecimiento de las redes y sistemas federales contra las intrusiones cibernéticas. Así, realizan un llamamiento al gobierno federal para que modernice sus sistemas de tecnología de la información invirtiendo en "soluciones duraderas a largo plazo que sean seguras por diseño" y mejorando los requisitos básicos de ciberseguridad. Además, pide alinear este gasto con el enfoque de 'confianza cero' que impulsó en la Administración en 2022.

También, reclama a las agencias que prioricen los esfuerzos para mejorar el equipo humano para la investigación de delitos de *ransomware*, los ataques de denegación de servicio y la lucha contra "el abuso de la moneda virtual para lavar los pagos de rescate". Además, la Casa Blanca ya tiene el candidato a director cibernético nacional. Se trata de **Harry Coker,** un antiguo funcionario de la CIA y de la Agencia de Seguridad Nacional, que continuará la labor de **Chris Inglis.**


GHENOVA
CIBERSEGURIDAD
Soluciones realistas a problemas reales.
• Consultoría
• Auditoría
• Concienciación
• Formación
GHENOVA
ENGINEERING THE FUTURE

EE.UU.

Paso en ciberconcienciación

Poco antes de verano, también se presentó el último borrador de la 'Ley de Concienciación sobre Seguridad Cibernética' que, entre otros aspectos, permitirá a la **Agencia de Seguridad de Infraestructura y Ciberseguridad** (**CISA**) poner en marcha una nueva campaña público-privada que promueva las mejores prácticas cibernéticas en las pequeñas empresas y las comunidades desatendidas.

Acceso remoto seguro

Además, la CISA ha publicado, en colaboración con la **Agencia de Seguridad Nacional** (**NSA**), la **Oficina Federal de Investigaciones** (**FBI**), el **Centro de Análisis e Intercambio de Información Multiestatal** (**MS-ISAC**) y la **Dirección Nacional de Cibernética de Israel** (**NCD**), una guía para que tanto el sector público, como el privado, mejoren la ciberseguridad de los accesos remotos.

EN BREVE

JUSTICIA de EE.UU. creará una nueva unidad para juzgar a los responsables de ciberataques impulsados por estados-nación

El **Departamento de Justicia** estadounidense está poniendo en marcha una nueva sección, dentro de su **División de Seguridad Nacional**, que se especializará en juzgar la actividad cibernética extranjera maliciosa. En concreto, se busca que esta nueva unidad pueda "aumentar la escala y la velocidad de nuestras campañas de disrupción y enjuiciamientos de amenazas cibernéticas del estado-nación, así como de ciberdelincuentes patrocinados por el estado", destacó el fiscal general adjunto **Matthew Olsen**, responsable de la división, durante un evento en Washington.

La nueva Sección Cibernética de Seguridad Nacional contará con fiscales que estarán "formados para actuar rápidamente tan pronto como el FBI o un socio de la comunidad de Inteligencia identifique una amenaza y estaremos en condiciones de apoyar las investigaciones y la interrupción", añadió, a la vez que explicó que, de momento, esta iniciativa está en una primera fase.

El MIT presenta un marco de trabajo para evaluar la eficacia de los esquemas de ofuscación

Bautizado como 'Metior', el marco de trabajo dado a conocer por investigadores del **Instituto Tecnológico de Massachusetts** (**MIT**) busca facilitar el análisis cuantitativo de la información que un atacante podría obtener de un programa víctima protegido por un esquema de ofuscación, para limitar la capacidad del atacante de obtener información confidencial sin eliminarla por completo.

Así, el objetivo de 'Metior' es que los ingenieros y científicos puedan estudiar varios factores, como los programas de las víctimas, las estrategias de los atacantes y las configuraciones de los esquemas de ofuscación para determinar el alcance de la fuga de información. Para probar su eficacia, sus responsables aplicaron el marco a tres casos, mostrando su valor facilitando información sobre las diferentes estrategias de ataque y revelando comportamientos que no se entendían completamente. La publicación de 'Metior' se produce poco después de que los investigadores de seguridad de Google revelaran un nuevo marco para desarrollar herramientas seguras de IA generativa.

La próxima Ley de la Iniciativa Nacional Cuántica buscará priorizar la inversión en I+D

Durante una audiencia en la **Comisión de Ciencia, Espacio y Tecnología de la Cámara**, para volver a actualizar la Ley de Iniciativa Cuántica Nacional, el director de la **Oficina Nacional de Coordinación Cuántica** en la **Oficina de Política Científica y Tecnológica** de la Casa Blanca, **Charles Tahan** (en la imagen), dio a conocer que se va a poner un peso especial en desarrollar iniciativas de investigación más avanzadas, abarcando varias agencias federales y utilizando los fondos proporcionados en el NQI, que expirará a fines del año fiscal 2023 sin la reautorización del Congreso. "En primer lugar, nuestro objetivo debe ser continuar avanzando rápido y potenciar a nuestros científicos y empresarios, mantener la comunidad científica abierta", explicó Tahan.

También, avanzó que se está estudiando el despliegue de un programa de satélites cuánticos, además de continuar apoyando las iniciativas de investigación puestas en marcha para, entre otros aspectos, crear "las primeras piezas de una computadora cuántica viable y operable", así como dar la posibilidad a que el Departamento de Energía pueda iniciar un programa de computación de alto rendimiento posterior, con casi 180 millones de euros al año, en aras de incorporar tecnología cuántica en la arquitectura de las supercomputadoras.

MADRID,
28 AL **30** DE
NOVIEMBRE

XVII JORNADAS STIC CCN-CERT

V JORNADAS DE CIBER DEFENSA: ESPDEF-CERT

COMPARTIR PARA GANAR

#XVIIJORNADAS**CCNCERT** | **#V**JORNADAS**ESPDEFCERT**

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

U23 PRESIDENCIA ESPAÑOLA CONSEJO DE LA UNIÓN EUROPEA

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

espdef-cert Mando Conjunto del Ciberespacio

IBEROAMÉRICA

Se calcula que la industria de ciberprotección crecerá más de un 12% este año, superando los 20.000 millones de euros

América Latina y Caribe comienzan a alcanzar niveles notables de ciberseguridad a través de la puesta en marcha de SOC nacionales y leyes específicas

México, Brasil, Colombia, Perú y Chile son los cinco países con más ciberamenazas en Iberoamérica. Así lo destaca un reciente informe realizado por **Etek International** en el que también se subraya que el 63% los delitos con motivos financieros encabezan la lista. De media, se recibe en la región un ataque cada 45 segundos con un coste medio de 231.000 euros. Entre los sectores más afectados se encuentran el financiero, seguido de salud, energía, fabricación y gobierno.

Como en el resto del mundo, el informe también corroboró un aumento notable en la peligrosidad, sofisticación y tasa de éxito de las ciberamenazas y avanza que, para la segunda parte del año, podrían experimentar un crecimiento importante, sobre todo, a través de *ransomware-as-a-service* (RaaS) y exfiltración de información sensible mediante *malware*.

Se trata de unas cifras preocupantes que están generando todo tipo de iniciativas por parte del sector público y privado en Iberoamérica donde, según un informe de **Ocean Report,** el mercado de ciberprotección podría crecer más de un 12% este año, con un valor de casi 20.000 millones de euros.

Notables esfuerzos

Así, **Mercosur** (Mercado Común del Sur) ha dado un paso más para impulsar un acuerdo de cooperación en protección. Los mandatarios de los países que forman parte de este bloque económico, así como de los estados asociados, participaron en la LXII Cumbre de Presidentes de la organización, en julio, donde fue notable que, según la nota de prensa oficial, se felicitaron por "los avances en la negociación de un 'Acuerdo de coordinación, respuesta y colaboración de las autoridades nacionales de los Estados Partes ante el uso malicioso del espacio cibernético, a fin de mantener el acceso abierto, seguro, estable, accesible, pacífico e interoperable del entorno cibernética".

Además, son notables las inversiones e iniciativas que se están poniendo en marcha en países como México, donde destaca la apuesta de la **International Chamber of Commerce México** (ICC México) para facilitar la aprobación de una Ley Federal de Ciberseguridad que permita "un crecimiento sostenible, así como fomentar la confianza", señaló la cámara empresarial.

También, los **Comisionados del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales** (INAI) de México reiteraron al poder legislativo la urgencia de la creación de una ley de ciberseguridad, así como la actualización de la normativa de protección de datos personales.

Por su parte, **Colombia** ha anunciado que dedicará algo más de 2,4 millones de euros a la creación de su propio Centro de Ciberseguridad. "En cualquier elemento estratégico que queramos hacer en términos de desarrollo de los ecosistemas, la seguridad cibernética es fundamental. Por eso, desde el primer día que llegamos al ministerio, decidimos crear este hub que hoy lanzamos y que ya tiene los recursos", explicó el Ministro TIC, **Mauricio Lizcano.**

Chile también ha dado pasos notables con la aprobación de su 'Política Nacional de Ciberseguridad', plasmada en un documento con cinco pilares de acción: el primero, centrado en contar con una "infraestructura resiliente"; el segundo, dedicado a los derechos de las personas; el tercero, a la cultura de ciberseguridad; el cuarto, a la coordinación nacional e internacional; y el quinto, de fomento a la industria y la investigación científica. Además, el país también tiene en marcha una iniciativa para crear su Agencia Nacional en este ámbito.

Acuerdos internacionales

Además, en uno de los primeros anuncios realizados en la reciente gira europea del presidente de Chile, **Gabriel Boric,** el mandatario, recibido por el presidente español **Pedro Sánchez,** en España, firmó varios acuerdos, entre ellos, uno para mejorar la ciberseguridad del país compartiendo esfuerzos.

No es el único acuerdo notable en la región, ya que, entre otros, **Costa Rica** contará con más de nueve millones de euros por parte EE.UU., para "fortalecer sus defensas cibernéticas", fruto de la colaboración que han impulsado recientemente ambos países.

En este sentido, Estados Unidos continúa estableciendo y fortaleciendo alianzas estratégicas en este ámbito en la región. En agosto, más de 30 jueces, fiscales y policías de **Uruguay**, **Perú** y **Argentina** se reunieron en Montevideo (Argentina), para


SUSE
La Confianza Digital:
Un Valor Clave para el Futuro de las Organizaciones
Mantén la confianza digital con las funciones de seguridad 360° de SUSE, una integración perfecta que aborda los problemas críticos de ciberseguridad al tiempo que permite a las organizaciones liberar todo su potencial innovador.
SUSE
Descarga la guía gratuita
www.suse.com/digital-trust/

IBEROAMÉRICA

intercambiar conocimiento en una cumbre sobre cibercrimen organizada por el programa Internacional de Hacking Informático y Propiedad Intelectual (ICHIP), del **Departamento de Justicia y del de Seguridad Nacional** estadounidenses. De cualquier forma queda mucho que hacer en Iberoamérica. Según un análisis de **Jorge M. Vega,** publicado por el **Real Instituto Elcano,** titulado 'Gobernanza público-privada de la ciberseguridad en América Latina: momento agridulce', se destaca que, a pesar de que en la región, "la ciberseguridad es reconocida por países y organismos regionales como una responsabilidad multisectorial compartida, la implementación práctica de esta dinámica colaborativa presenta claroscuros y carece de mediciones internacionales específicas que permitan su seguimiento y comparación".

EN BREVE

ESPAÑA acoge el primer encuentro entre diplomáticos especializados en diplomacia digital y cibernética del ámbito europeo e iberoamericano

El **Instituto Nacional de Ciberseguridad de España** (Incibe), en coorganización con el **Ministerio de Asuntos Exteriores**, la **UE** y el apoyo de la **Organización de Estados Americanos** (OEA) y el **Departamento de Estado de EE.UU.**, acogió en verano el encuentro ´EU-Americas Regional Dialogue on Cyber and Digital Diplomacy´, en el que reunió, por primera vez, a diplomáticos de más de 30 países especializados en ciberprotección y política digital de América y Europa. El encuentro se realizó dentro de los diferentes actos que se están llevando a cabo por la presidencia española y durante la celebración de la octava edición del Cybersecurity Summer BootCamp en León, que este año contó con más de 260 alumnos, de 23 países.

Durante dos jornadas, los participantes asistieron a diferentes ponencias con un programa especialmente centrado en ciberdiplomacia, contando con tres mesas redondas y una clase magistral de expertos internacionales de alto nivel. En la primera de ellas, se abordó el desarrollo de estrategias globales de ciberseguridad. En la segunda, se centraron en el camino a seguir para la diplomacia tecnológica regional y multilateral, y en la última, se analizaron las herramientas cibernéticas y digitales de la UE en América Latina.

Precisamente, en colaboración con la OEA, también se celebraron los 'International CyberEx', para fortalecer de las capacidades de respuesta ante incidentes cibernéticos, así como una mejora de la colaboración y cooperación ante este ámbito en el que tomaron parte miembros de la Organización, así como otros países con CSIRT, invitados por el Incibe

BRASIL quiere poner cuanto antes en marcha su Agencia Nacional de Ciberseguridad, consciente de estar rezagada en este ámbito

La **Oficina de Seguridad Institucional de la Presidencia de la República** (GSI) ha destacado que el país "ya está atrasado" en ciberprotección, por lo que supone de freno no contar con una Agencia Nacional de Ciberseguridad. Por ello, el GSI, que elabora la propuesta de Política Nacional de Ciberseguridad, incluyó a **ANCIber** en el borrador de su proyecto de ley, con un presupuesto anual que podría rondar los 113 millones de euros y un equipo de 800 profesionales, acorde a las "dimensiones social y económica" del país.

En este sentido, en el reciente congreso CyberGov 2023, se destacó la necesidad de contar con la Agencia como organismo de coordinación, "distribuyendo conocimiento a los segmentos más vulnerables del ecosistema digital para elevar el nivel básico de madurez cibernética", comenzando por los que "soportan servicios esenciales".

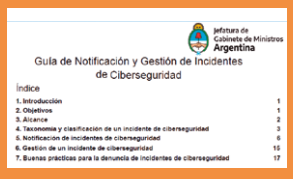
Para 2028 se estima un déficit de 2,5 millones de profesionales de protección cibernética en la región

Se calcula que Iberoamérica y Caribe precisarán, en un lustro, de 2,5 millones más de profesionales especializados en TIC para dar respuesta a las necesidades del mercado. Así lo destaca el informe 'Talentos Digitales 2023', de **Huawei**, realizado por **IDC**, que "su demanda ha estado creciendo constantemente en los últimos años, creando una brecha con la oferta. Además de eso, a menudo existe el grave problema del desajuste entre la oferta y la demanda en términos de habilidades", ha explicado el vicepresidente de Asuntos Públicos de Huawei para la región, **César Funes.**

Por ejemplo, el 73,2% de los preguntados de empresas de México, Perú, Colombia y Brasil confesó que encontrar profesiones cualificados está resultando muy complejo tanto por el número cada vez mayor que se demanda, como por el incremento de la edad de los empleados en la región y el aún bajo número de jóvenes con estudios superiores relacionados con lo digital. En concreto, las dos áreas más demandadas por los participantes en este ámbito son la ciberseguridad (39%) y las operaciones de TI (33%).

Aprobada en ARGENTINA la primera guía de notificación de ciberincidentes para el sector público

La **Subsecretaría de Tecnologías de la Información,** de la Jefatura de Gabinete de Ministros, ha aprobado una guía de recomendaciones para la notificación y gestión de incidentes de ciberseguridad en el sector público. Según sus impulsores, aunque no es obligatoria, sí permitirá dar un paso importante para mejorar la protección de los activos de información y garantizar una respuesta efectiva frente a los riesgos cibernéticos en el entorno digital.


Jefatura de Gabinete de Ministros Argentina

Guía de Notificación y Gestión de Incidentes de Ciberseguridad

Índice

En ella, se ofrece desde una clasificación de incidentes, hasta recomendaciones de mejores prácticas de notificación, los protocolos de respuesta y recuperación necesarios con los que hay que contar y cómo mejorar la colaboración con el **Centro Nacional de Respuesta a Incidentes Informáticos** (CERT.ar).

Además, en el país se inauguró en verano la Red Iberoamericana de Blockchain y Ciberseguridad (RIBCi), coordinada por la **Universidad Tecnológica Nacional** (Facultad Regional Córdoba), con la participación de 13 grupos de investigación y cuatro cámaras provenientes de ocho países iberoamericanos.

Entelgy Innotec
SECURITY

Live confident,
be (cyber) secure

The winning teams

Red Team

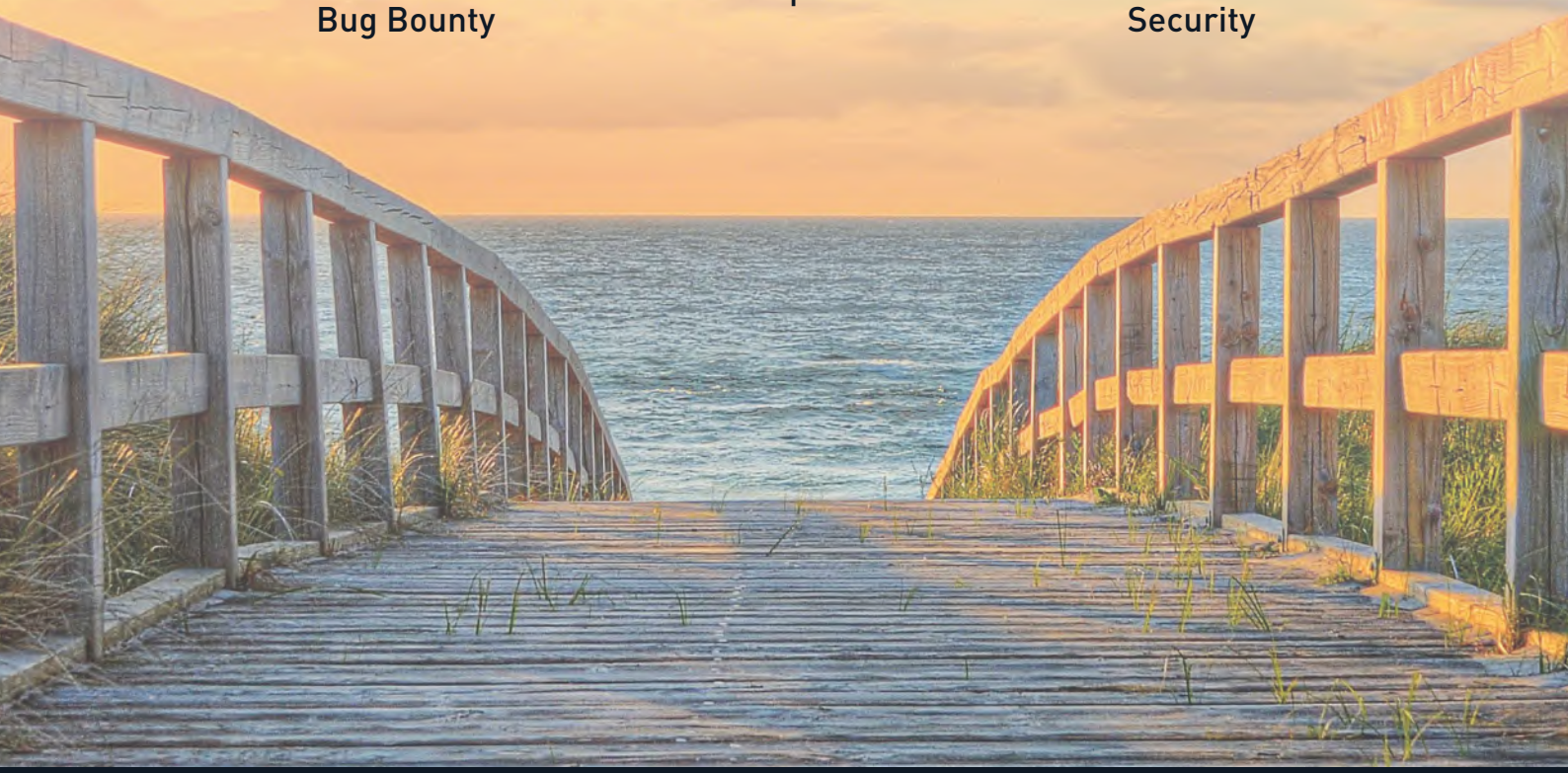
- Pentesting
- TIBER Exercises
- Atomic & Purple Team
- Private Bug Bounty

Golden Team

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

Blue Team

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



innotec.security

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

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

Además, el Consejo de Seguridad de la ONU celebra su primera reunión en torno a esta tecnología y sus implicaciones, ya que se estima que esta moverá 41.160 millones de euros para 2027

EUROPA y EE.UU. podrían presentar un 'Código de Conducta de la IA' en octubre y MICROSOFT pide un marco global para su regulación

La efervescente popularización de la Inteligencia Artificial, especialmente en el último año, está despertando en la comunidad científica una preocupación similar a la que hubo con los físicos nucleares conscientes del potencial, para lo bueno y lo malo, de esta tecnología. De cualquier forma, la creciente demanda de soluciones de ciberprotección impulsadas por estas sofisticadas capacidades no ha pasado desapercibida para el mercado. Según un informe de **Grand View Research**, se espera que el mercado global de IA en seguridad cibernética alcance 41.160 millones de euros para 2027, con un crecimiento anual del 23,3% hasta ese año.

Ley europea de IA

De cualquier forma, sí existen diferentes iniciativas gubernamentales para reducir el riesgo de un impacto malicioso, que algunos expertos han llegado a comparar con los efectos de un 'bomba atómica'. Así, el **Parlamento Europeo** ha continuado desarrollando el borrador de la denominada 'Ley de IA', proponiendo nuevas medidas para controlar los "modelos fundamentales". Entre ellas, destaca desde un enfoque escalonado para los modelos de IA (de 'riesgo bajo y mínimo', 'riesgo limitado', 'alto riesgo' y 'riesgo inaceptable'), hasta la ausencia de regulación para las herramientas de IA de 'riesgo bajo y mínimo'. Además, se quiere poner en marcha una base de datos de sistemas de IA de uso general y de alto riesgo para explicar dónde, cuándo y cómo se implementarán en suelo comunitario. Y, al igual que con el Reglamento General de Protección de Datos (RGPD), en la ley se estipulan multas de hasta 30 millones de euros o 6% de las ganancias globales para las compañías que la incumplan.

Pero aún queda por hacer. En la primera reunión de la presidencia española sobre el borrador, el llamado triálogo político, en julio, no hubo avances notables quedando emplazados sus participantes para verse de nuevo del 26 de septiembre al 3 de octubre.

Por otro lado, el gobierno estadounidense ha incrementado su presión sobre la **Comisión Europea** para que acelere el desarrollo de su propuesta de 'Código de Conducta de AI', para tener un texto consolidado para la Reunión de Ministros de Comercio del **G7** en Osaka-Sakai, a fines de octubre. Precisamente, España ha sido pionera en este ámbito con la aprobación del Estatuto de la Agencia de Supervisión de IA (ver sección noticias).

Y es que el estamento político es consciente de que los ciberdelincuentes usaran en imparable *crescendo* la IA para desarrollar ataques más sofisticados. Organismos como **Europol,** han advertido en su 'Informe de Tendencias y Situación del Terrorismo de la UE (TE-SAT) 2023', sobre los riesgos del metaverso y la amenaza terrorista utilizando la IA. De hecho, la **ONU** celebró en verano, presidido por el secretario de Relaciones Exteriores del Reino Unido, **James Cleverly,** su primer Consejo de Seguridad sobre Inteligencia Artificial.

Una década decisiva

En EE.UU. se está siguiendo de cerca sus implicaciones para la ciberseguridad y la privacidad de los datos. Así, el propio presidente, **Joe Biden**, reunió en una jornada a muchos de los referentes tecnológicos del país para debatir sobre lo que denominó los "riesgos y enormes promesas" de la IA. "Veremos más cambios tecnológicos en los próximos 10 años que los que vimos en los últimos 50 años", destacó al principio del encuentro con ocho participantes, referentes en esta tecnología.

Es especialmente significativo que, en verano, trascendiera el hecho de que el **Departamento de Comercio** de EE.UU. se esté preparando para implementar una prohibición sobre la capacidad de las empresas estadounidenses de proporcionar servicios en la nube que empleen procesadores avanzados de IA a las empresas chinas, según Computer World. Una medida que de aplicarse afectaría al negocio de empresas como **Microsoft, Google** y **Amazon,** y evitaría que las entidades chinas eludan las restricciones a la exportación de chips avanzados que se utilizan en el entrenamiento de IA al obtener acceso a ellos a través de servicios de pago en la nube, según expertos en seguridad nacional.

Crecimiento del *malware*

Por su parte, **Palo Alto Networks** presentó su estudio 'What's Next in Cyber', en el que alerta de que casi la mitad de las organizaciones en todo el mundo consideran que este tipo de tecnología tendrá un gran impacto en su seguridad (49%), mientras que cuatro de cada 10 compañías españolas valoran que la aplicación de la IA permi-

CROWDSTRIKE

La Referencia en Seguridad de Endpoints 100% en la nube

Inteligencia sobre amenazas

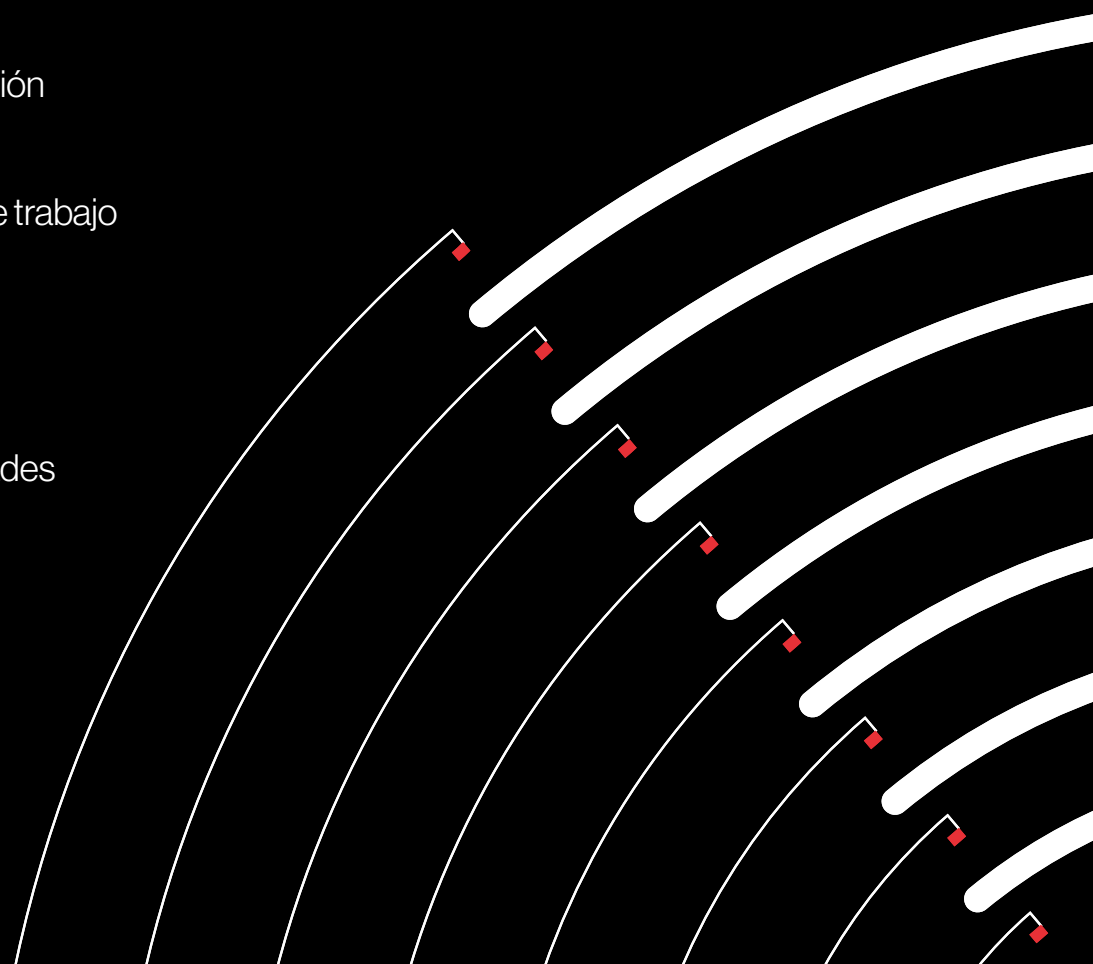
Protección de identidad

Antivirus de nueva generación

Protección de las cargas de trabajo

Control de dispositivos

Evaluación de vulnerabilidades



crowdstrike.com

te una mayor rapidez resolutiva a la hora de protegerse. Además, la unidad de investigación e inteligencia de amenazas de la compañía, Unit 42, destacó que ha registrado un incremento del *malware* relacionado con ChatGPT. Concretamente, un crecimiento de 910% en este tipo de detecciones y se llegaron a identificar hasta 118 ataques diarios de URLs relacionadas con dicha plataforma de IA.

Eso sí, la industria de la ciberseguridad también está logrando avances notables. Entre ellos ha destacado la investigación realizada por expertos de **Kaspersky** en la que probaron 5.265 URLs (2.322 de *phishing* y 2.943 seguras) preguntándole al conocido ChatGPT (GPT-3.5).

"¿Este enlace conduce a un sitio web de *phishing*?", y en cuya respuesta, el *chatbot* tuvo una tasa de detección del 87,2% y una tasa de falsos positivos del 23,2%.

Motivos de preocupación

Por otra parte, **Eset** ha alertado, dentro de los riesgos que la IA representa para la protección, de la posibilidad de que se generalicen los ciberataques a infraestructuras críticas, como son los sistemas de generación de energía y la red eléctrica, los hospitales, los servicios de salud, la cadena de suministro global e incluso las cadenas de suministro digitales y la propia Internet. De hecho, en Reino Unido se ha dado a conocer un estudio realizado por **VMware**, en el que más de la mitad (56%) de los ciudadanos destacaron no confiar en que el Servicio Nacional de Salud (NHS) utilice IA para analizar los datos de los pacientes debido a problemas de seguridad y privacidad. Eso sí, el 45% de los encuestados dijo que estaban abiertos a que el NHS usara IA para mejorar los servicios, y el 44% estaba satisfecho con el uso de estas tecnologías.

Novedades de la industria

Por su parte, **Google,** propietario del *chatbot* generativo de IA Bard, empresa matriz del laboratorio de investigación de **IA DeepMind,** ha presentado su **Secure AI Framework (SAIF),** que se ofrece como "un marco conceptual audaz y responsable para ayudar a asegurar la tecnología de IA de forma colaborativa". Otras, como **Accenture,** han anunciado una inversión que rondará los 2.700 millones de euros en IA para acelerar la 'reinvención' de sus clientes.

Marco multilateral

Además, el presidente de Microsoft, **Brad Smith,** (en la imagen) aprovechando su participación en un evento en Bruselas, destacó la postura de la compañía respecto a la IA. En este sentido, avanzó que se ha elaborado un plan de acción de cinco puntos para regularla en Europa, acorde a la legislación que se quiere aprobar por parte del Parlamento.

Eso sí, también destacó que para que las normativas respecto a esta tecnología sean eficaces es preciso que se cuente con un marco multilateral que conecte las diferentes normas nacionales y garantice que un sistema de IA certificado como seguro en una jurisdicción también pueda calificarse como seguro en otra.

En concreto, debería basarse en el trabajo ya realizado en la **OCDE** para desarrollar los principios para una IA segura y fiable, proporcionar recursos para que los desarrolladores de una IA regulada salvaguarden la protección de estos sistemas de acuerdo con los estándares internacionales acordados, además de fomentar la innovación y el acceso, proporcionando un medio para el reconocimiento mutuo del cumplimiento y la seguridad a través de las fronteras. "La regulación de la IA es un camino, no un destino. Nadie tiene todas las respuestas, y es importante que escuchemos, aprendamos y colaboremos", destacó Smith.

Los hackers consideran que la IA no podrá reemplazar su creatividad en investigaciones y gestión de vulnerabilidades

El 72% de los investigadores informáticos, contextualmente enmarcados bajo el paraguas de los 'hackers', dicen confiar en que la IA no puede reemplazar la creatividad humana en la investigación de seguridad y la gestión de vulnerabilidades, según un estudio anual de la compañía **Bugcrowd,** titulado 'Inside the Mind of a Hacker 2023', en el que se ha preguntado a más 1.000 profesionales de este este ámbito de 85 países, incluidos EE.UU, Australia, Brasil, Canadá, Etiopía, India, Francia, Jordania, Singapur y el Reino Unido, entre otros.

En él, los propios investigadores destacaron su escepticismo sobre la posibilidad de perder su trabajo por la IA. Y, de hecho, reconocieron que mejora su día a día, ya que la usan de forma intensiva para la automatización de tareas (50%), análisis de datos (48%), la identificación de vulnerabilidades (36%), validación de hallazgos (35%) y realización de reconocimientos (33%).

También, resulta interesante que el 64% considere que esta tecnología ha incrementado el valor de lo que hace. La investigación, entre otros datos de interés, constató además que la apreciación de los investigadores de ciberseguridad sobre la importancia que dan las empresas a este ámbito. El 27% de los participantes indica que menos del 10% entienden su riesgo, entre el 10% y el 25% sí lo tienen más o menos claro, y un 16% destacó que más de la mitad de las compañías lo tiene claro y comprenden que pueden ser ciberatacadas.

CURSOS de Especialización

Prepara la vuelta al cole con nuestros cursos para profesionales

- Cursos Ciberseguridad
- Cursos GRC
- Cursos Privacidad

¡PARA MÁS INFORMACIÓN!

info@es-ciber.com

ES-CIBER

Ha incorporado notables modificaciones sobre las obligaciones de informes, los productos altamente críticos y su vida útil

El CONSEJO de la UE da luz verde al texto de la Ley de Ciberresiliencia que entra en su última fase, a la espera de su aprobación por el PARLAMENTO

La Ley de Ciberesiliencia (Cyber Resilience Act, CSA) continua a buen paso. En julio, los estados miembros acordaron una "posición común sobre los requisitos de seguridad para los productos digitales", para que "sean seguros antes de ingresar al mercado". "Este es un hito importante para la presidencia española y esperamos adelantar, en la medida de lo posible, las negociaciones con el Parlamento", destacó la secretaria de Estado de Digitalización e IA en funciones, **Carme Artigas.**

Así, el texto aprobado introduce requisitos obligatorios de ciberseguridad para el diseño, desarrollo, producción y puesta a disposición en el mercado de productos de hardware y software para evitar la superposición de requisitos derivados de diferentes leyes en los estados miembro de la UE. El reglamento propuesto se aplicará a todos los productos que estén conectados directa o indirectamente a otro dispositivo o red. Hay algunas excepciones, para los cuales los requisitos de ciberseguridad ya están establecidos en las normas de la UE existentes, por ejemplo, en dispositivos médicos, aviación o automóviles.

La propuesta tiene como objetivo llenar los vacíos, aclarar los vínculos y hacer que la legislación sobre ciberseguridad existente sea más coherente al garantizar que los productos con componentes digitales, por ejemplo, los productos de 'Internet de las cosas' (IoT), sean seguros a lo largo de toda la cadena de suministro y a lo largo de su ciclo de vida completo. Por último, el reglamento también permite a los consumidores tener en cuenta la ciberprotección al seleccionar y utilizar productos que contengan elementos digitales, brindándoles la oportunidad de tomar decisiones informadas con las características adecuadas de ciberseguridad.

Qué se mantiene y qué cambia

El **Consejo Europeo** ha resaltado el valor de algunos elementos propuestos por la **Comisión,** como la necesidad de implementar una 'responsabilidad de cumplimiento' hacia los fabricantes, que "deben garantizar la conformidad con los requisitos de seguridad de los productos con elementos digitales que se comercializan en el mercado de la UE, incluidas obligaciones como la evaluación del riesgo de ciberseguridad, la declaración de conformidad y la cooperación con las autoridades competentes". También, establece unos requisitos esenciales para los procesos de tratamiento de vulnerabilidades de los fabricantes concernidos y obligaciones de los operadores económicos, como importadores o distribuidores, en relación con estos procesos.

Junto a ello, se han incluido varias modificaciones notables sobre el alcance de la legislación propuesta, incluso, con respecto a las categorías específicas de productos que deben cumplir con los requisitos del reglamento, como lo que atañe a las obligaciones de notificación de vulnerabilidades o incidentes explotados activamente a las autoridades nacionales competentes (a través de sus CSIRT), en lugar de a la **Agencia de la UE para la Ciberseguridad (Enisa),** creándose también una plataforma única de notificación.

Además, especifica nuevos elementos para la determinación de la vida útil esperada del producto por parte de los fabricantes, y se incluyen nuevas medidas de apoyo a las pequeñas empresas y microempresas, así como una declaración simplificada de conformidad.

De esta forma, este acuerdo queda ya pendiente de que la presidencia española entable negociaciones con el Parlamento Europeo. De hecho, se realizará una votación sobre el documento acordado en la **Comisión de Industria, Investigación y Energía del Parlamento,** el 18 y 19 de septiembre, a la que seguirá una votación los días 27 y 28 de noviembre, finalizándose el proceso en una posible sesión plenaria en diciembre.

EE.UU. pondrá en marcha una ley de 'etiquetado cibernético' bajo los criterios propuestos por el NIST

EE.UU. ha dado a conocer su programa de etiquetado 'Cyber Trust Mark' con un objetivo similar a la Ley de Ciberresiliencia europea (CSA): permitir a los consumidores conocer el grado de ciberseguridad de cualquier producto conectado que se adquiera. La iniciativa, propuesta por la responsable de la Comisión Federal de Comunicaciones (FCC), **Jessica Rosenworcel,** busca elevar el nivel de ciberprotección en dispositivos comunes, incluidos refrigeradores inteligentes, microondas inteligentes, televisores inteligentes, sistemas de control de clima inteligente y rastreadores de actividad física inteligentes, entre otros. La medida, de momento, ha sido bien acogida por el mercado, fabricantes y minoristas como **Amazon, Best Buy, Google, LG Electronics USA, Logitech** y **Samsung Electronics** han mostrado públicamente su apoyo a ella.

Según ha trascendido, el programa aprovechará las propuestas del **Instituto Nacional de Estándares y Tecnología** (NIST) para certificar y etiquetar productos exigiendo, entre otros aspectos, contraseñas predeterminadas únicas y seguras, protección de datos, actualizaciones de software y capacidades de detección de incidentes.

Así, una vez aprobada, los consumidores podrán comprobar el grado de ciberprotección de un producto a través de un 'sello de garantía, con un logotipo y escudo fácil de identificar y que permite comprobar que los productos que cumplen con los criterios establecidos". Eso sí, aún queda mucho para aprobarse. De momento, la FCC abrirá un periodo de consulta pública y se espera su puesta en marcha para 2024, casi a la vez que la CSA en Europa. A este esfuerzo se suman otros de carácter sectorial, como el anunciado por el **Departamento de Energía** que, junto con el **National Labs** y referentes en este ámbito, quieren establecer requisitos de etiquetado de seguridad cibernética para medidores inteligentes e inversores de energía.

CIBERSEGURIDAD

Nuestro reto, tu tranquilidad

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

¿Qué podemos hacer por ti?

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

marketing.TIC@gmv.com

gmv.com

gmv®
INNOVATING SOLUTIONS

Dará a las personas y empresas un mayor control a través de un derecho de portabilidad reforzado

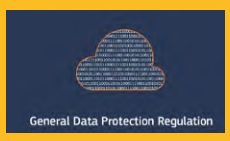
Nueva Ley de datos: el CONSEJO y el PARLAMENTO llegan a un acuerdo y se espera que se haga realidad para antes de final de año

Con el fin de hacer de la UE un referente de una sociedad basada en los datos, la presidencia del **Consejo** y los representantes del **Parlamento Europeo** alcanzaron en julio un acuerdo provisional sobre un nuevo reglamento sobre normas armonizadas sobre el acceso justo a los datos y su uso (ley de datos). La nueva legislación también tiene como objetivo facilitar el cambio de proveedores de servicios de procesamiento de datos, establecer salvaguardas contra la transferencia ilegal de datos por parte de los proveedores de servicios en la nube, y prevé el desarrollo de estándares de interoperabilidad para la reutilización de datos entre sectores.

En concreto, el reglamento establece nuevas reglas sobre quién puede acceder y utilizar los datos generados en la UE en todos los sectores económicos. Así, pretende "garantizar la equidad en la asignación del valor de los datos entre los actores del entorno digital, estimular un mercado de datos competitivo, abrir oportunidades para la innovación basada en datos y hacer que sean más accesibles para todos", destacan sus impulsores. Dará a las personas y empresas un mayor control sobre sus datos a través de un derecho de portabilidad reforzado, copiando o transfiriendo datos fácilmente desde diferentes servicios, donde se generan a través de objetos, máquinas y dispositivos inteligentes. La nueva legislación busca con ello empoderar a los consumidores y las empresas al darles voz sobre lo que se puede hacer con los datos generados por sus productos conectados.

El texto también contiene medidas para evitar el abuso de los desequilibrios contractuales en los contratos de intercambio de datos debido a términos injustos impuestos por una parte con una posición de negociación significativamente más fuerte, entre otras**.** El acuerdo dará lugar a la esperada 'Ley de Datos' de la UE, una vez sea aprobado por el Consejo y el Parlamento Europeo.

El RGPD evoluciona con importantes cambios, sobre todo, para casos transfronterizos



La **Comisión Europea** ha propuesto cambios en el RGPD destinados a mejorar la cooperación entre las autoridades de protección de datos (DPA) que trabajan en su aplicación en casos transfronterizos. Las reglas son el resultado de una 'lista de deseos', de octubre de 2022, enviada a la Comisión por el **Consejo Europeo de Protección de Datos** (EDPB), que opera un proceso de resolución de disputas cuando las DPA no pueden ponerse de acuerdo sobre el camino a seguir. Como se sabe, el RGPD tiene una regla de 'ventanilla única' por la cual, la DPA principal se selecciona de acuerdo con el país de la UE en el que se encuentra la entidad bajo investigación. Sin embargo, dado que la mayoría de los gigantes tecnológicos de EE.UU. tienen su sede en Irlanda, algunos de los casos transfronterizos de más alto perfil han creado tensión entre la Comisión de Protección de Datos de Irlanda (DPC) y otras DPA nacionales.

Por ello, la propuesta proporciona reglas detalladas para apoyar el buen funcionamiento del mecanismo de cooperación y coherencia establecido por el RGPD, armonizando reglas en áreas como de la de derechos de los denunciantes eliminando, por ejemplo, armonizando los requisitos para que una denuncia transfronteriza sea admisible.

Aprobados los logotipos para identificar a los intermediarios de datos confiables de la UE

EU Recognised Data Intermediary

EU Recognised Data Altruism Organisation

La **Comisión** ha aprobado los logotipos comunes para identificar fácilmente a los proveedores de servicios de intermediación de datos confiables y a las organizaciones altruistas de datos en la UE, que conectarán a los titulares de datos, tanto individuos como empresas, con los usuarios de datos.

Los proveedores y organizaciones concernidas que cumplan las condiciones consagradas en la Ley de Gobernanza de Datos y opten por el uso de logotipos, deberán exhibirlos claramente en todas las publicaciones en línea y fuera de línea. El uso de estos logotipos en tota la UE diferenciará los servicios de confianza reconocidos de otros servicios, contribuyendo a la transparencia en el mercado de datos. El logotipo de las organizaciones reconocidas en la UE con este distintivo deberá ir, además, acompañado de un código QR con un enlace al registro público de la UE de organizaciones de altruismo de datos reconocidas, que estará disponible a partir del 24 de septiembre de 2023.

Los logotipos han sido adoptados mediante el Reglamento de Ejecución y serán registrados como marcas, para protegerlos de un uso indebido.

La AEPD actualiza su herramienta Gestiona y su guía sobre el uso de *cookies*

La **Agencia Española de Protección de Datos** (AEPD) ha presentado una nueva versión de su herramienta 'Gestiona', orientada especialmente a pequeñas entidades públicas o privadas, y que permite gestionar los tratamientos, realizar la gestión de riesgos y, en su caso, dar soporte para la realización de las evaluaciones de impacto. La herramienta ahora cuenta con un diseño más intuitivo e incorpora las últimas directrices recogidas en las guías publicadas por la Agencia.

Gestiona RGPD
Registro de Tratamientos y Evaluación del Riesgo

La solución ha sido mejorada, de forma notable, con una profunda transformación de la herramienta original, permitiendo gestionar el Registro de Actividades de Tratamiento de una entidad con hasta 500 tratamientos, de forma integrada. Además, incluye funciones para identificar los factores de riesgo para los derechos y libertades de las personas cuyos datos se tratan y hacer una primera evaluación del riesgo intrínseco.

Además, la AEPD ha actualizado la Guía sobre el uso de las cookies para adaptarla a las Directrices 03/2022 sobre patrones engañosos del **Comité Europeo de Protección de Datos** (**CEPD**), contando, como ocurrió con versiones anteriores, con la participación de los sectores afectados (las asociaciones **Adigital, Anunciantes**, **Autocontrol** e **IAB Spain**).

FACTUM

IAM

Identity and Access Management

El control de accesos que protege tu identidad

Control de acceso basado en roles
Acceso con privilegios
Autenticación multi factor

+200 clientes en el mundo +140 especialistas +14 años de experiencia

En noviembre, celebrará su primera Conferencia Integral de Defensa Cibernética en Berlín

La OTAN refuerza su apuesta por la ciberdefensa, basada en la disuasión y poniendo en marcha su Capacidad Virtual de Apoyo a Incidentes Cibernéticos

La reunión de los jefes de Estado y de Gobierno de la **OTAN** en julio, en Vilnius (Lituania), puso sobre la mesa, entre otras novedades, la apuesta de la alianza por una defensa del ciberespacio a través de nuevas capacidades y alianzas. En su declaración final, los participantes recordaron que la postura de disuasión y defensa de la Alianza "se basa en una combinación adecuada de capacidades de defensa nuclear, convencional y antimisiles, complementada con capacidades espaciales y cibernéticas", siempre con "herramientas militares y no militares de manera proporcionada, coherente e integrada".

Políticas de disuasión

Así pues, entre otros aspectos, se decidió impulsar más "medidas significativas para mejorar la postura de disuasión y defensa de la OTAN en todos los dominios, incluido el fortalecimiento de las defensas avanzadas y la capacidad de la Alianza para reforzar rápidamente a cualquier aliado que se vea amenazado". Una declaración que, en el ámbito cibernético, se plasma en "continuar nuestro trabajo en operaciones multidominio, habilitado por la Transformación Digital de la OTAN, que impulsa aún más nuestra ventaja militar y tecnológica, fortaleciendo la capacidad para operar de manera decisiva en los dominios terrestre, aéreo, marítimo, ciberespacial y espacial".

Y es que, en el punto 66 de sus conclusiones se recuerda que "el ciberespacio es cuestionado en todo momento, ya que los actores de amenazas buscan cada vez más desestabilizar la Alianza". Por ello, se manifestó el compromiso de los participantes a emplear toda la gama de capacidades para disuadir, defender y contrarrestar todo el espectro de ciberamenazas, incluso considerando respuestas colectivas".

Nuevo concepto de ciberdefensa

Para ello, se aprobó impulsar "un nuevo concepto para mejorar la contribución de la defensa cibernética a nuestra postura general de disuasión y defensa. Integrará aún más los tres niveles de ciberdefensa de la OTAN (político, militar y técnico), asegurando la cooperación civil-militar en todo momento en tiempos de paz, crisis y conflicto, así como el compromiso con el sector privado, según corresponda". Con él, se reafirma "y mejora su Compromiso de Defensa Cibernética", presentando "la nueva Capacidad Virtual de Apoyo a Incidentes Cibernéticos (VCISC) para respaldar los esfuerzos nacionales de mitigación en respuesta a importantes actividades cibernéticas maliciosas". Con ella se quiere "proporciona a los aliados una herramienta adicional de asistencia".

La declaración de la cumbre también anunció nuevas alianzas para "desarrollar asociaciones mutuamente beneficiosas y efectivas, según corresponda, incluso con países socios, organizaciones internacionales, la industria y la academia", así como "promover nuestros esfuerzos para mejorar la estabilidad internacional en el ciberespacio".

Además, se adelantó que, en noviembre próximo, se celebrará la primera Conferencia Integral de Defensa Cibernética de la OTAN en Berlín, reuniendo a los responsables de la toma de decisiones a nivel político, militar y técnico.

Los estadounidenses temen más al ciberterrorismo que a la guerra nuclear, en sus preocupaciones geopolíticas, según una investigación de GALLUP

La empresa de consultoría y análisis **Gallup** ha realizado una amplia investigación sobre las principales preocupaciones geopolíticas entre los estadounidenses.

Un informe en el que el 85% de los participantes consideró una "amenaza crítica", el ciberterrorismo, por encima de otras preocupaciones tradicionales como una guerra nuclear.

Inquietud más allá de la ideología política

La encuesta, realizada en febrero entre más de un millar de habitantes de 50 estados del país, evidenció que esta inquietud va más allá de cualquier ideología política por cuanto, entre republicanos y demócratas calificaron las amenazas cibernéticas como críticas en el 86% de los casos y en aquellos de los que se mostraron independientes esta cifra alcanzó el 79%.

Unanimidad por invertir

Precisamente, uno de los datos más llamativos del informe es la unanimidad por invertir y hacer frente a ciberamenazas, sin importar el partido por el que se apueste.

xMDR

powered by cipher
a Prosegur company

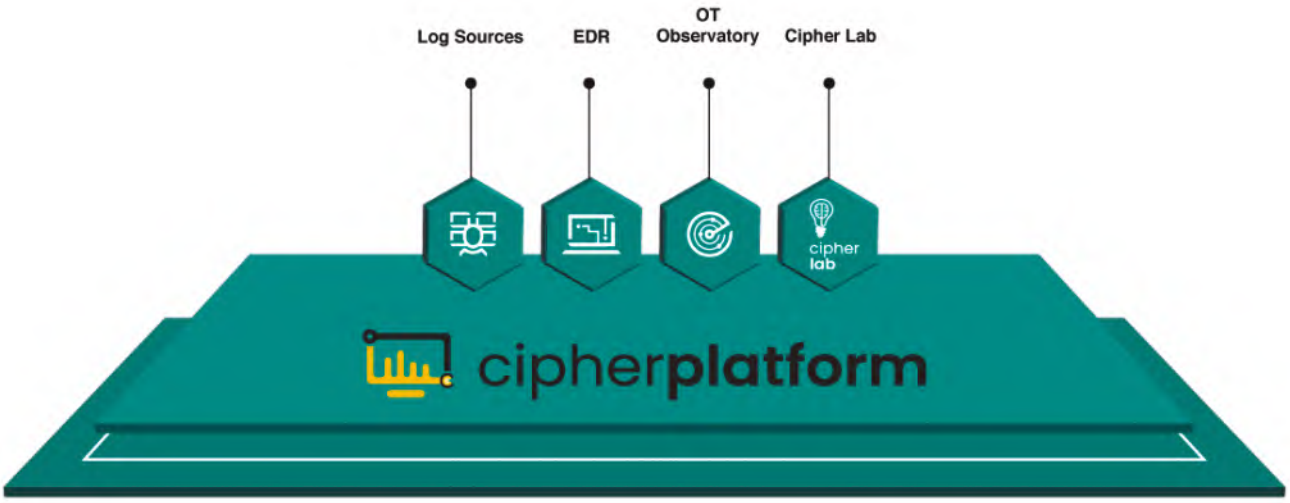
Modelado digital del adversario y aplicación de procesos cognitivos

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

Con **xMDR** consigues:

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

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



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

www.cipherxmdr.io cipher ciphersec ciphersec

Ofrecerá información y facilitará la decisión del Mando en caso de que se produzcan ataques a satélites, también cibernéticos, desde y por satélites enemigos

El primer Escuadrón de objetivos de la FUERZA ESPACIAL estadounidense cobra vida preparado para la guerra espacial y electromagnética

La **Fuerza Espacial de los Estados Unidos** ha activado su primera unidad dedicada a registrar y obtener la máxima información de los satélites de otras naciones y de las estaciones terrestres que los apoyan. El **75.º Escuadrón de Inteligencia, Vigilancia y Reconocimiento** (ISRS) se activó el 11 de agosto en la Base de la Fuerza Espacial Peterson, en Colorado. Esta unidad es parte de la Space Delta 7 y se convierte en el primer escuadrón de objetivos de la rama, diseñado para explorar las capacidades espaciales del adversario y presentar las mejores opciones a la Fuerza Conjunta para, si fuera necesario, neutralizar la amenaza. "Hoy es un momento histórico para nosotros", declaró el teniente coronel **Travis Anderson**. "La idea de esta unidad comenzó hace cuatro años en el papel y, probablemente, ha estado en la mente de varios oficiales de inteligencia de la Fuerza Aérea de EE.UU. incluso desde antes", añadía.

La 75º ISRS tiene como finalidad preparar y presentar paquetes de inteligencia sobre un objetivo adversario y el sistema del que forma parte. Eso podría incluir información sobre un satélite, una estación terrestre o la señal intermedia.

En concreto, analizará sus capacidades espaciales, incluidas las amenazas de fuerzas contraespaciales. Estas últimas, "también llamadas fuerzas de ataque espacial, son capacidades espaciales diseñadas para impedir a EE.UU. utilizar nuestros sistemas satelitales durante un conflicto", se explica en el comunicado. Estos sistemas van desde láseres terrestres que pueden cegar sensores ópticos en satélites hasta dispositivos que pueden interferir señales o realizar ataques cibernéticos para piratear sistemas satelitales enemigos. Algo que preocupa de forma especial, ya que se los sistemas espaciales cada vez son más críticos para la Seguridad Nacional.

"La evaluación de los sistemas espaciales puede ser una tarea difícil", explica el medio especializado **Air and Space Forces Magazine.** "Por ejemplo, los satélites de doble uso pueden presentar un desafío para los oficiales de inteligencia para evaluar sus amenazas: China puede afirmar que un brazo robótico acoplado a un satélite está destinado a la eliminación de desechos espaciales, pero también podría usarse para capturar y perturbar otros satélites". "A medida que las capacidades espaciales de los enemigos adversario se vuelven más sofisticadas, también deben hacerlo las capacidades contraespaciales de Estados Unidos", puntualiza.

El SENADO de EE.UU. abre el camino para crear una rama militar independiente especializada en lo cibernético

El **Senado estadunidense** aprobó, en julio, un proyecto de ley de política de defensa anual que autoriza 816.000 millones de euros para la defensa nacional durante el próximo año fiscal. Conocido como Ley de Autorización de Defensa Nacional (NDAA), ayudará a establecer la agenda política del Pentágono y autorizar cómo el Departamento de Defensa (DOD) puede utilizar los fondos federales.

Comando Cibernético de EE.UU. Foto: **Josef Cole**

En él, según informa The Record, se incluye una enmienda de la senadora **Kirsten Gillibrand** (D-NY), que ordena al DOD recurrir a la Academia Nacional de Administración Pública en aras de realizar una evaluación para establecer un séptimo servicio militar 'ciberespecífico', sumándose a los ya existentes (Ejército, el Cuerpo de Marines, la Armada, la Fuerza Aérea, la Espacial y la Guardia Costera)

La medida busca que la Academia pueda "realizar una evaluación sobre la conveniencia de establecer una Fuerza Armada separada, dedicada a operaciones en el dominio cibernético" y cómo se "compararía en desempeño y eficacia con el modelo actual". Una idea que, al parecer, los responsables del Pentágono no ven de forma positiva, argumentando que el Comando Cibernético de EE.UU. todavía está madurando y podría incitar a algunas de las ramas militares existentes a degradar la misión digital.

"Sin embargo, es precisamente debido a los seis servicios existentes, y a su prolongada incapacidad para proporcionar al Comando Cibernético personal capacitado y equipado para luchar contra adversarios extranjeros en línea, que algunos formuladores de políticas y otras personalidades creen que es hora de, al menos, considerar una Fuerza Cibernética, en lugar de dedicar más tiempo a tratar de alinearlos mediante la legislación", se explica. De cualquier forma, es un paso notable: tras años de debate sobre su idoneidad, el proyecto de ley encarga al Pentágono evaluar si es aconsejable establecer un servicio separado dedicado a las operaciones cibernéticas o perfeccionar el enfoque existente del Comando Cibernético de EE.UU.

La detección de ciberataques se reduce de 21 a 16 días, según el M-Trends 2023 de MANDIANT

La compañía **Mandiant** ha presentado la versión en español de su informe M-Trends 2023 sobre tipos de ataques, sectores más afectados, así como las tácticas, técnicas y procedimientos (TTP) más recientes de los atacantes, entre otros aspectos.

Realizado con datos obtenidos entre enero y diciembre de 2022, en él sus responsables destacan que el año pasado vino marcado por "cómo se desdibujaron los límites entre el ciberespacio y el mundo real, sobre todo en relación con el conflicto en Ucrania, en el que los atacantes intentan causar interrupciones en infraestructuras críticas y, al mismo tiempo, influir en la narrativa".

En cuanto a métricas es relevante que el tiempo de permanencia, de media, se ha reducido de 21 a 16 días, respecto a la anterior edición del informe, "lo que significa que los ataques se están detectando más rápidamente que antes". Además, recuerda que, por primera vez desde 2019, "en todo el mundo, las fuentes externas notifican más a las organizaciones de situaciones de ataque que los equipos internos", lo que supone un avance en ciberprotección a través de la colaboración nacional e internacional.

El documento también explica que los *exploits* y el *phishing* siguen siendo el vector de ataque más utilizado, presentes "en más de la mitad de las intrusiones que investigamos".

BABEL

Business focused CYBERSECURITY

eSOC Centro de Operaciones de Seguridad

eSOC INDUSTRIAL

Red Nacional de SOC

ens

FIRST

CSIRT.es

ISO 20000

ISO 27001-2

babelgroup.com

Hasta noviembre en fase de borrador, se espera la publicación del documento definitivo para principios de 2024

NIST presenta la primera actualización completa en una década de su marco de ciberseguridad dando más peso al Gobierno

Después de considerar los comentarios de la comunidad concernida durante más de un año, el **Instituto Nacional de Estándares y Tecnología** (**NIST**) estadounidense ha presentado una nueva versión, preliminar, de más de 50 páginas, de su *Cybersecurity Framework (CSF) 2.0*, siendo la primera vez que se acomete una actualización tan completa desde que se presentara en 2014. El CSF proporciona orientación de alto nivel, incluido un lenguaje común y una metodología sistemática para gestionar el riesgo cibernético en todos los sectores y ayudar en la comunicación entre el personal técnico y no técnico. En su década de vida ha sido descargado más de dos millones de veces por usuarios en más de 185 países.

Novedades notables

El borrador del CSF 2.0 contiene cambios importantes. Entre ellos, destacan "desde el alcance del marco, que se ha ampliado (explícitamente) para proteger la infraestructura crítica, como hospitales y plantas de energía, hasta para brindar ciberseguridad para todas las organizaciones, independientemente de su tipo o tamaño. Además, la suma de un nuevo pilar, el de la función de gobierno, a los ya existentes - identificar, proteger, detectar, responder y recuperar-, cubre cómo una organización puede tomar y ejecutar sus propias decisiones internas para respaldar su estrategia de ciberprotección", destacan desde el NITS, desde donde también recuerdan que esta versión "enfatiza que la ciberseguridad es una fuente importante de riesgo empresarial, junto con los riesgos legales, financieros y de otro tipo como consideraciones para el liderazgo superior".

Asimismo, el marco busca proporcionar una orientación mejorada y ampliada sobre su implementación, especialmente, para la creación de perfiles que lo adapten a situaciones particulares. "La comunidad ha solicitado ayuda para utilizarlo en sectores económicos y casos de uso específicos. Es importante destacar que el documento incluye ahora ejemplos de implementación para las subcategorías de cada función para ayudar a las organizaciones, sobre todo, a las empresas más pequeñas, a utilizar el marco de manera efectiva", comentan sus responsables.

En este sentido, "un objetivo importante del CSF 2.0 es explicar cómo las organizaciones pueden aprovechar otros marcos, estándares y directrices tecnológicos del NIST y otros lugares, para implementar el CSF. Para ello, se ha lanzado una herramienta de referencia CSF 2.0. Este recurso en línea permite a los usuarios explorar, buscar y exportar los datos de CSF Core en formatos consumibles por personas y legibles por máquinas". En el futuro, esta herramienta proporcionará 'Referencias informativas' para mostrar las relaciones entre el CSF y otros recursos para facilitar el uso del marco junto con otras orientaciones para gestionar el riesgo de ciberseguridad.

Uso ampliado

Con esta versión, "tratamos de reflejar el uso actual del marco de ciberseguridad y también anticipar su uso futuro", explicó **Cherilyn Pascoe** del NIST, desarrolladora principal del marco. "El CSF se creó para infraestructuras críticas, como las industrias bancaria y energética, pero ha demostrado ser útil en todas partes, desde escuelas y pequeñas empresas hasta gobiernos locales y extranjeros. Queremos asegurarnos de que sea una herramienta útil para todos los sectores, no sólo para aquellos designados como críticos". El NIST acepta comentarios públicos sobre el borrador hasta el 4 de noviembre. Sus impulsores planean publicar la versión final de CSF 2.0 a principios de 2024.

La COMISIÓN DE BOLSA Y VALORES de EE.UU. exige que las empresas que coticen notifiquen los ciberataques en un plazo máximo de cuatro días

La **Comisión de Bolsa y Valores** (**SEC**) de EE.UU. aprobó, a finales de julio, varias regulaciones publicadas en su web, así como los formularios que obligará a rellenar, que exigirán que las empresas que cotizan en bolsa divulguen las infracciones de seguridad cibernética que representan un riesgo material para los resultados de una empresa en un plazo máximo de cuatro días hábiles.

Con ellas, el regulador pretende que los inversores tengan mayor transparencia sobre este ámbito. "Ya sea que una empresa pierda una fábrica en un incendio o millones de archivos en un ciberincidente puede ser igual de importante para los inversores", destacó en un comunicado el presidente de la SEC, **Gary Gensler.**

Eso sí, también ha generado un debate en el sector desde que se dio a conocer su borrador en 2022, ya que muchos expertos consideran que identificar qué tipos de infracciones estarían dentro de lo afectado por esta norma puede representar un desafío para muchas empresas, además de complicar su resolución dándolas a conocer antes de terminar su gestión. Hasta ahora, existían reglas en esta línea, pero ésta marca un aspecto determinante: las divulgaciones de incumplimiento serán públicas en los formularios 8-K presentados ante la comisión y estarán disponibles para los inversores. Además, aunque las empresas que cotizan ya están obligadas a informar esta nueva iniciativa acorta notablemente los tiempos de hacerlo.

Obligaciones notables

Entre sus aspectos más llamativos destacan desde su definición más amplia de 'incidente de ciberseguridad', entendiendo como "un evento no autorizado, o una serie de eventos no autorizados relacionados, en o realizados a través de los sistemas de información de un 'registrante' que pone en peligro la confidencialidad, integridad o disponibilidad de los sistemas de información de un 'registrante' o cualquier información que resida en ellos, hasta facilitar, a través de un formulario, los procesos de una empresa, si los hay, para evaluar, identificar y gestionar riesgos materiales de amenazas a la ciberseguridad con suficiente detalle para una inversionista razonable para entenderlos". Además, en su artículo 106 también exige que las empresas describan la supervisión de los riesgos de las amenazas a la ciberseguridad por parte de la junta directiva, entre otros aspectos.

Aiuken Cybersecurity

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

Managed Detection & Response Services
la evolución de un MSSP.

www.aiuken.com

El CNI contará con 30 millones de euros para crear un Centro de Ciberseguridad 5G propio

España ha dado un paso muy importante para fortalecer sus capacidades en ciberprotección de las redes 5G. A finales de agosto, el **Consejo de Ministros** aprobó una transferencia de crédito, por importe de 30 millones de euros, desde el presupuesto del **Ministerio de Asuntos Económicos y Transformación Digital** (MAETD) a **Defensa,** para la ejecución del programa de infraestructura Base 5G para servicios específicos del **CNI** y para la creación de un '**Centro de Ciberseguridad 5G**'.

Este convenio se suscribió entre la **Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales** y el **Centro Nacional de Inteligencia** (CNI), en cumplimiento del Componente 15, Inversión 6, del Plan de Recuperación, Transformación y Resiliencia.

El objetivo principal del convenio es desplegar por parte del CNI su propia red 5G y participar en la creación de un centro de seguridad de 5G, con el objetivo de potenciar las capacidades propias, aumentar el conocimiento de esta tecnología y sus vulnerabilidades y, con ello, mejorar en la seguridad, velocidad, confidencialidad e integridad de las comunicaciones.

En contraprestación, el MAETD realizará una aportación económica en el marco de la ejecución del citado Convenio, que tendrá como objetivo cubrir los gastos que generan las actuaciones referidas anteriormente.

Todas estas actuaciones se enmarcan dentro del Componente 15 'Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G', del Plan de Recuperación, Transformación y Resiliencia y más concretamente en la Inversión 6 'Despliegue del 5G: redes, cambio tecnológico e innovación'. Eso sí, al cierre de esta edición, se desconocía donde estará ubicado el Centro -o si lo hará en las instalaciones del CNI donde ya está el CCN-, así como su organigrama.

OBITUARIO

Ángel Pablo Avilés, alma mater de la iniciativa X1Red+Segura

Pocos profesionales son tan queridos en el sector como **Ángel Pablo Avilés**, Chief Security & Strategy Officer de **SmartHC** desde hace más de un lustro, y conocido por su simpático y popular apodo de 'Angelucho'.

De forma inesperada, en agosto, falleció dejando una trayectoria impecable primero como Guardia Civil, habiendo participado en la guerra de los Balcanes en los años 90, y formando parte del Grupo de Delitos Telemáticos (GDT) de la Guardia Civil de 2007 a 2018, en el que desempeñó gran parte de su labor profesional. Y, en segundo lugar, como impulsor del área de ciberprotección de Smart HC, con notable éxito.

Su capacidad para empatizar, ayudar a menores y padres a proteger su cibermundo le llevó a ser considerado, posiblemente, uno de los ponentes más prolijos en participaciones en congresos de ciberseguridad, a través de ponencias y talleres, en prácticamente todas las citas técnicas del sector en España, dirigidos a padres, madres y niños mostrándoles las bondades, pero, también, los riesgos de Internet. "Somos nuestra peor vulnerabilidad, pero también somos nuestro mejor antivirus", le gustaba recordar al final de sus intervenciones.

Cofundador de la iniciativa **X1Red+Segura,** que en 2019 reconoció con una mención honorífica la buena labor de Revista SIC, y autor de dos libros, sin duda deja un gran vacío en el sector, no solo por su afán divulgador sino, también, por las tutorías de muchos jovenes, algunos de los que fueron detenidos por el GDT, y a los que ayudó a reinsentarse en el ámbito de la ciberseguridad. Desde Revista SIC queremos enviar el pésame y dar un fuerte abrazo a su familia y amigos esperando que, desde donde está, siga con su gran labor protegiendo el cibermundo de los más indefensos.

SIC

Aprobado el estatuto de la AGENCIA ESPAÑOLA DE SUPERVISIÓN DE IA, que tendrá su sede en A Coruña

El **Consejo de Ministros** aprobó a finales de agosto un Real Decreto por el cual se da luz verde al estatuto de la **Agencia Española de Supervisión de la Inteligencia Artificial** (AESIA), que estará ubicada en A Coruña (en la imagen, la presentación de la que fue su candidatura) fruto del trabajo conjunto de los **ministerios de Hacienda** y de **Asuntos Económicos y Transformación Digital**.

Según destacan fuentes de Moncloa, la "transformación digital es prioritaria en la línea de acción del Gobierno, como lo refleja la Agenda Digital 2026". Dicha Estrategia incluye diferentes planes estratégicos, entre ellos la Estrategia Nacional de Inteligencia Artificial (ENIA), que tiene como objetivo "proporcionar un marco de referencia para el desarrollo de una AI "inclusiva, sostenible y centrada en la ciudadanía".

En concreto, esta estrategia, que forma parte de lo anunciado en el Plan de Recuperación, Transformación y Resiliencia (PRTR), pretende situar a España como país puntero en IA y, de hecho, con esta iniciativa seremos "el primer país europeo en tener un órgano de estas características", anticipándonos al Reglamento europeo de IA que, entre otros aspectos, establecerá para los Estados miembros la obligación de seleccionar una 'autoridad nacional de supervisión' que se encargue de supervisar la aplicación de la normativa en esta materia.

Cualquier nube

Transformación empresarial

Fusiones y adquisiciones

Cambios empresariales

Trabajadores híbridos

Automatización

Seguridad que está lista para + Cualquier situación

Nuevos riesgos

Convergencia

Amenazas internas

Lo inesperado

Su próximo gran movimiento

+

Netskope, líder global en ciberseguridad, está redefiniendo la seguridad de la nube, las redes y los datos, para ayudar a las organizaciones a aplicar principios de Zero Trust y proteger su información. La plataforma inteligente Netskope Security Service Edge (SSE) es rápida, fácil de usar y protege las personas, los dispositivos y los datos dondequiera que vayan, pase lo que pase.

Conozca cómo Netskope ayuda a sus clientes a estar listos para cualquier situación, visite netskope.com/es

netskope

Entidades locales y autonómicas, como el País Vasco, Málaga y Valencia, continúan con la puesta en marcha de iniciativas para mejorar su protección

El Gobierno aprueba 70 millones más de inversión en ciberseguridad para entidades locales

El **Consejo de Ministros** autorizó, poco antes de las pasadas elecciones de julio, una transferencia de crédito por importe de 70 millones de euros, del **Ministerio de Política Territorial** al de **Asuntos Económicos y Transformación Digital** para reforzar la ciberseguridad en el marco de la transformación digital y modernización de las entidades locales del Plan de Recuperación, Transformación y Resiliencia, en concreto, de la componente 11, inversión 3. Se trata de un acuerdo que continúa lo marcado en mayo, junto con la **Secretaría de Estado de Digitalización e Inteligencia Artificial**.

Así, según lo aprobado, 60 millones serán para la contratación de los servicios de ciberseguridad de las entidades locales que conforman el ámbito subjetivo de este acuerdo; siete millones para el servicio de apoyo a las entidades locales que se prestará mediante convenio entre la Secretaría General de Administración Digital y el CCN; y otros tres millones para la oficina técnica de la citada Secretaría General en sus labores de apoyo a la implementación del proyecto.

Y a principios de verano, se publicó el concurso de casi 50 millones de euros, por parte del **Ministerio de Asuntos Económicos y Transformación Digital,** para la "implantación de un Centro de Operaciones de Ciberseguridad para Entes Locales único y centralizado que permita coordinar las diferentes actividades encaminadas a la mejora de la ciberseguridad de estas, mediante el despliegue de paquetes de servicios de ciberprotección", con una duración de 24 meses.

El concurso se compone de dos bloques. Por un lado, para la "provisión e implantación del servicio horizontal, global y centralizado, que permita soportar la operativa del **COCS-EELL**". Y, por otro, para "el despliegue y operación de las soluciones de ciberseguridad para los entes locales en cada provincia".

En cuanto a las entidades comunitarias, lo más notable fue la aprobación por parte del Gobierno Vasco de la **Cyberzaintza,** la **Agencia Vasca de Ciberseguridad** (**Euskadiko Zibersegurtasun Agentzia**), para "combatir la ciberdelincuencia de una manera integral y transversal", en Euskadi (ver información ampliada en noticias de este número). Dependerá del Departamento de Seguridad y, en coordinación con la **Ertzaintza**, vigilará y coordinará la lucha contra el cibercrimen y los ciberataques a la ciudadanía, empresas y sector público vasco. Se espera que comience a trabajar en los próximos meses, ya que se basará en lo hecho por el **Basque Cybersecurity Centre** (BCSC).

OCC y Ertzaintza

Precisamente, también en el País Vasco, el ministro del Interior en funciones, **Fernando Grande-Marlaska,** y el vicelehendakari primero del Gobierno vasco**, Josu Erkoreka,** acordaron reforzar la cooperación en la lucha contra la ciberdelincuencia. En concreto, se impulsará una mayor cooperación entre la **Oficina de Coordinación de Ciberseguridad** (OCC) de Interior y la **Ertzaintza,** especialmente, en análisis forenses digitales y ciberinteligencia, además de compartir información sobre las incidencias que puedan afectar a los operadores de servicios esenciales ubicados en la región. Además, se ha aprobado que la Ertzaintza se incorpore al Observatorio de la Cibercriminalidad.

Por su parte, la Presidencia de la **Generalitat Valenciana** y la **Universidad de Alicante** (UA) suscribieron un convenio de colaboración para impulsar acciones de digitalización y ciberseguridad en la comunidad, durante 2023. En concreto, se destinarán 85.000 euros a la UA para fortalecer las políticas digitales y las TIC.

Además, el **Ayuntamiento de Valencia** ha anunciado que reforzará con un millón de euros la ciberseguridad para evitar fraudes como el robo a través de ataques BEC, de cuatro millones de euros a la EMT en 2019.

Por su parte, la **Universidad de Las Palmas de Gran Canaria** pondrá en marcha su propio Centro de Operaciones de Seguridad con el que busca incrementar sus capacidades de prevención, vigilancia y detección de amenazas de los sistemas informáticos y agilizar la respuesta a posibles riesgos.

Crecimiento de Málaga

Por otro lado, el **Clúster de Ciberseguridad de Málaga**, creado a finales del año pasado, ha ampliado su ámbito a toda Andalucía estableciendo también su sede en el **Centro de Ciberseguridad de la Comunidad,** que está en el Palmeral de las Sorpresas, en la ciudad. La idea es que el clúster se alinee estratégicamente con los objetivos del organismo andaluz y se convierta en una "herramienta clave para el desarrollo de la ciberseguridad en la región y su posicionamiento a nivel nacional y europeo".

Por su parte, Aragón inauguró, en verano, su centro de ciberseguridad autonómico en las instalaciones de **Aragonesa de Servicios Telemáticos,** en el Parque Tecnológico Walqa, de Huesca. Con una inversión inicial de 2,4 millones, se integrará a finales de año en la red nacional de SOC, con otra inversión adicional de 2,8 millones.

De otra parte, la **Comisión de Transformación Digital** de la **Cámara de Comercio de Castellón** ha acordado la realización de diferentes acciones encaminadas a tratar temas de gran relevancia empresarial, como la ciberseguridad, la inteligencia artificial o las tecnologías emergentes, durante el segundo semestre del año. Entre otras iniciativas, el próximo 18 de octubre se presentará el 'Programa de Ciberseguridad 2023' y cómo las empresas de la región pueden aprovechar sus recursos. En formación, **Castilla-La Mancha** ha puesto en marcha 38 nuevos ciclos y seis cursos de especialización en FP, muchos de ellos centrados en digitalización y ciberseguridad.

Ciberprotección consistorial

Palencia, una vez conseguida la certificación en el ENS, ha puesto en marcha su Oficina Técnica de Seguridad de la Información, además de un SOC. Por su parte, **Santa Cruz de Tenerife** dedicará 66.000 euros a contar con un SOC, que ha sido adjudicado a **Sothis Servicios**, con fondos europeos.

Como curiosidad, el **Ayuntamiento de Granada** realizó una simulación de un ataque de *phishing* por correo-e enviado a sus 2.200 trabajadores de los que 600 lo abrieron y facilitaron sus claves, según explicó el responsable del área de Innovación, el concejal **Francisco Herrera.** Otros ayuntamientos, como el **Paterna** (Valencia), también se han sometido a pruebas de *hacking* ético para concienciar y sensibilizar sobre la importancia de la protección de datos y la ciberseguridad.

Descubre nuestro valor

Westcon

Potenciamos tu negocio con las mejores soluciones IT

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

www.westconcomstor.com

GALICIA presenta su estrategia de ciberseguridad 2030 este otoño, da su 'ok' al CECIGA y anuncia CIBER.gal 2023

Galicia es pionera en materia de ciberseguridad gracias al constante trabajo y esfuerzo de la **Agencia para la Modernización Tecnológica de Galicia** (**Amtega**) por situar esta tecnología y capacidades en un lugar central y prioritario en el día a día de ciudadanos y profesionales. Una de sus apuestas más recientes es la creación de la **Estrategia Gallega de Ciberseguridad 2030**, que con el fin de tener en cuenta todas las perspectivas, experiencias y necesidades, como novedad se desarrolló facilitando la colaboración de todas las entidades adheridas al Nodo CIBER.gal, las cuales decidieron aportar su grano de arena. Así, las líneas de acción más destacadas de esta nueva estrategia que próximamente será presentada (prevista para el último trimestre de 2023), son continuar formando y concienciando en ciberseguridad a toda la sociedad, apoyar a empresas y ciudadanos para un mayor nivel de protección, colaborar y cooperar frente a la ciberdelincuencia, poner en marcha el **Centro de Excelencia en Ciberseguridad de Galicia** (el **CECIGA**), impulsar la innovación, el desarrollo y la investigación aplicada a la ciberseguridad, promover el talento especializado e impulsar a Galicia como parte de la red de centros de competencias en ciberseguridad. Particularmente para el sector público, la estrategia también abarcará líneas enfocadas hacia la promoción y homogenización de los servicios y herramientas de ciberseguridad en las AAPP, optimizar las operaciones en ciberseguridad, impulsar y fortalecer el CSIRT.gal, mejorar el gobierno de la ciberseguridad en la autonomía, promover el cumplimiento normativo en materia de seguridad y definir e implantar el plan director de seguridad de la Xunta de Galicia.

Imágenes emuladas de lo que será el CECIGA en 2024

El CECIGA toma impulso

La Xunta anunció en agosto la contratación de las obras para la construcción del **Centro de Excelencia en Ciberseguridad de Galicia (CECIGA)** en los terrenos ourensanos del Parque Tecnológico de Galicia, en San Cibrao das Viñas, que supondrá una inversión de más de 6 millones de euros.

Como ya también adelantara SIC en ediciones anteriores, nace con el objetivo de fortalecer "la ciberseguridad" en el entorno de la administración pública, de la ciudadanía y de las empresas; apoyar la innovación en el sector productivo mediante el logro de la excelencia en la investigación; "fomentar el desarrollo de proyectos vinculados a la ciberseguridad" y promover el emprendimiento en este ámbito.

El departamento de Infraestructuras de la Xunta licitó las obras a lo largo de dicho mes, para poder adjudicarlas en otoño y empezarlas a principio de 2024. El objetivo con el que se trabaja es poder poner en marcha el nuevo centro en 2025, ya que las obras cuentan con un plazo de ejecución de 20 meses.

El edificio que albergará el CECIGA se construirá en la parcela 3Y de la Tecnópole, con una superficie útil de más de 2.100 m². Se configura en cuatro bloques rotando sobre un espacio central, de planta circular y formato poligonal, que albergará las funciones para las que es concebido.

El edificio se utilizará también con el objetivo de fomentar la I+D+i y el emprendimiento, en un modelo de colaboración público-privada. El futuro centro se va a encargar de supervisar "la ciberseguridad de las administraciones públicas" a través de una sala de monitorización en la que se controlarán los sistemas informáticos de las entidades interesadas y se detectará cualquier alerta. El recinto contará además con una sala específica para casos de crisis.

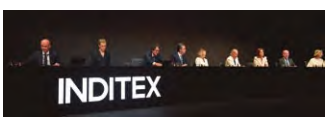
Además, dispondrá de un centro demostrador en el que pondrán a prueba nuevas tecnologías para después mostrarlas al sector productivo que va a ser destinatario de las mismas o con laboratorios y otros espacios que pueden usar las empresas y emprendedores.

El III Encontro CIBER.gal, el 2 y 3 de noviembre en Santiago

La tercera edición del **Encontro CIBER.gal**, el evento de referencia en materia de ciberseguridad gallego, se celebrará los días 2 y 3 de noviembre en la Ciudad de la Cultura de Galicia, en Santiago de Compostela. De nuevo, será desarrollado presencialmente aunque para aquellos que no puedan acudir se retransmitirá en modalidad *online*,

INDITEX anuncia en su junta de accionistas un grupo asesor especializado en ciberprotección

Inditex ha querido reforzar su ciberprotección a través de la creación de un nuevo comité asesor de ciberseguridad. La compañía ha creado un órgano permanente de carácter asesor y consultivo integrado por expertos en materia de seguridad de la información, y muy especialmente de ciberprotección, según se ha dado a conocer en su junta general de accionistas.



El objetivo es "reforzar el proceso de toma de decisiones e impulsar la estrategia del grupo en esta materia", han destacado desde la Junta, a la vez que se recuerda que, con esta iniciativa, se busca "poner todos los medios posibles para proteger los datos y la información sensible no solo de las empresas sino, también, de sus grupos de interés, incluyendo clientes, proveedores y accionistas".

wisesecurity
GLOBAL
A Var Group Company

DISCOVER OUR UNIVERSE

DISCOVER WISE SECURITY GLOBAL

We build CyberTrust. We create CyberSecurity

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

FRAUDFENSE, la apuesta del SANTANDER, BBVA y CAIXABANK para compartir información y datos relevantes para hacer frente al fraude financiero

Banco Santander, **BBVA** y **CaixaBank** se han unido para hacer frente a uno de los grandes retos a los que se enfrenta el sector bancario, el fraude financiero.

Las tres entidades españolas están trabajando en herramientas para intercambiar información y datos relevantes que ayuden a prevenir el crimen financiero.

En este contexto, bajo el nombre de **FrauDfense**, se ha constituido la compañía que aglutinará iniciativas antifraude de las tres entidades y que ha sido 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, será su director general.

Carlos Requena, director general de FrauDfense

En una primera fase, la alianza abordará la creación de una herramienta de intercambio de información -en la nube, en demarcación europea- que permitirá compartir 'modus operandi' fraudulentos y medidas de respuesta satisfactorias frente a ellos.

En todo momento preservará la seguridad y la privacidad de la información compartida.

Un objetivo común

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.

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.

Banco Santander, BBVA y CaixaBank ocupan los puestos más altos del sector financiero nacional y despliegan sus productos y servicios más allá del mercado español.

La unión de estas tres entidades para luchar de forma conjunta contra el fraude financiero supone un importante avance en España, con la puerta abierta a la ampliación de la colaboración.

Banco Santander cuenta con una presencia relevante en una decena de mercados internacionales, 161 millones de clientes y una posición como uno de los grandes bancos del mundo por capitalización bursátil.

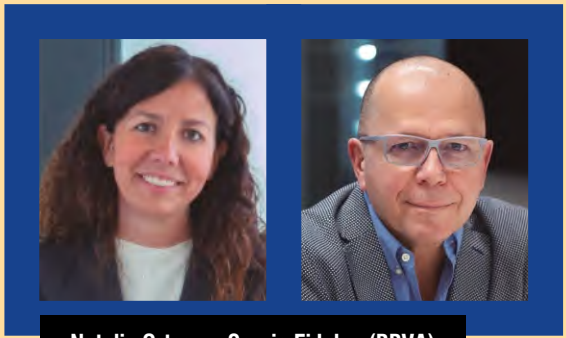
A la entidad liderada por Ana Botín se suma BBVA, con más de 68 millones de clientes y presencia en más de 25 países.

A estos dos gigantes financieros se suma también CaixaBank, con más de 20 millones de clientes y la mayor red de oficinas y cajeros en España y Portugal, con una fuerte presencia en la España rural.

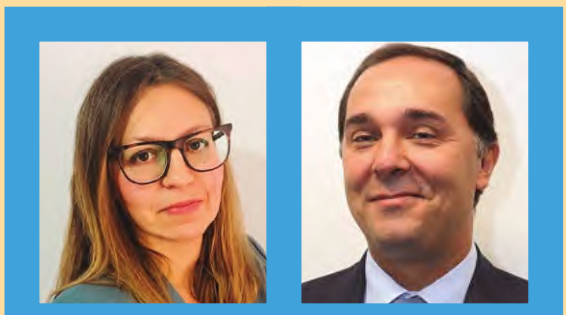
CONSEJO DE ADMINISTRACIÓN

Además del citado **Carlos Requena** como primer ejecutivo, FrauDfense cuenta con un consejo de administración compuesto por dos representantes de cada entidad: **Carles Solé**, CISO de Banco Santander España, 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 Gobierno del Fraude, y **Lorenzo Malo**, CISO de CaixaBank. Ortega, de BBVA, es la primera presidenta de FrauDfense, cargo que se irá renovando cada dos años entre los miembros de las tres entidades integrantes del proyecto.

Carles Solé y Daniel Barriuso (Santander)



Natalia Ortega y Sergio Fidalgo (BBVA)



Sofia Karapatsiou y Lorenzo Malo (CaixaBank)

Adelántate al fin de soporte de **Windows Server 2012**

En octubre de 2023 muchas organizaciones pueden convertirse en el objetivo principal para los ciberataques. **Virtual Patching** actúa como medida de seguridad contra las amenazas:

- Gana tiempo adicional
- Evita tiempos de inactividad innecesarios
- Mejora el cumplimiento de la normativa
- Proporciona una capa adicional de seguridad
- Proporciona flexibilidad

Explora las funcionalidades de Virtual Patching y protege tu empresa mitigando riesgos asociados a vulnerabilidades

Escanea el código QR para más información ▶

INDRA se refuerza con ICA, a través de SIA, pero ESPAÑA pierde 'ADN nacional': la italiana SESA GROUP se hace con WISE SECURITY GLOBAL y la holandesa COMPUTEST SECURITY con INCIDE

El gasto en ciberseguridad en el primer trimestre de 2023 creció a más de 16.500 millones de euros en todo el mundo, un aumento del 12,5 % en comparación con el mismo periodo del año anterior, según Canalys. Por áreas, la inversión en protección de la identidad aumentó un 14,3% y la de los teletrabajadores también ha impulsado, con un 16% más de gasto, la de servicios de seguridad perimetral (SSE). Asimismo, es notable que 12 proveedores de ciberprotección supongan el 48,6% del mercado.

El mercado no ha dejado de moverse aunque, según algunos analistas, vive un momento de ralentización. En el segundo trimestre de este año, se registraron 148 acuerdos de financiación, un 35% menos respecto a los 228 en el mismo periodo del año anterior, marcando el nivel más bajo en años, según datos de **Crunchbase.** Igual ha pasado en las operaciones de capital riesgo en el sector, que se redujeron a casi 1.420 millones de euros en el segundo trimestre de 2023, una caída del 63% respecto al mismo periodo anterior, según el analista.

Indra se hace con ICA, a través de SIA, y valora la adquisición de Epicom, Factum compra activos de Core Netsworks, Eulen y Asecco abren nuevas líneas de ciberprotección, Grupo Sesa se hace con Wise SG, Computest con Incide; fuera de España Thales adquiere Imperva y Tesserent, Outpost24 a Sweepatic, Bitdefender a Horangi Cyber Security y el fondo TPG se queda con la unidad de gobiernos e infraestructura crítica de Forcepoint. S2 Grupo se refuerza con una inyección de 20 millones de capital y Xygeni cuatro millones, entre otras operaciones de interés.

De cualquier forma, sigue habiendo adquisiciones y fusiones notables. En España, ha destacado la compra por parte de **Indra** de **ICA Sistemas y Seguridad** (ICASyS), a través de **SIA.** Asimismo, **Evolutio** se ha hecho con la tecnológica española **Dagram.** Por otra parte, la CNMC autorizó la operación de concentración por la que el mayorista **V-Valley** se ha hecho con la compañía **Lidera** por algo más de cinco millones de euros. **Factum** ha adquirido activos de **Core Networks**, centrada en la gestión de identidades y de accesos.

Asimismo, **Wise Security Global** se ha integrado en **Var Group,** propiedad de la multinacional italiana **Sesa Group.** Una operación con la que la empresa española refuerza su "posición en el mercado y abre nuevas oportunidades de crecimiento". Por su parte, la holandesa **Computest Security** ha comprado **Incide**, una firma española especializada en respuesta a incidentes y la protección de red, al frente de la que está como CEO y fundador **Abraham Pasamar.** Además, **Advantio** se incorporará al **Grupo Integrity360** para ser un referente europeo en este ámbito, bajo la denominación **Advantio Joins Integrity360**. También, ha trascendido, según **Infodefensa,** que **Indra** ha reactivado las negociaciones para la compra de **Epicom** a **Duro Felguera**. Además, ha sido relevante la creación de nuevas líneas de ciberseguridad tanto por parte de la compañía **Eulen,** como por **Asseco**, que ha puesto en marcha un *holding* dentro del que tendrá una empresa específica en este ámbito: **Sora Anzen Company.** Por su parte, **Babel** continúa con su internalización con la compra de la consultora mexicana **Ironhit**.

Intensa actividad

Fuera de nuestras fronteras, ha trascendido la compra de la estadounidense **Imperva** por parte de **Thales,** propietaria de la vasca **S21sec,** por más de 3.200 millones de euros, así como de la australiana **Tesserent**, por 119 millones. Con estas operaciones estratégicas, la compañía gala prevé generar con su negocio de ciberseguridad más de 2.400 millones de euros este año. **Outpost24,** propietaria de la española **Blueliv**, ha comprado a la belga **Sweepatic**, que posee una plataforma de gestión de superficie de ataque externa (EASM).

Además, **Domainr,** que proporciona un medio programable en tiempo real para comprobar la disponibilidad y el estado de los dominios, ha sido adquirida por **Fastly,** que también ha anunciado la disponibilidad general de su entidad certificadora de TLS (AC), **Certainly,** presentada en febrero de este año con disponibilidad limitada. Por su parte, **Check Point** se ha hecho con la *startup* israelí **Perimeter 81**, por 453 millones de euros, una cifra muy alejada de su valoración hace 14 meses que superaba los 920 millones. Su objetivo es fortalecer la seguridad de la red para trabajadores remotos e híbridos. **Bitdefender** ha anunciado que se hará con **Horangi Cyber Security**, de Singapur, para incorporar sus tecnologías de Cloud Infrastructure Entitlement Management (CIEM) y Cloud Security Posture Management (CSPM), en su plataforma de análisis de seguridad y riesgo unificado GravityZone.

La firma de inteligencia empresarial **CyberRisk Alliance** ha comprado **LaunchTech Communications,** una agencia de comunicaciones y relaciones públicas especializada en compañías de tecnología y seguridad cibernética. **Snyk** se hizo con la israelí **Enso Security**, por unos 45 millones de euros, centrada en la gestión de posturas de seguridad de aplicaciones (ASPM). Por su parte, el gigante de capital privado **TPG** ha anunciado que adquirirá la unidad de negocios de Gobiernos Globales e Infraestructura Crítica (G2CI) de **Forcepoint**, por la que pagará en torno a 2.230 millones de euros. Así esta área, creada en 2018, se dividirá quedando como una entidad independiente que impulsará la oferta SASE de la compañía con nuevas capacidades e integraciones de terceros. Se espera que la operación se cierre en el cuarto trimestre de 2023.

Rondas de inversión

En este apartado, ha destacado que **S2 Grupo** recibió 20 millones de un préstamo sindicado para desarrollar su plan estratégico. La operación ha sido coordinada por **Banco Sabadell** y cuenta con el apoyo de **Banco Santander, Caixabank, BBVA** y **Deutsche Bank.** La española **Xygeni**, centrada en soluciones SaaS para la seguridad de la cadena de suministro de software, cerró una ronda de financiación que se concreta en una inversión de cuatro millones de euros, lo que la permitirá internacionalizarse en Europa y EE.UU., salto cualitativo previsto para fines de 2023. Quizá la operación más llamativa en rondas de financiación fuera de España ha sido la de la *startup* israelí **Cyera**, fundada en 2021, que logró alrededor de 90 millones de euros de la serie B. Además, **OneTrust** consiguió recaudar 138 millones de euros.

Symantec™

Data-Centric SASE

Westcon | Symantec by Broadcom Software

Sepa más acerca de Symantec y su
Secure Web Gateway escaneando el QR code:

Contacto:

www.westconcomstor.com/es/es/vendors/symantec.html

symantec.es@westcon.com

broadcom.com

La entidad ha colaborado en el desarrollo de una herramienta para que compartir datos de ciberprotección y fraude sea más flexible y seguro

CAIXABANK participa en el consorcio europeo CONCORDIA para definir las bases del ecosistema europeo de ciberseguridad

CaixaBank ha participado, junto a otras 59 entidades de 21 países europeos, en el consorcio **Concordia**, dotado por la **Comisión Europea** con 16 millones de presupuesto, cuyo objetivo ha sido definir las bases del ecosistema europeo de ciberseguridad. El proyecto, enmarcado en el programa Horizonte 2020 que arrancó en enero de 2019 y ha finalizado este año, se ha centrado en la definición de una hoja de ruta para mejorar la coordinación y comunicación entre organismos, empresas y Estados de Europa en esta materia.

Dentro del consorcio, CaixaBank ha participado, junto con **Atos IT Solutions and Services Iberia**, en el desarrollo de una herramienta para que compartir datos relacionados con la ciberprotección y el fraude financiero (como casos de *phishing,* cuentas bancarias, tarjetas…) sea más flexible y seguro.

En concreto, la entidad, el único banco español integrante de este proyecto, ha ayudado a configurar esta herramienta para poder, por ejemplo, definir con mucho detalle qué información es necesaria anonimizar y grupos concretos con quién compartirla. Por ello, el proyecto abarca diferentes ámbitos que van desde el de investigación e innovación, hasta el de educación, economía, inversiones, asuntos legales y políticos, normalización, certificación y, también, el de desarrollo del ecosistema europeo de la ciberseguridad.

Proyectos europeos de investigación

Además de este consorcio, CaixaBank ha participado en otros proyectos europeos de los que **SIC** se hizo eco en su número 154, a través de un artículo de **Ramón Martín de Pozuelo y Marino Maawaad,** dentro del programa Horizonte 2020, dotado con 80.000 millones de euros, ampliados a 95.510 millones en el actual plan 'Horizonte Europa' para 2021-2027 con el objetivo de garantizar que Europa cuente con ciencia "de primer nivel" y elimine las barreras para la innovación.

En total, CaixaBank ha conseguido formar parte de diez consorcios en los últimos años, con una financiación recibida en innovación tecnológica y de ciberseguridad superior a los 2,5 millones de euros. Entre ellos, figuran otros proyectos como **AI4CYBER**, **Rewire** y **Green.dat.ai,** entre otros.

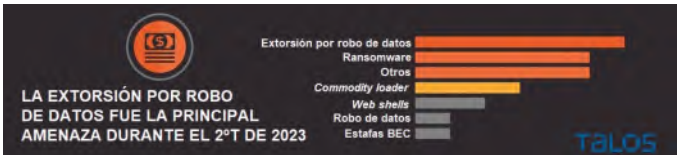
La UNIÓN EUROPEA pondrá en marcha, en dos años, un sistema de verificación de documentos digitales con notable presencia de la industria española

Cinco organizaciones españolas (**FNMT, Izertis, Validated ID, Gataca** y **Logalty**) participarán de forma activa en el proyecto europeo 'EBSI Vector', con 10 millones de euros de presupuesto, integrado por 50 socios de 20 países, para simplificar el proceso para que los ciudadanos vean reconocidas y aceptadas sus credenciales en distintos países, según Cinco Días. Se trata de una iniciativa comunitaria que busca poner en marcha un sistema de verificación de documentos digitales, con tecnología blockchain, para toda la UE. Entre otros usos, por ejemplo, permitirá que diferentes documentos oficiales, como el título universitario, pueda llevarse en el móvil (en una *wallet* digital) siendo consultado y válido en todos los países. Un reto del que se hizo eco en profundidad la abogada Paloma Llaneza, CEO de Razona LegalTech, en **IdentiSIC 2022.**

En concreto, la iniciativa se centrará en tres ámbitos, el educativo, para el uso digital de las titulaciones, el de la seguridad social, permitiendo disponer en el móvil de la tarjeta sanitaria europea y, también, para registros comerciales, que permiten a las personas jurídicas actuar como tal. En definitiva, se trata de desarrollar una solución, en un plazo de dos años, que sea utilizable en toda Europa, escalable y que pueda crecer con la integración de más documentos.

La extorsión por robo de datos crece, según CISCO, que amplía su acuerdo en ciberresiliencia con KYNDRYL

Durante el segundo trimestre del año, **Cisco** respondió a un creciente número de incidentes de extorsión por robo de datos, constituyendo la principal ciberamenaza en dicho periodo al suponer el 30% del total de interacciones del Centro de Respuesta. Los ciberdelincuentes roban la información de la víctima y amenazan con filtrarla o venderla a menos que se paguen sumas variables de dinero, lo que elimina la necesidad de implementar *ransomware* o cifrar los datos. Esto difiere del método de *ransomware* de doble extorsión, con en el que los adversarios extraen y cifran archivos y exigen un pago para revelar la clave de descifrado. La extorsión por robo de datos no es un fenómeno nuevo, pero la cantidad de incidentes de este trimestre sugiere que los actores de ciberamenazas lo ven cada vez más como un medio viable para recibir un pago final.



Los grupos de extorsión RansomHouse y Karakurt fueron los más activos, generalmente obteniendo acceso a entornos a través de cuentas válidas, *phishing* o explotación de vulnerabilidades. Continuando con la tendencia del primer trimestre del año, el sector de atención sanitaria fue nuevamente el vertical más atacado.

Acuerdo con Kyndryl

En paralelo, Cisco anunció una asociación tecnológica ampliada con **Kyndryl** para prestar servicios de ciberresiliencia.

A través de este acuerdo, utilizarán la completa cartera de software, hardware y equipos de red de Cisco con el marco de ciberresiliencia de Kyndryl para ayudar a los clientes a abordar y responder de forma proactiva a los incidentes cibernéticos.

CONOZCA EL

MÁS COMPLETO

HEALTH-CHECK

DE

CIBERSEGURIDAD

LEET SECURITY

SOLICITE SU DISCOVERY SESSION EN:

WWW.LEETSECURITY.COM

info@leetsecurity.com

915798187

CORREOS, pionera en el sector en certificarse en el nuevo Esquema Nacional de Seguridad con el fin de mejorar la madurez de sus procesos

Con el objetivo de mejorar la madurez de los procesos de seguridad de la información y aportar valor y confianza a todos sus clientes desde la perspectiva de la ciberseguridad, **Correos** obtuvo en junio la nueva certificación del ENS (Esquema Nacional de Seguridad) con las exigencias del Real Decreto 311/2022 del 3 de mayo, por el que se regula el ENS en el ámbito de la Administración Electrónica y que sustituye al Real Decreto 3/2010, de 8 de enero, convirtiéndose así en pionera en el sector del transporte/paquetería/logística en obtener este modelo de buenas prácticas.

Como es sabido, este nuevo Esquema Nacional de Seguridad del RD 2022 tiene como objetivo garantizar la seguridad de la información en el sector público y engloba hasta 75 medidas actualizadas, clasificadas en marco organizativo, marco operacional y medidas de protección.

La obtención de esta certificación proporciona a Correos un marco normativo de control que permite optimizar la gestión de los procesos y la protección frente a amenazas internas y externas cuidando su principal activo: la información.

La certificación en el nuevo ENS supone un valor añadido en términos de seguridad de la información para empleados, proveedores, clientes, colaboradores y para el conjunto de la sociedad. Como resultado, Correos se ha convertido en la primera empresa de la SEPI y del sector en obtener la certificación de la actualización este importante marco normativo.

Esta certificación forma parte del compromiso de Correos en materia de ciberseguridad, ya que diariamente la compañía se esfuerza en fortalecer y mejorar sus procesos de seguridad de la información. Tanto es así que, de cara al futuro, continuará potenciando su estrategia de ampliar la obtención de certificaciones para estar a la vanguardia de las nuevas exigencias y garantizar la protección de la información a todos los niveles.

Correos nace hace más de 300 años y, tras una continua adaptación al mercado, hoy es el operador líder del sector en España. Actualmente, la estrategia de la compañía está centrada en la internacionalización, la sostenibilidad y la transformación digital. Con más de 48.000 profesionales, la empresa presta servicio a la ciudadanía a través de su red de 2.389 oficinas, distribuyendo cerca de 6,6 millones de envíos diarios. El Grupo Correos cuenta con tres filiales: **Correos Express** dedicada a la paquetería urgente, **Nexea** especializada en soluciones multicanal para las comunicaciones masivas de las empresas y **Correos Telecom** encargada de la gestión y comercialización de infraestructuras de telecomunicación. Perteneciente al **Grupo SEPI**, forma parte de un *holding* empresarial que abarca un total de 15 empresas públicas.

Jesús Mayor, Jefe de Área de Seguridad de la Información de Correos

"Con las certificaciones queremos homologar nuestro nivel de madurez con los marcos de referencia de nuestro entorno, con el objetivo de generar confianza y transmitir fiabilidad a nuestros clientes"

– ¿Qué entidad en concreto ha llevado a cabo la certificación?

– El proceso de adecuación a la nueva versión del Esquema que está regulada en el Real Decreto 311/2022, se estuvo trabajando con la empresa Babel en tanto que la auditoría de certificación se llevó a cabo con Aenor. Actualmente es la empresa certificadora que Correos utiliza tanto para las nuevas certificaciones como para la renovación de las actuales.

– En su opinión profesional como CISO, ¿cuáles son las principales mejoras que la adopción del ENS propicia en lo que a su actividad específica de ciberprotección concierne?

– Con las certificaciones en materia de Ciberseguridad no estamos buscando de manera directa mejorar en Seguridad, sino homologar nuestro nivel de madurez con los marcos de referencia de nuestro entorno, con el objetivo de generar confianza y transmitir fiabilidad a nuestros clientes.

Jesús Mayor (Correos)

Este hecho no es incompatible con el aprovechamiento que hacemos del proyecto de Certificación buscando consolidar nuestros procesos y desarrollar las oportunidades de mejora que se detectan.

– A futuro, ¿qué otras certificaciones concretas podrían estar evaluando llevar a cabo?

– Estamos evaluando la posibilidad de certificarnos en el medio plazo en la ISO 27701 de Privacidad, aunque nuestra estrategia no es solo crecer en marcos de Certificación que puedan ser "atractivos" para el negocio, sino también ampliar el alcance de nuestras actuales certificaciones con nuevos procesos y/o servicios de nuestro Ecosistema Digital, en los que el atributo de la Seguridad se perciba demandando o pertinente. Un ejemplo de esta estrategia fue la decisión en 2022 de incluir en nuestros alcances la "Solicitud del voto por Correo" y que, contra todo pronóstico, se convirtió en un asunto mediático durante las pasadas elecciones municipales.

kartos©

#AlwaysWatching

XTI watchbots

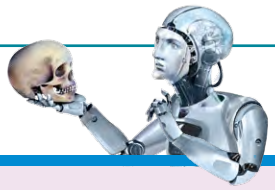
Plataforma de cibervigilancia e inteligencia

XTI
Extended CTI
Watchbots Platform

- EASM (External Attack Surface Management)
- DRPS (Digital Risk Protection Services)
- SRS (Secutity Rating Services).

www.enthec.com

CAVILACIONES SEGURAS



De Nerd-CISO a Pulgar-CITO

Comienzo hoy mis cavilaciones hablando de la historia de la tecnología en las empresas. Los más antiguos del lugar recordarán aquellos tiempos en los que la máquina del fax era tan imprescindible como es ahora el correo electrónico. Este ejemplo me sirve para demostrar cómo la tecnología ha pasado de ser un elemento importante a convertirse en una pieza imprescindible de todos los procesos que hoy en día conforman una organización.

El aumento en importancia de la tecnología ha requerido que la posición del responsable de tecnología en una empresa haya también subido posiciones en el escalafón jerárquico empresarial. Esta adaptación, sin embargo, es más lenta que la pervasividad de la tecnología. Aún es frecuente ver a directores de tecnología, los llamados CIOs, reportando al director de operaciones, el COO, quien reporta a su vez al órgano de dirección ("management body").

PulgarCito

Con la legislación europea en ciberseguridad, el foco se coloca en la gestión del riesgo tecnológico y la naturaleza "colectiva" de su conocimiento en la alta dirección. No hay una mención "individualizada" para un miembro del órgano de dirección en concreto. Será interesante ver a cuántos CISOs encontraremos en tan altas jerarquías, y cuántos seguirán trabajando como modestas anclas de confianza en jerarquías inferiores (los Pulgar-CITOs).

La seguridad informática dio sus primeros pasos, como no podía ser de otro modo, dentro de los departamentos de tecnología. El responsable de seguridad, el CISO, ha reportado tradicionalmente al responsable de tecnología (CIO), quién "traducía" a la alta dirección los mensajes del CISO, carente de habilidades sociales ("Nerd-CISO"). Aún es muy frecuente encontrar organizaciones en las que el CISO está a dos o tres niveles de reporte del consejo: CISO a CIO y éste a COO.

La llegada de legislación europea enfocada en la ciberseguridad nos trae interesantes novedades. En concreto, NIS2 es la directiva para mejorar la ciberseguridad en la UE. Su fecha límite de transposición a la legislación nacional es septiembre de 2024. DORA es el reglamento enfocado a la resiliencia digital de las entidades financieras, cuyos estándares técnicos serán de obligado cumplimiento en enero de 2025.

NIS2, en su artículo 20, indica que "los Estados miembros garantizarán que los miembros de los órganos de dirección de las entidades esenciales e importantes deban asistir a formaciones … para adquirir conocimientos y destrezas … que les permitan detectar riesgos de ciberseguridad" y, en el recital 38, menciona que los estados miembros "deben poder designar o crear una o varias autoridades nacionales competentes encargadas de la ciberseguridad".

DORA, en su artículo 5, estipula que el órgano de dirección "asume la responsabilidad última de gestionar el riesgo tecnológico" y sus miembros mantendrán al día de manera activa conocimientos y capacidades suficientes para poder comprender y evaluar el riesgo tecnológico. Es más, dicho órgano creará un cargo, o designará a un miembro de la alta dirección ("senior management"), como responsable de supervisar la exposición al riesgo del uso de proveedores de tecnología.

Dos observaciones: primera, el foco se coloca en la gestión del riesgo tecnológico y, segunda, la naturaleza "colectiva" de su conocimiento en la alta dirección. No hay una mención "individualizada" para un miembro del órgano de dirección en concreto. Será interesante ver a cuántos CISOs encontraremos en tan altas jerarquías, y cuántos seguirán trabajando como modestas anclas de confianza en jerarquías inferiores (los Pulgar-CITOs).

Imagino que la clave es la responsabilidad. Recordemos que la CISO es aquella o aquel profesional que continúa siendo funcional aún en momentos críticos, como es en pleno ataque ciber a la empresa: un líder que tendrá que seguir afilando su "hacha comunicativa" con sus superiores mientras gestiona el riesgo tecnológico desde la confianza.

Dr. Alberto Partida

linkedin.com/in/albertopartida

C1be3rW4ll: MARLASKA clausuró su tercera edición, con más de 155.000 asistentes, destacando el reto de parar amenazas "cada vez más sofisticadas y complejas"

El ministro del **Interior** en funciones, **Fernando Grande-Marlaska,** clausuró en junio la tercera edición de **C1be3rW4ll,** con más de 200 ponentes, en un acto en el que, acompañado por el director general de la **Policía Nacional**, **Francisco Pardo**, destacó que "cuando hablamos de ciberseguridad, todas y todos somos imprescindibles". Con más de 6.500 participantes presenciales y más de 150.000 alumnos de Policía de 82 países distintos, el congreso, impulsado por Policía Nacional y celebrado en su Escuela Nacional en Ávila, tuvo como título 'Futuro inmersivo'.

Así se abordó de forma especial los desarrollos de IA y realidad virtual y aumentada que afectan ya a la seguridad colectiva y cuya irrupción en los procesos de digitalización es la causa de que "el reto que tenemos por delante sea todavía más grande", recordó Grande-Marlaska. "Son amenazas cada vez más sofisticadas y complejas que nos obligan a todas las instituciones concernidas, públicas y privadas, a un esfuerzo añadido para adquirir la preparación necesaria y ser capaces de neutralizar esos riesgos", resaltó.

BeDisruptive™

¡Emprende tu Road to SASE!

Revolucionamos el mundo de la seguridad con el lanzamiento de Managed SASE.

Gestión unificada y plena visibilidad de tus políticas de acceso a las aplicaciones y datos de tu organización, alcanzando el máximo nivel de seguridad y control, sin importar las complejidades del entorno.

Road to SASE by BeDisruptive

www.bedisruptive.com

Además, el Mando Espacial, del Ejército del Aire, 'despegará' en otoño

El MANDO CONJUNTO DEL CIBERESPACIO ya tiene en marcha su escuela militar para formar a soldados y cabos en este ámbito

Las instalaciones del **Mando Conjunto del Ciberespacio** (**MCCE**) ya acogen el primer curso de su centro dedicado a la formación cibernética para integrantes de la Escala de Tropa y Marinería (soldados y tropa), en su cuartel de Retamares, en Madrid. Se trata de un centro docente militar conjunto para militares del Ejército de Tierra, de la Armada y del Ejército del Aire en capacidades de ciberdefensa.

Con él, buscan ofrecer una capacitación a los que pidan plaza en la unidad desde la que se planean, dirigen, coordinan, controlan y ejecutan las operaciones militares en el ciberespacio para asegurar la libertad de acción de las Fuerzas Armadas en este ámbito. Eso sí, para ser admitidos en la formación, los aspirantes deben acreditar ciertos conocimientos y cursos relacionados con la ciberdefensa.

Mando Espacial

Además, el **Ministerio de Defensa** pondrá en marcha en otoño el **Mando Espacial**, dentro del Ejército del Aire y del Espacio, para disponer de una estructura operativa militar que permita actuar en labores de protección y control de la seguridad nacional en la realidad 'ultraterrestre'. Según consta en el BOE, su objetivo será la preparación de sus unidades, además de "la dirección, planeamiento, organización y coordinación de las funciones que posibiliten la vigilancia, control y operación en el espacio", ante las "amenazas" que puedan surgir, al igual que ya se vigilan en los espacios terrestre, marítimo, aéreo y ciberespacial, según se ha publicado en el BOE.

Acuerdo para la ID3

Por otra parte, Defensa ha adjudicado tres de los lotes del acuerdo marco de la Infraestructura Integral de Información para la Defensa (ID3) a **Telefónica** y **Evolutio**, con un contrato que ronda los 30 millones de euros. El concurso fue formalizado por la Dirección Económico Financiera de la Dirección General de Infraestructura del Ministerio a principios de verano.

Proyectos DIANA

Asimismo, la **Universidad Politécnica de Madrid** y el **Ejército del Aire y del Espacio** han sido elegidos por la **OTAN** para acoger cuatro centros de prueba de su programa de aceleración tecnológica DIANA (Defense Innovation Accelerator for the North Atlantic). En concreto, los de la UPM estarán dedicados a Neurotecnología e IA (NeuroTechAI), coordinado por el catedrático **Enrique J. Gómez Aguilera,** y a Comunicaciones Cuánticas (UPM-DQC), dirigido por el catedrático **Vicente Martín.** Los otros dos se situarán en las instalaciones del Ejército del Aire en Torrejón de Ardóz, donde está el Flight Test Center (CLAEX) y el Institute for Aviation Medicine (CIMA).

S21SEC recibe la máxima categoría en la certificación del Esquema Nacional de Seguridad de AENOR

S21sec, de **Thales Group,** ha recibido por parte de **Aenor** los certificados de la renovación del Esquema Nacional de Seguridad (ENS) de categoría Alta según el RD 311/2022, para todos los servicios de su portafolio (servicios gestionados y servicios profesionales) y de la ISO 27701 del Sistema de Gestión de la Privacidad de la Información, siendo una de las empresas pioneras en España en su obtención y la primera en el País Vasco.

De izq. a der.: Jesús Gómez-Salomé (Aenor); Pablo Echevarría (S21sec); Rafael Gª Meiro (Aenor) y José Prieto (S21sec)

La compañía ha obtenido esta certificación en su máximo nivel para toda su cartera gracias al estricto cumplimiento con los requisitos para una protección adecuada de sus sistemas, servicios, datos y comunicaciones. Esta certificación se suma al resto de sus acreditaciones, entre ellas las ISO 9001:2015, el ISO 27001:2017, el ISO 20000-1:2018, el ISO 22301:2020 e ISO 14001:2015.

Ataques contra el sector energético

Además, la empresa ha publicado su 'Threat Landscape Report', con datos de su Cyber Threat Intelligence Unit, en el que alerta del significativo aumento de los ciberataques en la industria energética a causa del conflicto bélico entre Rusia y Ucrania, además de destacar que las amenazas dirigidas contra este sector provienen de grupos guiados por diferentes estados, como la República Popular China o la Federación Rusa, así como por *actores hacktivistas.*

El CONSEJO NACIONAL DE CIBERSEGURIDAD celebra una nueva reunión para conocer los retos del segundo semestre del año en este ámbito

El **Consejo Nacional de Ciberseguridad**, presidido por **Esperanza Casteleiro**, directora del **Centro Nacional de Inteligencia** (CNI), se reunió a mediados de julio para compartir información y dar a conocer las últimas novedades en cuanto a la presidencia española del Consejo de la UE en el ámbito de la ciberseguridad, la trasposición de la directiva NIS2 y los grupos de trabajo europeos relacionados. Además, se abordó el estado de situación de la propuesta de Reglamento Europeo de Cibersolidaridad, publicada el 18 de abril de 2023, que tiene como principal objetivo la mejora de la preparación, la detección y la respuesta a los ciberataques en toda la UE. Durante la reunión, también se informó a los participantes de los últimos ciberincidentes de importancia vividos en España, así como el estado de la Red Nacional de SOC y la Red europea de SOCs, el Plan Nacional de Ciberseguridad y el Real Decreto-ley de Ciberseguridad del 5G.

¿Podrías resistir la tentación de mirar su contenido?

Solo se necesita encontrar un USB por casualidad para infectar un dispositivo con malware. Transformar los comportamientos de los empleados es fundamental, pero se necesita una plataforma de capacitación completa diseñada para maximizar la efectividad de los procesos de aprendizaje. Tres vectores de aprendizaje para desarrollar las tres principales características defensivas de cada individuo: el conocimiento, la percepción del peligro y la prontitud.

Cyber Guru

SECURITY AWARENESS TRAINING THAT WORKS!

www.cyberguru.it/es

ESTE ES UN QRCODE SEGURO

DEFENSA aprueba su Estrategia Industrial marcando el camino de las inversiones en este ámbito

El **Ministerio de Defensa** ha puesto en marcha la Estrategia Industrial de Defensa (EID) 2023. Se trata de la hoja de ruta con la que el gobierno quiere destacar el camino que debe seguir el sector en los próximos años. El documento publicado en el Boletín Oficial de Defensa (BOD) y firmado por la secretaria de Estado de Defensa en funciones, **Amparo Valcarce,** aprueba las directrices generales de la EID apostando por la producción en España y por la industria nacional, siempre que sea posible.

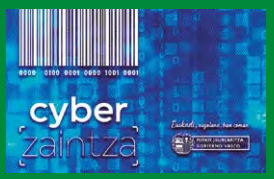
"La finalidad de la EID 2023 se basa en maximizar el rendimiento de la inversión en defensa, potenciar el tejido industrial y tecnológico, y promover la generación de empleo y el fomento de la cohesión territorial", ha destacado desde el Ministerio. Para ello, se basará en tres ejes: por un lado, incrementar el nivel de autonomía estratégica en materia de industria de defensa, para reducir la dependencia de terceros; por otro, contribuir a la estrategia europea en este ámbito; y, por otro, consolidar la Base Industrial y Tecnológica de Defensa (BITD). Aspectos en los que, lógicamente, también estará presente la ciberdefensa, entre otros, en lo que la atañe en la creación de una próxima 'nube de combate', así como del uso que se le dé en estos entornos a tecnologías cuánticas y de IA, según destaca el documento aprobado.

El INCIBE organiza un InfoDay para presentar las oportunidades en el sector Defensa para emprendimiento

El **Instituto Nacional de Ciberseguridad de España** (Incibe), y **la Dirección General de Armamento y Material** (DGAM), del **Ministerio de Defensa,** organizaron en verano una jornada dedicada a las 'Oportunidades en el sector Defensa para emprendimiento en ciberseguridad". En ella, además de dar a conocer el programa Emprende que, hasta el 31 de diciembre de 2023, cuenta con una Invitación Pública para el desarrollo de actuaciones de captación de ideas de negocio, incubación y aceleración de proyectos de emprendimiento, se mostraron los aspectos más destacados del programa DIANA (o Acelerador de Innovación de Defensa de la **OTAN**), creado con el objetivo de promover soluciones de uso dual basadas en tecnologías disruptivas y emergentes con aplicación al sector de la Defensa y la Seguridad Nacional, pero que también puedan tener aplicaciones en el ámbito civil. Precisamente, entre sus aspectos más señalados, está el lanzamiento de un proyecto piloto destinado a *startups* innovadoras que sean capaces de presentar soluciones dentro de las tres áreas prioritarias de trabajo identificadas por la OTAN.

'Luz verde' a la AGENCIA DE CIBERSEGURIDAD DE EUSKADI, bajo la denominación 'Cyberzaintza', que dará sus primeros pasos en otoño

Tras muchos meses de preparación, en junio, el Gobierno Vasco aprobó la creación de la **Cyberzaintza,** la Agencia de Ciberseguridad de Euskadi que busca combatir la ciberdelincuencia de una manera integral y transversal. Para ello, se ha dado luz verde por parte del Consejo de Gobierno al 'Proyecto de Ley de Creación de la Agencia Vasca de Ciberseguridad-Euskadiko Zibersegurtasun Agentzia'. Se trata de un organismo público, con personalidad jurídica propia, que estará regido por un texto normativo de 13 artículos distribuidos en tres capítulos, más una disposición adicional, otra transitoria y tres finales. De esta forma, al cierre de esta edición, sólo quedaba su validación por parte de la cámara vasca por el procedimiento de lectura única. Por ello, se espera que se ponga en marcha no más tarde de este otoño.



Esta Agencia trabajará, principalmente, en tres frentes. Por un lado, en la lucha contra la ciberdelincuencia en coordinación con la Ertzaintza; por otro, en la protección de las infraestructuras y datos públicos, protegiendo y promoviendo un "adecuado funcionamiento de las infraestructuras digitales del sector público vasco". Además, será la encargada en la región de la protección de las infraestructuras y datos empresariales, en coordinación con el equipo de promoción económica del gobierno vasco. De esta forma, cogerá el testigo del Centro Vasco de Ciberseguridad (BCSC) creado en 2017. En este sentido, su personal y medios materiales actualmente adscritos pasarán a integrarse en la nueva agencia.

Estructura

En cuanto a su organigrama, el organismo estará dirigido por una persona designada por el gobierno vasco y un Consejo de Administración integrado por 16 personas y presidido por la persona que ostente el cargo de responsable del Departamento de Seguridad.

SIA, de INDRA, se hace con ICA SISTEMAS, a la vez que el grupo se reorganiza para ganar peso en defensa y tecnología

Para fortalecer su oferta de servicios de ciberseguridad y su posición en el Sector Público, **Indra,** a través de su compañía SIA, ha adquirido a **ICA Sistemas y Seguridad (ICASyS)**. Con este paso impulsa aún más el nuevo paradigma para la defensa activa que ofrece a las organizaciones a través de su servicio SIA eXtended MDR. La operación da continuidad a su estrategia de crecimiento; en particular, en el ámbito de la detección de ciberamenazas, "con Mónica NGSIEM, un sistema automatizado de gestión de información y eventos de seguridad desarrollado por ICASyS, adoptado por el CCN como la plataforma Next Generation SIEM en la administración pública y organismos dependientes, y producto nacional certificado, en nivel 'Alto, en sus funcionalidades de seguridad en el ENS", destacan desde la empresa, además de recordar el valor de su solución Lógica NGSIEM, "único NGSIEM nacional y europeo certificado Common Criteria y producto cualificado y aprobado por el CCN".

Por otro lado, el Consejo de Administración aprobó en verano una nueva estructura organizativa en torno a cuatro áreas: defensa y seguridad, tecnología y consultoría digital (Minsait), gestión del tráfico aéreo (ATM) y movilidad. Además, ha trascendido que, posiblemente, haya reactivado su interés por hacerse con la empresa **Epicom.**

Es muy difícil recuperar la reputación perdida.

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

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

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

Síguenos en: • @s2grupo • s2grupo.es

S2 GRUPO

Anticipando un mundo **ciberseguro**

A instancias del Ministerio de Asuntos Exteriores, UE y Cooperación junto con el INCIBE

LEÓN acoge el primer encuentro entre diplomáticos especializados en diplomacia digital y cibernética del ámbito europeo e iberoamericano

El **Instituto Nacional de Ciberseguridad de España** (Incibe), en coorganización con el **Ministerio de Asuntos Exteriores**, la **UE** y el apoyo de la **Organización de Estados Americanos** (OEA) y el **Departamento de Estado de EE.UU.**, acogió en verano el encuentro ´EU-Americas Regional Dialogue on Cyber and Digital Diplomacy´, en el que reunió, por primera vez, a diplomáticos de más de 30 países especializados en ciberprotección y política digital de América y Europa (en la imagen, los participantes). El encuentro se realizó dentro de los diferentes actos que se están llevando a cabo por la presidencia española y durante la celebración de la octava edición del Cybersecurity Summer BootCamp, que este año contó con más de 260 alumnos, de 23 países.

Durante dos jornadas, los participantes asistieron a diferentes ponencias con un programa especialmente centrado en ciberdiplomacia, contando con tres mesas redondas y una clase magistral de expertos internacionales de alto nivel. En la primera de ellas, se abordó el desarrollo de estrategias globales de ciberseguridad. En la segunda, se centraron en el camino a seguir para la diplomacia tecnológica regional y multilateral, y en la última, se analizaron las herramientas cibernéticas y digitales de la UE en América Latina.

Precisamente, en colaboración con la OEA, también se celebró en León los 'International CyberEx', para fortalecer de las capacidades de respuesta ante incidentes cibernéticos, así como una mejora de la colaboración y cooperación ante este ámbito en el que tomaron parte miembros de la Organización, así como otros países con CSIRT, invitados por el Incibe. Además, el Instituto, como Centro de Coordinación Nacional (NCC-ES) del **Centro Europeo de Competencia en Ciberseguridad** (ECCC), celebró el 'Taller de NCC sobre Ciberseguridad en la Presidencia Española', sobre la aplicación de políticas específicas (NIS2, Cyber Resilience Act, European Certification Schemes), con el fin de establecer acciones de apoyo y financiación.

Acuerdo con Ucrania

Por otro lado, para impulsar el apoyo de España a Ucrania en el ámbito cibernético, el Incibe, a través de su director general, **Félix Barrio**, realizó una visita oficial al **Servicio Estatal de Comunicaciones Especiales y Protección de la Información de Ucrania** (SSSCIP), donde, junto a **Oleksandr Potii**, subdirector del SSSCIP, se selló un acuerdo, marcándose una hoja de ruta de los primeros pasos para desarrollar una mayor cooperación entre los dos países en materia de ciberseguridad.

El GOBIERNO acuerda cuáles son los supuestos de validez de sistemas de identificación y firma-e en la administración con sistemas de registro distribuido

El **Consejo de Ministros** aprobó en verano un acuerdo por el que se determinan los supuestos de validez de sistemas de identificación y firma-e en la administración del Estado cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido. Se trata de una iniciativa fruto del objetivo de la UE de conseguir que, para 2030, el 80% de los ciudadanos se beneficien del despliegue de una identidad digital fiable y controlada por el usuario, que le permitirá acceder a los servicios digitales en línea de los sectores público y privado, reforzando la privacidad y cumpliendo plenamente la legislación vigente en materia de protección de datos.


BOLETÍN OFICIAL DEL ESTADO

III. OTRAS DISPOSICIONES

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

En este contexto, la **Comisión Europea** adoptó la Recomendación (UE) 2021/946, de 3 de junio de 2021, sobre un conjunto de instrumentos común de la UE para adoptar un enfoque coordinado de cara a un Marco para una Identidad Digital Europea. A partir de esta Recomendación, España viene participando en numerosos grupos de trabajo en aras de definir los requerimientos funcionales, técnicos y de seguridad en relación con una cartera digital que almacene credenciales verificables de identidad de los ciudadanos. .

Paso notable en España

Así, para "poder cumplir los compromisos adquiridos por España en el liderazgo de las propuestas señaladas sobre identidad digital y credenciales e infraestructura *blockchain* que han sido seleccionadas por la Comisión en el marco del programa Europa Digital", se ha acordado por el Consejo de Ministros un acuerdo por el que considera "válido un sistema de identificación y firma de los interesados por medio de una credencial incorporada a la Cartera digital cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido basado en la **Infraestructura Europea de Servicios de Blockchain** (EBSI), en el contexto de los proyectos europeos". También permitirá "un sistema de identificación y firma de los interesados por medio de una credencial cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido incorporada a la Cartera digital española, para su utilización en los casos de uso del **Consorcio europeo Digital Credentials For Europe** (DC4EU) en el nuevo marco de identidad digital europea".


Barracuda®
Protege usuarios, sedes e IoT con Barracuda SecureEdge.
Consigue protección SASE de calidad Enterprise para tu negocio.
barracuda.com

• EFEMÉRIDES •

Fujitsu: 50 años presentes en el futuro de España

Fujitsu inició su camino en España en 1973 con la instalación del primer ordenador en la Universidad de Barcelona, la constitución de SECOINSA y la apertura de la fábrica de Málaga, germen del Parque Tecnológico de Andalucía en 1977, el diseño y comercialización de los primeros cajeros automáticos que favorecieron la implantación de una extensa red de cajeros que impulsaron el desarrollo de una más que notable red de servicios, que fue vez clave para nuestra contribución durante décadas a la modernización de servicios públicos. Posteriormente, llegaron hitos tan importantes como la instalación del Supercomputador más potente de España en el CESGA en 1993, la apertura de la división de I+D de Fujitsu en Madrid en 2014, la apertura del Centro de Desarrollo de Aplicaciones en Sevilla, la creación del centro de desarrollo de soluciones para la Justicia en Valencia y del centro de gestión de redes de autoservicio bancario en Barcelona, la puesta en marcha del Centro de Ciberseguridad en Sevilla o el establecimiento en Madrid del centro de excelencia en Big Data, Analytics o Inteligencia Artificial para Europa.

Nuestro presente es igual de prometedor. Hoy por hoy, estamos ejecutando los primeros proyectos de genómica en Madrid y Murcia, prestando servicios avanzados de ciberseguridad en el ámbito de Internet of Medical Devices, protegiendo redes 5G privadas, e implantando sistemas biométricos para el acceso a los ciudadanos a los servicios públicos y entidades financieras.

FUJITSU
50º ANIVERSARIO
2023

Ciberseguridad: el reconocimiento a Fujitsu España

Fujitsu recibía recientemente diversos reconocimientos a su labor profesional en el ámbito de la ciberprotección. Dicho reconocimiento viene derivado del importante crecimiento en España en esta materia, de nuestro buen hacer con nuestros clientes y del *feedback* recibido por parte de analistas de referencia. Por un lado, el estudio sobre Outsourcing TI en España 2022 de Whitelane Research y Quint posiciona a Fujitsu en la primera posición en el indicador de ciberseguridad. Asimismo, la consultora Penteo ha posicionado también a Fujitsu como una de las mejores compañías de España en servicios de ciberseguridad.

Gracias a dicha confianza y a la apuesta de nuestra matriz, Fujitsu ha abierto además un Near Response Center en España más concretamente en Sevilla que, entre otros, prestará servicios de ciberseguridad a otros clientes de Fujitsu en Europa.

Innovación en ciberseguridad

En los últimos 3 años Fujitsu ha conseguido un importante crecimiento en sus servicios de ciberseguridad. A modo de ejemplo, en la actualidad Fujitsu protege desde España más de 400.000 *endpoints* con tecnologías líderes en el mercado.

Además, estamos participando en iniciativas y proyectos innovadores en materia de ciberseguridad, como es la aplicación de técnicas biométricas (facial y voz) para la modernización de servicios digitales, la investigación en tecnología cuántica, la ciberprotección en redes 5G privadas, así como la ciberseguridad aplicada en la protección hospitalaria en redes de Internet of Medical Devices, donde estamos realizando proyectos pioneros en España.

Javier Pérez García
Head of Cybersecurity
FUJITSU ESPAÑA

Las españolas INDRA y ZEROLYNX velaron por la seguridad del 23J junto al Mº DEL INTERIOR

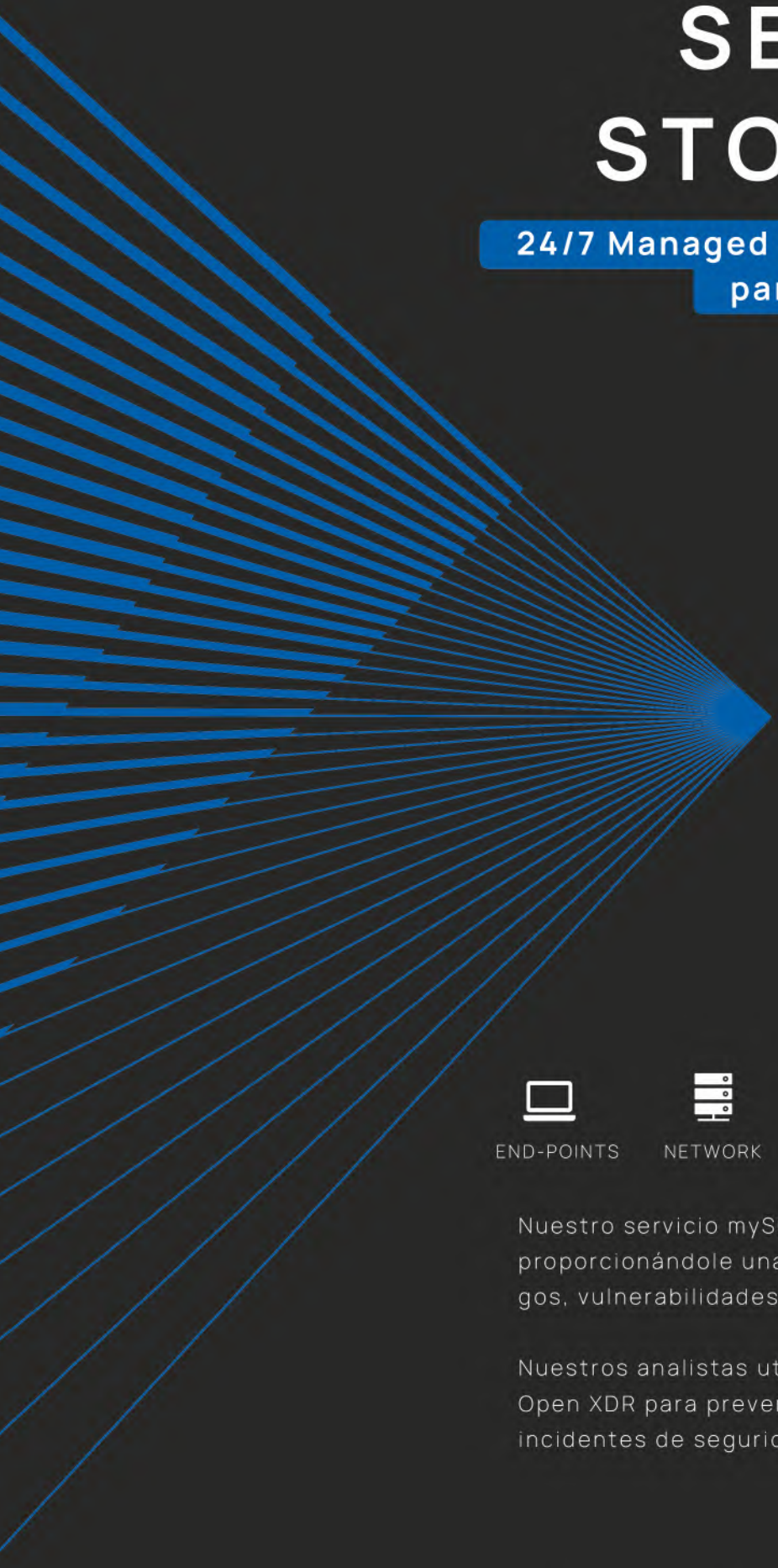
El pasado 23 de julio tuvieron lugar las elecciones generales en España, unos comicios que llamaron al voto a más de 37 millones de electores. El proceso, que ya de por sí y, por razones obvias, requería de unos procesos de seguridad encomiables, vino precedido de varias semanas de ciberataques por parte del grupo NoName57, el cual protagonizó una oleada de embates a diferentes infraestructuras críticas de nuestro país, tanto públicas, como privadas. Estos hechos, unidos a la elevada tensión internacional, llevaron al **Ministerio del Interior** al despliegue de un dispositivo de seguridad sin precedentes organizado por la **Dirección General de Política Interior**, responsable del correcto desarrollo del proceso electoral, donde todas las medidas de protección fueron cuidadas para salvaguardar el éxito del proceso electoral ya concluido. La consultora española **Indra**, como adjudicataria encargada de proporcionar el sistema de recuento del voto, fue la responsable de implantar y operar el sistema completo, gestionando las diferentes aplicaciones de consulta a las que pudieron acceder tanto la ciudadanía de forma directa, como las agencias de comunicación y demás interlocutores. Dentro de este proceso, Indra bajo la supervisión directa de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, departamento tecnológico de Interior encargado de apoyar a la Dirección General de Política Interior en todo lo relativo a la correcta implantación de la infraestructura tecnológica y de comunicaciones en los procesos electorales, fue también la responsable de velar por la seguridad del entorno, garantizando la integridad, disponibilidad y confidencialidad del proceso de recuento y puesta a disposición de la información de voto.

Asimismo, y junto al apoyo del **CCN-CERT**, Interior decidió optar por otra consultora también española, **Zerolynx**, con el fin de contar con una segunda organización que auditase la seguridad de la infraestructura desplegada, y pusiese a prueba su resiliencia ante ataques de gran magnitud.

Como ya es sabido por todos, los comicios se desarrollaron sin incidentes a pesar de que diferentes actores maliciosos aprovecharan la jornada para perpetrar ataques a otras infraestructuras públicas y privadas.

SEE MORE.
STOP MORE.

24/7 Managed Detection & Response para todos sus entornos.



mySOC®
by Advens

END-POINTS NETWORK CLOUD APPLICATIONS OT/IOT

Nuestro servicio mySOC® protege todos sus entornos, proporcionándole una visibilidad completa de sus riesgos, vulnerabilidades y amenazas externas.

Nuestros analistas utilizan nuestra plataforma mySOC Open XDR para prevenir, detectar y responder a los incidentes de seguridad con usted en tiempo real.

Descubra nuestros servicios en www.advens.com

INTERIOR reorganiza su estructura con especial impacto en el ámbito cibernético y establece un punto de coordinación

La Unidad Central de Ciberdelincuencia de la POLICÍA impulsa tres 'Ciberbrigadas' para fortalecer la estructura de investigación de los delitos cometidos a través del uso de TIC

El **Ministerio de Interior,** a través de la Orden INT/859/2023, de 21 de julio, ha acometido una reorganización de su estructura para "conseguir la máxima eficacia y racionalización". Entre otras novedades, en el ámbito cibernético, en su sección dos, se apuesta por fortalecer la "estructura de investigación de los delitos cometidos a través de la utilización de las TIC con la integración, en la **Comisaría General de Policía Judicial,** de la **Unidad Central de Ciberdelincuencia,** potenciando las competencias en este tipo de especialidad criminal con una nueva **Brigada Central de Fraudes Informáticos.**

Tres 'ciberbrigadas'

Así, se establece que la **Unidad Central de Ciberdelincuencia** (UCC), que dependerá de la **Comisaría General de Policía Judicial,** se encargará de la investigación y persecución, nacional e internacional, de las actividades delictivas con nuevas tecnologías o sistemas de información relacionadas con el patrimonio, el consumo, la indemnidad del menor, la pornografía infantil, la libertad sexual, el honor, la intimidad, las redes sociales, los fraudes, la propiedad intelectual e industrial; así como de aquellas que atenten contra la confidencialidad, la integridad y la disponibilidad de los sistemas de información y comunicaciones". Además, se constituye como **Centro de Prevención y Respuesta E-Crime** de la Policía.

La UCC estará formada por tres Brigadas: la **Central de Investigación Tecnológica,** encargada de "la investigación de los delitos contra las personas cometidos mediante el uso de las nuevas tecnologías", la **Central de Seguridad Informática**, responsable de "la persecución de delitos de alta especialización relacionados con ciberataques, creación y distribución de software malicioso, utilización de criptovalores como mecanismo de intercambio monetario en el entorno cibercriminal, delitos contra la propiedad intelectual con nuevas tecnologías y fraudes BEC (Business Email Compromise), así como del apoyo a las unidades de la Comisaría General y territoriales". Y, también es notable, que es el punto de contacto del **Convenio de Budapest.** Por último, también formará parte de la UCC la **Brigada Central de Fraudes Informáticos**, que se crea con esta nueva organización, centrada en "la investigación de tipologías delictivas relacionadas con los fraudes cometidos a través de internet y el uso de las telecomunicaciones".

Punto de coordinación

Asimismo, establece un punto de coordinación en lo cibernético materializado en la **Unidad Central de Apoyo Tecnológico**, que impulsará "la actividad operativa de la Policía Nacional en lo referente a la aplicación de nuevas tecnologías, con especial atención al ámbito de la ciberseguridad, la ciberinteligencia y la lucha contra la cibercriminalidad, estableciéndose como órgano de coordinación entre los diferentes departamentos de la Dirección General de la Policía en estas áreas". De ella dependerán el Área de Transformación Digital y Coordinación en Ciberseguridad, que funcionará como punto de encuentro "de las unidades operativas que despliegan su actividad en el ciberespacio", y el Área de Desarrollo Tecnológico.

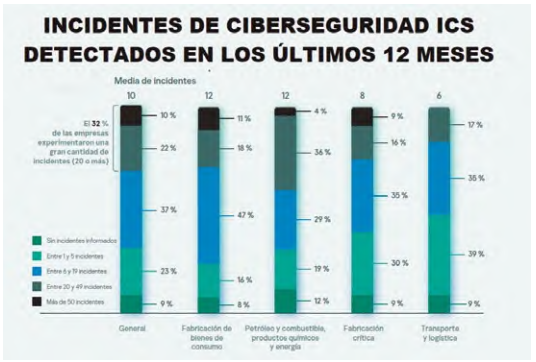
TELEFÓNICA TECH se reorganiza por mercados en vez de tecnologías buscando más simplicidad en su estructura

Telefónica Tech, filial de **Telefónica,** ha decidido pasar a organizarse por mercados geográficos, en vez de hacerlo, como hasta ahora, por tecnologías. Hasta el momento, Telefónica Tech tenía dos grandes divisiones: el negocio Cloud (nube), el más grande y que incluía ciberseguridad; y el negocio de Internet de las Cosas (IoT) y Big Data. Así, a partir de ahora, unificará todos los negocios y servicios, con el objetivo de poder dar un servicio más completo al cliente y de forma coordinada y parecerse más a las estructuras que tienen grandes tecnológicas.

Además, Grupo Telefónica ha decidido integrar sus **Telefónica I+D** y **Telefónica Digital** para crear una enseña unificada bajo la marca Telefónica Innovación Digital. La nueva sociedad, que espera constituirse a final de año, estará bajo la dirección de **Chema Alonso,** Chief Digital Officer (CDO) de la compañía.

KASPERSKY alerta del aumento de ataques a OT/ICS con costes un 59% más altos que el de otro tipo de empresas

Durante 2022, el equipo de **Kaspersky** realizó una investigación con la participación de 306 profesionales de empresas de más de 1.000 empleados en todo el mundo, con el fin de profundizar en los riesgos de la ciberseguridad que afectan a las organizaciones que usan tecnología operativa (OT). Entre sus aspectos más relevantes, destaca que los ataques a los sistemas de control industrial (ICS) se incrementaron durante 2021. Por ejemplo, se constató un aumento relativo del 45% en la incidencia de *spyware* en ordenadores usados con propósitos ICS, un incremento del 43% en casos de *scripts* maliciosos y páginas de *phishing*, bloqueados en dispositivos que ejecutaban sistemas industriales.



Por otro lado, Kaspersky celebró el quinto aniversario de su 'Iniciativa Global de Transparencia' (GTI). Así, actualmente, los datos de sus clientes en Europa, EE.UU., Iberoamérica, Oriente Medio y Asia-Pacífico se almacenan y procesan en dos centros de datos ubicados en Zúrich.

Además, fruto de su buen hacer, Kaspersky también ha superado con éxito la auditoría de Control de Organización de Servicios para Organizaciones de Servicios (SOC 2).

TEHTRIS

FACE THE UNPREDICTABLE

XDR/HONEYPOTS

DECEPTIVE RESPONSE

- Honeypots que simulan servicios falsos para detectar posibles intrusiones
- Protege áreas de tu red en las que no se puede instalar un agente de endpoint
- Supervisa los ataques dirigidos a tu organización

ERES EL PROTECTOR DEL CIBERESPACIO

HIPERAUTOMATIZA TU SEGURIDAD

MADE IN EUROPE

afaq ISO 27001 Information Security AFNOR CERTIFICATION 2009/102155

CONTACTA CON NOSOTROS

spain@tehtris.eu
tehtris.com

OBITUARIO

Kevin Mitnick 'el Cóndor', pasa

Considerado para muchos como el hacker más conocido de los años 90, el 'Condor' como fue popularmente llamado, falleció en julio, a los 59 años, por un cáncer de páncreas.

Dotado de un gran talento y querencia por deambular por entre las líneas rojas 'difusas', Mitnick fue procesado en varias ocasiones -y encabezó la lista de los 'más buscados' del FBI-, siendo detenido por última vez en febrero de 1995 por entrar en algunos de los ordenadores supuestamente más seguros de EE.UU., así como por conseguir más de 20.000 números de tarjetas de crédito. Su pericia en ingeniería social -encandilamiento de secretarias mediante- fue notable.

Entre las muchas anécdotas que rodean su vida está desde aplicársele el atenuante de 'adicción a los ordenadores', lo que le permitió ser sentenciado a sólo un año de prisión en 1988, hasta la recompensa ofrecida por él, en 1992, por parte del FBI. En su última persecución, en los años 90, llegó a entrar en el ordenador de otro experto en ciberseguridad, que se había ofrecido como voluntario al FBI para localizarse, el japones **Tsutomu Shimomura,** y que finalmente consiguió detenerle. Fue condenado a cinco años de cárcel e, incluso, durante tres tuvo prohibido acercarse a un ordenador o móvil sin el permiso de su oficial de libertad condicional, ya que, según el fiscal, con solo una llamada era capaz de provocar un holocausto nuclear. Así, su vida generó varios libros e, incluso, la película Takedown, en el año 2000, aunque con numerosos errores biográficos.

Desde hace dos décadas, tras salir de prisión, totalmente reinsertado, fue ponente en numerosos congresos –no pocos de ellos en España: eGallaecia, Cluster Madrid…–, siendo un consultor activo en este ámbito y trabajando como Chief Hacking Officer (CHO) en la empresa de concienciación **Knowbee**. "Mis delitos fueron simples delitos de allanamiento de morada. Mi caso es un caso de curiosidad", destacó quitando importancia a sus acciones ilegales. Su último libro, 'Ghost in the Wires: My Adventures as the World's Most Wanted Hacker', fue un éxito de ventas del New York Times. Desde **Revista SIC** nos sumamos a los que lamentan su pérdida y enviamos nuestras condolencias a amigos y familiares.

SIC

BABEL potencia su presencia internacional con la adquisición de la consultora mexicana IRONBIT

Babel, multinacional tecnológica de origen español especializada en soluciones y servicios de transformación digital, ha adquirido la consultora tecnológica mexicana **Ironbit.** Esta operación supone un paso más en el proceso de internacionalización de la firma, que en los próximos años quiere que este país sea uno de sus principales mercados. Con esta compra, la empresa española supera los 3.300 empleados, de los que 500 estarán en México.

Además, esta integración la permite incrementar y consolidar su portafolio y reforzar sus capacidades en áreas como *Big Data* y *Analytics,* realidad aumentada y virtual, y tecnologías *mobile*, que se unen a tecnologías como IA, ciberseguridad e hiperautomatización, entre otras, en las que ya está posicionada como una firma referente. La compra de Ironbit forma parte de la estrategia de crecimiento de Babel, que en los últimos años ha realizado importantes adquisiciones, como la de la unidad de servicios profesionales en España de la multinacional alemana **Software AG,** la compañía especializada en ciberseguridad, **Ingenia,** y la costarricense **Grupo Babel.**

La nueva operación es un paso más en el plan estratégico definido por la compañía y denominado 'Plan Marte 2025', que supone su hoja de ruta para lograr los 300 millones de euros de facturación y un EBITDA de 30 millones para 2025. En el ejercicio fiscal de 2023 las previsiones son superar los 180 millones de euros.

CROWDSTRIKE crea el primer grupo de Operaciones Contra Adversarios de la industria ofreciendo su servicio Identity Threat Hunting

CrowdStrike ha anunciado la creación de un nuevo grupo de Operaciones Contra Adversarios a través de un equipo de analistas y el uso de "tecnologías de última generación para detectar y detener la actividad de los ciberdelincuentes", destaca la compañía. En concreto, esta propuesta empleará sus capacidades de Falcon Intelligence y Falcon OverWatch. "Desde nuestro nacimiento, la filosofía que nos ha guiado ha sido 'no tienes un problema con el *malware*, tienes un problema con los ciberdelincuentes' y esto es, hoy en día, más real que nunca", ha comentado **Adam Meyers**, responsable del equipo del recién creado grupo.

Primera novedad

Así pues, como respuesta al creciente número de ataques basados en identidades y al incremento en la sofisticación de las técnicas utilizadas por los delincuentes, el equipo de CrowdStrike también ha presentado su primer producto: Identity Threat Hunting, ya disponible como parte de la solución Falcon OverWatch Elite, sin coste adicional para sus usuarios. En él se combina la inteligencia sobre motivaciones y técnicas de los ciberdelincuentes con las herramientas Falcon Identity Threat Protection y Falcon OverWatch para identificar y remediar las credenciales comprometidas rápidamente, analizar movimientos laterales y reducir el impacto de las acciones de los cibercriminales con cobertura 24/7.

Además, la compañía ha presentado su 'Informe Anual de Amenazas' en el que destaca que los ataques basados en identidades, las intrusiones interactivas y el uso legítimo de herramientas de gestión y monitorización remota ha crecido de forma exponencial en el último año. También, alerta de que el 62% de las intrusiones se realizó desde cuentas válidas. Asimismo, es muy revelador que los especialistas de la empresa han comprobado que, de media, los ciberdelincuentes alcanzan sus objetivos en tan solo 79 minutos, cinco menos que el año pasado. Y recuerda que las intrusiones basadas en identidades, los ataques a la nube y el uso de herramientas de gestión remota son las mayores amenazas actuales para una organización.

Certificación del CCN

Por otro lado, la plataforma CrowdStrike Falcon ha sido certificada por el **CCN** en la Categoría Alta de la Cualificación CPSTIC (Catálogo de Productos y Servicios de Seguridad para las Tecnologías de la Información y la Comunicación).

La Cualificación del CPSTIC español llega después de que CrowdStrike obtuviera también la autorización de Nivel de Impacto 5 (IL5) por parte del Departamento de Defensa de EE.UU.

QUE ESTE OTOÑO
NINGÚN RANSOM SE LLEVE TUS HOJAS

SEGURIDAD E INTELIGENCIA

www.zerolynx.com

ZEROLYNX

También, ha sido adjudicataria de un contrato de 32 millones, junto a varias empresas, para servicios de I+D en ciberprotección

La ESA vuelve a confiar en GMV con un contrato de más de 200 millones para garantizar, entre otros retos, la ciberseguridad de la segunda generación de Galileo

La **Agencia Espacial Europea** (ESA) ha adjudicado a la multinacional tecnológica española **GMV** el desarrollo del segmento terreno de control del sistema de validación en órbita de la segunda generación del GPS europeo Galileo (conocida como G2G), por más de 200 millones de euros. Entre sus retos está la introducción de servicios y tecnologías para la mejora de los ya existentes, el aumento de la precisión y robustez del sistema, el incremento de la seguridad, así como la reducción de los costes de mantenimiento del sistema. El contrato ganado se suma así a los ya firmados por la compañía para la primera generación de Galileo (G1G), superando los 500 millones de euros contratados desde 2018.

El segmento terreno que se acaba de adjudicar se encargará del control de las dos nuevas plataformas de satélites de segunda generación, actualmente en fase de diseño y producción, de la que se espera lanzar un total de 12 satélites en los próximos tres años. Además de introducir el control y monitorización de los nuevos satélites, este nuevo proyecto supone una evolución tecnológica, ya que, según destacan desde GMV, incluye características como criptografía poscuántica, despliegue de microservicios, mejoras en la automatización, así como nuevos interfaces de usuario, entre otros. "Estas mejoras contribuirán a la creación de un segmento terreno flexible, escalable, expandible, robusto y autónomo", explican.

Adjudicación en I+D

Además, GMV ha sido una de las ganadoras, junto con otras empresas, del concurso convocado por el **Incibe** por valor de 32 millones de euros, para diferentes servicios de investigación y desarrollo (I+D) en ciberprotección. El Instituto ha adjudicado a **Tree Technology** el mayor importe de esta licitación (5,94 millones), mientras que la UTE de GMV (**GMV Soluciones Globales Internet, GMV Aerospace and Defence** y **Grupo Mecánica de Vuelo Sistemas**) se ha hecho con 5,2 millones de euros, e **Inetum España** con 4,9 millones. Además, **Mnemo Evolution & Integration Services** recibirá 4,72 millones, **Fractalia IT System,** 3,3 millones; **Tecnologías Plexus**, 2,97 millones, **Italtel,** 2,5 millones; y **Navantia,** 2,45 millones.

Ciberprotección en UAV

Asimismo, **GMV** y la **Agencia Gallega de Innovación** de la **Xunta de Galicia** han firmado un contrato para el desarrollo de un sistema de ciberseguridad que permita detectar interferencias de radiofrecuencia en el entorno del **Centro de Investigación Aeroportada de Rozas** (CIAR), adjudicado por un importe de 1,6 millones de euros. GMV también ha sido la adjudicataria del contrato para la provisión de servicios de ciberseguridad de Puertos del Estado y autoridades portuarias, además de implementar un Plan Director, por un importe de 4,4 millones de euros. Además, **Eviden,** de **Atos,** ha firmado un acuerdo con GMV para desarrollar la solución SkyMon para el nuevo centro que está poniendo en marcha **Hisdesat.** La tecnológica española también se ha hecho con la *spin-off* de la **Universidad de Vigo**, **Alén Space,** especializada en nanosatélites.

El borrador del OWASP TOP 10 para los 'Modelos de Lenguaje de Gran Tamaño', como ChatGPT, identifica sus principales problemas

En unos meses marcados por el abundante eco mediático de vulnerabilidades, como las dadas a conocer en **Apple** o **Fortinet,** el **Open Web Application Security Project,** conocido como **Owasp**, ha publicado un ranking con los principales riesgos de seguridad de API en sistemas de IA, que contiene muchas coincidencias con la que ya publicó hace cuatro años, también algunas redefiniciones y algunos nuevos conceptos.

Así, los dos primeros continúan siendo los mismos: la autenticación de nivel de objeto rota (API1) y la de usuario rota (API2). En tercer lugar, está la autorización de nivel de propiedad de objeto roto (API3), que suele ser por una exposición excesiva de datos. La sigue en cuarto lugar la API4, que cambia de falta de recursos y limitación de velocidad a consumo de recursos sin restricciones y continua en quinta posición la API5, de autorización de nivel de función rota.

En definitiva, los expertos han valorado positivamente este ranking, que se puede consultar en la web de la organización, aunque también han destacado que no supone un cambio radical de las amenazas y riesgos publicados anteriormente. De cualquier forma, sí supone una actualización, en ciberprotección de API, de utilidad para cualquier profesional en este ámbito.

ENTELGY INNOTEC SECURITY, primera empresa que consigue acreditar, en un solo proceso, los estándares más altos

Entelgy Innotec Security ha recibido las certificaciones ISO 22301, ISO 27001 y ENS (Esquema Nacional de Seguridad), así como dos calificaciones Leet para los servicios de Consultoría y de Monitorización. En ambas, ha logrado una nota significativa, BBB, en las dimensiones de Confidencialidad, Disponibilidad e integridad.

Así, la empresa, según han destacado sus responsables, se convierte en la primera en lograr, al mismo tiempo, todas estas certificaciones y calificaciones. Para ello, ha contado con el asesoramiento de **Leet Security**. De hecho, la buena nota obtenida en las calificaciones Leet también le han resultado útiles para certificar la seguridad de sus servicios en **Pinakes**. Se trata de una plataforma, gestionada por el **Centro de Cooperación Interbancaria** (CCI), que funciona con un sistema similar al usado por las agencias de calificación financiera como **Moody's**.

Además, Entelgy Innotec ha logrado la ISO 22301, que constata que cuenta con planes y procedimientos para garantizar la continuidad de sus operaciones comerciales, la ISO 27001, que certifica la implementación de un sistema de gestión de la seguridad de la información para proteger información confidencial y gestionar los riesgos relacionados, así como el ENS.

CIBERSEGURIDAD

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

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

Todas las respuestas que buscas están en aenorciberseguridad.com

AENOR

Confía

MADRID DIGITAL apuesta por ALL4SEC adjudicándole la protección del correo-e en un contrato a tres años por más de un millón de euros

Madrid Digital, la Agencia para la Administración Digital de la **Comunidad de Madrid,** ha adjudicado a **All4Sec** el concurso para la renovación del servicio de protección de su correo electrónico corporativo. El contrato, valorado en más de un millón de euros, tiene una duración de tres años e incluye los servicios de migración a la nube y soporte 7x24 a la operación del actual modelo de protección, basado en **Cisco** Secure Email (CES). El objetivo es permitir la gestión eficiente y segura de los correos-e que diariamente envía y recibe el organismo autónomo.

Madrid Digital ha valorado la oferta presentada por All4Sec como la más ventajosa tanto técnica como económicamente, teniendo en cuenta los 120.000 usuarios que se verán beneficiados por el servicio y que tendrán cobertura frente al análisis de *malware* asociado a correos internos y externos, así como en el uso seguro de aplicaciones de envíos masivos de comunicaciones institucionales.

La propuesta de All4Sec incluye, además, la revisión de la infraestructura actual que deberá ser migrada a un nuevo servicio en la nube, en línea con la estrategia de Madrid Digital de migrar su servicio de correo-e al *cloud*. Cabe mencionar que All4Sec dispone de una dilatada experiencia en el asesoramiento, despliegue, operación y mantenimiento de este tipo de infraestructuras y que, en 2021, fue reconocida por Cisco España por su 'Excelencia en Arquitecturas de Seguridad'.

"La adjudicación de este contrato supone un nuevo reconocimiento al trabajo que venimos desarrollando en el mercado de la ciberseguridad desde hace más de nueve años", ha destacado el CEO de la compañía, **Alfonso Franco.**

Actualmente, All4Sec proporciona servicios profesionales de ciberprotección a clientes nacionales e internacionales y, fruto de su buen hacer, también fue galardonada en 2017 con un **Premio SIC.**

Las vulnerabilidades 'críticas' marcan su máximo histórico en 2022

Las vulnerabilidades continúan siendo uno de los grandes talones de Aquiles para la ciberprotección corporativa. Y, a pesar de los avances en su detección y parcheo, la situación no ha mejorado. Según un estudio de **Skybox Security,** la cantidad de las reportadas al gobierno de EE.UU. en 2022, volvieron a alcanzar su máximo histórico con un incremento del 25%.

Los datos, analizados a través de la Base de datos Nacional de Vulnerabilidades (NVD), han sido facilitados en el 'Informe de tendencias de amenazas y vulnerabilidades de 2023' de la empresa en el que destaca que "es el sexto año consecutivo en que el volumen de vulnerabilidades recién descubiertas alcanzó un máximo histórico", con más de 192.000 publicadas durante la última década. En cuanto a su gravedad, el 80% de los CVE de 2022 fueron de importancia media o alta y un 16% críticas. Eso sí, también es cierto que el número de errores críticos se redujo del 20% de la anterior edición.

Los datos corroboran los publicados por la compañía **Palo Alto Networks** que también ha elaborado un completo estudio, a través de su **Unit 42,** en el que constata que las vulnerabilidades han aumentado un 55%, respecto a 2021.

La necesidad de defenderse con más rapidez impulsa la adopción de SECaaS, Confianza Cero e IA de cara a una mejor ciberprotección desde plataformas

Las empresas están adoptando con más frecuencia soluciones de seguridad como servicio (SECaaS) y acelerando la adopción de IA y de estrategias de Confianza Cero, según la más reciente edición del informe 'State of Application Strategy Report (SOAS)' de **F5**. El 42% de los responsables de TI encuestados afirmó que la "velocidad en la mitigación de amenazas" es la razón principal para recurrir a SECaaS, lo que implica basarse en modelos *cloud* para subcontratar servicios de ciberprotección. Para un 18% este enfoque también supone una ayuda a la hora de lidiar con la falta de talento interno.

Hacia la Confianza Cero y la IA

Según las respuestas recogidas en el informe, *el Zero Trust* sobresale como el enfoque más relevante a nivel global, escalando desde la tercera posición en la que se situaba en la edición del informe de 2022. "Es importante destacar también cómo la promesa de una mayor rapidez de reacción está acelerando el uso de AI/ML en el ámbito de la seguridad", comenta el ingeniero de soluciones de la empresa en España, **José Manuel Flores.** "En este sentido, el informe SOAS refleja que un 41% de las organizaciones tiene previsto o ya ha implementado (23%) asistencia mediante IA. Además, para todas ellas, la seguridad es su principal caso de uso".

Asimismo, la rapidez continúa motivando los esfuerzos de automatización. Este año, la seguridad de la red ocupa un lugar casi tan alto como el de la infraestructura de sistemas, situándose como la tercera función más automatizada dentro del grupo de las seis principales funciones de TI. La seguridad de la red, cada vez más con un modelo como servicio, también se está beneficiando de la aplicación de la IA.

Otro hallazgo notable de la investigación es que casi nueve de cada diez encuestados (88%) afirman que sus organizaciones están adoptando una plataforma de seguridad. De hecho, casi dos tercios (65%) espera utilizar una plataforma para la protección de la red o para la gestión de accesos e identidades. Mientras tanto, el 50% se está moviendo a una plataforma para proteger las aplicaciones web y las API desde el centro de datos hasta *el edge.* Otro 40% quiere una plataforma para las necesidades de seguridad del negocio, como soluciones *antibot* y antifraude.

PINK IS THE NEW BLACK

#GETREADYTOHUNT #GETREADYTOHACK

BLACKARROW
offensive driven defense

RED TEAM,
THREAT HUNTING &
INCIDENT RESPONSE

www.tarlogic.com

Powered by
TARLOGIC

En su propuesta de 'Código de buen gobierno' recomienda a las empresas trabajar en 13 ámbitos concretos

El FORO NACIONAL DE CIBERSEGURIDAD da un nuevo paso con cinco amplios informes centrados en concienciación, gobierno, ciberdefensa y formación

El **Foro Nacional de Ciberseguridad** (FNCS), dependiente del **Consejo Nacional de Ciberseguridad,** ha presentado cinco nuevos informes elaborados por Grupos de Trabajo, fruto de la iniciativa de colaboración público-privada del último año. Se trata de un paso más de esta acción plural cuyo arranque data de julio de 2020, que pretende convertirse en un "espacio de encuentro para dar respuesta a las dudas y preocupaciones que se asocian a la ciberseguridad en un entorno de colaboración global", como lo definen sus responsables.

En esta ocasión, los trabajos publicados se han centrado en la ciberprotección del ciudadano, la responsabilidad social corporativa, el impulso a la industria y a la I+D+i, la formación especializada, así como en las necesidades de ciberdefensa. Así, el documento titulado 'Brújula de la ciberseguridad del ciudadano: Hacia un Plan estratégico de ciberseguridad ciudadana' responde a la necesidad marcada por Estrategia Nacional de Ciberseguridad de impulsar una mayor implicación de toda la sociedad, mediante el fomento de una cultura de protección cibernética, para evolucionar desde la concienciación al compromiso, en el entendimiento de que la población es corresponsable de la ciberseguridad nacional.

Asimismo, continúa lo sugerido por la Carta de Derechos Digitales en la que se indica que los poderes públicos deben velar por el derecho a la ciberprotección de los ciudadanos, promover su sensibilización y su formación en este ámbito, buscando la colaboración de la sociedad civil. En este sentido, el informe se ha hecho a modo de guía para convertirse en un instrumento orientativo en el que se analizan 10 ámbitos -redes sociales, contraseñas y credenciales, ingeniería social, primer acceso a las TIC, trámites y compras *online*, privacidad e información personal, IoT, protección del dispositivo, IA y denuncia, soporte y ayuda-, que el Foro considera que representan actualmente un mayor ciberriesgo y sobre los que más atención hay que prestar.

Código de buen gobierno

Igualmente, se ha publicado el 'Código de Buen Gobierno de la Ciberseguridad', fruto del trabajo del grupo compuesto por expertos en la materia, así como del análisis de distintas normativas y estándares existentes, examinadas desde una perspectiva práctica y actual, para la mejora del buen gobierno corporativo. Su objetivo es proponer a las organizaciones las prácticas dirigidas a sustentar el modelo de buen gobierno de la ciberseguridad que "faciliten la gestión de la protección de las redes y los sistemas de información y contribuya a mejorar el proceso de toma de decisiones en este ámbito por parte de los órganos de gobierno de las organizaciones y, en especial, por el órgano de administración", recuerda el documento. Así, ofrece abundantes recomendaciones de alcance general, organizadas en 13 principios entre los que están la proporcionalidad, hasta la ética y el cumplimiento, el modelo de gestión, la dotación de recursos, la ciberinteligencia, la necesidad de informes periódicos y de la gestión del riesgo, entre otros.

En tercer lugar, el 'Impulso a la Industria y a la I+D+i. Resumen de propuestas y trabajos de la fase 2' continua el documento publicado en la primera fase de los trabajos del FNCS donde se definía el 'qué' se debe hacer (taxonomía), para continuar ahora con la cadena de valor que identifique el 'quién', con los actores principales en el ecosistema, y terminen en un futuro con el 'cómo y cuánto', tras concretarse en el barómetro integral de la ciberseguridad. En este sentido, la puesta en marcha del **Observatorio de la Ciberseguridad** (Observaciber), está impulsando que los trabajos planificados en el barómetro deban estar alineados para la segunda parte del año 2023 con Observaciber.

Por su parte, con el documento titulado 'Marco de competencias para programas superiores de formación especializada en ciberseguridad', se pretende definir uno de competencias -específicas y básicas- que sirva como referencia para el diseño de programas superiores de formación especializada. En él se identifican conocimientos que se pueden considerar como prerequisitos de acceso para adentrarse en programas superiores específicos en ciberprotección (por ejemplo, postgrados) o que permitan definir competencias relacionadas con el área de la ciberseguridad, pero en un nivel básico o fundamental (por ejemplo, en los primeros cursos de Grado).

Ciberdefensa

Por último, el Foro ha publicado el 'Informe sobre las necesidades, capacidades y retos para la colaboración público-privada en materia de ciberdefensa en las empresas del sector de la defensa y la seguridad'. Para su realización, se han recabado las opiniones a través de un cuestionario respondido por profesionales del ecosistema nacional de la ciberseguridad y la ciberdefensa de empresas, universidades y centros de investigación y tecnológicos relacionados con los organismos participantes en este grupo.

De esta forma, se quiere ofrecer una 'foto' de las capacidades tecnológicas aún en desarrollo, así como los servicios y productos en el mercado demandados por el sector de la Defensa y la Seguridad. Además, es de especial interés su identificación de áreas de mejora en el ámbito de la ciberdefensa y ciberprotección planteando la necesidad de invertir y desarrollar sistemas de planificación, mando, coordinación y control de operaciones en el ciberespacio, sistemas de defensa, activa y pasiva, de explotación para extraer datos e información de las redes y sistemas, así como sistemas de respuesta, para lograr un efecto sobre los activos del adversario, entre otros aspectos.

WatchGuard

WATCHGUARD FOR SOC – EFICIENCIA Y PROACTIVIDAD

Empowering the SOC

Threat Hunting

Detección, investigación y respuesta

Ciber Resiliencia

Anticípate a las ciberamenazas en constante evolución

WatchGuard for SOC se basa en la combinación de soluciones de seguridad avanzada y plataforma de threat hunting para buscar, detectar y responder de manera eficiente a amenazas que hayan logrado evadir otras protecciones en endpoints, servidores, entornos virtuales y dispositivos móviles.

SEGURIDAD ENDPOINT AVANZADA

AUTENTIFICACIÓN MULTIFACTOR

SEGURIDAD DE RED

NUBE SEGURA WI-FI

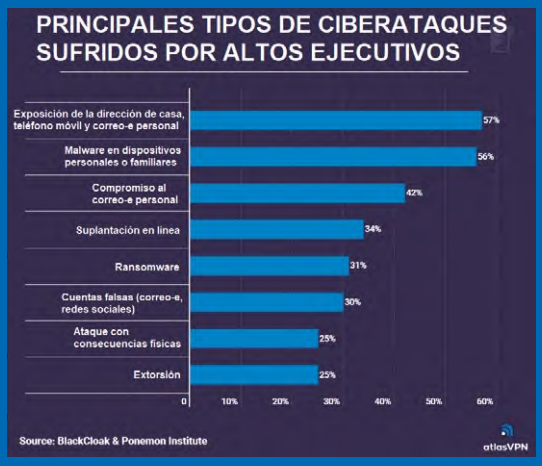
Contacto: **900 840 407** **strategic.accounts@watchguard.com** **www.watchguard.com**

Entre sus consecuencias está el robo de información confidencial, la suplantación e, incluso, posibles incidentes físicos

El 42% de los ejecutivos sufrió un ciberataque grave en los últimos dos años y sólo cuatro de cada 10 compañías protege de forma expresa a la alta dirección

El 42% de los ejecutivos o sus familiares experimentaron un ciberataque, cuyas consecuencias fueron tan graves como una violación de datos de toda la empresa, según un informe realizado, en mayo de 2023, por **BlackCloak** y el **Instituto Ponemon**, y del que se ha hecho eco **Atlas VPN**. En él, se muestra el impacto cada vez más notable de los ciberataques en la vida personal de los profesionales de la alta dirección.

El informe contó con la opinión de más de 500 profesionales de ciberseguridad de diferentes sectores y, entre los resultados obtenidos, también evidenció que gran parte de las empresas carecen de la preparación para prevenir o mitigar el daño potencial infligido a sus organizaciones. Entre las consecuencias, un 66% destacó la pérdida de clientes o socios comerciales, un 47% resaltó el robo de datos financieros confidenciales, un 36% confesó haber sufrido el robo de activos corporativos valiosos como la propiedad intelectual, un 33% daños reputacionales y un 27% la pérdida de clientes o empleados, afectando gravemente en un 24% de las ocasiones a la estrategia comercial y en un 18% a datos de investigación y desarrollo.



A ello, se suma que un 62% de las empresas no cuentan con un equipo dedicado a prevenir o responder a ataques contra los ejecutivos y sus familias.

Entre las amenazas dirigidas contra la alta dirección, según el estudio, destacan las infecciones de *malware* en dispositivos personales o familiares (56%), el compromiso del correo-e (42%), la suplantación de identidad en línea (34%), el *ransomware* (31%) e, incluso, ataques físicos como *swatting* (25%).

No es un tema nuevo: en **Securmática 2022** ya se prestó mucha atención a él en una ponencia del Global Chief Digital Security Officer de **Telefónica**, **Juan Carlos Gómez Castillo**, que mostró cómo la compañía tiene implementado una estrategia para asistir a la alta dirección en este tipo de situaciones.

El coste medio de una filtración de datos alcanza los cuatro millones de euros en 2023, su máximo histórico

IBM ha dado a conocer la nueva edición de su informe anual sobre el coste de las filtraciones de datos en el que destaca que, de media, ya suponen más de cuatro millones de euros en 2023, con un 15% de incremento, respecto a los últimos tres años, llegando a un máximo histórico. El estudio constató que, si bien el 95% de las organizaciones han experimentado más de una infracción en el último año, en el 57% de los casos se ha trasladado su coste a los consumidores y en un 51% ha supuesto un incremento de la inversión en ciberprotección.

Curiosamente, el estudio también destaca que la IA y la automatización han permitido incrementar la velocidad de respuesta en la identificación y contención de infracciones, marcándose una media de 214 días, en todo el ciclo de vida de la gestión de la brecha de seguridad, respecto a los 322 de las compañías que no usan esta tecnología. Además, es notable que las víctimas de *ransomware* que involucraron a los cuerpos y fuerzas de seguridad en la gestión del incidente ahorraron 425.000 euros respecto a las que no lo hicieron. De cualquier forma, el 37% de ellas no contactaron con ellos.

La POLITÉCNICA DE MADRID realiza una prueba práctica mostrando el éxito de los primeros desarrollos del proyecto europeo de ciberseguridad cuántica

La **Universidad Politécnica de Madrid** (UPM) está participando en el proyecto de creación de la **Infraestructura Europea de Comunicaciones Cuánticas** (EuroQCI), a través del desarrollo de un software basado en *redes* definidas por software (SDN). Para demostrar su eficacia, los responsables del proyecto han mostrado sus capacidades a través de una videoconferencia "ultrasegura", a escala, durante la jornada 'Digital Assembly' organizada por el **Consejo** y la **Comisión Europea**. Los investigadores que han participado en este desarrollo explican que, utilizando lo que se denomina "distribución cuántica de claves", es posible asegurar que los datos transmitidos a través de una red sean "invulnerables" a cualquier intento malicioso de interceptación o descifrado, inclusive si el atacante es un ordenador cuántico.

Además, esta videoconferencia, en vivo, ha sido la primera demostración técnica de la EuroQCI: una ambiciosa colaboración firmada por los 27 estados miembros, la Comisión y la **Agencia Espacial Europea.** El objetivo es establecer un canal "ultraseguro" de comunicaciones para las administraciones públicas, "salvaguardar" la infraestructura crítica y "fortalecer" los sistemas de encriptación en toda la UE.

CYBASQUE renueva su Junta Directiva apostando por la colaboración

Las 64 organizaciones de la **Asociación de Industrias de Ciberseguridad del País Vasco** (Cybasque), celebraron en Bilbao su Asamblea General Anual, en la que se han analizado las diferentes líneas de trabajo de la entidad, sus proyectos a corto y medio plazo, y se ha procedido a renovar parcialmente a su junta directiva.

Xabier Mitxelena, de la empresa **Cybertix,** ha sido reelegido presidente de la entidad y estará acompañado en la nueva junta por: **Álvaro Fraile** (**ITS-Ayesa**), **Jesús Urien** (**PwC**), **Azucena Hernández** (**Eurocybcar**), **Ángel Echevarría** (**Entelgy Innotec**), **David González** (**Ikerlan**), **Francisco Valencia** (**Secure&IT**), **Pablo Echevarría** (**S21Sec-Thales**), **Luis Á. del Valle** (**Sealpath**), **Gerard Vidal** (**Opscura**) y **Eder San Millán** (**Versiald**).

En la actualidad, la comunidad autónoma vasca aglutina al 10% de las entidades de ciberseguridad de España, según datos del **Basque CyberSecurity Centre**, dando trabajo a más de 4.500 personas en Euskadi.

LOGICALIS
Architects of Change

Blindaje Zero Trust para el gobierno de identidades y accesos

IBM Security Verify

La identidad y los privilegios de acceso se han convertido en el principal vector de ataque contra los activos digitales de una organización, tanto locales como en la nube. Según las estimaciones, el 70% de los usuarios cuenta con más privilegios de acceso de los que realmente necesita. Están sobreautorizados.

Esta realidad expone a las organizaciones a un riesgo fatal contra sus intereses tecnológicos y económicos. Pero, ¿cómo protegerse?

La tecnología Zero Trust de IBM es la respuesta más completa y eficaz a este gran desafío. Su familia pionera, IBM Security Verify, proporciona una gestión completa del gobierno de identidades y accesos, tanto en entornos locales como de nube híbrida.

Una alternativa, casi una filosofía, que busca siempre el equilibrio entre seguridad y facilidad de uso e incorpora novedades tecnológicas, como Single Sign-On, autenticación avanzada y acceso adaptativo.

Autorice en función del contexto, defiéndase de los ataques internos y proteja a sus empleados y clientes con IBM Security Verify.

Su cuenta de resultados lo agradecerá.

¿Necesita la mejor estrategia de defensa?

Si quiere saber más sobre IBM Security Verify descárguese el siguiente QR

¿Qué podemos hacer por su organización?

Contacte con Logicalis y conozca cómo podemos ayudarle.

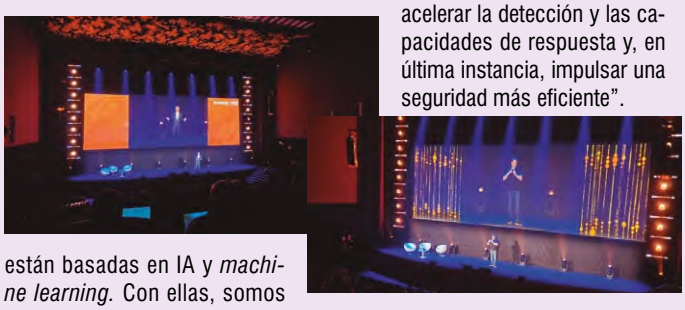
Para más información, visite www.es.logicalis.com

Email: marketing-es@es.logicalis.com

PALO ALTO NETWORKS destaca, en la edición española de su 'Ignite Tour', el impacto de la IA y el *machine learning* en ciberprotección

Palo Alto Networks celebró, poco antes de verano, y por primera vez en España, una edición de su evento 'Ignite Tour 2023', con la presencia de **Helmut Reisinger,** CEO de EMEA & Latinoamérica, junto a **Marc Sarrias,** Country Manager para Iberia de la compañía. En él, diferentes especialistas de la multinacional mostraron los principales hitos, la transformación del sector y la inversión en automatización, donde la IA acelera la detección y, en última instancia, impulsa una labor más eficaz para la seguridad de las empresas.

Entre otros aspectos de interés, sus analistas destacaron cómo el *ransomware* continúa siendo una de las grandes preocupaciones de las empresas, habiendo registrado pagos, por parte de una compañía, de 6,2 millones de euros, con un coste medio por incidente de 314.000 euros. Frente a ello, Reisinger recordó que "la ciberseguridad es un problema de datos, y la mejor forma de resolver estas cuestiones es con la ayuda de algoritmos basados en IA. Por eso, nuestras soluciones de seguridad de red, *cloud* y SOC optimizados



están basadas en IA y *machine learning.* Con ellas, somos capaces de detectar cada día 1,5 millones de nuevos ataques en todo el mundo".

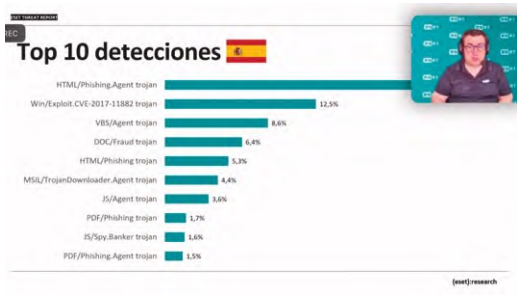
También, destacó que la principal táctica de extorsión, utilizada por el 70% de los grupos de cibercriminales, fue la amenaza de filtración de datos a través de la *dark web*, una cifra que supone un 30% más que en 2021. Por ello, Sarrias aconsejó a los "equipos de seguridad de nuestro país cambiar su forma de pensar sobre los SOC a una mentalidad que dé prioridad a la automatización para acelerar la detección y las capacidades de respuesta y, en última instancia, impulsar una seguridad más eficiente".

Durante la jornada, la compañía mostró también muchas de sus soluciones para proteger los datos críticos de las empresas y las aplicaciones que se ejecutan, permitiendo la defensa ante amenazas y ataques que podrían poner en peligro las operaciones críticas, el cumplimiento normativo y la seguridad de los propios trabajadores. Además, se recordó que, según su investigación, 'What 's Next in Cyber', casi la mitad de las empresas (47%) ya apuestan por la IA para una resolución más rápida de los incidentes de seguridad, además de considerarla determinante un 39% de los encuestados para la detección de amenazas, el triaje de alertas y la respuesta a incidentes pueden automatizarse casi por completo en el SOC.

Por otra parte, la empresa ha firmado un acuerdo con **Orange Business y Orange Cyberdefense** para ofrecer a las empresas una solución SASE gestionada de forma nativa en la nube, a través de modelo operativo simplificado para los clientes, con responsabilidad de extremo a extremo, mejorando su agilidad, eficiencia, rendimiento y seguridad.

ESPAÑA, primer país de Europa y el tercero del mundo más atacado por los ciberdelincuentes, según ESET

En su informe de amenazas, con datos de diciembre de 2022 a mayo de 2023, dado a conocer en rueda de prensa, **Eset** ha destacado que, durante la primera mitad de este año, muchos grupos de ciberdelincuentes han sido capaces de adaptarse para seguir logrando que sus ataques tuvieran éxito, explotando vulnerabilidades, obteniendo accesos no autorizados, robando y filtrando información y estafando a todo tipo de usuarios.



Además, a través de su director de Investigación y Concienciación en nuestro país, **Josep Albors,** se alertó de que España sigue siendo uno de los países donde más incidentes se producen, recordando casos destacados como los del **Hospital Clinic, Euskaltel** o **Telepizza,** entre otros.

Además, recordó que "una amenaza que ha regresado con fuerzas renovadas es la conocida como sextorsión". De cualquier forma también resaltó que "lo verdaderamente preocupante de este tipo de extorsión es que, recientemente, el FBI alertaba del uso de imágenes y vídeos manipulados por parte de delincuentes para extorsionar a las personas cuya imagen había sido utilizada de forma ilícita, algo que puede suponer un serio problema si esta práctica criminal se extiende".

WATCHGUARD celebra su 'Partner Roadshow' mostrando sus capacidades y su apuesta por el canal

La compañía ha realizado un *roadshow* dedicado a *partners*, bajo el nombre **'WatchGuard Sync',** dando a conocer los aspectos más relevantes de su portafolio en torno al puesto final, la migración a la nube y las ultimas novedades de producto, así como las "mejores tácticas de *x-sell* para aumentar ingresos, consejos y trucos del programa de *partners*", recordaron sus participantes. Así, entre otros aspectos se mostró lo más relevante sobre su propuesta de migración a WatchGuard Endpoint, el repaso de los principales modelos de su gama de cortafuegos Firebox, como su T45, entre otros, además de dar a conocer diferentes casos de uso de su WatchGuard Authpoint, su herramienta de autenticación multifactor, además de su XDR y del servicio red SYNC, del que se pudo conocer a fondo sus capacidades.

Aprovechando la jornada, y ante las preguntas de SIC, el *country* manager de la compañía para Iberia, **Carlos Vieira**, explicó que, entre otros grandes retos, para el corto plazo la empresa va a apostar fuerte por el XDR, por ayudar a los socios de canal en su camino hacia el enfoque de SOC de Watchguard, así como por sus MRD Services. A largo plazo, "hay áreas que estamos investigando para entrar y desarrollar y, en mi opinión personal, serán algunas como SASE o *Firewall as a Service* y otras tecnologías. Áreas que estamos monitorizando para adquirir compañías o realizar desarrollos propios en este ámbito", puntualizó.

Centro de
Ciberseguridad Industrial

XXI International Experiences Congress

Industrial Cybersecurity – *Bilbao*

Del 3 al 5 de octubre de 2023

Virtual y presencial en Hotel Occidental Bilbao

ANFITRIÓN

Basque CyberSecurity Centre

PATROCINADORES **GOLD**

accenture · Capgemini · Cyberium · Deloitte. · Entelgy Innotec Security · Fortinet · kaspersky · Phoenix Contact · Rockwell Automation · S2 Grupo · SIA An Indra company · Siemens · Stormshield · tecnalia Member of Basque Research & Technology Alliance · Telefónica Tech · tenable · txOne networks

PATROCINADORES **SILVER**

getronics · Radiflow

PATROCINADORES **BRONZE**

SECUREIT by LKS

APOYO INSTITUCIONAL

CNPIC · Fundación Borredá · incibe_ 017 · ISA Sección Española · PESI · red seguridad · TEDAE

El Foro Económico Mundial se hace eco de un estudio, de la Universidad de Oxford, que analiza el enfoque de ciberprotección frente a la capacidad de recuperación en la alta dirección

Los CEO entienden mejor el concepto de resiliencia cibernética que el de ciberseguridad y consideran un error confiar ciegamente en el equipo técnico

El **Foro Económico Mundial** (**WEF**) se ha hecho eco de los resultados del estudio de la **Universidad de Oxford** e **ISTARI**, sobre el estado de la ciberseguridad y la resiliencia en el ámbito corporativo, con la participación de 37 altos ejecutivos de multinacionales de EE.UU., Europa y Asia. Entre ellos, se contó con nueve CEO que han tenido que gestionar ciberataques "devastadores" en sus organizaciones.

Así, entre otros datos de interés, la gran mayoría de los preguntados (72%) confesaron "sentirse incómodos" al tomar decisiones de seguridad cibernética y, por ello, prefieren hablar en su lugar del concepto de resiliencia delegando en el CISO lo respectivo a la ciberprotección. "Los hallazgos presentan una oportunidad para que los CISO alienten de manera proactiva a sus CEO a avanzar hacia un estado de confianza informada", destaca el WEF en un artículo en su web. Además, comprender cómo piensan y sienten los directores ejecutivos en este sentido, "les permite apoyar de manera más efectiva a su CEO en la gestión del riesgo cibernético y solicitar un apoyo más significativo para sus iniciativas", recuerda el informe. Entre otras razones, el documento explica que la mayoría de los directores ejecutivos han ascendido de rango a través de dominios comerciales tradicionales, como finanzas, operaciones o marketing y muy pocos comenzaron su carrera en tecnología y mucho menos en ciberprotección, por lo que "muy pocos están familiarizados con estos conceptos".

La investigación también evidenció que los CEO se sintieron cómodos al pasar a una conversación sobre resiliencia cibernética, que fue puesta en valor, de forma notable, por los que ya han sufrido un ciberataque de gravedad. "Experimentar un ataque les hizo comprender que la protección perfecta es un juego perdido. En cambio, comenzaron a verlo como una 'sorpresa predecible' que todas las organizaciones pueden sufrir. Por lo tanto, cambiaron su prioridad estratégica para mejorar la resiliencia cibernética de su organización", dice el estudio.

Por último, es muy revelador que todos los participantes destacaran su confianza en sus equipos de ciberseguridad para hacer su trabajo, aunque los que habían sufrido un ciberataque también reconocieron que "hacerlo ciegamente" fue un error, habiendo sido necesario una mejor "comprensión" y conciencia de los trabajos que realizan los expertos técnicos, según resalta el estudio entre sus conclusiones.

ENISA propone un marco de seguridad para la IA y alerta de los ciberriesgos del sector Salud

"¿Es posible una IA segura y confiable? La UE lidera el camino", bajo esta premisa la **Agencia de Ciberseguridad de la Unión Europea** (Enisa) publicó en verano cuatro informes sobre los retos más trascendentales de la IA, buscando establecer buenas prácticas en este ámbito. Así, el primero de ellos, ofrece un marco escalable para guiar a las autoridades nacionales de ciberseguridad (NCA) y la comunidad de IA para asegurar los sistemas, operaciones y procesos de Inteligencia Artificial.

Junto a ello, ha dado a conocer otro dedicado a la ciberseguridad y privacidad en IA en dos casos de uso: previsión de demandas en redes eléctricas y diagnóstico por imagen médica. Además, ha publicado otro sobre 'Investigación en IA y ciberseguridad' en el que identifica cinco necesidades que se deberían tener en cuenta en futuros desarrollos de políticas e iniciativas de financiación de la UE.

Amenazas en Salud

Enisa también ha publicado su primer panorama de amenazas cibernéticas para el sector de la Salud, donde el *ransomware* representa el 54% de los ataques. Los datos de los pacientes, incluidas las historias clínicas electrónicas, fueron los activos más atacados (30%). De manera alarmante, dice el informe, casi la mitad de todos los incidentes (46%) tuvieron como objetivo robar o filtrar datos de organizaciones de salud. Los hospitales, en particular, fueron los más afectados (42% de los incidentes informados). Les siguen, las autoridades, organismos y agencias de salud (14%) y la industria farmacéutica (9%). El análisis se basa en un total de 215 incidentes informados públicamente en la UE y los países vecinos.

Confianza de Enisa en empresas españolas

Además, Enisa ha confiado el desarrollo de sus servicios web en la tecnológica coruñesa **Altia** que, junto con **Bilbomatica,** que también forma parte de su grupo, ha ganado el contrato marco de 2,4 millones de euros que sacó a concurso público para el desarrollo de servicios informáticos en su página web.

Por otro lado, cabe destacar que la Agencia ha abierto un periodo de consultas abiertas, hasta el 16 de septiembre, para la evaluación de su propuesta Marco Europeo de Certificación de Ciberseguridad.

La comunidad ASRG alcanza más de 15.000 socios compartiendo información para reducir las vulnerabilidades en automoción

Lo que comenzó en 2016 como una idea sencilla, crear una comunidad de profesionales de ciberseguridad especializados en automoción que, compartiendo información, permitieran a las marcas de coches incorporar sistemas más seguros por diseño, se ha convertido en uno de los referentes del sector y, actualmente, el **Grupo de Investigación de Seguridad Automotriz** (ASRG, por sus siglas en inglés) ya supera los 15.000 asociados, en 57 lugares, cada una con autonomía y eso sí, al margen de los acuerdos de confidencialidad que cuentan los participantes con las empresas para las que trabajan, en pro de "promover el desarrollo de soluciones de seguridad para productos automotrices".

Así, a través del ASGR también se plantean debates sobre cómo se deberían dividir las redes en un coche o la necesidad de averiguar quién está haciendo qué función y qué unidad de control electrónico (ECU) para implementar de forma práctica la ciberseguridad por diseño, por cuanto "muchas de las vulnerabilidades que llegan a los vehículos comenzaron en la cadena de suministro de software mucho antes de que se entregara al fabricante del vehículo", destaca su gran impulsor, **John Heldreth**, jefe de operaciones de ciberseguridad automotriz en **Volkswagen AG.**

MDR

Servicio de Monitorización y Respuesta que combina la visibilidad de la infraestructura proporcionada por la SIEM y las capacidades de detección y respuesta de la plataforma EDR. Diseñado para alinear las necesidades del cliente, **dando respuesta a los incidentes de forma automática**.

38%

Es el crecimiento de los ciberataques globales durante 2022 en comparación con 2021.

41%

De los incidentes de seguridad durante 2022 involucró phishing, malware o ransomware.

43%

De los ataques tuvieron como objetivo a las PYME, donde la seguridad es menos robusta.

¿Qué ventajas ofrece?

- Alineado con las necesidades y criticidades del negocio.
- Monitorización global utilizando múltiples tecnologías.
- Herramienta requerida en múltiples regulaciones y normativas.
- Enriquecido con Threat Intel de S21sec.
- Evolución e innovación alineada con la madurez del cliente.
- Respuesta automatizada ante incidencias, y respuesta forense ante incidentes críticos.

Solicita una llamada con un ***Experto de S21sec:***

+34 900 840 730

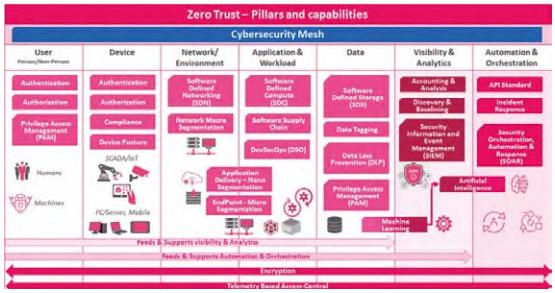
www.s21sec.com

marketing@s21sec.com

S21SEC

Cyber Solutions by Thales

Los ciberataques globales crecen un 8% y alcanzan la cifra récord de 1.258 ataques por semana, la cifra más alta de los dos últimos años



Check Point Research, la división de Inteligencia de Amenazas de la firma de ciberseguridad, ha publicado su Informe Global de Ciberataques del segundo trimestre de 2023, en el que se muestra que han aumentado un 8% los ataques producidos por semana, respecto al mismo periodo del año pasado, alcanzando el punto más alto de los últimos dos años con un promedio de 1.258 ciberataques.

Por sectores, los más afectados son los de educación e investigación, y el de gobierno y militar, con una media de 2.179 y 1.772 incidentes semanales, respectivamente. No obstante, el cambio más significativo se produjo en los sectores minorista y mayorista, así como en consultoría, con un aumento interanual del 38%, lo que se traduce en 1.105 y 958 ataques semanales, respectivamente.

Por áreas geográficas, Europa logró evitar el fuerte crecimiento, siendo la región menos afectada, aunque los datos muestran un aumento del 5%. España consiguió invertir esta cifra, con una disminución del 5% para asentarse en los 1.154 ciberataques por semana. Las regiones más afectadas fueron África (con un 23%) y APAC (22%).

El estudio también destaca que, durante el segundo trimestre de 2023, una de cada 44 organizaciones en todo el mundo sufrió un *ransomware*, lo que representa una disminución del 9% respecto a 2022. Las industrias más afectadas fueron las de gobierno/militar, el sector de la salud y el de educación/investigación.

Protección en la nube

Junto a ello, Check Point, también publicó una interesante investigación, en colaboración con **Cybersecurity Insiders**, bajo el título, 'Cloud Security Report 2023'. Para llevarla a cabo contó con la opinión de más de 1.000 profesionales de todo el mundo y, en ella, destaca la preocupación por parte del 76% de las empresas participantes ante el aumento de los ataques a las redes basadas en *cloud*. Además, el 60% indica que la mala o inadecuada configuración de las plataformas en la nube es la amenaza más importante. De hecho, más del 70% tiene dificultades para gestionar el acceso a múltiples soluciones de ciberprotección. Algunos de los principales problemas son la falta de visibilidad y control. A ello se suma que el 58% de las empresas tiene previsto almacenar más de la mitad de su carga de trabajo en la nube.

Por otra parte, la compañía ha sido reconocida como 'líder' en el informe 'The Forrester Wave: Enterprise Email Security Q2 2023', por las destacadas capacidades de protección que ofrece su solución Harmony Email & Collaboration.

VMWARE y otros gigantes tecnológicos refuerzan su apuesta por los estándares informáticos confidenciales

La multinacional **VMware** ha anunciado una nueva asociación de referentes tecnológicos para acelerar el desarrollo de aplicaciones informáticas confidenciales. Como se sabe, la computación confidencial se basa en un entorno de ejecución confiable para salvaguardar la integridad y confidencialidad de las aplicaciones y los datos, incluso en la nube y en la infraestructura de terceros.

Entre otras iniciativas, para lograrlo VMware ha estado trabajando en el proyecto Certifier Framework for Confidential Computing, que también ha sido apoyado por **AMD, Samsung** y miembros de la comunidad **RISC-V Keystone.**

"La API de Certifier simplifica y unifica en gran medida el soporte de operaciones y programación para plataformas informáticas confidenciales de múltiples proveedores al proporcionar una administración simple de la confianza del cliente, incluida la evaluación de atestación, el almacenamiento seguro, la inicialización de la plataforma, el intercambio de secretos, los canales seguros y otros servicios", destacan, entre otros aspectos, los responsables de VMware.

"La computación confidencial tiene el potencial de proteger las cargas de trabajo sin importar dónde se ejecuten, incluso en configuraciones de múltiples nubes y perimetrales. El desafío ha sido ayudar a los clientes a adoptar e implementar el estándar con facilidad", ha destacado el CTO de VMware, **Kit Colbert.**

El *malware* impulsado por IA, principal preocupación de las empresas españolas en la seguridad de las identidades digitales

En su informe '2023 Identity Security Threat Landscape Report', realizado junto con **Vanson Bourne, CyberArk** analiza cómo las difíciles condiciones económicas y la innovación tecnológica, con la evolución de la IA, junto con un esperado crecimiento del 217% de identidades humanas y de máquinas, están aumento los riesgos basados en la identidad digital. De hecho, en el estudio, realizado a 500 profesionales de 16 países (entre ellos, España), destaca que el 99% de los profesionales de seguridad españoles encuestados esperan que las amenazas habilitadas por IA afecten a su organización este año, con el *malware* impulsado por IA como preocupación principal.

Así, resalta que todas las empresas españolas participantes prevén este año problemas relacionados con la identidad derivados de recortes impulsados por la economía, factores geopolíticos, la adopción de la nube y el trabajo híbrido. Mientras que un 50% afirma que esto sucederá como parte de una iniciativa de transformación digital, como la adopción de la nube o la migración de aplicaciones heredadas. Además, en España un 69% espera problemas relacionados con la ciberseguridad debido a la rotación de empleados. También, es de interés que, en el mundo, un 68% destacó que implementarán más herramientas SaaS en los próximos 12 meses en comparación con lo que tienen ahora.

Superficie de ataque ampliada

El informe también subraya que el 57% de las empresas españolas considera que el acceso a datos de elevada sensibilidad por parte de los empleados no está adecuadamente asegurado y que es mayor el número de máquinas que tiene acceso a datos sensibles frente al número de humanos.

En concreto, el acceso a las credenciales sigue siendo el primer riesgo para los encuestados en España (37%), seguido de la evasión de la defensa (30%), la ejecución (33%), el acceso inicial (21%) y la escalada de privilegios (26%).

EXCLUSIVE NETWORKS

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.

allot ARISTA CLOUDIAN Cymulate druva exabeam

Extreme networks FORTINET Gigamon HashiCorp HYCU imperva

infoblox LogRhythm MORPHEUS netskope NOZOMI NETWORKS ONE IDENTITY

paloalto NETWORKS proofpoint rubrik SentinelOne sysdig TANIUM

tenable THALES ThriveDX tufin wasabi ZIMPERIUM

www.exclusive-networks.com/es

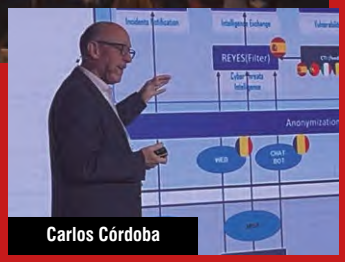
Se mostraron los grandes retos en su cumplimiento y cómo los están acometiendo desde consejerías públicas, hasta *startups*

El 'V Encuentro del ENS', del CCN, muestra los avances en la adecuación a su nueva versión, los retos de la RNS y visibiliza la necesidad de crear una Agencia Nacional de Ciberseguridad

Bajo el lema 'La gestión de la ciberseguridad como tarea clave', la quinta edición de los 'Encuentros ENS' contó con más de 400 personas de forma presencial y más de 1.500 en remoto. La jornada fue inaugurada por la directora del **CNI, Esperanza Casteleiro,** quién recordó que hay que "ser conscientes de que los actores están bien preparados y buscan una oportunidad para llevar a cabo ciberataques de alto impacto". Frente a ellos, destacó que hay que "ofrecer una defensa común". En este sentido, puso en valor el Esquema Nacional de Seguridad (ENS) como una "adecuada línea de defensa y prevención". Además, aprovechando el congreso, el CCN otorgó a título póstumo el Premio a la contribución a que el ENS sea un estándar de referencia a **Joaquín Seco**, de la empresa **CSA**, con más de 20 años de experiencia, cuyo galardón recogió su viuda, **Rosana Zamora.**

Esperanza Casteleiro

Miguel Angel Amutio



Carlos Córdoba

La jornada comenzó con una ponencia del jefe de Área de Normativa y Servicios de Ciberseguridad del CCN, **Pablo López,** quien mostró cómo ha evolucionado el Esquema y cuáles son sus retos, con el objetivo de "conseguir diagnósticos proactivos", además de resaltar la importancia de que todo el mundo aporte para continuar mejorándolo. Acto seguido, **Rocío Alvarez,** ingeniera del CCN, habló de los riesgos de la cadena de suministro y cómo hacerles frente con la metodología 'C-SCRM'. También, fue muy seguida la exposición de **Mar de las Heras**, de **Procesia,** y **Alberto Francoso**, de la **OCC,** del **Mº de Interior,** sobre cómo contar con un proceso eficaz de ciberseguridad, a través de las metodologías como μCeENS, que facilita alcanzar la Certificación de Conformidad con el ENS.

A continuación, se sucedieron interesante exposiciones de **Carlos Seisdedos** (**ISecAuditors**) y **Antonio Grimaltos** (**Comunidad Valenciana**), **Myriam Sánchez** (**Accenture**), **Gloria Tamayo** (**WatchGuard-Cytomic**), **Alberto Olmos** (**S2 Grupo**) **Marcos Rubio** (**Tucuvi**), **Antonio Ramos** (**Leet**) **Eduardo Solís** (**Entelgy Innotec**), **José C. Cerezo** (**Google**) y **José M. Cardona** (**Google**).

Finalizaron las jornadas dos conferencias muy ilustrativas, a cargo del director de Planificación y Coordinación de Ciberseguridad de la **Secretaría General de Administración Digital**, **Miguel Ángel Amutio,** que repasó cómo encaran la ciberprotección países como EE.UU. y mostró en profundidad cómo lo está haciendo Europa. Por su parte, el jefe del Área de Centros de Operaciones de Ciberseguridad del CCN, **Carlos Córdoba,** puso en valor que "la Red Nacional de SOC ya que es un proyecto que se está abordando a nivel europeo", y animó a los representantes de la industria presentes a adherirse a él. Para finalizar, **Javier Candau,** jefe del Departamento de Ciberseguridad del CCN, clausuró el encuentro haciendo un balance de todo lo expuesto durante la jornada.

"La Agencia Nacional de Ciberseguridad no es cuestión de ser o no ser: la cuestión es cuándo y cómo"

Como colofón a la sesión matinal, se celebró un panel sobre 'El gobierno de la ciberseguridad nacional, hacia dónde vamos', moderado por el editor de **Revista SIC**, **Luis Fernández**, y en el que participaron **Rafael García** (**Mando Conjunto del Ciberespacio**), **Luis Jiménez** (Subdirector General del **CCN**), **Álvaro de Lossada** (**Oficina de Coordinación de Ciberseguridad** del **Mº del Interior**), **Tomás Roy** (**Agencia de Ciberseguridad de Cataluña**), **Miguel Martín** (**Incibe**) y **Andrés Ruiz** (**Departamento de Seguridad Nacional**).

Participantes en el debate

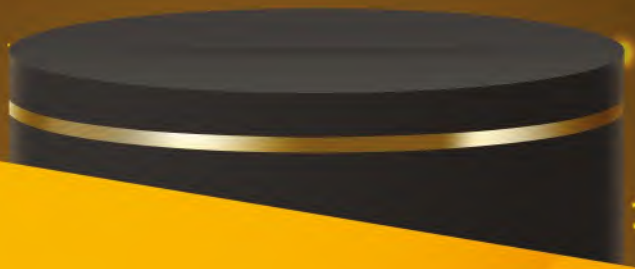
En él, se abordaron asuntos relevantes sobre la llevanza de la ciberprotección nacional quedando patentes la pluralidad de puntos de vista, pero, sin duda, el tema más trascendente y que más controversia suscitó fue si se debería crear una Agencia Nacional de Ciberseguridad, algo que en la mayoría de estados europeos y de nuestro entorno occidental, es un hecho. Igualmente, cómo y quién debería estar al frente, así como bajo qué paraguas debería estar ubicada, cuáles serían sus capacidades, coordinacion y disponibilidad de recursos, fueron aspectos nada triviales en los que los participantes dejaron entrever 'sensibilidades' distintas.

También, se dio a conocer que, aprovechando la trasposición de NIS2, verá la luz una tercera Estrategia Nacional, según Ruiz, así como el buen trabajo de España en ciberprotección, en palabras de Jiménez.

Por su parte, el general García Hernández destacó la necesidad de mayor concienciación teniendo en cuenta que "el ciberespacio es único, no existe una parte militar separada de una civil". Martin consideró que en ciberseguridad "hay margen de mejora" pero "estamos haciendo muchas iniciativas que van marcando el camino". Precisamente, De Lossada comentó el esfuerzo que se está realizando en la mejora de capacidades, en Interior, para luchar contra el cibercrimen. Roy destacó la importancia de la colaboración y coordinación "imprescindibles" para tener éxito en protección cibernética.

HORNETSECURITY

365 PERMISSION MANAGER



MEJORA TU CUMPLIMIENTO EN MICROSOFT 365

- OBTÉN UNA FÁCIL VISTA GENERAL DE LOS PERMISOS
- DEFINE DIRECTIVAS DE USO COMPARTIDO
- IDENTIFICA Y AUDITA INFRACCIONES

PRUEBA AHORA GRATIS

BEDISRUPTIVE y la FUNDACIÓN GOODJOB firman un acuerdo para favorecer la inclusión laboral de personas con discapacidad

BeDisruptive ha firmado un acuerdo de colaboración con la **Fundación GoodJob** para participar en el Programa IMPACT#include, la iniciativa de empleabilidad impulsada por la Fundación con el objetivo de dar acceso al mercado de trabajo ordinario a personas con discapacidad en el sector.

Este convenio cumplirá dos objetivos muy importantes: por un lado, la compañía desarrollará uno de los ejes fundamentales de su política de Responsabilidad Social Corporativa (RSC), como es favorecer la inclusión sociolaboral de personas con discapacidad; y, por otro lado, la Fundación GoodJob seguirá desarrollando su objetivo principal, la inserción laboral de estas personas en la empresa ordinaria. De hecho, BeDisruptive ya ha incorporado a las dos primeras personas a través de este programa en el puesto de Cybersecurity Assistants, donde tendrán importantes funciones como las de dar soporte a los servicios gestionados del BeSOC. Además, para incentivar la participación de los empleados de BeDisruptive en sus proyectos de RSC y que puedan aportar su *expertise,* se ha puesto en marcha un programa de voluntariado, por el cual la compañía computa un porcentaje de las horas en las que realice dicho voluntariado como horas laborales.

Programa pionero

Hasta el momento, en el Programa IMPACT#include, el primero de este tipo realizado en España, en el que **SIC** es impulsor desde sus inicios, se han formado en siete ediciones 350 personas con discapacidad de diferentes áreas geográficas de España y cerca del 70% de ellas han conseguido empleo tras esta capacitación (datos hasta la sexta edición del programa). En septiembre dará comienzo la octava edición.

ASSECO SPAIN GROUP presenta un nuevo *holding* poniendo en marcha SORA ANZEN COMPANY, su nueva marca de ciberseguridad

Asseco Spain Group, multinacional tecnológica con más de tres décadas de experiencia en el mercado y una sólida presencia en España, dio a conocer la creación de su nuevo *holding*. Se trata de un movimiento estratégico que apuesta por la especialización de sus servicios para satisfacer las necesidades de sus clientes y del mercado. El objetivo a largo plazo de la compañía es seguir impulsando la transformación digital y la innovación para liderar la vanguardia tecnológica y la producción de software en Europa.

El nuevo *holding* corporativo Asseco Spain Group estará compuesto por: **Sora Anzen Company** (especializada en ciberseguridad), **AID Solutions** (centrada e IA, Data analytics e IoT), **Raxon** (de Infraestructuras y soluciones de IT) y **Valorista** (de soluciones globales de IT y servicios de alto valor). En concreto, Sora Anzen Company se enfocará en servicios de ciberprotección avanzada, ofreciendo soluciones para infraestructuras de IT, auditorías de seguridad, simulacros de ataques y un Centro de Seguridad Gestionado.

BREVES

■ **Revista SIC** ha publicado la actualización de su cuadro de CERT/CSIRT, con sede en España, en los principales foros de referencia como **Enisa, First, Trusted Introducer** y **Csirt.es**. Entre otras novedades, destaca el cambio de nombre de eSOC **Ingenia** a eSOC **Babel,** tanto en First como en Csirt.es; la entrada en First de InnovaSUR-CSIRT y la de LiveSOC CSIRT, de **Inetum**; así como el cambio de denominación de **CSA**-CSIRT a CSA Global CSIRT. Además, sale de todos los foros **NUNSYS**-CSIRT y entran en el listado de **Enisa** el BeSOC, de **BeDisruptive**, **Aiuken** CSIRT (aunque ya estaba Cert-Aiuken), **Evolutio**-CERT, GCT-CSIRT (ES) de Grail Cyber Tech, **P3rseus** CERT.

■ **Teldat** está trabajando junto a **Check Point** en un nuevo conjunto de herramientas Secure Access Service Edge (SASE), basadas en la SD-WAN de Teldat. Además, poniendo en valor su trabajo en este ámbito, la empresa acaba de recibir el sello 'Cybersecurity Made in Europe', que entrega la **European DIGITAL SME Alliance.**

■ **Getronics** ha inaugurado nuevas instalaciones para su Centro de Operaciones de Seguridad en Barcelona con el que dará soporte 24x7 en materia de ciberseguridad a empresas de todo el mundo. Cuenta con un equipo de cerca de 30 expertos dedicados a monitorizar, evaluar y reaccionar proactivamente ante cualquier tipo de ataque.

■ **Isaca** se ha sumado a la **Organización Europea de Ciberseguridad** (ECSO) "con el objetivo de avanzar en este ámbito, fomentar la colaboración e impulsar la confianza digital en toda Europa". Su participación permitirá "compartir su experiencia, recursos e iniciativas". También servirá, según destacan desde la asociación, "para potenciar de múltiples maneras la iniciativa **Women4Cyber** de ECSO y el programa SheLeadsTech, de la fundación One In Tech de Isaca".

■ Las compañías **LastPass y Varonis** ha firmado un acuerdo de distribución para Iberia con el mayorista **Ingecom**. A través del primero, ofrecerá su solución para complementar otras de su portafolio como las de **Okta** y **Yubico**, ampliando el área de IAM/MFA. Con el segundo, espera mejorar su oferta de protección del dato a través de la solución Varonis Data Security Platform que busca identificar y proteger los datos corporativos, así como la detección de amenazas internas y ciberataques, además de facilitar los trabajos de cumplimiento.

■ **Acronis** y **Also** han renovado su acuerdo en Iberia para apoyar la evolución de los proveedores de servicios en la península. "La simplificación y una mejor resiliencia están en el centro de la demanda del mercado y las soluciones de ciberprotección de Acronis, junto con las capacidades de mercado de Also, están construidas para proporcionar beneficios relevantes al canal: mayor seguridad, optimización de costes y, en general, una mejor experiencia operativa", destacan.

■ **Nunsys** ha adquirido a la empresa valenciana de ingeniería de servicios industriales **Esfera Ingeniería**, que la permitirá, a través del Grupo Nunsys+Sothis fortalecer su equipo de procesos, con amplio *expertise* en el sector alimentario, e integrar soluciones complementarias en el ámbito farmacéutico y químico-cosmético. Esfera Ingeniería está compuesta por un equipo de más de 60 profesionales y una experiencia de más de dos décadas, con proyectos realizados en más de 15 países.

■ El Código de Derecho de Ciberseguridad, recopilado y editado por el **Incibe,** fue actualizado a finales de julio con la inclusión de la Orden INT/859/2023, de 21 julio, en la que se desarrolla la estructura orgánica y funciones de los servicios centrales y territoriales de la Dirección General de la Policía. El código se puede descargar del BOE.

NO PENSAR EN LOS RIESGOS PUEDE SER FATAL PARA TU NEGOCIO

NUESTRA MISIÓN ES PROTEGERLO

- Análisis y Consultoría Seguridad
- Formación y Sensibilización de Empleados
- Implantación de Soluciones tecnológicas
- Soporte, Monitorización y Mantenimiento
- Auditoría de Seguridad y test de intrusión
- Procedimientos y Cumplimiento normativo
- Outsourcing & Headhunting
- Ciberseguridad para PYMES

European Commission
Horizon 2020
European Union funding for Research & Innovation
SEAL OF EXCELLENCE

www.all4sec.es | info@all4sec.es
916 366 544

S·C PREMIOS 2017

V-VALLEY distribuirá las soluciones de OASIX, del GRUPO AIRE, además de incorporar la propuesta de VU

V-Valley ha firmado sendos acuerdos de distribución con **Oasix,** la división de *cloud* y centros de datos del Grupo Aire, y **VU**. Respecto del primero, son expertos en ofrecer soluciones innovadoras para que empresas y organismos públicos puedan disponer de herramientas eficaces para acometer su transformación digital. Con esta nube pública española, los clientes de V-Valley podrán crear y gestionar una infraestructura virtual *cloud*, ampliarla y reducirla en tiempo real según sus necesidades de negocio, y pagar únicamente por los recursos IT que necesiten. Todo ello en un entorno seguro gracias a su alta exigencia en protección y compromiso con el cumplimiento del Esquema Nacional de Seguridad (ENS) nivel alto.

Como se sabe, Oasix cuenta con un amplio abanico de servicios IT automatizados y altamente eficientes, que se centran en crear infraestructuras fáciles de implementar y disponibles para consumir en la modalidad *as a Service* o de pago por uso, permitiendo a los *partners* disponer de sus soluciones sin depender de grandes inversiones. Además, Oasix apuesta por la cercanía del dato, y ofrece una conectividad de ultra baja latencia y sistema Anti-DDoS incluido en todos sus servicios.

En paralelo, **VU** también se ha incorporado al catálogo de V-Valley, ofreciendo sus soluciones de "protección de identidad y prevención de fraudes mediante la construcción de experiencias digitales seguras y sin fricciones, tanto para usuario final como para empresas, a lo largo de un proceso de transformación digital". Gracias a este acuerdo, los clientes del mayorista podrán acceder a las soluciones del fabricante, teniendo acceso a la gestión del ciclo de vida completo del usuario gracias a sus productos de Authentication Management y Onboarding Management.

TARLOGIC firma un acuerdo con la multinacional CHECKMARX para reforzar sus servicios de pruebas de seguridad de aplicaciones

Tarlogic Security y **Checkmarx** han llegado a un acuerdo para que la compañía de ciberseguridad española forme parte del programa de socios proveedores de servicios de seguridad gestionados (MSSP) de Checkmarx, una empresa especializada en la fabricación de tecnología orientada a la revisión de aplicaciones. La alianza con la multinacional, permitirá a la firma gallega ayudar a las empresas a evaluar su software de una forma más rápida y eficiente.

Así, Tarlogic, que cuenta con sedes en Santiago de Compostela y Madrid, empleará la plataforma Checkmarx One Application Security Platform, para prestar los servicios de pruebas de seguridad de aplicaciones a sus clientes en todo el mundo. Esta solución nativa *cloud* contribuirá a potenciar el catálogo de servicios de Application Security Testing (AST) de Tarlogic a través de capacidades como análisis estático del código fuente (SAST), análisis de composición de software (SCA), seguridad de la cadena de suministro (SCS) o pruebas de seguridad de aplicaciones dinámicas (DAST). Además, de cara a listar las APIs presentes en código fuente y eliminar las APIs fantasmas y mitigar los riesgos, también ofrece la protección necesaria, así como en modo *Infraestructure as code Security* (IaC) para analizar la infraestructura IT y detectar configuraciones inseguras que puedan poner en riesgo a una organización.

La decisión de llegar a un acuerdo de colaboración con una empresa como Checkmarx forma parte de la estrategia de internacionalización de Tarlogic, que ya está presente Estados Unidos, Europa y Oriente medio.

NOMBRAMIENTOS


● Quien venía siendo en los últimos años CISO Global del Grupo, **Daniel Barriuso**, la multinacional financiera española **Santander** le ha promocionado a Chief Transformation Officer, sucediéndoles en las tareas de ciberprotección **Hazel Díez Castaño,** como Global Chief Information Security Officer. Barriuso, uno de los más destacados profesionales españoles en este ámbito, además es Presidente del Consejo de FS-ISAC Europa, y fue responsable de ciberseguridad en BP, Credit Suisse y ABN Amro, entre otras. Por su parte, Díez fue Global CISO en Dufry Group, así como en Santander Global Tech y ocupó roles de responsabilidad en Aviva y Deloitte, entre otras. Es Ingeniera Informática por la Universidad de Nebrija.


● **BBVA** ha reconocido la buena labor de **Mariano Rebollo** y de **Carlos del Amo** ascendiéndoles a CISO Corporate Functions Engineering y a Global Head of Red Team, respectivamente. Rebollo es físico por la UAM y, con anterioridad, ocupó roles de responsabilidad en Mapfre, BearingPoint y Arthur Andersen Business Consulting, entre otras. Del Amo, hasta ahora Purple Team Global Manager de la entidad, cuenta con amplia experiencia habiendo trabajado para GMV, WIPO y Accenture. Es ingeniero de Telecomunicaciones por la Politécnica de Madrid.

● **Carlos Requena** es el Director General de **FrauDfense**, compañía que aglutina las iniciativas antifraude de las entidades Banco Santander, BBVA y CaixaBank, presentada ante los diferentes supervisores y reguladores competentes. Especializado en Prevención del Fraude y Ciberseguridad, cuenta con una muy amplia experiencia en banco líder, especializado en la Prevención de Fraude y en el desarrollo de Proyectos Estratégicos: puesta en funcionamiento del área de Fraude y la creación de un banco 100% digital.

● **Banco Sabadell** ha fichado a **Pedro Frutos** como IT & Data Risk Control Director. Ingeniero Superior de Telecomunicaciones por la ETSIT, en la Universidad Politécnica de Madrid, ha desempeñado gran parte de su trayectoria en la firma EY.

● **Laura Iglesias** ha sido ascendida a Head of Cyber Security Spain & EU Cluster en **Vodafone.** Ha ocupado cargos de responsabilidad en entidades como Banco Santander donde ha llegado a ser Global Head of Cybersecurity Strategy, además de haber trabajado para Telefónica y Produban, entre otras. Es ingeniera de Telecomunicaciones por la Universidad de Valladolid.


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

La inversión pública en ciberseguridad alcanzó los 81 millones de euros en el primer semestre del año

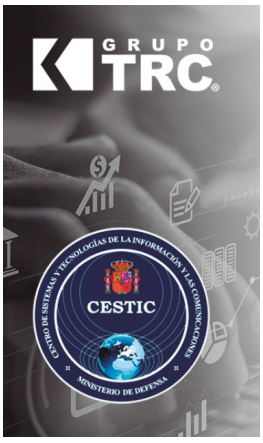
Pese al incremento de ciberataques a organismos públicos, las convocatorias electorales han propiciado una reducción en el número de adjudicaciones e inversiones en ciberseguridad en el primer semestre del año. Según datos de la plataforma **AdjudicacionesTIC,** de enero a junio la inversión de la Administración Pública en este ámbito fue de algo más de 81 millones de euros, repartidos en 300 adjudicaciones, un 33,1% menos que en el mismo periodo de 2022.

El organismo público más dinámico fue la **Administración General del Estado** con 72 contratos por un valor de 44,78 millones de euros. Destacan los 17 contratos del **Ministerio de Defensa** por 9,49 millones de euros, los dos por 8,21 millones de la **Gerencia de Informática de la Seguridad Social** (GISS) y los 4,63 millones de un contrato de la **Agencia de Ciberseguridad de Cataluña.**

La inversión por parte de las CC.AA. representó el 28,94%, siendo Cataluña, la Comunidad de Madrid y Aragón las zonas más activas. Entre otros proyectos, los más importantes fueron el de 'Servicios de seguridad de los sistemas de información de la **Seguridad Social**', adjudicado por 6,9 millones a **Indra** (lote 1) y el contrato del Acuerdo Marco, 'Adquisición, instalación y puesta en servicio de equipamiento para dotar a varias ubicaciones de la **Comunidad de Madrid** de infraestructura de comunicaciones para conectarse con seguridad a otros nodos de la I3D', adjudicado a **Acuntia** por 6,3 millones.

El CESTIC adjudica a TRC dos lotes del Acuerdo Marco de ciberseguridad de DEFENSA, por casi 12 millones, para reforzar la protección del CESTIC

TRC, empresa especializada en la prestación de servicios de alto valor añadido de ciberseguridad y en integración de tecnología, proporcionará servicios avanzados para el **Ministerio de Defensa**. El contrato la ha adjudicado a TRC dos lotes, por importe de 11,7 millones de euros, para el suministro y servicios para la gestión, interoperabilidad y coordinación en la prevención, detección y respuesta de amenazas en la I3D, durante cuatro años. Un plazo de ejecución necesario para buscar una mejor productividad y limitar los riesgos del servicio interno, según destaca la empresa.



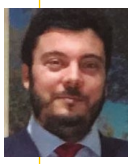
Así TRC reforzará la protección cibernética del CESTIC a través de la monitorización de posibles amenazas en la red interna, tareas de mantenimiento y análisis de la superficie de red que pueda tener expuesta ante la explotación de potenciales vulnerabilidades.

"Es un orgullo para TRC ser seleccionados para este importante proyecto y estamos comprometidos a brindar soluciones innovadoras y eficaces para una rápida detección de posibles ataques de la red interna e implantar herramientas que fortalezcan la seguridad y defensa de esta institución española" , ha resaltado el director del área de ciberseguridad de la compañía, **Carlos Díaz.**

TRC cuenta con una amplia trayectoria y experiencia en el desarrollo e implementación de soluciones tecnológicas de ciberseguridad avanzadas para diversos sectores, incluyendo el de defensa. Su equipo de expertos cuenta con una filosofía de puesta en marcha de servicios a medida basados en el análisis detallado de riesgos, detección de vulnerabilidades e implementación de tecnologías para potenciar y mantener los niveles de madurez de protección establecidos.

Esta nueva adjudicación de dos de los lotes presentados, consolida el liderazgo de la empresa en el mercado de integración y servicios TI, afianzando su posición y proyectando un futuro prometedor en la industria de la seguridad nacional. TRC continuará trabajando en estrecha colaboración con el Ministerio de Defensa para ofrecer soluciones personalizadas y eficientes que se adapten a las necesidades específicas de la institución.

NOMBRAMIENTOS



● **Santander SCF** ha promocionado a **Ramón de la Iglesia** a Global Head of Governance, Risk and Compliance. Graduado en Informática por la Universidad de Islas Baleares, también ha desempeñado roles de responsabilidad en Tunstall Televida y Nextel, entre otras.

● **Grupo Cajamar** ha designado como Gerente de Gobierno de los Servicios de Ciberseguridad a **Guillermo Conesa.** Hasta ahora Global CIO de BeDisruptive, ha trabajado para BCC Eurovía Informática, Sothis, Deloitte e EY, entre otras. Es ingeniero industrial por la Universidad Miguel Hernández de Elche.

● **ING** ha fichado a **Félix Gallego** como responsable de Arquitectura de Ciberseguridad.Ingeniero de Informática de Sistemas por la Pontificia de Salamanca, ha trabajado para Sia, Santander Consumer y Banco Santander, entre otras.

● **Enrique Maza** se ha incorportado como CISO a **Aszendit Tech.** Con anterioridad venía siendo Cybersecurity & Business Resilience Senior Manager en Marsh & McLennan Companies, tras Telefonica y S21sec. Es Ingeniero Técnico en Informática por la UNED.

● **Nalanda Global** ha incorporado como CISO a **Daniel Gonzalo.** Con anterioridad, desempeñó diferentes roles de responsabilidad en Tunstall, Avatel telecom, NTT Data y Airbus Defence and Space, entre otras. Es ingeniero de Telecomunicaciones por la Rey Juan Carlos de Madrid.

● **Knowmad Mood** ha fichado a **Francisco José Pérez** como CISO. Con una amplia trayectoria ha trabajado para NTT Data, Miratech, Wellness Telecom y Simosa IT, de Abengoa, entre otras. Es ingeniero en informática por la Universidad de Sevilla.

● **Jonathan González** ha puesto en marcha una nueva compañía, **Safe Byte Labs,** en la que asumirá el cargo de CEO y Lead Architect. Con una amplia trayectoria profesional ha trabajado para Amazon Web Services, Scheneider Electric y DXC, entre otras.

NOVARED

Innovación en CiberSeguridad

EXPERTOS EN CIBERSEGURIDAD

Para mitigar los riesgos de su negocio

27 AÑOS EN IBEROAMÉRICA

protegiendo a nuestros clientes

novared.net

comunixgroup.com

Escuela de Hacking Ético de Novared

Calle Orense 16 6ºC. 28020, Madrid
+34 91 771 23 90
infoesp@novared.net

EXCLUSIVE NETWORKS incorpora TENABLE Nessus a su cartera X-OD para ofrecer más capacidades en la evaluación de vulnerabilidades

Exclusive Networks ha incorporado a Tenable Nessus, solución de evaluación de vulnerabilidades, a su cartera de servicios disponibles a través de X-OD, su innovadora plataforma de consumo por suscripción. Como se sabe, dicha herramienta ofrece una de las bibliotecas de comprobaciones de vulnerabilidades y configuraciones más grandes del mundo, continuamente actualizada, y con el apoyo del equipo experto en investigación de vulnerabilidades de **Tenable.** "La combinación de Nessus y X-OD permite a los socios ofrecer por primera vez a los clientes la evaluación de vulnerabilidades como servicio", a través de un modelo de consumo, "basado en suscripciones, generando nuevas oportunidades de ingresos recurrentes", ha destacado el vicepresidente Senior de Desarrollo Empresarial Global y Ecosistemas de Exclusive Networks, **Denis Ferrand-Ajchenbaum.**

Apuesta por la innovación

Por otro lado, el mayorista celebró su 'SummerUp Festival' con más de 250 asistentes, entre socios y clientes. Aprovechando el evento, su directora general para Iberia, **Carmen Muñoz,** destacó que la primera parte del año estuvo "marcada por la simplificación del consumo de la tecnología y el paso hacia la economía de suscripción". Asimismo, adelantó que la innovación y la disrupción serán determinantes en la segunda, apostando por "mantener un equilibrio entre las tecnologías consolidadas y nuevas en el mercado". En este sentido, parte de su estrategia pasa por identificar potenciales casos de uso y, mediante el análisis de las diferentes tecnologías que surgen, identificar cuáles son las que mejor se pueden adaptar no solo a la resolución de dichos casos de uso, sino también, a la casuística específica de cada país.

HORNETSECURITY e INGRAM MICRO suscriben un acuerdo estratégico

Hornetsecurity e **Ingram Micro** han firmado una alianza estratégica que permitirá a las empresas "protegerse de manera más efectiva frente a las crecientes ciberamenazas y garantizar la integridad de sus datos confidenciales", destacan ambas compañías, que también recuerdan que, con ella, "Hornetsecurity ganará en capilaridad y mejorá su presencia en el mercado español".

Actualmente, es, según explica la compañía, "el único proveedor de ciberseguridad capaz de ofrecer protección, *backup* y formación en una única plataforma única, sencilla y confiable". De esta manera, su propuesta pasa por que el usuario esté protegido durante las tres etapas de un ciberataque: previniendo la incursión de ataques, protegiendo con las barreras más elaboradas del mercado y realizando respaldos del entorno del usuario, por lo que en caso de un cifrado efectivo se puedan recuperar todos los datos y salvaguardar, de esta manera, la continuidad del negocio.

Por último, en su portafolio también ocupa un lugar destacado la formación, "para que el ataque que logre llegar al usuario sea detectado por éste", indican. Asimismo, señalan que su catálogo de soluciones "es el único que cubre el ciclo completo de protección frente a amenazas externas, proporciona servicio 24x7 en español, y cumple rigurosamente con el RGPD, al poseer la mayoría de los centros de proceso de datos en Europa y, más concretamente, uno en Barcelona".

Además, cabe recordar que la empresa dispone de la Certificación de Conformidad por parte del ENS.

NOMBRAMIENTOS

● La alemana **Fabienne Tegeler** ha sido elegida Presidenta del Consejo de Administración de la **Agencia de Ciberseguridad de la Unión Europea** (Enisa). Jefa de la Sección de Gestión de Clientes y Asuntos Legales de la Oficina Federal Alemana para la Seguridad de la Información (BSI), se incorporó recientemente como miembro alemán del Consejo de Administración de la Agencia.

● El ente **Supervisor Europeo de Protección de Datos** (EDPS) ha ascendido al español **Leonardo Cervera** a Secretario General. Hasta ahora director de la organización, en la que lleva desde 2010, también ha trabajado para la Comisión Europea, la Universidad de Duke y la de Málaga, entre otras. Con una muy solvente trayectoria -incluso se postuló como candidato para dirigir la AEPD, en medio del aun irresuelto *affaire* de la agencia española-, es licenciado en Derecho por la Universidad de Málaga.

● **Sandoz** contará con **Eduard Blasi** como Head of Data Privacy & Digital AI Policies. Hasta ahora DPO en Boehringer Ingelheim, ha trabajado para Marimon Abogados, Prodat y es actual Vicepresidente Tercero de la Asociación Profesional Española de Privacidad. Es abogado por la Autónoma de Barcelona.

● **Mercedes Oblanca** ha sido elegida por **Accenture España** como presidenta para España, Portugal e Israel, sustituyendo en el cargo a Domingo Mirón. Hasta ahora Senior Managing Director, ha desarrollado toda su trayectoria en la consultora en la que comenzó en 1992. Desde 2020, Oblanca ha liderado la división de negocio de Industria, Consumo y Distribución. Es matemática por la Autónoma de Barcelona y cuenta con un programa de Dirección General del IESE.

● El último Consejo de Ministros, antes de las elecciones, ascendió al general de división y responsable del **Centro de Inteligencia de la Fuerzas Armadas (CIFAS), Antonio Romero Losada,** a teniente general para elevar el organismo al mismo nivel que el Mando de Operaciones dentro del Ministerio de Defensa. Tras salir de teniente en 1986, de la Academia General de Zaragoza, estuvo destinado en el Tercio Juan de Austria, de la Legión. Ha participado en operaciones internacionales en Bosnia Herzegovina, Kosovo, Afganistán y Líbano. Además, ha estado al frente de la Brilat Galicia VII y, desde 2019, dirige el CIFAS.

● **Miguel Angel Cañada** ha sido designado por **Incibe** como Head of National Coordination Centre (NCC-ES), dado que el organismo ha sido elegido como Centro Nacional de Coordinación por parte de nuestro país, para el Centro Europeo de Competencia en Ciberseguridad (ECCC) de la Comisión Europea. Hasta ahora, era responsable de relaciones institucionales y estrategia. También forma parte del consejo de directores de la ECSO, en la que es vicepresidente. Ha trabajado para la OEA, el Banco Interamericano de Desarrollo y Kren4, entre otras.

● **Pablo López-Aguilar** se ha incorporado a la **Global Cyber Alliance** como Associate Director of the Internet Integrity Program. Hasta ahora Director de Tecnología e Investigación del APWG (Antiphishing Work Group), también ha trabajado para la Universidad Pompeu Fabra y RespondON, de la que es Cofundador. Es licenciado en Telecomunicaciones por la Pompeu Fabra.

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

Formará parte de su compañía Var Group que cuenta con más de 350 especialistas en ciberprotección y consultoría

WISE SECURITY GLOBAL se integra en el grupo empresarial italiano SESA GROUP para reforzar su posicionamiento internacional

La compañía española **Wise Security Global** se ha integrado en el grupo empresarial italiano **Sesa Group,** incorporándose a **Var Group,** que ha adquirido el 51% de su capital, y cuenta con una plantilla de 350 especialistas en el ámbito de la ciberprotección y la consultoría.

De izquierda a derecha son Gorka Jiménez, CEO Wise Security Global, Francesca Moriani, CEO de Var Group, Jose Luis Yela, Presidente de Wise Security Global, Alessandro Fabbroni, CEO de Sesa

"Esta integración nos aporta numerosos beneficios, ya que no solo expandirá nuestra capacidad y recursos, sino que también potenciará nuestros servicios y equipos". "Mantendremos no sólo nuestra propia marca, sino nuestra propia identidad cultural, valores y saber hacer que tanto nos han distinguido siempre, y seguiremos funcionando como de costumbre solo que con más capacidad de servicio y recursos", resaltan desde Wise Security Global.

Sesa Group, especializada en el sector de la innovación tecnológica y los servicios informáticos y digitales para el ámbito corporativo, tiene una facturación anual que ronda los 2.900 millones de euros y una plantilla con alrededor de 4.700 empleados. Con esta operación busca fortalecer su portafolio de ciberprotección a través de Wise Security, que cuenta con sedes en Barcelona, Bilbao, Madrid, Pamplona y Zaragoza, con un equipo en Iberia de más de 120 profesionales que se integrarán en la compañía italiana. Cabe rescordar que Wise ofrece servicios de respuesta a incidentes y asesoramiento en la protección de datos empresariales a través de un SOC dedicado, además de soluciones propias de Identidad Digital y Evidencia Digital basadas en *blockchain*, y cuenta con una amplia cartera de clientes nacionales e internacionales de sectores tan diversos como el bancario, el de seguros y el de deporte. En 2023 espera alcanzar unos ingresos integrados de más de 10 millones de euros.

FACTUM adquiere activos de CORE NETWORKS, agregando a su portafolio una nueva línea enfocada en la gestión de identidades y de accesos

Factum, participada por **Banco Santander,** a fin de ampliar su portafolio de servicios de ciberseguridad y obtener presencia más intensa en la rama de IAM (Identity and Access Management), ha adquirido activos de la empresa **Core Networks.** Mediante esta operación, el grueso de su equipo de especialistas en protección IAM pasará a formar parte de Factum. Se trata de una nueva unidad que gestiona el control sobre la seguridad de grandes empresas, como **Vodafone,** y organismos públicos, como la **Guardia Civil**. Así, la integración de esta nueva línea de servicios aportará amplias capacidades de gestión de identidades y de accesos, incluyendo el control de acceso basado en roles, el acceso con privilegios y la autenticación multi factor.

"Las soluciones de ciberseguridad centradas en la gestión de identidades y de accesos, generan valor para nuestros clientes y complementa nuestro portafolio de servicios", ha destacado el CEO de Factum, **Iosu Arrizabalaga.**

La operación continua el plan estratégico de Factum de ampliar sus capacidades mediante la incorporación de firmas especializadas, materializada, entre otras, con la adquisición de la consultora Secura, en 2022.

NOMBRAMIENTOS

Idoia Ormazabal se ha incorportado **aDvens Iberia** como Human Resources Business Partner. Graduada en Deusto en ADE, con anterioridad ha trabajado para Ackermann International, Laboral Kutxa y Kutxabank, así como para Seguros Bilbao, entre otras.

Duro Felguera ha fichado a **Adolfo Pérez Coronado** como director de Desarrollo de Negocio para su área de Ciberseguridad. Con una amplia experiencia en el sector, ha ocupado roles de responsabilidad en Applus+ Laboratories, donde ha estado casi un lustro, además de haber trabajado en Safe-T Data, S21sec, Buguroo y Telefónica, entre otras. Es ingeniero por la Pontificia de Salamanca.

BeDisruptive ha reforzado su equipo con la incorporación de **Javier Fernández Urdinguio,** como Global Product & Services Director, y de **Mireya Santoyo**, nueva Global Marketing Director. Urdinguio es Ingeniero Industrial y cuenta con más de 20 años de experiencia en compañías como Sistemas Informáticos Abiertos, Accenture, S21sec o Factum. Santoyo, que ha trabajado una década en EE.UU., ha sido Product Manager en Currys Plc, además de haber sido Senior Product Marketing Manager en Orange España, Marketing and Communications Director en Grupo Recoletas, Marketing and Communications Manager en Agile Content, y Marketing Director en Factum, del Grupo Santander.

EVOLUTIO se hace con DAGRAM para reforzar su presencia en la integración de servicios *cloud*

Evolutio, cuyo principal accionista es la gestora independiente de capital privado **Portobello Capital**, ha comprado la tecnológica española **Dagram**. Este movimiento permitirá a la primera sumar talento y capacidades, fortalecer su cartera de servicios para aportar valor al cliente y seguir avanzando como uno de los principales integradores de servicios *cloud* de nuestro país.

Dagram es una firma especializada en la integración de soluciones de seguridad, *networking*, sistemas y nube. Cuenta con oficinas en Barcelona y Mallorca, una plantilla de más de 60 profesionales expertos en el sector.

En el área de seguridad y networking, Dagram implementa soluciones basadas en alianzas con Fortinet, Trend Micro y Splunk. En el ámbito de infraestructuras y nube cuenta con certificaciones con firmas como Microsoft Azure o VMware. Ambas compañías comparten estas alianzas estratégicas en sus respectivas redes de *partners*, lo que facilitará la creación de sinergias y acelerará la integración de más servicios de valor añadido para sus clientes.

CYBER DEFENSE MNEMO

Plataforma de MNEMO para la gestión de ciber amenazas.

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

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

Mnemo

mnemo.com

España | México | Colombia | Perú | Ecuador

SOLICITA UNA DEMO

TF-CSIRT Trusted Introducer

CSIRT.es

Red Nacional de SOC

S2 GRUPO recibe 20 millones de un préstamo sindicado para desarrollar su plan estratégico en los próximos años

La empresa valenciana **S2 Grupo**, una de las más pujantes del ecosistema español, ha recibido un préstamo sindicado de 20 millones de euros para el desarrollo de su plan estratégico en los próximos años. La operación ha sido coordinada por **Banco Sabadell** y cuenta con el apoyo de **Banco Santander, Caixabank, BBVA** y **Deutsche Bank.** Su objetivo es apostar por su plan estratégico para los próximos años y "consolidar a España como una de las naciones europeas con mayor proyección en ciberseguridad del continente", explica la compañía. "Conseguir la soberanía digital europea y así limitar la dependencia de herramientas de seguridad de terceros países", ha explicado el socio director, **José Rosell**, sobre la apuesta de la compañía para desarrollar herramientas que permitan alcanzar en España la soberanía digital.

El plan de crecimiento de S2 Grupo contempla la especialización en ciberseguridad en sectores críticos como el industrial, la salud, la automoción o el ámbito de la defensa. La compañía cuenta actualmente con más de 650 empleados y tiene previsto incrementar su plantilla a 1.000 profesionales en ciberseguridad. En 2022, logró una facturación de 32,7 millones de euros, lo que supuso un crecimiento de más del 30% con respecto al año anterior.

Cuenta con instalaciones en Valencia, Madrid, Sevilla, Barcelona, San Sebastián, Bruselas, Bogotá, Brindisi, Santiago de Chile, México, Róterdam y Lisboa.

S21SEC califica sus servicios en estándares de ciberseguridad LEET SECURITY y PINAKES

S21sec, de **Thales Group** en 2022, ha obtenido la calificación BBB en **Leet Security** y **Pinakes** tras superar el proceso de auditoría gestionado por la compañía de calificación. Esta certificación supone un reconocimiento del alto nivel de ciberseguridad de la compañía, así como de la garantía de su servicio y asesoramiento a los clientes, en línea con el compromiso de S21sec por cumplir los más altos estándares de protección y normativas aplicables al sector.

Herminio del Campo (Centro de Coordinación Interbancario) y Pablo Echevarría (S21sec-Thales)

La empresa obtuvo este reconocimiento, en concreto, por sus servicios de consultoría y asistencia técnica y seguridad gestionada, realizadas en instalaciones de cliente o mediante acceso remoto, así como por sus servicios de monitorización de alertas e incidentes ofrecidos desde el SOC/CERT de la organización. "Así, estos dos 'sellos' confirman el alto nivel de ciberseguridad del servicio certificado. Esta calificación se lleva a cabo a través de una valoración de las medidas de protección integradas por el proveedor en la construcción y operación del servicio evaluado", destacan desde la empresa. Con ellos, la compañía suma estas nuevas calificaciones al completo Sistema de Gestión Integrado de S21sec en el ámbito de la seguridad, privacidad, continuidad del negocio, calidad y medioambiente; regido por los estándares internacionales EN/ISO 9001, 14001, 20000-1, 22301, 27001, 27701 y por el ENS.

"Este tipo de certificaciones aportan numerosos beneficios tanto para la compañía como para el cliente, ya que asegura una mayor ventaja competitiva y genera una sólida confianza en torno a nuestros servicios. Con ello, hemos demostrado la calidad de nuestro negocio en un momento clave para el sector, que está experimentando un crecimiento del 30% con respecto a los dos últimos años, y se prevé que siga en aumento", ha resaltado **Pablo Echevarría,** director general de S21sec en Iberia.

NOMBRAMIENTOS


● **PwC** ha reconocido la buena labor de **Andrés Diego Hontiveros** ascendiéndole a socio *equity* (con participación en el capital de la firma) y a **Jesús Urien** a socio. Ambos trabajan en el área de consultoría. Hontiveros, hasta ahora Socio-Partner de Business Security Solutions, comenzó en 2007 en la firma, habiendo trabajado también para Axpe Consulting y Grupo CMC. Es ingeniero de Telecomunicaciones por la Universidad de Valladolid. Urien, con la misma titulación y universidad, lleva en PwC desde 2021. Con anterioridad trabajó en Deloitte, donde comenzó su trayectoria profesional. En total, PwC ha promocionado a 921 profesionales de distintas áreas de la organización.


● **SUSE** ha fichado en calidad de CEO a **Dirk-Peter van Leeuwen** y a **Werner Knoblich,** muy reconocido en el área del Open Source, como Director Financiero (CRO). Van Leeuwen, con más de dos décadas en roles de responsabilidad en Red Hat, ha ocupado varios puestos de alta dirección supervisando las ventas, el marketing y las operaciones, más recientemente como Vicepresidente Senior y Director General de América del Norte, y antes de APAC. Knoblich ha ejercido como líder comercial senior en código abierto durante más de dos décadas y ha trabajado para compañías como Mambu y Red Hat.

● **Alfonso Minaya** se ha incorporado a **Evolutio** como Director de Operaciones de Ciberseguridad. Ha sido CEO de LagoSolar, Director de Desarrollo en Duro Felguera Digital Security, además de haber tenido destacados roles en Entelgy Innotec y Mnemo, entre otras. Fue durante un lustro, por parte de Ciudadanos, Asesor de Fomento, Movilidad y Medio-Ambiente y Responsable de Infraestructuras Críticas.

● **Inetum** ha promocionado a **David Rubio** a Head of Cybersecurity Operations. Ingeniero informático por la Alfonso X, ha desempeñado roles de responsabilidad en compañías como Aon, KPMG, Grupo SIA y PwC, entre otras.

● **Cipher** ha incorporado a **Ainoa Guillén** como Global Cybersecurity Intelligence Lead. Graduada en Criminología por la Universidad de Murcia, ha trabajado para Blueliv (ahora Outpost24), Tarlogic, Sec2Crime y ha sido colaboradora del proyecto europeo Vince, además de ser docente en Universae.

● **DXC** ha fichado a **Mara Fernández** como Security Delivery Lead. Con amplia trayectoria profesional, ha trabajado para Seresco, Liberbank y Thales. Es ingeniera Informática por la Universidad de Oviedo.

zscaler™

Experience your world, secured

Transformación de la seguridad

Pase de la seguridad heredada a un modelo de confianza cero

Modernización de la infraestructura

Simplifique la conectividad de las sucursales y la nube

Habilitación del lugar de trabajo moderno

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

www.zscaler.es

TEHTRIS despliega una red mundial de *honeypots* nómadas para atrapar a los ciberdelincuentes

Tehtris ha puesto en marcha una nueva generación de *honeypots* cuyo objetivo es atraer cualquier forma de actividad maliciosa en la red para identificarla y neutralizarla. Según la compañía, se trata de señuelos "nómadas" que detectan las actividades de los actores maliciosos en todo el mundo para seguir mejor la evolución de las ciberamenazas y ayudar a las organizaciones a adaptar sus sistemas de defensa. Desplegada en la nube, la red comprende más de 1.300 *honeypots* nómadas en 50 países.

Como se sabe, los *honeypots* existen desde hace muchos años, aunque su formato estático les hizo perder valor con el tiempo. Ahora Tehtris intenta volver a sacarlo partido a través de su enfoque de '*honeypot* nómada'. Se trata de una de las primeras aplicaciones del concepto emergente de Automated Moving Target Defense (AMTD), presentado por Gartner como una tecnología que mejorará profundamente las técnicas de ciberdefensa. Para 2025, se espera que el 25% de las aplicaciones en la nube de todo el mundo aprovechen las funcionalidades AMTD. Y es que, la tecnología AMTD representa una transición de un enfoque de defensa pasivo a uno proactivo mediante el despliegue de nuevos mecanismos de señuelos dinámicos y capacidades de automatización para actuar más rápidamente en la superficie de ataque.

"Gracias a su red mundial de *honeypots* nómadas, Tehtris posee un conocimiento en tiempo real sobre el panorama mundial de las ciberamenazas", destacan desde la compañía. También, recuerdan que sus informes de tendencias sobre las actividades ciberdelictivas detectadas y analizadas a través de dicha red son compartidas con instituciones como la **ANSSI** y la **Cyber Threat Alliance**.

PROSEGUR y la UNIVERSIDAD DE DEUSTO forman a estudiantes de ingeniería para afrontar los retos del futuro de la seguridad

Por segundo año consecutivo, **Prosegur** ha colaborado con la **Universidad de Deusto** para ofrecer al alumnado del Grado de Ingeniería en Diseño Industrial formación puntera en materia de seguridad. A través de un proyecto que abordó los desafíos futuros del sector, los jóvenes han desarrollado habilidades para crear servicios de seguridad mejorados, presentando soluciones e identificando oportunidades para reducir riesgos y satisfacer las necesidades de los clientes.

Durante un curso de 10 semanas, los 39 estudiantes de la asignatura de Laboratorio de Diseño, repartidos en 10 grupos de trabajo, recibieron formación complementaria con el objetivo de que puedan aplicar y complementar los conocimientos adquiridos en su formación académica. El trabajo de los estudiantes estuvo supervisado por profesionales de la compañía que han dado *feedback* a los proyectos presentados y que han contribuido a su desarrollo y aprendizaje. En concreto, se les planteó seis retos de seguridad, a los cuales los estudiantes propusieron diversas soluciones: cómo mejorar la defensa de las obras de arte en los museos, cómo mejorar la percepción de la seguridad en el metro de grandes ciudades, el diseño de la evolución del servicio de tele-rondas en base a la incorporación de la IA, la definición de nuevos casos de uso para el KiSOC, el diseño de nuevos servicios basados en el uso de la IA y cómo ChatGPT puede mejorar el trabajo de los operadores de seguridad. Finalmente, en junio, los equipos presentaron en las oficinas de Prosegur sus proyectos ante los profesionales directamente implicados de las distintas áreas de negocio de la compañía.

NOMBRAMIENTOS

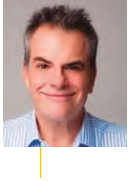
La **Agencia de Ciberseguridad de Cataluña** ha incorporado a **Helena Rodríguez Pérez** como Responsable de Seguridad de la Información. Graduada en Telecomunicaciones por la UPC y con un MBA por la UPF BSM de Barcelona, ha trabajado también para MútuaTerrassa Egermátic y PwC, entre otras.

Isaca ha designado como nuevo CEO a **Erik Prusch**. Con sede en el estado de Washington, Prusch aportará a la organización una importante experiencia en tecnología y liderazgo. Licenciado por la Universidad de Yale, ha sido Consejero Delegado de Outerwall, Lumension, NetMotion Wireless, Clearwire y Borland, además de miembro del consejo de RealNetworks, Wash, Calero Software y Keynote Systems. También, fue director financiero de varias empresas públicas, como Identix y Borland, y de divisiones de empresas públicas, como Gateway Computers y PepsiCo. Comenzó su carrera en Deloitte & Touche (entonces Touche Ross).

Commvault ha incorporado a **Maite Ramos** como Directora General para Iberia, procedente de Dynabook (antes Toshiba), donde desempeñó el cargo de Directora General para Iberia durante los últimos tres años. Previamente, trabajó como Directora de Marketing y Directora de Proyectos de Generación de Demanda para EMEA de HP, tras su paso por Lenovo, donde también ocupó cargos de responsabilidad. Es licenciada en Ciencias Económicas por la Universidad de Valladolid, además de contar con un MBA por el IESE.

EY ha nombrado a 24 nuevos socios de cuota de los que destacan, en el ámbito de la ciberprotección, **Jordi Juan,** Socio del área de Consultoría Tecnológica y Ciberseguridad. Igualmente, ha ascendido a socio a **Diego Ruiz Ramírez,** Director del Área de Ciberseguridad. Juan cuenta con más de 20 años de experiencia y comenzó su carrera en el Silicon Valley como Ingeniero de I+D+i de dispositivos de ciberseguridad en red. Es ingeniero de Telecomunicaciones por la Politécnica de Cataluña. Ruiz, con una dilatada carrera profesional de más de 17 años, comenzó trabajando en Banco Santander y ha asesorado a múltiples empresas del sector privado y público en la supervisión, gestión y ejecución de proyectos de este ámbito.

Deloitte ha designado 33 nuevos socios, dos de ellos para su área de negocio de ciberseguridad. Se trata de **Daniel Hernández** y **Raul Moreno Vicente,** ambos socios de Risk Advisory, especializados en ciberprotección. Hernández es graduado en ADE por la Unir, ha trabajado para SegurCaixa Adeslas, Class MF, Barclays y Grupo Banco Popular. Moreno, por su parte, ha desempeñado roles de responsabilidad en Fibratel, Consulintel e Iecisa.



La compañía de origen español **CounterCraft**, ha reconocido el buen trabajo de **David Brown** como CRO ascendiéndole a CEO de la empresa. Con amplia experiencia en el sector, ha ejercido entre otros puestos de responsabilidad como Vicepresidente de Verve Industrial Protection, ForeScout Technologies y ZeroFOX.

Akamai

25 AÑOS
1998 - 2023

Akamai Connected Cloud

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

- Content Delivery
- Cyber Security
- Cloud Computing

www.akamai.com

GADESOFT e INNOVATE, a MNEMO COMPANY, se alían para la formación en servicios de ciberseguridad sobre MICROSOFT

David Pérez Lázaro (Innovate, de Mnemo) e Ignacio González (Gadesoft)

Innovate, compañía del **grupo Mnemo**, ha sellado un acuerdo estratégico con **Gadesoft** para colaborar en iniciativas conjuntas que permitan acelerar el crecimiento de los servicios de formación en protección de **Microsoft** y los servicios de consultoría, implantación y gestión de seguridad basadas en tecnologías del fabricante.

Para ello, Innovate cuenta con un Centro de Excelencia de Seguridad Cloud, especializado en Microsoft, con un equipo de consultoría y operaciones de seguridad que han desplegado con éxito sus soluciones de protección en múltiples clientes en España hasta convertiste en el primer MSSP 100% español en alcanzar la categoría de 'Partner de Soluciones de Seguridad' de Microsoft en 2022. A su vez, Gadesoft, con 25 años de experiencia en servicios de formación, ha sido primer Learning Partner Local, a nivel mundial, en lograr el reconocimiento como 'Partner de Soluciones de Servicios de Formación' en las seis áreas de especialización identificadas por Microsoft, entre ellas seguridad, y en ofrecer a sus clientes formaciones de alta calidad en todas ellas. "Innovate tiene una estrategia de crecimiento en seguridad Microsoft donde es clave contar con socios especializados como Gadesoft para tener un portafolio que de soluciones completas al cliente final, y la formación es uno de los elementos clave que necesitamos", ha destacado el CEO de Innovate, **David Pérez Lázaro.**

"Concebimos la formación tecnológica como uno de los pilares imprescindibles en el desarrollo de la carrera de cualquier técnico y, por ello, nos centramos en desarrollar nuestros propios cursos y soluciones que llegan allá donde los clientes necesitan ayuda", ha explicado el CEO de Gadesoft, **Ignacio González.**

LIDERA incorpora a RED SIFT a su catálogo para proteger frente a ataques al correo-e, dominios, marca corporativa y activos expuestos a Internet

Lidera ha suscrito un acuerdo de distribución con **Red Sift** para ofrecer sus soluciones que hacen frente a vulnerabilidades en el perímetro del correo-e, dominios, marca corporativa y activos expuestos a Internet. Al proporcionar una cobertura completa de la huella digital de una organización mediante la mejor detección y supervisión de su clase, la plataforma de resiliencia digital de Red Sift permite a las organizaciones descubrir de forma proactiva amenazas BEC, descubrir casos de fraude en dominios similares, identificar vulnerabilidades de los activos expuestos a internet y proteger la marca corporativa. Junto con sofisticadas funciones de *machine learning* y remediación, provee las herramientas para luchar contra el *phishing* y garantizar el cumplimiento continuo de los protocolos de seguridad del correo-e y la web.

Como se sabe, Red Sift, a través de una solución 100% SaaS, provee a los equipos de ciberseguridad con un mecanismo de defensa automatizado y muy eficaz contra los ataques de usurpación de identidad, al mismo tiempo que refuerza el cumplimiento de las normativas de las organizaciones.

"Tal y como indica Gartner, el correo-e sigue siendo un importante vector de ataque tanto para el *malware,* como para el robo de credenciales a través del *phishing*. "Este nuevo acuerdo está motivado por la creciente demanda de este tipo de tecnologías debido al aumento en el número de ciberataques en el entorno web, para el mercado de medianas y grandes empresas", destacan desde ambas compañías.

NOMBRAMIENTOS

● **Google** ha promocionado a **José Carlos Cerezo** a Head of EMEA Southern Security and Compliance Team. Posee amplia experiencia en ciberprotección con foco en nube, habiendo trabajado con anterioridad en Symantec, Microsoft y RSA Security, entre otras. Es Ingeniero en Informática por la Politécnica de Madrid.


● **One eSecurity** ha fichado a **Antonio Sepúlveda** como Director Técnico para EMEA y a **Carlos Araújo** como Threat Hunting & Threat Research. Ha desempeñado gran parte de su trayectoria en el Incibe, donde llegó a ser responsable de ciberseguridad para la Industria. También, ha trabajado en Capgemini, Sopra Steria y Accenture, entre otras. Es licenciado en Físicas por la Uned y tiene un Máster en Ciberseguridad por la UCAM. Araújo es ingeniero informático por la Universidad de Alicante y ha trabajado para el Mando Conjunto de Ciberespacio, Isdefe y Telefónica Tech.


● **V-Valley** ha nombrado como consejeras a **Luisa Paolucci,** Head of Sales & Marketing Datacenter Technologies, Cloud & EAAS Area, y a **Conxi Palmero,** Directora de Alianzas Estratégicas del Grupo Esprinet. Así, junto con Javier Bilbao-Goyoaga, Presidente, y Hugo Fernández, Consejero, Paolucci y Palmero pasan a formar parte del consejo de administración de V-Valley Advanced Solutions España. Paolucci cuenta con más de 17 años de experiencia, participando activamente en los procesos de transformación digital de modelos *on premise* tradicionales hacia modelos *as a service*. Palmero, licenciada en Económicas por la Universitat Pompeu Fabra de Barcelona, comenzó su carrera profesional en auditoría y consultoría en PwC y, ya con 25 años de experiencia en el sector, ha colaborado durante más de dos décadas con el Grupo Sesa en áreas estratégicas de desarrollo.




● **Exclusive Networks** ha ampliado su plantilla en el mercado ibérico con nuevas incorporaciones. En concreto, se han sumado al mayorista **Alejandro Huerta,** como Director Técnico, así como **Jorge Alberto Ramiro Muñoz** y **Martín Morey** como System Engineers. Además, se incorpora al departamento de Compras **Rosana Sánchez.** Huerta, ingeniero de Telecomunicaciones por la UAM, ha ocupado roles de responsabilidad en Telefónica Tech, Sinfoges y SIC Proyectos. Ramiro ha trabajado para Prosol, Anadat Consultin y Sermicro, entre otras. Morey, ingeniero de Materiales, cuenta con una amplia trayectoria en compañías como DXC, CDS, Dinsa y Agora Solutions.

20 ANIVERSARIO

Predecir
lo que importa

La Alianza Líder que garantiza
la **gestión de vulnerabilidades**
y compliance técnico

tenable

mdtel
Platinum Partner

tenable ASSURE

www.mdtel.es
marketing@mdtel.es

* Tenable nombrada la única elección de los clientes de Gartner Peer Insights™ de 2021 para la evaluación de vulnerabilidades

GOOGLE CLOUD presenta su propuesta para luchar contra el blanqueo de capitales, asistido por IA, para entidades financieras

El blanqueo de capitales es un problema complejo. Se calcula que al año se blanquea entre el 2% y el 5% del PIB mundial, es decir: hasta 2.000 millones de euros anuales. Para ayudar a luchar contra él, **Google Cloud** ha presentado Anti Money Laundering AI (AML AI). Se trata de un producto asistido por inteligencia artificial (IA) y diseñado para ayudar a las entidades financieras a detectar el blanqueo de capitales de manera más eficaz y eficiente.

Según la compañía, la mayoría de los productos de monitorización de lucha contra el blanqueo de capitales (LBC) existentes se basan en reglas que están definidas manualmente, las cuales arrojan bajos índices de identificación de actividades sospechosas. Sin embargo, AML AI de Google Cloud permite disponer de una puntuación consolidada del riesgo del cliente y resulta una alternativa a las alertas de transacciones basadas en reglas.

El riesgo se computa en base a los datos del banco, dentro de los cuales se incluyen los patrones transaccionales, el comportamiento en la red y los datos KYC (también denominados "Conozca A Su Cliente") para identificar casos y grupos de clientes minoristas y comerciales de alto riesgo. El producto puede adaptarse a cambios subyacentes en los datos, brindando resultados más precisos, para aumentar así la eficacia general del programa y mejorar la eficiencia operativa.

Además, AML AI de Google Cloud utiliza modelos de lenguaje propios creados originalmente para Google Search, así como tecnologías de Google Cloud, como Vertex AI y BigQuery. El producto gestiona las complejidades que supone ejecutar modelos de lenguaje a escala al facilitar explicaciones enriquecidas de los resultados previos. Clientes como **HSBC, Bradesco** y **Lunar** ya han usado esta tecnología como su principal sistema de monitorización de transacciones de LBC.

SANTANDER y OXENTIA FOUNDATION ponen en marcha un reto global que busca los mejores proyectos en ciberprotección

Banco Santander ha presentado junto a **Oxentia Foundation**, el Santander X Global Challenge | Cyberprotect the Future. Un reto global dirigido a *startups* de 11 países -Alemania, Argentina, Brasil, Chile, EE.UU., España, México, Portugal, Polonia, Reino Unido y Uruguay- para que aporten soluciones innovadoras en aras de dar respuesta a los desafíos a los que se enfrenta la sociedad en materia de ciberseguridad.

El reto, cuyo plazo de inscripción estará abierto hasta el 28 de septiembre, seleccionará seis proyectos ganadores que recibirán 120.000 euros en premios: 30.000 euros para las tres *startups* vencedoras (10.000 cada una) y 90.000 para las tres mejores *scaleups* (30.000 para cada una).

Además, tendrán acceso a Santander X 100 (la comunidad global de emprendimiento con los proyectos más destacados de Santander X que les conecta con los recursos que necesitan para crecer) y la oportunidad de presentar su proyecto a **Forgepoint Capital** y a los equipos de ciberseguridad y **Fintech Station** de Banco Santander, optando a desarrollar una prueba piloto. "El objetivo no es solo identificar a estas *startups,* sino también apoyarlas durante esta jornada, permitiéndoles llegar al impacto al que aspiran. Estas empresas a menudo pueden tener un enfoque más ágil para aplicar tecnologías y estar más dispuestas a experimentar con ideas innovadoras, lo que termina por apoyar en la creación de un ecosistema más seguro", ha explicado la CISO Global de Banco Santander, **Hazel Diez Castaño.**

NOMBRAMIENTOS

● **Aiuken** ha reconocido el buen trabajo de **Néstor Carriba** nombrándole Chief Revenue Officer (CRO). Con un Máster en Marketing y Ventas por el EAE Business School, con anterioridad trabajó en HPE y BancTec, entre otras.

● **Kaspersky** ha promocionado a **Marc Rivero** ascendiéndole a Lead Security Researcher. En la multinacional desde 2020, también colabora con el APWG (Antiphishing Work Group). Con anterioridad trabajó para McAfee, la Cyber Threat Alliance, CrowdStrike, S21sec y Deloitte, entre otras.

● **Qualys** ha anunciado el nombramiento de **Dino DiMarino** como Director de Ingresos (CRO, Chief Revenue Officer). Con más de 20 años de experiencia ha ocupado roles de responsabilidad en Snyk, Mimecast, así como en EMC y RSA Security durante más de 12 años. Es licenciado en Administración de Empresas por la Universidad Wilfrid Laurier de Waterloo, Canadá.

● **Babel** ha reforzado su Dirección de Estrategia e Innovación con la incorporación de **José de Ramón** como Business Partner & Strategic Alliances Executive. Con más de 30 años de experiencia, ha ejercido diversos roles de responsabilidad en PegaSystem, PwC, Santander Global Tech, ISBAN, IBM y General Motors, entre otras. Es Ingeniero de Sistemas por la Universidad Politécnica de Madrid.

● **S2 Grupo** ha continuado fortaleciento su equipo con la llegada de **Javier Ruiz Rioja** como Sales Team Leader para la Zona Centro. Ha desarrollado su dilatada carrera profesional en compañías como Dimension Data, NTT y S21sec, donde fue Gerente de Grandes Cuentas para Industria y Energía.

● **Armis** ha contratado a **Jordi Medina** como Enterprise Sales Account Manager. Con amplia experiencia en el sector, ha trabajado con anterioridad para Tufin, HID Global, IBM y Check Point, entre otras.

● **Eulen** ha apostado por **Juan Miguel Sucunza** como Vicepresidente Ejecutivo y por **José Ricardo López** como Director de Consultoría y Ciberseguridad del Grupo. Sucunza, hasta ahora miembro del Consejo Asesor, es ingeniero por la Universidad de Navarra y ha trabajado para Icer Brakes, Nucap Europe, Sodena e Icer Rail. López, con una amplia experiencia, ha trabajado para Dimoba, Sareb, Accenture e EY, entre otras.

● **BlackArrow,** de Tarlogic, se ha reforzado con **Sergi Ortega** como Incident Response Manager. Con una amplia experiencia ha desempeñado diferentes roles en este ámbito en empresas como Draäger, Seat, Panda Security, Abast y Valeo, entre otras.

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

NETSKOPE Intelligent SSE se integra con AMAZON Security Lake para frenar amenazas en entornos híbridos de teletrabajo y actualiza su programa de canal

Netskope anuncia la integración de su solución Intelligent Security Service Edge (SSE) con la plataforma Amazon Security Lake de **Amazon Web Services** (AWS). La solución resultante permite descubrir eventos de seguridad de manera mucho más rápida. Amazon Security Lake es un servicio que centraliza automáticamente los datos de seguridad de una organización procedentes de sus entornos de AWS, de proveedores de SaaS y de fuentes locales y en la nube en un lago de datos diseñado específicamente para que los clientes puedan actuar sobre los datos de seguridad con mayor rapidez, simplificando su gestión en entornos híbridos y multinube.

De esta forma, los clientes de Netskope pueden ahora exportar registros de la plataforma Netskope Intelligent SSE a Amazon Security Lake, que administra los datos a lo largo de su ciclo de vida con configuraciones de retención de datos personalizables. Asimismo, convierte y conforma los datos de seguridad entrantes al *Open Cybersecurity Schema Framework* (OCSF).

Además, la compañía ha puesto en marcha un nuevo Programa de Proveedores de Servicios Gestionados (MSP), como una extensión de su propuesta de canal 'Netskope Evolve Partner Program'. Este ha sido creado para ayudar a los socios a ampliar sus flujos de ingresos con una vía de acceso adicional al mercado y ofertas de servicios beneficiosas. Asimismo, ofrece opciones de licencia flexibles, recursos dedicados para *partners* MSPs y una nueva acreditación de soporte técnico que complementa la especialización en prestación de servicios de Netskope.

FASTLY pone en marcha una estrategia comercial con nuevos precios, paquetes simplificados y más niveles gratuitos para popularizar el uso de su plataforma

Fastly ha dado a conocer nuevos precios y paquetes simplificados para sus servicios principales. Se trata de una iniciativa con la que pretende "facilitar a empresas de todos los tamaños probar, comprar y utilizar la potente plataforma la compañía", destacan sus responsables que recuerdan que los nuevos usuarios podrán adoptar los paquetes de *content delivery*, seguridad y *edge computing*. También, "permite configurar una oferta y experiencia aún más atractivas para los grandes clientes existentes que buscan ampliar sus despliegues", añaden.

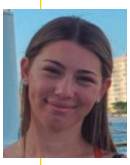
Así, además de ofrecer una tarifa plana para los clientes que no quieren gestionar el consumo basado en el uso, se ha apostado por una política de precios "sencillos, transparentes y competitivos, sin letra pequeña ni cargos ocultos". Con esta nueva estrategia los clientes tienen la flexibilidad de combinar paquetes para satisfacer sus necesidades particulares.

Cabe destacar asimismo que Fastly ha ampliado su nivel gratuito para facilitar que todo el mundo pueda probar sus servicios de *delivery,* seguridad, computación y observabilidad, sin compromiso. También, ha aumentado el número de opciones de prueba de autoservicio. Además de las herramientas analíticas internas Domain Inspector y Origin Inspector, ya están disponibles las pruebas gratuitas de WebSockets y Fanout. Los clientes pueden utilizar estas herramientas en el *edge,* lo que permite a su *app* participar en actualizaciones bidireccionales con audiencias muy grandes en tiempo real.

NOMBRAMIENTOS

Kyndryl ha contratado a **Javier Miguel Martín** como Cloud Security Leader. Máster en tecnología de la información por la Oberta de Cataluña, ha desempeñado diferentes roles en compañías como BBVA, Telefónica, Orange Bank e EY, entre otras.

Jessica Salgado se ha incorporado a **Cipherbit,** la unidad independiente del grupo Oesía, como adjunta al CCO. Desde 2018 Project Manager Ciberseguridad en el Grupo, ha trabajado más de una década para Total, y ha ocupado roles de responsabilidad en compañías como Cemex. Es ingeniera en Química por la Universidad Simón Bolivar y cuenta con un máster en finanzas por la EAE Business School.



Exclusive ha potenciado su equipo con la llegada de **Victoria García**, Product Specialist y **César Obispo**, Junior Account Manager, además de **Marisol León**, como Marketing Intern y **Verónica Pasqualon**, encargada de potenciar la adquisición de talento (Talent Acquisition Intern). García ha trabajado para Let's trade the barber factory, Transportes Gadi y Grupo A Field Marketing. Obispo, graduado en Turismo por la Complutense de Madrid, ha desarrollado gran parte de su carrera en Arrow ECS. León, especializada en Comunicación y Medios Digitales, ha trabajado para Marketing Intern. Pasqualon cuenta con un máster en gestión de recursos humanos por la Oberta de Cataluña y ha estado en compañías como Codurance.

Veridas ha ampliado su equipo norteamericano con **Kevin Vreeland** como Director General. Cuenta con más de 30 años de experiencia y ha ocupado roles de responsabilidad en Acuant, MorphoTrust, Ardence –que luego fue comprada por Citrix– o Vasco, entre otras.

Óscar Llama ha sido contratado por **SIA** como Cybersecurity Sales Specialist. Ingeniero Informático ha ocupado diferentes puestos comerciales en Telefónica Tech, Ingecom, Spamina y Nuvias Advanced Networking, entre otras.

Cuando la tecnología permite el progreso,
ESET está aquí para protegerlo.

www.eset.es

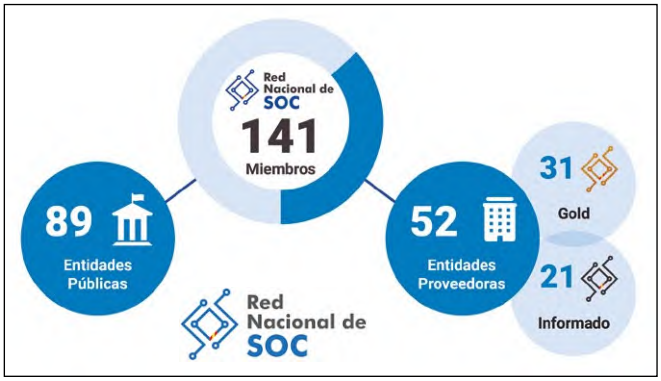
ESET®
Digital Security
Progress. Protected.

Red Nacional de SOC: 140 entidades públicas y privadas intercambian más de 30 alertas diarias sobre ciberamenazas

Notificar de forma inmediata cualquier indicio de ciberataque para que sus integrantes puedan mejorar su capacidad de protección, implementando las medidas preventivas necesarias, es el principal objetivo de la Red Nacional de SOC (RNS). Liderada y coordinada por el Centro Criptológico Nacional, a través de esta iniciativa pionera a nivel nacional e internacional, sus más de 140 miembros disponen de acceso en tiempo real a información sobre ciberamenazas que permite la detección de posibles incidentes de ciberseguridad.

Carlos Córdoba

Hace ahora dos años, en octubre de 2021, el **Centro Criptológico Nacional** puso en marcha la **Red Nacional de Centros de Operaciones de Ciberseguridad (RNS).** Nacía como respuesta a la necesidad de coordinar los diferentes SOC desplegados en las distintas administraciones públicas, muchos de ellos en colaboración con el propio CCN (en ministerios, diputaciones, comunidades autónomas, cabildos o entidades locales) y, sobre todo, ante la constatación del cambio de paradigma que han supuesto los acelerados procesos de transformación digital.



Desde el CCN se constató que la respuesta y protección individual dejaron de ser suficientes en un escenario en el que la superficie de exposición y las ciberamenazas crecían de forma exponencial. Era, por tanto, preciso sustituir el modelo reactivo por uno de defensa activa para conseguir una mejor protección del sector público español. Y para ello, era indispensable avanzar de la notificación individual del incidente al intercambio de esta información, compartiendo entre las distintas entidades los detalles necesarios para lograr ventajas competitivas frente al atacante.

Este objetivo coincidía además con las prioridades de la Comisión Europea que, en diciembre de 2020, daba a conocer la **Estrategia de Ciberseguridad de la Unión Europea** para la Década Digital. En ella se apostaba abiertamente por la creación de "una red de centros de operaciones de seguridad en toda la UE, la mejora de los centros existentes y el establecimiento de otros nuevos". En este sentido, conviene señalar que España, junto con Italia, Luxemburgo, Portugal y Rumanía, han formado un consorcio para el desarrollo de una red europea de SOC que permita promover el intercambio de información entre estos cinco países.

En esta situación, el CCN-CERT decidió liderar la puesta en marcha de la **Red Nacional de SOC** para dar respuesta a este nuevo ecosistema de la ciberseguridad en el que es determinante promover la notificación colectiva de ciberamenazas para prevenir su materialización y evitar que se repliquen determinados ciberataques.

El CCN-CERT tiene el convencimiento de que si entre todos los SOC que dan protección al sector público se comparte información sobre las tácticas, técnicas y procedimientos de nuevas amenazas, se mejorarán las capacidades de detección y respuesta a posibles ciberincidentes.

Para que un organismo pueda ser admitido en la Red Nacional de SOC como entidad pública, debe cumplir cuatro requisitos: Pertenecer al sector público español, disponer de servicios de ciberseguridad o de SOC, aceptar el código ético y de conducta profesional de la RNS y tener instalada y utilizar la herramienta LUCIA (o en proceso de instalación).

Estado actual de la RNS

Tras la prueba piloto iniciada en 2021, durante el año 2022 la Red Nacional de SOC evolucionó hasta alcanzar las **141 entidades adheridas en la actualidad**, entre SOC públicos y los pertenecientes a las empresas que les prestan servicios. Ministerios, diputaciones, cabildos, entidades locales, y operadores de servicios esenciales forman parte de esta plataforma de intercambio de información sobre ciberamenazas, mediante la que se comparten **de media diaria alertas de más de 30 incidentes de ciberseguridad**.

El principal activo de la Red Nacional de SOC es la información que se comparte sobre indicadores de ataque **(IOA)** y de compromiso (**IOC**) no identificados dentro de la comunidad para alertar y promover las acciones preventivas necesarias. Actualmente, los miembros de la RNS comparten información de distinto tipo:

- Direcciones IP de atacantes (o supuestos atacantes).
- Dominios de sitios comprometidos (o supuestamente comprometidos).
- URL específicas con contenido dañino.
- Firmas o Hashes de ficheros con contenido dañino
- Direcciones de correo propagadoras de contenido dañino.
- Reglas de detección de amenazas, por comportamiento de red (reglas SNORT), por contenido dañino (reglas YARA) o por comportamiento monitorizado en los SIEM (reglas SIGMA).

Es importante destacar que a través de la Red Nacional de SOC no se comparte información que

Está previsto integrar en esta Red Nacional no solo a los SOC de los organismos de la AA.PP. española, sino además a todos aquellos que operan en España. Esta participación se hará extensiva también a otras comunidades y foros de intercambio de información nacionales, como CSIRT.es, o internacionales, como la Red Europea de SOC (ENSOC).

pueda contener datos de víctimas de posibles ataques. Tampoco se intercambian informes o investigaciones genéricas sobre amenazas en el ciberespacio si éstas no se están materializando o no han sido detectadas por los miembros de la RNS.

¿Quién forma parte de la RNS?

Desde que entró en funcionamiento, la Red Nacional de SOC ha sido reconocida por su excelente labor. En la comunidad, ya es considerado el principal **instrumento para coordinar la colaboración y el intercambio de información** entre los Centros de Operaciones de Ciberseguridad del sector público español.

A día de hoy, son miembros de la RNS los SOC de los organismos de la Administración Pública española, las entidades proveedoras y privadas que con personal propio prestan sus servicios de ciberseguridad a entidades públicas (en este caso con distintos niveles de participación); y entidades invitadas a las que, sin cumplir alguno de los dos requisitos anteriores, se les da acceso a la información intercambiada en la propia Red; pero como explicaremos más adelante, esta composición evolucionará próximamente.

Para que un organismo pueda ser admitido en la Red Nacional de SOC como entidad pública, debe cumplir cuatro requisitos:

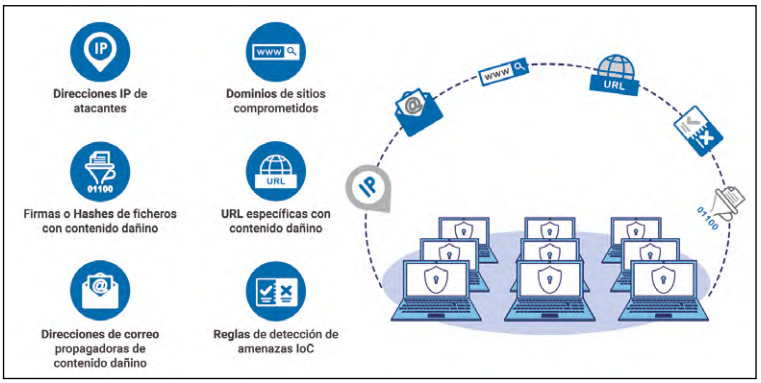
1. Pertenecer al sector público español.
2. Disponer de servicios de ciberseguridad o de SOC.
3. Aceptar el código ético y de conducta profesional de la RNS.
4. Tener instalada y utilizar la herramienta LUCIA (o en proceso de instalación).

Por su parte, las empresas que desean adherirse como Proveedores deben hacerlo en calidad de "empresa" (pública o privada), y para formar parte de la RNS han de cumplir con las siguientes premisas:

- Prestar servicios de ciberseguridad o de SOC al sector público
- Aceptar el código ético y de conducta profesional
- Utilizar LUCIA para notificar incidentes al CCN-CERT en nombre de alguno de sus clientes (o estar en proceso de implantación).

Para garantizar su calidad, la información técnica compartida por los miembros de la RNS está sometida a un **proceso de valoración continuo** en el que se evalúa la naturaleza y relevancia de las aportaciones realizadas por cada miembro, puesto que el nivel de implicación de los miembros de la RNS es determinante a la hora de permanecer en la Red. Por otra parte, el **parámetro de calidad** también interviene en la evaluación de la información intercambiada. Desde su puesta en marcha, la RNS ha recibido **más de 5.000 eventos de ciberseguridad**; sin embargo, alrededor de un 20% fueron descartados por no cumplir las condiciones para ser compartidos por el resto de los miembros.

Además, con el objetivo de fomentar la **participación y el intercambio,** la RNS dispone de un mecanismo, dirigido exclusivamente a las entidades proveedoras, que puntúa la colaboración y posiciona a los miembros en dos niveles en función de su actividad dentro de la Red ("**Gold**" e "**Informado**").



Próximas mejoras de la RNS

Si bien el objetivo de la Red Nacional de SOC continuará siendo la ampliación de las capacidades de protección frente a ciberamenazas a través del intercambio de información, el Centro Criptológico Nacional tiene trazadas las líneas principales para mejorar la efectividad de la información compartida a través de esta red de nodos de centros de operaciones de ciberseguridad.

Como punto de partida, está previsto integrar en esta Red Nacional no solo a los SOC de los organismos de la Administración Pública española, sino a **todos aquellos que operan en España**. La participación en la Red se hará extensiva **también** a **otras comunidades y foros** de intercambio de información **nacionales**, como CSIRT.es, **o internacionales**, como la Red Europea de SOC (ENSOC).

En paralelo a esta expansión, desde el CCN se están definiendo **pautas concretas para enriquecer la información compartida** con el objetivo de lograr un intercambio de datos más eficaz. Por ello, está previsto incluir en el intercambio información de contexto (fuentes externas) y mejorar los criterios de caducidad de la información compartida, descartando falsos positivos y haciendo uso de los protocolos de compartición PAP/TLP. También está previsto ampliar de manera procedimentada la tipología de la información a compartir e incluir casos de uso para detección, métricas de SOC, o buenas prácticas de gestión.

Asimismo, se está trabajando en el establecimiento de **nuevos criterios de puntuación**, que midan y evalúen la naturaleza del incidente compartido y **que penalicen los falsos positivos**. En este sentido, y como novedad, la clasificación por niveles se hará extensible a todas las entidades privadas, en base a la puntuación recibida por su información compartida, y se añadirá un nivel "Inhabilitado" cuando no exista registro de actividad. Se cambiará también el nombre de los actuales niveles a "Oro" (en lugar de "Gold") y "Plata" (en lugar de "Informado").

A corto plazo, la RNS medirá la eficacia de la información cuando se produzcan los bloqueos de los indicadores compartidos y se proporcionarán **nuevas capacidades** a los miembros a partir de la información global recibida:

- **Prevención**: mediante notificación de vulnerabilidades.
- **Detección:** mediante correlación de alertas.
- **Gestión:** mediante cuadros de mando centralizados.
- Entre todos los SOC integrados en esta Red y a través del intercambio y la participación colectiva de sus miembros, se logrará una mejora sustancial de las capacidades nacionales de prevención, detección y respuesta a ciberamenazas. ■

Las empresas que desean adherirse como Proveedores deben hacerlo en calidad de "empresa" (pública o privada), y para formar parte han de cumplir con las siguientes premisas: Prestar servicios de ciberseguridad o de SOC al sector público, aceptar el código ético y de conducta profesional, y usar LUCIA para notificar incidentes al CCN-CERT en nombre de alguno de sus clientes (o estar en proceso de implantación).

Carlos Córdoba
Jefe del Área de Centros de Operaciones de Ciberseguridad
CENTRO CRIPTOLÓGICO NACIONAL

SEC2GRID: Transformando la cadena de suministro para soluciones seguras a largo plazo en redes eléctricas inteligentes

Dentro del propósito de generar confianza en la sociedad y resolver problemas importantes, en PwC colaboramos en el proyecto Sec2Grid, financiado por el Gobierno Vasco a través del programa Hazitek. En dicho proyecto, un consorcio de empresas formado, entre otros, por i-DE parte del grupo Iberdrola, empresa de distribución de referencia, que a través del Global Smart Grids Innovation Hub (GSGIH), aglutina a los principales fabricantes de este tipo de dispositivos (Arteche, Ingeteam, Ormazabal, ZIV y Zigor), así como otros proveedores de servicios especializados como Barbara, y con el soporte de la asociación GAIA y el centro tecnológico Ikerlan. La colaboración entre todos estos actores nos permite abordar los desafíos y establecer una estrategia integral para proteger las redes inteligentes de ciberamenazas.

César Tascón / Gonzalo Gómez-Abad

Desde hace ya varios años, la ciberseguridad en entornos industriales adquirió una importancia creciente debido al aumento de las superficies de ataque y la alta implementación de tecnologías de operación (OT) en sectores clave de la transformación digital, como el energético y de fabricación. Este escenario ha seguido siendo impulsado por la creciente incidencia de ataques informáticos, cambios en las regulaciones gubernamentales y una mayor conciencia entre los actores del mercado sobre la necesidad de adoptar medidas sólidas de protección cibernética.

Las *Smart Grids*: Un entorno desafiante para la ciberseguridad

Las *Smart Grids*, también conocidas como redes inteligentes, representan un entorno altamente eficiente y confiable para el despliegue de una amplia gama de dispositivos autónomos conectados. Con la transición de los sistemas energéticos hacia la era digital, especialmente con la incorporación del Internet de las cosas (IoT), estas redes eléctricas equipadas con IoT poseen un alto nivel de autonomía gracias a su estructura peer-to-peer descentralizada.

Sin embargo, esta evolución también ha traído consigo un aumento significativo en la superficie de ataque y la presencia de vulnerabilidades en los dispositivos de las *Smart Grids*. Ataques tanto físicos como lógicos pueden comprometer la confidencialidad, integridad y disponibilidad de la red eléctrica, lo que representa un riesgo importante para la seguridad nacional y la continuidad del suministro eléctrico. Diversos factores, como el aumento en la cantidad de dispositivos electrónicos inteligentes (IED), el uso de componentes de terceros, la utilización de protocolos de Internet y el mantenimiento inadecuado, han contribuido a este escenario.

El papel clave de la ciberseguridad en la cadena de suministro

En el complejo ecosistema de las redes inteligentes, la ciberseguridad ocupa un lugar central en la cadena de suministro. Desde la fabricación de los dispositivos hasta su instalación y mantenimiento, cada eslabón debe ser asegurado para garantizar una operación segura y confiable.

Dentro del propósito de generar confianza en la sociedad y resolver problemas importantes, en PwC colaboramos en el proyecto Sec2Grid, financiado por el gobierno vasco a través del programa Hazitek. En dicho proyecto, un consorcio de empresas formado, entre otros, por i-DE parte del grupo Iberdrola, empresa de distribución de referencia, que a través del Global Smart Grids Innovation Hub (GSGIH) aglutina a los principales fabricantes de este tipo de dispositivos (Arteche, Ingeteam, Ormazabal, ZIV y Zigor), así como otros proveedores de servicios especializados como Barbara, y con el soporte de la asociación GAIA y el centro tecnológico Ikerlan. La colaboración entre todos estos actores nos permite abordar los desafíos y establecer una estrategia integral para proteger las redes inteligentes de ciberamenazas.

La importancia de la detección temprana de amenazas y actualizaciones ágiles

Para asegurar la seguridad a largo plazo de las redes inteligentes nos hemos enfocado en dos pilares fundamentales en los que hemos visto mayores carencias. El primero de ellos es la detección temprana de amenazas.

Esta se logra mediante la implementación de tecnologías basadas en fuentes de información abiertas, correlación de eventos, inventarios hiper detallados e Inteligencia Artificial (IA) para descubrir y detectar vulnerabilidades en dispositivos IoT y conectados a estas redes. La anticipación es una de las claves para evitar posibles ataques reduciendo la ventana de exposición a las amenazas de ciberseguridad industrial.

La IA se ha convertido en una herramienta crucial para identificar patrones y comporta-

mientos anómalos en el tráfico de datos de las redes eléctricas. Los algoritmos de aprendizaje automático pueden analizar grandes volúmenes de datos en tiempo real, lo que permite detectar y mitigar posibles amenazas en tiempo casi real. A lo largo del transcurso del proyecto todos los participantes han evidenciado que debíamos estar a la vanguardia de la investigación en el desarrollo de estas tecnologías, lo que nos ha permitido alcanzar significativos avances en la detección y neutralización de ataques cibernéticos.

El segundo pilar se centra en el despliegue ágil y eficiente de actualizaciones y parches de seguridad. En este sentido, los dispositivos IoT no siempre tienen capacidad de poder actualizarse de manera ágil. Para superar esta situación, se han empleado técnicas de análisis de vulnerabilidades a gran escala que nos permiten identificar y verificar la existencia de vulnerabilidades en todo el parque de dispositivos. Para ser ágil, es necesario realizar un análisis de la capacidad de explotación de las vulnerabilidades detectadas de manera que posteriormente se puedan coordinar de un modo óptimo y automatizado las actualizaciones de seguridad necesarias.

Obviamente, para asegurar que las operaciones no se ven interrumpidas es necesario probar los cambios propuestos antes de la actualización a un entorno de producción. Para ello contamos con réplicas de estos escenarios desplegadas de manera que se puedan probar las actualizaciones y revisar que la funcionalidad de los dispositivos o de la operación no se vea afectada.

Estas técnicas están orientadas a minimizar el tiempo que transcurre entre la detección de las vulnerabilidades y el despliegue de la corrección en campo, reduciendo al máximo la capacidad de que puedan ser explotadas por posibles atacantes. El objetivo es mantener los dispositivos de las redes inteligentes actualizados y protegidos contra las más recientes amenazas conocidas en tiempo récord.

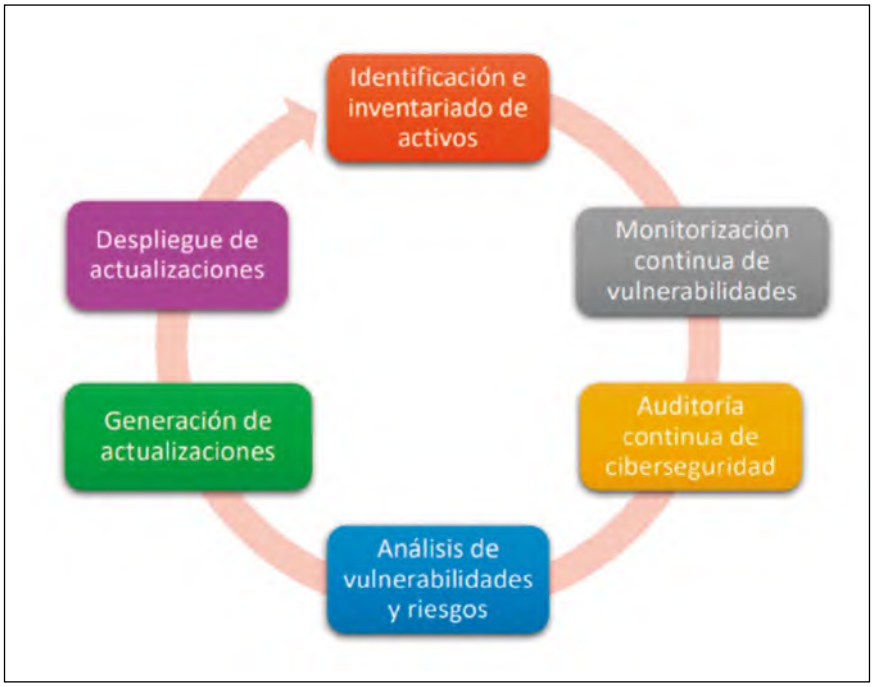
El procedimiento definido en línea con los dos pilares fundamentales del proyecto se basa en un ciclo de acciones que se llevan a cabo de manera coordinada y semi-automatizada.

En primer lugar, se realiza la identificación e inventariado detallado SBOM de todos los activos de la Smart Grid tanto de los paquetes de software instalados en cada equipo así como la configuración de los mismos que permitirá hilar más fino en el análisis de vulnerabilidades. Este repositorio de información común en el que se incorpore información de todos los fabricantes por igual será el punto de acceso único para integrar con los próximos pasos.

Posteriormente, se lleva a cabo un proceso de monitorización y auditoría continua de vulnerabilidades conocidas y aquellas vulnerabilidades *in-the-wild* a través del análisis de fuentes de inteligencia (OSINT) y equipos de detección consiguiendo así evaluar de manera preliminar los posibles riesgos y vulnerabilidades en los dispositivos.

Con la información obtenida, se procede al análisis exhaustivo de vulnerabilidades y riesgos a partir de la información previa recabada y correlando todas las fuentes de información para estudiar la viabilidad y el impacto final de una vulnerabilidad detectada, lo que permite priorizar las acciones y enfoques más efectivos para proteger la red. Puede que a lo largo del análisis se determine que la vulnerabilidad no tiene impacto debido a versiones de software instaladas o incluso debido a configuraciones necesarias para explotar la vulnerabilidad que no apliquen.

La transformación de la cadena de suministro hacia soluciones seguras en redes inteligentes es una tarea desafiante pero vital para garantizar la seguridad nacional y la confiabilidad del suministro eléctrico en España.



A partir de este análisis, se generan las actualizaciones necesarias para corregir las vulnerabilidades identificadas y se prueban en réplicas de escenarios de producción antes de su implementación en campo.

Este ciclo de acciones se desarrolla de manera orquestada, continua y fluida, permitiendo una rápida respuesta a las vulnerabilidades detectadas. La capacidad de anticiparnos, analizar,

generar y desplegar actualizaciones rápidamente es esencial para minimizar la posibilidad de que los posibles atacantes puedan explotar las vulnerabilidades y salvaguardar la seguridad de las redes eléctricas inteligentes.

Una cadena de suministro segura y colaborativa

En la industria de la ciberseguridad, la colaboración entre los distintos actores es esencial para abordar las complejas amenazas que enfrentamos en la era digital. En este caso, la colaboración de PwC con los fabricantes y proveedores de tecnología como Arteche, Ingeteam, Ormazabal, ZIV, Zigor y Barbara así como con i-DE en su rol de distribuidora, y el centro tecnológico Ikerlan, es fundamental para asegurar que los dispositivos y componentes que se integran en las redes inteligentes cumplan con los más altos estándares de seguridad. No hay que olvidar que estos componentes en muchas ocasiones tienen requisitos de ejecución en tiempo real y realizan funciones críticas, conviviendo en un ecosistema heterogéneo compuesto por dispositivos de diferentes fabricantes pueden actuar de un modo coordinado.

Esta colaboración sin precedentes permite una mayor transparencia y trazabilidad a lo largo de toda la cadena de suministro, lo que facilita la identificación y mitigación de posibles vulnerabilidades desde el diseño hasta la implementación y el mantenimiento. El enfoque global permite compartir diferentes visiones, facilitando posibles desarrollos de nuevas tecnologías que hagan frente a los retos del sector. Las soluciones planteadas hasta ahora en el mundo OT no son del todo efectivas por lo que abordar el problema desde la perspectiva de todos los actores de la cadena de valor puede proporcionar una visión compartida que permita plantear soluciones colaborativas generadas sobre tecnologías diferenciadoras.

Aun con los grandes avances que hemos podido hacer, creemos que todavía no es suficiente. El campo de la ciberseguridad en redes inteligentes y la protección de la cadena de suministro sigue evolucionando rápidamente. A medida que las tecnologías continúan avanzando, también lo hacen las ciberamenazas. Esto requerirá que las empresas, fabricantes y los investigadores sigamos trabajando juntos para estar un paso adelante de los ciberdelincuentes y asegurar la resiliencia y seguridad de nuestras infraestructuras críticas. Aquellas entidades que no se tomen esto en serio, corren el riesgo de quedarse atrás en el mercado pues no podrán cubrir los estándares de seguridad de las principales compañías.

La idea es seguir liderando el camino hacia soluciones más seguras y avanzadas para las redes inteligentes a la vez que el negocio pueda ganar en agilidad y mayores prestaciones. La detección temprana de amenazas y el despliegue ágil de actualizaciones son solo el comienzo de un enfoque integral que aborde los desafíos futuros y garantice un suministro eléctrico confiable y seguro para España en la era digital.

Al construir un ecosistema de colaboración y confianza con empresas como Ingeteam, Arteche, Ormazabal, ZIV, Zigor, Ikerlan, Barbara, así como i-DE actor clave del sector, PwC reafirma su compromiso de proteger los activos más valiosos de sus clientes y garantizar la seguridad cibernética en la era de las redes inteligentes.

Conclusión

La transformación de la cadena de suministro hacia soluciones seguras en redes inteligentes es una tarea desafiante pero vital para garantizar la seguridad nacional y la confiabilidad del suministro eléctrico en España. La colaboración con los fabricantes de dispositivos, y la adopción de tecnologías avanzadas, como la Inteligencia Artificial y Edge Computing, demuestran la apuesta de PwC y todos los participantes del proyecto en la búsqueda de soluciones digitales efectivas y de vanguardia. La detección temprana de amenazas y el despliegue ágil de actualizaciones son los cimientos sobre los cuales se construirá un futuro energético seguro y resiliente en la era digital.

A medida que avanzamos hacia un mundo cada vez más conectado, es fundamental que las compañías eléctricas, los fabricantes y las entidades gubernamentales continúen colaborando y trabajando en conjunto para fortalecer las redes inteligentes contra las ciberamenazas. La ciberseguridad no solo es una responsabilidad individual, sino una tarea colectiva que requiere un enfoque integral y una voluntad constante de adaptarse a los desafíos cambiantes del panorama cibernético. Además, aquellos actores que no se tomen en serio la ciberseguridad corren el riesgo de quedarse atrás en el mercado.

En este contexto, PwC se enorgullece de ser un actor líder en la industria de la ciberseguridad, ofreciendo soluciones innovadoras y colaborando con socios estratégicos, para proteger las infraestructuras críticas de España. Al construir un ecosistema de colaboración y confianza con empresas como Ingeteam, Arteche, Ormazabal, ZIV, Zigor, Ikerlan, Barbara así como i-DE, actor clave del sector, PwC reafirma su compromiso de proteger los activos más valiosos de sus clientes y garantizar la seguridad cibernética en la era de las redes inteligentes. ■

César Tascón
Socio
Gonzalo Gómez-Abad
Director
Business Security Solutions
PwC

comforte

¿ESTÁ LISTO PARA MEJORAR LA DEFENSA DE LOS DATOS?

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

www.comforte.com

“Gestionar la ciberseguridad de una multinacional de seguros y de salud, dos sectores que viven a ritmos tecnológicos y regulatorios diferentes, te transforma como CISO”

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

Iván Sánchez López

CISO Global de BUPA

Informático de profesión, Iván Sánchez es un tecnólogo que desde el principio de su carrera se ha dedicado a la gestión de la seguridad de la información en distintas posiciones. Conoce bien el mundo de la consultoría especializada, el de los operadores de telecomunicaciones, el de la logística y, por supuesto, el de seguros y el de salud. En la actualidad, y en su calidad de CISO Global de Bupa, pasa buena parte de su tiempo entre la matriz del Grupo en Londres y la central de una de sus integrantes, Sanitas, en Madrid, compañía de la que fue también CISO. Y cuando se le pregunta por cuál de las dos tiene una posición más madura en ciberseguridad, sonríe y lanza una contestación a la altura: "No voy a especular. Pero le daré datos: Iñaki Ereño, el actual CEO del Grupo Bupa –y antes consejero delegado de Sanitas– es español. Y su CISO global, también". Touché.

– Es usted uno de los CISO españoles más internacionales. Y se observa que desde los inicios de su carrera profesional ha estado ligado a la disciplina de la seguridad de la información. ¿Fue una casualidad del destino o realmente se sintió cautivado por esta práctica?

– Creo que fue la combinación de ambas cosas. Por un lado, ya desde bien joven tenía un enorme interés en todo lo relacionado con la tecnología y por entender cómo funcionaba, imagino que también películas como "Juegos de Guerra" o "Hackers" tuvieron mucho que ver. Pero también hubo muchas casualidades del destino. Durante la carrera escogí, sin tener muy claro de qué iba, la asignatura de Auditoría y Seguridad Informática, y tuve la suerte de tener unos excelentes profesores. Esto hizo que me decidiera por trabajar en el sector y, una vez dentro, tuve también la suerte de dar mis primeros pasos bajo la tutela de grandes responsables, que confiaron en mí y me ayudaron a desarrollarme como profesional de la Seguridad de la Información.

– El sector de salud es esencial, crítico y sus datos se entienden especiales en el RGPD. Pero, además, el que sea objeto de ciberataques que pueden desembocar en filtraciones de datos es algo extraordinariamente sensible para la opinión pública, más allá de las polémicas del cumplimiento o normativo y las sanciones. En términos generales, y con su privilegiada visión, ¿está hoy más preparada para gestionar este tipo de riesgos asociados con la ciberseguridad la sanidad privada que la pública, al revés, o no hay datos que permitan enjuiciar esta cuestión?

– Es difícil responder la pregunta de manera general, únicamente con la perspectiva de sector público o privado. Creo que el entorno de amenazas para ambos se ha incrementado y es más complejo porque el modelo de salud se está transformando de manera acelerada y después de la pandemia somos más conscientes de su importancia, lo que también nos pone un poco más bajo el foco del atacante. Pero del mismo modo, creo que tanto el sector público como el privado están hoy mejor preparados que hace unos años. Personalmente he visto como en el último lustro el sector ha dado un paso de gigante en términos de madurez. Lamentablemente esto no significa que no sigamos viendo ciberataques donde empresas de salud del ámbito público o privado se vean afectadas, y eso a lo que nos lleva es a la necesidad de que, tanto desde el ámbito público como el privado, se siga trabajando conjuntamente por la mejora de las capacidades del sector, por ejemplo compartiendo información o dando soporte en caso de incidente, sobre todo si tenemos en cuenta que no se trata de ámbitos aislados, ya que desde el punto de vista del paciente, en muchísimas ocasiones hablamos de la misma persona como usuario del sector público y del privado.

– Con una brillante carrera profesional en Sanitas, y tras integrarse esta en Bupa, ha pasado usted a la posición de CISO Global de esta compañía de origen británico. Antes de preguntarle por los aspectos específicos de seguridad de la información, quisiera rogarle que explicara qué modelo de servicio TIC están construyendo en Bupa y a qué transformaciones en los servicios TIC obliga el grupo a las compañías que se van integrando en él.

– Bupa es una compañía con más de 75 años de historia que se crea en Reino Unido tras la segunda guerra mundial para dar respuesta a, en aquel momento, un inexistente sistema de salud. Se concibe como una mutua para sus asociados y sin accionistas, y desde entonces experimenta un enorme crecimiento, dando servicio hoy en día a unos 22 millones de clientes en más de 20 países. El modelo de mutua se ha mantenido hasta la actualidad, lo que nos permite reinvertir todo el beneficio en la mejora de la compañía, incluidos los servicios de Tecnología.

Desde el punto de vista de la provisión de servicios TIC, en su mayoría estos se prestan desde las propias unidades de negocio del Grupo, que normalmente están encuadradas en un país o una región, lo que les permite tener un cierto grado de autonomía.

Desde el Grupo se definen los objetivos estratégicos y las principales líneas de actuación, y también se prestan algunos servicios TIC que son transversales a todas las regiones. Con nuestro modelo actual, las compañías del Grupo no se ven obligadas a grandes transformaciones de su *core* tecnológico, si bien estos últimos años sí se han visto en la necesidad de adoptar modelos *Cloud*, ya que es un facilitador clave para la transformación del negocio y que viene impulsado desde el propio Comité Ejecutivo Global. En algunos casos, ese movimiento a la nube sí ha supuesto acelerar en algunas regiones.

– En consonancia con este modelo, ¿cómo está organizada la función de seguridad de la información a efectos del Grupo y qué grado de libertad se permite a cada compañía integrada?

– La función de seguridad de la información de Bupa está enmarcada dentro del área de Tecnología. Ello quiere decir que trabajamos bajo el modelo de provisión de servicios TIC que he mencionado antes, pero con mayor nivel de integración entre los diferentes países. La función Global de Seguridad está encabezada por mí, a continuación, tenemos las regiones (tres, Europa & Latam, APAC y Reino Unido & mercados globales) y por último tenemos los países o unidades de negocio que pertenecen a estas regiones. Por ejemplo, la región de Europa & Latam (donde trabajé antes de ser nombrado para el rol Global) incluye a España (Sanitas), Polo-

nia, Turquía, Brasil, Chile, México y una compañía con sede en Miami. Cada una de las regiones cuenta con un CISO y su equipo, y este a su vez tiene responsables de seguridad en cada uno de los países, que también cuentan con equipos locales. Además de la función de Seguridad, existe una de Riesgos y Cumplimiento que hace supervisión como segunda línea, y se organiza de una manera muy parecida al área de Seguridad. Bupa está muy regulada en la parte del negocio asegurador (que es la más importante), por lo que la segunda línea es fuerte y tiene un foco importante en la Seguridad de la Información.

En cuanto a los comités de dirección, tanto los regionales como especialmente el Global, son muy conscientes de la relevancia que ha tomado nuestro ámbito y cada vez nos piden más foco en tener una función integrada que, asumiendo las diferencias que puedan existir a efectos de negocio, asegure un nivel de protección homogéneo entre países y regiones. Estamos justo ahora en ese proceso.

– ¿Se siente apoyado por los órganos de administración y la alta dirección?

– Reporto al menos trimestralmente al Consejo y al Comité ejecutivo Global, y quizá es el momento en toda mi carrera profesional donde he encontrado más apoyo en el comité para sacar adelante nuestras iniciativas, lo que por otra parte mete cierta presión, ya que cada vez quieren estar más y mejor informados.

– ¿Interviene como CISO en la gestión de la ciberseguridad de la OT/IoT operativa en el Grupo?

– Dentro de las funciones del CISO está la de seguridad OT/IoT, ámbito en el que estamos haciendo bastantes cosas. Pero, por ser honesto, necesitamos hacer muchas más. Todavía quedan áreas en el ámbito de Seguridad IT tradicional donde seguir mejorando y no hemos tenido capacidad de entrar en ámbitos como OT/IoT. Una de las razones es que la digitalización del sector no era elevada y no existía un modelo de ataque basado en OT, pero esto ha cambiado y sigue cambiando a pasos acelerados y ahora el mIoT (Medical IoT) es ya una realidad, con lo que aparecen escenarios reales de amenaza.

– ¿Cómo han formalizado la relación de Seguridad de la Información con el DPO en todo el ciclo de vida de los tratamientos TIC de datos sanitarios?

– La figura del DPO es clave para nosotros, por el tipo de datos que gestionamos y la regulación a la que estamos sometidos. Ya antes de existir el GDPR y de formalizar la figura del DPO, contábamos con un modelo de relación con el área Legal y de Riesgos & Cumplimiento para definir y validar los requisitos en cualquier proyecto de tratamientos de datos en el ámbito sanitario porque, siendo conscientes de la necesidad de innovación y de desarrollo de nuevos servicios, el Grupo tiene un apetito muy bajo en lo que al uso indebido de datos de salud se refiere. Con la aprobación del GDPR y la formalización del rol del DPO, el Comité de Seguridad y Privacidad creció en importancia y actualmente tiene supervisión directa del Consejo. Esto nos permite tener un Comité con participación de responsables de negocio, y con capacidad de revisión y aprobación de las iniciativas relevantes. Ahora bien, aunque estos cambios han venido en gran medida impulsados por GDPR hemos extendido el modelo de trabajo al resto de geografías, puesto que en muchas de ellas no existía una regulación fuerte en lo que al tratamiento de datos sensibles se refiere.

– Lograr un nivel de ciberseguridad aceptable en la cadena de suministros es imperioso. ¿Cómo gestionan este particular en sus líneas de negocio, incluyendo a los intermediarios?

– Ha tocado uno de los temas para mí más relevantes ahora mismo. Estos últimos años hemos estado dedicados a mejorar y reforzar nuestras medidas de segu-

"Revisamos la ciberseguridad de nuestra cadena de suministro. Pero el enorme esfuerzo que esto conlleva puede llegar en ocasiones a ser difícil de justificar internamente. Los proveedores deben ser capaces de facilitarnos el proceso y, al tiempo, asumir parte de los costes".

ridad internas, porque era lo adecuado en ese momento y porque la complejidad y longitud de nuestra cadena de suministro no era ni de lejos la que hay ahora.
En la actualidad nos encontramos con que el número de proveedores se ha multiplicado en todas las áreas de negocio, y no todos ellos entienden la ciberseguridad de la misma manera ni existe un nivel "aceptable" y comparable entre ellos, por lo que estamos poniéndole mucho foco y esfuerzo.
Hace tiempo que intentar someterlo todo a un contrato dejó de ser práctico, por lo que en Bupa hemos creado equipos para la revisión de la cadena de suministro tanto en primera línea (dentro del equipo de Ciberseguridad) como en segunda línea, que trabajan tanto en el descubrimiento de los proveedores como en su posterior categorización en función de su complejidad e identificación del potencial riesgo en función de sus controles. Pero es un esfuerzo y coste enorme, y que puede llegar a ser difícil justificar internamente, por lo que creo que aquí los proveedores deben ser capaces de ayudarnos no solo facilitando el proceso, sino asumiendo además parte de los esfuerzos y costes. Las iniciativas que ya hay en este sentido en sectores como por ejemplo en banca me parecen fantásticas.

– Los distintos colectivos de profesionales del sector salud llevan a gala cuidar la confidencialidad de los datos. Pero quizá hoy se sientan desbordados por las capacidades de los servicios TIC que utilizan y también inquietos por la posibilidad de que puedan dejar expuestos datos sin saberlo al ser objeto de engaños. ¿Son receptivos estos colectivos a la hora de recibir formación sobre seguridad de la información?

– Cada sector tiene un tipo de usuario distinto y seguro que cada CISO al que pregunte podría decirle que sus usuarios son los más complejos o difíciles de tratar. Pero en mi caso, habiendo trabajado en sectores muy diferentes, creo que el colectivo médico puede ser uno de los más complejos, cuando no el más complejo. Partiendo de la base, como bien comenta, que están tremendamente concienciados en todo lo relativo a la confidencialidad y el buen uso de los datos, hay que entender que su relación con la tecnología es muy distinta a cualquier otro sector. Por un lado, como decía antes, el sector se está digitalizando de manera acelerada y eso quiere decir que cada vez tienen más herramientas a su disposición y que, además, cambian cada vez más rápido.
Por otro lado, los profesionales médicos son un colectivo con una gran movilidad. Quiero decir que no es infrecuente ver a un profesional trabajando a la vez en la sanidad pública y la privada, y dentro de la privada, en diferentes grupos de salud a la vez. En cada uno de esos ámbitos se va a encontrar unos controles, unos sistemas y unas tecnologías diferentes, lo que les genera cierta ansiedad y esa sensación de sentirse desbordados. Y un usuario en esas condiciones puede no ser consciente del impacto que tiene un uso incorrecto de su contraseña o del manejo de información sensible. La manera que tenemos de abordarlo en el Grupo Bupa es tratando de implementar un modelo de seguridad centrado en el usuario, lo que quiere decir que tiene en cuenta factores como por ejemplo la usabilidad o la experiencia del usuario, y nos ha funcionado muy bien. Esto nos ha ayudado a tener una buena relación con el usuario y la asistencia y respuesta a las formaciones que se les ofrecen es positiva. Sin duda queda por hacer, porque está viniendo cada vez más tecnología médica y tendremos que seguir formándoles en el buen uso de la misma.

– ¿Cuáles son los retos específicos a los que se enfrenta hoy el sector de seguros de salud y servicios de salud en materia de ciberseguridad y resiliencia?

– Hace bien en diferenciar ambos sectores, el de seguros y el de salud, porque tienen retos completamente diferentes. Por un lado, en el sector de seguros, el principal reto al que nos enfrentamos es el regulatorio. Históricamente la regulación en el sector financiero estaba centrada en banca, y con los años han alcanzado un nivel de madurez alto y de alguna manera homogéneo en el sector. Posteriormente, la regulación ha virado hacia el sector asegurador, partiendo desde ese nivel alto ya alcanzado, lo cual es un reto importante a la hora de la adaptación, y por supuesto el coste que supone. Y esto en el Grupo Bupa es aún más complejo porque estamos sometidos a cinco reguladores del sector asegurador por los diferentes países y regiones en los que operamos. Hemos hecho las cosas adecuadas, pero por supuesto la regulación va evolucionando y no podemos quedarnos quietos. Por otro lado, en el sector de salud, los retos son bien distintos. Curiosamente, no son retos regulatorios, puesto que no existen reguladores o normas como sí existen en el entorno asegurador, sino que los retos son, sobre todo, en el ámbito de la ciber-resiliencia. Un hospital es un entorno que opera 24x7x365, no puedes 'parar' de prestar servicio, por lo que el impacto que tiene un ciberataque es enorme y puede llegar a comprometer vidas humanas (como ya ha sucedido en varios incidentes en entornos hospitalarios). Este es un escenario verdadero de "ataque híbrido", con lo cual tienes que

"¿Cómo reparto mi tiempo como CISO? En el momento presente dedico un 10% a Operación, un 40% a Gobierno, y un 50% Gestión. Y siempre estoy interactuando con otras funciones y comités de la compañía para seguir posicionando en su agenda el área de Ciberseguridad".

"Reporto al menos trimestralmente al Consejo y al Comité Ejecutivo Global. Quizá sea este el momento en mi carrera profesional donde he encontrado más apoyo y, al tiempo, una creciente demanda de información de alta calidad".

entrenar la respuesta y la recuperación ante un ciberataque.

Sea como fuere, hay un reto común a ambos sectores: el de la digitalización, que puede llegar a aumentar la superficie de ataque si no se adopta con la seguridad tecnológica, y el proceso de seguridad incorporado en la gestión.

– **Medir la madurez en ciberseguridad de uno contra sistemas reconocidos internacionalmente, y poder compararse con otros jugadores del mismo sector usando el mismo sistema de medida, es crucial. ¿Vamos por el buen camino? De poder hacerse, ¿cómo cree que quedaría Bupa en el "ranking"?**

– Creo que sí, estoy muy a favor. Tener la capacidad de medirse contra un modelo reconocido y posteriormente poder compararse es una buena práctica. Ahora bien, la implementación de un modelo de comparación homogéneo no es fácil porque, como decíamos antes, la presión regulatoria varía por regiones, así como los recursos y presupuestos también varían. Pero esto no quiere decir más que hay trabajo por hacer para llegar a ese modelo homogéneo. Es el buen camino.

En Bupa hemos hecho varios ejercicios de análisis de madurez bajo el modelo del NIST-CSF, que han resultado muy relevadores puesto que nos ayudaron a identificar partes del Grupo donde era necesario un impulso en la madurez de ciberseguridad y nos compararon con el sector, estando por encima de la media. Ahora que se nos viene una actualización del NIST-CSF, tiene sentido que nos planteemos un ejercicio bajo este nuevo modelo.

En cuando a cómo quedaría Bupa hoy en día, es algo aventurado por mi parte, pero creo que no saldríamos mal en base a los ejercicios anteriores que comento y por la inversión del grupo y la dedicación y capacidades de nuestro equipo de Ciberseguridad a nivel Global.

"El alcance en el sector salud de la tecnología y los servicios mIoT (Medical IoT) ha generado modelos de ataque y escenarios reales de amenaza propios, que vienen a sumarse a los del entorno TIC tradicional".

– **¿Tiene participación en la prescripción de tecnologías con finalidades de ciberseguridad en el Grupo y capacidades de fijar requisitos de ciberprotección que debe cumplir el Grupo en los servicios en nube?**

– Sí, es parte de mi función y de la revisión del modelo de Ciberseguridad del Grupo que comentaba anteriormente. Bupa opera negocios muy diferentes en multitud de regiones, y tenemos que asegurar que contamos con la tecnología adecuada para nuestras necesidades, por lo que la convergencia hacia soluciones y plataformas es fundamental para reducir carga operativa y optimizar las inversiones en ciberseguridad. Operar 10 tecnologías en 10 países para cumplir un mismo propósito es ineficiente, porque los equipos trabajarán de manera aislada y los costes se multiplican. La compartición de información será inexistente o limitada y a la larga eso hará que estemos peor preparados ante un adversario que concentra sus esfuerzos en atacarnos. Ahora bien, tampoco veo un modelo donde el 100% de las tecnologías se hayan integrado a nivel grupo, puesto que siempre habrá necesidades locales muy diferentes entre países, por eso tenemos un grado de flexibilidad. Queremos ir hacia este modelo, y eso incluye las soluciones y servicios de seguridad en la nube donde además es mucho más fácil la convergencia porque los proveedores ya son globales de por sí.

– **¿Cuántos proveedores de tecnologías y servicios TIC, incluidos los de ciberseguridad, gestiona como CISO?**

– Depende mucho de la región o el país al que nos refiramos, pero si hablamos por todas las funciones de CISO del Grupo Bupa, creo que podemos estar en un entorno de alrededor de 400 proveedores de tecnología, de los cuales aproximadamente un tercio son proveedores de servicios y tecnologías de ciberseguridad.

– **Una última pregunta: ¿qué porcentaje de su tiempo dedica a las distintas áreas de gestión de la ciberseguridad?**

– Ha ido cambiando con el tiempo y con mi evolución dentro del Grupo Bupa. En mi rol anterior de CISO de Sanitas y de la región de Europe & Latam, repartía mi tiempo posiblemente algo así como un 40% Operación, 30% Gobierno, y 30% Gestión (con dirección, otros departamentos, etc.). Por lo general estaba bien repartido, aunque en ocasiones podría dejar poco margen a la gestión en momentos de alta operación.

Por suerte, los integrantes del equipo de Ciberseguridad de Sanitas son excelentes, y me ayudaron a crear cada vez más margen para la gestión, lo que me permitió una mayor y más frecuente interlocución con los comités de dirección.

Actualmente en mi rol de CISO del Grupo, quizás hablamos de un 10% Operación, 40% Gobierno, y 50% Gestión, y paso la mayor parte de mi tiempo interactuando con otras funciones del Grupo y comités para seguir posicionando al área de Ciberseguridad en la agenda de la compañía. ■

ARMIS

Contacta con nosotros
armisiberia@armis.com

Visualiza y asegura todos tus activos.

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

armis.com/es

En buena compañía

La ciberseguridad efectiva como base de la resiliencia empresarial

La legislación sobre ciberseguridad y resiliencia ya promulgada por la UE (NIS2 y DORA) y por muchos países, dibuja el camino que deben seguir las corporaciones y los integrantes de las cadenas de suministro para transformar los sistemas de gestión de riesgos en su camino hacia la operativa digital plena, caracterizada por una automatización granular casi estándar, el respeto en tiempo y forma de los derechos de las personas en el tratamiento de sus datos, y la inversión ponderada en ciberseguridad para ponérselo lo más difícil posible a la floreciente delincuencia.

Si hay una normativa disruptiva en el modo de enfocar la resiliencia operativa y, en su marco, la calidad, mejora continua y efectividad de la ciberseguridad, es DORA. Este reglamento sectorial, que afecta a entidades financieras y sus clientes, se enmarca en la más pura tradición de la gestión de riesgos en la empresa (que traspasa fronteras), y que servirá también para ir fijando experiencias que puedan trasladarse a otros sectores (regulados o todavía no regulados) distintos del financiero.

Securmática –cuyo lema este año es "En buena compañía"– presenta un programa fiel reflejo de lo manifestado en los párrafos anteriores, en el que organizaciones usuarias privadas de distintos sectores (el más representado, sin duda, el de banca) y públicas, junto a sus proveedores principales, van a exponer iniciativas y proyectos en distintos frentes de la gestión de la seguridad de la información, la ciberseguridad y, en última instancia, la resiliencia.

* Es posible obtener una versión en pdf del programa del congreso en www.securmatica.com

PARTICIPANTES Y PONENCIAS *

Conferencia inaugural

La resiliencia digital del sector financiero

- **Silvia Senabre**, Jefa del Grupo de Riesgo Tecnológico de la Dirección general de Supervisión del Banco de España

BANCO SANTANDER: Resiliencia colectiva. El camino de la colaboración hacia un ecosistema más seguro

- **Hazel Díez Castaño**, CISO Global en Grupo Santander

BBVA: Seguridad embebida: Distribuyendo el centro de gravedad para garantizar la ejecución

- **Roberto Ortiz Plaza**, CISO del área Global Software Development. BBVA
- **José Ignacio Garrido**, Global Head of Information Security en BBVA

EL CORTE INGLÉS: Transformación de la función de Ciberseguridad en un grupo empresarial multisectorial

- **Enrique Solbes**, CIO Global de Grupo El Corte Inglés
- **Alejandro Ramos**, CISO Global de Grupo El Corte Inglés
- **Jesús Romero**, Socio responsable de Business Security Solutions. PwC

ABANCA: ¿Cómo sintetizar todos los datos sobre riesgo humano en un solo indicador que permita gobernar tu programa de concienciación?

- **Carlos Pérez Saldaña**, CISO de Grupo Abanca
- **Javier Ruiz de Ojeda**, Consultor GRC Senior en Áudea Seguridad de la Información

CONGRESO DE LOS DIPUTADOS: Una experiencia práctica de la transición de una administración pública hacia la ciberseguridad como servicio

- **José Andrés Jiménez Martín**, Jefe del Dpt. de Asesoramiento Técnico de la Dirección de TIC del Congreso de los Diputados
- **Auxiliadora Ureña Serena**, Responsable de Desarrollo de Negocio de ciberseguridad en Babel

GRUPO INDUKERN: Fugas de información sensible, un reto para las empresas

- **Iván Muñoz Lois**, Responsable de Ciberseguridad en Grupo Indukern
- **Roger Ares Viñas**, Senior Manager de Riesgos Tecnológicos y ciberseguridad en KPMG

RENFE: El reto actual de la detección y respuesta en servicios esenciales

- **Francisco Lázaro**, CISO y DPO de Renfe
- **Lorenzo Mateu**, Director de Desarrollo de S2 Grupo
- **Óscar Navarro**, Director del Área Industrial de S2 Grupo

AGENCIA DE CIBERSEGURIDAD DE CATALUÑA: Integración continua: Fusión de responsabilidades para crecer en capacidades ciber

- **Tomás Roy Catalá**, Director de la Agencia de Ciberseguridad de Cataluña
- **Rafael Ortega García**, Director de Operaciones de Factum

BANCA MARCH: Transformación de la función de seguridad

- **Javier Gayoso Enrique**, CISO de Banca March
- **Juan López-Rubio Fernández**, Senior Director de Alvarez & Marsal

BETMEDIA: Identidades Digitales Descentralizadas como eje estratégico

- **Sam M. Barranco**, Director de Operaciones de Betsfy (Grupo Betmedia)
- **Óscar Flor**, Digital Identity Director de Wise Security Global

GRUPO MÁSMÓVIL: Consolidación en un único SOC de las operaciones de ciberseguridad

- **Jesús Ángel Santos López**, Director de Infraestructura, Workplace y Seguridad en Grupo Másmóvil
- **Juan Miguel Velasco**, CEO y Fundador de Aiuken Cybersecurity

CAIXABANK: Bug Bounty y Red Team como medios necesarios para asegurar la ciberseguridad

- **Mario Maawad Marcos**, Director de Innovación en Seguridad y Red Team de CaixaBank
- **Gonzalo Sánchez Delgado**, Hacking Service Manager de Entelgy Innotec Security

CAIXABANK: Cómo proteger una plataforma de datos e IA corporativa: amenazas, controles y tecnología

- **Jesús Muñoz Núñez**, Director de CSIRT & Security Analytics de Digital Security de CaixaBank
- **José Carlos Cerezo Luna**, Head of EMEA South Security and Compliance Team de Google Cloud

MEDIASET: Ciberseguridad de calidad durante 30 años en buena compañía

- **Ramón Ortiz**, Responsable de Seguridad de Mediaset
- **Óscar Riaño**, Responsable del CERT de GMV

SABADELL DIGITAL-BANCO SABADELL: Arrojando luz en zonas oscuras. Defensa contra amenazas avanzadas

- **Adolfo Hernández**, CISO en Sabadell Digital y Director de Operaciones de Seguridad de Banco Sabadell
- **Nuria Andrés Pastor**, Especialista en Soluciones de Ciberseguridad, Cumplimiento e Identidad para el Sector Financiero en Microsoft

PALLADIUM HOTEL GROUP: Lecciones aprendidas en servicios de Detección y Respuesta a Incidentes

- **Francisco García Lázaro**, CISO Corporativo de Palladium Hotel Group
- **Rubén Gómez**, Responsable de servicios de Detección y Respuesta a Incidentes y Responsable de Arquitectura de Ciberseguridad de Fujitsu

PROSEGUR: Redefiniendo la Ciberseguridad: Automatización Inteligente para una protección eficaz

- **Miguel Ángel Carretero**, CISO Global de Prosegur Compañía de Seguridad
- **Carlos Fernández**, Responsable Global de la división xMDR en Cipher

ADEVINTA: Cibervigilancia en marketplaces: Protegiendo y asegurando la confianza del usuario

- **Laura Caballero**, CISO en Adevinta Spain
- **Vicente Martín**, Vicepresidente Senior de Producto en Outpost24

ING España: La evolución de la función del CISO: mejora y madurez continua

- **Gustavo Lozano**, Chief Information Security Officer. ING España
- **Víctor Hernández**, Managing Director, Financial Services Security Lead en Accenture Iberia

GRIFOLS: Evolución de las capacidades de Ciberseguridad en buena compañía

- **Susana Calvo**, Director Information Security Office de Grifols
- **Marcos Sánchez Martínez**, Manager de Ciberseguridad en EY España

** El orden en el que aparecen aquí las conferencias es meramante informativo y no se corresponde con su ubicación final en el programa*

CONFERENCIA INAUGURAL

La resiliencia digital del sector financiero

Silvia Senabre
Jefa del Grupo de Riesgo Tecnológico de la Dirección General de Supervisión Banco de España

Sinopsis: "La transformación digital del sector financiero, acelerada en los últimos años, es clave para su competitividad y para ofrecer a los clientes servicios personalizados de modo ágil, efectivo e innovador. Sin embargo, esta digitalización conlleva un incremento de los riesgos relacionados con la tecnología, no solo por el aumento de los ciberataques sino también debido a la enorme complejidad de los entornos tecnológicos de las entidades financieras. A ello hay que sumar la creciente dependencia de proveedores tecnológicos especializados, que se han convertido en actores críticos para el sector.
En este contexto, garantizar la resiliencia digital de las entidades financieras resulta crucial y se ha convertido en una prioridad para reguladores y supervisores, como evidencia la efervescencia legislativa en este ámbito. Destaca especialmente el Reglamento DORA, que va a suponer un punto de inflexión para el sector".

BBVA: Seguridad embebida: Distribuyendo el centro de gravedad para garantizar la ejecución

Sinopsis: "La superficie de ataque no para de crecer y la sofisticación de los atacantes no tiene límites. Si a estas dos condiciones sumamos la transformación de las compañías a través de servicios digitales, el resultado es un listado ingente de tareas y proyectos a ejecutar para garantizar una postura adecuada de seguridad. Para ejecutar dichas tareas es fundamental, al menos en organizaciones grandes y complejas, la involucración de numerosos stakeholders. Si además queremos tener éxito en la ejecución, es totalmente necesario que todos los participantes sean conscientes y corresponsables de las acciones a llevar a cabo para mitigar el potencial riesgo de ciberseguridad. Por este motivo, para lograr una ejecución eficaz y eficiente, hay que hacer partícipe a todas las unidades, principalmente a aquellas donde reside o se puede materializar el riesgo. Esto lo estamos consiguiendo con la denominada seguridad embebida que explicaremos durante la ponencia".

Roberto Ortiz Plaza
CISO del área Global Software Development en BBVA

José Ignacio Garrido
Global Head of Information Security en BBVA

BANCO SANTANDER: Resiliencia colectiva. El camino de la colaboración hacia un ecosistema más seguro

Hazel Díez Castaño
CISO Global en Grupo Santander

Sinopsis: "La evolución de las capacidades de la ciberdelincuencia global, fomentadas por la impunidad y un alto retorno de la inversión, redunda en un coste exponencial para la sociedad. Combatir el cibercrimen es un gran desafío para el que la acción individual no es suficiente. Es necesario un cambio fundamental hacia una respuesta colectiva de la sociedad, el gobierno y las organizaciones. Iniciativas enfocadas en impulsar la colaboración, fomentar la innovación y construir una sólida cultura de ciberseguridad son la única opción para mejorar".

CONGRESO DE LOS DIPUTADOS: Una experiencia práctica de la transición de una administración pública hacia la ciberseguridad como servicio.

José Andrés Jiménez Martín
Jefe del Departamento de Asesoramiento Técnico de la Dirección de Tecnologías de la Información y de las Comunicaciones del Congreso de los Diputados.

Auxiliadora Ureña Serena
Responsable de desarrollo de negocio de ciberseguridad en Babel

Sinopsis: "El Congreso de los Diputados es un órgano constitucional de importancia capital en la arquitectura institucional del Estado español, como encarnación del poder legislativo dentro de las Cortes Generales y su posición preeminente en el marco del bicameralismo asimétrico establecido por la Constitución Española de 1978. La ponencia expondrá los principales retos que enfrenta la Cámara en materia de ciberprotección y las líneas básicas de su estrategia en este aspecto, la transición del Congreso de los Diputados hacia la ciberseguridad como servicio, desde la concepción hasta la ejecución práctica de la mano de Babel, desglosando el engarce del proyecto de ciberseguridad en el marco de transformación digital y digitalización del Congreso de los Diputados, así como las perspectivas de evolución para el futuro a corto y medio plazo".

GRUPO INDUKERN: Fugas de información sensible, un reto para las empresas

Iván Muñoz Lois
Responsable de Ciberseguridad en Grupo Indukern

Roger Ares Viñas
Senior Manager de Riesgos Tecnológicos y Ciberseguridad en KPMG

Sinopsis: "La tecnología cada día está más presente en nuestro trabajo, utilizando múltiples dispositivos, compartiendo información digital a distintas personas o guardando ficheros en múltiples ubicaciones. Este contexto híbrido y diversificado hace que sea un reto para las empresas conocer y controlar la información que utilizan sus empleados. Veremos en esta sesión cómo las organizaciones pueden identificar la información sensible que gestionan, protegerla adecuadamente y evitar casos de fuga, que pueden tener un impacto legal, reputacional o económico. Comentaremos qué tipo de soluciones se pueden implementar para descubrir, monitorizar y minimizar los riesgos de fuga de información".

EL CORTE INGLÉS: Transformación de la función de Ciberseguridad en un grupo empresarial multisectorial

Enrique Solbes
CIO Global
Grupo El Corte Inglés

Alejandro Ramos
CISO Global
Grupo El Corte Inglés

Jesús Romero
Socio responsable
Business Security Solutions PwC

Sinopsis: "El grupo El Corte Inglés se encuentra inmerso en un ambicioso plan de transformación digital, como uno de los ejes principales de la estrategia corporativa diseñada para consolidar su tradicional posición de liderazgo en el corto y medio plazo. Durante la ponencia se analizará la evolución de la función de ciberseguridad del grupo que habilitará esa transformación, garantizando la resiliencia del negocio, la continuidad de las operaciones y la protección de los activos digitales".

ING España: La evolución de la función del CISO: mejora y madurez continua

Sinopsis: "Durante los últimos años, la función del CISO en ING ha evolucionado, incrementado las responsabilidades y el perímetro. Los trabajos realizados han permitido a ING evolucionar la postura de seguridad, automatizando y madurando muchos procesos, permitiendo de esta forma utilizar los recursos disponibles en áreas menos maduras. Gracias a este esfuerzo, el nivel de resiliencia ha mejorado, pero también la visión de la alta dirección sobre el trabajo y los beneficios generados por el área de seguridad".

Gustavo Lozano
Chief Information Security Officer
ING España

Víctor Hernández
Managing Director, Financial Services Security Lead en Accenture Iberia

BANCA MARCH: Transformación de la función de seguridad

Javier Gayoso
CISO de Banca March

Juan López-Rubio
Senior Director
de Alvarez & Marsal

Sinopsis: "La función de seguridad o ciber seguridad ha tomado en los últimos tiempos una especial relevancia desde todos los puntos de vista. Los atacantes son cada vez más sofisticados y cada paso de la digitalización da lugar a una mayor abstracción y a los consiguientes riesgos de seguridad y fraude. Por otro lado, los negocios y los clientes también esperan que sus riesgos sigan siendo bajos en cada uno de los puntos de contacto con el banco. La respuesta ha sido un incremento de la seguridad que supone un formidable reto para la función de seguridad que tiene que cambiar y transformarse para dar respuesta a estos y a los nuevos retos que se vislumbran en el horizonte".

AGENCIA DE CIBERSEGURIDAD DE CATALUÑA: Integración continua: Fusión de responsabilidades para crecer en capacidades ciber

Tomás Roy Catalá
Director de la Agencia de
Ciberseguridad de Cataluña

Rafael Ortega
Director de Operaciones
de Factum

Sinopsis: "Las amenazas y lo más importante, los vectores de ataque y las TTP evolucionan igual o más rápido que la tecnología. Durante la pandemia las tecnologías que permitieron el teletrabajo durante el confinamiento fueron objeto de ataques (VPN, RDP, VDI), con foco en el *endpoint* y el usuario, basándose fundamentalmente en la explotación de vulnerabilidades del software y la escalada de privilegios. Según nuestros datos, en la actualidad, los ataques de *ransomware* están basados en copias, credenciales, obsolescencia tecnológica o deficiencia de parcheo y configuraciones, con foco en la cadena de suministro o terceras partes. Tenemos claro que en un futuro muy próximo los vectores de ataques serán las aplicaciones y los puestos de trabajo que dan acceso a ellas, con el objetivo de conseguir atacar a la información.

Las anteriores etapas las hemos resuelto con protección, pero sobre todo con capacidades de detección y respuesta. ¿Pero qué capacidades tendremos para detectar y responder a las amenazas e incidentes contra la información durante la ejecución de las aplicaciones? ¿Cómo podremos diferenciar el uso de una credencial y un acceso, respecto a su abuso? La monitorización de las aplicaciones y la experiencia del usuario es una materia ampliamente desarrollada por los centros de control IT bajo el epígrafe de observabilidad. La capacidad inteligente de analizar, investigar y definir unas acciones de respuesta a un incidente son los puntos fuertes del SOC/CERT. Fusionar estas capacidades con las áreas de control IT, desde nuestro punto de vista, son el único camino para aprovechar el Threat Intel, la respuesta rápida, la reducción de costes y riesgos en la capa de aplicación. La colaboración y corresponsabilidad de IT y Ciber en las tareas de *threat hunting*, remediación y respuesta a los incidentes en las aplicaciones, mediante la observabilidad, es el único camino para incorporar la ciberseguridad al rendimiento y la experiencia del usuario y conseguir proteger la información".

ADEVINTA: Cibervigilancia en marketplaces: Protegiendo y asegurando la confianza del usuario

Laura Caballero
CISO en Adevinta Spain

Vicente Martín
Vicepresidente Senior de Producto en Outpost24

Sinopsis: "Adevinta es una empresa cuyo negocio se basa en los marketplaces, con marcas reconocidas como Infojobs, Milanuncios, Coches.net y Fotocasa. Su principal enfoque es ayudar a las personas a encontrar lo que están buscando, y para ello, situa a los usuarios como su máxima prioridad. Sin embargo, en un entorno digital en constante cambio, donde tanto los usuarios como las plataformas están expuestos a diversas amenazas, es crucial adoptar medidas más allá de lo convencional para mitigar estos riesgos. En este contexto, Adevinta apuesta por soluciones innovadoras basadas en cibervigilancia, las cuales se integran de forma escalable en su día a día. En particular, en un entorno donde la protección de las credenciales de los usuarios es fundamental, ya que son la puerta de acceso a los servicios y a la información personal, contar con un sólido sistema de cibervigilancia resulta imprescindible. Este sistema no solo se encarga de monitorizar las técnicas de robo de credenciales tradicionales –como las exfiltraciones o los *stealers*–, sino que también realiza un seguimiento exhaustivo de las nuevas técnicas, como los *traffers*. Mediante una aproximación proactiva, Adevinta se dedica a integrar estas medidas de cibervigilancia en su operativa diaria, con el objetivo de proteger a los usuarios y prevenir posibles ataques cibernéticos. Esta estrategia garantiza la seguridad tanto de los usuarios como de las plataformas en las que operan".

BETMEDIA: Identidades Digitales Descentralizadas como eje estratégico

Sinopsis: "Betmedia es una red social exclusiva para el mundo de las apuestas deportivas, en la que pueden interaccionar los usuarios, los pronosticadores y *coaches* profesionales, y las casas de apuestas, ofreciendo información y servicios gratuitos o de pago por uso o suscripción. Esta plataforma permite a los usuarios encontrar las mejores apuestas de pronosticadores de todo el mundo y convertirse en *tipsters* creando sus propios pronósticos. Betmedia desea alcanzar dos hitos estratégicos con la implementación de la solución conjunta de Wise DID Authenticator y OneLogin: 1) Acercarse a un modelo de gestión de identidades que se adapte a las nuevas regulaciones europeas, cada vez más exigentes en el ámbito de las apuestas, simplificando el proceso de alta y gestión que realiza el usuario y pudiendo verificar inequívocamente la edad de sus usuarios; y 2) Por otro lado, poder permitir a futuro a sus usuarios, mediante sus identidades digitales, acceder a otros sistemas y aplicaciones. De este modo, los *partners*, operadores o empresas afiliadas o asociadas a Betmedia podrán tener acceso directo a la gran base de datos de usuarios que tiene esta plataforma, facilitando las posibilidades comerciales de ambas marcas".

Sam M. Barranco
Director de Operaciones de Betsfy (Grupo Betmedia)

Óscar Flor
Digital Identity Director de Wise Security Global

GRUPO MÁSMÓVIL: Consolidación en un único SOC de las operaciones de ciberseguridad

Jesús Ángel Santos
Director de Infraestructura, Workplace y Seguridad en Grupo Masmóvil

Juan Miguel Velasco
CEO y Fundador de Aiuken Cybersecurity

Sinopsis: "Grupo MásMóvil seleccionó vía RFP el proyecto de tecnología de Aiuken Cybersecurity para la gestión de los SOCs del Grupo, que incluye: MásMóvil, PepePhone, Euskatel, R, Telecable, Levara, Yoigo, MásMóvil, Llamaya, Lycamobile y Virgin Telco. Este proyecto de más de seis meses ha ayudado a consolidar las operaciones, así como una mejora en la eficiencia de la ciberseguridad del Grupo. Todo ello sin afectar los sistemas productivos de la compañía ni la operativa de los clientes".

RENFE: El reto actual de la detección y respuesta en servicios esenciales

Francisco Lázaro
CISO y DPO de Renfe

Lorenzo Mateu
Director de Desarrollo de S2 Grupo

Óscar Navarro
Director del Área Industrial de S2 Grupo

Sinopsis: "La gestión de la seguridad en RENFE es un proceso muy maduro debido a la gran envergadura de sus infraestructuras y a la importancia de sus servicios para el funcionamiento normal de la sociedad. Desde hace más de dos décadas ha invertido mucho para el desarrollo e implementación de un modelo eficiente de gestión de la ciberseguridad, el cual incluye la segregación de funciones dentro de su organización de seguridad. Por sus manos han pasado numerosas tecnologías sobre las que ir construyendo este modelo de ciberseguridad y más recientemente ha apostado por implementar GLORIA como un punto fundamental de sus capacidades de Detección y Respuesta. Apuesta, así, por las capacidades que desde el CCN y S2 Grupo se han puesto a disposición del sector público. Así mismo, se está abordando un modelo propio de Ciberseguridad en el ámbito especifico Ferroviario, que incluye la puesta en operación dentro de ese ámbito de las capacidades de detección avanzada, incluso en el material rodante mediante el uso de sondas embarcadas para la monitorización, tanto del tráfico IT como del OT".

ABANCA: ¿Cómo sintetizar todos los datos sobre riesgo humano en un solo indicador que permita gobernar tu programa de concienciación?

Carlos Pérez Saldaña
CISO de Grupo Abanca

Javier Ruiz de Ojeda
Consultor GRC Senior en Áudea
Seguridad de Información

Sinopsis: "Los CISOs de las empresas se enfrentan al desafío desproporcionado de reclutar a todos los empleados de la compañía (pertenezcan o no a las áreas de seguridad o tecnología) 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 constantemente (contenidos formativos a la carta, campañas de comunicación, simulaciones de ataques, inteligencia artificial, etc.), 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. 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 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, o 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".

CAIXABANK: Bug Bounty y Red Team como medios necesarios para asegurar la ciberseguridad

Mario Maawad Marcos
Director de Innovación en Seguridad y Red Team de CaixaBank

Gonzalo Sánchez Delgado
Hacking Service Manager de Entelgy Innotec Security

Sinopsis: "Una mayoría creciente de organizaciones ya están familiarizadas con la ejecución de ciberejercicios de *red team*, y sin embargo todavía no han dado el salto a la ejecución de campañas de *bug bounty*. Durante la presentación se expondrá cómo los servicios de *Bug Bounty* y *Red Team* pueden ser potenciados conjuntamente para acelerar procesos y conseguir resultados exponenciales, despejando dudas o temores sobre servicios nuevos a través de experiencias de primera mano".

CAIXABANK: cómo proteger una plataforma de datos e IA corporativa: amenazas, controles y tecnología

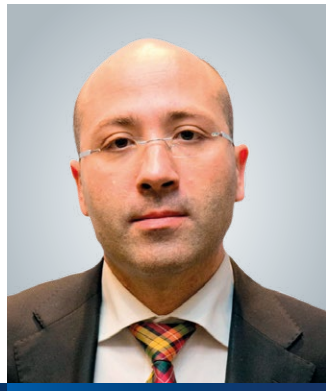
Jesús Muñoz Núñez
Director de CSIRT & Security Analytics de Digital Security en CaixaBank

José Carlos Cerezo
Head of EMEA South Security and Compliance Team de Google Cloud

Sinopsis: "CaixaBank y Google Cloud han anunciado un acuerdo estratégico para acelerar la transición de la entidad hacia el entorno *cloud* e impulsar la innovación en tecnologías de análisis de datos durante los próximos años. El acuerdo supone que CaixaBank hará uso de las capacidades de Google Cloud en los ámbitos de *cloud computing*, análisis de datos e inteligencia artificial (IA) para desarrollar nuevos servicios financieros y acelerar la transformación digital de la organización. Los servicios y arquitecturas desplegados en Google Cloud, en el alcance de este acuerdo, necesitan de los más estrictos controles de seguridad, que garanticen la protección y defensa contra amenazas, la privacidad y protección de los datos y la disponibilidad de los mismos. En esta sesión se especificará el objetivo del proyecto, los controles desarrollados y cómo se están aplicando".

MEDIASET: Ciberseguridad de calidad durante 30 años en buena compañía

Ramón Ortiz
Responsable de Seguridad de Mediaset



Óscar Riaño
Responsable del CERT de GMV

Sinopsis: "Mediaset es un grupo de comunicación con más de 30 años de existencia, que incluye filiales dedicadas a la televisión, distribución, venta y producción de contenidos, plataformas de emisión digitales, agencias de noticias, publicidad, etc. Durante estas tres décadas, Mediaset ha progresado en el desarrollo de sus capacidades de ciberseguridad, acorde a la naturaleza de su negocio, su expansión y los nuevos modelos digitales de prestación de servicios audiovisuales. Sin duda el mayor reto ha sido adaptar servicios tradicionales de ciberseguridad hacia entornos concretos y específicos necesarios para la entidad. En este sentido es importante contar con un compañero de viaje capaz de adaptarse a estas necesidades tan concretas, prestar servicios de calidad en varias líneas de actividad muy diferentes y aportar liderazgo y flexibilidad en un entorno tan complejo y cambiante como el que estamos viviendo".

SABADELL DIGITAL-BANCO SABADELL: Arrojando luz en zonas oscuras. Defensa contra amenazas avanzadas

Adolfo Hernández
CISO en Sabadell Digital y Director de Operaciones de Seguridad de Banco Sabadell

Nuria Andrés Pastor
Especialista en Soluciones de Ciberseguridad, Cumplimiento e Identidad para el Sector Financiero en Microsoft España

Sinopsis: "La defensa proactiva contra un panorama de amenazas cada vez más avanzado, así como un perímetro tecnológico corporativo más difuso y extendido día tras día, es una tarea compleja sin las capacidades adecuadas. La detección de anomalías, identificación de actividades maliciosas, contextualización en tiempo real sobre cajeros, servidores, *cloud*, puesto de trabajo o terminales móviles serían inabordables sin las soluciones adecuadas. Además, las capacidades de inteligencia artificial aplicadas en el ámbito de la ciberseguridad abren un interesante abanico a la automatización, industrialización y profesionalización en la defensa ante las ciberamenazas. Durante la ponencia se explicarán los principales hitos de la colaboración entre Microsoft y Banco Sabadell, los resultados obtenidos hasta la fecha y el *roadmap* a futuro".

PALLADIUM HOTEL GROUP: lecciones aprendidas en servicios de Detección y Respuesta a Incidentes

Francisco García Lázaro
Corporate Information Security Senior Director – CISO de Palladium Hotel Group

Rubén Gómez
Responsable de servicios de Detección y Respuesta a Incidentes y Responsable de Arquitectura de ciberseguridad de Fujitsu

Sinopsis: "Palladium Hotel Group es una entidad de referencia en el sector turístico nacional, sector cada vez más evolucionado digitalmente y, por tanto, las amenazas tecnológicas son consideradas una prioridad. Palladium ha abordado diferentes proyectos de ciberseguridad, entre los que se incluye la evolución de sus servicios SOC y sus servicios de Detección y Respuesta a Incidentes de Seguridad. Un proyecto para el cual Palladium ha contado con el equipo de ciberseguridad de Fujitsu. En la ponencia, se presentarán las principales lecciones aprendidas, factores claves de éxito, modelo de servicio y modelo tecnológico, así como los principales beneficios, tanto desde un punto de vista de ciberseguridad como para el negocio".

PROSEGUR: Redefiniendo la Ciberseguridad: Automatización Inteligente para una protección eficaz

Miguel Ángel Carretero
CISO Global de Prosegur Compañía de Seguridad

Carlos Fernández
Responsable Global de la división xMDR en Cipher

Sinopsis: "En el dinámico entorno cibernético de hoy en día, salvaguardar a las empresas de los adversarios digitales se ha convertido en una prioridad indiscutible. Sin un profundo entendimiento de las tácticas y estrategias empleadas por estos actores, las organizaciones se exponen al riesgo de sufrir ciberataques, lo que puede resultar en filtraciones de datos, pérdidas económicas y daño a la reputación. Conscientes de esta realidad, Prosegur con su *partner* Cipher aborda este desafío mediante una reevaluación integral de su estrategia de ciberseguridad".

GRIFOLS: Evolución de las capacidades de Ciberseguridad en buena compañía

Susana Calvo
Director Information Security Office de Grifols

Marcos Sánchez Martínez
Manager de Ciberseguridad en EY España

Sinopsis: "Debido al aumento exponencial de las ciberamenazas y la constante evolución de su complejidad, las empresas de cualquier sector tienen la necesidad de aumentar drásticamente sus capacidades en ciberseguridad. Sin embargo, las numerosas ofertas de soluciones tecnológicas y terceras partes que prometen ser la solución única a los retos de ciberseguridad actuales, pueden dificultar la toma de decisión de los responsables de seguridad de las compañías. Por eso, para evolucionar las capacidades de seguridad de manera eficiente, es imprescindible que las compañías cuenten con Partners en ciberseguridad que trabajen de manera integral en todas las capas de seguridad; desde el análisis de situación actual y definición de la estrategia de evolución tecnológica y organizativa de los servicios de seguridad de la compañía, hasta la propia ejecución de las operaciones de ciberseguridad en la compañía de manera coordinada con los equipos de operaciones de la compañía (IT y seguridad)".

>> Jorge Dávila

European Fashion Victims

Las sociedades se parecen mucho a los ciudadanos que las componen, por lo que tienen tendencias a presentar las mismas debilidades que éstos. Al igual que existen modas periódicas que mantienen en marcha el motor de la producción y del despilfarro a nivel de los ciudadanos de a pie, en las decisiones de los estados y estructuras supranacionales también pueden estar cautivadas por estériles modas. La Unión Europea no es ajena a esta debilidad y también sigue sus modas. Dado el impacto que este proceder tiene en nuestras economías y en nuestro deambular histórico, conviene que echemos un vistazo a cuáles son algunas de las "modas" –European Fashion Victims[1]– actualmente en este rincón el mundo.

El 9 de noviembre de 1989 la Democracia occidental comenzó su lento declinar, y todavía hoy continua en el mismo sentido. En esa fecha, cae el denominado Muro de Berlín[2] que se instaló el 13 de agosto de 1961 para separar la zona de la ciudad correspondiente a la República Federal de Alemania (RFA), Berlín Oeste, de la capital de la República Democrática Alemana (RDA), Berlín Este. Ese muro físico y administrativo fue el símbolo más conocido de la Guerra Fría y de la división de una Alemania vencida. Por una parte, lo llamaban "Muro de Protección Antifascista" (Antifaschistischer Schutzwall), mientras que los medios de comunicación y parte de la opinión pública occidental se referían a él como Muro de la Vergüenza (Schandmauer).

La idea de ese muro erigido por la RDA era impedir la migración masiva de ciudadanos del este hacia occidente. En aquellos años y hasta 1989 la Europa continental era importante porque en sus campos se desarrollaba una nueva guerra en la que no eran armas balísticas y explosivas lo que se utilizaban, sino conceptos y economías.

Por una parte, el bloque pro soviético se deshacía en elogios al sistema económico programado socialista y de lo bien tratados que estaban todos sus trabajadores. En esa utopía oriental (decía que) se había desterrado la desigualdad y a cada cual se le trataba según sus méritos y sus necesidades. Sin embargo, prácticamente todo venía marcado por el estado, único agente en esa sociedad de (supuestos) pares.

Por otra parte, teníamos a los ciudadanos occidentales liberados del nazismo, pero sometidos a un capitalismo económico que fomentaba las desigualdades y ensalzaba la plutocracia. Ambos bloques intentaban sublevar a los ciudadanos del otro bloque; los soviéticos intentaban sublevar a los obreros y ciudadanos oprimidos, y los de occidente hablaban de la Democracia y de la capacidad y posibilidad de cualquiera para elegir "libremente" su destino. Desde aquellos años la Democracia, entendida como la capacidad para organizar y desarrollar, (supuestas) elecciones colectivas del futuro por sufragio directo e igualitario, ha sido utilizada como emblema de Europa, y como arma arrojadiza (junto a la defensa de los derechos humanos) ante cualesquiera iniciativas totalitarias, de las que hay hoy en día existen muchas (Rusia, China, India, etc.).

Una Civilización Europea

En el crisol de esa batalla se fraguó la idea de lo que hoy llamamos Europa, aunque sus orígenes quizás realmente habría que buscarlos en el Imperio Romano y sus interacciones con los "bárbaros" del norte y del este de nuestro continente. Toda esa historia da lugar a lo que podría considerarse una Civilización Europea ahora basada más en "valores" morales, éticos y culturales que en la potencia económica o militar, propiamente dicha.

Caído el muro, pierden eficiencia los argumentos de la guerra fría, la organización social y económica soviética prácticamente nadie la defendería hoy en día, pero tampoco la **democracia** y la **sociedad de consumo** con la que se amilanó durante tiempo a los ciudadanos soviéticos. Cayó el muro de Berlín y Alemania se reunificó, la idea de una Unión Europea de países soberanos se siguió repitiendo tenazmente, pero desde hace cuatro décadas lo que está creciendo en el escenario de la antigua guerra fría es el autoritarismo y grupos claramente antidemocráticos[3].

Siguiendo el modelo de que las Civilizaciones nacen, crecen y mueren[4] en función de muchos factores organizativos y culturales pero, sobre todo, de factores económicos, ahora Europa debe encontrar cómo desarrollar peculiaridades que la hagan atractiva y poderosa si quiere seguir ocupando algún puesto en el teatro geoestratégico del planeta.

Dado que Europa son valores sociales y organizativos, y que es un mercado con bastante gente con un nivel de vida envidiable (y envidiado), no tiene fácil competir en escenarios basados en el trabajo barato y la abundancia de mano de obra. Tampoco tenemos una economía centrada en la guerra (eso sólo trae penuria a sus habitantes y riqueza a sus dirigentes) por lo que poco o nada podemos imponer los europeos a otros.

Los eWallets que cada estado miembro desarrolle tendrán en común ser contenedores digitales, probablemente cifrados, que guarden en su interior los documentos públicos que constituyen los certificados digitales de atributos. Su uso, es decir, la extracción e inclusión de documentos en ellos, requerirán algún tipo de autenticación segura por parte del usuario y ¿cómo se va a conseguir eso?

La Unión Europea se encuentra en una encrucijada esencial, en la que todos, muy nerviosos, intuyen que, si no se hace algo y no se hace bien, en unas cuantas generaciones nadie se acordará de lo que hoy es nuestro día a día.

En esa encrucijada las instituciones europeas parecen haber optado por la generación de "valor añadido" y hacer que haya que contar con Europa para la producción y por un desarrollo de servicios valiosos para futuros y presentes ciudadanos/consumidores exigentes.

Lo que ocurre es que esa decisión no sé si está suficientemente madurada puesto

[1] Ver https://es.wikipedia.org/wiki/Fashion_victim
[2] Ver https://en.wikipedia.org/wiki/Berlin_Wall
[3] Ver https://es.wikipedia.org/wiki/Extrema_derecha
[4] Ver https://es.wikipedia.org/wiki/Estudio_de_la_Historia_(Arnold_J._Toynbee)

que su resultado más directo ha sido lanzar a Europa a indagar (como pollo sin cabeza) en todas las direcciones "de moda", a ver si pueden desarrollar capacidades de suficiente valor añadido como para justificar que el mundo siga contando con ella en las próximas décadas.

Aunque son varias las modas posibles, querría centrarme en solo dos. Por una parte, está el Problema esencial y todavía no resuelto, de los sistemas digitales actuales que es el de la **Identidad Digital**, y sus parientes cercanos que son la **Autenticación** y la **Autorización**. Por otra parte, está el pánico que se está intentando establecer sobre la inseguridad de los sistemas criptográficos actuales frente a la muy cacareada **Amenaza Cuántica**.

En el primer caso tenemos al Reglamento Europeo eIDAS2, y por otra, las recomendaciones de la Comisión Europea para desarrollar escenarios a prueba de ataques "cuánticos".

Segundas partes eIDAS

El 23 de julio de 2014 el Parlamento Europeo y el Consejo de la Unión Europea aprobaron la entrada en vigor del reglamento eIDAS (*electronic IDentification, Authentication and trust Services*), relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en Europa.

Además de definir los distintos tipos de firma electrónica, eIDAS regula también los servicios de: Sellado y marcado de tiempo, correo electrónico certificado, creación, verificación y validación de certificados para la autenticación de sitios web, documentos electrónicos, así como cuales deben ser los mecanismos de identificación y autenticación, sus distintos niveles y su interoperabilidad entre los estados miembros.

En 2021, aparece eIDAS2 que es la segunda versión del reglamento de Identificación Electrónica, Autenticación y Servicios de Confianza, cuyo objetivo es, una vez más, promover interacciones digitales seguras dentro y entre los estados miembros de la UE.

eIDAS proporciona cobertura legal para prestar servicios de confianza, implementar servicios de identificación, certificados digitales y firma electrónica, además de permitir la identificación remota por vídeo para aquellos casos en los que haga falta una verificación presencial de la identidad de las personas. Esencialmente, el eIDAS establecía un marco necesario para habilitar servicios de identificación y firma electrónica **reconocidos de forma mutua en los distintos estados miembros desde septiembre de 2018**.

Sin embargo, tan solo 14 países miembros han notificado al menos un sistema de identidad electrónica y **sólo un 59% de los residentes en la UE** tienen acceso a sistemas transfronterizos de identidad electrónica, lo que implica una escasa implantación en el sector público.

eIDAS2 es una nueva propuesta publicada el 3 de junio de 2021 que supone una evolución de eIDAS para atender las carencias identificadas, así como a su baja implantación en el sector público. eIDAS2 tienen como objetivo que de aquí al año 2030, su adopción llegue a un 80% de ciudadanos.

Sin embargo, eIDAS no cubre la provisión de **atributos electrónicos**, como certificados médicos o cualificaciones profesionales, dificultando el reconocimiento legal en Europa de estas credenciales. Además, tampoco permite el control por parte de los usuarios de los datos que se intercambian en los procesos de verificación.

Los eWallets no aportan ningún control duradero del titular a la distribución de sus datos. Una vez entregado el certificado de atributos, este documento digital auto-contenido, puede ser transmitido a terceros, acumulado en nuevas bases de datos, etc., y todo ello sin control real alguno por parte del titular. eIDAS tampoco permite el control por parte de los usuarios de los datos que se intercambian en los procesos de verificación.

Propuestas de eIDAS2

Por eso eIDAS2 propone la creación de una **identidad digital europea** "controlada" por los ciudadanos a través de una cartera o *wallet* de identidad digital (EDIW, **European Digital Identity Wallets**) y que pueda ser leída por cualquiera para verificar la identidad de los ciudadanos.

eIDAS2 amplía la lista de servicios de confianza incluyendo los **servicios de archivo electrónico**, los **libros mayores electrónicos**, la **gestión remota de dispositivos de firma electrónica** y la creación de **sellos electrónicos**.

Con eIDAS2 se facilitaría los procesos de verificación en cualquier circunstancia simplemente implantando la tecnología que lee el e-ID de los ciudadanos a través de sus eWallets. El uso de estos eWallets permitirá que sus titulares **se puedan identificar con su teléfono móvil** en **procesos *online* y presenciales** (*offline*) en su acceso a cualesquiera servicios.

Con la posesión y gestión de su eWallet, su titular podrá disponer de la información administrativa y datos de ciudadanos que estén en cualquier organismo público o privado, consultar expedientes, perfiles sanitarios, información fiscal, bancaria, universitaria, o de cualquier otro tipo. Así, por ejemplo, con su eWallet, el ciudadano podría abrir una cuenta bancaria en cualquier estado miembro de la UE, podría acceder a su perfil sanitario a través de la identidad digital europea, podría alquilar un vehículo o cualquier servicio mediante su e-ID, podría compartir datos financieros entre bancos de distintos estados miembros (ingresos, calificación crediticia, etc.).

La cartera de identidad digital de la UE

En eIDAS2 se define la **cartera de identidad digital de la unión europea** (IDUE) como: "*un producto y servicio que permite al usuario almacenar datos de identidad, credenciales y atributos vinculados a su identidad, con el fin de proporcionarlos a las partes informadas a petición de estas y de utilizarlos con fines de autenticación, en línea y fuera de línea, para un servicio de conformidad con lo dispuesto en el artículo 6 bis, así como para crear firmas y sellos electrónicos cualificados*".

En concreto el artículo 6.3 de la propuesta eIDAS 2 establece:

Las carteras de identidad digital europea permitirán al usuario:

a) solicitar y obtener, almacenar, seleccionar, combinar y compartir de forma segura, transparente y rastreable por el usuario, los datos de identificación de persona jurídica y la declaración electrónica de atributos que sean necesarios para autenticarse en línea y fuera de línea con el fin de acceder a servicios públicos y privados en línea;

b) firmar por medio de firmas electrónicas cualificadas.

Según esto, un ciudadano europeo podría llevar en el móvil y compartir de manera segura documentos como el DNI, el carnet de conducir, un título académico, la tarjeta sanitaria, recetas electrónicas, el carnet profesional, certificados bancarios, historiales médicos, entre otros.

La UE propone que cada estado miembro emita una cartera digital personal que permita a los ciudadanos almacenar y gestionar los datos de identidad y los **testimo-**

nios electrónicos de atributos de forma segura en sus dispositivos.

Un concepto clave en estos eWallets son los "atributos" que serían determinadas informaciones acerca de una persona. Por ejemplo, la fecha de nacimiento, las licencias profesionales o el expediente académico, credenciales societarias, etc. Estos atributos se autenticarán mediante una declaración electrónica certificada de atributos (testimonios), emitidas por cualquier entidad que tenga potestad para establecer lo testimoniado como una Universidad o un **Prestador Cualificado de Servicios de Testimonios** asociado a ella.

Con su eWallet el usuario podrá autenticarse e identificarse, almacenar e intercambiar informaciones administrativas como, por ejemplo, su nombre, apellidos, fecha de nacimiento, nacionalidad, derecho a residir, trabajar o estudiar en un determinado estado miembro, o incluso sus cualificaciones profesionales, historial de empleo o su solvencia crediticia.

Con este nuevo enfoque, la divulgación de los datos de identidad podría ser selectiva. Del mismo modo que las tarjetas bancarias se utilizan hoy en día para autorizar los pagos, las carteras digitales europeas **autorizarán la divulgación de información de confianza** sobre los usuarios a ciertas partes informadas, **bajo el efímero "control" del titular**.

Los usuarios de esas carteras llevarán en sus móviles una *app* que incorporará los datos electrónicos de identidad que ellos decidan y podrán utilizarlos en cualquier país de la Unión Europea. Una característica que también hay que tener en cuenta es que el eIDAS2 pretende incluir en el uso de ese eWallet la **gestión/autorización del usuario en el tratamiento de sus datos personales**. Se pretende que los usuarios puedan **limitar formalmente** la entrega de testimonios de atributos de identidad a los que sean estrictamente necesarios para recibir un servicio y, de algún modo, **que se pueda retirar el consentimiento para el tratamiento de datos**.

La idea es que el reglamento eIDAS2 se apruebe antes de las siguientes elecciones al Parlamento Europeo que están previstas para mayo/junio de 2024. Los estados miembros de la Unión Europea tendrían desde entonces, si no hay modificaciones sobre el texto inicial, menos de tres años para lanzar una cartera de identidad digital para sus ciudadanos.

El 1 de febrero de este año, la Comisión Europea hizo pública la primera "EU Toolbox[5] for the European Digital Identity Wallet (EUDI Wallet)", un proyecto clave desarrollado entre varios estados miembros. En línea con esta iniciativa, la Comisión también está desarrollando programas concretos en áreas de alta prioridad como son los carnets de conducir, los historiales médicos digitales, los pagos, y las cualificaciones profesionales.

Aunque todo este esfuerzo es encomiable dentro de la necesaria transformación de la Unión Europea en algo más que un mercado común de capitales, bienes y fuerza laboral, está por ver a dónde llega. Para empezar, ya estamos en la versión dos del eIDAS de hace ya bastantes años y una parte de su contenido es enmendar algunas ausencias de la versión inicial.

¿Y los análisis de seguridad de la propuesta?

Ahora bien, en la documentación europea consultada se echan en falta los análisis de seguridad de la propuesta. Por ejemplo, ¿qué pasa si un usuario pierde o le roban el móvil donde tiene instalado su eWallet electrónico? ¿Cuántas copias habrá de cada eWallet y dónde estarán guardadas, quién tendrá acceso a ellas?

Los eWallets que cada estado miembro desarrolle tendrán en común ser contenedores digitales, probablemente cifrados, que guarden en su interior los documentos públicos que constituyen los certificados digitales de atributos. El uso de esos contenedores, es decir, la extracción e inclusión de documentos en ellos, requerirán algún tipo de autenticación segura por parte del usuario (que sólo debería ser el titular) y ¿cómo se va a conseguir eso?

Los eWallets no son nada diferente a cualesquiera contenedores cifrados que ya hay en el escenario digital avanzado y, como ellos, tienen el mismo problema esencial: **la autenticación cierta y única del titular legítimo** de los mismos.

Otro frente que dejar en claro cuanto antes es que los eWallets no aportan ningún control duradero del titular a la distribución de sus datos. Una vez entregado el certificado de atributos, éste documento digital auto-contenido, puede ser transmitido a terceros, acumulado en nuevas bases de datos, etc., y todo ello sin control real alguno por parte del titular. Lo del consentimiento en la gestión de datos personales sigue siendo una norma sin posibilidad de exigir realmente su estricto cumplimiento. Los eWallets no tienen nada que ver con las quimeras de las Identidades Auto-Soberanas, aunque algunas veces puedan sonar parecidas.

Lo que sí hay que reconocerle a esta nueva **faltriquera digital** de la Unión Europea, es que podría/debería cambiar el modo de almacenar los datos de los ciudadanos y de los estados. Si cada uno de los titulares tuviera en exclusiva los documentos de atributos que le corresponden, **no existirían y podrían estar prohibidas las bases de datos centralizadas**. En ese caso, los ciudadanos podrían "desaparecer", voluntaria o involuntariamente, sin dejar el más mínino rastro y eso es malo, al menos para las necesidades historiográficas de cualquier sociedad avanzada.

Hay que reconocerle a esta nueva faltriquera digital de la UE que podría/debería cambiar el modo de almacenar los datos de los ciudadanos y de los estados. Si cada uno de los titulares tuviera en exclusiva los documentos de atributos que le corresponden, no existirían y podrían estar prohibidas las bases de datos centralizadas.

Por lo anterior, no es razonable pensar en que las únicas copias de los certificados de atributos fueran a estar en exclusiva en los eWallets de sus titulares; al menos existirán también, en bases de datos controladas por las fuentes que generan dichos atributos y con ello, una autoridad suficientemente elevada **podría reconstruir cualquier eWallet previamente generado** sin colaboración ni permiso de su titular.

En cualquier caso, la misma existencia de documentos digitales auto-contenidos, verificables por cualquiera, hace que, su uso, su presentación frente a quien así lo requiera, **suponga una inevitable fuga de información** y una posibilidad de reconstruir sin posible control grandes bases de datos sin el más mínimo consentimiento del titular.

Aunque las propuestas de los eWallets realmente hiciesen lo que prometen/insinúan, deberían estudiarse sus efectos en manos de una sociedad de **1) inadaptados tecnológicos** (por edad o por formación) y de **2) narcisistas despreocupados** del rastro digital que genera su frenética existencia en redes sociales y demás abrevaderos de moda; sobre todo porque, en conjunto, constituyen la mayoría de nuestras sociedades.

[5] Ver https://digital-strategy.ec.europa.eu/en/news/european-digital-identity-wallets-commission-publishes-first-technical-toolbox-towards-prototypes y https://ec.europa.eu/newsroom/dae/redirection/document/93678

Amenaza Cuántica

Todos los documentos y noticias relacionadas con la computación cuántica y su impacto sobre los sistemas de seguridad actuales deben analizarse con cuidado, no vaya a ser que seamos víctimas de algún engaño. En todos los casos que me vienen a la memoria[7], todos los discursos parten de axiomas que aceptan, **como acto de fe y sin el más mínimo rubor**, que la Computación Cuántica ya está aquí y que en cuestión de pocos años que los actuales Criptosistemas Asimétricos dejaran inexorablemente de ser aceptablemente seguros.

A la luz de esa "*verdad revelada*" (¿por quién, a quién y en beneficio efectivo de quién?) se lanzan **1)** campañas de renovación de los **criptosistemas asimétricos** con **algoritmos completamente nuevos, inmaduros** y **no suficientemente probados**, y **2)** la inminencia de la amenaza diciendo que "*los malos*" (¿quiénes serán realmente? ¿qué pruebas hay de ello?) ya están guardando información cifrada "*para poderla descifrar cuando tengan disponibles ordenadores cuánticos*" como quien tiene PCs, tabletas o GPUs a su capricho.

Estos razonamientos, me recuerdan al **Melanocetus johnsonii**[8] (Diablo Negro), pez abisal que muestra a la víctima una lucecita (bioluminiscencia) que aterroriza o atrae al pececillo y le invita a huir en la dirección contraria que es, precisamente, donde le espera el depredador con su enorme boca seguida de sus sistema digestivo.

En nuestro escenario no creo que en la dirección marcada por la Amenaza Cuántica esté ningún depredador dispuesto a digerirnos, pero sí veo **legiones de pescadores que se benefician de aguas tan revueltas**. Al final, ya no es que los centenares de millones que gasta la Unión Europea en estos temas terminen siendo simplemente "*beneficio de pescadores*" (no necesariamente europeos, ni generadores de ninguna tecnología revolucionaria), sino que esas **pérdidas evitables 1)** nos lastran en lo de encontrar de un puesto avanzado para Europa en la geopolítica del futuro planeta y, evidentemente, **2) no resuelven el problema de que las tecnologías de seguridad actuales no son eternamente infalibles** y requieren de un natural y continuo mantenimiento como cualquier otro ejemplo del ingenio humano.

Hoy en día no pueden considerarse seguras longitudes de claves que sí lo eran hace 30 años, ni las actuales longitudes de claves pueden considerarse eternamente seguras, por lo que el miedo a que dentro de cierto tiempo sí tendrán tus enemigos capacidad para entender lo que ahora cifras, **es algo que siempre ha estado ahí** y que no es patrimonio de ninguna Amenaza Cuántica.

Recordemos que ya en 1949 el irrepetible Claude Shannon[9] demostró[10] que los algoritmos conocidos hasta entonces eran "*rompibles*" todos, excepto uno. Ese autor nunca publicó –porque no lo sabía– cómo podían romperse efectivamente, pero sí estableció, sin lugar a dudas, que algún día podrían romperse. A pesar de haber reducido el arsenal criptográfico a un solo algoritmo seguro, el cifrado de Vernam[11] u OTP[12], el mundo siguió adelante adaptando las seguridades efectivas de los distintos algoritmos a las capacidades de sus contrincantes y teniendo en cuenta la variable tiempo; lo que hoy es imposible, mañana podrá ser difícil, pero acabaremos viendo que es muy fácil.

Si llegan los ordenadores cuánticos algún día, veremos **1)** si realmente son una amenaza, y **2)** alargaremos las longitudes de las claves para que sean inservibles (los Quantum Computers) durante cierto tiempo. El secreto eterno existe, pero no de la manera que algunos piensan. **El secreto eterno existe siempre que sea irreversible**.

No hay ningún proceso documentado cuyo secreto pueda considerarse eterno mientras existan los contenidos de esos documentos o registros (incluso si en su momento fueron cifrados). La única posibilidad de que algo permanezca en secreto eternamente es que no quede de ese algo nada escrito, ningún registro, ningún testigo, ningún recuerdo. En la historia de la humanidad hay innumerables hechos que permanecen secretos y que siempre lo estarán, y todos ellos tienen en común que de ellos no hay el mas mínimo registro, documento, o testigo.

La Amenaza Cuántica no resulta ser una amenaza tan amenazante como algunos están interesados en hacernos creer, y dedicarle excesiva atención (peor aún si es en exclusiva) **no va a ayudar a Europa en su búsqueda de un lugar bajo el futuro sol**. Sin embargo, sí le puede hacer perder un montón de recursos, tiempo y oportunidades alternativas no identificadas.

Conclusiones

La psicología de las sociedades no es muy diferente de la de sus individuos, por lo que en las decisiones gubernamentales (nacionales o supranacionales) no es raro ver componentes fácilmente identificables en el comportamiento de cualquiera. Por ello, es razonable esperar que también haya modas en el comportamiento de los estados. Lo que no es tan fácil de aceptar es que, además, no haya una componente racional en lo que estos entes supra-ciudadanos hacen o persiguen. Lo que pasa es que la racionalidad no es única, sino que depende del modelo lógico en el que se basa, por lo que es razonable en uno puede no serlo en otro.

El secreto eterno existe siempre que sea irreversible. No hay ningún proceso documentado cuyo secreto pueda considerarse eterno mientras existan los contenidos de esos documentos o registros (incluso si en su momento fueron cifrados).

Teniendo en cuenta que estamos viviendo en el modelo lógico del máximo beneficio para el capital, muy bien pueden tener éxito medidas tomadas a la sombra de modas[13] caprichosas y sin justificación objetiva comprobable pero, aun así, no por ello van a ser una estrategia inteligente pensando en el medio o largo plazo.

En nuestra realidad sigue pendiente **el problema de la autenticación robusta y segura** de individuos físicos y jurídicos y los eWallet no van a arreglar este problema, pero sí van a abrir la posibilidad de que los europeos nos involucremos algo más en la custodia y circulación de nuestros datos personales, ¡Algo es algo y con ello *Europe would be different*!

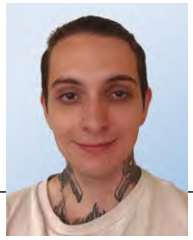
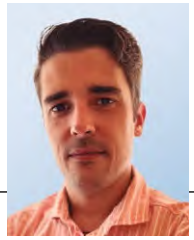
Lo que sí está claro es que el tinglado de la Europa actual no está como para poder caer en despilfarros tan engorrosos como los asociados con nuevas versiones cuánticas del tradicional cuento de "Pedro y el lobo", y no terminar pagándolo con futuras irrelevancias a medio y largo plazo. ■

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

[6] Ver https://dle.rae.es/faltriquera
[7] Ver, por ejemplo, https://www.epc.eu/content/PDF/2023/Cybersecurity_DP.pdf
[8] Ver https://en.wikipedia.org/wiki/Humpback_anglerfish
[9] Ver https://en.wikipedia.org/wiki/Claude_Shannon
[10] Ver https://en.wikipedia.org/wiki/Communication_Theory_of_Secrecy_Systems
[11] Ver https://en.wikipedia.org/wiki/Gilbert_Vernam
[12] Ver https://en.wikipedia.org/wiki/One-time_pad
[13] Ver https://dle.rae.es/moda

Profundizando en DevSecOps

Puede que se entienda como infraestructura orientada a DevOps un diseño que cuenta con escalado, alta disponibilidad, y automatización. Pero nos quedaríamos cortos, puesto que la infraestructura orientada a DevOps es mucho más que eso, es una forma de pensar, de diseñar, de implementar, y de mantener. El núcleo de este "mindset" es la eficiencia mediante automatización o el uso de herramientas/plataformas sin comprometer en ningún momento la seguridad. Para el ejemplo seleccionado de infraestructura en *cloud* del presente artículo, los autores tratarán principalmente la Disponibilidad, asociándola además a la escalabilidad y reducción de costes. Para reflejar esto se exponen dos ejemplos de infraestructura. Ambas tienen un diseño orientado a DevSecOps sobre AWS pero una de ellas falla en algunos puntos claves que pueden afectar al proyecto a largo plazo.


Adrián Sanz / Alejandro Pérez / Javier Blanco

Si tuviéramos que definir Atalanta, nos posicionaríamos como empresa "boutique", donde buscamos ofrecer a nuestros clientes, un servicio personalizado y de alto valor. Esto es gracias al equipo humano y de profesionales que la componen, así como de las herramientas y soluciones que utilizamos, teniendo capacidades en diversas áreas como consultoría estratégica, Formación, Blue & Red Team, así como en DevSecOps, que es en lo que nos centraremos desde Evoltrue, marca con la que operamos este tipo de proyectos.

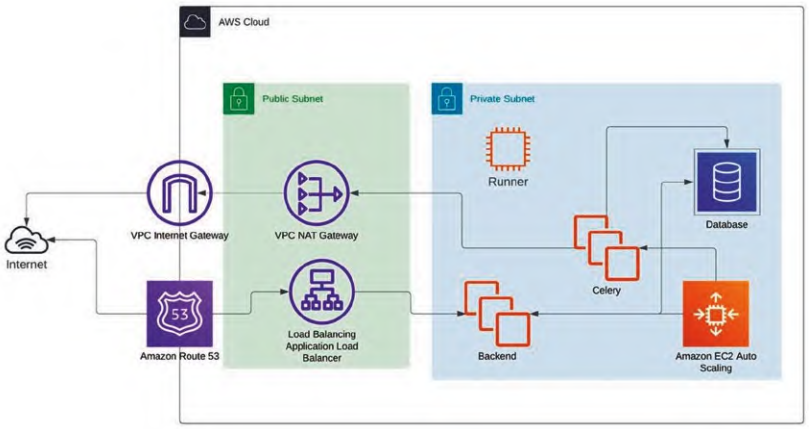
Siempre que escuchamos o leemos sobre DevSecOps nos hablan de Análisis de Código Estático (SAST), Análisis de Código Dinámico (DAST) y Análisis de la Composición del Software (SCA) para librerías de terceros. Si bien son partes importantes, componen una mínima parte del ciclo de desarrollo seguro.

Es fácil de entender que cuando se produce un fallo de seguridad o vulnerabilidad en nuestro ciclo de desarrollo, el coste es exponencialmente mayor de resolver cuanto más avanzada es la capa del ciclo de desarrollo en la que se produce o detecta este fallo.

Omitiendo la primera capa del ciclo, la de Planificación y la importancia de disponer, por ejemplo, de un completo y realista Modelado de Amenazas para evitar una alta criticidad en aquellas vulnerabilidades que detectemos en el día a día, existe una parte fundamental a tener en cuenta que, en casos de un diseño incorrecto, nos puede generar grandes pérdidas, la infraestructura, y es sobre esta parte de la que vamos a hablar en este artículo.

Seguramente al leer que vamos a tratar el tema de infraestructura se nos ha venido a la cabeza la Infraestructura como Código (IaC) y el uso de contenedores porque pueden ser seguros…, pues en realidad no. Una infraestructura no sólo se compone de contenedores y estos no tienen por qué ser seguros. Son muchos casos en los que vemos en clientes situaciones como el Docker Compose expuesto o aplicaciones vulnerables que nos permiten pivotar o saltar al host anfitrión desde el propio contenedor.

Son muchos los temas al tratar la seguridad en la infraestructura en un ciclo DevSecOps, como protección de las llaves de repositorios, procedimientos de revisión de subida de *releases*, etc., (y nos dilataríamos mucho en este artículo), y aún así el riesgo de un ataque dirigido siempre está presente incluso en empresas con alta seguridad como pudimos ver con casos como el ataque que sufrió SolarWinds en su cadena de suministro.



Al mirar la seguridad siempre debemos tener al menos tres conceptos base sobre los que priorizar, no siendo los únicos. Estos conceptos base son los indicados por CIA, es decir, Confidencialidad, Integridad y Disponibilidad. Para el ejemplo seleccionado de infraestructura en *cloud* del artículo, trataremos principalmente la Disponibilidad, asociándola además a la escalabilidad y reducción de costes.

Partiendo de la imposibilidad de conocer el crecimiento y necesidades reales de cara a un futuro a medio-largo plazo de nuestras aplicaciones, es importante partir de una alternativa que nos permita, de forma sencilla, disponer de una escalabilidad sin límites. Por eso partiremos de una infraestructura en *cloud* frente a la tradicional *on premise*, y concretamente para este ejemplo nos decantamos por AWS (Amazon), siendo aplicable este ejemplo a otras nubes existentes.

Puede que se entienda como infraestructura orientada a DevOps, un diseño que cuenta con escalado, alta disponibilidad, y automatización. Pero nos quedaríamos cortos, puesto que la infraestructura orientada a DevOps es mucho más que eso, es una forma de pensar, de diseñar, de implementar y de mantener. El *core* de este "mindset" es la eficiencia mediante automatización o el uso de herramientas/plataformas, sin comprometer en ningún momento la seguridad.

Para reflejar esto vamos a ver dos ejemplos de infraestructura. Ambas tienen un diseño orientado a DevSecOps sobre AWS pero una de ellas falla en algunos puntos claves que pueden afectar al proyecto a largo plazo.

***Nota 1**: Nos centraremos únicamente en un entorno y solo en la infraestructura necesaria para la aplicación. Se excluyen ciertos elementos fuera del alcance del artículo.*

LightersInfo

Esta empresa cuenta con una API REST a la que se conectan diferentes comercios de terceros para obtener información sobre el precio de los encendedores. La empresa solo ofrece la API.

El proyecto está escrito en Django, parte de él se conecta a diferentes fuentes mediante tareas asíncronas usando Celery, actualizando la información en una base de datos PostgreSQL, esta información es la que se sirve a los comercios.

La creación de infraestructura está automatizada mediante *pipelines* con Terraform sobre AWS, la aplicación se despliega sobre las máquinas que se encuentran actualmente levantadas, y se reinicia el servicio tras el despliegue mediante Ansible.

El despliegue de la infraestructura y la aplicación se realiza desde el mismo *runner.* Los servidores se encuentran distribuidos en 1 zona de disponibilidad, y se autoescalan en función de la carga de CPU.

Para 'securizar' el código de Terraform, usan Terrascan en cada despliegue, adicionalmente cuentan con herramientas como Prometheus + Grafana + Alert Manager para monitorizar diferentes KPIs (versión de código desplegada, estado del servicio, estado de DB, métricas de hardware, conexiones *in/out*) y cuentan con *prom-executor* para reaccionar activamente a algunas de las métricas. Un ejemplo real, es un *script* que se lanzaba cuando una query tardaba cinco minutos, este *script* enviaba por correo a ciertos *developers* la pila del proceso que lanzó la *query*.

***Nota 2**: Las máquinas auto-escaladas cuentan con un CloudInit para actualizarse el código a la versión correspondiente antes de iniciar el servicio.*

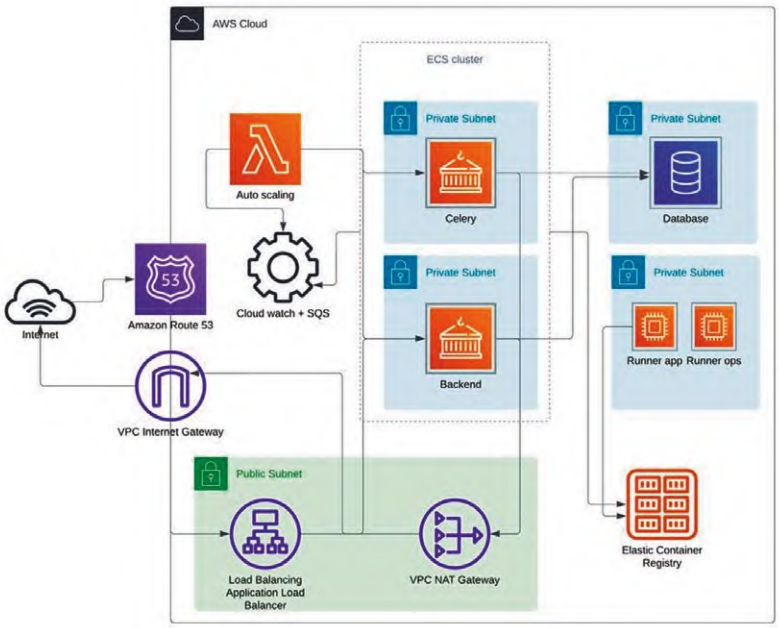
Lighsters & CO

Esta empresa usa el mismo modelo de aplicación, pero con una infraestructura diferente.

Optan por un *cluster* ECS + Fargate (contenedores *serverless*) en AWS, la carga se balancea mediante un ALB (*Application Load Balancer*), y se auto-escala en función de dos métricas en Cloudwatch, CPU y memoria (el escalado se realiza mediante una función lambda. Como alternativa se puede usar el escalado integrado para un menor mantenimiento, pero con este sistema tenemos el control completo del escalado)

El despliegue se realiza mediante *pipelines* y contamos con dos *runners*, uno para el despliegue de la infraestructura con Terraform, y otro para el despliegue de la aplicación, con un conjunto de *docker* (construye la imagen con el código y la sube) + terraform (despliega la nueva versión de la imagen). Cómo último detalle, la base de datos se mantiene igual.

Para 'securizar' el código usan Terrascan y para asegurarse de no sobrepasar costes usan Infracost, además usan la funcionalidad *built-in* de escaneo de vulnerabilidades de ECR para evitar desplegar imágenes con vulnerabilidades críticas o que puedan afectar a la aplicación. Finalmente cuentan con Ivre, un *shodan self-hosted* para escanear la infraestructura de forma interna/externa de forma continua, y para monitorizar ciertos KPIs, usan prometheus + grafana + loki + alert-manager + cloudwatch exporter



Comparativa

A pesar de las diferencias, ambos modelos son viables, pero el primero tendrá una serie de problemas a cambio de la simplicidad del mismo. El precio, la disponibilidad, y la escalabilidad.

El coste es superior en el primer ejemplo por el simple hecho de usar EC2. Es menos eficiente que ECS + Fargate. Esto mismo es lo que causa que la escalabilidad sea peor en el primer ejemplo. En el segundo podemos escalar de forma más eficiente, y con un coste menor, la disponibilidad se ve afectada en cada despliegue del primer ejemplo, por cómo se despliega (reiniciando el servicio de las máquinas existentes), en el segundo, usando *rolling-updates* para actualizar la imagen que usamos en el cluster, no hay *downtime*. Finalmente, a nivel de seguridad, ambos usan Terrascan pero el segundo ejemplo cuenta con escaneo de vulnerabilidades en ECR y un sistema de monitorización más refinado con Ivre para escanear continuamente la red tanto interna como externa

Por último, en relación con el control de accesos, se usa IAM + Security Groups en ambos ejemplos.

Después de esta explicación sobre despliegue y arquitectura en DevSecOps, vale la pena mencionar y resaltar qué, hoy en día, se hacen imprescindibles las herramientas de DevSecOps con escáneres SAST, DAST y SCA (entre otros). Si bien cada día las aplicaciones utilizan más tecnologías y son más complejas, las técnicas de piratería lo son por igual. Dicho esto, herramientas de mercado son esenciales en toda la fase de desarrollo y a tener en cuenta por los equipos de DevOps a la hora de eliminar vulnerabilidades en el código, y desde Atalanta recomendamos su uso.

Los escáneres SAST, bien utilizados y filtrados, resulta extremadamente útiles de cara a evaluar el código, ver vulnerabilidades, seguimiento de vectores de ataque y mejora en los equipos de desarrollo. Además, es interesante citar documentaciones como las de OWASP a la hora de hacer desarrollo seguro.

Los SCA aportarán una visión de cara a cómo estamos de actualizados con aplicaciones de terceros y, cómo estas pueden estar vulneradas según qué versión estemos utilizando. Debemos de tener en cuenta cuáles se usarán en pre y cuáles no y, ver la viabilidad en caso de tener que actualizar a versiones más seguras.

Los DAST darán color y estilo como si fuera css con html a nuestra auditoría. Son necesarios para ver los flujos de nuestra *app*, como se comporta y cuán seguros son los *endpoints*. Si hemos hecho un buen trabajo en QA tendremos mucha precisión a la hora de saber que *inputs* 'sanitizar', si estamos filtrando información sensible o si se puede dar mal uso a Jason Web Tokens de otros usuarios. ■

Adrián Sanz
Senior DevSecOps Engineer
adrian.sanz@atalantago.com

Alejandro Pérez
DevSecOps Engineer
alejandro.perez@atalantago.com

Javier Blanco
Director de servicios Red Team, DevSecOps y Formación
javier.blanco@atalantago.com

ATALANTA

CISCO: Resiliencia para un futuro híbrido y multi-cloud

Cisco ha refinado y enriquecido su potente y adaptativa plataforma Cisco Security Cloud en la que ofrece múltiples soluciones de ciberseguridad que permiten a clientes proteger a sus usuarios, dispositivos, aplicaciones y datos en entornos multi-nube, aportando una mejor y más rápida detección y respuesta frente a amenazas y unificando así mismo la gestión de políticas. Al tiempo, la multinacional americana ha incorporado en Cisco security Cloud las primeras capacidades de IA generativa: el Asistente de Políticas y el Asistente SOC.

Ángel Ortiz Álvarez

La forma en la que interactuamos con la tecnología nunca ha sido tan diversa, dinámica y distribuida. Hoy día, contamos con conectividad continua a internet y podemos acceder a aplicaciones y datos distribuidos a lo largo de las diferentes nubes desde cualquier dispositivo y lugar.

Ahora bien, la conectividad continua también ha traído consigo un cambio fundamental en las arquitecturas tecnológicas. En la actualidad, el 82% de los responsables de TI de todo el mundo han adoptado arquitecturas de nube híbrida, y el 58% de las organizaciones utilizan entre dos y tres nubes públicas de Infraestructura como Servicio (IaaS). Además, el 95% del tráfico web está cifrado, lo que limita la visibilidad. Las aplicaciones, en definitiva, se alojan en todas partes. Y ya no podemos hablar de un perímetro de seguridad que proteger, como hacíamos hace tan solo 10 años.

La ciberseguridad, por tanto, nunca ha sido tan importante. Pero debe estar alineada con este nuevo entorno si queremos evitar que los atacantes continúen aprovechándose de las vulnerabilidades existentes y esquivando los actuales controles mediante el empleo de técnicas cada vez más complejas y avanzadas, en un número, además, cada vez mayor.

Sin embargo, nos encontramos con que, a menudo, las organizaciones intentan resolver estos retos añadiendo más controles de seguridad con nuevos proveedores, dando lugar a una combinación de soluciones dispares con su consiguiente complejidad e ineficiencia operativa. La realidad es que, aunque haya arquitecturas que puedan soportar cierto nivel de escalado y expansión, la mayoría de ellas, eventualmente, requerirá una re-arquitectura más holística. Es aquí donde entra en juego la plataforma Cisco Security Cloud.

Hacia la 'nube' de seguridad

Hace algo más de un año, Cisco anunció su intención de desarrollar su **plataforma Cisco Security Cloud**. Por aquel entonces, era nuestra visión estratégica para esa plataforma integrada, global, impulsada por inteligencia artificial y entregada en la nube.

Hoy día, Cisco Security Cloud es ya una realidad tangible desde la que ofrecemos múltiples soluciones de seguridad que permiten a nuestros clientes proteger a sus usuarios, dispositivos, aplicaciones y datos en entornos multi-cloud; aportando una mejor y más rápida detección y respuesta frente a amenazas y unificando así mismo la gestión de políticas (figura 1).

Vamos a repasar a continuación las últimas soluciones, ofrecidas desde la Cisco Security Cloud, cuyo lanzamiento hemos anunciado en los últimos meses.

Cisco XDR (eXtended Detection & Remediation)

La sofisticación de los ataques hace que cada vez sean más difíciles de detectar analizando las contramedidas de seguridad individuales. Por ejemplo, hoy día cuando recibimos un correo electrónico de *phishing* selectivo, parece que el mismo proviene de alguien a quien conocemos y que sabe datos sobre nosotros (como nuestro jefe o un familiar), especialmente en la era de la IA y ChatGPT. Es decir, la relación "señal a ruido" obtenida de la pura observación de las contramedidas individuales, es cada vez menor.

Cuando analizamos la cadena completa del ataque y vemos que, tras abrir dicho correo, nos llevan a un sitio web sospechoso para a continuación descargar un "payload" e iniciar un movimiento lateral en nuestra red, es cuando únicamente podemos correlar dichas acciones e identificar que efectivamente estamos siendo objeto de un ataque.

Cisco XDR es una solución diseñada para ser capaces de identificar la secuencia completa de este tipo de ataques. *Correla* y analiza telemetría y alertas que provengan de las siguientes contramedidas de protección (que pueden ser de Cisco o de terceros): el Endpoint, la Red de Datos (gracias a su NDR integrado), los firewalls, la identidad, el Correo Electrónico, la Navegación y la Nube. Junto con la telemetría de Talos de estos entornos y potentes motores de analítica de datos e inteligencia artificial, es capaz de descubrir la anatomía completa de los ataques y de desencadenar acciones de respuesta en cada uno de estos entornos.

Cabe destacar que la solución XDR de

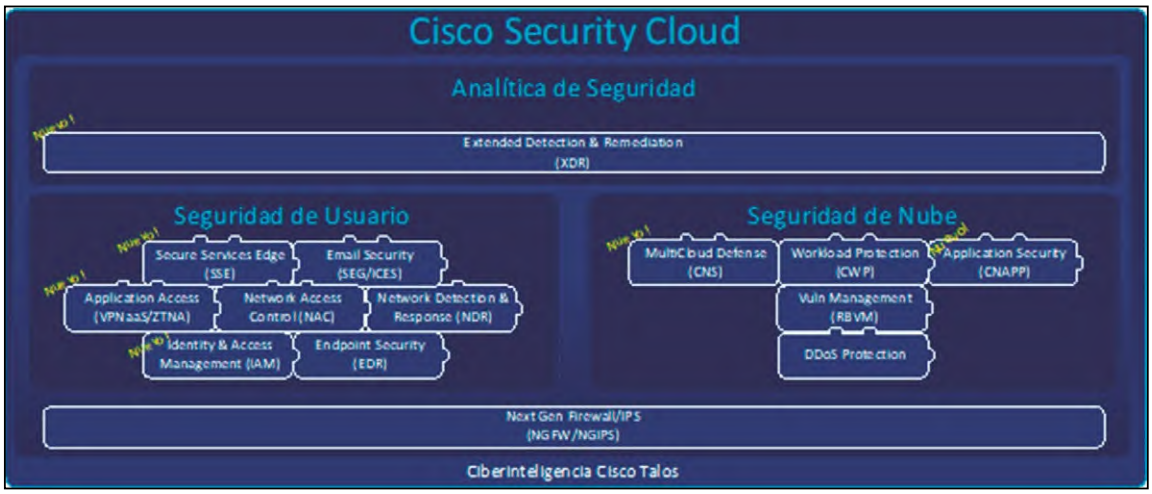


Figura 1.- Servicios ofrecidos desde Cisco Security Cloud

OneseQ by alhambra

Si te pillan...

...que sea con los deberes hechos.

Gestiona Ciberincidentes antes de que ocurran.

Alerta Temprana

Respuesta

Monitorización Activa

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

Detección de Intrusión

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

Respuesta ante Incidentes

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

Equipo de Respuesta ante Incidentes

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

CCN centro criptológico nacional

Catálogo de Empresas y Soluciones de Ciberseguridad – Empresa Registrada incibe_

Red Nacional de SOC

Accredited by Trusted Introducer

FIRST

CSIRT.es

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

Cisco, a diferencia de otras soluciones existentes en el mercado, no necesita que ninguna de las contramedidas de las que recibe telemetría y alertas sean de Cisco, siendo la solución más abierta del mercado en cuanto a número de fabricantes soportados y la más amplia en cuanto al número de fuentes de telemetría recibidas. (Figura 2).

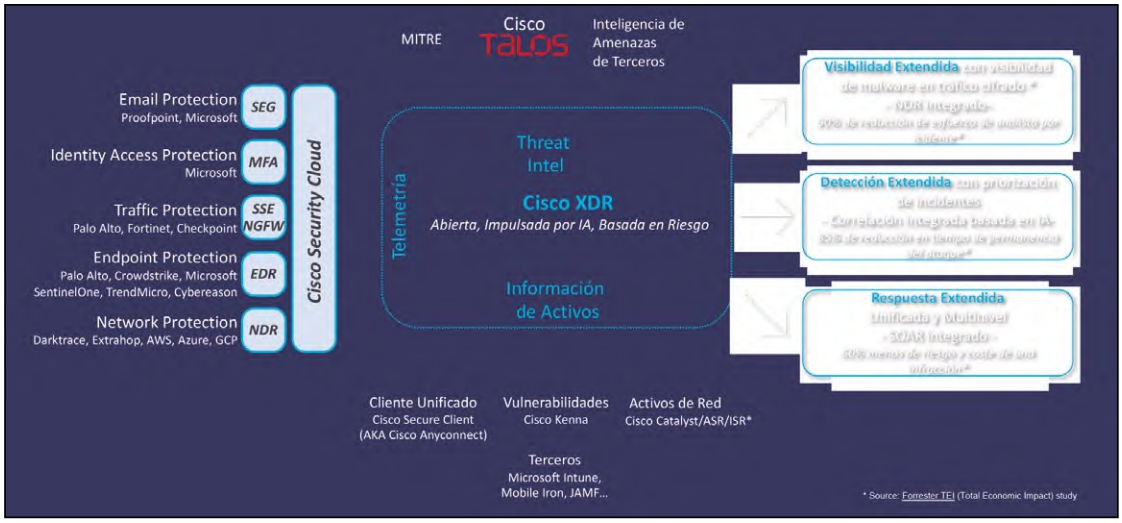


Figura 2.- Arquitectura Cisco XDR

Cisco Secure Access (SSE)

Hoy día, con la evolución a la *cloud* y el auge del trabajo híbrido, los usuarios se ven obligados a navegar por experiencias de acceso incoherentes y a re-autenticarse a lo largo del día, mermando su productividad. Se necesita una nueva aproximación que facilite el trabajo híbrido asegurando el acceso de los usuarios de manera sencilla a través de cualquier ubicación, cualquier dispositivo y cualquier aplicación ¿Por qué no puede el usuario, simplemente, encender su dispositivo y ponerse a trabajar (con independencia de la aplicación a la que acceda)?

Esto es precisamente lo que aporta la nueva plataforma SSE de Cisco, denominada Cisco Secure Access, que elimina la carga del usuario y proporciona una experiencia optimizada con acceso a todas las aplicaciones, no sólo a algunas, permitiendo la eliminación efectiva de las VPN en el cliente.

Además de incluir las funcionalidades de nube básicas para SSE (ZTNA, SWG, CASB y FWaaS) añade capacidades diferenciales como Protección DNS, DLP Multimodo, VPNaaS, RBI o Monitorización de la Experiencia con la Plataforma ThousandEyes de Cisco. Todo ello en una única suscripción y consola.

Cisco Multicloud Defense

Cisco Multicloud Defense proporciona una capa de seguridad de red unificada a través de las principales nubes, incluyendo AWS, Azure, GCP, OCI o nubes privadas. Con su enfoque de controlador único centralizado, simplifica la gestión y la protección de la seguridad en toda la infraestructura multinube del cliente.

A medida que su red evoluciona, Cisco Multicloud Defense evoluciona con ella. Aprovechando la visibilidad de la red y su integración en los diferentes entornos cloud, elimina los silos y permite administrar y automatizar las políticas de todos los entornos de nube en un solo lugar con una sola política. Es la propia solución la que se encarga de traducir esta política unificada a las diferentes nubes. A medida que cambian los entornos, la administración de políticas de múltiples nubes basada en etiquetas mantendrá las políticas actualizadas casi en tiempo real, minimizando la redundancia y ahorrando tiempo de administración a los equipos de seguridad.

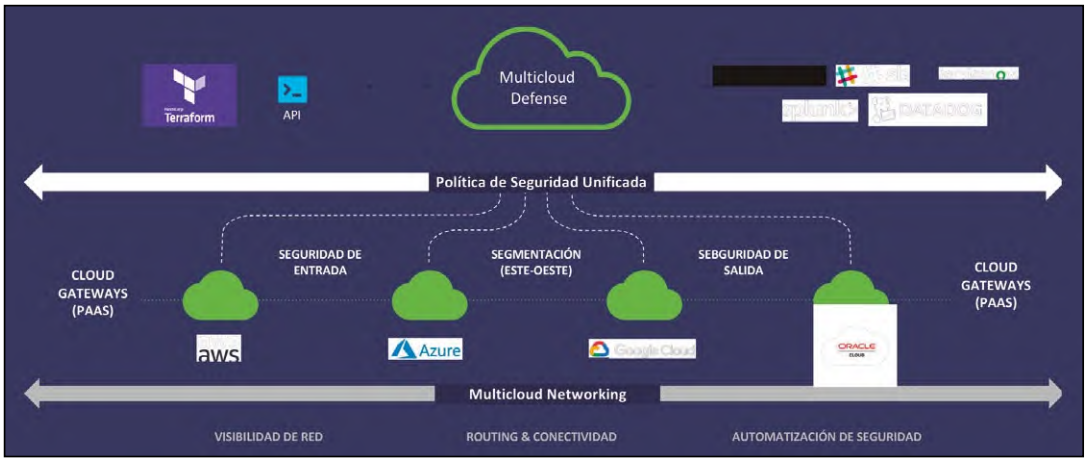


Figura 3.- Cisco Multicloud Defense

IA generativa: mejor respuesta y gestión simplificada

La Plataforma Cisco Security Cloud continúa evolucionando, tanto con desarrollos orgánicos como con la incorporación de adquisiciones inorgánicas. Un elemento clave es el uso extensivo de Inteligencia Artificial, y por ello también hemos anunciado las primeras capacidades de IA generativa, que permiten a las organizaciones:

- Reducir la complejidad de las políticas. El Asistente de Políticas generativo permite a los administradores describir políticas de seguridad granulares y evaluar la mejor manera de implantarlas en su infraestructura.
- Detectar y remediar rápidamente las amenazas. El Asistente SOC permitirá detectar y responder a las amenazas con mayor rapidez. Cuando se produzca un incidente, contextualizará los eventos a para indicar a los analistas qué ha ocurrido y cuál ha sido su impacto. A continuación, se puede interactuar con el asistente para determinar el mejor enfoque de corrección aprovechando una amplia base de conocimientos de posibles acciones. ■

Ángel Ortiz Álvarez
Director Ciberseguridad España
CISCO

Espacio TiSEC planteó el estado y grandes retos del ciberseguro y cómo responde la ciberprotección con una veintena de referentes del sector, la industria y la administración

La ciberpóliza recupera auge, afina mejor la medición y llega a la Dirección como recurso estratégico para transferir el riesgo

El mercado mundial del seguro cibernético rozó los 13.000 millones de euros en primas en 2022, según la firma especializada GuyCarpenter. Y los analistas consideran que no dejará de crecer en los próximos años. Fruto de esta demanda en plena efervescencia, Revista SIC celebró el 13 y 14 de junio la cuarta edición de su Espacio TiSEC, dedicada expresamente a este ámbito, bajo el título 'Ciberseguridad endeble y ciberpólizas'. Dos jornadas que contaron con más de 360 inscritos, tanto presencial como en línea, y en las que se debatió, a través de una veintena de referentes, sobre su situación actual, su utilidad para transferir riesgos y sus grandes retos. No faltaron mesas de debate polémicas sobre si es lícito pagar o no los rescates de *ransomware* y que mostraron la realidad estadística. El evento contó con el apoyo de Aon, Tokio Marine HCC, Barracuda, Cyber Guardian, Kaspersky y Stormshield.

La industria del seguro cibernético está cogiendo de nuevo velocidad. En un mercado donde ya se ha alcanzado una masa crítica de clientes, como consecuencia a una demanda a la que ha sabido responder el sector con pólizas y coberturas adaptadas al riesgo actual, muchos analistas confirman una reactivación de la contratación y la oferta, fruto de un mercado de ciberpólizas donde cada vez se mide mejor el riesgo y, también, la apuesta por transferirlo por parte de las empresas.

La cuarta edición de Espacio TiSEC, dedicada a este ámbito y a cómo reducir el riesgo frente a amenazas colosales, persistentes y crecientemente sofisticadas como el *ransomware*, comenzó de la mano de **Alfredo Zorzo,** director de Ciberseguros de **One eSecurity,** con una ponencia de título polémico: 'El fin de los ciberseguros'. En ella mostró cómo han ido evolucionando desde su gestación y resaltó que, en los últimos años, este mercado ha estado marcado por el impacto del *ransomware,* "que está ya excluido en algunas pólizas o se limita". A pesar de ello, en el último año, las suscripciones han crecido porque "las empresas entienden que necesitan este tipo de pólizas".

En un giro lleno de ironía, el ponente recordó que 'fin' no es sólo el final de algo sino, también, el objeto con el que se ejecuta algo. Así, destacó un amplio listado con lo que aporta el ciberseguro, "aunque muchos sectores consideran que ha tocado techo". En él destacó los beneficios que da la competencia en este ámbito, la madurez que evidencia, la mejora de comportamientos y su negociación, las alternativas que hay en el mercado, lo que facilita, lo que supone tanto en el aspecto legal y, también, la evolución de los cuadros de mando y el equilibrio entre la ciberseguridad y los ciberseguros, algo que, "algunos", recordó, "consideran que debería clarificarse a nivel mundial".

No obstante, también recordó que esta área de negocio tiene que superar los actuales problemas como muchos riesgos que las aseguradoras consideran "no asegurable", el incremento de los costes de respuesta y de impacto, las limitaciones de las coberturas, los ataques estado-nación, así como las mejoras de la ciberseguridad que pueden hacer que se apueste por invertir en ella más que en las pólizas como tal, entre otros aspectos.

La visión del mediador

A continuación, **Verónica Jiménez**, Director Specialty Cyber Solutions de **Aon** y **Carlos Bereciartua,** Director de Ciber Consulting de **Aon España,** hablaron de cómo se está viendo la evolución de este tipo de mercado desde el punto de vista de los mediadores. Así, Jiménez destacó que, en el lado asegurador, se está planteando esta área como una oportunidad en la que cada vez hay más competencia. "Aunque el proceso de suscripción es cada vez más riguroso, pero la mayor madurez de las empresas también está haciendo que sean más rápidos", y recordó que las exclusiones de ciberguerra están marcando el sector este año.

En su ponencia subrayó que se ha pasado de un mercado muy duro a otro más favorable, con la mayoría de las aseguradoras intentando aumentar sus carteras en ciberseguros. De cualquier forma, comentó que "la tecnología operativa y el riesgo de la cadena de suministro o riesgo sistémico siguen siendo objeto de gran escrutinio por parte de los suscriptores, lo que pone de relieve la necesidad de recopilar y presentar datos de calidad en el momento de la renovación". En cuanto a perspectivas de futuro, Jiménez destacó la exclusión de guerra, que ya está contemplada, igual que se está estudiando la posibilidad de sufrir el "riesgo de un evento sistémico o catastrófico, por ejemplo, por proveedores de servicios en nube".

Bereciartua, por su parte, comentó la presión que existe para lograr una ciberresiliencia. "Los ciberriesgos cambian continuamente, lo que puede dificultar que las empresas establezcan las medidas adecuadas". Así, resaltó los tres niveles ejecutivos de la empresa y recordó que "llegar al seguro a través del CISO es complicado porque hay que hacerlo a través de la dirección, que tiene que tener claro a qué riesgos se enfrentan". Junto con la necesidad de que la dirección esté muy integrada en la gestión de los ciberriesgos, destacó la importancia del rol del mediador como Aon, "actuando como puente para conseguir el seguro de la mejor forma posible".


Alfredo Zorzo


Verónica Jiménez


Carlos Bereciartua


Isaac Guasch


Cristina Brau

La visión de la aseguradora

Isaac Guasch, Cyber Security Leader de **Tokio Marine HCC,** y **Cristina Brau**, Junior Cyber Underwriter de la compañía, dieron una visión en profundidad de uno de los referentes en este ámbito. "Nuestro principal reto es transmitir por qué hacemos cuestionarios con un nivel concreto de detalle para ser capaces de trabajar de

forma conjunta". "Es importante saber no sólo que se tiene MFA o Confianza Cero, sino que además la compañía muestra un notable nivel de madurez", dijo Guasch, que puso en valor "la actitud de las empresas que evidencian que se preocupan por su ciberseguridad, qué tienen planes de gestión de crisis y qué evolucionan en ello más que tener o no una medida de protección concreta".

Brau recordó que "cuanto más sólidas son las medidas preguntadas en un cuestionario, mayor será el grado de seguridad. Por eso, hay cuestionarios muy extensos, pero tiene explicación: cuanto más se conoce de una compañía, más ajustado será el precio y las coberturas". Los dos expertos explicaron que aseguradoras y *brokers* van de la mano y puso en valor cómo se han creado nuevos productos de seguro adaptados a las tendencias de amenazas. "La buena noticia es que hay pólizas de ciberseguridad no sólo para grandes compañías sino, también, para pymes. Pero el producto no va a ser el mismo porque los riesgos son diferentes y no podemos hacer esos ejercicios de analizar su riesgo de la misma manera, porque son muy complejos", destacó.

Los especialistas de Aon también resaltaron que, además del mercado de grandes organizaciones, cada vez más pymes buscan contar con una ciberpóliza, por lo que se han personalizado para este tipo de compañías. "Lógicamente, la contratación es más ágil y sencilla, pero también sus coberturas son más limitadas. La buena noticia es que ya hay disponibilidad de pólizas cibernéticas para todo tipo de empresas".

El papel del CISO en las pólizas

Finalizó este primer bloque con la intervención de uno de los CISOs españoles con mayor solvencia y trayectoria, **Francisco Lázaro**, de **Renfe**, "compañía que tuvo el primer ordenador que llegó a España y que también fue la primera en poner un departamento de ciberseguridad". En su ponencia explicó cómo se trabaja en este ámbito en Renfe. "Nosotros definimos hacia dónde hay que ir y supervisamos, pero lo hace otro grupo de operaciones de ciberseguridad. En cierto modo es parecido al trabajo del DPO, asesoramos pero "no limpiamos pescado". En una ponencia muy ilustrativa mostró cómo la compañía de transporte está trabajando, desde hace seis años, en su primera ciberpóliza, cuyo concurso está cerca de ver la luz. En este sentido, puso en valor que cuando "trabajas en ciberseguridad empiezas por la protección, pero terminas preocupándote por las capacidades de recuperación. Hay que trabajar en reducir probabilidad, riesgo o ambas cosas. Cuando se habla de ciberseguros la clave es qué voy a hacer para reducir esa probabilidad, impacto o para transferir el riesgo", destacó. "Cuando vas creciendo te das cuenta de que necesitas más supervisión". De hecho, recordó que, a final de año, Renfe espera registrar más de 3.000 eventos de ciberseguridad diarios como parte de su visión proactiva en este terreno, recordando también, con orgullo, que "desde hace años, cualquier compra que hace la compañía lleva la protección cibernética en sus pliegos, para incorporarla por defecto, igual que la protección de datos". Y es que, entre sus conclusiones destacó que es fundamental para contratar un ciberseguro tener capacidad de análisis y visibilidad de lo que ocurre en la empresa, tanto en OT como en TI, "teniendo claro los objetivos". De cualquier forma, también lamentó que no existe un marco común para pedir información del grado de madurez de los proveedores por parte de los operadores de servicios esenciales.


Francisco Lázaro

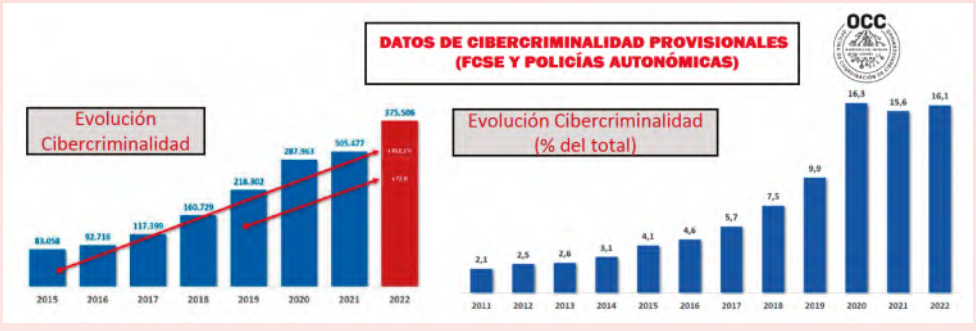

Javier Candau


Juan Delfín Peláez


Álvaro de Lossada

El impacto del *ransomware*

Comenzó el segundo bloque del primer día con un clarificador debate, moderado por el editor de Revista SIC, **Luis Fernández,** con la participación de **Javier Candau,** jefe del Departamento de Ciberseguridad del **CCN, Juan Delfín Peláez,** responsable del Sector Estratégico Financiero y TIC del **Incibe,** así como **Álvaro de Lossada**, jefe de la **OCC,** sobre la 'Evolución del impacto del *ransomware* en ámbitos públicos y privados'. En su intervención, Candau destacó la necesidad de tener procedimientos de actuación en incidentes críticos y la importancia de implementar la doble autenticación, entre otros aspectos, para dificultar los ataques de *ransomware*, a través de la defensa activa. Peláez, que recordó que el Incibe registró el año pasado más de 118.000 incidentes, precisó que el 60% eran intentos de fraude y de instrucción aprovechando sistemas vulnerables. De Lossada, por su parte, recordó que el *ransomware*, como cualquier actividad delictiva, tiene como último fin el lucro económico y, por lo tanto, hay que actuar con ese enfoque de atajar el delito alertando de la gran organización y medios con las que cuenta los grupos criminales.



Además, respondieron a si es proporcional los rescates que reclaman los cibercriminales en casos de *ransomware*, en relación al tamaño de las víctimas. "Y sí, claro que se ajusta porque te conocen", recordó Candau, añadiendo Peláez que también tienen en cuenta, por ejemplo, la sanción a la que se puede exponer la empresa por fugas de datos. De hecho, De Lossada destacó que entre el 30% y el 80% de las empresas pagan, aunque también coincidieron en que muchas compa-

COLOQUIO PRIMER DÍA

Más coordinación, transparencia, confianza e inversión en seguridad, claves para impulsar el mercado asegurador ciber

Para concluir la primera jornada, tuvo lugar un interesante debate, moderado por el redactor de SIC, **José Manuel Vera,** en el que intervinieron **José Antonio Castro** (Cyber Guardian), **Isaac Guasch** (Tokio Marine HCC), **Miguel López** (Barracuda) y **Verónica Jiménez** (Aon), quienes ofrecieron sus impresiones finales y respondieron a las preguntas de la audiencia. La primera cuestión que suscitó interés fue si existe margen para, con una madurez alta en ciberseguridad, bajar el precio de las ciberpólizas. Tanto para Guasch, como para Jimenez, la respuesta fue clara y concisa: "sí". Aunque Guasch la matizó argumentando que, siempre y cuando, "la revisión de los riesgos y las medidas sigan evolucionando y sofisticándose, además de estar al día con las tendencias de las amenazas". "Si se cumple con eso, hay margen para que los precios bajen", puntualizó. En este sentido, López añadió que uno de los parámetros más importantes que repercuten en el coste de una ciberpóliza "es la postura de ciberseguridad. Y aquí, uno de los grandes desafíos es optimizar la inversión". Para ello, "los proveedores podemos implantar soluciones que optimicen la postura de protección del cliente", recordó. De igual forma, Castro apuntó que "el producto de seguridad cibernética y ciberaseguramento encaja muy bien". El directivo también mostró su visión acerca de las pólizas ciber dentro de 10 años, vaticinando que "todo deberá estar orientado a la madurez, pero será algo común". López indicó, asimismo, que "el rumbo que sigue es el de la 'comoditización'". Para Guasch será un producto "más granular y específico". Y Jiménez, por su parte, explicó que, de hecho, "el seguro cibernético ya ha evolucionado respecto a hace una década y se van adaptando a los nuevos retos. Creo que habrá un seguro cibernético de protección personal, además del corporativo", presagió.

José Antonio Castro, Isaac Guasch, Miguel López y Verónica Jiménez

El coloquio prosiguió con otras cuestiones que recalaron en qué está haciendo mal la industria de ciberseguridad y el sector asegurador. Por un lado, y como representantes de este último, Guasch indicó que "lo que más se echa de menos es la transparencia" y Jiménez afirmó que, en el lado positivo, "estamos trabajando más coordinados para obtener información, tendencias, etc., y se tiene que seguir por este camino". Por parte de los proveedores, López manifestó que "no se está haciendo nada mal, quizá hay áreas de mejora", pero "están evolucionado a una velocidad muy rápida y muy bien en un sector muy dinámico". Eso sí, Castro destacó la "confianza percibida", como un aspecto que habría que mejorar "tanto por parte de las aseguradoras como de todos los que intervenimos en ese potencial mercado". Y es que, "en general, en el mundo asegurador se transmite mucha confianza en pólizas tradicionales, como las de hogar, y tenemos que llegar también a ese entorno de confianza en el mundo de las ciberpólizas".

ñías se recuperan de este tipo de ataques sin sucumbir ala extorsión económica, por lo que se recomienda no hacerlo y, en último caso, de suceder, delegar la negociación a los expertos de las fuerzas y cuerpos de seguridad, además de denunciarlo, ya que permite adquirir una información del cibercrimen que puede ayudar en ese y otros casos. Candau aprovechó para sugerir al sector asegurador, como medida para medir la ciberprotección de una organización, utilizar el Esquema Nacional de Seguridad. Eso sí, también se comentó que el mero pago del rescate no supone un delito y no hay sentencias de condena en este ámbito.

Para mejorar la protección frente a amenazas como el *ransomware,* Candau pidió mayor colaboración y compartición de información, mientras que Peláez apostó, además, por invertir en concienciación y formación a los equipos técnicos, además de destacar la necesidad de contar con políticas de ciberseguridad robustas y conocidas por todos, según De Lossada.

Referentes de la industria

A continuación, cogió el testigo el *country manager* de **Barracuda** en Iberia, **Miguel López**, con su ponencia 'Ciberdefensa y ciberseguros: dos caras de la misma moneda'. En ella, el directivo mostró de forma muy ilustrativa cómo cada vez es mayor el impacto de los ciberataques, con casos como Ferrari, el Clinic de Barcelona o The Guardian, poniendo en valor el enfoque de contar con *backups* que permitan recuperar la información. Además, comentó que, en 2022, el 38% de las víctimas sufrieron varios ataques de este tipo en el mismo año y que el sólo el 51% consiguió recuperar la información por sus medios. En este sentido, apostó por tecnologías como las de su compañía para ayudar a reducir el riesgo e implementar, entre otros, el doble factor de autenticación (MFA), control de acceso a la red, *backups* inmutables… además de tener un plan de ciberseguridad y respuesta, probándolo en ciberejercicios para saber cómo reaccionar y qué priorizar si sufres un incidente crítico.


Miguel López

Recordó, asimismo, la importancia de reducir el área de exposición que supone el correo-e, "con hasta 13 tipos de ciberamenazas identificadas a través de él", y puso en valor tecnologías como *sandbox* para evitar este tipo de amenazas, aunque "sólo el 18% cuenta con ésta". Asimismo, recomendó

apostar por enfoques como el de Confianza Cero y la necesidad de contar con herramientas forenses para determinar por dónde han entrado los cibercriminales, y desplegar mecanismos de respuesta y de recuperación. En este sentido, comentó la necesidad de que "las empresas de ciberseguridad y las de ciberseguros trabajen juntas. No tiene sentido las unas sin las otras. Una póliza cibernética no puede sustituir a la ciberprotección y viceversa".

Terminó las ponencias de la primera jornada, **José Antonio Castro**, responsable global de **Cyber Guardian**, quien mostró cómo puede mejorarse la ciberseguridad en las pymes a través de su plataforma, "basada en tres pilares: máxima protección, sencillez y modelo de precios sencillo". Un enfoque que permite a este tipo de empresas contar con un "nivel de ciberseguridad continuo y entendible para anticiparse a los riesgos". Así explicó cómo permite contar con seguridad en los equipos, el correo-e, la navegación e involucrar también a los empleados a través de, por ejemplo, simulaciones de *phishing*. Además, permite monitorizar de forma proactiva las redes para responder "a las amenazas más avanzadas, tanto de riesgos internos como externos, y de la forma más sencilla posible". Por eso, comentó que "la plataforma Cyber Guardian también supone una notable ayuda para las aseguradoras y para conseguir una ciberpóliza, ya que permite entender el nivel de seguridad de cualquier empresa a través del *scoring* dinámico que ofrece, adaptado a cada perfil de organización".

Segunda jornada: dando respuestas

Comenzó la segunda jornada de Espacio TiSEC de la mano de **Julio San José**, *managing director* de Transformación Digital y Ciberseguridad de **Alvarez&Marsal**, con una ponencia sobre cómo desarrollar y disponer de un 'Cuadro de mandos de riesgo continuo', que permita ir "hacia un consenso entre asegurados y aseguradoras".

En su intervención, destacó que actualmente no se puede "trabajar en momentos puntuales para medir el riesgo respecto a la póliza". Por ello, denominó su propuesta como 'modelo continuo', que supone "conocer los riesgos y poder revisarlos cada día, cada mes, cada año y, en definitiva, en cualquier momento".

En concreto, explicó que la virtud de este cuadro de mandos de riesgo continuo es "permitir ver lo que otros no ven con una ventaja clara para el asegurado, por cuanto se establece una relación de confianza con un proveedor estratégico como es la aseguradora, ya que transferimos lo que no podemos proteger". Además, comentó la necesidad de trabajar de arriba abajo, ya que el cuadro de mandos sirve para la aseguradora, para los CISO, para auditoría interna y "es posible, incluso, ponerlo en modo piramidal para representar muchas cosas". Eso sí, debe cumplir una serie de premisas, como estar basado en "un marco de trabajo claro para que sea entendido por todo el mundo", dijo destacando que, a través de esta propuesta, también la alta dirección puede conocer el nivel de ciberseguridad de la organización "de un solo vistazo" e, incluso, destacar lo que realmente sea relevante para la Junta. "En definitiva, se trata de adoptar con él un enfoque estratégico apostando por el cuadro no como una herramienta sino como un método, que permita el acercamiento y consenso con la aseguradora".


José Antonio Castro

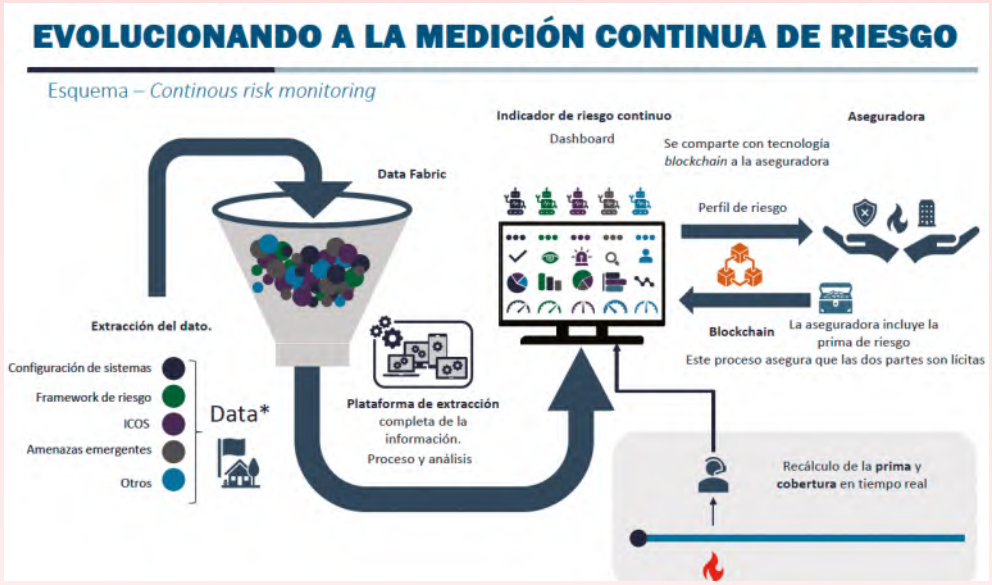

Julio San José


Juan Gayá


Antonio Osuna

Buenas prácticas

A continuación, el director de riesgos y seguros de **El Corte Inglés**, y miembro de la junta directiva de la **Asociación Profesional Española de Gerentes de Riesgos y Seguros** (**Agers**), **Juan Gayá,** presentó en primicia la 'Guía Ciber: buenas prácticas en protección de ciberriesgos (para no expertos)'. En su intervención, destacó la importancia de hablar para no 'entendidos' en ciberseguridad. Un objetivo que se ha venido plasmando, desde 2017, en la publicación de sucesivos documentos para este ámbito, el primero de terminología especializada. "Para gestionar ciberriesgos hay que prevenirlos y, también, transferirlos", recalcó mostrando los aspectos más destacados de la última guía, que incluye notables buenas prácticas de gestión de riesgos, basándose en el enfoque del NIST. "Se trata de medidas genéricas para todo tipo de amenazas porque el riesgo cero no existe, pero sí hay que intentar detectarlas lo antes posible para tener el menor impacto, sabiendo cómo gestionarlo". Como colofón a su intervención, desveló el tema de la próxima publicación de Agers, prevista para 2024, que tratará sobre cómo poder conocer el alcance de una póliza de seguro sin tener un sinestro. "Cada vez se tiene más conciencia de la importancia de las pólizas cibernéticas



COLOQUIO SEGUNDO DÍA

Principales métricas en la obtención de un ciberseguro: alinearse con estándares, el número de amenazas, continuidad de negocio y la cantidad de activos críticos

Como colofón a Espacio TiSEC, la segunda jornada concluyó con un distendido debate para reflexionar sobre algunos de los temas tratados durante el encuentro. En esta ocasión, se reunieron en el estrado **Thomas Dupont** (Stormshield), **Julio San José**, (Alvarez&Marsal) y **Marc Rivero** (Kaspersky), quienes comenzaron analizando el estado actual de los ciberseguros. Los tres intervinientes coincidieron en considerar que están "en fase de maduración", por lo que "no se está haciendo nada mal", añadía San José. Eso sí, "el mercado del cibercrimen va muchísimo más deprisa y nos hemos quedado atrás", recordó. Precisamente, sobre este último apunte se pidió la opinión de los ponentes sobre qué es lo que hace falta para ir por delante del cibercrimen. El directivo de Alvarez&Marsal indicó que "no podemos ir por delante, pero podemos acercarnos". "El cibercrimen juega en otra liga porque están perfectamente organizados, no tienen reglas éticas, ni tienen que cumplir la ley en ningún país del mundo, además de ser grandes profesionales, aunque en el lado equivocado. Así que, debemos de trabajar para reducir esa distancia y en ser más resilientes". Rivero señaló que es fundamental que "los CISO intenten alinear la organización con los estándares y reglamentos de ciberseguridad, así como con el *framework* MITRE ATT&CK, entre otras acciones, para ponérselo lo más difícil posible y no ser un *target* fácil". Para Dupont "es importante colaborar entre todos, organizaciones públicas, privadas, etc., así como aumentar la cultura de la ciberseguridad, no solo en lo empresarial, sino también en el ámbito personal que, en mi opinión, está abandonada".

Thomas Dupont, Julio San José y Marc Rivero

A continuación, el debate siguió con cuestiones como qué se puede aprender del cibercrimen para ser más resilientes o qué tipo de métricas deberían de priorizar las empresas para conseguir un mejor ciberseguro. Ante esta última pregunta, Dupont destacó "cumplir con las normas y los estándares y, sobre todo, transparencia". San José especificó "el tiempo que se está disponible, además del número de incidentes, tomando como 'incidente' cualquier cosa que provoca una disrupción, por un tiempo prudencial". Rivero coincidió en el número de incidentes, además de añadir "un porcentaje de alineación con estándares, como NIST o ISO, y la cantidad de activos que son sensibles en la organización".

El debate concluyó con una ronda final acerca de por qué los ciberseguros se han convertido en un recurso imprescindible. Para Dupont, "es algo obligatorio y, si la póliza no cubre todo lo que queremos, al menos, debe cumplir y ayudar con los riesgos y daños a terceros". San José subrayó que "sin una ciberpóliza se carece de una correcta gestión de los riesgos porque eres incapaz de protegerlo todo". Rivero concluyó apuntando que "según el sector en el que te muevas, también hay que tener en cuenta lo que te va a exigirte un ciberseguro tomando en consideración qué te cubre y qué no, así como el tipo de aseguradora donde se decida obtenerlo", entre otros aspectos.

para proteger las cuentas de la empresa gracias a la transferencia del riesgo, algo de lo que cada vez es más consciente la alta dirección".

Acto seguido, el responsable de Arquitectura y Riesgos del **Grupo Santa Lucía**, **Antonio Osuna**, explicó las consideraciones más importantes que las compañías tienen en cuenta para la viabilidad en la contratación de una ciberpóliza. En este sentido, mostró cómo se analizan los riesgos de los seguros, destacando que para conseguir uno cibernético hay que implicar y trabajar de forma transversal con muchos departamentos de la empresa, siempre liderados por el de ciberseguridad. También recordó que, actualmente, aparte del impacto económico, las compañías aseguradoras miran mucho la capacidad de respuesta a un incidente.

"Actualmente, el sector es conservador a la hora de ofrecer este tipo de productos, pero sí considera que es rentable y que no depende sólo del CISO, ya que estos incidentes impactan en el negocio". Por ello, indicó que para lograr una ciberpóliza adecuada hay que involucrar a la alta dirección. De hecho, comentó que "cada vez más empresas de calificación financiera tienen en cuenta qué pólizas de este tipo tienes. Y que no es fácil conseguirla, ya que ahora, por las cantidades que se piden cubrir tienes que negociar con varias aseguradoras para que cubran cada tramo de un incidente". "Y es que la valoración del riesgo ciber, con pocos datos históricos, hace que el apetito de las aseguradoras por él sea más bajo de lo esperado". De cualquier forma, también destacó que se trata de un mercado en el que hay muchos competidores de confianza, donde se puede escoger y que cada vez es más evidente

en las empresas que "la ciberseguridad es un tema para el Consejo de Administración, no solo para los CISO".

Pagar o no pagar rescates

Al igual que en la primera jornada, también tuvo lugar un segundo debate de muy elevado interés, en esta ocasión sobre 'Pagar, no pagar… o como si no', tras un ataque de *ransomware*, moderado por el director de Revista SIC, **José de la Peña,** y en el que participaron algunos de los máximos expertos en la materia, como el Fiscal Delegado contra la Criminalidad Informática de la **Fiscalía Provincial de Madrid, Fidel Solera,** el teniente coronel **Juan Sotomayor,** jefe del **Departamento contra el Cibercrimen** de la **UCO** de la **Guardia Civil,** y el comisario jefe de la **Brigada Central de Seguridad Informática,** de la **Unidad Central de Ciberdelincuencia**, de la **Policía Nacional, Juan Carlos Sancho.**


Fidel Solera


Juan Sotomayor


Juan Carlos Sancho

Se trató de un coloquio en el que los participantes fueron muy directos y resolutivos. "Pagar como tal no es constitutivo de un delito, pero sí puede tener derivadas por a quién estás pagando, o a dónde va ese dinero y, lo más importante, qué te han robado para que quieras pagar el rescate, qué responsabilidad tienes sobre esos datos, etc.", comentó Solera. Sotomayor pidió mayor colaboración con las fuerzas y cuerpos de seguridad (FF.CC.SE), "ya que la denuncia y permitir que seamos nosotros quienes negocien puede, además, dar mucha información sobre los atacantes y la trazabilidad de estos pagos en criptodivisas". Sancho, de cualquier forma, recordó que en cada área geográfica hay leyes distintas sobre este tema poniendo el caso de Carolina del Norte donde está prohibido pagar a grupos terroristas o de *ransomware*, por lo que no se producen ataques de este tipo, ya que los cibercriminales son conscientes de que lo tiene más complicado para cobrar. Los tres, eso sí, pidieron que se denuncie más este tipo de ataques, ya que facilita su trabajo e, incluso, puede permitir recuperar lo pagado, además de la información robada, aunque sea de forma puntual. "Hay que colaborar más", pidió Sancho, recordando muchas operaciones policiales con éxito en este ámbito, que han sido facilitadas gracias a la implicación del sector privado "porque, a diferencia de otros ámbitos, aquí la Inteligencia la llevan las empresas".

Además, recordaron que las FFCCSE han adquirido muchas capacidades, experiencia y medios en los últimos años y cada vez se actúa de forma más exitosa contra el crimen cibernético. Así, pusieron en valor el cada vez mayor número de equipos conjuntos de investigación que permiten que se trabaje a la par en las denuncias hechas en diferentes países. Por eso, también plantearon si debería ser obligatorio la notificación del pago del rescate. "Que más allá de la obligación o no puede tener un aspecto ético, por lo que supone una ayuda para investigar", dijo Sotomayor. Eso sí, "hay que tener claro cuándo comunicar ya que, si se han hecho cosas rápido, pueden haberse cometido, incluso, delitos", dijo Solera que recordó las notables aportaciones que ha hecho la última actualización, de 2015, de la Ley de Enjuiciamiento Criminal al respecto.

No faltó en el debate la referencia a la acción ofensiva realizada por los **Mossos d'Esquadra**, tras el ataque sufrido por el Hospital Clinic, autorizada por un juez. "Hay que tener mucho cuidado con este tipo de actuaciones, ya que suelen ser delictivas e, incluso, se puede llegar a obtener información que ha sido robada y que tampoco deberíamos tener", dijo Solera.


Marc Rivero


Thomas Dupont

Y se recordó que ya se está viendo una tendencia en el mundo de los ciberseguros que es el propio fraude de la empresa reclamando la indemnización por ciberataque, cuando realmente no se ha producido. Por eso, "en algunos países para que el seguro responda se pide que haya una denuncia penal y una investigación en firme", como el caso de Francia, "para evitar como cuando se denunciaba que te habían robado el *radio cassette* para sacar dinero", dijo Sotomayor.

Propuesta de la industria

Cerraron Espacio TiSEC dos destacados especialistas, **Marc Rivero**, senior Security Researcher, Global Research and Analysis Team de **Kaspersky** y **Thomas Dupont,** presales Engineer para Iberia de **Stormshield.**

Rivero mostró en una ponencia basada en la inteligencia de amenazas de la compañía, cómo actúa el cibercrimen, dando a conocer las diferentes etapas de un ataque de *ransomware*, cada vez más como 'modelo de servicio' y desgranando qué hay detrás de los principales grupos cibercriminales que se logran con él. En este sentido, puso en valor que las empresas actúen, cada vez, de forma más proactiva. De cualquier forma, también recordó que cada año, se calcula que se pagan en torno a 5.000 millones de euros por extorsiones cibernéticas. Por eso, también destacó la necesidad de contar con socios de confianza para hacerles frente en todo tipo de aspectos, también, en caso de ser víctima, en la negociación "que termina siendo como una partida de ajedrez" y buscar que se cometan errores.

Por su parte, Dupont destacó cómo se puede reducir el riesgo a través de la tecnología que ofrece su compañía evitando, por ejemplo, la escala de privilegios cuando los cibercriminales entran en la red o facilitando la recopilación de indicadores de compromiso (IoC). "Entre la detección y la remediación pueden pasar horas y días y puede provocar movimientos laterales de los atacantes", así que "actuar rápido es vital", dijo a la vez que recordó que para reducir el riesgo hay que minimizar la superficie de ataque, por ejemplo, a través de aplicaciones maliciosas, incluso, descargadas de la tienda oficial de Windows.

Además, mostró cómo sacar partido de la tecnología de ciberprotección en tres casos de uso muy concretos: frente a USBs maliciosos, frente a un ataque DDoS a un servidor web de Windows y a atacantes que entran en la red corporativa buscando vulnerabilidades y tomar el control de los recursos críticos, además de frente a archivos maliciosos llegados por correo-e. ■

Enrique Cubeiro

Director de Ghenova Ciberseguridad

>Por **José Manuel Vera**
>Fotografía: **GHENOVA**

"Ofrecemos la ciberseguridad que mejor se adapta a las circunstancias de nuestros clientes, con un enfoque realista y práctico"

Directo, pausado y con la experiencia que da haber llegado a ser jefe del Estado Mayor y de Operaciones del Mando Conjunto del Ciberespacio, Enrique Cubeiro apostó en enero por el ámbito civil como director de ciberseguridad de la compañía Ghenova, un referente en el sector naval y en transformación digital. Desde entonces, ha desarrollado un amplio portafolio de servicios en el que no descarta ofrecer también productos.

– Viene del mundo de la ciberdefensa, ¿por qué apostó por Ghenova?

– Lo que más me sorprendió cuando conocí el Grupo fue su ritmo de crecimiento, tanto en plantilla como en volumen de negocio, y la decidida voluntad de la alta dirección por continuar en esa línea. Impresiona saber que este año superaremos el millar de empleados cuando antes de la pandemia apenas eran 500. Cuando en enero se creó la unidad de negocio de ciberseguridad, la intención era contribuir a ese crecimiento para lo que se establece un ambicioso objetivo de plantilla en términos cuantitativos y cualitativos para finales del 2025. Ahora mismo, Ghenova Ciberseguridad es la unidad de negocio más joven del Grupo. Pero, como el resto, nace con ese sello Ghenova que se cimenta en el entusiasmo, el compromiso y el afán de innovación. Y eso es algo que conocen y aprecian nuestros clientes. Por otra parte, contamos con una amplia cartera de clientes y una potente estructura que le permite optar con garantías de éxito tanto a contratos sencillos, como a proyectos muy complejos.

– Dicen desde Ghenova que "integrar la ciberseguridad en la estrategia de la empresa es clave para gestionar adecuadamente el riesgo tecnológico"…

– Por lo general, las empresas y organizaciones están llevando a cabo transformaciones digitales un tanto sobrevenidas y desordenadas, en la mayoría de los casos sin una planificación en condiciones y sin un asesoramiento especializado. Yo suelo emplear siempre el mismo símil para explicar la situación a la que esto lleva y es, precisamente, el del proceso inverso: imaginemos que todo nuestro negocio, activos, información… está en formato digital y un día decidimos convertirla en formato físico; está claro que haríamos sin dudarlo una considerable inversión para adquirir almacenes, puertas blindadas, cerraduras, cámaras de videovigilancia, sistemas contraincendios, detectores de humos… Sin embargo, a la inversa cuesta aplicar un esquema similar.

Y, a mi juicio, la razón es muy sencilla: las personas a las que corresponde tomar la decisión no perciben la necesidad de hacerlo porque, desde su punto de vista, eso de la ciberseguridad ni se ve ni se nota. A los profesionales de la ciberprotección nos corresponde cambiar esa forma de ver las cosas.

– Entre sus lemas destaca el que dice que ofrecen "soluciones realistas a problemas reales mediante el uso de la tecnología"…

– Con él queremos expresar que en ciberseguridad siempre vamos a ofrecer lo que mejor se adapte a las circunstancias de nuestros clientes, con un enfoque realista y práctico. Igual que un estanco y una joyería requieren soluciones de seguridad física muy diferentes, una empresa cuyos activos y actividades se ubiquen mayoritariamente en Internet requerirán una inversión mucho más importante que otra que apenas tenga una dimensión digital. Queremos que nuestros clientes entiendan los pros y contras de cada solución y elijan con conocimiento de causa la opción que mejor se adapte a sus necesidades, sus circunstancias y, muy importante, su presupuesto.

– Su amplio portafolio está centrado en cuatro áreas: consultoría, auditoría, concienciación y formación. ¿Cuáles son las que esperan generar más negocio y con qué valor diferencial?

– Nuestra evaluación es que el efecto combinado de transformación digital, cumplimiento de normativa, exigencia de los clientes y ciberamenaza creciente van a llevar a muchas empresas, inexorablemente, a contratar este tipo de servicios. Y no sólo en el ámbito de las tecnologías de la información, sino también en las de operación, campo en el que la penetración de la ciberseguridad es todavía muy escasa, pero que resulta tanto o más vulnerable frente a las ciberamenazas.

Aunque esas cuatro áreas suponen una oferta de servicios importante, somos muy conscientes de que en los próximos años nuestro portafolio debe crecer en consonancia con nuestro nivel de ambición. Nuestra intención es ir abarcando una gama de servicios cada vez más amplia, pero en esta fase inicial nos hemos circunscrito a aquellos que no requieren grandes inversiones en infraestructuras o no dependan de perfiles de nicho, por definición muy caros y difíciles de reclutar, y aún más de mantener. Tampoco descartamos entrar el mercado de productos y ya tenemos algunas interesantes ideas al respecto, pero no es probable que sea algo que abordemos a muy corto plazo.

– En un mercado tan competitivo y fragmentado en España como es el de la ciberseguridad, ¿cuál es su baza, respecto a sus competidores?

– Nuestra baza será una relación muy cercana y de absoluta confianza con nuestros clientes.

– Ghenova también está muy presente en el sector naval, ¿Van, también, a ofrecer una propuesta de valor en este sector?

– Ghenova tiene una fuerte vocación marítima que se traduce en un gran número de proyectos que tienen que ver con el mar: buques de todo tipo, gemelos digitales de fragatas, sistemas de mantenimiento predictivo para buques, estaciones de eólica marina, plantas de producción de algas… El sector marítimo comienza a ser consciente de que cada vez resulta más atractivo para las ciberamenazas y que es tan vulnerable a ellas como difícil de defender.

El que Ghenova cuente en sus filas con expertos en naval, ciberseguridad, IA, digital, *data analytics* o eólica marina, sumado al espíritu innovador del Grupo, facilita el abordar proyectos de este tipo, algo en lo que llevamos ya tiempo trabajando.

– Siempre han contado con un área de negocio potente en 'transformación digital' con una propuesta, sobre todo, por la industria 4.0, el software y la simulación y los gemelos digitales. ¿Qué papel juega en este ámbito la ciberseguridad?

– No puede haber transformación digital sin ciberseguridad. Software, simuladores y gemelos deben contar con requisitos de ciberseguridad desde su fase conceptual. La IA, el aprendizaje automático o el *blockchain,* áreas tecnológicas que también domina el área de negocio de Digital, están cada vez más presentes en todas las facetas de la ciberseguridad. Por ello, raro es el día que no tenemos alguna reunión con los representantes de Digital y cada vez es más habitual que nuestros recursos se involucren de forma conjunta en proyectos de todo tipo, algunos de ellos en el ámbito del I+D+i.

– La clave para la ciberprotección, en base a su experiencia…

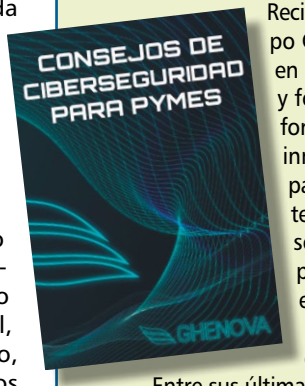
– Obviamente, en algo tan complejo no pude haber un solo elemento clave. Pero si tuviera que elegir el más determinante, no lo dudaría: estar alerta. Consejo que vale tanto para el ámbito personal, como para el empresarial. Por tal motivo, la concienciación es uno de los servicios que ofrecemos y sea, probablemente, el que resulte más rentable para la mayoría de empresas y organizaciones.

– Por último, ¿en qué medida las lecciones hasta ahora aprendidas del conflicto ucranio-ruso están marcando el devenir de la ciberdefensa y la ciberseguridad?

Ghenova tiene una fuerte vocación marítima y este sector comienza a ser consciente de que cada vez resulta más atractivo para las ciberamenazas y que es tan vulnerable a ellas como difícil de defender.

– Antes del inicio de la invasión, los analistas vaticinaban un muy rápido colapso del ciberespacio ucraniano que afectaría a infraestructuras críticas y servicios esenciales en todo el abanico de sectores: energía, comunicaciones, transporte, agua… Y que ese colapso marcaría el fin de la resistencia ucraniana. Pero nada de eso ocurrió. Con el tiempo hemos ido sabiendo las causas de ese inesperado desenlace y que podrían resumirse en una frase: Si Ucrania resiste es, fundamentalmente, gracias al enorme esfuerzo, decisión, imaginación y entusiasmo que está empleando en defender a toda costa su ciberespacio (para lo cual, han contado con mucha ayuda exterior). De ahí que la ciberseguridad y resiliencia de sus infraestructuras y las capacidades de ciberdefensa a sus fuerzas armadas, incluidas las ofensivas, resulten hoy factores clave para la supervivencia de un Estado. ■

GRUPO GHENOVA: la apuesta por mostrar la ciberprotección como una inversión que genera negocio

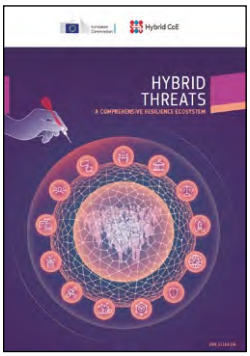


Recién creada este año, la unidad de negocio de ciberseguridad de Grupo Ghenova aspira a ser uno de los referentes del sector centrándose en cuatro áreas muy concretas: consultoría, auditoría, concienciación y formación. Además, espera compartir sinergias y estar presente de forma transversal en muchos de los grandes proyectos en los que está inmersa la multinacional, con sede en Ferrol, en medio centenar de países. En definitiva, su portafolio se basa en "ayudar a nuestros clientes a mantener la seguridad de sus activos, diseñamos soluciones de seguridad adaptadas, formamos a sus equipos y optimizamos sus procesos con el convencimiento de que integrar la ciberseguridad en la estrategia de la empresa es clave para gestionar adecuadamente el riesgo tecnológico", indican sobre el valor diferencial que esperan aportar.

Entre sus últimas iniciativas, destaca la publicación de una ilustrativa guía de ciberseguridad para facilitar la protección de las empresas de este ámbito. "Los apasionados de la ciberseguridad muchas veces nos olvidamos de que, para la gran mayoría, se trata de un asunto incomprensible, opaco y feo", recuerdan desde la compañía a la vez que subrayan que, por ello, "desde la primera página pretende ser inteligible para todos, confiable y, sobre todo, llevar al convencimiento de que invertir en ciberseguridad es una excelente inversión que puede suponer una ventaja competitiva y hasta un factor clave para la supervivencia", explica Cubeiro.

Pide un enfoque holístico similar al aplicado en normativas como NIS2 o DORA

La Comisión propone un marco de trabajo para hacer frente a las amenazas híbridas buscando el mayor grado de resiliencia



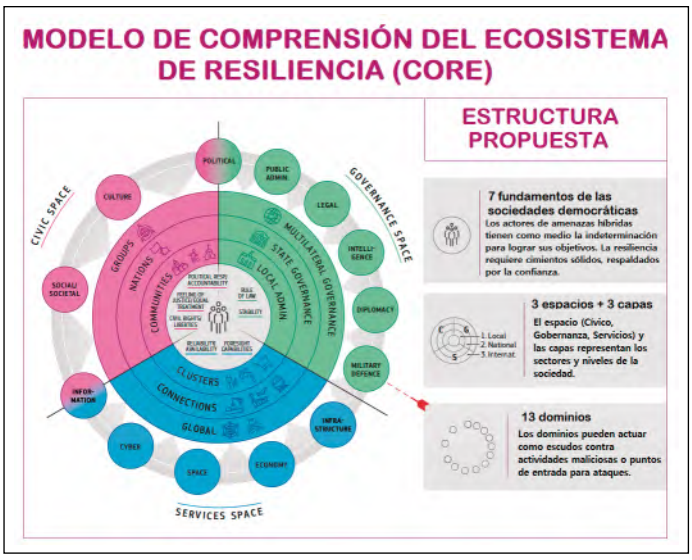
Las amenazas híbridas son consideradas en la UE uno de los aspectos más preocupantes por el impacto que tienen, directamente, en la sociedad democrática y nuestro estilo de vida. A pesar de que, desde 2020, hay en marcha un modelo conceptual para luchar contra ellas, en junio el Parlamento pidió una estrategia coordinada para aumentar la resiliencia de la UE ante las injerencias extranjeras y la manipulación de información y proteger las elecciones europeas. Esta iniciativa se plasmó en la aprobación de un amplio informe en el que los eurodiputados alertaron de una probable escalada y refinamiento de las injerencias extranjeras, la desinformación y los ataques a la democracia, sobre todo, en el periodo previo a las elecciones europeas, que se celebrarán en junio del próximo año, por parte de países como Rusia y China.

El Parlamento llamó la atención, de forma especial, sobre el "peligroso fenómeno de la desinformación por encargo: proveedores que ofrecen a agentes gubernamentales y no gubernamentales sus servicios para propagar desinformación —por ejemplo a través de la *deepweb*— con la intención de sabotear los comicios". "La injerencia extranjera en los procesos democráticos representa una creciente amenaza para la seguridad de los estados miembros y la UE. Debemos actuar con urgencia", destacó la ponente de la propuesta, la letona **Sandra Kalniete.**

Marco de resiliencia

Precisamente, para ayudar a luchar contra las amenazas híbridas a los responsables gubernamentales, el **Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas** (**Hybrid CoE**) y el **Centro Conjunto de Investigación de la Comisión Europea** han desarrollado un marco para "repensar la resiliencia de manera integral", plasmado en su informe 'Amenazas híbridas: un ecosistema integral de resiliencia', en el que han participado, entre otros expertos, la española **Marina Alonso Villota,** Research Assistant de la **Universidad Bundeswehr**, de Munich.

En su primera parte, el documento define qué son amenazas híbridas así como sus principales objetivos: "socavar y dañar la integridad y el funcionamiento de las democracias", "manipular la toma de decisiones establecida" y "maximizar el impacto creando una cascada de efectos, en particular adaptando ataques y combinando elementos de dominios para sobrecargar los sistemas mejor preparados con consecuencias negativas impredecibles".



A continuación, propone un modelo para hacerlas frente denominado 'Ecosistema Integral de Resiliencia' (o CORE), que parte de dos premisas: la gran interconexión de las sociedades abiertas y la necesidad de contar con respuestas coordinadas ante cualquier posible amenaza, participando la sociedad en todos sus niveles. El marco se basa en cuatro pilares: por un lado, siete aspectos fundamentales de los sistemas democráticos que están en el corazón del ecosistema. Por otro lado, en los dominios que son parte integral del sistema y que deben contar con resiliencia, actuando como escudos frente a actividades maliciosas. En tercer lugar, plantea la necesidad de proteger un ecosistema con tres espacios –cívico, gobernanza y servicios– que representa a la sociedad y sus sectores. Finalmente, muestra las capas del ecosistema que representan los diferentes niveles que existe en la sociedad, desde los más locales hasta los más internacionales.

Para hacer frente a este tipo de amenazas, se propone un enfoque integral para ecosistemas resilientes (CARE). Este concepto "es un componente clave para contrarrestar las amenazas híbridas" y debe "aprovechar las medidas de resiliencia de diferentes dominios", construyendo la respuesta "sistémicamente considerando las dependencias e interdependencias entre las diferentes partes de la sociedad".

Además, pone a iniciativas como la Directiva de Seguridad (NIS2) o la de Resiliencia de Entidades Críticas (DORA) como ejemplos de enfoque holístico en Europa, ya que se tratan de normativas que "consideran varios dominios y el ciclo completo de resiliencia desde la mitigación de vulnerabilidades hasta la presentación de informes y la mejora de las estructuras de gobierno".

Precisamente, entre otros aspectos, resalta que la "información es el dominio más usados por los actores de amenazas híbridas para causar interrupciones, sobre todo, en el espacio cívico", con "efecto cascada", por lo que aconseja desarrollar la resiliencia en este ámbito, fomentando la confianza en los medios de comunicación y el acceso a noticias de calidad, la transparencia en comunicación, salvaguardar el diálogo democrático y ser transparente con quién hay detrás de medios de comunicación y redes sociales. También, alerta del uso del *deepfake, bots* y robo-periodismos, pidiendo la protección de los medios libres e independientes.

Además, el informe analiza, de forma muy ilustrativa y en profundidad, varios casos de amenazas híbridas, entre ellos, lo ocurrido a raíz de la guerra de Ucrania con el gaseoducto Nord Stream 2, la injerencia rusa en Cataluña, el caso de la Covid-19 o las diferentes revueltas sociales vividas en Francia en los últimos años. Por último, el documento recuerda que "desarrollar una cultura de seguridad necesaria en la UE y en cada estado para construir resiliencia contra las amenazas híbridas requerirá un cambio de paradigma en la cultura de las organizaciones y funcionarios que trabajan en esta área, con comprensión de temas multidisciplinares". Pone como ejemplo la necesidad de "que los responsables de ciberseguridad, altamente cualificados, también se capaciten en área relacionadas con la comunicación y viceversa". De cualquier forma, el documento avanza que la UE está trabajando en "una caja de herramientas híbridas para mejorar su resiliencia, incluida su repuesta" frente a estas amenazas. ■

A ello se suma la complejidad para dar con personal especializado, incrementar la concienciación interna y contar con el apoyo del negocio

La popularización de tecnologías como GenIA, representadas por ChatGPT, dispara el estrés de los CISO por el incremento de la incertidumbre y el riesgo

La apuesta por la digitalización y la incorporación, a toda velocidad, de las nuevas tecnologías está haciendo que, cada día, los responsables de ciberseguridad de las empresas ganen en responsabilidades y, también, sufran un mayor estrés. Así lo destaca un estudio realizado por la firma **Salt Security,** en el que contó con la opinión de 300 CISO y CSO destacaron que, en un 90%, "la transformación digital presenta riesgos imprevistos". En este sentido, mostraron su preocupación un 91% por la complejidad por contratar personal cualificado, así como que esté al día en las nuevas amenazas y tecnologías. "Debido a que los servicios digitales introducen nuevos tipos de ataques, su defensa exige nuevos conocimientos y capacidades, por lo que la contratación de talento calificado es esencial", destaca el informe de la encuesta.

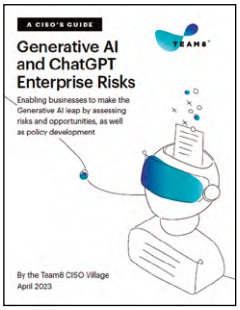
Además, los participantes también comentaron que tienen numerosos "problemas personales derivados de infracciones (48%) y un mayor riesgo y responsabilidad por cometer errores". Así los tres principales desafíos que surgen de la digitalización son la cadena de suministro (38%), las API (37 %) y la adopción de la nube (35%).

Preocupación por la IA

A ello se suma todo lo que está suponiendo la popularización de la aplicación de la IA, también en ciberseguridad. De hecho, el 94% de los CISO preguntados en un estudio de **Group-IB** lo consideran uno de los grandes riesgos, junto a la incertidumbre macroeconómica y el clima geopolítico (ambos con un 92%). Eso sí, destacan que pueden aprovechar la IA defensiva para contrarrestar la IA adversaria. De cualquier forma, según el estudio, la compañía detectó más de 26.800 registros en la Dark Web, en mayo de 2023, procedentes cuentas de ChatGPT. La razón para que este número sea tan alto es que cada vez más empleados usan el *chatbot* para su trabajo, ya sea desarrollo de software o comunicaciones comerciales. Un empleo que hace que ChatGPT almacene el historial de consultas de los usuarios y las respuestas de la IA, exponiéndolo en caso de acceso no autorizado, como ya ha pasado, sobre todo por parte de grupos cibercriminales, como **Raccoon.**

CISOs frente a GenAI

Para impulsar la ciberprotección frente a la IA Generativa (GenAI), representada en productos como ChatGPT, la compañía **Team 8** ha publicado el documento 'Generative AI and ChatGPT Enterprise Risks', dirigido a los CISO, para facilitar la adopción de medidas que reduzcan los riesgos que se está adquiriendo por el despliegue de sistemas con GenAI.



A modo de guía, en él se plantean diferentes recomendaciones que los responsables de ciberseguridad pueden acometer para mejorar la protección respecto al uso de *chatbot* con IA. Así, entre otras acciones, se plantea la necesidad de elaborar cuestionarios para los responsables de cada área en los que respondan quién está usando la IA y para qué propósito, así como qué protección tienen los datos cuando se interactúa con *chatbots* y otros softwares con IA.

También, se recuerda que los riesgos asociados con GenIA son manejables siempre que se cuente con una política a medida para la organización, con la colaboración de las partes interesadas relevantes. Además, identifica en cuatro los riesgos de usar esta tecnología en el mundo corporativo: sus efectos en las operaciones y procesos internos, la necesidad de confiar la seguridad de terceros, los retos legales y regulatorios derivados de su adopción, así como los riesgos de la fuga de datos generados, en ocasiones, "de forma innecesaria".

Frente a ellos, el informe aconseja "identificar aquellos relevantes y sus impactos para la organización, establecer políticas organizacionales sobre cómo y quién puede usar estas herramientas creadas específicamente para GenIA, de manera que mitiguen la posible amenaza a niveles aceptables, elegir proveedores de IA apropiados en función de la seguridad y la personalización de políticas que ofrecen a los clientes, por ejemplo, la exclusión voluntaria y retención de datos y, también, tener claras algunas alternativas de IA similares, pero bajo el control de la empresa".

En el documento no falta el recuerdo a los peligros que supone la IA en cuanto a la cadena de suministro. El aumento de los riesgos de subcontratación puede clasificarse en tres categorías amplias: dependencia de la seguridad de terceros al procesar información empresarial, dependencia del control de calidad de terceros al producir contenido y código e integración con tecnologías GenAI.

Políticas específicas

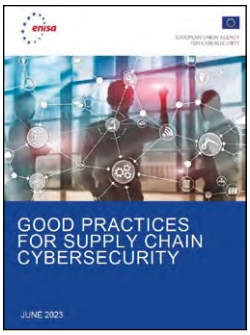
"Desafortunadamente, muchos CISO se han encontrado detrás de la curva de adopción de GenAI y corren el riesgo de ser vistos como bloqueadores comerciales en lugar de habilitadores. Por lo tanto, pueden sentirse presionados para permitir la inteligencia artificial generativa, en general, pero hacerlo de manera indiscriminada podría crear un riesgo irracional", lamenta el documento.

Por ello, también plantea que "el rol de CISO necesita evolucionar para adaptarse a los nuevos riesgos empresariales, especialmente, considerando el desarrollo de la regulación en esta área", recordando que, en el contexto de la ley de IA de la UE, ya en su última fase, algunos han descrito a los CISO como 'Embajadores de confianza'.

Es decir, se reconoce a este tipo de profesionales como "un catalizador para desarrollar un enfoque más amplio del riesgo, que incluye un énfasis adicional en la recopilación de datos, el uso, la gobernanza y las infraestructuras". También aconseja, para entender el rango de potenciales ataques, consultar la 'Taxonomía simple' del **Berryville Institute for Machine**, con ejemplos detallados de los potenciales incidentes. Ello permitirá adoptar "políticas dedicadas" centradas en IA y *machine learning* (ML), "para cubrir varios tipos de tecnologías y servicios de terceros que pueden ser consumidos en la compañía". ■

Enisa analiza los riesgos de la cadena de suministro de TIC/OT, de los que existe concienciación pero no cuentan con los recursos adecuados

Gran parte de los operadores de servicios esenciales y digitales europeos carecen de presupuestos y roles específicos para evitar los ataques a sus proveedores

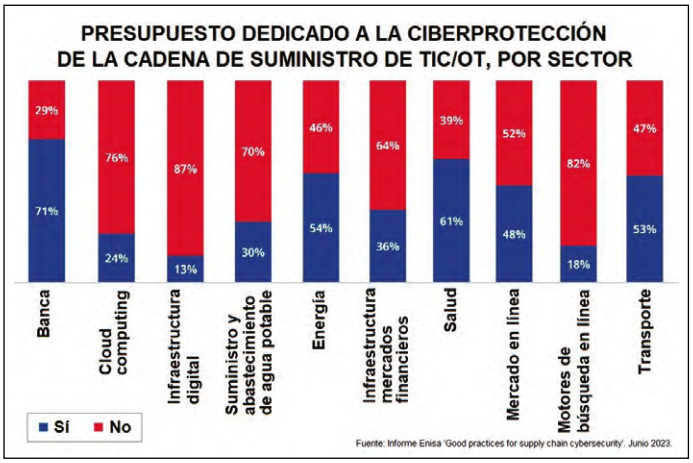


Los ataques a terceros continúan creciendo en número y complejidad. De hecho, a principios de año se produjo lo que la compañía **Mandiant** considera que podría ser el primer caso de un 'ataque doble' a la cadena de suministro de software. Se trata de la explotación de una vulnerabilidad en la herramienta DesktopApp del fabricante **3CX**, que se produjo en marzo como consecuencia de un compromiso anterior, afectando a más de 600.000 empresas, incluidas marcas como American Express, BMW, Air France, Toyota e Ikea.

Este hecho ponía sobre la mesa una vez más la importancia de la gestión de riesgos de terceros, así como "el creciente interés de los grupos cibercriminales de llevar a cabo este tipo de ataques como vector de infección inicial para comprometer y propagarse por un amplio abanico de organizaciones". Así lo destaca la **Agencia de Ciberseguridad de la Unión Europea** (Enisa) en un informe sobre 'Buenas prácticas de la cadena de suministro de ciberseguridad', publicado en junio, en el que analiza este gran desafío.

El documento subraya la magnitud de las amenazas a la cadena de suministro de TIC/OT en Europa, a partir de los resultados de una encuesta realizada entre abril y junio de 2022 a 1.081 a operadores de servicios esenciales (banca, energía, salud, transporte, etc.) y proveedores de servicios digitales (nube informática, mercados en línea y motores de búsqueda en línea), de los 27 estados miembro, y su relación con diferentes tipos de proveedores (como fabricantes, distribuidores, integradores, MSP y proveedores de servicios de computación en la nube).

Entre sus hallazgos más reveladores y preocupantes destaca que, en el 66% de los ataques, los proveedores no sabían cómo habían sido comprometidos o carecían de transparencia al respecto. Agravando el problema, el estudio también resalta que dichos ataques no solo se dirigen a empresas, sino también a repositorios de código abierto conocidos, como NPM, Python y RubyGems. Y es que, "estas plataformas, debido a su uso generalizado y naturaleza abierta, son susceptibles a actividades maliciosas, incluida la inyección de *malware*, que a menudo pasa desapercibida durante un período prolongado", según explica el estudio.



Concienciación sin recursos

Eso sí, de las organizaciones encuestadas, el 86% había implementado políticas de seguridad relacionadas con terceros en la cadena de suministro de TIC/OT. De acuerdo con el informe, el sector bancario podría considerarse como el más maduro en este ámbito (98%), seguido del de Salud (93%), el de Energía y del de Transporte (ambos con un 92%).

No obstante, a pesar de la existencia de políticas de ciberseguridad, Enisa también encontró que más de la mitad (53%) no dispone de un presupuesto asignado para esta área, frente al 47% que sí lo tiene. El sector bancario vuelve a estar a la cabeza, con el mayor porcentaje de presupuestos dedicados, seguido de Salud, Energía y Transporte.

Para la Agencia, estos datos denotan que, "aunque las organizaciones entienden la importancia de la seguridad de la cadena de suministro de TIC y OT, no asignan recursos a este ámbito. Incluso cuando invierten en proyectos de ciberseguridad en este sentido, la mayoría lo hace sin estructuras corporativas claras de gobierno". Tal es así, que el 76% no tiene funciones ni responsabilidades dedicadas a ello.

Además, destaca que, incluso, "la clasificación de un incidente de la cadena de suministro como tal es engorrosa debido a la falta de criterios concretos".

Certificaciones, la vía más elegida para mitigar riesgos

La Agencia también se interesó por los procedimientos o técnicas de mitigación de riesgos de terceros que poseen los operadores de servicios esenciales y digitales participantes. En este caso, las certificaciones de seguridad de los proveedores fue la forma más adoptada (61%). Asimismo, un 43% recurría a servicios de calificación de seguridad y el 37% a debida diligencia o evaluaciones de riesgo. Junto a ello, también señala que el 52% tiene una política rígida de parcheo, en la que, como mucho, el 20% de sus activos no están cubiertos. Sin embargo, existe un 13,5% de las organizaciones que no tiene visibilidad del parcheo del 50% o más de sus activos de información.

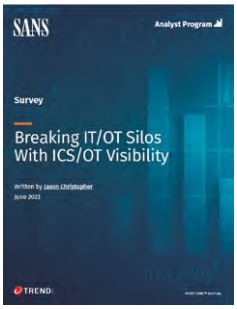
De cualquier forma, la criticidad de los ataques a terceros es tal que cerca del 40% de los directores ejecutivos de las organizaciones encuestadas manifestaron sufrir impactos adversos debido a un incidente relacionado con sus proveedores externos. Asimismo, más de la mitad (58%) mostró su preocupación por que sus socios sean menos resistentes que su propia organización, prediciendo que esto influirá sustancialmente en su enfoque de la ciberseguridad en el futuro.

Buenas prácticas propuestas

Enisa también propone en el documento una serie de buenas prácticas que deben cubrir las entidades que forman parte de la cadena de suministro de productos y servicios de TIC/TO, desde la producción hasta el consumo. Además, sugiere llevar a cabo un 'Ciclo de gestión de riesgos específico'. Un aspecto esencial ya que, "la mayoría de las organizaciones encuestadas no cuentan con un programa de gestión de vulnerabilidades que cubra todos los activos de la organización", según apunta a raíz de los datos analizados. En dicho ciclo de vida recomienda apostar por la evaluación de riesgos, la gestión de relaciones con proveedores que ayude a administrar la cadena de suministro con políticas, procedimientos y acuerdos que aborden los riesgos relacionados, la gestión de vulnerabilidades para comprender dichos riesgos y la implementación de parches en función de una política de mantenimiento bien definida, así como la calidad de los productos y servicios que debe medirse y mejorarse de forma continua. ■

La detección, el inventario de activos y la gestión de identidades se consideran capacidades prioritarias, según el Instituto Sans

La falta de visibilidad, capacitación y comunicación, principales barreras para alinear las operaciones de seguridad de TI y OT en entornos industriales

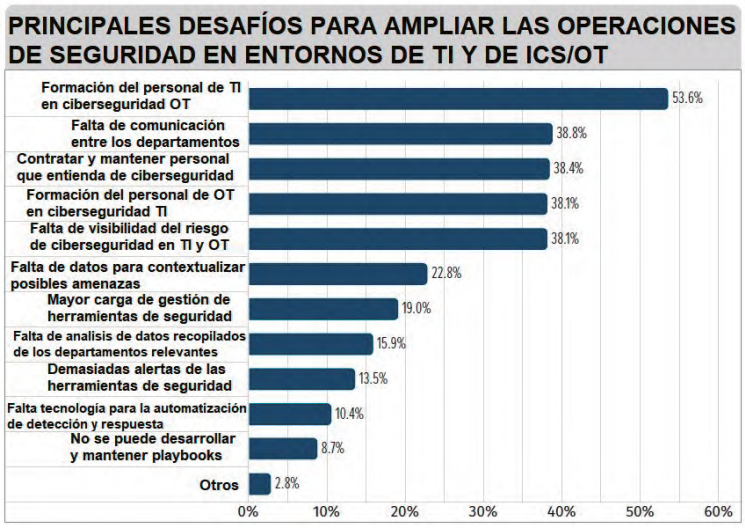


Los ciberataques dirigidos al sector industrial han crecido de forma exponencial durante la última década. Ante ello, muchas organizaciones están ampliando las capacidades de sus centros de operaciones de seguridad (SOC) a los dominios OT. El problema es que, en dicho proceso, existen grandes desafíos relacionados con la falta visibilidad, así como de habilidades y dotación de personal, que impiden una adecuada identificación, detección y respuesta de amenazas.

Así lo ha destacado el **Instituto Sans** a raíz de los resultados obtenidos de su reciente informe 'Breaking IT/OT Silos With ICS/OT Visibility', realizado en colaboración con **Trend Micro**. Se trata de una investigación que contó con la participación de cerca de 350 responsables de seguridad de TI y OT de sectores tan críticos como el de energía, TI, ingeniería y fabricación, y en la que explora cómo estos profesionales abordan los obstáculos que surgen para ampliar la visibilidad de los activos en entornos ICS/OT, evitar los silos entre TI y OT, así como incrementar su grado de madurez.

Entre sus hallazgos, el estudio subraya que la mitad de los encuestados cuentan con un SOC que incluye algún nivel de visibilidad de ICS/OT. Sin embargo, "incluso en las áreas donde las capacidades de SOC de TI y OT se están fusionando, la visibilidad aún es incompleta". Por ejemplo, mientras que el 80% dijo que su SOC cuenta con capacidades de monitorización para los activos de TI de su ICS, que incluyen interfaces hombre-máquina (HMI), estaciones de trabajo y sistemas de planificación de recursos empresariales (ERP), solo el 50% afirmó tener capacidades similares para sus activos OT, como controladores lógicos programables (PLC), sensores y unidades terminales remotas (RTU).

Eso sí, a medida que los sectores industriales continúen con su transformación digital y se avance hacia la Industria 4.0, las líneas entre TI y OT seguirán desdibujándose. En este sentido, ante la pregunta sobre qué capacidades deberían integrarse, los participantes se decantaron, principalmente, por la detección de ciberincidentes (63,6%), seguida por el inventario de activos (57,3%), la gestión de identidades y accesos (57%), el análisis de eventos cibernéticos (55,6%), así como la gestión de amenazas y la inteligencia (51%), entre los cinco primeros.



Barreras en la convergencia TI-OT

Si bien hay beneficios notables de alinear algunas partes de los programas de seguridad de TI y OT, la investigación también recuerda que existen muchas barreras para conseguirlo. El mayor desafío en la alineación de las operaciones de seguridad de TI y OT está relacionado principalmente por las personas (51,2%), muy por encima de los procesos (28,4%) y la tecnología (18,6%).

De hecho, cuatro de las cinco principales trabas destacadas por los encuestados para ampliar las operaciones de seguridad en ambos entornos están relacionadas con los empleados. Más de la mitad (54%) mencionó la falta de capacitación en OT para el personal de TI como la principal limitación para mejorar SecOps, mientras que más de un tercio (38%) dijo que el de OT también carecía de formación en TI.

Además, el 39% indicó que los silos de comunicación entre departamentos contribuyen al bajo nivel de colaboración entre los responsables de TI y OT. Asimismo, un 38% destacó la necesidad de contratar y mantener a los empleados con conocimientos de ciberseguridad.

Desafíos para una adecuada visibilidad de los activos

Junto a ello, existen grandes desafíos que impiden disponer de visibilidad en todo el entorno ICS/OT. El primero de ellos recae en las limitaciones tecnológicas de los dispositivos y redes heredadas (44,8%). Y es que, "muchos de estos entornos tienen tecnología con décadas de antigüedad cuyas capacidades siempre estarán limitadas, en cuyo caso los profesionales de la seguridad deben centrarse en optimizar dentro de esas limitaciones o aprovechar otras fuentes de datos para detectar anomalías", señala la investigación. A ello, se le une el problema de que el personal de TI no comprende los requisitos operativos de OT (39,6%), además de que las tecnologías de seguridad de TI tradicionales no están diseñadas para sistemas de control y causan interrupciones en entornos OT (37,2%).

Cerrando la brecha

A pesar de estos problemas, los responsables de seguridad son conscientes de que esta falta de visibilidad entre sus entornos de TI y OT es crítica y están redoblando sus esfuerzos. Según la investigación, de los encuestados que no tenían visibilidad de ICS/OT en su SOC (o un SOC independiente específico de OT), el 67% indicó que tenía planes para incluir estas capacidades. Además, el 76% de aquellos usan una solución de detección y respuesta de punto final (EDR) y el 70% de los que se benefician de las herramientas de monitorización de seguridad de red (NSM) tiene pensado implementarlas en dispositivos OT en los próximos dos años.

Y es que, "la convergencia de TI y OT ya está impulsando la transformación digital para muchas organizaciones industriales, pero para gestionar eficazmente el riesgo en estos entornos, las operaciones de seguridad de TI y OT (SecOps) también deben converger", destacan los responsables del informe. ■

Por capacidades, los MSSP son unos de los servicios más demandados seguidos de GRC y consultoría, entre otros

El mercado continúa reorganizándose, aunque muy alejado de las cifras de compras y fusiones de los años anteriores

Con la apuesta por la transformación digital y la popularización de entornos híbridos impulsados por el teletrabajo, la ciberseguridad se ha convertido en un activo crítico con una demanda continua. Por ello, su mercado continúa muy activo buscando ofrecer más capacidades y encontrar nichos que permitan obtener un valor diferencial a las empresas. De cualquier forma, en un reciente artículo de análisis de **TechCrunch** se recuerda que, en el último año, la inversión en seguridad cibernética ha caído muy por debajo de los máximos históricos registrados hasta ahora. Una buena prueba de ello es que las compañías del sector recaudaron 2.436 millones de euros en el primer trimestre de 2023, muy alejados de los 5.800 millones del mismo periodo en 2022, con una caída del 58%. Sin embargo, a pesar de estas cifras también se recuerda que "los inversores siguen siendo optimistas. La explosión de los grandes modelos de lenguaje y la IA generativa tiene entusiasmados a muchos con el potencial de la tecnología en ciberseguridad. Otros creen que la necesidad de proteger la nube y los dispositivos conectados, junto con una caída en las valoraciones, hace que ahora sea el momento perfecto para invertir".

Por ello, es especialmente interesante el análisis publicado por el digital británico **Securityweek,** firmado por **Eduard Kovacs,** editor gerente de la publicación. En él, destaca que entre el 1 de enero y el 30 de junio, se anunciaron 214 acuerdos de fusiones y adquisiciones (M&A) relacionados en este ámbito. Unas cifras muy ilustrativas si se comparan con las de 2022, cuando se registraron 455 transacciones, 234 en la primera mitad de año, registrando un descenso importante. "La mayoría de los acuerdos anunciados en la primera mitad de 2023 involucraron a empresas en los EE.UU., lo que no es sorprendente si se tiene en cuenta que es más probable que las empresas en este país celebren acuerdos de fusiones y adquisiciones como parte de una estrategia de expansión o salida".

Crecimiento en Asia

Por zonas geográficas, América del Norte y Europa continúan a la cabeza en número de operaciones, aunque el análisis también destaca el crecimiento en Asia, con 26 transacciones anunciadas en la primera mitad de 2023, en comparación con las 29 de todo el año pasado, aunque lejos de las 42 de 2021, muchas de ellas relacionadas con compañías israelíes, que continúan siendo uno de los principales motores de acuerdos de fusiones y adquisiciones en la región, junto con las originarias de India, Emiratos Árabes Unidos y Singapur.

Por países, el más activo en este ámbito ha sido EE.UU. seguido del Reino Unido, lo que se mantiene estable en los últimos tres años, con Canadá, Alemania y Australia complementando el 'podio a 5'. Resulta curioso cómo otras naciones están ganando protagonismo como es el caso de Suecia que, en el primer trimestre de este año, superó a Canadá y Alemania, con una docena de fusiones y adquisiciones que involucraron a empresas del país.

En cifras, en el primer semestre, se conocieron 30 acuerdos financieros por un valor de casi 4.600 millones de euros, muy lejos de los 39 que se produjeron el año anterior por más de 46.000 millones, con una media de 56,8 millones por operación.

Precisamente, por montante, las grandes firmas de capital privado lideraron las principales operaciones con casos tan destacados como la compra por parte de **Thoma Bravo** de **Magnet Forensic,** por 1.172 millones de euros, **Francisco Partners** que se hizo con **Sumo Logic** por 1.500 millones, y **Crosspoint Capital Partners** que pagó por **Absolute Software** 784 millones. "De hecho, las firmas de capital privado estuvieron involucradas en 20 de las fusiones y adquisiciones del primer semestre de este año, más que el total anual de 2022 o 2021. En una cuarta parte de los casos, las compañías de inversión adquirieron proveedores de servicios de seguridad administrados (MSSP)", destaca Kovacs, quien también recuerda que "de todos los acuerdos anunciados en el primer semestre de 2023, 82 involucraron MSSP", una cifra ligeramente superior a los 66 de la primera mitad de 2022.

El análisis también destaca que, en cuanto a servicios de gobernanza, gestión de riesgos y cumplimiento (GRC), se mantienen en número respecto a los anunciados en el primer semestre de 2022, al igual que los acuerdos que involucran a proveedores de soluciones de identidad.

También se resalta, por tipos de servicios, la bonanza de capacidades para gestión de riesgos, la evaluación y las pruebas de penetración, ya que están presentes en más de 30 acuerdos.

Igualmente, el informe constata una "caída significativa" en las operaciones sobre seguridad de redes y protección de datos, respecto al año pasado, cuando fueron la segunda y cuarta categoría en fusiones y adquisiciones cayendo este año a la novena y décima posición, respectivamente, en el primer semestre. Frente a ello, se han incrementado las operaciones de compañías que ofrecen servicios de consultoría de seguridad, con 17 adquisiciones anunciadas en el primer semestre, más del doble de la primera mitad de 2022 y casi tanto como todo ese año. ■

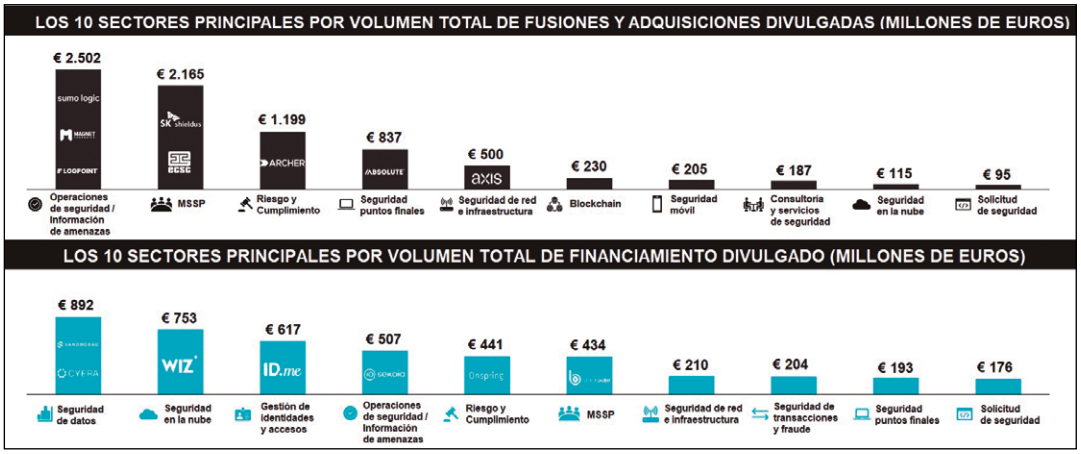
Se ha registrado el primer 'decacornio', compañía *startup* que supera los 10.000 millones de dólares de valoración

Los inversores buscan operaciones de valor, aunque en 2023 las negociaciones se dilatan por la gran diferencia entre lo que estiman pagar y lo que las empresas consideran que valen

"La primera mitad de 2023 experimentó una desaceleración continua en la actividad financiera y de fusiones y adquisiciones cibernéticas, siguiendo una tendencia que persistió durante todo 2022. Dicho esto, las acciones públicas en este ámbito se han recuperado considerablemente desde principios de año, lo que indica una estabilización en las valoraciones tras de una fuerte caída. En general, el 'conservadurismo' debería persistir durante el resto del año, aunque recientemente los compradores de capital privado se han vuelto más agresivos". Así lo ve el socio director, **Eric McAlpine**, de la compañía **Momentum Cyber,** especializada en el asesoramiento estratégico en operaciones económicas en ciberprotección y que, regularmente, ofrece un completo informe sobre el mercado. Eso sí, su conclusión es positiva: "en general, esperamos que la actividad estratégica comience a recuperarse notablemente en la segunda mitad de 2023 y en 2024".

El informe, con más de 150 páginas y abundantes gráficos de interés, destaca que en la primera mitad de este año se anunciaron 130 acuerdos de fusiones y adquisiciones, por valor de más de 8.100 millones de euros, con una inversión media por operación de 80 millones de euros. A estas cifras hay que añadir otras 423 de ampliación de capital, en las que las empresas consiguieron recaudar casi 4.800 millones de euros, sumando un total de 533 por casi 13.000 millones. Por ello, el informe destaca que "la ciberseguridad sigue siendo uno de los sectores tecnológicos más activos en los mercados público y privado".

Así, entre las operaciones que supusieron cifras más elevadas destacaron la compra de **SK Shieldus** por **EQT Partners** por algo más de 2.000 millones de euros, **Sumo Logic** por **Francisco Partners** por casi 1.500 millones de euros, **Magnet Forensics** por **Thoma Bravo** por poco más de 1.100 millones y **Absolute Software** por **Crosspoint Capital** por 802 millones.



Los más activos

Por sectores, los más activos en fusiones y adquisiciones en el primer semestre de 2023 fueron los de consultoría y servicios de seguridad (30), MSSP (19), SecOps / IR / Threat Intel (15) y gestión de identidades y accesos (14). Eso sí, este último apartado fue, en montante económico, uno de los que más dinero acaparó con casi 2.756 millones de euros, en torno al 17% del total.

En cuanto a operaciones de financiación, los que más fondos aglutinaron fueron los de Riesgo y Cumplimiento (80), Seguridad de Datos (58), SecOps / IR / Inteligencia de Amenazas (42) y Gestión de Identidades y Accesos (41),

Como dato curioso, se registró el primer 'decacornio' en ciberseguridad –empresas que valen diez veces lo que las denominadas 'unicornios: 10.000 millones de dólares–. Se trató de la compañía de origen israelí **Wiz** que, con una recaudación de 300 millones superó esa barrera en valoración.

Tecnologías de mayor interés

El informe también recuerda que, según lo mostrado en la Conferencia RSA, los temas en protección cibernética que están despertando mayor interés son los que incluyen tecnologías de uso y protección con IA, los que permiten 'hacer más con menos en un entorno económico incierto", y el cada vez mayor interés por la gestión segura de datos, activos e identidades. Además, se recuerda que los inversores buscan oportunidades de valor, aunque, en muchas ocasiones, las expectativas de valoración "de muchos fundadores y ejecutivos de *startups* siguen siendo más altas que las ofertas actuales, lo que provoca períodos de negociación más largos".

Tendencia ascendente

En definitiva, "el hielo se está derritiendo en los mercados cibernéticos estratégicos a medida que se acelera el interés por las próximas inversiones y fusiones y adquisiciones. Si bien vimos cerrar un puñado de transacciones 'premium' en el primer semestre de 2023 para empresas centradas en SSE, ITDR, CSPM y GenAI, esperamos ver un mayor volumen y una actividad de fusiones y adquisiciones y financiación mucho más proactiva en todo el mercado 'ciber' en la segunda mitad de este año. Incluye AppSec, DSPM, AI Security, SSE y, como siempre, servicios de seguridad. Suponiendo que no se produzcan más *shocks* en los mercados públicos, tenemos la esperanza de esta segunda mitad también traiga consigo el inicio de una tendencia ascendente sostenida en la actividad de transacciones para 2024 y más allá", resumió como conclusión del informe su director general, **Dino Boukouris.** ■

Comforte AG: Innovación segura a través de la seguridad centrada en los datos

Los métodos tradicionales de ciberseguridad que se enfocan en proteger infraestructuras y redes están demostrando ser inadecuados para proteger datos sensibles; un enfoque más eficaz es proteger los datos directamente. Aplicar una filosofía de protección centrada en los datos los protege frente al acceso no autorizado al dejarlos sin significado y permite el crecimiento y la innovación, al garantizar su uso seguro para operaciones y análisis comerciales. Durante más de 20 años, comforte AG ha sido líder en seguridad de datos, especializándose en la protección de sistemas de misión crítica. La plataforma de comforte de seguridad de datos ofrece sólidas capacidades de descubrimiento, clasificación y protección utilizando tecnologías de preservación de la privacidad. Esta estrategia centrada en los datos garantiza y mejora el cumplimiento, tiene una reducción del riesgo gracias al uso seguro de los datos y un menor impacto de las brechas.

Hoy, los enfoques de ciberseguridad centrados en la seguridad de infraestructuras y redes ya no son suficientes para defenderse del espectro de las amenazas cibernéticas modernas. Afortunadamente, cada vez más personas se están dando cuenta de la efectividad de la seguridad centrada en los datos, que realmente protege la información sensible de peligros como el robo o la exposición, y también fomenta la innovación a través del uso responsable de dichos datos.

A diferencia de los métodos convencionales que protegen solo las infraestructuras, este enfoque los protege directamente, asegurando su **confidencialidad, disponibilidad y exactitud**. Aquí, exploramos los beneficios de esta estrategia y cómo la **Plataforma de Seguridad de Datos de comforte** puede ayudar a las organizaciones a alcanzarlos.

Adoptar la seguridad centrada en los datos: una decisión inteligente para CISOs y CIOs

La seguridad centrada en los datos tiene en cuenta los dos retos principales: las limitaciones de la prevención de brechas tradicional y el delicado equilibrio entre su acceso seguro y su usabilidad. Esta aproximación aborda estos desafíos empleando una estrategia de confianza cero y privacidad primero. Los datos confidenciales se pueden reemplazar con *tokens*, manteniendo flujos de trabajo sin interrupciones y mitigando los riesgos. Esto proporciona una sólida última línea de defensa, ya que hace que la información protegida carezca de significado para los usuarios no autorizados.

Para explicar la *tokenización* a través de una analogía, consideremos el proceso en un casino donde se intercambia dinero por fichas para jugar. Estas fichas son únicas para cada casino y se administran de forma centralizada, lo que permite un control y una auditoría totales. No tienen ningún valor fuera del casino, pero dentro de ese ecosistema, representan su dinero, permitiendo sus actividades sin ninguna restricción.

Así como la introducción de fichas revolucionó la industria de los casinos, el enfoque de seguridad centrado en los datos revoluciona la forma en que las organizaciones abordan la protección de datos.

Capacidades de la plataforma de seguridad de datos de comforte

La Plataforma de Seguridad de Datos de comforte ofrece las siguientes capacidades principales:

1. **Descubrimiento y clasificación de datos:** localiza de forma automática y continua los datos sensibles en toda la organización, escaneando los entornos. Al mapear datos en toda la organización, los usuarios obtienen información sobre las relaciones de datos, los niveles de sensibilidad y las medidas de seguridad.
2. **Protección de datos:** métodos como la *tokenización* y el cifrado preservan el formato y protegen los datos confidenciales dondequiera que estén, lo que los hace utilizables para el procesamiento y el análisis.
3. **Habilitación de análisis de datos seguros y conforme al marco legal vigente**: realiza análisis de datos con confianza, abarcando sin problemas los modernos ecosistemas de datos, incluidos los entornos de nube y las colaboraciones con terceros.

Otras funcionalidades

Otras funcionalidades incluyen **una gama de algoritmos ajustados** para cumplir con los requisitos de cada elemento y así alinear las estrategias de protección con las necesidades específicas del negocio; **Políticas de seguridad configurables** para lograr el equilibrio adecuado entre protección y utilidad; **Arquitectura flexible, elástica y autorreparable** para una fácil escalabilidad y adaptación a los nuevos requisitos; **Integración de control de acceso y auditoría** con la infraestructura de IAM para una administración centralizada y una aplicación coherente de las políticas de seguridad; S**oporte para enfoques actuales de CI/CD DevOps** que integran seguridad en sus herramientas (SaC) como parte del ciclo de vida del desarrollo de software; **Opciones de integración flexibles**, incluidos interceptores inteligentes y potentes APIs que admiten múltiples idiomas y *scripts*; **Capacidades de integración listas para usar** que permiten la implementación de la protección de datos sin necesidad de realizar cambios en las aplicaciones del cliente.

Este enfoque brinda beneficios significativos para las empresas en tres áreas principales:

1. **Análisis de datos**: las capacidades de preservación de formato e integridad referencial permiten a las empresas operar con datos protegidos para diversos casos de uso y flujos de trabajo operativos.
2. **Estrategia en la nube**: un enfoque de protección “Trae Tu Propio Cifrado” (BYOE), que ofrece varios beneficios como el envío de datos protegidos, la reducción de la dependencia de los proveedores de servicios.
3. **Desarrollo de nuevas aplicaciones**: integración optimizada de la privacidad y la seguridad en los flujos de trabajo de los desarrolladores de software desde el principio, en lugar de tratarlo posteriormente.

Es esencial destacar que la seguridad centrada en los datos elimina la idea errónea de que su protección y su utilización es imposible o un desafío inmenso, especialmente para las organizaciones proactivas y con visión de futuro.

Reconociendo la imposibilidad de prevenir todos los ciberataques, un enfoque centrado en la seguridad en los datos demuestra ser más efectivo para prevenir infracciones, promover el crecimiento del negocio, el cumplimiento normativo y la mitigación de riesgos. ■

Ricardo Escrivà Ferrer
Iberian Country Manager
comforte AG

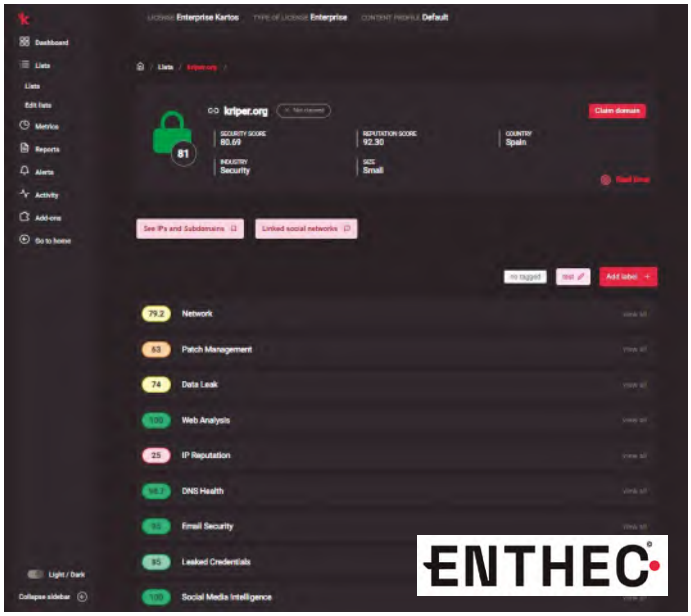
KARTOS de ENTHEC: plataforma para el hallazgo de toda la información de las compañías que no saben que tienen accesible y podría usarse en un ciberataque

Kartos es una plataforma de Ciberinteligencia desarrollada completamente en España que emula la búsqueda de información que realizan los cibercriminales en Internet, Deep Web y Dark Web durante las primeras fases de un ataque. Esa información se entrega a las empresas para que puedan mejorar sus sistemas de protección con información extremadamente precisa que no conocían. Está totalmente automatizada, por lo que funciona de forma continua y es estrictamente no intrusiva lo que la convierte en una herramienta de referencia para la monitorización de la cadena de suministro y terceros.

Las empresas cada vez son más conscientes de la importancia que tiene el perímetro externo en la defensa de sus organizaciones. Es imposible crear una estrategia de protección completa si no se tiene toda la información. Y aunque en lo referente al interior del perímetro es posible disponer de una información exhaustiva, estructurada y constante de lo que está ocurriendo, en lo que se refiere a lo que ocurre fuera de su perímetro (incluidos los terceros con los que se relaciona) esto ha sido hasta ahora algo casi imposible de conseguir.

La propuesta de Kartos viene a solucionar este problema ya que proporciona a las empresas toda la información que tienen expuesta y accesible en Dark Web, Deep Web e Internet y Redes Sociales, categorizada y estructurada de forma que puedan tomar las medidas de remediación o mitigación que estimen necesarias de manera inmediata, antes de que los Cibercriminales puedan encontrarla y utilizarla para efectuar un ciberataque, un ataque reputacional, un daño legal o cualquier otra actividad delictiva relacionada con propiedad intelectual o información confidencial.

La información se estructura en nueve categorías: Red, Gestión de Parches, Documentos Filtrados, Salud de DNS/Phishing, Reputación IP, Seguridad de email, Seguridad Web, Credenciales Filtradas y Redes Sociales, consideradas desde el punto de vista de la Ciberseguridad y la detección de amenazas. Sobre el funcionamiento y las posibilidades de esta herramienta de Ciberinteligencia, es importante destacar varios aspectos que son relevantes a la hora de considerar su utilización frente a otras alternativas:



1. Funciona de manera totalmente automatizada, lo que en la práctica quiere decir que la monitorización se realiza de forma continua y en tiempo muy cercano al real. Es cierto que muchos equipos de ciber realizan este tipo de tareas con personal dedicado y combinando diversos tipos de herramientas y desarrollos propietarios que aportan una información muy valiosa. Pero son enormes las diferencias en la capacidad y la sencillez de la configuración y las búsquedas, la cantidad y calidad de la información recogida, el número de horas invertidas por las personas del equipo, y la rapidez en la que se encuentra cualquier brecha, que se reporta al sistema de forma casi inmediata, lo que permite minimizar el tiempo de exposición.

2. Es común hablar de la cantidad de falsos positivos que ofrecen herramientas de este tipo, y que hacen que muchas veces su uso sea farragoso y poco útil. En el caso de Kartos, la plataforma de Ciberinteligencia incorpora varios motores de Inteligencia Artificial, cada uno con un propósito diferente. Uno de ellos está entrenado para extraer el contexto de las empresas que monitoriza, aprendiendo de la información que encuentra. De esta forma se reduce enormemente el número de falsos positivos haciendo que la información que se entrega sea extremadamente precisa. Además, incorpora funcionalidades adicionales que permiten al usuario o gestor configurar la herramienta para añadir información al contexto y eliminar datos que no sean relevantes o exactos.

3. Es una herramienta estrictamente no intrusiva, lo que permite la monitorización continua y constante de las terceras partes sin necesidad de llenado de formularios o los condicionantes y autorizaciones legales que se necesitan para realizar determinadas acciones de comprobación de los estándares de Ciberseguridad en empresas externas, lo que aumenta la objetividad de los resultados y el acceso a la información real.

Kartos es una plataforma de CiberInteligencia y Ciberseguridad, orientada a la remediación y mitigación de amenazas en el menor tiempo posible. Reúne en un solo interfaz las capacidades de detección de problemas en Superficie Externa de Ataque (en el sentido más amplio posible, ya que incluye la Cadena de Suministro), Riesgo Digital (ya que permite detectar y acceder todos los activos digitales expuestos y accesibles) y el Scoring de Riego para la priorización de tareas.

Dentro de su agresivo plan de desarrollo, está previsto el lanzamiento de nuevas funcionalidades en próximos meses. Entre ellas se incluyen una potente plataforma de búsqueda específica de información, la monitorización del grado de cumplimiento en lo que respecta a exposición de información y riesgo de estándares de cumplimiento (como la ISO 27.001 o PCI) y la posibilidad de monitorización exhaustiva de la información y datos confidenciales pertenecientes a personas VIPs de las compañías usuarias de la plataforma. ■

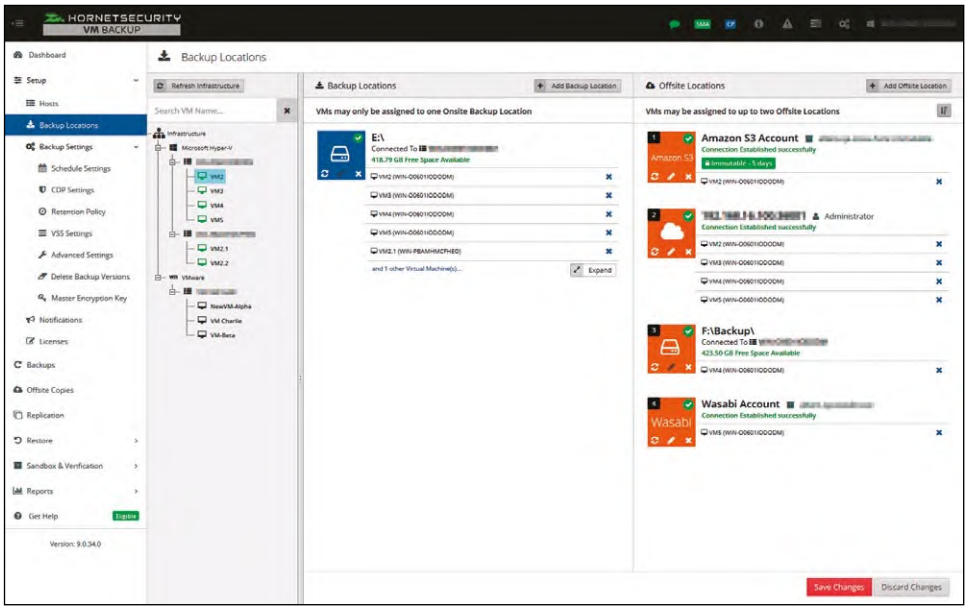
Lola Miravet González
COO
ENTHEC SOLUTIONS

VM Backup de Hornetsecurity: La importancia de elegir una solución de respaldo adecuada

Elegir una buena solución de *backup* es fundamental para poder garantizar la integridad y disponibilidad de los datos de los sistemas y la continuidad del negocio. A medida que aumenta el número de ciberataques, cada vez más empresas se convierten en el principal objetivo de los ciberdelincuentes que buscan acceder a datos confidenciales. En este contexto, y según nuestro reciente Informe de Ciberseguridad (elaborado anualmente por nuestro laboratorio de seguridad, Hornetsecurity Lab), casi seis de cada 10 ataques de *ransomware* tienen su origen en correos electrónicos maliciosos o ataques de *phishing*.

Lo que hace que los ataques de *ransomware* sean especialmente lucrativos para los ciberdelincuentes es el hecho de que, según nuestro estudio de 2022 sobre esta tipología de ataques el **9,2% de las víctimas acaban pagando el rescate**. Mientras los ciberdelincuentes se benefician de esto, los costes del tiempo de inactividad, la pérdida de datos y los rescates pagados pueden alcanzar fácilmente **un millón de euros** para las empresas objetivo.

Aún más preocupante es el hecho de que, de acuerdo al anterior estudio, hasta el **15% de los ataques de *ransomware*** tenían como objetivo específico las copias de seguridad. Esto pone de relieve la necesidad de soluciones de respaldo resistentes para máquinas virtuales Microsoft Hyper-V y VMware.



Dentro del contexto de ciberataques actual y del marco regulativo, es importante tener en cuenta los siguientes aspectos:

- **Protección de Datos**: Una solución de *backup* debe ser confiable y asegurar que los datos estén protegidos frente a pérdidas, daños o borrados accidentales. Los fallos de hardware, errores humanos o ataques cibernéticos pueden ocurrir en cualquier momento y debemos minimizar el riesgo de pérdida de información.
- **Cumplimiento normativo**: Que nos permita adaptarnos a los marcos legislativos de nuestra empresa y cumplir esquemas regulativos presentes y futuros (NIS2).
- **Continuidad de Negocio y Recuperación ante Desastres**: Dado que los datos son uno de los activos más importantes de la empresa, su propiedad intelectual, debemos garantizar que en caso de caída de un sistema o de un ataque de *ransomware* la solución de *backup* podrá contribuir a mantener la continuidad del negocio al permitir una rápida recuperación y minimizar las interrupciones.

Dicho lo anterior, al considerar elegir una solución, se debe tener en cuenta del mismo modo:

1. Que sea adaptable a nuestra estrategia de copia de seguridad, posibilitando una estrategia de copia de seguridad 3-2-1-1, que amplía la capacidad de acceder a una **copia intacta y totalmente recuperable** de sus datos cuando se produce un desastre.
2. **Replicación en WAN** para poder disponer de un tiempo de recuperación (RPO) mínimo.
3. **Facilidad de la recuperación** que permita una **implementación rápida y sencilla.**
4. **Seguridad de las copias,** garantizando la posibilidad de disponer **protección contra *ransomware*** que garantice que los datos no son borrados ni encriptados.
5. **Escalabilidad y compatibilidad**, que pueda adaptarse al crecimiento de nuestro negocio y de nuestros sistemas, incluyendo posibilidad de ***backup* de sistemas** en nube como puede ser **Microsoft 365.**
6. **Monitorización y notificación de eventos** que ocurran en nuestros respaldos y restauraciones y que nos permitan conocer el estado de estos sin necesidad de acceso al sistema de *backup*.
7. **Pruebas y restauraciones** que permitan verificar la integridad de nuestras copias de seguridad.
8. **Soporte Técnico**, verificando que siempre vamos a disponer de la ayuda necesaria en caso de necesitarla, en cualquier horario.

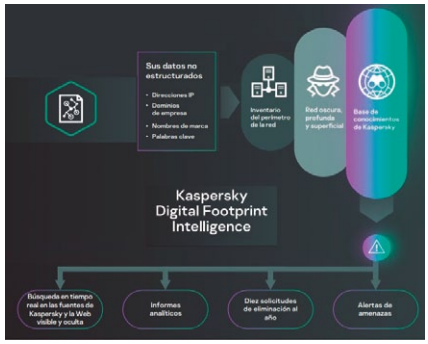
Una de las mejores soluciones en este sentido es VM Backup de Hornetsecurity. La propuesta combina **flexibilidad, fiabilidad** y potentes funciones de copia de seguridad que permiten al usuario crear fácilmente copias de seguridad de máquinas virtuales Hyper-V y VMware, ofreciendo protección contra *ransomware* mediante el **Almacenamiento Inmutable en la nube**, deduplicación en línea aumentada para reducir el almacenamiento, una plataforma de gestión centralizada, replicación optimizada para WAN y protección continua de datos.

Las copias de seguridad están protegidas con almacenamiento inmutable en la nube, lo que significa que los datos no pueden ser borrados ni modificados por nadie durante un tiempo determinado. El uso de espacio de almacenamiento en la nube inmutable proporciona protección adicional para las copias de seguridad existentes. ■

Manuel Achaques
Responsable de Preventa Iberia, Italia y Latam
HORNETSECURITY
achaques@hornetsecurity.com

KASPERSKY ACTUALIZA VARIAS DE SUS SOLUCIONES INCREMENTANDO SUS CAPACIDADES FRENTE AL *PHISHING* Y EN LOS PUNTOS FINALES

Kaspersky ha llevado a cabo una importante actualización de varias de sus propuestas, destacando aquellas para la protección de la huella digital de las empresas y de seguridad para pymes, como son **Digital Footprint Intelligence** y **Endpoint Security Cloud Pro.**



Con la primera, la compañía busca ofrecer una respuesta a los más de 500 millones de intentos de acceso a sitios web fraudulentos, descubiertos por sus analistas en 2022. Para ello, ha incluido en su herramienta Digital Footprint Intelligence capacidades de rastreo, detección y eliminación de cuentas falsas en Facebook, Snapchat, Instagram y Twitter, así como de aplicaciones falsas publicadas en *marketplaces*, como App Store y GooglePlay, donde los cibercriminales intentan apropiarse de marcas de confianza para realizar estafas. Frente a ello la solución permite a las empresas defenderse de estas amenazas rastreando fuentes públicas en Internet, proporcionando información detallada sobre posibles actividades maliciosas realizadas en su nombre. De hecho, a principios de año, el servicio se mejoró con la integración de alertas en tiempo real para Targeted Phishing, que puede detectar webs de *phishing* contra marcas o servicios en línea.

Protección de *endpoints*

Kaspersky, también ha mejorado su solución Endpoint Security Cloud Pro, aumentando la protección de los puntos finales para las pymes. Entre sus novedades más notables destacan la incorporación de análisis de causa-raíz (*root-cause*), *cloud discovery,* bloqueo de datos y capacitación para administradores de TI.

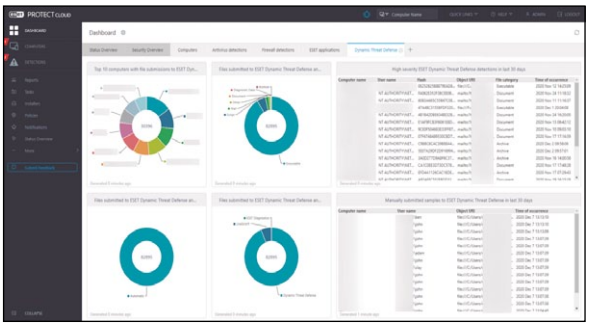
Junto a ello, ha actualizado su **Kaspersky Anti Targeted Attack Platform** (KATA) y **Kaspersky Endpoint Detection and Response Expert** (KEDR Expert), permitiendo ahora configurar Windows en el *sandbox* para adaptarse mejor a la infraestructura del cliente para que "combatir los enlaces y archivos maliciosos sea más sencillo", apuntan sus responsables. Asimismo, gracias a una mayor personalización de la herramienta es posible configurar el nombre de la cuenta del usuario, el idioma del sistema (inglés/ruso), instalar aplicaciones, etc.

Además, para mejorar el rendimiento de la solución KEDR Expert, ha integrado capacidades EDR en Kaspersky Endpoint Security para Linux y para Windows, respectivamente. "La telemetría e información recopilada por EDR se puede enviar a sistemas de terceros a través de API, lo que proporciona más eficiencia para los sistemas de empresas SIEM, SOAR o XDR ya existentes", explican desde la compañía.

KASPERSKY
www.kaspersky.es

ESET REFUERZA, A TRAVÉS DE ONTINET.COM, LA PROTECCIÓN PARA LOS SERVIDORES AWS

Ontinet.com, distribuidor exclusivo de **Eset** en España, ha desarrollado una protección avanzada para los servidores en la nube de Amazon Web Service. **Eset Amazon Web Service**, busca así dar respuesta a la necesidad de proteger la información en los servidores *cloud* de Amazon. Se



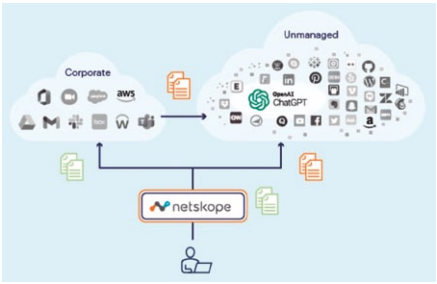
trata de una solución "fruto de la necesidad de un cliente que acudió a nosotros para que protegiéramos la información que alojaba en los servidores en la nube de Amazon" destaca su director de servicio técnico y servicios, **Raül Albuixech**, añadiendo que, "en ese momento, nuestros programadores iniciaron el proceso de desarrollo de lo que ha acabado siendo Eset Amazon Web Service, una solución que ofrece la protección que nuestro cliente estaba buscando y que amplia nuestro portafolio".

En concreto, el producto refuerza la seguridad de las instancias EC2, servidores virtuales en la nube, y los *buckets* de S3, unidades de almacenamiento, a través del análisis de todos los documentos que se suben al servidor de AWS en busca de *malware* antes de almacenarlos, rechazando los que están infectados, manteniendo a salvo los datos y permitiendo una protección avanzada contra cargas maliciosas y archivos no deseados.

ONTINET
https://ontinet.com
ESET
https://www.eset.com/es

NETSKOPE INCORPORA A SU PORTAFOLIO MAYOR SEGURIDAD DE APLICACIONES DE IA GENERATIVA, COMO CHATGPT

Los riesgos que entrañan el uso, cada vez mayor, de aplicaciones como ChatGPT, está provocando que, en la actualidad, un 10% de las organizaciones bloquen su uso. Así lo recoge **Netskope** que, para evitarlo, ha desarrollado una solución de protección de datos para ayudar a las empresas a gestionar de forma segura el uso por parte de los empleados de ésta y otras aplicaciones de Inteligencia Artificial (IA) generativa, como Google Bard y Jasper.



La compañía ofrece a través de su **Zero Trust Engine**, como parte de su plataforma **Intelligent Security Service Edge** (SSE), capacidades para la habilitación segura de estas aplicaciones, entre las que destaca mayor visibilidad a través de una nueva categoría web especialmente creada para identificar dominios de IA generativa, que permite a los equipos configurar políticas de control de acceso y protección en tiempo real, así como gestionar el tráfico específico en estas aplicaciones.

También, incluye control avanzado de acceso, con la capacidad de supervisar, permitir o bloquear los datos confidenciales de la empresa (como el código fuente) para que no se publiquen en *chatbots*. Junto a ello, ofrece protección avanzada de datos, con la capacidad también de supervisar y permitir o bloquear publicaciones y cargas de archivos a los *chatbots*, así como soporte para el cumplimiento normativo del RGPD, CCPA y HIPAA, entre otras legislaciones.

NETSKOPE
https://www.netskope.com/es

ZSCALER AMPLÍA SU PLATAFORMA ZERO TRUST EXCHANGE CON SERVICIOS PARA IDENTIFICAR, MITIGAR Y GESTIONAR ATAQUES A GRAN ESCALA

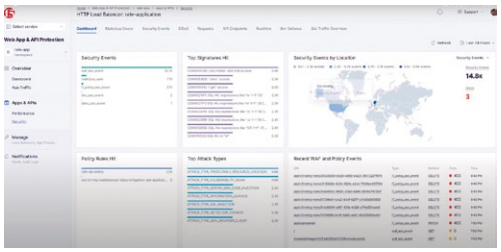
Zscaler ha puesto en marcha cuatro servicios aumentando las capacidades de su plataforma **Zscaler Zero Trust Exchange**. La compañía mejora así la supervisión y remediación de ataques sofisticados, además de ofrecer un planteamiento nuevo para conectar de forma segura oficinas y sucursales.

Por un lado, destaca su **Risk360**, que se presenta como una potente herramienta de remediación de riesgos a través del cálculo y visualización de los mismos. Para ello, ofrece su cuantificación en tiempo real, en todas las fases de los ataques, así como visualización en cuatro tipos de elementos: personal, terceras partes, aplicaciones y activos. Asimismo, bajo el nombre de **Zero Trust Branch Connectivity**, la compañía ha presentado otro servicio con el que busca eliminar el desplazamiento lateral de las amenazas, ofreciendo conectividad Zero Trust impulsada por IA/ML, desde las sucursales hasta el centro de datos y los entornos multi nube. Entre otras características, permite reemplazar, a través de capacidades de Confianza Cero, las VPN de punto a punto y las conexiones MPLS, mejorando la protección de los usuarios, las aplicaciones y los datos.

Con **Zscaler ITDR,** la firma ofrece, además, la posibilidad de reducir el riesgo de ataques de identidad gracias a la visibilidad continua, la supervisión de riesgos y la detección de amenazas. Para ello, cuantifica el riesgo, descubre configuraciones erróneas, ofrece monitorización en tiempo real y busca evitar la escalada de privilegios, además de proporcionar una guía de reparación de problemas, entre otros aspectos. Por su parte, su propuesta **ZSLogin**, agiliza y facilita la labor de los administradores de TI reforzando la seguridad con una gestión centralizada de privilegios, autenticación multifactor sin contraseña y la gestión automatizada de identidades de administrador, entre otros.

ZSCALER
www.zscaler.com

TELEFÓNICA TECH Y F5 LANZAN UN SERVICIO PARA DETECTAR AMENAZAS Y VULNERABILIDADES, EN TIEMPO REAL, EN LAS APLICACIONES



Telefónica Tech y **F5** han ampliado su alianza con el lanzamiento del nuevo servicio gestionado **Defensa de Aplicaciones Web** (WAD), que está basado en SaaS y desplegado sobre la plataforma *cloud* distribuida de F5 (F5 Distributed Cloud).

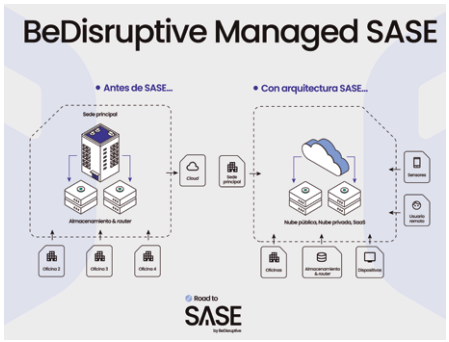
La solución permitirá a los clientes empresariales de Telefónica Tech detectar amenazas y vulnerabilidades en tiempo real combinando la recopilación masiva de telemetría con reglas programables, inteligencia artificial y aprendizaje automático. En particular, está destinada a proteger las aplicaciones corporativas desde un único panel de control, independientemente de dónde estén desplegadas: en las instalaciones del cliente, en múltiples nubes o en el *edge.*

El servicio está reforzado, además, por el equipo del Centro de Operaciones de Ciberseguridad (SOC) de la operadora, que da soporte y monitoriza los entornos en la nube durante las 24 horas y 365 días del año. Este respaldo incluye la clasificación de problemas de alta gravedad, la investigación de alertas y la provisión de recomendaciones de corrección. Cabe destacar, asimismo, que el nuevo servicio incluye las capacidades de F5 de Cortafuegos de Aplicaciones Web (WAF), *bot defense*, seguridad de APIs, así como mitigación de ataques de Denegación de Servicio Distribuido (DDoS).

"El despliegue de WAD en la Plataforma de Nube Distribuida de F5 añadirá velocidad a una capa de seguridad crítica, al tiempo que proporcionará flexibilidad a nuestros clientes empresariales para desplegar, asegurar y operar aplicaciones en un entorno multinube donde sea necesario: en el centro de datos, despliegues híbridos o a través de múltiples nubes", ha resaltado el director de marketing de producto de Ciberseguridad de la teleco, **Juan Campillo**. "Nuestra asociación va mucho más allá de proporcionar una plataforma tecnológica, y seguiremos apoyando a Telefónica con esfuerzos de habilitación y comercialización tanto en EMEA como fuera de ella", ha añadido la vicepresidenta de SP Managed Services en F5, **Mariana Agache.**

TELEFÓNICA TECH
https://telefonicatech.com
F5
www.f5.com/es_es

BEDISRUPTIVE CREA MANAGED SASE PARA OFRECER GESTIÓN UNIFICADA, VISIBILIDAD Y PROTECCIÓN EN EL ACCESO A LOS RECURSOS EN LA NUBE



A pesar de la gran acogida que están experimentando las estrategias SASE (Secure Access Service Edge), en las que Gartner pronostica una adopción del 80% para 2025, frente al 20% de 2021, la transición puede resultar un desafío para muchas organizaciones, debido a su complejidad. Consciente de esta problemática, **BeDisruptive** busca facilitar el camino a las empresas a través de su **Managed SASE**, una solución gestionada que incluye capacidades Managed SSE (Security Service Edge) y DDR (DNS Detection & Response). Con ella, ofrece "gestión unificada y plena visibilidad convergiendo los mejores productos de seguridad en una única solución SASE gestionada, sin necesidad de tener un único proveedor, desplegada en la nube e integrada con las soluciones actuales del cliente, ya sean SaaS, PaaS, etc.", comentan desde la compañía.

Entre sus ventajas más notables, según BeDisruptive, está su flexibilidad, ya que permite el acceso directo a la red o la nube desde cualquier lugar, facilitando la adopción de nuevos modelos de negocio digitales. Además, también pretende reducir la complejidad, a través de la consolidación de servicios en un modelo en la nube que elimina una gran variedad de soluciones heredadas y simplifica el esfuerzo operativo. A ello se suma que ofrece un mayor rendimiento al mejorar y acelerar el acceso a los recursos de Internet mediante una infraestructura de red global, optimizada para baja latencia, así como alta capacidad y disponibilidad.

Además, cuenta con capacidades de Zero Trust Network Access (ZTNA), seguridad frente amenazas, como *phishing*, *malware*, *ransomware* y acciones internas malintencionadas, así como de protección de datos, tanto dentro como fuera de la organización (incluyendo nubes públicas, así como entre instancias personales y empresariales en aplicaciones *cloud*), y una gestión y aplicación de políticas centralizadas, entre otros aspectos notables.

BEDISRUPTIVE
www.bedisruptive.com/es

DELINEA REDUCE EL RIESGO DE *PHISHING* CON POLÍTICAS PRECONFIGURADAS EN PUESTOS DE TRABAJO

Delinea ha presentado la actualización de su **Privilege Manager**, su solución para proporcionar controles de elevación de privilegios para usuarios y aplicaciones en estaciones de trabajo. Las últimas mejoras facilitan significativamente su uso, al preconfigurar varias de las políticas de elevación de privilegios más comunes a través del marco Workstation Policy Framework. El objetivo es, entre otros, minimizar a las compañías las posibilidades de sufrir ataques de *phishing*.

Así pues, la compañía incluye en el Workstation Policy Framework cinco medidas para poder construir, de forma rápida, una base para gestionar los controles de acceso privilegiado y crear una línea seguridad fundamental en las estaciones de trabajo de Windows y Mac, sin interrumpir la productividad de los usuarios.

En concreto, las medidas que se introducen como políticas preconfiguradas son la protección contra el *malware*, evitando que los ataques Living Off the Land Binaries and Scripts (LOLBAS) sean ejecutados por 'aplicaciones padre' comúnmente explotadas, así como permitir que se ejecuten los instaladores de aplicaciones del catálogo de seguridad firmado por Microsoft. También, ha creado una política que se dirige a los procesos comunes del sistema de soluciones de desarrollo de software, incluidos los procesos secundarios, y minimiza los retrasos causados por la solicitud de elevación de privilegios. Además, cuenta con una directiva que aprueba previamente y eleva de forma silenciosa cuatro instaladores definidos de Microsoft Visual Studio y otra centrada en capturar intentos de elevación de aplicaciones, en aquellas que no son de Microsoft.

Cabe destacar, junto a todo ello, que los clientes de Delinea pueden comparar sus políticas con este marco e introducir las que falten en sus entornos. Además, Privilege Manager proporciona un control granular sobre la capacidad de añadir, modificar o eliminar usuarios en estaciones de trabajo, a través de PowerShell, incluso en sesiones PowerShell con privilegios totalmente elevados.

DELINEA
https://delinea.com/es

WATCHGUARD AUTHPOINT TOTAL IDENTITY SECURITY REFUERZA LAS CAPACIDADES DE PROTECCIÓN DE LAS IDENTIDADES CON MFA, MÁS INTELIGENCIA Y FACILIDAD DE USO

Bajo el nombre **AuthPoint Total Identity Security**, **WatchGuard** ha dado a conocer un completo *bundle* que combina la galardonada autenticación multifactor (MFA) AuthPoint, con capacidades de monitorización de credenciales en la Dark Web, y un gestor de contraseñas corporativas. Este nuevo producto, junto con las políticas *zero trust* basadas en riesgos de la arquitectura Unified Security Platform de la compañía, permite a los proveedores de servicios gestionados (MSP) proporcionar una ciberseguridad avanzada desde WatchGuard Cloud.

A través de dicha solución, la compañía ofrece el Servicio AuthPoint MFA, proporcionado en WatchGuard Cloud, para facilitar la configuración y gestión de métodos de verificación en línea y fuera de línea, y políticas de acceso en los puntos finales, VPNs y aplicaciones web, así como la configuración de portales de aplicaciones de inicio de sesión único en múltiples despliegues de clientes. También, destaca el Servicio de Monitorización de la Dark Web, con el que notifica a los clientes cuando se encuentran credenciales comprometidas de hasta tres dominios supervisados en bases de datos de brechas de credenciales recién adquiridas.

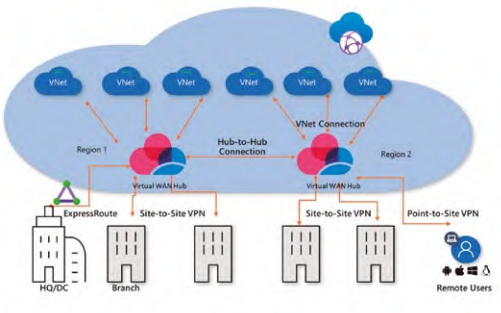
Cade destacar también, su gestor de contraseñas con el que impone un estándar más alto para las contraseñas y ayuda a reducir la frecuencia de las solicitudes de restablecimiento de las mismas. "No es necesario recordarlas, ya que se almacenan de forma segura en el almacén y están protegidas por la contraseña compleja y exclusiva de cada usuario, lo que garantiza que sólo ellos puedan descifrar y acceder a las credenciales que contienen", afirman desde la compañía. Así pues, cuando los usuarios necesitan acceder a sus *apps*, pueden recuperar sus contraseñas utilizando la aplicación móvil AuthPoint para iOS y Android, y/o la extensión del navegador para autocompletar las credenciales para una experiencia general de inicio de sesión único más fluida.

WATCHGUARD TECHNOLOGIES
www.watchguard.com/es

CHECK POINT AMPLÍA SU CORTAFUEGOS EN LA NUBE PARA ASEGURAR LA WAN VIRTUAL DE MICROSOFT AZURE A TRAVÉS DE UNA PROTECCIÓN CENTRALIZADA

Check Point ha integrado de forma nativa su cortafuegos en la nube de próxima generación (NGFW), **CloudGuard Network Security**, con **Microsoft Azure Virtual WAN**, con lo que busca proporcionar una prevención avanzada de amenazas y seguridad de red de varias capas en nubes públicas, privadas e híbridas, permitiendo a las empresas migrar a Azure con mayor confianza y eficiencia operativa.

Cabe recordar que Microsoft Azure Virtual WAN es un servicio de red de Microsoft que, entre otras características, permite a sus clientes simplificar las funcionalidades de red, seguridad y enrutamiento para impulsar la escalabilidad, el ahorro de costes y un mayor rendimiento. Con dicha integración, Check Point pretende mejorar y complementar la seguridad de Azure Virtual WAN, ofreciendo una protección centralizada.



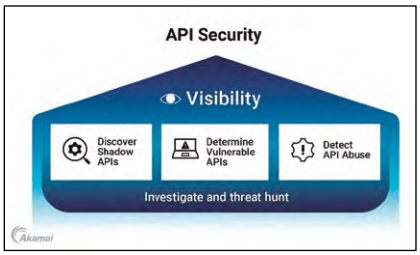
Para proporcionar protección, CloudGuard ofrece prevención de amenazas avanzada impulsada por capacidades de cortafuegos, IPS, Control de Aplicaciones, IPsec VPN, Anti-Virus and Anti-Bot, DLP, así como Extracción de Amenazas (Threat Extraction), con la que protege de manera proactiva contra amenazas conocidas y desconocidas contenidas en documentos mediante la eliminación de contenido explotable, además de Emulación de Amenazas (Threat Emulation) frente a los ataques de día cero.

Asimismo, cabe destacar que CloudGuard está diseñado acorde a los principios de la nube de elasticidad, disponibilidad, resiliencia y soporte continuo para el crecimiento del tráfico, y se implementa de forma sencilla en el centro de Virtual WAN desde el *marketplace* de Azure Marketplace. Además, se integra con Azure Routing Intent para la inserción de seguridad: "una forma centralizada más simple, rápida, consistente y escalable de asegurar redes de múltiples radios", puntualizan desde la compañía.

CHECK POINT
www.checkpoint.com

AKAMAI CREA API SECURITY PARA PROTEGER LAS API DEL ABUSO EMPRESARIAL Y EL ROBO DE DATOS

Bajo el nombre de **API Security**, **Akamai** ha desarrollado un producto para detener los ataques dirigidos a la interfaz de programación de aplicaciones (API) y detectar el abuso empresarial dentro de las API. La compañía buscar reducir los ataques contra ellas, que en 2022 batieron récord, según su más último informe sobre el Estado de Internet. Uno de los mayores problemas de los ataques dirigidos a estos entornos es que, una vez que la API recibe la autorización de una aplicación web y un producto de protección de API, los equipos de seguridad dejan de tener visibilidad sobre su uso dentro de la organización, según destaca la compañía.



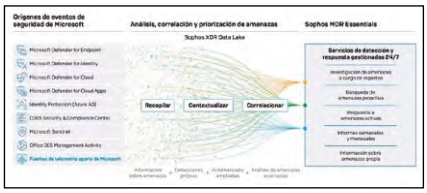
Para evitarlo, esta solución proporciona una visibilidad completa de la actividad de las API, utilizando análisis de comportamiento para detectar amenazas complejas además de mejorar las detecciones mediante el análisis de los datos históricos almacenados de forma exclusiva en un lago de datos.

En definitiva, con esta propuesta busca ofrecer detección, visibilidad y auditoría de riesgos de API, además de capacidades de detección y respuesta que facilitan la investigación completa y la búsqueda de amenazas. Con la ayuda del servicio gestionado de búsqueda de amenazas Shadow Hunt, API Security envía señales de aprendizaje automático a analistas humanos para que las investiguen. Además, API Security complementa a su herramienta App & API Protector (AAP).

AKAMAI TECHNOLOGIES
www.akamai.com/es/es

SOPHOS PRESENTA SU SOLUCIÓN MDR PARA MICROSOFT DEFENDER

Sophos ha presentado **Managed Detection and Response (MDR) para Microsoft Defender**, un servicio gestionado que proporciona las capacidades de respuesta a amenazas avanzadas para empresas que utilizan Microsoft Security. Este producto añade una capa crítica de protección 24/7 a través de la suite Microsoft Security para puntos finales, SIEM, identidad, nube y otras soluciones, para protegerlas contra el *ransomware* y el robo de información, entre otros ciberataques.



Para ello, integra telemetría de una amplia gama de herramientas de seguridad de Microsoft, "a diferencia de otras ofertas de MDR que limitan la compatibilidad con Microsoft Defender para Endpoint o Microsoft Sentinel y ofrecen capacidades mínimas de respuesta a amenazas", explican desde la compañía. Dicha telemetría se consolida, correlaciona y prioriza automáticamente con información del Ecosistema de Ciberseguridad Adaptativa de Sophos y la unidad de inteligencia de amenazas Sophos X-Ops, formada por más de 500 analistas de seguridad, expertos en búsqueda de amenazas, equipos de respuesta ante incidentes, científicos de datos y otros especialistas de Sophos en todo el mundo.

SOPHOS
www.sophos.com/es-es

CISCO OPTIMIZA SU SOLUCIÓN DE XDR AÑADIENDO LA RECUPERACIÓN AL PROCESO DE RESPUESTA

Cisco ha mejorado su solución de detección y respuesta extendida (XDR, Extended Detection and Response), **Cisco XRD**, añadiendo la recuperación al proceso de respuesta. Con ello, la compañía "redefine las demandas de sus clientes brindando una recuperación casi en tiempo real para las empresas tras un ataque de *ransomware*", según sus responsables.

Con el lanzamiento de esta herramienta en la Conferencia RSA de este año, Cisco proporcionó a las organizaciones mayores capacidades de telemetría y visibilidad en la red y los terminales. Ahora, "al reducir a casi cero el tiempo entre el comienzo de un ataque de *ransomware* y la captura instantánea de información crítica para el negocio, Cisco XDR respalda aún más esa visión y mejora de forma notable su Security Cloud: una plataforma de seguridad unificada, impulsada por IA y entregada en la nube", explican desde la empresa. Así, con las nuevas funcionalidades de Cisco XDR, los equipos de los SOC podrán detectar, realizar instantáneas y restaurar automáticamente los datos críticos para el negocio ante los primeros signos de un ataque de *ransomware*, a menudo antes de que se mueva lateralmente a través de la red.

CISCO
www.cisco.com/c/es_es

SUSE DESARROLLA NUEVAS CAPACIDADES PARA SU PLATAFORMA LINUX INSIGNIA

Suse ha presentado nuevas capacidades en la última versión de **Suse Linux Enterprise 15 Service Pack 5** (SLE 15 SP5), diseñada para ofrecer informática de alto rendimiento para cargas de trabajo de IA/ML, además de haber ampliado sus funciones de parcheo 'en vivo'.

SUSE anunció la última versión en su evento SUSECON en Munich, junto con un nuevo informe en el que afirma que más del 88% de los equipos de TI han informado al menos un incidente de seguridad en la nube durante el año pasado.

Para dar solución a estos problemas, la firma está mejorando su paquete de seguridad de infraestructura para que los clientes, socios y comunidades de código abierto puedan ejecutar de forma segura sus cargas de trabajo de aplicaciones en la nube, el *edge* y los centros de datos.

Entre otros aspectos destacados está su capacidad para brindar privacidad a los entornos de nube y de *edge* con computación confidencial, que permite a los clientes ejecutar máquinas virtuales completamente cifradas para proteger el procesamiento de datos en dichos entornos.

La infraestructura de SAP también se ha asegurado con descubrimiento automático y observabilidad total de servidores, instancias de nube, bases de datos de SAP HANA, SAP S/4HANA, aplicaciones y clústeres de NetWeaver.

SUSE
www.suse.com

grupo ica
Sistemas y Seguridad

EVOLUCIONA

HACIA UNA CIBERSEGURIDAD PROACTIVA CON EL SERVICIO AYUNTAMIENTOS SEGUROS

Elige el pack que más se adapta a tus necesidades

PACK A PROTECCIÓN Y RECUPERACIÓN - DETECCIÓN Y RESPUESTA	PACK B DETECCIÓN Y RESPUESTA AVANZADA
• Protección frente a amenazas conocidas y desconocidas. • Protección y recuperación frente a malware, ransomware, phishing, cryptomining. • Recuperación de información y archivos dañados o perdidos tras un ataque. • Sin importar desde dónde trabajes o a qué red te conectes. • Compartición de información y gestión de incidentes centralizados. • Monitorización y detección de amenazas en tiempo real. • Bloqueo de conexiones sospechosas en la red. • Contención de ataques dirigidos.	• Monitorización y detección avanzada de amenazas en tiempo real. • Alerta temprana de vulnerabilidades. • Intervención experta ante incidentes de seguridad*. *(intervenciones limitadas)
¿Para quién?	***¿Para quién?***
Organizaciones con una infraestructura de red básica que necesiten proteger el puesto de trabajo de sus usuarios. *Administraciones que ya cuenten con personal informático.* *Instituciones que necesiten recuperar toda su información rápidamente en caso de ataque.*	*Organizaciones con infraestructuras de seguridad.* *Instituciones con departamentos de informática o seguridad.* *Administraciones cuya actividad requiere ciberseguridad avanzada.*

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

Los días 2 y 3 de noviembre en Santiago de Compostela

CIBER.gal convoca su III edición con la estrategia de Ciberseguridad 2030 de Galicia en el horizonte

La tercera edición del **Encontro CIBER.gal**, el evento de referencia en materia de ciberseguridad gallego, se celebrará los días 2 y 3 de noviembre en la Ciudad de la Cultura de Galicia, en Santiago de Compostela. De nuevo, será desarrollado presencialmente aunque para aquellos que no puedan acudir se retransmitirá en modalidad *online*, siempre bajo inscripción previa.

Próximamente serán publicados los detalles del mismo en la web del **Nodo CIBER.gal**, quien lo organiza a través de su entidad propulsora y fundadora, la **Amtega,** y el apoyo del Colegio Profesional de Ingenieros Informáticos de Galicia.

Así, de forma ya consolidada, el día 2 de noviembre contará en la mañana con actividades destinadas al sector público, abarcando temas como los retos y tendencias para la Administración o la ciberseguridad como prioridad del sector público gallego ante los Fondos Next Generation.

Ya a la tarde se desarrollarán actividades destinadas principalmente al tejido empresarial que contarán, entre otras, con un reconocido ponente referente en el mundo de la ciberprotección, los mitos y oportunidades de los escenarios en la nube y la convergencia entre la ciberseguridad y la IA. Ya en la segunda jornada, el día 3, abrirá de nuevo con el exitoso concurso de *Ciberseguridade no cole!*, el que alcanzó en su última edición la participación de más de 4.000 escolares de centros educativos de Galicia. Además, contará también este año con una representación teatral, y se hablará de tecnología inclusiva y las ciberamenazas de las redes sociales, entre otras. Como en ediciones anteriores, la organización brinda la oportunidad a todas aquellas entidades que lo deseen de poder apoyar la celebración del evento a través del patrocinio.

Toda la información estará disponible en la web del Nodo CIBER.gal: **https://ciberseguridadegalicia.gal/gl/cibergal/encontro-cibergal**.

El 18 y 19 de octubre en León

INCIBE celebrará el 17Enise, rindiendo homenaje al 017

El **Instituto Nacional de Ciberseguridad de España** (Incibe) celebrará su gran congreso anual para el ámbito corporativo, en León, el 18 y 19 de octubre. Los profesionales del sector, el ecosistema emprendedor, además del entorno académico e investigador se reunirán en unas jornadas que, este año, tendrán un especial foco en la colaboración y rendirá homenaje al servicio que se ofrece a través del 017 de ayuda en ciberprotección, una de las iniciativas más notables de Incibe.

Como en otras ocasiones, el objetivo de las jornadas es "propiciar un encuentro que genere oportunidad de negocio e internacionalización para la industria española de ciberseguridad, estimular el *networking* entre profesionales y proporcionar a los asistentes y expositores una experiencia de participación positiva, donde puedan establecer relaciones entre los diferentes agentes".

En la última edición, bajo el lema 'Facing the future together', el Enise contó con 75 ponentes nacionales e internacionales y la presencia de 82 *stands* comerciales e institucionales, la participación de más de 2.400 asistentes presenciales de 21 países, y más de 1.600 personas por *streaming*.

Del 3 al 5 de octubre, en Bilbao

El CCI celebrará su XXI International Experiences Congress Industrial Cybersecurity con un enfoque muy práctico

Como parte fundamental de su actividad, el **Centro de Ciberseguridad Industrial** (CCI) celebrará su 'XXI Congreso Internacional de Experiencias en Ciberseguridad Industrial 2023', en Bilbao (España), del 3 al 5 de octubre, en colaboración con el **Basque CyberSecurity Centre**, que hará de anfitrión. "Será uno de los eventos de referencia para el mercado europeo, y punto de encuentro e intercambio de conocimiento, experiencias y relaciones de todos los actores involucrados en este ámbito", destacan sus impulsores.

En esta ocasión, el enfoque del congreso será práctico, basado en casos de aplicación reales y lecciones aprendidas gestionando el riesgo de la industria digital. Permitirá a los profesionales de OT e IT, fabricantes industriales, de ciberseguridad, ingenierías, consultoras, integradores, usuarios finales y operadores de infraestructuras críticas compartir conocimiento y experiencias sobre las distintas percepciones de la realidad que hoy en día es la Ciberseguridad Industrial.

Será en formato en línea y espera tener dos presenciales cada año

El (ISC)² SPAIN CHAPTER comenzará su andadura nacional con su primera jornada en octubre

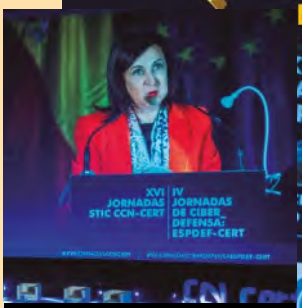
El **(ISC)² Spain Chapter**, fundado a mediados de año y presidido por **Alejandro Cardarso,** comenzará su andadura, en octubre, con la celebración de su primera jornada en formato de tarde, que abrirá Cardarso, presentando el capítulo español. Además, contará con expertos como **Diogo Donadoni** y **Roberto Santiago Martínez**, que explicarán el programa de introducción CC (Certified Cybersecurity) y profundizarán en lo que aporta el marco MITRE, así como con **Luis Miguel Quian**, que hablará sobre la 'Gestión de la resiliencia: del ciberincidente a la crisis', y **Rodrigo Cantera**, sobre seguridad en redes OT.

La iniciativa ya tiene en marcha su página web (www.isc-2chapter-spain.com), para registrarse como miembro, si se está certificado por el (ISC)², así como conocer más información de la jornada. La organización tiene como reto para 2024 celebrar dos eventos presenciales.

Del 28 al 30 de noviembre, en Madrid, también contarán con una importante representación de organismos europeos

CCN y MANDO CONJUNTO DEL CIBERESPACIO, bajo el lema 'Compartir para ganar', celebrarán las XVII Jornadas STIC, dentro de la presidencia española del Consejo de la UE

Organizadas por el **Centro Criptológico Nacional,** del **CNI,** y el **Mando Conjunto del Ciberespacio** (MCCE), del 28 al 30 de noviembre volverán a celebrarse en los cines Kinépolis en Madrid las **Jornadas STIC**, en su edición XVII por parte del CCN y la V de Ciberdefensa por parte del **ESPDEF-CERT**. Bajo el lema 'Compartir para ganar', tendrá este año un especial significado por cuanto será uno de los últimos grandes actos, en el ámbito de la ciberseguridad, dentro del marco de la presidencia española del Consejo de la Unión Europea. Además, contará con el apoyo institucional del **Departamento de Seguridad Nacional** (DSN), la **Oficina de Coordinación de Ciberseguridad** (OCC) del **Ministerio del Interior** y del **Incibe,** así como de la **Organización de Estados Americanos** (OEA), además de entidades de referencia como **RootedCON,** el **Centro de Ciberseguridad Industrial** (CCI), **Goodjob** y **Women4Cyber,** entre otras.



La Ministra de Defensa Margarita Robles inauguró las Jornadas STIC 2022

El General Rafael García Hernández (MCCE) y Luis Jiménez (CCN), coorganizadores, durante el acto inaugural en 2022

Las jornadas comenzarán el día 28, sobre las nueve de la mañana, con una conferencia magistral del jefe del Departamento de Ciberseguridad del CCN, **Javier Candau,** con el repaso de lo hecho por el organismo en 2023 y sus grandes retos para 2024.

Durante los tres días, se ofrecerán conferencias de forma simultánea en siete salas. En concreto, en el primero, la 25 se dedicará a ponencias sobre 'Amenazas y tendencias', la 18 al 'ENS y cumplimiento normativo', la 19 a 'Operaciones militares en el ciberespacio', la 20 a 'Rooted Labs' y la 16 a 'Productos y tecnologías de seguridad'.

La segunda jornada también contará con un módulo dedicado a la 'Super SOC Network', así como otro a 'Tecnologías cuánticas y Postcuánticas (Pyqtec)', además de otros, el último día, a ciberinteligencia, a control industrial, inteligencia artificial y, también, a las principales novedades en ciberseguridad 5G. Por supuesto, en gran parte de ellas habrá animadas mesas redondas y debates sobre los temas que más preocupan al sector desde las estrategias de ciberdefensa, hasta los retos de los CISO, así como conferencias de marcado carácter técnico.

Eso sí, por su 'carácter europeo' sus organizadores esperan que, a su público habitual –sector público español e iberoamericano, empresas estratégicas y compañías especializadas del sector, y ámbito universitario– se sume una importante representación de organismos europeos y profesionales del sector de la ciberseguridad de la UE.

Las jornadas finalizarán con una ponencia magistral y la clausura por parte de las autoridades, además de entregarse los 'Premios Atenea 2022'. En la última edición se contó con 11.200 asistentes, de 31 países, 4.257 de forma presencial.

El 16 de septiembre en la Ciudad de las Artes y las Ciencias

ROOTEDCON Valencia regresa con una edición llena de investigaciones novedosas

El más destacado congreso nacional de ciberseguridad técnica y uno de los más relevantes de Europa, **RootedCON**, regresa con su edición en Valencia, la octava que se realiza en la capital del Turia. Una jornada en la que los organizadores esperan reunir a más de 500 asistentes y que también contará con un día, el 15, dedicado a los denominados RootedLabs, con actividades formativas y talleres para interesados en ciberseguridad y cuyo acceso es independiente a la RootedCON, en el espacio AEDIT de la **Fundación Universidad-Empresa de la Universitat de València.**

En ellos se impartirán cursos dedicados a 'Read Team Operations', 'Mi primera revisión de directorio activo', 'Malware Threat Hunting' o 'Hacking ético de aplicaciones móviles' de la mano de profesionales reconocidos, como **Eduardo Arriols, Jorge Escabias, Roberto Amado, David Meléndez Cano, Carlos Alberca, Daniel González y Pablo González.** Cabe recordar que los Rooted Labs se desarrollarán en paralelo al programa oficial de las Jornadas. Las entradas y la información ya están disponibles en la web de RootedCON.

Por otro lado, el congreso celebrará, por primera vez en Iberoamérica, una edición allí con la 'RootedCON Panamá', del 4 al 6 de octubre. Sus responsables ya celebraron una edición internacional en Hong Kong en 2016.

LA CLAVE PILAR (LOS TELEGRAMAS SECRETOS DEL GOBIERNO CIVIL DE MÁLAGA)

Autor: Alberto Peinado Domínguez
Editorial: Umaeditorial
Año: 2023 – 175 páginas
ISBN: 978-84-1335-230-5
www.umaeditorial.uma.es

Interesante y original obra del solvente investigador malagueño de la UMA, por su especialización y profundidad sobre telecomunicaciones, criptografía y sociedad, que son analizadas desde el prisma que ofrece la ciudad de Málaga. La histórica relación que mantiene la ciudad con las telecomunicaciones constituye el contexto perfecto para el criptoanálisis de una serie de telegramas cifrados enviados o recibidos por el Gobierno Civil entre 1934 y 1940: registros domiciliarios anteriores a la Guerra Civil, el control de la prensa durante la contienda y las órdenes recibidas de la Dirección General de Seguridad en Madrid tras el conflicto. Se presenta aquí la 'Clave Pilar', utilizada en 1940.

Su recuperación, en 2018, ha supuesto un importante hallazgo criptográfico que ha ayudado a completar el catálogo de los cifrados de cinta móvil empleados en España desde finales del siglo XIX. El análisis de éstos y otros telegramas cifrados con claves similares son también, presentados y analizados, constatando la invariabilidad con el paso del tiempo, de las relaciones entre telecomunicación, criptografía y sociedad.

Además, resulta de especial interés la recopilación de muchos de los telegramas que usaron la clave Pilar, de los que se ofrecen abundantes imágenes, un aspecto que dota al libro de relevancia académica para los que trabajan en temas, como la historia de la criptografía, la ciberseguridad y las comunicaciones secretas en el ámbito militar.

CIBERINTELIGENCIA DE LA AMENAZA EN ENTORNOS CORPORATIVOS

Autor: Mario Guerra Soto
Editorial: RA-MA
Año: 2023 – 772 páginas
ISBN: 978-8419857453
www.ra-ma.es

Extensa y pormenorizada obra dedicada a la inteligencia cibernética de amenazas en la que el autor destaca el valor, para cualquier empresa, de conocer minuciosamente sus activos, su exposición, sus vulnerabilidades propias o debidas a terceros, su potencial 'explotabilidad' y el impacto que ésta supondría para la continuidad de negocio.

Mario Guerra, reconocido profesional en este ámbito, plantea así una obra, dividida en ocho capítulos, para iniciados y expertos, con la que podrán desarrollar y mejorar sus capacidades como analistas de ciberinteligencia en los niveles técnico/táctico, operacional y estratégico, a través de marcos de trabajo como el de Recorded Future o Mandiant. Eso sí, dado que la ciberinteligencia de la amenaza constituye una capacidad transversal para la organización, su lectura resultará también de enorme utilidad a sus equipos de ingeniería de detección, respuesta a incidentes, *threat hunting*, forense digital, análisis de *malware*, *Red Team* y *Purple Team,* además de a responsables de SOC y a CISO. También, resultará de interés a criminólogos, periodistas, analistas antifraude, militares y miembros de las FCSE interesados en el cibercrimen en Web 2 y Web3, las operaciones de influencia, el ciberespionaje y las operaciones militares en el ámbito del ciberespacio.

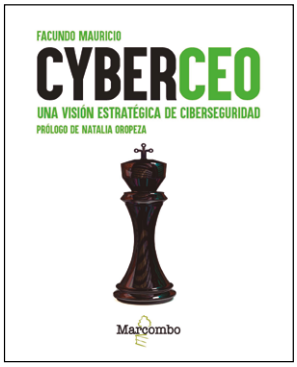
SEGURIDAD OFENSIVA EN MACHINE LEARNING. +100 PROMPTS INJECTIONS EN CHATGPT: ATACANDO Y DEFENDIENDO ORGANIZACIONES CON PROMPT ENGINEERING

Autor: Dr. Alfonso Muñoz
Editorial: Publicación independiente
Año: 2023 – 167 páginas
ISBN: 979-8399420615
www.amazon.es

El inquieto y prolífico **Alfonso Muñoz** –referente español en criptografía y temas aledaños, de la que ha impartido conferencias y publicado numerosos libros–, con esta novedad editorial en castellano, busca dar un paso más en esta disciplina para que el lector entienda la utilidad, ventajas e inconvenientes de la inteligencia artificial (IA) aplicada a la ciberseguridad. Para ello, pone foco en nuevos paradigmas y, sobre todo, en las aplicaciones prácticas de los modelos LLM (*Large Language Model*), como el popular ChatGPT. "He recopilado y organizado decenas de ejemplos, *prompt injection* y *prompt engineering*, usando más de 200 referencias de obligada lectura, para comprender de forma sencilla su utilidad real y restricciones. Espero que le resulte provechoso y le ahorre tiempo en la evaluación de esta nueva tecnología", destaca el autor.

"Llevo más de 20 años trabajando en el campo de la ciberseguridad, protegiendo organizaciones apoyándome en sinergias con disciplinas variadas y verificando (atacando) las contramedidas desplegadas. Es en este escenario donde cualquier profesional debe analizar la enorme utilidad de la IA en numerosos ámbitos de nuestra sociedad moderna, incluido la seguridad cibernética, y reflexionar sobre los riesgos inherentes de esta tecnología antigua pero vitaminada con el acceso a grandes volúmenes de información, capacidades de computación y nuevos desarrollos algorítmicos, especialmente en el campo de las redes neuronales", añade.

CYBERCEO: UNA VISIÓN ESTRATÉGICA DE CIBERSEGURIDAD

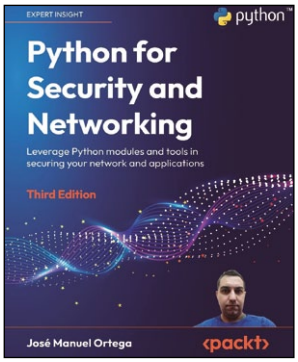


Autor: Facundo Mauricio.
Natalia Oropeza (Prólogo)
Editorial: Marcombo
Año: 2023 – 324 páginas
ISBN: 978-8426735713
www.marcombo.com

"Sencillo, pragmático y desafiante". Así define este libro su autor, con un título que aunque a priori despista, trata con solvencia centrar esta disciplina como uno de los elementos intrínsecos a la alta dirección y con el que busca ofrecer un enfoque que permita "abordar la ciberseguridad de forma estratégica, integral y cerotécnica", explica. "Dirigido a ejecutivos que delegarán el cómo, pero necesitan comprender el qué y por qué", en él ofrece un recorrido amplio con una mirada histórica del impacto de la tecnología y sus consecuencias sociales, económicas, comerciales y organizacionales. Así, en sus capítulos intenta aportar "una perspectiva estratégica, propia de los líderes que buscan comprender los conflictos y las oportunidades de la era digital". "Un futuro cada vez más conectado y complejo requiere una estrategia sólida en ciberseguridad. No se trata solo de protegerse de las amenazas, sino de maximizar las potencialidades transformadoras de la digitalización, de aprovechar la IA, el *blockchain* y las posibilidades que ofrece la ciberprotección como un diferenciador y eje innovador del mañana".

El libro, además, cuenta con una invitada de referencia como es **Natalia Oropeza,** Chief Cybersecurity Officer en Siemens, prologuista del volumen y compañera del autor en la multinacional, quien destaca la necesidad en el mundo ejecutivo de dejar de ver la ciberseguridad solo como una responsabilidad técnica y comenzar a verla también, como una oportunidad.

PYTHON FOR SECURITY AND NETWORKING: LEVERAGE PYTHON MODULES AND TOOLS IN SECURING YOUR NETWORK AND APPLICATIONS



Autor: José Manuel Ortega
Editorial: Packt Publishing
Año: 2023 – 586 páginas
ISBN: 978-1837637553
www.packtpub.com

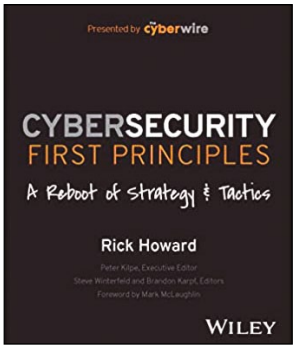
Tercera edición de esta obra con una notable actualización, tanto en nuevos capítulos como en información que, como resultado, ha sido reescrito en más del 50%, además de adaptar los *scripts* del conocido lenguaje de programación, Python, a su reciente versión 3.10. Así pues, a lo largo de este libro, de carácter técnico, el autor muestra cómo la combinación de la última versión del conocido lenguaje con un mayor enfoque en la seguridad de la red puede ayudar a mejorar las defensas contra los ciberataques.

En concreto, pretende servir de guía para construir una red segura con la ayuda de las secuencias de comandos de Python.

Para ello, ofrece amplia información de todo tipo de temas, desde la creación de una red hasta los procedimientos que debe seguir para protegerla. En su parte final, dedica un apartado a cómo crear aplicaciones seguras utilizando técnicas de criptografía y esteganografía, además de mostrar cómo proteger con este lenguaje de programación los puntos finales, entre otros aspectos de interés.

En definitiva, esta novedad editorial resultará de gran interés para ingenieros de redes, administradores de sistemas y otros profesionales de la seguridad que buscan superar problemas comunes de redes y protección con Python.

CYBERSECURITY FIRST PRINCIPLES: A REBOOT OF STRATEGY AND TACTICS



Autor: Rick Howard
Editorial: Wiley
Año: 2023 – 400 páginas
ISBN: 978-1394173082
https://onlinelibrary.wiley.com

En esta obra, **Rick Howard**, director de ciberseguridad, analista jefe y miembro principal de The Cyberwire, 'desafía' la sabiduría convencional de las mejores prácticas, estrategias y tácticas actuales de seguridad y argumenta que la profesión necesita volver al principio. Así, a lo largo del libro, muestra de manera convincente los argumentos a favor del primer principio absoluto de la ciberprotección y analiza las estrategias y tácticas necesarias para lograrlo.

La obra, además, ofrece un excelente repaso de la historia de la seguridad informática desde la década de 1960, hasta principios de la década de 2020, explicando por qué ha fallado, además de mostrar qué se debería mejorar, estrategias y tácticas que deberían adoptarse para tener mayor impacto y eficacia, así como diferentes estudios de ataques que se han producido –desde el hackeo a la empresa OPM, en 2015, hasta el de DNC, en 2016, o de Colonial Pipeline, en 2019–. A través de ello, ofrece una propuesta de cómo calcular el riesgo cibernético, tanto en grandes compañías como en medianas y pequeñas. En definitiva, se trata de un libro escrito de forma amena y que resultará de interés para los profesionales del sector en todos los niveles: desde ejecutivos de negocios hasta los sénior especializados o, incluso, los que se quieran dedicar a este ámbito y busquen las mejores oportunidades profesionales.

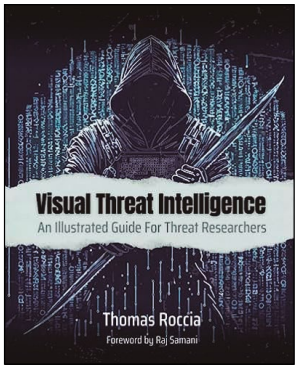
MARCO NORMATIVO DE LA UE PARA LA TRANSFORMACIÓN DIGITAL

Autor: Eloy Velasco (Coordinador)
Editorial: La Ley
Año: 2023 – 512 páginas
ISBN: 978-84-19446-36-7
https://tienda.wolterskluwer.es

Esta monografía examina el impulso regulatorio de la UE a la transformación digital de sus 27 estados miembro, promoviendo la innovación tecnológica y salvaguardando la protección de los datos personales. El resultado es un marco normativo sólido y coherente en aspectos tan transversales como la ciberseguridad, los servicios y mercados digitales, la ciberdelincuencia, la prueba digital, la identidad digital y los terceros de confianza, los criptoactivos, los medios de pago digitales, la inteligencia artificial, la privacidad y un largo etc. Este desarrollo legislativo, basado en los principios y derechos digitales en los que se enmarca, ha ayudado a fomentar la innovación y la competitividad en el mercado digital europeo, así como a proteger los derechos y libertades de los ciudadanos y las empresas.

Además, de su extensión, también destaca por su calidad con notables aportaciones de grandes especialistas como **José de la Mata**, magistrado-juez, miembro nacional de España en Eurolust; **José Luis Piñar**, catedrático de Derecho Administrativo de la USP-CEU; **Ofelia Tejerina**, abogada y presidenta de la Asociación de Internautas; **Elvira Tejada**, Fiscal de Sala del Tribunal Supremo coordinadora nacional contra la ciberdelincuencia; así como el propio **Eloy Velasco**, magistrado-juez de la Audiencia Nacional; y **Natalia Jiménez**, DPO del Canal de Isabel II, entre otros.

VISUAL THREAT INTELLIGENCE: AN ILLUSTRATED GUIDE FOR THREAT RESEARCHERS



Autor: Thomas Roccia
Editorial: Publicación independiente
Año: 2023 – 148 páginas
ISBN: 979-8373228374
www.amazon.com

Prologado por el reconocido **Raj Samani**, esta obra funciona a modo de guía mostrando los principios de la inteligencia de amenazas de forma visual y sencilla, a la vez que ofrece amplia información, con diagramas y gráficos, sobre los conceptos más complejos de este ámbito, con ejemplos prácticos.

Así, ofrece desde una buena visión de las principales motivaciones de los actores de amenazas, hasta sus metodologías de ataque más usadas, analizadas a través del ciclo de vida de la inteligencia de amenazas, el modelo diamante de análisis de intrusiones y el marco Mitre ATT&CK. También, ofrece información sobre cómo pensar como los cibercriminales, trabajar con indicadores de compromiso (IOC), y usarlo para priorizar, según el enfoque de 'pirámide del dolor', los aspectos que más exigen centrarse en ellos para lograr capacidades anticipativas a través de herramientas de inteligencia de amenazas cruciales como Yara, Sigma y MSTICpy, para rastrear *malware* y analizar datos.

No falta el análisis de algunos conocidos incidentes de los últimos años como NotPetya, Shamoon y Sunburst, con lecciones aprendidas y, también, algunos de sus aspectos más llamativos como el incremento de capacidades de los ataques para crear señales falsas para engañar a las investigaciones.

DOCUMENTOS SiC
Nº 40
SEPTIEMBRE 2023

elastic

La analítica de datos, en el corazón de la ciberseguridad

- Capacidades XDR a través del SIEM, protegiendo endpoints y nube
- Ciberprotección avanzada con un ADN innovador en IA
- Velocidad, escalabilidad y flexibilidad

María Campos
Regional VP South EMEA de Elastic

Más de 20.000 organizaciones usan su tecnología en todo el mundo

Elastic: ciberseguridad centrada en la analítica del dato con un ADN innovador en IA

Desde su fundación en el año 2012, Elastic se ha convertido en uno de los referentes mundiales en ciberseguridad con un enfoque diferenciador en la protección del dato y una propuesta transversal a través de su tecnología de búsquedas, observabilidad y la aplicación intensiva de la inteligencia artificial y el *machine learning* al SIEM, protección del punto final y la red, con orquestación y capacidades anticipativas.

Vivimos en un mundo impulsado por los datos. Ya lo decía el escritor Arthur Conan Doyle, 'padre' de Sherlock Holmes, cuando destacaba que sin datos no hay nada: es como intentar "hacer ladrillos sin arcilla". Y pocas multinacionales representan tan bien el valor de los datos en ciberseguridad como la estadounidense Elastic, uno de los grandes referentes mundiales en tecnología de búsquedas -para "que todos encuentren las respuestas que importan"-, observabilidad y, también, protección cibernética de última generación.

Su historia comenzó en 2004, en un apartamento de Londres, cuando su fundador y CEO, **Shay Banon** desarrolló un innovador motor de búsqueda para facilitarle el trabajo a su mujer, que necesitaba encontrar recetas de cocina en Internet para sus clases en la prestigiosa escuela de cocina Le Cordon Bleu. Una idea que pronto se convirtió en el corazón de una empresa, fundada en 2012, cuya tecnología permite "encontrar instantáneamente información relevante y procesable", a través de la búsqueda, la observabilidad y la seguridad en el ámbito corporativo. En definitiva, un éxito que la compañía ejemplifica con una frase que resume su objetivo y buen hacer: "Buscar. Observar. Proteger".

Reinventando la ciberseguridad

Y las cifras de negocio lo avalan. Con más de 20.000 clientes en todo el mundo y cotizando en la Bolsa de Nueva York desde 2018, Elastic superará los 80.000 millones de euros de facturación en 2023 –casi el doble que hace cinco años–, de los cuales, 23.000 millones provendrán de su negocio de ciberseguridad. Un éxito que, en el mercado de ciberprotección, se basa en una propuesta completa orientada a los requisitos de las actividades y negocios, que permite analizar grandes cantidades de datos logrando resultados relevantes, en tiempo real, para contar con capacidades proactivas de ciberprotección. Para ello, la compañía ofrece a través de su plataforma una solución escalable, en tiempo real, en una única pila de tecnología abierta que se puede implementar en cualquier lugar. "Miles de organizaciones en todo el mundo ya la usan para encontrar instantáneamente información procesable de cualquier tipo de datos y potenciar sistemas de misión crítica", recuerdan desde la organización. Este enfoque le ha permitido ganar en pocos años destacados clientes como Auchan, Booking y Airbus, en el área de búsquedas, Telefónica y Zurich en observabilidad, y Personal Capital, Proficio, Entel, el Mando de Combate Aéreo de EE.UU., NetApp y la Universidad de Oxford, entre otras, en ciberprotección. Gracias, entre otros aspectos, a lo que conlleva en eficiencia de inversión, reducción de costes y, también, velocidad a la hora de integrar soluciones

Con su plataforma unificada de búsqueda, observabilidad y ciberseguridad, Elastic brinda la posibilidad de despliegue en modo SaaS (Azure, Google, AWS...), facilitando los entornos de colaboración DevSecOps.

para unificar y optimizar los flujos de trabajo para poder bloquear ataques complejos en el menor tiempo posible.
Elastic, además, está comprometida con la transparencia y la apertura con la comunidad de ciberseguridad, "y este es el principal motivo por el que creamos y mantenemos nuestra lógica de detección de forma pública junto con todos los que estén interesados", resaltan desde la organización.

Tecnología para todo tipo de entornos

A través de una plataforma unificada de búsqueda, observabilidad y seguridad, la empresa brinda la posibilidad de despliegue en modo SaaS, en cualquier nube pública (desde Azure hasta Google y AWS) facilitando la integración, en este ámbito, de los equipos de desarrollo, operaciones y seguridad. Entre las razones de su crecimiento

La multinacional aplica la IA, de forma intensiva, a la gestión de amenazas, la capacidad de contar con alertas automatizadas y de disponer de *chatbots* de ciberprotección.

está que permite contar con altas capacidades de detección y respuesta extendidas (XDR), basándose en el SIEM, la seguridad del *endpoint* y la nube. Todo bajo una premisa: que la ciberseguridad es un problema de datos. Buena prueba de ello es que, en una de las más recientes actualizaciones de Elastic Security, se han incluido más de 1.100 reglas prediseñadas para que sus usuarios configuren y pongan en marcha sus detecciones y monitorización de protección lo antes posible. Todo ello con una apuesta decidida por la innovación y tecnologías como su Elasticsearch Relevance Engine (ESRE), su motor para la "democratización de la IA". Y es que la multinacional aplica la IA, de forma intensiva, a todas sus soluciones y, en el caso de ciberseguridad, a la gestión de amenazas, la capacidad de contar con alertas automatizadas y en disponer de *chatbots* de ciberprotección.

Reconocida por los analistas

Todo ello ha permitido que, en muy poco tiempo, su negocio de ciberseguridad experimente un crecimiento exponencial, siendo reconocida por analistas como Gartner, situándola como líder en el 'cuadrante mágico' de Insight Engines; Forrester, que la nombró líder en The Forrester Wave: Security Analytics Platforms, Q4 2022; así como IDC, que la situó como actor principal en su IDC MarketScape: Worldwide SIEM 2022 Vendor Assessment.

Elastic Security Labs: lucha contra el cibercrimen compartiendo inteligencia

Disponer de capacidades anticipativas es clave para alcanzar una ciberseguridad madura. Por ello, la compañía cuenta con una unidad especializada en ciberinteligencia denominada 'Elastic Security Labs'. Se trata de un equipo de más de 40 ingenieros de ciberprotección, profesionales e investigadores "que comen y respiran seguridad". "Es nuestra pasión", destacan desde la organización, a la vez que recuerdan que investigan temas de seguridad, *malware*, *ransomware*, tácticas, grupos de actividad, adversarios y todo lo relacionado con la seguridad cibernética. Un trabajo que plasman en informes publicados de forma habitual sobre grupos adversarios, amenazas emergentes o nuevos patrones de ataque, así como las últimas vulnerabilidades descubiertas. "Los recursos de inteligencia ante amenazas, como el 'Reporte global de amenazas de Elastic 2022', son fundamentales para que los equipos corporativos puedan evaluar sus capacidades y experiencia en la identificación y la prevención de amenazas", destacan sus integrantes de esta unidad.

Una propuesta para calcular con precisión el valor de la ciberseguridad

Elastic quiere hacer la ciberseguridad simple. Entre sus últimas iniciativas para conseguirlo destaca su 'Calculadora de valor' aplicada a la ciberprotección. Se trata de una "herramienta interactiva con la que se puede cuantificar rápido las eficiencias financieras", que la compañía ofrece a cada empresa a través de cómo mejorar "los KPI en torno al riesgo, los costes y la productividad. Los números cuentan la historia: lograr una visibilidad holística reduce el riesgo, mejora la productividad e impulsa el ahorro de costes y la recuperación de ingresos", destacan desde la organización. En definitiva, se trata de mostrar cómo desde la compañía se "ayuda a cualquier organización a descubrir algunas de esas incógnitas desconocidas con datos", explica la CISO de la empresa, **Mandy Andress**. "En Elastic, observamos el gran valor que nuestros clientes han logrado al usar nuestra tecnología. Al proporcionar esta herramienta de cuantificación, esperamos ayudarles a lograr una comprensión de cuánto valor podrían generar ellos también", recuerdan desde la multinacional que ofrece esta herramienta a través de su web.

María Campos,
Regional VP South EMEA de Elastic

Con más de dos décadas dedicadas a ciberseguridad, situándose en primera línea de grandes multinacionales, María Campos desembarcó hace un año y medio en Elastic para responsabilizarse del Sur de Europa. Un reto para el que sus habilidades de liderazgo, ventas y comprensión técnica, le están permitiendo trasladar con éxito al mercado la estrategia de una compañía que apuesta por un enfoque donde prima la protección del dato a través de una plataforma que combina la búsqueda y la observabilidad, capacidades muy demandadas especialmente en entornos de nube.

"Elastic permite encontrar entre todos los datos los que de verdad interesan y lo hace en tiempo real y a escala, sin importar su formato o ubicación"

– Cuenta con más de 20 años en ciberprotección. ¿Qué es lo que más ha cambiado y cuál será el enfoque que permitirá proteger el mundo hiperconectado y complejo al que nos aventuran la IA, el 5G, *blockchain*…?

– La ciberseguridad ha ido siempre de cómo proteger los datos, las aplicaciones, los sistemas y cómo asegurar la resiliencia del negocio. Lo que ocurre es que el contexto ha cambiado mucho: los datos, las aplicaciones, los sistemas ya no están solamente dentro de los límites de nuestras organizaciones. Vivimos en un mundo hiperconectado, que además es híbrido y multi-*cloud*. Si echamos un vistazo a todo lo que está por venir en el campo de IA, la situación se complica aún más con los llamados *adversarial attacks,* que pueden aprovecharse de engañar al comportamiento humano y hacer mejor ingeniería social. El número de dispositivos conectados sigue incrementándose exponencialmente, así como los datos generados y las propias aplicaciones. La democratización de las nuevas herramientas y su disponibilidad de acceso para todos, buenos y malos, hace que el *gap* en protección siga creciendo. Como consecuencia la ciberresiliencia debe ser foco continuo y prioritario. Y para ello la visibilidad es clave. Si puedo monitorizar y entender lo que pasa en mi entorno, puedo actuar. Necesitamos trabajar para ser más ciberresilientes.

– Elastic es un referente en analítica de datos y motores de búsquedas. ¿Cuál es su valor diferencial respecto a su competencia?

– Nuestro motor de analítica de datos destaca por varios motivos: por cómo ha sido creado (solución *on-prem* y solución multi-*cloud*); por su código abierto con todo el poder de la Comunidad; por su concepto de plataforma (que evita la duplicidad de datos al integrar multitud de herramientas disponibles bajo un mismo paraguas); por su capacidad de ingesta de datos de cualquier formato; por su forma de licenciamiento (que permite afrontar el crecimiento sin disparar los costes); y, entre otros, por su arquitectura de datos (que permite ir enfriando el dato desde capas *hot* a *frozen* con tiempos de respuesta muy bajos y períodos de retención de años). Es una de las plataformas más abiertas y potentes que existen en el mundo del *data lake*.

– ¿Cuándo decidieron aplicar estas capacidades a la ciberseguridad y con qué enfoque?

No es algo nuevo. Elastic, como empresa que viene del mundo Open Source, ha contado con la ventaja de que millones de usuarios han construido casos de uso para múltiples disciplinas y una de ellas ha sido ciberseguridad. Muchos usuarios empezaron a utilizar Elastic

como *data lake* de seguridad hace años y comenzamos a ver el valor de integrar distintas capacidades sobre la plataforma: reglas, gestión de casos, *workflows* especializados, *dashboards*, etc. Creemos que hay que aproximarse a la ciberseguridad como un problema de datos: es necesario entender quién está haciendo qué en mi red, qué ocurre en mis aplicaciones y que todo esto pase en tiempo real. Si correlacionamos todos los datos de seguridad y los alimentamos con *feeds* de inteligencia, podremos entender posibles anomalías.

– Elastic apuesta por una ciberprotección abierta, colaborando con comunidades de desarrollo y operaciones, ya que considera que "ser abiertos es la esencia de todo lo que hacemos". ¿Cómo lo ponen en práctica?

– Podemos integrarnos con todas las plataformas y contribuir con estándares abiertos (por ejemplo, OpenTelemetry). Esto conlleva abrir nuestro código fuente y ser más eficientes ante posibles ataques derivados, por ejemplo, de la manipulación de dicho código. También, que la comunidad contribuya a mejorar la plataforma y que abordemos el *gap* de talento en ciberseguridad con plataformas abiertas, democratizando el acceso al conocimiento.

– En su propuesta también destaca el uso de la Inteligencia Artificial. ¿Qué características específicas presentan sus algoritmos en este ámbito?

– En IA uno de los retos es entrenar los modelos y mantener la privacidad de los datos. La aplicación de la IA a través de modelos preconfigurados que identifican problemas de seguridad sin tener que preocuparse por cómo entrenar el modelo o disponer de equipos de ciencia de datos, permite automatizar la detección de anomalías y el análisis de causa raíz, lo que reduce el MTTR. Gracias a la integración con ChatGPT, se desarrollan casos de uso para automatizar la identificación y respuesta a incidentes de seguridad y facilitar el trabajo de los CSIRT. Pero esto sólo es el principio, porque Elastic acaba de lanzar un motor para potenciar la IA en aplicaciones de búsqueda.

– ¿Con qué fortalezas cuenta la compañía para reclamar su hueco en el mercado de ciberseguridad?

– La propuesta de ciberseguridad de Elastic se apoya en tres pilares: SIEM, EDR (Endpoint Detection and Response) y protección *cloud*, aglutinadas en una aproximación XDR (Extended Detection and Response), concebida como una solución de SecOps moderna y más ágil para el analista.

Elastic se diferencia por su versatilidad en entornos híbridos y multi-*cloud.* El SIEM puede 'ingestar' datos de cualquier entorno, proporcionar visibilidad unificada y actuar sobre los datos allá donde estén. Resuelve con ello la problemática de *performance* frente al coste.

"La propuesta de ciberseguridad de Elastic se apoya en tres pilares: SIEM, EDR y protección *cloud*, aglutinadas en una aproximación XDR, concebida como una solución de SecOps moderna y más ágil para el analista"

– ¿Cuántas personas dirige usted en España y en qué principales áreas está focalizada Elastic en nuestro mercado?

– Elastic es una empresa muy distribuida con equipos basados en prácticamente todos los países. En España cuenta con más de 100 personas; además del equipo comercial, canal, preventa, *customer success*, servicios, desarrollo de negocio, disponemos de un equipo de ingeniería, *product management* y soporte. Es una fortaleza poco habitual tener equipos técnicos tan amplios hablando español y en nuestra zona horaria.

– ¿Cómo pueden acceder las compañías a sus soluciones y en qué modalidad?

– Somos una empresa de canal (con una red de *partners* globales y locales) con un foco importante en el movimiento hacia la nube. También, comercializamos nuestra plataforma a través de los *marketplace* de los tres hiperescalares (Azure, Amazon Web Services y Google Cloud Platform). Como creemos que el mundo no es ni puramente *on-prem* ni 100% *cloud*, sino híbrido, ofrecemos soluciones en local y en la nube, tanto en IaaS como SaaS, en nuestra Elastic Cloud.

– ¿Qué objetivos se ha marcado a corto y medio plazo, y qué sectores y tipos de empresa son más susceptibles de adquirir sus soluciones?

– Queremos potenciar la divulgación de nuestra propuesta de ciberseguridad y llegar a ser tan reconocidos en este ámbito como en el mundo de la observabilidad y de la búsqueda. Distintas consultoras ya nos sitúan entre los tres líderes en analítica de seguridad.

Nos proponemos seguir creciendo a ratios del +40% en Elastic Cloud. La flexibilidad de nuestra plataforma permite construir todo tipo de casos de uso. Cualquier organización *data-driven* que requiera extraer más valor de sus datos es susceptible de ser cliente de Elastic. Y si su filosofía es híbrida y/o multi-*cloud*, somos sin duda una de las mejores opciones.

"Cualquier organización *data-driven* que requiera extraer más valor de sus datos es susceptible de ser cliente de Elastic. Y si su filosofía es híbrida y/o multi-*cloud*, somos sin duda una de las mejores opciones"

– ¿Con que frase resumiría el valor del I+D+i en su compañía?

– Elastic sigue avanzando para encontrar entre todos los datos (seguridad, negocio, observabilidad) los que de verdad importan y lo hace en tiempo real (milisegundos) y a escala (multi peta-byte), sin importar el formato o la ubicación. ●

Visión holística, escalabilidad e integración de soluciones orientadas al SOC

Elastic Security aúna altas capacidades XDR, a través de SIEM, seguridad de *endpoints* y protección de la nube en una plataforma unificada, abierta e integrada

Con un enfoque de ciberseguridad centrado en el dato, aplicando potentes capacidades de protección, procesamiento y visualización, Elastic Security permite contar con el contexto necesario y poder extraer información valiosa de seguridad. Para ello, su propuesta pasa por ofrecer capacidades tanto listas para usar como definidas por el usuario, escalables, en tiempo real, y aunadas en una única plataforma que se puede implementar según las necesidades de cada cliente.

Más del 90% de los datos que existen en el mundo han sido creados en los últimos dos años. Y su incremento es imparable: se calcula que, para 2025, se generarán más de 175 zettabytes, lo que supone diez veces más de los registrados hace una década, según IDC. Por ello, el dato se ha convertido en uno de los activos más críticos y valiosos para las organizaciones. También en ciberseguridad donde las diversas fuentes de datos permiten contar con el contexto crítico necesario en detecciones, búsquedas, investigaciones y respuesta a incidentes. Y pocas compañías entienden mejor este enfoque que Elastic, cuya propuesta se basa en considerar "la ciberprotección como un desafío de datos". Por ello, su oferta, bajo el paraguas de Elastic Security, pasa por ofrecer altas capacidades de detección y respuesta extendidas (XDR), abarcando soluciones SIEM, seguridad de punto final y protección en la nube, en una plataforma unificada, abierta e integrada.

En ella, la compañía aplica todo el potencial de sus reconocidas capacidades de búsqueda, análisis y observabilidad de grandes volúmenes de datos para proporcionar protección, detección y respuesta de amenazas complejas en cualquier entorno, aplicando el uso del *machine learning* (ML) e IA de forma transversal.

Búsqueda avanzada para reducir el riesgo

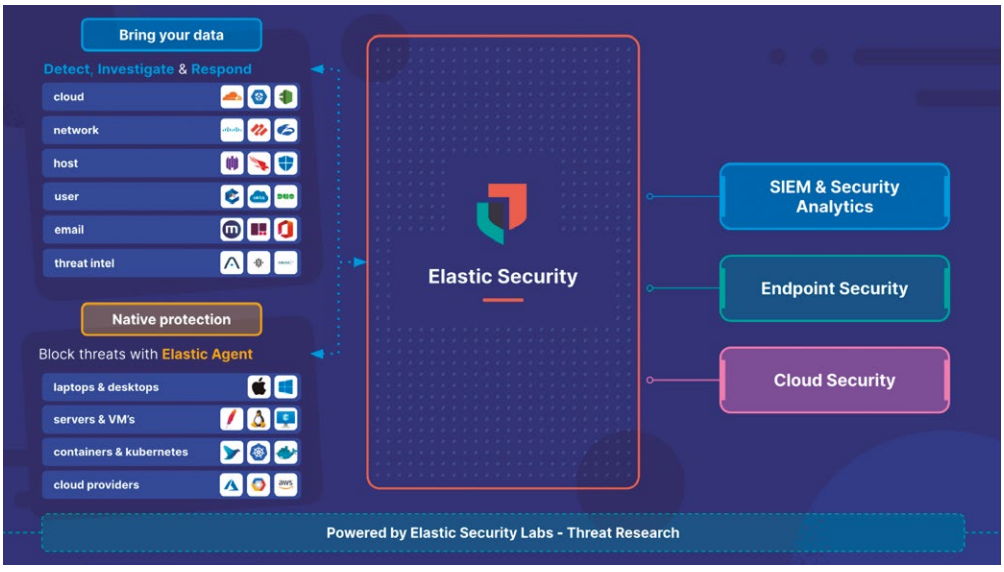
Elastic Security se basa así en Elastic Stack, un conjunto de herramientas de código abierto que proporciona grandes capacidades de búsqueda, análisis y visualización, que desde hace muchos años es utilizado por los equipos de seguridad como su base de datos para extraer información valiosa, y en cuyo núcleo se encuentra la tecnología de Elasticsearch. Para la compañía, una tecnología de búsqueda veloz, precisa y eficaz es clave para brindar una visibilidad holística, reduciendo el riesgo.

"Los datos pueden ayudar a identificar si un activo tiene una vulnerabilidad conocida e identificar dispositivos potencialmente vulnerables en una red", explican. Además, la búsqueda permite acelerar y refinar la detección de amenazas y limitar el daño de los ataques de *malware*, entre otros aspectos.

Por ello este tipo de plataformas se están convirtiendo en una herramienta imprescindible para los CISO.

Casos de uso

Todo ello permite disponer, con un único *data lake*, de potentes capacidades de protección, procesamiento y visualización de datos, y del contexto necesario para extraer información de seguridad valiosa. Los SOC pueden beneficiarse de casos de uso como la **monitorización continua** de la infraestructura local y basada en la *cloud*, la **búsqueda de amenazas** con información obtenida de análisis avanzados, así como **investigación y respuesta a incidentes** a través de la exploración de datos rápidamente y a escala, y la **protección automatizada contra amenazas,** impidiendo ataques complejos con ML y analíticas de comportamiento. ●



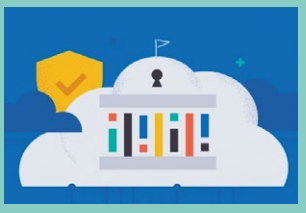
Protección completa del *endpoint*

Su plataforma también incluye, de forma unificada, la protección de puntos finales con su **Elastic Security para**

Endpoint. Con ella, la compañía ofrece una solución que bloquea el *ransomware* y el *malware*, interrumpe amenazas avanzadas con prevención sin firma y analíticas de comportamiento, además de contar con detección centralizada, reducción de falsos positivos y respuesta rápida y a escala, a través de una correlación *ad-hoc*. Entre sus características, destaca que reúne contexto detallado con OSquery e invoca acciones de respuesta remota en todos los *endpoints* distribuidos.

Seguridad de la nube

Para 'ir más allá' en su propuesta, Elastic presentó en 2022 **Elastic Security for Cloud**, con la que la compañía permite cumplir con la postura de protección para entornos híbridos y nativos *cloud* con detección y respuesta de infraestructura (IDR), para proporcionar a las empresas visibilidad profunda de las cargas de trabajo en la nube y contenedores, y ofrecer prevención, detección y respuesta. Entre otras capacidades permite la integración de la seguridad y observabilidad en una sola plataforma, disponiendo de la monitorización de los riesgos



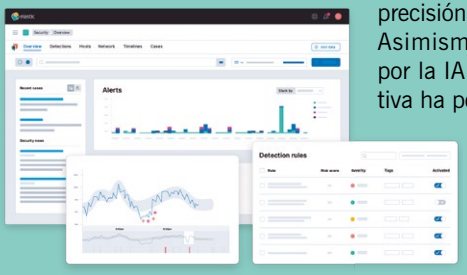
en procesos de implementación y las amenazas en tiempo de ejecución.

Capacidades SOAR nativas

También cabe destacar que, en su apuesta por capacitar a los SOC modernos para optimizar las operaciones de los analistas a través de la automatización, Elastic también anunció, en agosto de 2022, capacidades nativas de seguridad, orquestación, automatización y respuesta (SOAR) a través de Elastic Security. La solución está impulsada por su Elastic Agent y ofrece capacidades nativas de remediación y respuesta para todos los usuarios, así como alertas configurables e integración con otros proveedores de SOAR, lo que permite a las organizaciones implementar SOAR sin necesidad de comprar productos adicionales. Con ella, potencia el crecimiento de casos de uso 'con un solo clic' en cientos de fuentes de datos, al igual que la gestión de su software de protección de seguridad del *cloud* y *endpoints*.

Más allá del SIEM tradicional

Sobre la base del éxito de la compañía en tecnología de búsqueda y análisis de



grandes volúmenes de datos, Elastic creó una propuesta de soluciones con una aproximación XDR en cuyo corazón está el SIEM. Bajo la premisa de que "tu SIEM es tan bueno como los datos que ingesta y analiza", Elastic ofrece un enfoque de SIEM evolucionado, a través del cual, da acceso a todos los datos de seguridad, independientemente del tamaño, la escala o la ubicación, con visibilidad en todo el entorno, para detectar y responder a las amenazas más rápidamente y con mayor precisión.

Asimismo, su apuesta por la IA y la IA generativa ha permitido a Elastic hacer que estas capacidades estén disponibles para todos los analistas de seguridad, a través de su **Elastic AI Assistant**, impulsado por Elasticsearch Relevance Engine (ESRE), que permite interactuar con Elastic Security para investigación de alertas, respuesta a incidentes y generación o conversión de consultas utilizando lenguaje natural, incorporando numerosas indicaciones predefinidas para facilitar el trabajo de los usuarios, según sus necesidades.

Una estrategia diferencial

La plataforma unificada de Elastic, abierta e integrada con ingesta de datos flexible y soporte de la comunidad *open source*, sin bloqueo de proveedor, la ha permitido posicionarse en muy poco tiempo como uno de los referentes del mercado en este ámbito.

Para ello ofrece un valor diferencial apalancado en sus capacidades de protección nativa, con cientos de prevenciones, detecciones y reglas de respuesta mapeadas por MITRE, impulsadas por ML y complementadas con las investigaciones de su Elastic Security Labs.

Junto a ello, también destaca el hecho de estar construida para responder a las necesidades de escalabilidad de las empresas de una manera eficiente, así como la información automatizada a través, por ejemplo, de *runbooks* creados por expertos, enriquecimiento automatizado y gestión del riesgo integrado. A ello se suma que Elastic Security se puede utilizar en local y en la nube de AWS, Azure,

GCP, eliminando la necesidad de *backhaul* de datos.

Además, la manera en la que se licencia es reseñable ya que no se realiza por volumen de datos, sino por los recursos que se van a necesitar usar en el *clúster,* de forma que si se optimiza se consiguen modelos muy eficientes y competitivos en el sector.

Elastic de un vistazo

NYSE: ESTC

Somos la plataforma líder para soluciones impulsadas por tecnologías avanzadas de búsqueda, y ayudamos a todos –las organizaciones, sus empleados y sus clientes– a encontrar lo que necesitan más rápido, mientras mantenemos las aplicaciones funcionando sin problemas y protegiendo contra las amenazas cibernéticas.

Fundada en 2012

+ de 3.000 empleados

Presentes, con plantilla, en **más de 40** países

+ de 20.200 clientes

+ 54% de las compañías de Fortune 500 confían en Elastic

Para más información, comuníquese con nuestro equipo de ventas local en **elastic-revista-sic@elastic.co**

Actos y Convocatorias

RootedCON
Valencia, 15/16-9-2023
Panamá, 4/6-10-2023
Organiza: Asociación RootedCON.
Correo-e: info@rootedcon.com
Sitio: rootedcon.com

Strategic accounts Summit 23
Organiza: WatchGuard for SOC
Fecha: 19-9-2023
Lugar:
Meeting Place Castellana 81.
Madrid.
Correo-e: spain@watchguard.com
Sitio: secure.watchguard.com

Curso ISA-Internal Security Assessor
Organiza: Botech FPI y Solver 4 GP
Fechas: 27/28-9-2023
Lugar: Madrid
Correo-e: hugo.yepes@botechfpi.com
Sitio: solver4.com

Actividades CCI. Centro de Ciberseguridad Industrial
- **Taller de Diagnóstico de ciberseguridad en un entorno de automatización industrial,** 27/28-9-2023.
- **XXI Congreso Internacional de Experiencias en Ciberseguridad Industrial 2023,** 3/5-10-2023
- **Máster Profesional Online de Ciberseguridad Industrial,** inicio 19-10-2023.

Organiza:
Centro de Ciberseguridad Industrial-CCI.
Tel.: 910 910 751
Correo-e: info@cci-es.org
Sitio: cci-es.org

Programa #Include. VIII edición
Organiza: Fundación Goodjob.
Fechas: septiembre 2023
Correo-e: rrhh@goodjob.es
Sitio: fundaciongoodjob.org

Encuentro CIBER.gal 2023
Organiza: Ciberseguridad Xunta de Galicia
Lugar: Ciudad de la Cultura.
Santiago de Compostela.
Fechas: 2/3-10-2023
Sitio: ciber.gal

SECURMÁTICA 2023
- **En buena compañía**

Organiza: Revista SIC
Fechas: 3/5-10-2023
Lugar: Hotel Novotel Campo de las Naciones. Madrid.
Tel.: 91 575 83 24
Correo-e: info@securmatica.com
Sitio: securmatica.com

Fortinet Security Day
Organiza: Fortinet
Fechas: 10-10-2023
Lugar: Kinépolis.
Pozuelo de Alarcón. Madrid
Sitio: fortinet.com

17ENISE
Organiza: Incibe
Fechas: 18/19-10-2023
Lugar: Palacio de exposiciones.
León.
Sitio: incibe.es

PREMIOS SIC 2023
Se requiere invitación.
Organiza: Revista SIC
Fechas: 25-10-2023
Lugar: Villa Laureana

XVII Jornadas STIC CCN-CERT
- **V Jornadas de Ciberdefensa: ESPDEF-CERT**

Organizan: CCN-CERT y ESPDEF-CERT.
Fechas: 28/30-11-2023
Lugar: Kinépolis. Pozuelo. Madrid.
Correo-e: eventos@ccn-cert.cni.es
Sitio: jornadas.ccn-cert.cni.es

IdentiSIC
- **Ser… para creer**

Organiza: Revista SIC
Fechas: 15/16-11-2023
Lugar: Hotel Novotel Campo de las Naciones. Madrid.
Tel.: 91 575 83 24
Fax: 91 577 70 47
Correo-e: info@codasic.com
Sitio: revistasic.com/identisic

Cursos SANS INSTITUTE
- **Hacker tools, techniques and incident handling,** otoño 2023
- **Windows forensis analysis,** otoño 2023.

Organiza: One eSecurity
Lugar: Madrid
Tel.: 911 011 000
Correo-e: sans@one-esecurity.com
Sitio: one-esecurity.com/events_training.html

Formación en Ciberseguridad especializada
- **CEH (Ethical Hacking and Countermeasures v12)**
- **CND (Certified Network Defender)**
- **CCISO (Certified Chief Information Security Officer)**
- **CHFI (Computer Hacking Forensic Investigator)**
- **CSCU (Certified Secure Computer User)**
- **CPENT (Certified Penetration Testing Professional)**

Organiza: M2i Formación
Tel: 91 578 23 57
Correo-e: info@m2iformacion.com
Sitio: m2iformacion.com

AENOR Formación
- **Delegado de Protección de Datos**
- **ENS. Conceptos, implantación, evaluación y auditoría**
- **Gestión de la Continuidad de Negocio**
- **ISO 20000**
- **ISO 27000**

Organiza: AENOR
Tel: 91 432 61 25
Sitio: aenorciberseguridad.com

Cursos Ciberseguridad Westcon-Comstor
Organiza: Westcon-Comstor
Lugar: Madrid
Tel: 91 419 61 00
Correo-e:
academy.es@westcon.com
Sitio: https://academy.westconcomstor.com/es

Cursos ES-CIBER
Organiza: Escuela Superior de Ciberseguridad, ES-CIBER
Correo-e: info@es-ciber.com
Sitio: es-ciber.com

Centro de Formación Exclusive
Organiza: Exclusive Networks
Tel.: 91 197 66 01
Sitio: training.exclusive-networks.com/es-ES

INDICE DE ANUNCIANTES

(one) eSecurity

Readiness · Hunting · Detection · Response

¿Preparado para afrontar un ciberataque?

Confía en los mejores expertos

Emergency Incident Response (EIR)

Digital Forensics (DFIR)

Threat Hunting (TH)

Cyber Consulting (CyCon)

Cyber Exercises (CybEx)

Cyber Insurance (Cybins)

Managed Threat Hunting (MTH)

Compromise Assessment

San Francisco · Miami · Ciudad de México · Sao Paulo · Santiago de Chile · Bogotá · Madrid · Londres · Singapur

www.one-esecurity.com | info@one-esecurity.com | one-esecurity | Teléfono: +34 911 011 000

SECURMÁTICA 2023

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

3 · 4 · 5 OCTUBRE

En buena compañía

Organiza

Revista SIC

Copatrocinadores

accenture · Aiuken Cybersecurity · Audea · A&M · BABEL · cipher a Prosegur company · Entelgy Innotec Security

EY Building a better working world · FACTUM · FUJITSU · gmv Innovating Solutions · Google Cloud · KPMG · Microsoft

Outpost24 · pwc · S2 Grupo · sia An Indra company · Telefónica Tech · wisesecurity

www.securmatica.com