SIC

Hora de afinar

Nº 159 Abril 2024 – Año XXXIII

V-Valley | Lidera

ESPECIALISTAS EN ADVANCED SOLUTIONS

Mayor rentabilidad y valor en tus proyectos de Ciberseguridad Corporativa

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

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

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

A10 · Acronis · ARMIS · AREXDATA · BlackBerry · BACKBOX · Bitdefender · ca technologies A Broadcom Company
CHECK POINT · CLOUDFLARE · CYBERARK · Cyber Guru · elastic · ENTRUST · Fortanix
invicti · ivanti · Kaseya · kaspersky · NComputing · RED SIFT · SailPoint
securonix · Skyhigh Security · SONICWALL · sumo logic · Trellix · TREND MICRO · WatchGuard · XM Cyber

www.v-valley.com

seguridad@v-valley.com

SECURMÁTICA 2024

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

Manos a la obra...

... y bien acompañados

Organiza

Revista SIC

8·9·10 OCTUBRE

www.securmatica.com

Nº 159 Abril 2024 – Año XXXIII

SiC

Revista

Ciberseguridad, seguridad de la información y privacidad

www.revistasic.com

ENTREVISTA

José Ángel Álvarez
Director del CCMAD
AYUNTAMIENTO DE MADRID

ENTREVISTA

Vasu Jakkal
Vicepresidenta Corporativa de Seguridad, Cumplimiento, Identidad y Privacidad
MICROSOFT

ENTREVISTA

Luca Tagliaretti
Director Ejecutivo ECCC
CENTRO EUROPEO DE COMPETENCIA EN CIBERSEGURIDAD

9,856,348*

Cyber attacks prevented today.

Just another day of Security In Action.

checkpoint.com/action

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

CHECK POINT™

YOU DESERVE THE BEST SECURITY

SiC
Nº 159
Abril 2024

>> Sumario

>> en este número

DOCUMENTOS

• Ley de Inteligencia Artificial europea. Como cabía esperar, la denominada EU AI Act obtuvo, por parte del Parlamento Europeo en marzo, luz verde –en grado mayoritario–, para iniciar su odisea existencial, periplo al que se augura no pocos zarandeos normativos en sus derivadas legislativas conforme se vayan culminando los plazos de aplicación y cumplimiento. Con todo, supone un hito relevante en el empeño de impedir el libre albedrío de unas tecnologías potentemente disruptivas. Ahora queda por saber cómo se podrá conciliar el embridamiento europeo al uso desmedido de sus capacidades y, al tiempo, saber soltar cuerda para ser capaces de innovar con ella y poder competir en los frentes tecnológicos planetarios, más descarnadamente laxos en exigencias legislativas y éticas. Al tiempo, la lucha por saber qué bando aprovecha mejor sus colosales capacidades podrá percibirse conforme la promiscuidad de la IA sea aprovechada en mayor o menor medida por el bando de la ciberprotección y su opuesto, el de la ciberdelincuencia.

• Espacio TiSEC. A pleno SOC. Durante este evento, organizado por SIC en febrero del presente, se pudieron vislumbrar algunos movimientos que van a traer consecuencias al cada vez más poblado ramo de los MSSPs y que, muy posiblemente, hagan que los oportunistas se lo piensen dos veces a la hora de hacer el paripé e ir quemando el mercado con servicios malos y baratos. Ya está marcada la línea para considerar la ciberseguridad gestionada como una actividad esencial, y a los que la prestan, se les va a definir y se va a crear una certificación. De hecho, en nuestro país ya hay una experiencia piloto al respecto. El camino para la certificación de MSSPs ya está abierto en la UE. Démosle tres años de recorrido si no sucede algo que lo frene o lo acelere.

En la parte que le toca, el CCN, a través de la RNS, en la que ya pueden participar SOC privados, aventura que, tarde o temprano, solo los miembros con categoría GOLD (la categoría se mide por cantidad y calidad de compartición) tendrán opción de presentarse a concursos de las administraciones públicas. Y todos sabemos que, al final, el contratista privado (sea o no del Ibex35), siempre toma muy buena nota de estas circunstancias.

En el evento, se profundizó en algunos escenarios de sectorización que condicionan de forma evidente los servicios de ciberseguridad gestionada, en entornos tecnológicos (OT/IoT…) y en escenarios de TIC. A tal efecto se empieza a vislumbrar una especialización de SOC no generalistas, como los denominados de "misión crítica", los SOC de aplicaciones o aquellos denominados autónomos, por haber alcanzado un nivel de automatización elevado en muchos de los niveles de servicio y una plasticidad real en sus catálogos.

Bien puede decirse que se está preparando una revolución en el hoy superpoblado ecosistema de MSSPs+SOC, que va a provocar la racionalización en el número de jugadores y la aparición de un grupo selecto y distinguible de proveedores especializados comprometidos con la calidad y no tan sensible a los precios.

• Ciberseguridades nacionales. ¿Cómo organizarse? En esta edición la revista SIC ha afrontado un reto titánico; a saber: conocer cómo van organizando los estados europeos, los estados miembros de la UE y algunos otros estados no europeos la protección de su ciberespacio.

El trabajo ha sido apasionante y, al tiempo, extenuante. Por mucha cultura que se comparta, cada país es un mundo atado a su historia y a sus estructuras. Y la ciberseguridad es una disciplina y una práctica nueva que se ha ido acomodando a lo ya existente y, al tiempo, generando nuevos constructos a veces incalificables y todavía no maduros como para hacer un cuadro comparativo exhaustivo.

Sea como fuere, el lector sagaz encontrará en el especial de este número una información de alto valor, en momentos en los que la situación global no es especialmente tranquila, la de la UE, tampoco. Y la de España, menos, porque los posibles cambios legales y organizativos, orientados a la mejora de la gestión de la (ciber) seguridad nacional que pudieran derivarse de la trasposición de la NIS2 y de una futura ley de ciberseguridad, no están consensuados todavía. Y van a dar guerra.

Edita: Ediciones CODA, S.L. Goya, 39. 28001 Madrid (España) Tels.: 91 575 83 24 / 25 Fax: 91 577 70 47 **Correo-e:** info@revistasic.com www.revistasic.com **Editor:** Luis Fernández Delgado **Director:** José de la Peña Muñoz **Redacción:** Ana Adeva, José Manuel Vera **Colaboran en este número:** Luis Fernando Álvarez-Gascón, Gert Auväärt, Félix Barrio, Albert Calvo, Darragh McSweeney, Jorge Dávila, Jesús Díez, Javier Ferre, Antonio Grimaltos, Jordi Guijarro, Luis Jiménez, Alberto Partida, Alberto Pascual, Nil Ortiz, Antonio Requena, Nethaniel Ribco, José Luis Rojo, José Miguel Rosell, Florian Schütz, Fabienne Tegeler, Irene Yusta. **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

Trellix

Estés donde estés en tu viaje,

Trellix puede ayudarte en todos tus retos de ciberseguridad.

Detección de Ransomware

Estrategia Zero Trust

IA y Operaciones de Ciberseguridad

Seguridad Cloud

Modernización y SecOps

Reduce el riesgo, optimiza los costes y disminuye la complejidad con una plataforma XDR, interoperable y con capacidades avanzadas de IA.

- Xconsole
- Motor XDR
- Seguridad del Endpoint
- SecOps y Análisis
- Seguridad del Dato
- Seguridad de Red
- Inteligencia sobre Amenazas
- Seguridad del Correo Electrónico
- Seguridad Cloud

Para ver en directo nuestra IA, con sus capacidades de automatización y análisis predictivo, solicita tu demo en TRELLIX.COM

www.v-valley.com

V-Valley | Lidera

Duelo al amanecer en la (ciber)Seguridad Nacional

José de la Peña Muñoz
Director
jpm@codasic.com

Para que un Estado nación pueda emprender la hercúlea tarea de defender la porción de ciberespacio que considere suya, tiene que organizarse y dedicar medios humanos y materiales. Si acierta con la organización por la que opte en cada momento y va destinando medios humanos y materiales atinadamente, lo razonable es que esa defensa se vaya acercando a la excelencia, concepto ajeno al espacio-tiempo al que todo *Management Team* anhela llevar a su empresa, y que, desgraciadamente, es tan escurridizo como la *Integral Management* a la que aspiran los tradicionalistas de la *safety/security*, esos magníficos expertos que se encuentran en la pubertad digital.

> Me entristece que la ciberseguridad sea ya pura política. Nuestro Gobierno debería de tomar decisiones ante la NIS2 y una ENCS con un lustro de vida. Y los partidos políticos deberían de alcanzar consensos. Al fin y al cabo, el dinero no garantiza una organización mejor.

Como decíamos: hay que organizarse, o mejor, hay que ponerse de acuerdo en qué tipo de desorganización de la ciberseguridad es la más estable, la más conveniente, la que menos afecte a lo ya establecido… Y así, la mayoría de países hemos empezado a integrar como hemos podido esta faceta creciente de lo digital y ciberfísico en el ámbito civil y en el de la defensa militar.

En la UE, los "hermanos" de la privacidad se dieron cuenta de que las directivas las trasponían los estados miembros con asombrosa creatividad. En consecuencia, enfocaron la cuestión con una ley (el RGPD) para darnos pautas más precisas con las que equivocarnos en lo mismo. Pero en la conflictiva ciberseguridad, el vestido sigue siendo una directiva, la NIS1, y, casi ya en tiempo de descuento la NIS2, con el añadido de haber considerado pertinente diferenciar en otra directiva la resiliencia de las entidades críticas y de haber concebido una ley especial para el sector financiero, DORA, que trata sectorialmente (clientes y proveedores) la resiliencia operativa y, en su contexto, el control y mejora de la ciberseguridad efectiva. (Otras normas europeas relacionadas las dejaremos para una posterior entrega).

Enfrentamiento

Lo cierto es que tenemos que trasponer la NIS2 a la legislación española, hecho que nos da la oportunidad de mejorar algunos estratos del modelo de gobernanza de la ciberseguridad española, que emana estratégicamente de la Seguridad Nacional. Esta "mejora" lleva enfrentando a algunos actores estatales desde hace años. Hoy, el asunto es ya de público enfrentamiento entre dos posiciones aparentemente irreconciliables, la de aunar en un centro coordinador con poderes la gestión de todos los sabores de la (ciber) Seguridad Nacional, o la de mantener el modelo actual suprimiendo ineficiencias y duplicidades.

El CCN se manifiesta a favor de lo primero. INCIBE (que ha cambiado de forma jurídica), defiende lo segundo. El DSN, el MAEC, el MCCE y la OCC-SES no se posicionan públicamente. Pero todos entienden que hay espacio para la mejora.

Por tanto, lector, esta es hoy la España de la ciberseguridad que pudiera mejorarse: una orquesta sinfónica sin director en la que los esforzados músicos gestionan su papel en la partitura. Y, de cuando en cuando, se juntan colegiadamente en el Consejo Nacional de Ciberseguridad, "órgano de apoyo" al Consejo de Seguridad Nacional.

A un servidor, que lleva años en esto, le entristece ver trabajar como leones y avanzar en sus cometidos a los servidores públicos de la (ciber)Seguridad Nacional con tensiones más allá de las atribuibles a la sobrecarga de tareas, tanto en la ciberprotección como en el apoyo a la lucha judicial y policial contra la delincuencia. Claro que sí.

Pero más me entristece que la ciberseguridad sea ya pura política. Nuestro Gobierno debería de tomar decisiones ante la NIS2 y una ENCS con un lustro de vida. Y los partidos políticos deberían de alcanzar consensos. Al fin y al cabo, el dinero no garantiza una organización mejor. ●

Forcepoint

Secure Data Everywhere. Empower Work Anywhere.

La Seguridad del Dato protege tu información confidencial, las claves del negocio, el I+D de tu empresa y asegura la confianza de tus clientes. Seamos claros: la ciberseguridad es la protección del DATO.

forcepoint.com/use-case/data-security-everywhere

Luis Fernández Delgado
Editor
lfernandez@codasic.com

A rastras, mal y tarde

Manu Clavijo, un fiel compañero de mis otras correrías –las musicales–, tuvo el acierto de titular uno de sus últimos discos "A rastras, mal y tarde", sin duda una suculenta locución que hoy traigo a esta tribuna para centrar el contenido en esta ocasión.

A nadie se le escapa el sagaz significado de esta paráfrasis que, grosso modo, sugiere estarse 'obligado, forzado y/o de mala gana' a hacer algo. Cabe preguntarse si lo que ahora comentaré se adhiere a esta aseveración.

Hace justo un lustro en esta misma sección, que titulé en afrancesada expresión mayestática ***On verra,* Madrid** (ya veremos, Madrid), di cuenta del nacimiento del Cluster v2 de ciberseguridad matritense.

Una docena de años antes tuvo lugar el alumbramiento, postreramente fenecido, de la primera versión, nacida en 2007 bajo la denominación "Cluster de Seguridad y Confianza de la Comunidad de Madrid", a instancias del Instituto Madrileño de Desarrollo (IMADE) y de la por entonces Dirección General de Innovación y Tecnología de la Comunidad de Madrid.

> Enfocar atinadamente los esfuerzos en proyectar el sector de ciberprotección son objetivos cruciales para el loable propósito de ser, de una vez, el nodo de excelencia y referencia que por potencial le corresponde a Madrid.

El constructo no cuajó. Más allá de dilapidarse buena parte de su presupuesto en traerse de paseo mediático como cebo al carísimo y muy manoseado Kevin Mitnick –charleta de guardarropía mediante–, el su por entonces director –Lucio González–, no pudo ni evitar malograr el potencial ni el desencanto de su decena inicial de socios, fracasando en el empeño de dar continuidad y éxito a una idea inicialmente cautivadora con gran potencial. Al final este estéril esfuerzo quedó desvanecido feneciendo en un agónico concurso de acreedores en 2015.

Tras este desolador y fallido episodio, nos encontramos –ya doce años después– con la renacida *release 2*, que anuncia en 2019 su 'refundación' bajo la denominación **CyberMadrid**–**Clúster de Ciberseguridad de Madrid**, dando sus primeros pasos al constituir junta directiva y marcando sus objetivos. La pretensión de dicho Clúster, constituido como asociación sin ánimo de lucro, con personalidad jurídica propia y patrimonio propio independiente, es ser un punto de encuentro de empresas, asociaciones e instituciones, tanto públicas como privadas, que desarrollan actividades en el área de Madrid, en nuestro sector. Desde entonces, al frente figura un prestigioso profesional, –CISO en la actualidad– con una solvente trayectoria en la gestión de la ciberseguridad y conocimientos precisos de los retos tecnológicos asociados: **Damián Ruiz**. Más de 1.500 días después, el balance, lamentablemente, es escueto. Modestas cuando no tímidas acciones de relaciones sectoriales extramuros y, por el momento, hueros resultados con racimos hermanos.

Según declaraciones del actual Consejero de Digitalización de Madrid, Miguel López-Valverde, "Madrid es la locomotora tecnológica de España; un tercio de todas las empresas que se dedican a tecnología están ubicadas aquí y hay más de 280.000 personas en la Comunidad que se dedican al sector tecnológico".

Estos guarismos, que al parecer sitúan a la región como la segunda continental con más talento digital, no parecen corresponderse con el enjuto tejido de ciberseguridad asociado a CyberMadrid y al empaque de su actividad tras un quinquenio de recorrido. Las actividades del mismo, con *advisors* iniciales poco resultones, no han sido de gran relevancia y asiduidad, más allá de algunos eventos de similar contenido a los celebrados ya previamente en otras demarcaciones (por ejemplo, de salud y entornos sanitarios…) o mismamente el de este mes de abril sobre fraude digital, quizá tecnológicamente sobrecargado (un tema que por cierto ya desde SIC abordamos hace la friolera de 10 años con el premonitorio título de "El control de riesgos de fraude ante los nuevos escenarios").

De Madrid, aparte de postureos *selfialidosos* innecesarios, cabe esperar mucho, muchísimo más. Cabe ser y parecer proporcional al consistente, innovador y masivo potencial del tejido empresarial en ciberseguridad de la región, nutrirse de su pujanza y ganarlo para la causa.

Enfocar atinadamente los esfuerzos en averiguar y entender el tallaje de un efervescente sector madrileño que, aun así y con todo, adolece de dispersión, desconfianza y de estar mal atendido; cohesionarlo mediante la cooperación sincera y transparente, contribuyendo a su dinamización como es debido de cara a su proyección exterior, propiciando, por ejemplo, su exhibición en un marco ferial potente, útil y a la altura –en las antípodas de los sucedáneos descafeinados de todos conocidos–, son objetivos que deberían de estar muy presentes en un loable propósito cual es ser, de una vez, el nodo de excelencia y referencia que por potencial le corresponde a Madrid.

Con todo, para redondear el incomprensiblemente adormecido panorama matritense, las personas y entes residentes en la capital española seguimos (a fecha de cierre de esta edición) acéfalos de adalid al frente de la Agencia de Ciberseguridad de Madrid, que ufana anunció su esperanzador emerger a finales de 2023 y a fecha de hoy aun sigue huérfana tras el fallido fichaje inicial propuesto –y descartado– del pertinente Consejero Delegado para encomendar la llevanza de la Agencia bajo el precepto de *fichar* "a un profesional de reconocido prestigio en el ámbito de la ciberseguridad". Para más inri en este incómodo contexto y aunque Madrid Digital y CCMAD prosiguen sus quehaceres competenciales con nota, no es de buen gusto el afloramiento mediático de ciberincidentes como el sucedido en febrero pasado con el Consorcio de Transportes.

Otros entes gestores de ciberprotección pública de similar corte –Cyberzaintza (antes BCSC), ADA andaluza, Agencia de Ciberseguridad de Cataluña, CIBER.gal …–, para sonrojo de los concernidos, se han mostrado mucho más madrugadores y ya llevan años con acciones y fastos de mucha mayor enjundia y visibilidad.

La verdad es que a unos aún nos gusta no dejar las neuronas al *dolce far niente* en este asilvestrado berenjenal digital, recostadas haraganeando entre mullidas y narcotizantes nubes límbicas de transformación cibernética. Por el contrario, ansiamos que se tome carrerilla, se recorte distancia y se compita ágilmente en el frente del buen hacer en la ciberprotección.

Por lo que aguardamos expectantes a la *enmendalla*, y si a nuestro pesar prosiguiera el desatino y la inapetencia, aquí en SIC, residimos desde hace un pelín en estas esperanzadoras tierras –tal que 32 años mismamente– y algo sabemos de posibles candidatos a la llevanza, limpios de pelo, sesgo y paja. La consultoría sería gratis. Todo sea por *Madriz*.

onum.com
sales@onum.com

¿Con cuánta rapidez recibes alertas de seguridad, basadas en señales de advertencia en tus datos?

Onum te ayuda a obtener información profunda en tiempo real, para que puedas detener los eventos de seguridad al momento.

onum

Europa

Aprobado también el Reglamento revisado de eIDAS2 que creará carteras digitales para garantizar que el usuario tenga el control de sus datos

La UNIÓN EUROPEA llega a un acuerdo final de la Ley de Cibersolidaridad y modifica la de Ciberseguridad para certificar servicios gestionados

Las elecciones europeas en junio supondrán un parón a todas las iniciativas legislativas en marcha y, por ello, la presidencia belga de la UE está acelerando para poder aprobar las máximas posibles. Entre las negociaciones más relevantes ha destacado, el 20 de marzo, que el **Parlamento Europeo** y la **Presidencia del Consejo** llegaron a un acuerdo provisional sobre la llamada 'Ley de Cibersolidaridad', además de aprobar una enmienda de la Ley de Ciberseguridad (CSA) –aprobada en 2020–, que deberán ser aprobadas por ambas instituciones de forma definitiva para su adopción final.

Así, entre otros aspectos, como ya informó **Revista SIC** en números anteriores, la CSA establece un "sistema de alerta de seguridad cibernética", a través de una infraestructura paneuropea de centros de operaciones de ciberseguridad (SOC) nacionales y transfronterizos en la UE.

También, pretende poner en marcha un mecanismo de emergencia de ciberseguridad para aumentar la preparación y mejorar las capacidades de respuesta a incidentes, así como la implementación de un mecanismo de evaluación y revisión para valorar, entre otros, la eficacia de las actuaciones bajo el mecanismo de ciber emergencia y el uso de una 'ciberreserva', entrando en vigor 20 días tras su publicación. El presupuesto total para todas las acciones, en el marco de la Ley de Cibersolidaridad de la UE, es de 1.100 millones de euros, de los cuales aproximadamente dos tercios serán financiados a través del Programa Europa Digital.


Council of the European Union

Brussels, 20 March 2024
(OR. en)

8047/24

Interinstitutional File:
2023/0109(COD)

CYBER 86
TELECOM 131
CADREFIN 89
FIN 330
BUDGET 23
IND 179
JAI 512
CODEC 665

INFORMATION NOTE
From: General Secretariat of the Council
To: Delegations
No prev. doc.: 7589/24 + ADD 1
No. Cion doc.: 6612/23 + ADD 1
Subject: Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents - Letter sent to the European Parliament

At its meeting on 20 March 2024, the Permanent Representatives Committee (Part 1)

Certificación de MSSP

Por otra parte, la enmienda a la CSA, como ya se explicó en TiSEC 'A pleno SOC' -ver crónica en este número- pretende mejorar la ciberresiliencia de la UE apostando por la puesta en marcha de sistemas de certificación europeos para los 'servicios de seguridad gestionados', siendo el **CCN** el pionero en ofrecer una propuesta. Así, a la espera de la revisión periódica de la CSA –prevista para el 28 de junio–, el acuerdo provisional, entre otros puntos, define con precisión la definición de "servicios de seguridad gestionados" y garantiza la alineación con la Directiva NIS2, además de alinear sus objetivos con otros esquemas de certificación de este ámbito –desde 2019 se ha aprobado uno, para producto, estando en marcha el de nube y seguridad en 5G–.

Acuerdo final para el eIDAS2

Además, el 26 de marzo el Consejo adoptó un nuevo marco para una identidad digital europea (eID). El reglamento entrará en vigor 20 días después de su publicación en el Diario Oficial de la UE y se implementará completamente en 2026. El nuevo marco modifica el reglamento de 2014 sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interior (reglamento eIDAS), que sentó las bases para acceder de forma segura a los servicios públicos y realizar transacciones en línea y a través de fronteras en la UE.

EN BREVE

La COMISIÓN prepara un concurso para adquirir servicios profesionales de ciberseguridad para proteger sus instituciones

La **Comisión Europea** pondrá en marcha un concurso para la adquisición de servicios profesionales de ciberseguridad para garantizar la protección cibernética de las instituciones europeas. En concreto, se busca, por un lado, apoyar servicios operativos, tanto en lo que atañe a operaciones técnicas como la implementación de políticas, y, por otro, contar con servicios de asesoramiento y desarrollo de capacidades

El concurso se realizará a través del sistema dinámico de compras (DPS) de la Comisión Europea para servicios profesionales relacionados con servicios en la nube (Cloud II DPS) y se estructurará en tres lotes:

uno para servicios de operaciones técnicas; otro para el apoyo a la implementación de políticas, poniendo el foco en los servicios operativos en favor de la mejora continua de la madurez de la ciberseguridad; y un tercero para servicios de asesoramiento y desarrollo de capacidades que cubran estudios técnicos y de mercado, así como evaluaciones, vías de desarrollo y refuerzo de habilidades.

Si una IA suplanta a tu CEO...

¿Lo detectarías?

Phishing y concienciación con Deepfakes

¿'Suplantamos' a tu CEO?

www.zerolynx.com

ZEROLYNX

Europa

EN BREVE

DHS y DG CONNECT anuncian una iniciativa para alinear los enfoques transatlánticos de notificación de incidentes

La **Dirección General de Comunicaciones, Redes, Contenido y Tecnología** (DG CONNECT) de la **Comisión** y el **Departamento de Seguridad Nacional de EE.UU.** (DHS) anunciaron en marzo una iniciativa para comparar los sistemas de notificación de incidentes cibernéticos de EE.UU. y EU, bajo la Directiva NIS2. "Esta colaboración transatlántica se basa en sus esfuerzos para proteger a su gente, sus infraestructuras críticas y sus empresas contra actividades cibernéticas perjudiciales", destacaron sus responsables a la vez que recuerdan que este "informe conjunto desarrollado por DG CONNECT y DHS, con el apoyo de sus respectivas agencias de ciberseguridad, **Enisa** y **CISA,** proporciona una evaluación comparativa y una descripción objetiva de las recomendaciones de la Agencia Cibernética de EE.UU.".

Los ciberincidentes no reconocen fronteras y, a menudo, se exige a las empresas multinacionales que informen de incidentes en numerosas jurisdicciones. Estamos comprometidos a armonizar las normas de notificación de incidentes a nivel nacional y con socios de ideas afines como la Unión Europea siempre que sea posible. "Nuestro enfoque permitirá a las autoridades gubernamentales obtener la información que necesitan para brindar defensa cibernética y al mismo tiempo agilizar el proceso para las organizaciones víctimas", comentaron sus responsables.

Seis puntos clave

En concreto, el informe establece seis áreas principales para el análisis comparativo entre el informe del DHS y la Directiva de la UE, que incluyen: (1) definiciones y umbrales de notificación, (2) cronogramas, desencadenantes y tipos de notificación de incidentes cibernéticos, (3) contenidos de los informes de incidentes cibernéticos, (4) mecanismos de presentación de informes, (5) agregación de datos de incidentes y (6) divulgación pública de información sobre incidentes cibernéticos.

Se trata de un trabajo "fundamental ya que las autoridades gubernamentales pertinentes deben tener acceso a información sobre incidentes cibernéticos que afectan a sus ciudadanos o que, de otro modo, plantean preocupaciones de seguridad. Por ello, durante los próximos meses, tanto EE.UU. como la UE continuarán trabajando para poner en vigor regímenes de presentación de informes obligatorios, incluso mediante la implementación de disposiciones más precisas sobre el proceso de notificación de incidentes, el contenido de los informes y los plazos. Es importante mantenerse conectado sobre estos temas y alinearse cuanto sea posible", ha destacado la directora de Sociedad Digital, Confianza y Ciberseguridad de la DG Connetc, **Lorena Boix Alonso**.

Los desafíos y oportunidades de la estandarización de la ciberseguridad protagonizan la octava conferencia europea sobre este ámbito

En marzo, las **Organizaciones Europeas de Normalización** (ESO), **CEN, CENELEC** y **ETSI,** unieron fuerzas con **Enisa** para organizar su octava Conferencia de Normalización de Ciberseguridad. En ella, se debatió sobre el futuro de la estandarización europea de la ciberseguridad, los desafíos relacionados con la nueva legislación, los estándares para los nuevos requisitos de los productos digitales y la estandarización de la seguridad de las cadenas de suministro y sus componentes.

La conferencia se organizó en cuatro paneles. Uno para debatir el futuro de la normalización europea, otro sobre los desafíos de estandarización relacionados con la nueva legislación, un tercero sobre los nuevos requisitos que deberán cumplir para certificarse los productos digitales y, por último, también cómo estandarizar la seguridad de las cadenas de suministro y sus componentes.

Las inversiones en ciberprotección deberán duplicarse en la próxima legislatura para tener impacto, según el director general de la Unidad Digital de la UE

Las inversiones en ciberseguridad deberán duplicarse durante el próximo mandato de la **Comisión Europea** para garantizar la resiliencia del bloque a contraataques, destacó en marzo, **Roberto Viola,** director general de la Unidad Digital de la Comisión, en una conferencia en Bruselas, según **Euronews.**

En concreto, recordó que, en diciembre, la Comisión destinó 214 millones de euros para 2024 para este ámbito con el fin de mejorar la resiliencia colectiva frente a las ciberamenazas a través del **Centro Europeo de Competencia en Ciberseguridad** (ECCC), con sede en Bucarest.

Además, durante el congreso, se habló del reto de implementar a finales de año la NIS2 por parte de cada miembro. "Aún queda mucho por hacer en términos de nueva legislación, pero tenemos un desafío con la implementación. NIS2 ya es inmensa y la Ley de Resiliencia Cibernética también es exigente", afirmó **Despina Spanou,** jefa de gabinete del Comisario de Seguridad de la UE, **Margaritis Schinas.**

EE.UU.

El Departamento de Defensa ha pedido casi 13.400 millones de euros para acometer los retos en ciberdefensa para 2025

Un informe independiente alerta de un "panorama alarmante" que vive el COMANDO CIBERNÉTICO DE EE.UU. pidiendo un cambio estructural por ineficiencias

Estados Unidos es una de las grandes potencias cibernéticas del mundo a través de su **Comando Cibernético** (**Cybercom**) y las unidades cibernéticas de cada ejército. Sirva como ejemplo que para el año fiscal 2025, el **Pentágono** ha pedido un presupuesto que ronda los 13.400 millones de euros para gastos cibernéticos, incluyendo su programa para implementar un enfoque de Confianza Cero -con el objetivo de que se consiga en 2027-, el nuevo personal contratado y la inversión en investigación avanzada. Se trata de una cifra que supera en más de 920 millones a la del año anterior y que el **Departamento de Defensa** (DoD) justifica por su gran apuesta por lo cibernético para hacer frente a las amenazas que supone en este ámbito el avance de países como Rusia y China.

Críticas a los ciberejércitos

Frente a ello, se está cuestionando con dureza la forma de reclutar y generar especialistas cibernéticos en las Fuerzas Armadas del país. Un informe independiente de la **Fundación para la Defensa de las Democracias,** publicado en marzo, considera que hay que establecer "un servicio cibernético militar independiente para solucionar problemas 'alarmantes", según ha detectado. "El sistema de generación de fuerza cibernética de EE.UU. está claramente roto. Para solucionarlo se requiere el establecimiento de un ciberservicio independiente", afirma el informe que alerta de que "esta investigación pinta un panorama alarmante". "La ineficiente división del trabajo entre el Ejército, la Armada, la Fuerza Aérea y la Infantería de Marina impide generar una fuerza cibernética lista para llevar a cabo su misión. El reclutamiento se ve afectado porque las operaciones cibernéticas no son una prioridad absoluta para ninguno de los servicios. El sistema actual agrava estos desafíos de generación de fuerza. Cada uno de los servicios ha desarrollado sus propias soluciones, lo que genera inconsistencias y deficiencias".

La investigación se ha realizado a partir de entrevistas a 75 militares en activo y jubilados**,** pero con gran experiencia en liderazgo y mando, y se ha llevado a cabo por el contraalmirante retirado **Mark Montgomery,** director senior del **Centro de Innovación Cibernética y Tecnológica de FDD,** y **Erica Lonergan,** profesora asistente en la Escuela de Asuntos Públicos e Internacionales de la **Universidad de Columbia**. "Los servicios no se coordinan para garantizar que los alumnos adquieran un conjunto consistente de habilidades o que sus habilidades correspondan a los roles que finalmente desempeñarán en **Cybercom**", afirma.

"Los sistemas de promoción a menudo frenan al personal cibernético capacitado porque los sistemas fueron diseñados para evaluar a los miembros del servicio que operan en tierra, mar o aire, no en el ciberespacio", señala. Además, los participantes que defienden en el informe un "servicio cibernético independiente" argumentan que los cibercomandos no tienen una identidad distinta, ya que siguen siendo miembros de sus respectivos servicios, además de contar con estructuras de mando y control confusas, e incluso escalas salariales distintas según el destino. "Estos equipos de fuerzas de misión cibernética (ofensivos y defensivos) fueron diseñados inicialmente para ser conjuntos desde el principio, entrenados con los mismos estándares para que pudieran ser intercambiables y operar uno junto al otro.

Pero las complejidades de los servicios individuales han plagado ese diseño", comenta el estudio que pone de manifiesto que lo "preocupante que es que este modelo deficiente de generación de fuerzas esté impactando negativamente la preparación. Está impidiendo que la fuerza de misión cibernética realice operaciones o realmente crezca y se expanda", explicó Montgomery. Frente a estas críticas, los que se oponen a un ciberservicio independiente consideran que ahora no es el momento, destacando que el modelo actual aún precisa de madurez y que también supondrá una mejora notable la mayor autoridad que, en principio, se le dará a Cybercom.

Incidente notable

Por otro lado, ha sido muy mediático el ciberataque sufrido por la **Agencia de Seguridad de Infraestructura y Ciberseguridad** (CISA), aunque el organismo ha destacado que "no ha habido ningún impacto operativo", precisando, a través de un portavoz, que se trata de un "recordatorio de que cualquier organización puede verse afectada por una vulnerabilidad cibernética y contar con un plan de respuesta a incidentes es un componente necesario de la resiliencia".

Precisamente, esta Agencia ha publicado las prioridades para este año de su departamento de **'Colaboración Conjunta de Ciberdefensa'** (**JCDC**), que se centrará en incrementar sus esfuerzos por mejorar en capacidades de defensa frente a operaciones de amenazas persistentes avanzadas (APT), aumentar las protecciones básicas para los propietarios y operadores de infraestructuras críticas y anticipar tecnologías y riesgos emergentes.

Más medios ciberpoliciales


Christopher Wray

Estos objetivos están en consonancia con las prioridades indicadas en este ámbito por el director del **FBI**, **Christopher Wray,** a principios de año, quien recordó que hay "poca atención pública sobre el hecho de que los piratas informáticos de la República Popular China están atacando nuestra infraestructura crítica: nuestras plantas de tratamiento de agua, nuestra red eléctrica, nuestros oleoductos y gasoductos naturales, nuestros sistemas de transporte. Y el riesgo que eso representa para todos los estadounidenses requiere nuestra atención ahora". "No quiero que se piense que no podemos protegernos", dijo a los legisladores en una comparencia en el Congreso. "Pero sí quiero que el pueblo estadounidense sepa que no podemos permitirnos el lujo de ignorar este peligro". Para ello, la agencia pidió 58 millones de euros adicionales para este año para poder contar con más agentes, capacidades de respuesta mejoradas y fortalecidas de recopilación y análisis de inteligencia".

sia

An Indra company

Todas las grandes ciudades tienen un SOC IT

Es momento de añadir OT e IoT
y relacionar ambos mundos para responder a los desafíos actuales

Smart MDR

El servicio *end to end* más avanzado de detección y respuesta para cubrir las necesidades de ciberseguridad de las ciudades de hoy

- **Modelo de defensa proactivo**
- **Detección y respuesta avanzada**
- **Servicio E2E**
- **Optimiza el tratamiento de la información**
- **Respuesta más ágil ante incidentes**
- **Automatización con IA**
- **Mejor predictibilidad de la ciberdelincuencia**
- **Flexible y personalizable**

15 minutos
para detectar cualquier incidente

Solo un 2%
de falsos positivos y reducción en más de un 80% en alertas de escaso valor

5
Cyber Defense Centers
con equipos globales coordinados para mayor agilidad y eficiencia

Anticipa amenazas, minimiza riesgos, responde rápido.
Extiende la protección de tu ciudad más allá.

BEYOND CYBERSECURITY

siainfo@sia.es
sia.es

EE.UU.

EN BREVE

BIDEN aprueba una orden ejecutiva marítima para reforzar la ciberprotección de puertos y buques

El presidente de EE.UU. **Joe Biden,** ha firmado una orden ejecutiva con el objetivo de mejorar las ciberdefensas de los puertos marítimos a través de autoridades adicionales a la Guardia Costera, además de poner en marcha un proceso para establecer una normativa específica para el sector. Entre otros aspectos, el texto da a la Guardia Costera la autoridad para responder a incidentes cibernéticos, además de exigir al sector civil mayor inversión en este ámbito. De cualquier forma, avanza que el gobierno invertirá 18.500 millones de euros en infraestructura portuaria en los próximos años, primando también su ciberseguridad.

La orden sigue a una serie de advertencias de funcionarios de seguridad nacional de EE.UU. sobre un grupo de piratería, vinculado a China, llamado **Volt Typhoon** que ha atacado con éxito sectores de infraestructura críticos del país, entre otros, el sector marítimo, aspecto sobre el que se profundizó en **'Espacio TiSec'**, en marzo, a través de la propuesta de **GMV** para contar con SOCs sectoriales, especializados en este ámbito.

El DEPARTAMENTO DE ESTADO estudia no emitir visados a personas vinculadas al uso de software espía

El secretario de Estado de EE.UU., **Antony Blinken**, ha destacado en una conferencia en Singapur que se prevé negar visados, estudiando caso por caso, a las personas que quieran viajar al país pero hayan estado implicadas en el uso indebido de software espía comercial, continuando con lo marcado por Biden en 2023 cuando firmó una orden ejecutiva que prohíbe a las agencias federales utilizar este tipo de software comercial que se considera un riesgo para la seguridad nacional del país y que tiene identificados en una lista de proveedores realizada por el Departamento de Comercio. Las nuevas reglas se dirigirán a personas que "faciliten u obtengan beneficios financieros del uso indebido de software espía comercial", incluidos aquellos que participan en "el desarrollo, la dirección o el control operativo de empresas que suministran tecnologías como software espía comercial a los gobiernos, o aquellos que actúan en nombre de los gobiernos", según un comunicado del Departamento de Estado. Entre las más conocidas de este tipo están empresas como **NSO Group, Intellexa** y **Cytrox.**

NIST lanza la versión 2.0 de su Marco de Ciberseguridad, con seis funciones claves y más recursos para facilitar su aplicación

El **Instituto Nacional de Estándares y Tecnología** (NIST) ha publicado el documento definitivo de su actualización del Marco de Ciberseguridad (CSF), publicado en 2014 y muy utilizado para reducir el riesgo en este ámbito.

Entre otras novedades, la nueva propuesta cubre más sectores industriales y tipos de organizaciones, estructurando sus contenidos en torno seis funciones clave: identificar, proteger, detectar, responder y recuperar, junto con la de gobierno recientemente agregada de CSF 2.0. Además, como respuesta a los numerosos comentarios recibidos, NIST también ha ampliado la guía principal de recursos que acompañan al CSF "para que sea más fácil de poner en práctica". "CSF 2.0, que se basa en versiones anteriores, no se trata sólo de un documento, sino de un conjunto de recursos personalizables, para usar de forma única o en conjunto, a lo largo del tiempo, a medida que las necesidades de ciberseguridad de una organización cambian y sus capacidades evolucionan", ha manifestado la directora del NIST, **Laurie E. Locascio.**

EE.UU. publica una guía de ciberseguridad para los servicios públicos de agua y aguas residuales

La **CISA,** el **FBI** y la **Agencia de Protección Ambiental** (EPA) han publicado una 'Guía de Respuesta a Incidentes', destinada a ayudar a las organizaciones del Sector de Agua y Aguas Residuales (WWS) para mejorar su resiliencia cibernética y sus capacidades de respuesta a incidentes.

En ella se describe cómo los propietarios y operadores de servicios de agua pueden interactuar con socios federales para prepararse, mitigar y responder a incidente, además de establecer pautas para la notificación, detallando los recursos disponibles, los servicios y la capacitación sin coste, así como las recomendaciones a las diferentes empresas a colaborar y trabajar de forma conjunta con las unidades cibernéticas locales de las autoridades públicas y a acometer, de forma urgente, un plan de respuesta de incidentes.

SANS The most trusted source for cybersecurity training, certifications, degrees, and research

SANS Madrid Junio

10-15 Junio 2024

Madrid, ES

Ven a Madrid a uno de los cuatro cursos prácticos de ciberseguridad impartidos por expertos de la industria.

Descubre los pasos más efectivos para prevenir ciberataques y detectar adversarios con técnicas prácticas enseñadas por los mejores profesionales durante **SANS Madrid junio 2024**. Elige tu curso y regístrate ahora para una formación que podrás utilizar inmediatamente.

Características de SANS Madrid Junio 2024

- Formación presencial.
- Realiza tu formación durante el evento con apoyo de profesionales de primer nivel.
- Formación práctica en ciberseguridad impartida por expertos del mundo real y en activo.
- Laboratorios prácticos en un entorno virtual.
- Los cursos incluyen libros electrónicos e impresos.
- Todos los cursos están alineados con las certificaciones GIAC

Modalidad de enseñanza

SANS Live Training ofrece:

- **Opciones flexibles:** Formación interactiva y de inmersión con oportunidades para establecer contactos y aprender de otros profesionales.
- **Cursos de vanguardia:** Todos los cursos están diseñados para alinearse con funciones, deberes y disciplinas dominantes de los equipos de seguridad.
- **Formación de los mejores:** Los instructores de SANS son profesionales de la seguridad en activo que aportan sus amplios conocimientos y experiencias reales al aula.
- **La promesa de SANS:** Podrá aplicar las habilidades y técnicas que haya aprendido en cuanto vuelva al trabajo.

SANS NETWARS

NetWars Tournament

Con tu inscripción en este evento podrás participar en un exclusivo Torneo NetWars.

NOTA: El torneo NetWars no tendrá lugar necesariamente durante la misma semana que la formación. A medida que nos acerquemos a las fechas del evento, recibirás un correo electrónico con información adicional.

sans.org/cyber-ranges

"Fantástico, apasionante y atractivo. El instructor complementó el contenido del curso con escenarios reales relacionados, lo que mejoró la experiencia de aprendizaje y la hizo muy interesante."

—Eliza-May Austin, **Visa Inc**

Escanéame para descubrir los cursos que impartiremos en Madrid

+44 203 384 3470 emea@sans.org @SANSEMEA

América Latina y el Caribe fue, en 2023, la cuarta región que más ciberataques sufrió, con un 12% de los incidentes

CHILE aprueba su primera Ley de Ciberseguridad que da pie a la primera Agencia Nacional de la región

Los ciberataques en Iberoamérica se incrementaron un 56,4% entre 2021 y 2023, según un reciente informe de la Unit 42 de **Palo Alto Networks**. Una cifra en consonancia con los datos del estudio 'X-Force Threat Intelligence Index 2024' de **IBM**, que destaca que, en 2023, fue la cuarta región más atacada del mundo, con un 12% de los incidentes mundiales. Brasil (68%), Colombia (17%) y Chile (8%) fueron los países en los que los cibercriminales centraron más ataques, sobre todo, en sectores como *retail,* junto con finanzas y seguros.

El *malware* y, más concretamente, el *ransomware* estuvieron presentes en el 31% de los incidentes, seguido del acceso a servidores y el uso de herramientas con fines maliciosos, ambos con el 23%. Respecto al impacto, el 33% de los ataques conllevaron filtraciones de datos y un 22% resultaron en extorsión o afectación a la reputación de la marca.

Proporción de casos de respuesta a incidentes por región a los que respondió X-Force entre 2021 y 2023. Fuente: IBM X-force

Primera Agencia Nacional de Ciberseguridad

En cuanto a iniciativas regionales, ha destacado la promulgación en **Chile** de su 'Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información', –como ya se hizo referencia en SIC 158–, finalmente presentada a finales de marzo por el presidente de la República, **Gabriel Boric**, lo que conllevará la creación de su **Agencia Nacional de Ciberseguridad**, su primer CSIRT Nacional y otro de Defensa, además de impulsar su 'Política Nacional de Ciberseguridad' para 2023-2028, que busca que el país tengan "una infraestructura de la información robusta y resiliente que resista y se recupere de los ciberincidentes".

Por su parte, **Brasil** y **Paraguay** suscribieron un convenio de cooperación para "promover un entorno cibernético abierto, seguro, estable, accesible, pacífico e interoperable a nivel nacional e internacional, basado en el respeto de los derechos humanos y las libertades fundamentales para el desarrollo social y económico de ambos países".

Igualmente, el director ejecutivo de la **Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento** (AGESIC) de **Uruguay**, **Hebert Paguas,** destacó la necesidad de crear una "conciencia colectiva" en ciberseguridad, en el ámbito público, enmarcada en una estrategia que reúna a los principales actores del sector y que apueste por la colaboración privada como uno de los principales objetivos del gobierno. En este sentido, resaltó que, de momento, la legislación tiene una limitación "muy importante", dado que muchos ciberdelitos se cometen desde otros países, por lo que apuntó a la colaboración, coordinación y acuerdos internacionales como el camino a seguir para luchar contra los delincuentes.

En lo que respecta a **República Dominicana**, fue elegida en febrero para presidir el **Grupo de Trabajo de Medidas de Fomento de la Confianza en el Ciberespacio** (MFC) de la OEA, el cual busca aumentar la cooperación, transparencia, predictibilidad y la estabilidad entre los Estados en el uso del ciberespacio; Canadá asumirá el rol de vicepresidente.

Análisis de situación

Sin duda, en América Latina y el Caribe, al igual que en el resto del mundo la ciberseguridad es un aspecto crítico, aunque esta región "es única debido a su diversidad cultural y económica, lo que la hace particularmente desafiante en términos de ciberprotección. A medida que los países trabajan para crear un entorno digital seguro, deben abordar cuestiones que van desde la falta de acceso a Internet hasta amenazas cibernéticas cada vez más sofisticadas". Así se describe en el estudio 'Evolution of Cybersecurity - LAC 2023' recientemente publicado, llevado a cabo por el **Centro de Cibercapacidades de Latinomérica y el Caribe** (LAC4) y el **Ministerio de Relaciones Exteriores de Países Bajos**.

En él, se analiza cómo ha evolucionado la ciberseguridad en la región, desde sus inicios hasta la situación actual, cómo se están fortaleciendo las ciberdefensas, su marco regulatorio y las políticas en este ámbito, así como su infraestructura y capacidades en ciberseguridad, la colaboración y cooperación internacional.

Entre otros aspectos, el documento indica que "América Latina y el Caribe continúan enfrentando desafíos importantes, según un estudio de 2020 del Banco Interamericano de Desarrollo (BID) y la **Organización de Estados Americanos** (OEA). Muchos países de la región todavía tienen actividades e iniciativas *ad hoc* en materia de ciberseguridad sin una visión estratégica. Solo 13 países tienen estrategias nacionales de ciberseguridad y solo 9 tienen planes de protección de infraestructura crítica".

Además, destaca que "una parte importante del desafío radica en la integración y formalización de los CSIRT, mecanismos de cooperación nacionales e internacionales, educación formal y medidas de ciberseguridad para que el sector financiero pueda mitigar los riesgos asociados a una economía cada vez más digital y de consumo". Y es que, "el sector financiero es una infraestructura importante en la región". "Los diálogos regionales y la cooperación en esta materia aún están en sus inicios y fragmentados". No obstante, resalta iniciativas de cooperación internacional a través de programas conjuntos de capacitación, intercambio y ejercicios de simulación a través de organizaciones como LAC4, Cyber4Dev y EU Cybernet. Además, pone en valor el trabajo de la OEA y la **Comisión Económica para América Latina y el Caribe** (CEPAL).

Acuerdos

De forma paralela, también cabe resaltar la firma de acuerdos entre el **Instituto Nacional de Ciberseguridad de España (Incibe**), y la **Asociación Bancaria y de Entidades Financieras de Colombia** (**Asobancaria**), para impulsar la colaboración en este ámbito a través de la cultura de ciberprotección, así como con el **Instituto Federal de Telecomunicaciones de México**. Además, la OEA e Incibe ya han abierto el periodo de registro para el IX Cybersecurity Summer BootCamp, el programa internacional de capacitación, gratuito, en el que se pueden presentar solicitudes hasta el 18 de abril.

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

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

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

EY
Building a better working world

Inteligencia Artificial

La ONU también ha dado luz verde a su primera resolución sobre esta tecnología con el apoyo de toda la Asamblea, incluida China

El PARLAMENTO EUROPEO aprueba la primera Ley de IA del mundo mientras EE.UU. continúa analizando cómo regular y limitar su uso malicioso

Europa ha vuelto a convertirse en un referente normativo, con la aprobación en marzo de la Ley de Inteligencia Artificial por parte del **Parlamento Europeo,** estableciendo las salvaguardias sobre la IA de propósito general (GPAI), los límites al uso de sistemas de identificación biométrica por parte de las fuerzas del orden, así como la prohibición de puntuación social y de IA utilizadas para manipular o explotar las vulnerabilidades de los usuarios, además de regular el derecho de los consumidores a presentar quejas y recibir explicaciones significativas. En total, el texto fue aprobado por 523 votos a favor, 46 en contra y 49 abstenciones.

Además, es destacable que el uso de sistemas de identificación biométrica (RBI) por parte de las fuerzas del orden está prohibido en principio, excepto en situaciones enumeradas exhaustivamente y definidas de forma rigurosa y sólo puede implementarse si se cumplen estrictas salvaguardias. Por ejemplo, su uso está limitado en el tiempo y el alcance geográfico y está sujeto a una autorización judicial o administrativa previa específica. Dichos usos pueden incluir la búsqueda selectiva de una persona desaparecida o la prevención de un ataque terrorista. También, se prevén obligaciones claras para otros sistemas de IA de alto riesgo (debido a su importante daño potencial a la salud, la seguridad, los derechos fundamentales, el medio ambiente, la democracia y el Estado de derecho). Ejemplos de usos de IA de alto riesgo incluyen infraestructura crítica, educación y capacitación vocacional, empleo, servicios públicos y privados esenciales. Asimismo, la ley pide establecer entornos de pruebas regulatorios y pruebas en el mundo real a nivel nacional, y hacerlos accesibles a las pymes y las empresas emergentes, para desarrollar y capacitar una IA innovadora antes de su comercialización.

Revisión final

Eso sí, el reglamento aún está sujeto a una revisión final por parte de los juristas lingüistas y se espera que sea adoptado definitivamente antes de que finalice la legislatura (mediante el llamado procedimiento de corrección de errores). La ley también necesita ser respaldada formalmente por el **Consejo**. Una vez que lo haga, entrará en vigor 20 días después de su publicación en el Diario Oficial y será plenamente aplicable 24 meses, excepto: prohibiciones de prácticas prohibidas, que se aplicarán seis meses después y obligaciones para sistemas de alto riesgo (36 meses), entre otros aspectos.

Intenso debate

La norma es un paso importante en medio del intenso debate que hay en todo el mundo sobre los límites y alcance de las regulaciones en marcha. Además, ha sido significativo que la **Asamblea General de la ONU** aprobará a finales de marzo su primera resolución sobre IA, brindando apoyo global a un esfuerzo internacional para garantizar que la tecnología beneficie a todas las naciones, respete los derechos humanos y sea "segura y digna de confianza". La iniciativa, patrocinada por EE.UU. fue copatrocinada por 123 países, incluido China, y adoptada por consenso 'con un golpe de mazo' y sin votación, lo que significa que cuenta con el apoyo de los 193 países miembros de la ONU.

También, ha sido especialmente importante la iniciativa de la **Casa Blanca** que abrió un periodo de un mes de comentarios públicos sobre los riesgos y beneficios de tener los componentes clave de un sistema de IA disponibles públicamente para que cualquiera pueda usarlos y modificarlos, como parte de la orden ejecutiva firmada por el presidente **Biden** en octubre.

Asimismo, el gobierno de EE.UU. ha anunciado que obligará a implementar un nuevo requisito para que los desarrolladores de los principales sistemas de IA revelen los resultados de sus pruebas de seguridad al gobierno, según lo dispuesto en la Ley de Producción de Defensa. Asimismo, el Departamento de Comercio ha desarrollado un borrador de norma sobre las empresas estadounidenses en la nube que proporcionan servidores a desarrolladores extranjeros de IA.

Además, el **Departamento de Seguridad Nacional** (DHS) ha presentado una 'hoja de ruta' para usar IA de forma segura y respectando la privacidad por parte de las operaciones federales.

De cualquier forma, no han faltado este año varios casos preocupantes de uso malicioso de la IA. El más mediático fue una llamada suplantando la voz del presidente, Joe Biden, a los votantes del estado de New Hampshire, antes de las primarias del Estado a principios de año. También, se ha conocido el engaño a un empleado de una empresa de Hong Kong, a través de una videoconferencia, cuya imagen falsa fue generada por IA, y que logró convencerle para que realizara una transferencia de 23 millones de euros. Eso sí, del lado contrario, el **Departamento del Tesoro de EE.UU.** también anunció que, en 2022, recuperó 346 millones de euros gracias a un nuevo proyecto de detección de fraude impulsado por IA.

DXC TECHNOLOGY

Tu escudo infalible en la era digital

Asegura tu futuro digital con nuestro nuevo SOC

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

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

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

CONTACTA

Ponte en contacto con DXC Technology.

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

Inteligencia Artificial

IA abierta… o no

Sin duda, la IA está suponiendo un verdadero tsunami en todos los ámbitos. De hecho, las propias empresas que desarrollan sistemas con IA tampoco tienen claro si deben hacer accesibles o no los componentes que implementan esta tecnología. Entre los promotores de un enfoque abierto están desde **Meta Platforms,** matriz de Facebook, hasta **IBM.** De hecho, Meta ha anunciado que compartirá con la Casa Blanca lo que ha aprendido "al construir tecnologías de IA de manera abierta durante la última década, para que todos puedan seguir compartiendo sus ventajas", según una declaración escrita de su presidente de Asuntos Globales, **Nick Clegg.** También, ha sido notable la propuesta de **Google**, que ha presentado 'Iniciativa de Ciberdefensa IA para reforzar la ciberseguridad' con el objetivo de "ayudar a los defensores digitales a adelantarse a los atacantes y, a su vez, fortalecer la seguridad global". Una decisión que incluye casi 14 millones de euros en inversiones para el apoyo a *startups* –entre ellas la ciudadrealeña **Zepo,** especializada en concienciación–, pequeñas empresas, instituciones académicas e investigadores; así como para habilitar herramientas de seguridad de IA nuevas y de código abierto. Además, ha puesto en marcha su 'Google for Startups: AI for Cybersecurity', un programa de tres meses dirigido a reforzar el ecosistema transatlántico de ciberseguridad mediante el apoyo a la nueva ola de compañías emergentes del sector.

Problema de privacidad con GenAI

De cualquier forma, muchas empresas están prohibiendo usar la IA por los riesgos de privacidad que conlleva. Según un estudio de **Cisco,** cada vez hay más preocupaciones en entornos corporativos sobre la privacidad con GenAI.

Entre sus aspectos más relevantes destacados por los participantes en el informe están las amenazas a los derechos legales y de propiedad intelectual de una organización (69%) y el riesgo de divulgación de información al público o a los competidores (68%). Eso sí, la mayoría de las compañías ya están implementando controles para limitar la exposición: el 63% ha establecido limitaciones sobre qué datos se pueden ingresar, el 61% tiene límites sobre qué empleados pueden usar las herramientas GenAI y el 27% dijo que su organización había prohibido GenAI. No obstante, según un informe sobre el panorama de amenazas de la identidad, del año pasado, de **CyberArk,** cerca del 33% de los equipos de ciberseguridad en España ya usan la IA para detección y prevención de infracciones.

EN BREVE

MICROSOFT y OPENAI alertan del intenso uso de la IA que están haciendo grupos de APT para sus ataques conocidos

Según una investigación de **Microsoft** y **OpenAI,** se han identificado numerosos intentos de varios actores de amenazas afiliados al estado de utilizar modelos de lenguaje grande (LLM) para mejorar sus operaciones cibernéticas. "AI igual que lo hacen los defensores, los actores de amenazas están aprovechando la IA (más específicamente: los LLM) para aumentar su eficiencia y continuar explorando todas las posibilidades que estas tecnologías pueden ofrecer", destaca el informe que cita directamente a algunos grupos, respaldados por estados, entre los que están desde el actor de inteligencia militar ruso Forest Blizzard (STRONTIUM), hasta el norcoreano Emerald Sleet (THALLIUM), el iraní Crimson Sandstorm (CURIUM) y el chino Charcoal Typhoon (CHROMIUM), entre otros.

Por ello, la multinacional también ha anunciado principios destinados a mitigar los riesgos que plantea el uso de sus herramientas de IA y API por parte de amenazas persistentes avanzadas (APT), manipuladores persistentes avanzados (APM) y sindicatos cibercriminales.

OWASP da a conocer un listado con controles de verificación para implementar de forma segura IA generativa

El **Open Web Application Security Project** (OWASP) ha publicado la lista de verificación de gobernanza y ciberseguridad de LLM AI. Se trata de un documento de 32 páginas con el que se pretende ayudar a las organizaciones a crear una estrategia para implementar modelos de lenguaje grandes (LLM) y mitigar los riesgos asociados con el uso de estas herramientas de IA.

La iniciativa ha partido de un primer informe titulado '10 principales problemas de seguridad para aplicaciones LLM', publicado por OWASP a mediados de 2023, y que ha cristalizado en este nuevo documento, que ofrece una lista de pasos que recomienda acometer antes de implementar una estrategia de LLM, incluida la revisión de sus estrategias de capacitación en seguridad y resiliencia cibernética y la interacción con los líderes sobre cualquier implementación de IA en su flujo de trabajo. Además, proporciona una descripción general de cinco formas en que las organizaciones pueden implementar LLM, según sus necesidades.

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

El CONSEJO DE SEGURIDAD NACIONAL considera la ciberseguridad "más esencial que nunca" y la trasposición de la NIS2 antes de octubre

El presidente del Gobierno, **Pedro Sánchez,** presidió en marzo la reunión del **Consejo de Seguridad Nacional** (CSN) en la que se aprobó el Informe Anual de Seguridad Nacional 2023, así como las nuevas estrategias nacionales contra el terrorismo y de seguridad marítima.

El informe describe las consecuencias de los 16 riesgos identificados en la Estrategia de Seguridad Nacional 2021, siendo los dos escenarios de mayor preocupación la invasión de Ucrania y la de violencia entre Israel y Hamás en Gaza, además de campañas de desinformación.

El documento, de 284 páginas, repasa las iniciativas realizadas el pasado con la participación de entidades públicas, así como los principales retos para 2024 en este ámbito. Así, recuerda la labor del CNCS -que se reunió en dos ocasiones- y su trabajo en pro de la ciberprotección durante la Presidencia española del Consejo de la UE o para la trasposición de la Directiva NIS2. También, se pone en valor el trabajo de la Comisión Permanente de Ciberseguridad, grupo de trabajo del CNCS, y del **Foro Nacional de Ciberseguridad**, que ha permitido, a través de la colaboración público-privada, con más de 90 expertos, entre ellos el editor de **Revista SIC**, **Luis Fernández,** y su director, **José de la Peña**, publicar varios trabajos relevantes sobre 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.

En cuanto al ámbito regulatorio, se destaca que España tiene, en 2024, uno de sus principales retos en la transposición de la conocida como Directiva NIS2, cuyo trabajó comenzó en 2023 y debería estar culminado para el 17 de octubre, fecha límite para su adaptación nacional.

Ciberprotección, más esencial

El texto también considera que "la preparación y la eficacia en materia de ciberseguridad son más esenciales que nunca". De hecho, el documento, que refleja el número de incidentes detectados por el CERT del **CCN** y el del **Mando Conjunto del Ciberespacio**. También destaca que el año pasado fueron notificados a la **Oficina de Coordinación de Ciberseguridad** (OCC) del **Mº del Interior**, un total de 8.050 incidentes, con ataques mediáticos como el sufrido por diversas empresas y organismos, "entre los que destacan Puertos del Estado, Renfe y Adif".

Además, el informe recuerda que 2023 ha servido para consolidar la Red Nacional de SOC, liderada por el **CCN,** que cuenta actualmente, según el documento con 158 entidades adscritas y ha intercambiado, al día, 30 incidentes.

No falta el recuerdo a otras medidas la creación del Instrumento de Ciberresiliencia y Seguridad, dotado con 2.200 millones de euros.

Por otro lado, el **Consejo Nacional de Ciberseguridad (CNC)**, presidido por **Esperanza Casteleiro,** directora del CNI, se reunió a mediados de marzo para actualizar el estado de las ciberamenazas, analizar los últimos incidentes notables registrados y valorar las actuaciones realizadas durante 2023, así como la situación de las iniciativas legislativas relacionadas con la ciberseguridad en la UE, incluyendo la transposición de la Directiva NIS2.

El PP retoma en el Congreso la idea de crear una 'Reserva Estratégica de Talento en Ciberseguridad'

El **Grupo Parlamentario Popular** en el **Congreso** ha retomado la idea de 2017, que entonces impulsaron sus diputados **Ana Vázquez Blanco** y **Teodoro García Egea**, de contar con una reserva cibernética, en el ámbito de las Fuerzas Armadas.

Ahora, a través de una Proposición no de Ley, el diputado por Granada, **Carlos Rojas García**, ha propuesto la creación y regulación de lo que ha denominado 'Reserva Estratégica de Talento en Ciberseguridad', "dentro del ámbito específico de la ciberdefensa o para hacer frente a situaciones que afecten a la Seguridad Nacional". Una idea que se debatirá en la **Comisión de Defensa**.

Este tipo de reclutamiento tendría por objeto "incorporar las capacidades, conocimientos y habilidades aplicables al ciberespacio de los ciudadanos que voluntariamente decidan colaborar en cumplimiento del interés general de incrementar el nivel de ciberseguridad", y que debería encomendarse al **Mando Conjunto de Ciberdefensa** (**MCCD**) actualmente denominado **Mando Conjunto del Ciberespacio-MCCE**).


Carlos Rojas (PP)

Así pues, sería el encargado de "la selección de aquellas personas que por su experiencia y conocimientos técnicos o de otra índole en la materia puedan aportar talento a las capacidades existentes en las Fuerzas Armadas", siempre bajo las normas que rigen al resto de Reservistas Voluntarios, procurando "que los periodos de desarrollo de funciones militares por parte de los reservistas tengan la consideración de permisos retribuidos, previo acuerdo con la empresa".

En 2017, el entonces jefe del MCCD, general de División, **Carlos Gómez López de Medina**, apostó por crear una *ciberreserva* para contar con un "aumento de fuerza de manera flexible para cuando sea necesario y además se trataría de personal extraordinariamente cualificado".

NO SÓLO BUSCAMOS **PROTEGER** EL MUNDO, QUEREMOS **CAMBIARLO**

NUESTRA MISIÓN MÁS IMPORTANTE

+ EN ADVENS, NOS COMPROMETEMOS A PROTEGER ACTIVAMENTE A LAS EMPRESAS E INSTITUCIONES, DEJANDO UN IMPACTO POSITIVO EN LA SOCIEDAD.

+ ESTAMOS LIDERANDO UNA TRANSFORMACIÓN COMPLETA. UNA REVOLUCIÓN DE 360º EN EL ÁMBITO DE LA CIBERSEGURIDAD, AVANZANDO DE MANERA PROGRESIVA Y ESTRATÉGICA EN SU DESARROLLO.

ESTAMOS EN UNA MISIÓN
¿QUIERES SER PARTE DEL CAMBIO?

Advens
Security for the greater good

Su CERT se convierte en el primer CSIRT español en obtener la certificación Trusted Introducer

En marcha la IV convocatoria de INCIBE de Compra Pública de Innovación en ciberseguridad, con una inversión de 48 millones de euros

El **Instituto Nacional de Ciberseguridad de España** (Incibe) a través de la **Secretaría de Estado de Digitalización e Inteligencia Artificial**, ha publicado las bases de la 4ª convocatoria de su Iniciativa Estratégica de Compra Pública Innovadora (IEC-PI), en el marco del Plan de Recuperación, Transformación y Resiliencia, con la financiación de los fondos Next Generation. Esta nueva CPI está dotada con un presupuesto total de 48 millones de euros, derivado del presupuesto no adjudicado en las tres convocatorias anteriores. Con esta dotación, el organismo pretende poner en marcha proyectos innovadores de I+D de ciberseguridad sobre tecnologías emergentes y disruptivas de IA y/o computación *cloud*, *edge* o *distribuida* y, con una aportación económica de entre tres y hasta 12 millones de euros por proyecto.

Con ello, se busca la creación de soluciones de alto impacto estratégico que permitan hacer frente a las amenazas más avanzadas en sistemas expuestos, en espacios de datos, en los entornos distribuidos, en las comunicaciones y en los sistemas de información de empresas y entidades del sector público nacional con el objetivo global de proteger la información que reside y se transmite por ellos. De momento, Incibe ha adjudicado hasta la fecha 150,5 millones de euros a un total de 82 empresas, dentro de esta iniciativa para el desarrollo de 142 proyectos, tal y como se refleja en su mapa de Compra Pública de Innovación, en la web del organismo.

Entrega de la acreditación Trusted Introducer al Incibe

CERT de referencia

Por otro lado, el centro de respuesta ante incidentes de ciberseguridad para los ciudadanos y entidades de derecho privado en España, **Incibe-CERT**, se ha convertido en el primer CSIRT (Equipo de Respuesta ante Emergencias Informáticas) en España en recibir la certificación otorgada por el foro europeo, **Trusted Introducer**, del que el Instituto forma parte desde 2008. Esta certificación, reconocida internacionalmente, valida su capacidad y madurez para proporcionar servicios de gestión de incidentes con un elevado nivel de calidad.

De Colombia a Israel

El organismo también ha continuado la firma de acuerdos con actores destacados. Entre los más notables, ha destacado su alianza estratégica con la **Asociación Bancaria y de Entidades Financieras de Colombia** para impulsar la ciberprotección del sector financiero, el suscrito con la **Agencia Nacional de Ciberseguridad de la República Italiana** (ACN), para realizar actuaciones e iniciativas conjuntas que permitan desarrollar la cultura de la ciberseguridad en ambos países y con el **Centro de coordinación del equipo de respuesta a emergencias informáticas de Japón** (Jpcert/CC), para abordar "los desafíos emergentes" en este ámbito.

Asimismo, en febrero, su sede en León acogió un encuentro empresarial en el que dio a conocer la oferta de 10 compañías israelíes en busca de potenciales socios tecnológicos españoles. En cuanto a sus iniciativas en el ámbito académico, el Incibe ha presentado, junto con la **Universitat Pompeu Fabra** la nueva Cátedra de Ciberseguridad Artemisa, que también contará con la participación de la **Universidad París-Saclay** y el **Instituto Politécnico de París** y permitirá crear un laboratorio de *cyber range*, generando un entorno virtual para poner en práctica las habilidades y los conocimientos en este campo. Por otra parte, el ministro para la Transformación Digital y de la Función Pública, **José Luis Escrivá**, visitó a finales de marzo dos actividades notables del Incibe, Experiencia Incibe y CyberCamp, en Albacete.

HACIENDA anuncia la creación del Centro de Ciberseguridad y Protección de Datos de la AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA

El **Ministerio de Hacienda** ha puesto en marcha los mecanismos necesarios para la creación del Centro de Ciberseguridad y Protección de Datos de la **Agencia Estatal de Administración Tributaria** (AEAT) y de la Unidad Central de Sistemas de Atención al Contribuyente, según ha dado a conocer a través de una resolución sobre organización y funciones del Área de Informática Tributaria, publicada en el BOE.

Con ello, pretende reforzar la ciberprotección de la información tributaria, facilitando el cumplimiento de la normativa relativa a la protección de datos de carácter personal, ciberseguridad e infraestructuras críticas.

Dado que, según destaca la Agencia, los riesgos de sufrir ciberataques y amenazas cada vez son más grandes, la idea es disponer de este Centro que tendrá, entre otras funciones, la definición, implantación y mantenimiento actualizado de los planes de actuación que garanticen la recuperación de los servicios informáticos, dentro de los plazos establecidos, en caso de fallo total o parcial de la infraestructura tecnológica que utilizan.

CCN presenta las soluciones Elena y Ada para investigaciones y análisis avanzado de código dañino, celebrando sus 20 años de vida

El **Centro Criptológico Nacional** (CCN) cumplió 20 años el 12 de marzo, fecha en la que, en 2004, se publicó el Real Decreto 421/2004 que establecía el ámbito de actuación y las funciones del primer organismo español con responsabilidades en la ciberseguridad española. Con él, se convertía en el único organismo que, partiendo de un conocimiento de las amenazas y de las vulnerabilidades existentes, disponía de las capacidades necesarias para ofrecer garantías sobre la seguridad de productos y sistemas.

Además, el organismo ha presentado dos nuevas soluciones, Elena y Ada. La primera busca facilitar la capacitación de los profesionales en ciberseguridad. Se trata de una plataforma que permite a los usuarios adentrarse en el ámbito de la ciberinvestigación y practicar las técnicas, tácticas y procedimientos necesarios para realizar labores de este tipo. Por su parte, Ada es una plataforma para el análisis avanzado de código dañino con la que se mejora la detección de ciberamenazas de tipo *malware* en archivos, ficheros (.zip, pdf, documentos de office, etc.) y URLs.

Ya cuenta con 23 aceleradoras y 182 instalaciones de pruebas, con 44 empresas elegidas para desarrollar en ellas sus proyectos

DIANA, la aceleradora de innovación de la OTAN, duplica el tamaño de su red transatlántica, entrando el INCIBE y la UPM como centros de investigación

La **Aceleradora de Innovación en Defensa para el Atlántico Norte** (conocida como **DIANA**) de la **OTAN** anunció en marzo una importante expansión de su red transatlántica en este ámbito pasando de 11 a 23 aceleradoras y de 90 a 182 centros de pruebas en 28 países aliados. Organizaciones que "se centrarán en resolver algunos de nuestros mayores desafíos de defensa y seguridad y en agudizar nuestra ventaja tecnológica en áreas que van desde la IA y la cibernética hasta el 5G, la hipersónica y los sistemas autónomos", ha destacado el secretario general de la Alianza, **Jens Stoltenberg.**

En concreto, las aceleradoras afiliadas a DIANA brindan capacitación, financiamiento y asesoramiento comercial de primer nivel a los beneficiarios del programa, mientras que la red de centros de pruebas ofrece acceso a instalaciones de test de última generación. De momento, 44 empresas, con sus proyectos, han sido elegidas para trabajar en estas ubicaciones de entre más de 1.300 solicitantes.

Apuesta por el Incibe

Entre las nuevas incorporaciones a la red, se incluye la del **Instituto Nacional de Ciberseguridad** (**Incibe**) como nuevo centro de investigación e innovación, junto a la **Universidad Politécnica de Madrid,** por parte de España. Gracias a este paso, el organismo podrá optar al fondo de 1.000 millones de euros de ayuda prevista para los proyectos. Además, está trabajando para acoger uno de los tres laboratorios de certificación que la organización defensiva instalará en nuestro país.

DIANA se creó en 2022 para garantizar que la OTAN aprovechase lo mejor de la innovación de doble uso para la defensa y la seguridad transatlánticas, proporcionando a las empresas los recursos, las redes y la orientación para desarrollar tecnologías profundas que resuelvan desafíos críticos de defensa y seguridad, desde operar en entornos denegados hasta abordar amenazas a la resiliencia colectiva.

La OTAN ofrece un mapa interactivo con todos los integrantes de la red DIANA en **www.diana.nato.int**

ESET ESPAÑA presenta nuevo programa de canal y participa en la operación mundial Grandoreiro

Eset España ha tenido una participación muy activa durante la investigación que ha finalizado con la detención de varios integrantes del grupo de ciberdelincuentes responsables del caballo de Troya bancario, Grandoreiro. **Josep Albors**, director de Investigación y Concienciación de Eset España, fue uno de los expertos de la compañía que, junto con otras empresas y organismos oficiales, colaboraron proporcionando inteligencia sobre estas amenazas, permitiendo a la **Policía Federal de Brasil** la desarticulación de la *botnet* Grandoreiro.

De forma paralela, la compañía ha destacado que España es el país europeo con más detecciones de amenazas, el tercero a nivel mundial solo por detrás de Japón y EE.UU. Así se desprende de su Eset Threat Report, correspondiente a los meses comprendidos entre junio y noviembre de 2023. En esta edición, también destaca que el *phishing* y las inyecciones de código JavaScript malicioso en webs legítimas fueron las principales amenazas detectadas por la telemetría de la compañía. Otras como los *infostealers*, los troyanos bancarios y el *ransomware* han mantenido su presencia.

Ontinet.com, único distribuidor oficial para España y Andorra de Eset, ha presentado su nuevo Programa de Canal, diseñado para maximizar los beneficios y la rentabilidad de sus distribuidores. Para ello, cuenta con cinco niveles que se adaptan a las necesidades y objetivos de cada socio, y que incluyen un innovador sistema de márgenes con el que pueden aumentar sus beneficios. Todo ello se complementa con planes de negocio personalizados e incentivos adicionales.

Tecnología, servicios gestionados y canal de distribución, los pilares de BITDEFENDER para crecer

Con el objetivo de reforzar su posicionamiento en el mercado español, **Bitdefender** basará su estrategia de negocio en tres pilares fundamentales: tecnología avanzada de ciberprotección, servicios gestionados de detección y respuesta (MDR) y canal de distribución. Además, está impulsando su presencia internacional anunciando la apertura de un nuevo centro de operaciones de seguridad (SOC) en Singapur.

Los planes de la compañía en nuestro país se centran en incrementar su cuota de mercado en el área empresarial, donde ya es un jugador destacado. Sus soluciones para las empresas destacan por su efectividad, facilidad de uso y "altísima capacidad de detección de amenazas", destaca **Luis Fisas**, director de Ventas para el sur de Europa en Bitdefender. Entre sus últimas novedades, la compañía ha reforzado sus servicios MDR con el lanzamiento de Bitdefender Offensive Services. Además, anunció recientemente la solución Bitdefender Threat Intelligence (TI) y GravityZone Security for Mobile, entre otras.

Junto a ello, el canal de distribución es un pilar con cada vez más peso en la estrategia de Bitdefender en el mercado español. Y por ello, "en estos momentos queremos reforzarlo con la incorporación de *partners* que cuenten con la capacidad técnica necesaria para llevar a cabo proyectos de gran envergadura, pero también con otros que, siendo más modestos, dispongan de las capacidades necesarias para poder desenvolverse bien en el entorno de la ciberseguridad", comenta **Roberto Pérez,** director de Canal para Iberia en Bitdefender. Todos los beneficios que ofrece las compañías a sus socios de canal se reflejan en el programa Partner Advantage Network. En este sentido, entre sus iniciativas destaca la puesta en marcha del Partner Marketing Portal (PMP), una plataforma dinámica y automatizada para acciones de marketing que está disponible de forma gratuita y que aporta recursos y acceso a los fondos necesarios para complementar sus estrategias de ventas.


Luis Fisas

CROWDSTRIKE

Figure 1: Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (December 2023)

Líder por tercer año consecutivo Categoría de Plataformas de Protección de Endpoints Mejor posición por su integridad de Visión

Gartner

Publica cinco acuerdos marco de homologación de empresas

La AGENCIA DE CIBERSEGURIDAD DE CATALUÑA presenta un nuevo modelo de aprovisionamiento y contratación con inversiones de 232 millones de euros a cuatro años

El pasado 15 de marzo, el secretario de Telecomunicaciones y Transformación Digital de la Generalitat **Marc Realp**, presidió el acto de presentación del plan de inversión pública de la **Agencia de Ciberseguridad de Cataluña**, en una sesión celebrada con empresas del sector privado en el Distrito Digital, en L'Hospitalet del Llobregat.

"El nuevo modelo de ciberseguridad va mucho más allá, planificando una estrategia a cuatro años, focalizado en el equilibrio social y territorial, potenciando la incorporación y la generación de talento al sector y asegurando un mayor reparto del gasto entre múltiples proveedores. Para ello, invertiremos 232 millones de euros en más ciberseguridad para una Cataluña más digital", puntualizó Realp.

Por su parte, **Tomás Roy**, director de la Agencia de Ciberseguridad de Cataluña, presentó el nuevo modelo de aprovisionamiento, cuyo objetivo es dotarse de los instrumentos, del talento, de los servicios y de las capacidades necesarias. "Esta licitación define el camino que hemos trazado para alcanzar el objetivo que tenemos: un horizonte más ciberseguro" explicó.

Contempla cinco acuerdos marco, cada uno con diferentes necesidades de servicio:

- Consultoría y arquitectura de datos: Datos, seguridad, calidad CISOs, PMO, SMO, producto, innovación y capacitación técnica.
- Auditoría: Auditoría ENS, OAT, Auditoría ISO y otros.
- Comunicación, concienciación y difusión: Formadores, eventos, comunicación y traducción.
- Suministro y soporte de hardware: Soluciones de seguridad, infraestructura e integradores.
- Operación de la seguridad: Operadores, analistas, *pentesteros* e ingenieros.

Cada uno de estos acuerdos marco incluirá varios lotes según las necesidades del servicio. El total de los acuerdos marco suponen un valor estimado del contrato de 232 millones de euros distribuidos en 15 lotes durante este periodo.

Las empresas que quieran presentarse al proceso de contratación, podrán hacerlo hasta el 12 de este mes de abril. A fin de facilitar de manera clara la información más relevante sobre la contratación, la Agencia ha habilitado un apartado en su sitio web en el que se puede encontrar un conjunto de preguntas y respuestas. Además, también están disponibles varios vídeos explicativos para acompañar a las empresas en su proceso para presentar sus propuestas.

Con esta iniciativa da comienzo un nuevo modelo de aprovisionamiento y contratación que pretende dar una respuesta más eficiente y planificada a las necesidades de los diferentes servicios de la Agencia y agilizar y racionalizar la compra pública, reduciendo los plazos y favoreciendo la concurrencia.

Para hacer frente a los retos de la ciberseguridad, el Gobierno catalán ha ido incrementando progresivamente el presupuesto anual destinado a la inversión en los últimos años. Este año, y en los próximos cinco años, la cifra se multiplica para dar respuesta a la necesidad creciente de innovación continúa para garantizar la ciberprotección: si en 2023 se invirtieron 30 millones de euros, a partir de 2024 se destinarán 58. Esto servirá para desplegar un nuevo modelo más estratégico, que incorporará más talento y que ampliará el modelo de ciberseguridad a diferentes ámbitos y territorios de Cataluña, y no sólo al entorno de la Generalitat.

ENTI y UNIVERSIDAD DE BARCELONA anuncian un potente Grado de Ciberseguridad para el curso 2024-2025

El Aula Magna del Edificio Histórico de la Universidad de Barcelona acogió el pasado 7 de marzo la presentación del Grado de Ciberseguridad, que impartirá la **Escuela de Nuevas tecnologías Intercativas** (**ENTI-UB**), a instancias e impulso de la **Universidad de Barcelona**, a partir del curso 2024-2025. Este nuevo estudio universitario, que es pionero en Cataluña, nace para dar respuesta a la alta demanda de profesionales de este sector, en el que, según alguna fuente, se calcula que hay 12.000 vancantes. Junto a Josué Sallent –en su calidad de director del Grado– también participaron en la presentación el vicerrector de Política de Digitalización, **Xavier Triadó**, y el director de la Agencia de Ciberseguridad de Cataluña, **Tomás Roy**.

Sallent –con un solvente pasado en la ciberseguridad, pues fue director de Cesicat, entidad precedesora de la actual agencia– explicó que el grado forma parte de la rama de las ingenierías, constará de cuatro cursos (240 créditos ETC) y ofrecerá cuarenta plazas. "No solo debemos centrarnos en crear buenos profesionales: tenemos que ayudar a formar buenos ciudadanos y contribuir a su desarrollo personal", dijo Sallent. El grado incorporará una mención en ciencia de datos para abordar los retos derivados de la existencia y el uso que se hace de los datos.

El director del grado también anunció que el 17 de junio tendrá lugar, en el Espai Bital de L'Hospitalet, la primera hackatón de Ciberseguridad de Cataluña, dirigida a los alumnos de ciclos formativos de grado superior. El objetivo es que sirva de punto de encuentro para aprender nuevas habilidades y poder interrelacionarse con empresas del sector.

Por su parte, durante el acto de presentación, el director de la Agencia de Ciberseguridad de Cataluña, Tomás Roy, se mostró satisfecho de la creación de este nuevo grado, porque trabaja en la línea de la profesionalización de la ciberseguridad: "Estamos en un momento dulce porque ahora se valora nuestro sector como una función. Hay que seguir trabajando en la formación dentro del ámbito, sobre todo en lo que se refiere a la adquisición de determinadas capacidades y perfiles, como los auditores, los forenses, los gestores de incidencias, etc.", precisó Roy.

Como cierre, el vicerrector de Política de Digitalización de la UB, Xavier Triadó, remarcó que "el sector de la ciberseguridad tiene muchos retos y necesita una actualización continua, que será posible gracias a la búsqueda constante".

TD SYNNEX

La Ciberseguridad en bandeja

Facilitamos a nuestro canal soluciones que dan cobertura a todos los segmentos IT más vulnerables a ciberataques.

Seguridad integral

End Point
Identidad y acceso
Contenidos
Seguridad en la red
Seguridad automatizada y monitorización
Seguridad de aplicaciones

¡Destacamos la nueva incorporación de Palo Alto en nuestro catálogo de soluciones!

aruba Instant on · cisco Distributor · IBM Distributor · Lookout · NETWITNESS
opentext | Cybersecurity · paloalto NETWORKS · radware · RSA
SONICWALL · STORMSHIELD · VERACODE · vmware · WALLIX CYBERSECURITY SIMPLIFIED

Contacta con TD SYNNEX: Security_ES@tdsynnex.es

Determina sus funciones, además de marcarse cuatro objetivos con ocho líneas de actuación y un comité para medir la eficiencia del trabajo hecho

El GOBIERNO VASCO aprueba los estatutos de CYBERZAINTZA y la nueva Estrategia de Ciberseguridad de Euskadi con el horizonte de 2029

El **Consejo de Gobierno** dio luz verde, en marzo, al Decreto por el que se aprueban los Estatutos de la **Agencia Vasca de Ciberseguridad**, que establecen las bases legales del organismo y define sus objetivos, funciones y estructura. Así, se establece que la **Cyberzaintza**, en coordinación con la **Ertzaintza**, cuidará de la ciberseguridad pública de la región, persiguiendo el cibercrimen y protegiendo las infraestructura críticas y sensibles del país.

También, se la encomienda "proteger y velar por el adecuado funcionamiento de las infraestructuras digitales y datos del sector público vasco" e "impulsar una cultura empresarial cibersegura, para contar con entornos más resilientes que permitan el desarrollo sostenible de la sociedad vasca".

En concreto en su artículo siete se determinan sus funciones entre las que destaca la de prevenir y detectar incidentes de ciberseguridad y responder ante ellos, promover medidas de protección frente a las ciberamenazas, investigar y analizar tecnológicamente los ciberataques sobre infraestructuras tecnológicas, sistemas de información, servicios de tecnologías de la información. Además, también se le otorgan las funciones de equipo de respuesta a emergencias (CERT) y de respuesta ante incidentes de ciberseguridad (CSIRT), en coordinación con el resto de organismos concernidos. También se le encarga recoger los datos de las entidades que gestionan servicios públicos o esenciales en Euskadi y organizar actividades para impulsar la cultura de ciberseguridad, estableciéndose que la Cyberzaintza es la representante oficial del sector público vasco ante otros organismos en este ámbito.

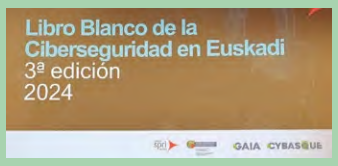
Estrategia Vasca de Ciberseguridad

En paralelo, también se ha aprobado la 'Estrategia Vasca de Ciberseguridad' que identifica sus desafíos hasta 2029, marcando el propósito, principios, objetivos y líneas de actuación de Euskadi este lustro. "La Estrategia Vasca de Ciberseguridad surge somo conclusión de este análisis y con el propósito de convertir a Euskadi en un país ciberresiliente y empoderar a su sociedad frente a la transformación digital", destaca el documento que se marca cuatro objetivos estratégicos y ocho líneas de actuación -ver gráfico-.

Además, determina que se contará con un modelo de gobernanza con tres comités a diferente nivel (estratégico, táctico y operativo) y otro que permita medir y "garantizar la eficiencia en la inversión".

Libro Blanco: la región acelera en el ámbito de la ciberprotección pasando de 111 organizaciones en 2018 a 242 en el último año

El País Vasco se presenta como un territorio atractivo para la inversión en ciberseguridad, con varias iniciativas de colaboración público-privada y un entorno fiscal favorable, según se desprende de la tercera edición del 'Libro Blanco de la Ciberseguridad en Euskadi', presentado en febrero, en Bilbao, en la Jornada 'Euskadi Digital segura: un ecosistema referente en Europa', organizada por la **Asociación de Industrias de Conocimiento y Tecnología** (GAIA), la **Asociación de empresas de ciberseguridad de Euskadi** (Cybasque) y el **Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente,** a través de **SPRI**.



Así, entre otras conclusiones del Libro Blanco, en lo que se refiere al ecosistema de ciberseguridad del territorio, Euskadi sobrepasa significativamente el número de empresas por millón de habitantes en comparación tanto con España, como con Europa. Concretamente, Euskadi supera las 79 empresas de ciberprotección por millón de habitantes, mientras que en el caso de España y Europa esta cifra se sitúa en 28 y 22,8 empresas por millón de habitantes, respectivamente. Este dato sitúa a Euskadi como una de las regiones de la UE con mayor concentración de empresas del sector, erigiéndose como una de las más activas a nivel europeo.

En este sentido, el **Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente** va a seguir avanzando, a través de SPRI, en su estrategia de favorecer el incremento y mejora de la ciberseguridad del tejido empresarial gracias, entre otros, al programa que este año dispondrá de un mínimo de 3,5 millones de euros.

ZSCALER y BT se unen para reforzar los servicios de protección de las empresas en la nube

Zscaler y **BT Group** han anunciado un *partnership* a través del cual, permitirá a BT ofrecer un conjunto completo de servicios de seguridad gestionados basados en la plataforma de seguridad en la nube Zero Trust Exchange impulsada por la IA de Zscaler. Como parte de este acuerdo, Zscaler también aportará a BT Group soluciones para proteger sus propias operaciones.

Así pues, los servicios gestionados de BT impulsados por Zscaler permitirán apoyar las iniciativas de reorganización de la conectividad, red y seguridad de las empresas. "En esta línea, proporcionan una mayor agilidad empresarial, reduce la complejidad de la infraestructura y protege a los clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar", indican sus responsables.

Las soluciones incluyen Zscaler for Users impulsado por su Zero Trust Exchange que cuentan con una puerta de enlace web segura (SWG, por sus siglas en inglés) que ofrece protección contra ciberamenazas en la nube e impulsada por IA, así como acceso de confianza cero a Internet y aplicaciones SaaS. También, cuentan con un servicio *cloud* que ofrece a los usuarios un acceso rápido y seguro con un enfoque Zero Trust.

Apuesta por el futuro.
Certifícate con ISACA Madrid.

Certificaciones en materia de gobierno, gestión de riesgos, cumplimiento, seguridad, control y auditoría de las tecnologías de la información y comunicaciones.

- Formación presencial y online
- Tasa de examen incluida
- Membresía 1 año gratuita
- Acceso gratuito a eventos
- Más de 1.200 profesionales asociados

Consulta las próximas convocatorias

Certificaciones

- CISA – Certified Information Systems Auditor. An ISACA® Certification
- CISM – Certified Information Security Manager. An ISACA® Certification
- CRISC – Certified in Risk and Information Systems Control. An ISACA® Certification
- CGEIT – Certified in the Governance of Enterprise IT. An ISACA® Certification
- CDPSE – Certified Data Privacy Solutions Engineer. An ISACA® Certification
- ITCA – Information Technology Certified Associate An ISACA® Certification
- CET – Certified in Emerging Technology An ISACA® Certification

Certificados

- CYBER SECURITY FUNDAMENTALS An ISACA Certificate
- CYBER SECURITY AUDIT An ISACA® Certificate
- COBIT An ISACA® Framework
- CCAK Certificate of Cloud Auditing Knowledge
- IT RISK FUNDAMENTALS An ISACA Certificate

WWW.ISACA.MADRID

ISACA® Madrid Chapter

Andalucía crea su Agencia y a su 'Clúster de Ciberseguridad', recientemente presentado, se adhieren 60 organizaciones como socios

Las CC.AA. apuestan por la ciberprotección a través de nodos dedicados, nuevas agencias e importantes inversiones específicas

Cataluña, Madrid y **País Vasco** son las tres regiones que, según el estudio 'Ciberseguridad en España en 2024: riesgos y tendencias', de **BeDisruptive,** tienen más riesgos de sufrir ciberataques este año, ya sea por acoger los principales eventos de la agenda política y social, como por ser objetivo de las actividades del cibercrimen. "España se enfrentará a grandes acontecimientos mediáticos y los cibercriminales no perderán la oportunidad de intentar sacar un beneficio económico de los mismos con sus actividades. Todas las regiones serán susceptibles de ser atacadas, pero es cierto que algunas tendrán que tener la guardia aún más alta", ha señalado el CTI Leader de la compañía, **Iván Portillo**. De cualquier forma, las que más riesgo tienen también son las más maduras en este ámbito, dice el documento.

Entre las últimas iniciativas puestas en marcha a nivel autonómico, ha destacado la presentación del **Clúster de Ciberseguridad de Andalucía,** con más de 60 entidades asociadas, como **Accenture, ADA, Aptan** (Asociación de Peritos Judiciales Tecnológicos de Andalucía), **Ayesa, Babel, Clúster OnTech, Cybercrin, Evolutio, Fujitsu, Ghenova, GMV, Hispasec, Inetum, Innovasur, Jtsec, Minsait-Indra-Sia, Orange España, Palo Alto Networks, Promálaga, PwC, Sofistic, Softcom, Telefónica, Universidades de Córdoba, Granada, Málaga** y **Sevilla, Vodafone Innovation Hub,** entre otras. Y, están pendientes de inscribirse -al cierre de esta edición- otras como **Kaspersky, Netskope, S2 Grupo, TDK, Unia, Zscaler, Puerto, Diputación** y **Ayuntamiento de Málaga**.

Ubicado en el **Centro de Ciberseguridad de la Comunidad** (CIAN), en Málaga, durante su presentación, el consejero de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa, **Antonio Sanz,** resaltó que el propósito del Clúster coincide con el de la **Agencia Digital de Andalucía** (ADA), de hacer que la tecnología mejore la vida de las personas y se convierta en motor de desarrollo en la comunidad. También en la región, **Mar López,** responsable de Ciberseguridad para Salud y Sector Público, en **Accenture** y fundadora y vicepresidenta en Women4Cyber, presentó en Málaga su iniciativa local 'Foro de Mujeres Cyberlíderes de Andalucía'.

Por su parte, la **Comunidad de Madrid** anunció una inversión este año de 23 millones para reforzar la seguridad informática de sus infraestructuras y sistemas de información, según destacó su consejero de Digitalización, **Miguel López-Valverde,** durante un simulacro de ciberataque a un hospital, organizado por la compañía **TRC**. Además, el servicio de Salud de la Comunidad (Sermas) también aumentará en 2024 el equipo de personas especializadas con perfiles técnicos, legales y mixtos, para que den un enfoque completo a la protección informática y a la privacidad. La Comunidad, asimismo, ha firmado un acuerdo con **Cisco** para reforzar la ciberseguridad en la región. Cabe destacar también que, al cierre de esta edición estaba aún pendiente de elegir al director de la Agencia de Ciberseguridad de Madrid, que podría estar operativa antes de verano.

Murcia, por su parte, prevé triplicar su inversión, tras los recientes ciberataques sufridos. Pasará de 950.000 euros a más de tres millones, según el consejero de Economía y Hacienda, **Luis A. Marín**, que participó en la inauguración de las primeras instalaciones de **Fortinet** en la región. Esta inversión permitirá extender los servicios de ciberseguridad de la Comunidad a cerca de 30 municipios de menos de 20.000 habitantes existentes.

Por su parte, la **Agencia para la Modernización Tecnológica de Galicia** ha entrado a formar parte de la **Alianza Global de Ciberseguridad,** la iniciativa internacional y intersectorial de la que forman parte más de 130 empresas e instituciones, dedicada a reducir el riesgo cibernético y mejorar el mundo interconectado. Con ello, continúa fortaleciendo el ecosistema del Nodo Gallego de Ciberseguridad CIBER.gal.

En **Castilla la Mancha,** el consejero de Hacienda, Administraciones Públicas y Transformación Digital, **Juan Alfonso Ruiz Molina**, confirmó que ya se ha dado el visto bueno a la creación de la **Agencia de Transformación Digital** de la Comunidad, un organismo autónomo del que dependerán aspectos relacionados con la ciberseguridad, la política de comunicaciones, el uso de la tecnología en la nube y de la AI.

En **Extremadura,** se ha dado a conocer que la Junta, a través de la Consejería de Economía, Empleo y Transformación Digital, con la colaboración de las diputaciones provinciales de Cáceres y Badajoz, ya coordina una estrategia de ciberseguridad regional conjunta para integrar a Extremadura en la Red Nacional de SOC (RNS).

Entidades locales

En cuanto a ayuntamientos, **Granada** ha reformado su normativa de ciberseguridad para tener mayor "defensa" frente a ataques informáticos, para "concienciar también al ciudadano y hacer una administración más sencilla y amable", ha destacado el concejal **Vito Episcopo.** Por su parte, el ayuntamiento de **Murcia** anunció que formará a sus empleados en este ámbito, a través de la plataforma de 'Smartfense', y el consistorio de **Badajoz** ha aprobado un presupuesto específico para la contratación de servicios complementarios destinados a la constitución de un Centro de Operaciones de Seguridad. Así, la partida de 2024 del Área de Tecnología y Digitalización, de la que dependerá este SOC, ha alcanzado los 11,4 millones de euros.

Por último, la **Diputación Provincial de Málaga** ha continuado avanzando en el proceso de adecuación al Esquema Nacional de Seguridad tras obtener la certificación de 13 ayuntamientos y otros 13 están en vías de conseguirlo. Además, está en vías de lograr la certificación en mCeENS de los sistemas de la Diputación y del **Patronato de Recaudación provincial.**

JUNTOS SOMOS MÁS

Ciberseguros Globales Fuertes

+900

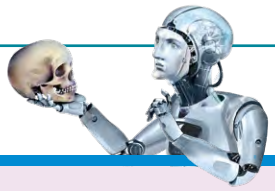
profesionales en España al servicio de la ciberseguridad

Innotec SECURITY

Part of **Accenture**

FIRST MEMBER · CERTIFIED BY TI TRUSTED INTRODUCER · Centro de Ciberseguridad Industrial · CSIRT.es · Red Nacional de SOC · ISACA · isms forum

CAVILACIONES SEGURAS



Lecciones tras un ciberataque

En la anterior "cavilación segura", titulada "2024: diario de un CISO", algunos de mis más fieles lectores creyeron que era una descripción de mi realidad laboral. Todo lo contrario: se trataba de uno de mis sueños, o pesadillas, más frecuentes. Dicen que escribir las experiencias oníricas contribuye a que se conviertan en realidad si son sueños o a desecharlas sanamente si son pesadillas. Veremos. Tengan por seguro que les informaré puntualmente si así ocurre.

En esta ocasión, siguiendo el mismo guión, compartiré los pasos que, como CISO de una compañía que cotiza en el IBEX 35, he tenido que seguir tras haber sufrido un ciberataque que trascendió a los medios de comunicación hace unas semanas.

"Ante el ciberataque, respondí a la obligación de enviar más de cinco formularios de reporte a distintas entidades, todos ellos con una estructura distinta y con exigentes plazos de entrega"

Observar cómo abren los noticieros en radio y televisión, tanto de cadenas públicas como privadas, así como los principales portales de noticias, con la primicia de un grave incidente de ciberseguridad ocurrido en la empresa en la que tú eres el máximo responsable de su seguridad es una experiencia única de la que se puede aprender mucho si se mantiene la calma y se practica la prudencia.

El primer hecho con el que tuve que enfrentarme: la información de la que se hicieron eco los medios de comunicación poco, muy poco, tenía que ver con lo que en realidad había sucedido. Pronto vi que tenía que tratar con tres desafíos: primero, responder y contener el ciberincidente; segundo, reportar a las autoridades relacionadas con la protección de infraestructuras nacionales críticas; y, tercero, informar directamente a los medios para mitigar los posibles efectos negativos que la desinformación podría causar a nuestros clientes.

El primer reto es, sin duda, esencial para la supervivencia de la organización que proteges. Afortunadamente todos los años realizamos un simulacro de respuesta a un ciberincidente severo, involucrando no sólo a los equipos técnicos, sino también a nuestro consejo de dirección, proveedores y clientes. Siempre encontramos debilidades a mitigar y escenarios que requieren nuevos métodos de actuación que no habíamos planeado anteriormente cómo tratar.

Para la segunda dificultad, al ser nuestra compañía un componente esencial de la infraestructura crítica de nuestro país, siguiendo la legislación europea NIS2, tuve que reportar al Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y, como también realizamos operaciones en Alemania, a la Oficina Federal de Seguridad de la Tecnología de la Información (BSI). El incidente nos causó una pérdida económica considerable, así que también tuve que denunciar el caso a las policías española y alemana. Al trabajar en un sector regulado, en paralelo, tuve que reportar lo sucedido, con todos sus detalles, a nuestra entidad reguladora nacional y a la europea. Los CERTs nacionales de los países en los que operamos también nos contactaron para conocer los detalles del ataque. En total, respondí a la obligación de enviar más de cinco formularios de reporte de ciber incidentes a distintas entidades, todos ellos con una estructura distinta y con exigentes plazos de entrega.

El tercer problema, la comunicación con el público, requirió la creación de un gabinete de prensa dentro de la compañía para gestionar directamente, sin intermediarios, las ventanas de información, el relato del impacto del incidente y los pasos que estábamos dando para volver a ponernos en pie: desde nuestra web y nuestra presencia en las redes sociales dábamos información consistente y real de nuestras actividades de respuesta y recuperación. De este modo evitábamos la desinformación, basada en rumores si cabe más perniciosos que la propia realidad.

Afortunadamente, hemos sobrevivido a esta "tormenta perfecta": hemos recuperado los sistemas impactados, hemos informado en todo momento a nuestros clientes y proveedores y el mercado ha premiado nuestra política de comunicación con una subida de la cotización de nuestras acciones.

En mi cuaderno de lecciones aprendidas he anotado los siguientes puntos: los simulacros anuales de ciberataques críticos son esenciales, dichas pruebas han de ser reales y deben involucrar a todas las partes presentes en la cadena de valor, tanto internas como externas. El proceso de reporte del incidente debe de realizarse de forma continuada y muy detallada para que podamos mantener el flujo de información requerido por las legislaciones nacional y europea, pero, preferiblemente, a través de un único canal, para evitar la duplicación de esfuerzo. Finalmente, el gabinete de prensa que gestione las crisis ciber reportará directamente al CISO y al CEO de la compañía e incluirá no sólo habilidades y experiencia en comunicación, sino también conocimiento en tecnología.

Así estaremos más preparados para resistir el próximo ciber incidente, que, tarde o temprano, afectará de nuevo a nuestros datos y sistemas.

Dr. Alberto Partida
linkedin.com/in/albertopartida

La ANSSI francesa crea un 'kit de ejercicios' para entrenar en incidentes a las empresas, durante los Juegos Olímpicos de París

Para prepararse y anticiparse antes posibles ciberincidentes durante los Juegos Olímpicos y Paralímpicos (JOP24), de julio a septiembre, la **Agencia Nacional de Seguridad de Sistemas de Información** (**ANSSI**) está ofreciendo a las empresas participantes una serie de 'kits de ejercicios' para ayudarlas frente a posibles crisis cibernéticas. Está diseñado y desarrollado específicamente para implementar un ejercicio que simule el contexto de los JOP24, que se complementa con el documento de la Agencia titulado 'Organización de un ejercicio de gestión de crisis cibernéticas'. "Los JOP24, por el interés que despiertan entre cientos de millones de personas y los importantes flujos financieros que generan, constituyen una oportunidad para actores con motivaciones diversas.

Desde la ANSSI se considera fundamental que "cada entidad sea consciente de su papel durante los JOP24, identifique los sistemas de información esenciales para el buen desarrollo del evento y prepare procedimientos operativos degradados si estos sistemas de información fueran objeto de un ciberataque (y no disponible)".

En concreto, el kit ofrece 12 formatos de ejercicios con tres niveles de dificultad, según el grado de madurez de la empresa en ciberprotección (se ofrece una autoevaluación para saber cuál realizar), que simulan los impactos comerciales más relevantes que podrían tener lugar en un ciberataque. El kit puede descargarse en https://cyber.gouv.fr

BARCELONA CYBERSECURITY CONGRESS

Fira Barcelona

MAY 21 - 23, 2024
BARCELONA - GRAN VIA VENUE

barcelonacybersecuritycongress.com
#BCC24

SECURE TODAY, SAFEGUARD TOMORROW

Register now with the promotional codes below and get your EXPO+ ticket for free or the FULL CONGRESS ticket now with 56% discount.

Join us!

EXPO+ PASS
FREE CODE: **2QJXJAAG**

FULL CONGRESS PASS
56% DC CODE: **MGVVAHAP**

•EFEMÉRIDES•

GMV: cuarenta años innovando. Treinta en ciberseguridad.

Me atrevo a afirmar, sin miedo a equivocarme, que la realidad de una multinacional española con más de 3.300 empleados, filiales en once países, clientes en más de 80, y una facturación próxima a los 400M€ desbordaría, cuarenta años después, las aspiraciones iniciales de su fundador, nuestro Profesor Juan José Martínez García. Sin embargo, esa realidad es el reflejo de las ideas que conformaron su visión emprendedora: la competitividad internacional del talento técnico que generan nuestras universidades, la pasión por la innovación y el trabajo bien hecho, cohesionados alrededor de un proyecto empresarial a largo plazo.

Nuestra proximidad a las actividades de I+D, inicialmente en mercados intensivos en tecnología como el aeroespacial y de defensa, siempre nos ha mantenido cercanos a las nuevas tecnologías e innovaciones con potencial disruptivo, como lo fueron las redes IP a comienzos de los 90. Nuestra apuesta por la "Seguridad Lógica" hace treinta años nos convierte, sin duda, en uno de los actores pioneros y decanos de la ciberseguridad española, con una propuesta global que nuestro lema "Secure eSolutions" sintetiza. Innovadores en aquel tiempo en dotarnos de un dominio "puntoes" y en implantar los primeros cortafuegos en nuestro país, iniciando así una declarada intención de continuar abriendo nuevos caminos, tanto en el plano tecnológico como el organizativo. De todos ellos hemos ido dando cuenta disciplinadamente en las páginas de la revista SIC: las certificaciones pioneras de nuestros SGSI, SGCN, SGP… nuestras herramientas propias de gestión de vulnerabilidades, gestión de eventos de seguridad, de vigilancia digital, de protección de ATMs, nuestra apuesta temprana por un SOC/CERT propio, … o implantaciones novedosas de la mano de *partners* líderes.

No podemos mirar el panorama de la ciberseguridad en estos treinta años sin una curiosa mezcla de admiración por la velocidad de la innovación, por un lado, y cierta desazón por promesas insatisfechas y la persistencia de algunos temas ya convertidos en clásicos, por otro. De la mano de cada nuevo ingrediente del cóctel tecnológico (las propias redes IP, la movilidad, la nube, la web 2.0 –redes sociales en particular– la Internet de las cosas…) han venido tanto una "bendición" en forma de nueva utilidad como un desafío adicional en el plano de los riesgos. Un desafío que es una carrera de armas en toda regla contra los atacantes, constituidos en toda una industria de capital privado y público en este tiempo.

Ciberseguridad: apuesta renovada

Ahora que se anuncia un nuevo concepto de identidad digital europea, y un nuevo soporte en el móvil para el eDNI en nuestro país, resultaría complicado afirmar que en este terreno se han excedido las expectativas. Difícil evitar cierta desazón por los limitados avances en la seguridad efectiva de los productos y servicios digitales, ahora que tenemos la CRA en ciernes…

Quienes hayan venido reclamando una mayor intervención de las administraciones vía regulación, dado que el mercado de forma patente no resolvía los desafíos de la seguridad, supongo que están en racha y de enhorabuena… aunque tal vez habrían deseado un panorama de cumplimiento más digerible y, en algunos casos, práctico. Algunos echamos de menos también mayores avances en la efectiva atribución y castigo al atacante, en lugar de colocar masiva y resignadamente casi todo el peso de esta pugna en el lado del atacado.

Quedan pendientes de correr ríos de tinta digital alrededor de temas recurrentes como el encaje organizativo de la ciberseguridad, la relación con la seguridad física, la transferencia de riesgos, los riesgos de la cadena de suministro y los que vaya abriendo la innovación tecnológica (IA, tecnologías cuánticas, IoT destacan en el horizonte actual). De manera que el desafío persiste, y eso nos motiva especialmente para seguir elevando nuestro nivel de excelencia, seña de identidad del equipo con el que he tenido el privilegio de recorrer estos años. En GMV confiamos en seguir contribuyendo a la construcción de una sociedad más segura y compartiendo nuestros logros en esta publicación, durante mucho tiempo.

Luis Fernando Álvarez-Gascón
Director General
GMV Secure eSolutions

En marcha la POST-QUANTUM CRYPTOGRAPHY ALLIANCE, abierta y colaborativa, de la mano de la FUNDACIÓN LINUX

La **Fundación Linux** ha creado la **Post-Quantum Cryptography Alliance** (PQCA). "Se trata de una iniciativa abierta y colaborativa para impulsar el avance y la adopción de la criptografía postcuántica", destacan sus impulsores a la vez que recuerdan que esperan acoger, en torno a ella, a expertos de la industria, investigadores y desarrolladores "para abordar los desafíos de seguridad criptográfica que plantea la computación cuántica, mediante la producción de implementaciones de software de alta seguridad de algoritmos estandarizados, al tiempo que respalda el desarrollo y la estandarización continuos de nuevos algoritmos poscuánticos".

Así, la PQCA buscará ser un punto de referencia para organizaciones y proyectos de código abierto que buscan bibliotecas y paquetes listos para producción, para respaldar su alineación con el denominado 'Aviso de ciberseguridad', de **la Agencia de Seguridad Nacional** (NSA) de EE.UU. Por ello, la alianza ha destacado su compromiso con "impulsar la agilidad criptográfica en todo el ecosistema durante los plazos descritos en el mismo".

De momento, se han unido a ella, como miembros fundadores, **AWS, Cisco, Google, IBM, IntellectEU, Keyfactor, Kudelski IoT, Nvidia, QuSecure, SandboxAQ** y la **Universidad de Waterloo,** entre otras organizaciones.Entre los primeros proyectos en los que participará la alianza destaca el Open Quantum Safe, creado hace una década por la Universidad de Waterloo, y que se ha convertido en uno de los proyectos de software de código abierto de referencia en este ámbito.

TOKIOTA

SOMOS UNA COMPAÑÍA INTELIGENTE EXPERTA EN SERVICIOS MICROSOFT Y CAPACIDADES CROSS DE CIBERSEGURIDAD PARA DESARROLLAR SOLUCIONES DE NEGOCIO.

Prevención de riesgos tecnológicos

Protección de datos e infraestructuras

Detección y respuesta ante ciberamenazas

Ciberseguridad con soluciones Microsoft

Nuestras capacidades, tu protección

www.tokiota.com

CISCO cierra la compra de SPLUNK y BROADCOM fusiona CARBON BLACK y SYMANTEC buscando competir con los 'gigantes' de la ciberprotección

Se calcula que el mercado mundial de IA para ciberseguridad rondará en este 2024 los 19.500 millones de euros, según Infinity Business Insights, experimentando un crecimiento anual que podría rondar el 23,3% hasta 2030. Sin embargo, las compras y fusiones en otras áreas, como la nube, el enfoque de confianza cero, la identidad, la visibilidad o la protección anti*phishing* continúan detrás de muchas de las operaciones más notables sucedidas en este trimestre.

Allurity se hace con SRLabs, Corus con Next Security, Babel con KinetIT y Evolutio con Securnet y Plusnet; Cisco cierra la compra de Splunk y Broadcom fusiona Carbon Black y Symantec, Hornetsecurity Group integra a Vade, Entrust adquiere Onfido, Zscaler a Avalor, CrowdStrike a Flow Security y Prowler consigue una ronda de inversión de más de cinco millones de euros.

En el ámbito nacional, la multinacional de alcance europeo **Allurity**, propietaria de la española Aiuken, ha reforzado su posición en el mercado global de la ciberseguridad con la compra en Alemania de **Security Research Labs** (SRLabs), continuando con su estrategia para liderar el sector en Europa, donde es ya una de las 10 firmas más grandes del ecosistema continental. De hecho, con esta operación, el grupo ya suma un total de ocho compras de empresas del ámbito, en los dos últimos años.

Además, la multinacional española **Corus,** ha incorporado a su oferta de consultoría y servicios tecnológicos para la transformación de las empresas a la compañía de servicios de ciberseguridad avanzada, **Next Security**. Así, esta última pasará a ser una nueva unidad de negocio, completando la propuesta del grupo con la incorporación de una amplia cartera de soluciones de protección basadas en Inteligencia Artificial (IA). Asimismo, **Evolutio** se hizo con **Plusnet Solutions** para afianzar su liderazgo en *customer experience* y con **Securnet,** empresa tecnológica portuguesa especializada en ciberseguridad y conectividad. La operación de la primera la permitirá acelerar capacidades en áreas clave como la integración y desarrollo de componentes tecnológicos, analítica, inteligencia artificial, automatización y biometría de voz.

Por su parte, **Babel** ha reforzado su posición global y se consolida como uno de los cinco principales *partners* mundiales de *outsystems* con la adquisición de la portuguesa **KinetIT**, que le permitirá posicionarse en el mercado luso como un actor clave en tecnologías exponenciales y en el área del *Low Code.*

Grandes operaciones

En el ámbito internacional, **Cisco** anunció en marzo haber completado la adquisición de **Splunk,** por casi 25.600 millones de euros, ganando en capacidades y oferta en visibilidad e información en toda la huella digital de una organización.

A esta gran operación se suma que **Broadcom** ha confirmado la fusión de **Carbon Black** con **Symantec** dando forma a su nuevo 'Enterprise Security Group', en el que realizará importantes inversiones. Además, **Hornetsecurity Group** ha integrado a la francesa **Vade,** especializada en seguridad del correo-e con más de 2.500 millones de mensajes analizados diariamente, se ha unido al grupo. **Entrust por su parte** ha adquirido **Onfido**, uno de los referentes en tecnología de verificación de identidad (IDV) basada en IA y en la nube.

Por su parte, **Zscaler** ha comprado la *startup* **Avalor**, especializada en la aplicación de la IA de forma específica a ciberprotección y **CrowdStrike** anunció que se hará con **Flow Security**, que ofrece una solución que protege los datos *cloud* en movimiento. La firma de capital privado **Haveli Investments** ha comprado **ZeroFox,** proveedor de "soluciones de ciberseguridad externas", por un montante de 322 millones de euros, con lo que dejará de cotizar en el índice Nasdaq. **Armis** ha adquirido a **Cyber Threat Cognitive Intelligence (CTCI),** especializada en caza de amenazas previas al ataque a través de IA.

Delinea ha anunciado un acuerdo definitivo para adquirir **Fastpath,** especializada en Gobierno y Administración de Identidades (IGA) y derechos de acceso de identidad. Este movimiento estratégico se une a su reciente adquisición de la *startup* israelí **Authomize** –un acuerdo que agrega tecnologías de respuesta y detección de amenazas de identidad (IDTR)– y marca una ampliación significativa en sus capacidades para mejorar el acceso privilegiado, los controles y la gobernanza, reduciendo el riesgo de ciberseguridad organizacional y asegurando el cumplimiento.

Por su parte, **Dynatrace** ha firmado un acuerdo definitivo para adquirir la británica **Runecast,** de mitigación de riesgos, seguridad y cumplimiento continuo, con sede en el Reino Unido. **Cohesity** que comprará los negocios de protección de datos de **Veritas,** creando un gigante de gestión y protección de datos valorado en, aproximadamente, 6.400 millones de euros.

Rondas de financiación

Entre las rondas de financiación más llamativas ha estado la realizada por **Prowler,** fundada por **Casey Rosenthal** y **Toni de la Fuente,** especializada en "facilitar la seguridad en la nube para todos". Ahora, fruto de su buen hacer ha recibido una inyección de 5,4 millones de euros en una ronda liderada por **Decibel VC.** Además, **Claroty** también consiguió una inyección de 92 millones de euros para continuar con su expansión global.

Además, **Device Authority**, ha recaudado 6,5 millones de euros para impulsar su plataforma de gestión de acceso e identidad de IoT empresarial. Asimismo, **Nozomi Networks** ha obtenido una inversión de más de 90 millones de euros, en la que participaron **Mitsubishi Electric** y **Schneider Electric**, para acelerar la misión de defender la infraestructura crítica de las amenazas cibernéticas.

myCloudDoor
Creating Future

MYCD-CERT

¿CÓMO PROTEGER TU ORGANIZACIÓN ANTE LAS CIBERAMENAZAS EMERGENTES?

PODEMOS SER TUS OJOS

Trabajamos para anticiparnos ante las últimas tácticas de ataque

Más que un SOC: Un aliado estratégico

Vigilancia constante | Anticipación y respuesta inmediata
Integración perfecta, seguridad reforzada | De la detección a la acción

MÁS INFORMACIÓN

Transforma tu Estrategia de Ciberseguridad con myCloudDoor MXDR
Detección y respuesta **24/7/365**

info@myclouddor.com | +34 911 85 31 50 | myclouddoor.com

FIRST
TF-CSIRT Trusted Introducer
Red Nacional de SOC
ens
ISO 9001
kiwa certificado ISO 27001 2290-5/24
kiwa certificado ISO 27701 2290-5a/24
A+ Applus®
Microsoft Solutions Partner Security Specialist Cloud Security Threat Protection

•EFEMÉRIDES•

S2 Grupo cumple 20 años convirtiéndose en el referente europeo en ciberseguridad y ciberinteligencia

Hace 20 años, cuando S2 Grupo abrió sus puertas como empresa especializada en ciberseguridad, este término no se utilizaba. Hablábamos de seguridad informática o de seguridad de la información y muchos nos decían que no había necesidad en el mercado de este tipo de servicios y que desarrollar tecnología nacional en este campo compitiendo con productos americanos, israelíes o rusos era, cuando menos, una temeridad o una tontería. Se equivocaban.

Han pasado 20 años, años de mucho trabajo, y de enormes cambios en la Sociedad. Cambios basados en una revolución tecnológica que nos ha traído muchas cosas buenas y algunas no tan buenas. En este entorno cambiante ha evolucionado también S2 Grupo. Acompañando a la Sociedad en este apasionante viaje.

S2 Grupo es una empresa de capital íntegramente español, especializada en el desarrollo de tecnología defensiva y ofensiva de ciberseguridad y en la prestación de servicios de ciberseguridad y ciberinteligencia. Su PTM, "Propósito de Transformación Masivo", se resume en una frase: "Anticipar un mundo ciberseguro", en definitiva analizar los cambios provocados por el uso y abuso de la tecnología para conseguir una sociedad digital libre y democrática donde impere la ley y donde se pueda desarrollar la vida tal y como la deseamos.

Desde su nacimiento en 2004 su objetivo ha sido garantizar la continuidad de los procesos y proteger los activos de empresas y organizaciones de todo tipo: información, sistemas de control, personas, etc, apostando por el desarrollo de tecnología nacional en sus ámbitos de actuación. Ahora cumple su 20º aniversario y mucho ha cambiado el panorama desde sus inicios, sin embargo, sólo ha acontecido lo que ya vaticinaban: la digitalización de la sociedad ha sido imparable y, con ello, la necesidad de ciberseguridad en todos los ámbitos de la sociedad.

S2 Grupo se ha convertido en una compañía de referencia a nivel nacional y europeo en ciberseguridad y ciberinteligencia. La empresa cerró 2023 con un volumen de negocio de 42 millones de euros, incluyendo una inversión en I+D superior a los 4 millones de euros, lo que supuso un crecimiento de más del 28% con respecto al año anterior, y una plantilla de más de 700 empleados. Presta sus servicios en más de 35 países y cuenta con instalaciones en Valencia, Madrid, Sevilla, Barcelona, San Sebastián, Bogotá, Santiago de Chile, Róterdam y Lisboa.

Altamente especializada en sectores estratégicos e infraestructuras críticas, cuenta con gran experiencia en administraciones públicas, en el sector industrial, en el de la salud, en transportes, alimentación, agua, finanzas, TIC y energías. En sus procesos, evalúan y mejoran la ciberseguridad de los sistemas de control industrial y, ante la tendencia a la convergencia de las Tecnologías de la Información (IT) y las Tecnologías para la Operación (OT), da soporte a las industrias para garantizar la seguridad de todo tipo de procesos en distintos sectores.

Ha conseguido que la tecnología de una empresa valenciana sea presentada al mundo como la base del modelo de seguridad español impulsado y defendido por el Centro Criptológico Nacional dependiente del Centro Nacional de Inteligencia. La tecnología que desarrolla está actualmente desplegada en empresas privadas de todo el mundo, en más de 200 organismos de la Administración General del Estado, en distintas Comunidades Autónomas y en entidades locales.

Esta misma tecnología se usa para garantizar la seguridad en procesos electorales de ayuntamientos, de Comunidades Autónomas, y del estado español, así como para garantizar la ciberseguridad en procesos electorales internacionales. **GLORIA** y **CARMEN** son los productos estrella de cibervigilancia y ciberinteligencia desarrollados en Valencia con proyección nacional e internacional.

Su objetivo es continuar creciendo en Europa y Latinoamérica, e invirtiendo en I+D+i, para desarrollar soluciones que permitan a Europa ser independiente tecnológicamente en ciberseguridad y ciberinteligencia. En este sentido, apuesta por trabajar para que España sea uno de los líderes mundiales en este campo apoyando el desarrollo de un Centro Europeo de Excelencia en Ciberseguridad.

Otro de los pilares de S2 Grupo está contemplado en su estrategia ESG, que describe su compromiso por desarrollar el negocio sin perder de vista su responsabilidad con las personas que trabajan en la compañía y con la sociedad. Por esto creó **#evoluciona2**, que son más de 150 iniciativas de buenas prácticas puestas en marcha para colaborar con los Objetivos de Desarrollo Sostenible (ODS) con el convencimiento de contribuir a un mundo mejor, más justo y ciberseguro.

S2 Grupo es también pionera en la concienciación y formación en ciberseguridad de vanguardia para todas sus disciplinas con impacto en la sociedad a través de proyectos como **ProtectIT** y **Enigma University**, en el que profesionales de la compañía, que son actualmente referentes internacionales en el ámbito de la ciberseguridad, forman a nuevas promociones de alumnos que quieren adentrarse en un sector que está en pleno crecimiento, impulsando sus conocimientos específicos y la captación de talento. Enigma está dirigido a estudiantes de grados universitarios relacionados con las Tecnologías de la Información, Ingeniería industrial, Inteligencia Artificial, Big Data, Bioingeniería e Ingeniería de Telecomunicación, principalmente.

Jose Miguel Rosell
Socio Fundador
S2 GRUPO

La notificación de vulnerabilidades crecerá otro 25% más este año

Los fallos de seguridad son considerados uno de los tres principales vectores de ataque por parte de los grupos cibercriminales. Y su número no dejará de crecer ya que, según un informe de **Coalition**, se prevé que este año se incremente la notificación de vulnerabilidades y exposiciones comunes (CVE) hasta las 34.888 vulnerabilidades (2.900 al mes), un 25% más que en 2023.

Y al desafío del mayor número que se registra, se suma el problema de parchearlas a la mayor brevedad posible desde que se notifican hasta que se solucionan, por lo que cada vez se apuesta más por priorizar esta labor, comenzando por determinar cuáles son realmente críticas.

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

MICROSOFT invertirá 1.950 millones en España para impulsar la IA y firma acuerdos con el CCN e INCIBE para mejorar la ciberseguridad nacional

El presidente del Gobierno, **Pedro Sánchez**, se reunió a mediados de febrero con el presidente de **Microsoft**, **Brad Smith**, quien, de visita en España, le anunció el plan de la compañía de cuadruplicar sus inversiones en nuestro país, alcanzando los 1.950 millones de euros en el año 2025.

Se trata de la mayor inversión de la multinacional tecnológica hasta la fecha en España, la cual, se destinará, principalmente, a impulsar el despliegue de la IA segura, e infraestructuras de nube. Para este último fin, Microsoft ya adelantó que abrirá una Región Cloud de Centros de Datos en la Comunidad de Madrid, y su intención de construir un Campus de Centros de Datos en Aragón, que dará servicio a empresas y entidades públicas europeas.

De izq. a dcha.: José Luis Escrivá, ministro de Transformación Digital; Pedro Sánchez, presidente del Gobierno; Brad Smith, presidente de Microsoft Corp.; Carol Browne, jefa de gabinete de B. Smith; y Alberto Granados, presidente de Microsoft en España

La colaboración se establece en el marco de la Estrategia Nacional de IA y la Estrategia de Ciberseguridad definidas por el Gobierno, y se articula en torno a cuatro líneas de actuación. Las dos primeras están encaminadas a la extensión del uso de la IA en la Administración pública y la promoción del uso de IA Responsable. En este marco, la tecnológica también anunció en febrero la creación del *Responsible AI Innovation Center* (RAIIC) en España, junto a 16 *partners* estratégicos, entre los que se encuentran **Accenture**, **DXC Technology, EY, KPMG, Minsait, PwC** y **Telefónica Tech**.

Las otras dos líneas de actuación tienen como objetivo el refuerzo de la ciberprotección nacional y la mejora de la ciberresiliencia de las empresas. Para ello, Microsoft y el **Centro Criptológico Nacional** (**CCN**) explorarán de forma conjunta la mejora de los mecanismos de alerta temprana y respuesta a ciberincidentes en las Administraciones públicas. Asimismo, se reforzará la ciberseguridad de las empresas, especialmente, pymes, junto al **Instituto Nacional de Ciberseguridad** (Incibe), ofreciendo acceso a la telemetría e información global sobre potenciales amenazas y ciberataques, además de llevar a cabo acciones de divulgación.

No cabe duda de que el uso de la IA está creciendo de forma exponencial. En España, "el 62% de las grandes empresas la utiliza y, cada vez más, la generativa, y un 25% planea hacerlo en los próximos 24 meses", destacó el presidente de Microsoft España, **Alberto Granados**, haciéndose eco de datos de IDC, durante el Microsoft AI & Innovation Summit, celebrado en Madrid el 20 de febrero, en el que se registraron más de 3.000 clientes y *partners*.

De hecho, "España aceleró el uso de la AI Generativa en 2023, multiplicándose por cinco en el último trimestre, y ya es el 4º país de Europa y el 9º del mundo", añadió el directivo, quien explicó que "estamos en el 'año 2' de la IA generativa, es decir, ya no se trata de pruebas de concepto sino de encontrar su caso de uso, y el objetivo es acelerar la adopción de los clientes y creemos que en España va a tener un impacto muy grande en la economía".

En este sentido, cabe destacar que, a partir de este abril, está a disposición de todo el mundo de forma general (GA) su solución estrella Microsoft Copilot for Security. Se trata de la gran apuesta de la compañía en IA generativa basada en datos a gran escala e inteligencia sobre amenazas, incluyendo más de 78 billones de señales de seguridad procesadas por Microsoft cada día, que combina con grandes modelos de lenguaje (LLM) para ofrecer perspectivas personalizadas y guiar a los profesionales para avanzar en sus estrategias de ciberprotección.

ZEROLYNX duplicará su facturación con un nuevo Plan Estratégico con más servicios, mayor internacionalización y un notable cambio societario

Para reforzar sus áreas de negocio y continuar el crecimiento marcado tanto fuera, como dentro de España, la española **Zerolynx,** que cumple seis años de vida en este 2024, ha puesto en marcha su Plan Estratégico 2024-2026., con el que espera poder triplicar su facturación a lo largo de los próximos tres ejercicios fiscales. Entre otras novedades, la estrategia tiene el sello de uno de los profesionales con más solvencia en este ámbito, **Manuel Monterrubio,** que se incorpora a la compañía como consejero –habiendo fundado empresas como **Alhambra IT** y **Exevi** (actualmente, integrada en **Sngular**)–.

Daniel González, Juan Antonio Calles y Manuel Monterrubio

Dentro de sus 'tripas', también se hicieron cambios considerables a lo largo de 2023, con la automatización de numerosos procesos bajo su nuevo CRM y una reestructuración a nivel directivo y societaria, donde **Juan Antonio Calles,** CEO de Zerolynx, y **Daniel González**, COO, controlan el 100% de la compañía. "Este ilusionante y ambicioso plan supone una rotura con nuestra zona de confort para construir un proyecto sólido y resiliente, que afronte de forma solvente los vaivenes de un mercado tan competido" resalta Calles.

Nuevo enfoque

El nuevo plan traccionará sobre tres ejes fundamentales: un nuevo portafolio de servicios mucho más amplio y completo, la expansión hacia nuevos mercados en los que hasta ahora no operaba y un crecimiento orgánico potente, con previsión de duplicar capacidades en 2026. De hecho, en su recién estrenada web pueden verse su nueva disposición, con un catálogo de servicios que cubre la totalidad de las funciones del NIST y que han mapeado con mimo y buen tino bajo dos escenarios diferentes: de forma sectorial, especializándose en las necesidades concretas de cada sector y de forma departamental, ofreciendo a cada área corporativa soluciones específicas para afrontar los problemas de seguridad desde su rol y posición en el consejo.

"Hemos apostado por un nuevo catálogo de soluciones con nuevos compañeros especializados, entre otras ramas, en sistemas, redes, Cloud, desarrollo seguro y GRC", explica González.

nunsys GROUP®

ERIS-CERT, CyberSOC especializado en Entorno de Operaciones OT/IoT/IoMT

SAFECLOUD de **SINGLAR**
es la Plataforma de Seguridad
de la Información Integral.

G-CONSULTING de **SINGLAR**
realiza la creación y seguimiento de Planes
Directores de Seguridad (PDS) y Privacidad.

SIRENA de **SINGLAR**
es la conexión con
plataformas de negocio.

SafeCloud®

G·Consulting compliance

SIRENA® Seguridad semántica

Nunsys integra tecnológicamente varios
productos propios de **Ciberseguridad**
SafeCloud, **G-Consulting** y **SIRENA** de Singlar

FIRST Engineering Security Together

CSIRT.es

TF-CSIRT

Red Nacional de SOC

Miembros cofundadores
y GOLD

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad
Categoría ALTA
RD 3/2010

"SOC Sothis ERIS-CERT"
Centro de operaciones de
Seguridad de la información

nunsys GROUP®

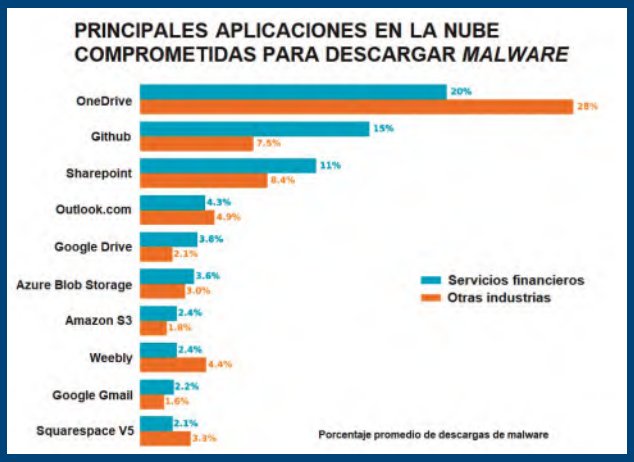
Especialistas en Seguridad Gestionada 24x7

960 500 631 nunsys.com

El *malware* a través de la nube ya representa el 50% de las descargas de las amenazas en sectores críticos

Los *infostealers* se ceban en el sector sanitario y el financiero sigue siendo uno de los principales objetivos del *ransomware*

Infostealers es la principal familia de *malware* y *ransomware* utilizada para atacar al sector sanitario, que figuró entre los principales sectores afectados durante 2023 por 'mega brechas', un tipo de ataques que llegaron a superar el millón de registros robados. Así se desprende de los datos recopilados por **Netskope Threat Labs**, que también han encontrado que el sector financiero se mantiene como uno de los principales objetivos de los grupos de *ransomware*.



En uno de sus más recientes informes, los especialistas de sus laboratorios analizaron el incremento sostenido de la adopción de aplicaciones *cloud* en Sanidad, así como las tendencias del *malware* en el sector. En este sentido, destacan entre otros aspectos que las descargas de software malicioso aumentaron el pasado año, pero se estabilizaron en el segundo semestre.

Así el *malware* distribuido a través de la nube terminó el año alcanzando el 40%, aproximadamente del total de descargas de *malware* en el sector, tras un máximo del 50% en junio, descendiendo ligeramente en la segunda mitad del año. Aunque Microsoft OneDrive siguió siendo la aplicación más popular en el sector de la sanidad, su uso fue significativamente inferior que en otros sectores. Slack ganó en popularidad, ocupando el segundo lugar en cargas (por detrás de OneDrive) y el quinto en descargas, una cifra significativamente superior a la de otros sectores.

Aplicaciones en la nube

Junto a este informe, Netskope Threat Labs publicó otro estudio en el que confirma una mayor adopción de aplicaciones en la nube en el sector de servicios financieros, y, al igual que en el sanitario, resalta el abuso de estos canales por parte de los criminales para eludir los controles de seguridad habituales en los ataques de *malware* y *ransomware*.

Aquí, las aplicaciones en la nube de Microsoft dominan este sector, especialmente OneDrive, Microsoft Teams y Sharepoint.

"El sector financiero sigue siendo uno de los más atacados por los grupos de *ransomware*, con los troyanos como el principal mecanismo de ataque", indican desde la compañía. "El malware distribuido a través de la nube representó el 50% de las descargas de software malicioso en el sector financiero, en línea con otros sectores, dada la capacidad de los atacantes para eludir los controles de seguridad habituales que dependen de herramientas como las listas de bloqueo de dominios y la monitorización del tráfico web, pero que no aplican los principios de confianza cero para inspeccionar rutinariamente el tráfico en la nube", terminan resaltando.

BANCO DE ESPAÑA selecciona a 14 compañías para su acuerdo marco, por 221 millones, para mejorar en digitalización y ciberseguridad

Accenture, Atos Spain y una unión temporal de empresas (UTE) integrada por **Ibermática** y **Altia** serán las compañías que más peso tendrán en el contrato que ha adjudicado el **Banco de España** y que cuenta con 221 millones de euros de presupuesto en tres lotes, en los están presentes estas cinco compañías.

En total, el organismo ha seleccionado a un total de 14 empresas que, a través de la figura de 'acuerdo marco', le darán servicio en sus necesidades de innovación y digitalización ante los "innumerables retos derivados de un entorno económico, social y tecnológico altamente cambiante", destaca el pliego. En concreto, con cuatro años de duración, el Banco de España contará con estas empresas para la "prestación de servicios profesionales de soporte, desarrollo y acompañamiento en el ámbito de las TIC", incluyéndose también, las actividades sujetas al ciclo de vida de las aplicaciones y productos.

En concreto, el primer lote, por 152 millones sin impuestos, contempla la contratación de servicios para la evolución, soporte y mantenimiento de iniciativas y soluciones de negocio. Además, de las mencionadas también participarán en él **Capgemini España, GMV Soluciones Globales Internet, Izertis** y la UTE conformada por **Inetum España** y **NTT Data.** El segundo, con 63,6 millones será para la evolución, implantación, soporte y mantenimiento de infraestructuras y ha sido adjudicado a **Indra, Inetum España, Logicalis Spain** y **Oesia Networks.** El tercero, por seis millones, para servicios de acompañamiento y soporte a la innovación, estrategia tecnológica y modelo operativo de TIC, ha sido adjudicado a Indra.

El organismo fijó entre los objetivos del plan estratégico 2024 la prioridad de una "modernización" para ser "más flexibles, eficientes e innovadores", junto al impulso decidido a su digitalización, la mejora continua de la ciberseguridad y la evolución hacia una organización más orientada al dato".

La POLITÉCNICA DE VALENCIA crea CIBERTRS, una *spin-off* especializada en protección y ciberinteligencia

La **Universitat Politècnica de València** (UPV) ha puesto en marcha una *spin off*, bautizada como **Ciber Tiempo Real Sistemas** (CiberTRS), que se centrará en ciberseguridad y ciberinteligencia, y a la que ha aportado su software HyBINT (Hybrid Intelligence), desarrollado por investigadores del Grupo de Sistemas y Aplicaciones de Tiempo Real Distribuido (SATRD). Se trata de un programa que permite integrar distintas fuentes de ciberinteligencia para el desarrollo de aplicaciones específicas de monitorización y detección de intrusiones mediante técnicas de inteligencia artificial (IA), particularmente *machine learning*.

"La fundación de esta empresa supone un nuevo reto para llevar al mundo empresarial desarrollos de investigación hasta ahora aplicados en grandes proyectos de protección de infraestructuras críticas", ha destacado **Manuel Esteve,** uno de los socios de la empresa e investigador del SATRD de la UPV. Junto a él, el equipo de CiberTRS lo completan **Israel Pérez Llopis**, investigador también de la UPV, y **Miguel Ángel Montalbo Cortinas,** abogado especialista en protección de datos. El grupo de la UPV promotor de CiberTRS ya ha desarrollado varios proyectos con el **Mando Conjunto de Ciberespacio** y la **Agencia de Defensa Europea** (EDA).

Westcon

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

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

Westcon | TechXpert

TechXperts

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

Westcon | Academy

Portal de e-learning (LMS)

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

Westcon | 3D Labs

3DLabs

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

Tech & Café

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

TechLab & Beers

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

www.westconcomstor.com

Partner success.
It's what we do.

•EFEMÉRIDES•

Asociación @aslan: 35 años pegados a la innovación

35 años dan para mucho. Durante ese tiempo, la Asociación @aslan se ha convertido en testigo y protagonista simultáneo de la rápida evolución tecnológica que ha vivido España. Más de tres décadas permiten enfrentar los envites de más de una crisis, incluida alguna propia y exclusiva del sector TIC como fue la de las *puntocom*; la irrupción de tecnologías disruptivas; las sucesivas generaciones de telecomunicaciones, un Efecto 2000 y hasta una pandemia.

En ese devenir frenético de acontecimientos y tecnologías, lo que ha permanecido inalterable en el tiempo es la quintaesencia de la Asociación, es decir, su compromiso a la hora de contribuir y divulgar la innovación digital. Desde que naciera en 1989, su empeño no ha sido otro que tejer un ecosistema digital en el que las empresas asociadas colaboren entre sí y saquen el máximo partido de sus sinergias.

A través de nuestro Congreso anual y, muy especialmente, de las más de 60 iniciativas que desarrollamos a lo largo del año (foros, almuerzos, seminarios, publicación de informes…), la Asociación @aslan ha desempeñado un rol fundamental aglutinando a actores clave en los procesos de transformación digital de muchas organizaciones. Hoy en día, los frutos de ese trabajo se plasman en un máximo histórico de empresas asociadas, rondando las 185, de las cuales más del 50% son internacionales y más del 30% cotizan en Nasdaq.

Puente de colaboración público-privada

Con un alcance que supera a los 100.000 profesionales, la Asociación @aslan es reconocida como un polo digital pegado al negocio y la innovación, en el que tanto empresas como Administraciones Públicas convergen con el resto del sector TIC para impulsar la modernización de sus infraestructuras y sistemas a las últimas tendencias.

En este sentido, tender puentes para fortalecer la colaboración público-privada es otra de nuestras máximas, considerando esta relación decisiva para que el sector de la innovación digital siga siendo decisivo para escalar posiciones en el ranking internacional de competitividad.

Durante estos 35 años, la Asociación se ha marcado fiel a sus principios con la finalidad de seguir creciendo en cantidad y, especialmente, en calidad, apostando por la diversidad de asociados tanto en actividad (fabricantes TIC, operadores, centros de datos, integradores, grandes distribuidores, proveedores *cloud*…) como en sectores estratégicos (utilities, logística, medios, sanidad…).

La ciberseguridad como imperativo

En esta andadura de más de tres décadas, la ciberseguridad ha ocupado un papel muy especial en la actividad de la Asociación. El incremento y sofisticación de las amenazas así lo han requerido, porque sin seguridad no hay margen para el éxito en los procesos de transformación digital. La superficie de ataque se ha amplificado de manera extraordinaria a medida que avanzaban nuevas tecnologías como los entornos *cloud* y el Internet de las Cosas (IoT) o que se apostaba más intensamente por la movilidad y el teletrabajo.

Desde la Asociación @aslan, con ayuda de todos nuestros asociados y para nuestros asociados, hemos prestado mucha atención a las nuevas tendencias y las mejores prácticas, poniéndolas en común y creando una base de conocimiento con los pies en el suelo. Esta escucha activa y esta aproximación eminentemente pragmática es la que hace muchos años nos llevó a negar que invertir en ciberseguridad sea una opción, sencillamente, es imperativo porque es algo inherente a la innovación digital. Ahora, además, se suma la ciberresiliencia, más aún con la irrupción de la Inteligencia Artificial (IA) y su papel ambivalente como vector tanto de ataque como de defensa.

35 años después, la clave de la Asociación @aslan para seguir manteniendo este nivel de actividad es subirse al tren de la innovación; no perderlo, ni nosotros ni nuestros asociados en este ecosistema de digitalización. Por otros 35 años más.

Alberto Pascual
Presidente
Asociación @aslan

CHECK POINT inicia su nuevo 'Partner Program' y colabora con MICROSOFT y NVIDIA en IA

Check Point ha anunciado la puesta en marcha de su nuevo Partner Program que tiene como objetivo fortalecer las capacidades y fomentar el crecimiento del sector. Entre otras mejoras, ofrece una simplificación de la estructura de niveles -Avanzado, Profesional, Premier y Élite, con beneficios diferentes en cada uno-, nuevos modelos de precios, certificación gratuita, una mayor especialización en áreas de gran valor, así como el relanzamiento de la aplicación, que ha sido evolucionada.

Además, la compañía ha anunciado sendas colaboraciones, una con **Microsoft** que utiliza el servicio Microsoft Azure OpenAI para mejorar Check Point Infinity IA Copilot, y otra con **NVIDIA** para mejorar la seguridad de la infraestructura de IA en la nube. Gracias a la integración con las DPU de NVIDIA, la nueva solución Check Point AI Cloud Protect permitirá mitigar las amenazas tanto a nivel de red, como de *host*. "Este enfoque integrado ayuda a garantizar que el sistema de seguridad conozca las actividades de la red y los procesos a nivel de *host*, lo que es crucial para salvaguardar el futuro de la IA", destacan desde Check Point.

Asimismo, ha alertado del aumento del uso de las herramientas y servicios de *spam* impulsados por IA y, en el marco de los servicios KYC (Know Your Client), cada vez más común en las empresas financieras, "se han creado servicios clandestinos que generan documentación falsa con ayuda de la IA y consiguen unos resultados muy fieles rápidamente", explican desde la compañía.

Junto a ello, Check Point ha destacado "el dramático incremento de los incidentes de *ransomware*", que se desprende de su '2024 Security Report'. El informe indica "un aumento del 90% en las víctimas extorsionadas públicamente por ataques de *ransomware*. Este tipo de ataques representa ahora el 10% de todo el *malware* detectado por los sensores la compañía". Además, "el número de víctimas extorsionadas públicamente se ha disparado hasta las 5.000, el doble que en 2023".

En su análisis, también evidencia una tendencia creciente en los ataques a dispositivos *Edge* y un aumento del *hacktivismo*. Además, Check Point ha detectado una escalada de los ataques a APIs web en 2024. En concreto, un aumento del 20% durante el primer mes del año, con respecto al periodo del anterior.

Centro de
Ciberseguridad Industrial

La ciberseguridad es el pilar de la industria inteligente.

La resiliencia se construye sobre la innovación y la experiencia.

Hazte miembro de CCI y accede a 8 plataformas para capacitar a tu equipo, diseñar proyectos seguros, caracterizar escenarios de ciberincidentes y encontrar servicios y soluciones de ciberseguridad industrial.

https://www.cci-es.org/plataformas

Paseo de las Delicias, 30 - 2°. 28045 Madrid. T +34 910 910 751

info@cci-es.org www.cci-es.org B blog.cci-es.org @info_cci

Ha presentado un fallo de seguridad en dispositivos con Bluetooth en RootedCON

Internacionalización, alto valor añadido en servicios y conservación del talento, pilares con los que TARLOGIC logró crecer un 30%

La firma gallega **Tarlogic** ha crecido el último año un 30% apostando por conservar el talento, internacionalizar su oferta –uno de cada cinco clientes ya es de fuera de España– y apostar por servicios de alto valor añadido. Así lo ha destacado su director de Operaciones y Financiero de la compañía, **Koldo Muñoz,** quien ha destacado la buena marcha de la compañía que ya supera los 12 millones de euros de facturación. "Necesitamos que nuestros profesionales estén bien remunerados, y a su vez, podamos competir en un mercado global con empresas que están en materia salarial en otras realidades. Día a día tratamos de buscar equilibrios incorporando el teletrabajo permanente desde cualquier ubicación", ha explicado.


Andrés Tarascó, cofundador de Tarlogic

La cifra consolida su tendencia de los últimos años (en el 2022 registró un alza de la facturación del 20%) y acelera el ambicioso plan de internacionalización activado por la empresa con sede en Madrid y en Santiago de Compostela. A corto plazo su objetivo es pasar del 20% al 50% de facturación con clientes internacionales alcanzando los 25 millones de ingresos, a través de clientes de sectores en los que la firma está muy implantada como Banca y Seguros, Retail, Telecomunicaciones, Energía y Sanidad.

Para conseguirlo, también se están acometiendo fuertes inversiones en innovación para poder crear nuevos productos y servicios, un aspecto en los que siempre ha destacado. "Queremos ser una compañía reconocida a nivel nacional e internacional por la calidad de nuestros servicios y productos, y esto pasa por tener a los mejores profesionales", ha comentado el cofundador de la empresa, **Andrés Tarascó** recordando su amplia gama de servicios y productos de alto valor añadido en campos como la ciberseguridad, ciberinteligencia, Red Team, *threat hunting* e *incidente response*.

Prueba de concepto

Por otro lado, aprovechando la celebración del congreso técnico RootedCON, el equipo de Tarlogic ha dado a conocer su nueva **auditoría de seguridad de Bluetooth (BSAM)** –que adelantó en un artículo, en SIC 158–, así como una demostración de cómo aprovechando vulnerabilidades de auriculares con esta tecnología de conexión se podrían escuchar conversaciones privadas cercanas, sin que el usuario se dé cuenta.

La prueba de concepto diseñada por el equipo de Innovación de Tarlogic y presentada por dos de sus integrantes, **Antonio Vázquez Blanco** y **Jesús María Gómez Moreno**, utiliza controles **BSAM** para detectar vulnerabilidades y conectarse a dispositivos sin que sus usuarios se den cuenta. En concreto, durante su exposición, profesionales de la compañía mostraron cómo **sortear la seguridad de los auriculares inalámbricos de grandes fabricantes** como **JBL** y **Samsung**.

La aplicación de la IA generativa al puesto de trabajo, protagonista en ASLAN2024

Bajo el título 'IA. Un gran avance en digitalización. Todo cambia', el Congreso&Expo ASLAN2024, organizado por la **Asociación @aslan,** que tendrá lugar el 17 y 18 de abril, abordará el impacto de la Inteligencia Artificial en el ecosistema de innovación y transformación digital. En esta 31ª edición, la organización ha querido centrar gran parte del programa en los retos y desafíos que trae consigo la aplicación de la IA generativa al puesto de trabajo, por lo que, entre otros aspectos, habrá un espacio dedicado al llamado 'Digital Workplace with AI'. "Las nuevas capacidades para realizar búsquedas de información mejoradas con procesamiento de lenguaje natural, la hiperautomatización inteligente, la generación de documentos contextuales o las recomendaciones o sugerencias personalizadas son solo algunas de las ventajas que trae consigo esta tecnología y que conduce a mayores niveles de productividad y eficiencia", destacan desde la asociación a la vez que recuerdan que también, supone grandes retos para la ciberseguridad y la privacidad.

El congreso también ofrecerá ponencias y mesas sobre ciberprotección e innovación digital y avanzará lo que está por llegar en los próximos años.

El 3D Lab de WESTCON-COMSTOR atrae a 1.500 usuarios y genera más de 25 millones de dólares en nuevos negocios para los *partners*

Westcon-Comstor ha dado a conocer su '3D Lab', una innovadora propuesta que permite probar soluciones de ciberprotección de varios proveedores para casos de uso diversos en un entorno de demostración virtual gratuito para *partners*, y que ya ha generado más de 23 millones de euros en nuevos negocios para sus socios desde su lanzamiento hace un año, a partir de soluciones de 12 fabricantes cuyos acuerdos se han cerrado tras las demostraciones de 3D Lab. Y es que, esta iniciativa les ayuda a que preparen demostraciones que permitan a sus clientes conocer de forma práctica el valor que aportan con su propuesta e integraciones, por ejemplo, de fabricantes como **CrowdStrike, Zscaler** y **Palo Alto Networks.**

Durante este año, más de 1.500 usuarios han hecho uso de los laboratorios y casos de uso del 3DLab que "destaca por su dinamismo, ya que permanentemente se van incorporando nuevos laboratorios", ha explicado el Director de Preventa del mayorista en España, **Iván Rodrigo,** que coordina esta iniciativa. "Hemos creado 3D Lab para que los socios puedan responder al auge de las plataformas de ciberseguridad 'todo en uno' y a la creciente demanda de soluciones multifabricante por parte de los usuarios finales", ha añadido **Daniel Hurel**, Vicepresidente de Cyber Security & Next Gen Solutions EMEA de Westcon-Comstor.

NEGOCIO Y CIBERSEGURIDAD

HAGA QUE SU NEGOCIO ESTÉ CIBERTRANQUILO

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

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

STORMSHIELD

www.stormshield.com

S2 GRUPO enciende nuevamente el crepitar de la ciberprotección en las Fallas

Por quinta vez en su dilatada historia, y entre la variadísima temática que jalonan sus imaginativas creaciones, las **Fallas** en Valencia volvieron a acoger en su reciente edición de 2024, a mediados de marzo, un tema cada vez más decididamente habitual en su temática convencional: la ciberprotección

Este hecho se debió una vez más a la innovadora acción puesta en marcha por la compañía especializada valenciana **S2 Grupo** en conjunción con la **Falla Chiva-Francisco de Llano**, plasmándose en su ideario: "Anticipando un mundo ciberseguro".

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

En este contexto "La Falla Cibersegura" 2024, se diseñó y construyó en torno a conceptos de ciberseguridad subyacentes al colectivo del reverso digital con el lema 'Cibermalotes'. Expertos de la compañía asesoraron en la creación del monumento –en esta ocasión diseñado por la afamada pareja **Cristina Camarasa** y **Alex Santaeulalia**–, quienes crearon un original conjunto figurinista infantil interactivo que enseña a los más pequeños, a partir del hashtag#_ciberseguridad, de manera divertida representando escenas de algunos de los riesgos más comunes en el mundo digital como son el robo de contraseñas, la tecnoadicción o el *phishing*, entre otros. **SIC**

42 millones de facturación en 2023, un 28% más, y una plantilla de 700 especialistas

José Miguel Rosell y Miguel Juan, cofundadores.

A tenor de los resultados cosechados, la trayectoria de S2 Grupo desde su creación continúa siendo fulgurante, habiendo cerrado 2023 con un volumen de negocio de 42 millones de euros, implicando un crecimiento del 28% con respecto al anterior y contando ya con setecientos especialistas en sus filas. Su vocación y pujanza expansiva genuinamente española les ha convertido en un referente internacional en ciberseguridad, presente en sectores de Distribución, Energía, Banca y Seguros, Sanidad, Industria y Administración Pública. Entre sus objetivos para este 2024, destaca continuar creciendo y aumentando la presencia de la ciberprotección en la industria 4.0, principalmente en el ámbito de OT.

S2 Grupo se ha convertido en líder del sector en España y Europa, y actualmente presta servicios en más de 35 países y cuenta con sedes en Valencia, Madrid, Sevilla, Barcelona, San Sebastián, Lisboa, Rotterdam, Bogotá, y Santiago de Chile. Es de destacar asimismo que en 2023 su inversión en I+D+i volvió a ser considerable, alcanzando los 4 millones, habiendo superado una vez más el 10% de la facturación anual sostenible.

S2 GRUPO y el MCCE acogen en Valencia a la delegación del MANDO DE CIBERDEFENSA DE JAPÓN

A mediados de marzo, S2 Grupo tuvo ocasión de abrir las puertas a la delegación del **Mando de Ciberdefensa Japonés**, encabezada por el general de brigada **Kimura Akitsugu**, en las instalaciones de la nueva y flamante sede –denominada La Centrifugadora, próxima a inaugurar– de la multinacional española de ciberprotección, acompañada por el vicealmirante **Javier Roca Rivera**, máxima autoridad del **Mando Conjunto del Ciberespacio-MCCE** español.

Bajo la dirección de los socios fundadores de la compañía española, **José Miguel Rosell** y **Miguel Juan**, hubo oportunidad de presentar a la delegación nipona las innovadoras soluciones en ciberseguridad, reafirmando el compromiso de S2 Grupo con contribuir a un futuro digital seguro. El encuentro destaca la posición como referente internacional en ciberseguridad de la empresa de origen valenciano.

comforte

¿Te preocupa que tu seguridad no cumpla con los estándares del PCI?

COMFORTE TIENE LA SOLUCIÓN QUE NECESITAS

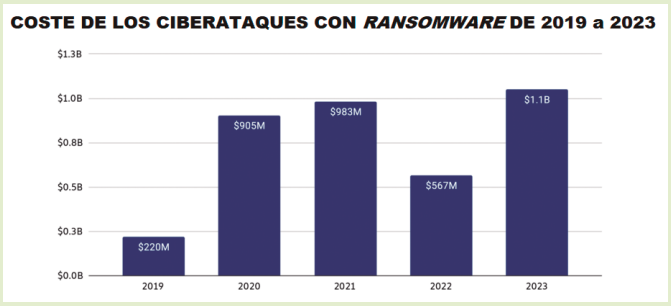
Simplifica el cumplimiento del PCI DSS v4.0 con Comforte AG y su plataforma de seguridad de datos

www.comforte.com

La fácil disponibilidad de herramientas de piratería y servicios de intermediario de acceso inicial (IAB) facilitó aún más su trabajo

El cibercrimen ganó en 2023 más de 924 millones de euros a través de rescates de *ransomware*, marcando un nuevo récord histórico

A pesar de todos los esfuerzos público-privados para luchar contra el *ransomware*, el año pasado se volvió a batir un triste récord: el de coste de rescates por este tipo de ataques superó los 1.000 millones de dólares (924 millones de euros), según datos de **Chainalysis,** especializada en *blockchain*, que, además, comentó que se trata de una estimación "conservadora". Y es que, esa cantidad no incluye el coste de la interrupción operativa, la pérdida de clientes y los gastos relacionados con la respuesta a incidentes y los análisis forenses de terceros. Sólo el rescate. Sirva como ejemplo que, a principios de año, dos nuevas víctimas de este tipo de ataques, la multinacionales **Clorox** y **Johnson Controls,** confesaron haber tenido tener pérdidas, en conjunto, de unos 70 millones de euros por este tipo de incidentes el año pasado.



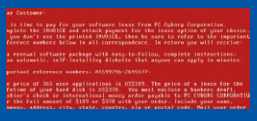
Los pagos de *ransomware* han ido en aumento desde 2019 cuando Chainalysis comenzó a registrar el mercado, además de una caída en 2022, con unas estimaciones de 524 millones de euros. Sin embargo, en 2023 se produjo una "gran escalada en la frecuencia, el alcance y el volumen de los ataques", impulsada por un aumento en el número de grupos que los llevan a cabo. Estos grupos se sintieron "atraídos por el potencial de obtener altas ganancias y menores barreras de entrada", reveló el informe. El *ransomware* como servicio (RaaS) también sigue teniendo un impacto enorme al atraer a más afiliados, muchos de los cuales apuntan a víctimas más pequeñas con rescates más bajos..

Ataques encadenados

También es de interés que, según un informe de **Cybereason,** en el que han participado un millar de profesionales de ciberprotección, casi cuatro de cada cinco (78%) de las organizaciones que pagaron una demanda de rescate se vieron afectadas por un segundo ataque de *ransomware*, a menudo por parte del mismo actor de amenazas. A casi dos tercios (63%) de estas organizaciones se les pidió que pagaran más la segunda vez. Y casi la mitad de las víctimas (46%) estimaron que las pérdidas comerciales rondan entre 0,9 y 9,3 millones de euros como resultado del ataque -incluso un 16% informó de pérdidas de más de 9,3 millones-.

El miedo a la difusión de datos robados, primera causa para pagar las extorsiones cibernéticas

Investigadores de la **Univerdad de Twente,** de Holanda, han realizado un estudio sobre cuáles son las razones que lleva a las víctimas de *ransomware* a pagar, en vez de optar por otras opciones. La primera es el miedo a que los datos robados sean filtrados en público. El documento también destaca que la decisión de pagar depende, en gran parte, de si la compañía dispone de copias de seguridad y si se tiene una empresa de respuesta a ciberincidentes (IR), lo que, en muchos casos, viene incluido con las pólizas cibernéticas. De hecho,



las empresas con un *backup* tienen, según el estudio, 27,4 veces menos de probabilidades de pagar el rescate que las que no lo tienen. Además, "contar con una póliza supone 2,7 veces mayores rescates, la exfiltración de datos corresponde a un aumento de 4,4 más, y cada aumento del 1% en los ingresos anuales de una víctima provoca un aumento del 0,12% de lo abonado".

El 60% de los profesionales europeos del sector cuestiona su formación académica, según KASPERSKY

Seis de cada diez profesionales en Europa cuestionan los conocimientos recibidos: un 17% considera que solo fueron algo útiles, el 27% ligeramente útiles y un 16% afirmó que no fueron de ninguna utilidad a la hora de cumplir con sus responsabilidades laborales. Así lo destaca un estudio realizado por **Kaspersky** a nivel global que, también, recomienda para incrementar el número de expertos en este ámbito apostar por enfoque multifacético centrado en el ámbito académico, en colaboración con las empresas. Asimismo, es de interés que el 48% de las empresas europeas necesitan más de medio año para encontrar un profesional cualificado en ciberseguridad. La falta de experiencia es uno de los mayores retos, junto con el alto coste de la contratación y la competencia global en la adquisición de talento. La multinacional también ha elaborado otro estudio sobre el mercado de la *dark web* en el último año, en el que alerta de un repunte significativo de robos y extorsiones y apuesta porque en 2024 habrá "una mayor presencia de servicios de criptomineros, de publicidad de páginas web fraudulentas".

Precisamente, como parte de sus esfuerzos de colaboración, la firma trabaja con **Interpol** en la lucha contra la ciberdelincuencia transnacional.

La ciberdelincuencia necesita sólo tres minutos para lograr sus objetivos, según CROWDSTRIKE

CrowdStrike ha hecho publicado su Informe Anual de Amenazas (Global Threat Report), en el que, tras estudiar la actividad de 230 grupos criminales, destaca un importante crecimiento en el robo de credenciales legítimas con las que los ciberdelincuentes explotan brechas en entornos *cloud* e incrementan la velocidad y el impacto de sus delitos sin ser observados. Entre otros datos de interés, alerta de que la velocidad con la que los ataques ocurren sigue acelerándose a tasas alarmantes. Eso sí, el tiempo medio para acceder a los sistemas corporativos se ha reducido desde los 84 minutos del año pasado a los 62 minutos este año. Sin embargo, se registró un ataque que consiguió su objetivo en tan sólo 2 minutos y 7 segundos y en tan solo 31 segundos un ciberdelincuente consiguió desplegar sus herramientas iniciales para intentar comprometer a sus víctimas. Además, advierte del incremento en el número de intrusiones interactivas y de las actividades de intrusión denominadas '*hands-on-keyboard*' (en un 60%) debido al uso de credenciales robadas para acceder a los sistemas de las empresas objetivo de los ataques, así como de los cada vez más numerosos ataques aprovechando la nube.

LOGICALIS
Architects of Change

Tu negocio, **siempre protegido**

Blindar los activos más valiosos de tu organización, los datos, es una obligación en un mundo cada vez más conectado, para evitar amenazas e impedir la interrupción de tu negocio:

Implementa una defensa proactiva en tiempo real para prevenir fugas de información y ataques.

Monitoriza constantemente identidades y accesos.

Realiza auditorías exhaustivas de la infraestructura IT para prevenir filtraciones de datos.

La tecnología PAM es tu mejor alternativa para estar siempre protegido y sin preocupaciones.

Logicalis Spain

Para más información, visita
www.es.logicalis.com/es/contacto

Ha ganado también varios contratos internacionales para sectores como las comunicaciones y el aéreo

GMV pone en marcha el programa de I+D+i 'Luis Valle' para desarrollar una nueva solución de identidad digital soberana y un SOC para el sector espacial

GMV ha obtenido el refrendo de la Iniciativa Estratégica de Compra Pública Innovadora (IECPI) del **Instituto Nacional de Ciberseguridad de España** (Incibe) para la puesta en marcha del Programa de I+D+i 'Luis Valle'. La propuesta de investigación del Programa se centra en dos proyectos: por un lado, el desarrollo de una solución de identidad digital soberana; y, por otro, la puesta en marcha de un centro de gestión de la ciberseguridad (SOC) para el sector espacial.

En cuanto al primero, la compañía destaca la importancia de la identidad digital soberana (SSI en inglés), por cuanto permite "el control personal de la información de identidad en la era digital", ya que es la propia persona quien gestiona sus datos, decidiendo cómo y cuándo comparte su información personal *online*. Un reto al que GMV quiere ofrecer su propuesta sustituyendo la tecnología *blockchain* que están usando para SSI las autoridades centrales de la UE de emisión identidades por otra alternativa denominada Criptografía Basada en la Identidad (CBI), en inglés *Identity Based Cryptography* y a veces *Identity Based Encryption* (IBE).

SOC espacial

En cuanto al segundo proyecto de investigación, se centrará en el desarrollo de un centro de gestión de la ciberseguridad (SOC) para el sector espacial, un ámbito que la UE considera crítico. En concreto, la investigación de GMV dará respuesta tecnológica a seis grandes retos en el caso de los SOC para el control espacial, como son la falta de trazabilidad de las acciones de los operadores los SOC, la falta de seguridad de los sistemas operativos y aplicaciones, en un entorno donde las conexiones hacia el exterior a través de Internet no son posibles, así como el problema de tener que hacer un bastionado manual de sistemas, la falta de herramientas de monitorización específicas para un centro de control de satélites, de compartición de inteligencia y, también, la escasez de equipos de respuesta a incidentes de ciberseguridad entrenados y especializados en centros de control de las organizaciones de espacio.

Por otro lado, GMV resultó adjudicataria de un contrato de 2,3 millones de euros, en Reino Unido, para desarrollar una nueva generación de *switch* White Rabbit basado en tecnología de hardware abierto. Además, desde principios de año, continua a buen ritmo liderando el proyecto AVIS de la **Comisión Europea**, mejorando la navegación de embarcaciones autónomas en vías navegables del interior de Europa, usando los sistemas europeos de navegación por satélite (E-GNSS) y Copernicus. La **Organización Europea para la Seguridad de la Navegación Aérea** (Eurocontrol), además, le adjudicó otro contrato para la evolución de Augur, servicio que este organismo presta gratis a pilotos, usuarios del espacio aéreo y proveedores de servicios de navegación aérea, desde 1998, y que verifica la integridad y fiabilidad de las señales GPS. El buen hacer de GMV ha sido reconocido con el galardón Aster a la "Trayectoria Empresarial", en los premios que desde 1982 organiza la **Escuela de Negocios ESIC.**

El Mº DE TRANSFORMACIÓN DIGITAL lanza una consulta pública para luchar contra la suplantación de identidad en llamadas telefónicas

El **Ministerio para la Transformación Digital y de la Función Pública**, a través de la **Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales,** presentó, hasta finales de marzo, una consulta pública con la que va a recopilar posibles iniciativas normativas y mecanismos técnicos y operativos que ayuden a poner freno a las estafas telefónicas de suplantación de identidad. Se trata de uno de los primeros acuerdos adoptados ante el incremento de estos fraudes tras las reuniones que el Ministerio ha mantenido con los diferentes agentes implicados. Estas estafas usan llamadas telefónicas y mensajes de textos alarmantes en los que los delincuentes se hacen pasar por supuestos agentes de una empresa de servicios o un organismo público, engañando al consumidor para que proporcione información personal y financiera confidencial, facilite sus claves personales o realice alguna acción.

La consulta tiene como objetivo acelerar el consenso de actuaciones frente a estas estafas que están causando importantes daños financieros y económicos a consumidores, empresas, entidades bancarias y organismos públicos.

La quinta parte de los ciberataques DDoS llevados a cabo en 2023 fueron dirigidos al sector transporte, según TEHTRIS

Al igual que el transporte de mercancías, el sector del transporte público se ve gravemente afectado por los ciberataques en las épocas de mayor tráfico. Las redes ferroviarias nacionales o los aeropuertos aumentan su vigilancia durante ciertos periodos, como los vacacionales o fines de semana en los que los ciberciminales suelen incrementar sus ataques, por su mayor demanda. Precisamente, según el informe anual Threat Intelligence de **Tehtris,** en 2023, el sector del transporte fue víctima de hasta un 17% del total de los ataques DDoS.

De hecho, los aeropuertos se han convertido en un objetivo prioritario en Europa desde que comenzó la guerra en Ucrania con más de 30 aeropuertos como víctimas de ataques DDoS. Sirva como ejemplo que, sólo en el primer semestre de 2023, los ciberataques dirigidos al sector de la aviación aumentaron un 24% a nivel global, una tendencia continúa acelerándose en 2024 a medida que incrementan las superficies de ataque y se sofistican las amenazas, según advierten los expertos de la compañía. Entre los sistemas que más riesgos presentan, por el beneficio que supone un ataque con éxito, están los de clasificación de equipajes, los de iluminación de pistas, además de los de protección por vídeo, obligatorios en la zona de embarque, y los sistemas de visualización a distancia, que ofrecen la información de seguimiento de aviones que usan los pasajeros.

¿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 que además presta servicios de ciberseguridad a otros países de Europa (CTC) (*)
- Centro de servicios de Ciberseguridad para Sanidad

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

Se dieron a conocer varias vulnerabilidades en sistemas Bluetooth e, incluso, en la infraestructura ferroviaria

ROOTEDCON 2024 reúne, junto a PROTAAPP, ISACA, SECURITERS y CRIPTORED, a 6.100 inscritos batiendo su récord

Durante tres días, en marzo, **RootedCON** se volvió a convertir en el congreso de ciberseguridad técnica de referencia en España. En su edición más numerosa –con más de 6.100 asistentes registrados–, cinco salas en paralelo y la colaboración en ellas de iniciativas y asociaciones como **Securiters, ProtAAPP, Criptored** e **Isaca,** los asistentes pudieron atender conferencias y mesas redondas en las que se revelaron posibles vulnerabilidades en infraestructuras críticas, como las balizas de la red ferroviaria, por parte de **David Meléndez** y **Gabriela García,** hasta en sistemas de comunicaciones como el Bluetooth, a cargo de investigadores de **Tarlogic.** Sin duda, las ponencias que centraron más atención fueron las relacionadas con la aplicación de la IA generativa a diferentes aspectos de la ciberseguridad.

No faltaron mesas redondas notables como la dedicada a emprendimiento en la que participaron referentes como **Daniel Solís, Pedro Castillo**, **Román Ramírez, Eduardo di Monte** y **Juan López**, siendo moderados por **Santiago Moral** Igualmente, se expusieron interesantes investigaciones técnicas del grupo APT **MuddyWater** por parte de expertos, como **Marc Rivero** y **Sandra Bardón,** o geopolítica con una ponencia sobre operaciones iraníes contra Israel. Además, la presidenta de la Asociación de Internautas, **Ofelia Tejerina**, aprovechó para dar a conocer su recientemente nombrada junta directiva.

También, se celebró la 'noche hacker' con más un centenar de participantes en busca de vulnerabilidades y que contó con un fondo de 1,4 millones para encontrar vulnerabilidades en nueve compañías. En total, se reportaron más de 44 fallos de seguridad, uno de ellos especialmente crítico. No faltó el recuerdo a un gran profesional fallecido el pasado año como es **Ángel Pablo Avilés 'Angelucho'**, a quién se dio, a título póstumo, el premio Raúl Jover por su labor en concienciación y por reinsertar a jóvenes que fueron detenidos por delitos cibernéticos. La directora de RootedCON, **Arantxa Sanz**, clausuró el encuentro recordando que este año será el de internacionalización del congreso con ediciones en Portugal y Panamá, entre otras.

FUNDACIÓN GOODJOB: cuando la accesibilidad digital se alía con la Ciberseguridad

En el contexto del multicongreso, la **Fundación GoodJob** organizó un debate bajo el tema de 'Accesibilidad Digital como clave en la ciberseguridad: Programa IMPACT#aliada', moderada por **César López**, Director General de la Fundación, que contó con la participación de **Marcos Manchado** (**MTP**), **Ricardo García** (**Atos Iberia**) **David Torres** (**NTT Data**) y **Román Ramírez**, Director Académico de los programas #IMPACT. Todos destacaron la necesidad de este tipo de programas que, además de formar, apuestan por la incorporación de los alumnos al mercado laboral.

Por otro lado, como ya dio cuenta SIC en su edición anterior, la Fundación fue reconocida con el 'Premio Zero Project 2024' a la educación inclusiva y tecnologías de la información y la comunicación (TIC). Un galardón que recogieron presencialmente en las Oficinas de las **Naciones Unidas,** en Viena, Austria, su presidente, **Jorge Albalate**, así como López y Ramírez, acompañados de compañeros de la Fundación y del agregado de la Embajada Española. Hasta el momento, se han formado más de 950 con este programa.

ANDALUCÍA celebra su tercer congreso regional constatando su firme apuesta autonómica por la ciberseguridad

En marzo pasado, organizado por la **Agencia Digital de Andalucía** (ADA), a través del **Centro de Ciberseguridad de Andalucía** (CIAN), se celebró en Málaga la tercera edición del Congreso de Ciberseguridad de Andalucía que contó con ponencias y mesas de debate en diferentes salas y, de forma paralela, con una zona expositiva con *stands* de las principales empresas del sector, zona para demostraciones, talleres prácticos y actividades de *networking*.

Antonio Sanz

El alcalde de la ciudad, **Francisco de la Torre**, y el consejero de Presidencia, **Antonio Sanz**, lo inauguraron ante los más de 3.500 asistentes, tanto en presencial como en *straming,* destacando la labor realizada en este ámbito en el último año. "La ciberseguridad no es sólo una inquietud y necesidad de una sociedad andaluza cada vez más digitalizada, sino también un sector económico en pleno auge en nuestra comunidad", comentó Sanz.

ROCKWELL AUTOMATION muestra la importancia de la ciberprotección en OT como pilar de la fábrica inteligente

En el marco de su ROKLive EMEA 2024, celebrado en febrero en Madrid, la compañía especializada en automatización industrial y transformación digital, **Rockwell Automation,** destacó su apuesta por el desarrollo de soluciones de ciberprotección avanzadas, diseñadas para apoyar a sus clientes en su camino hacia la digitalización y la 'fábrica inteligente'. Además, la empresa ha expandido sus servicios de seguridad gestionada mediante la colaboración con socios estratégicos como **Claroty, Dragos, Fortinet, Cisco** y **Verve**. Unas alianzas que permiten integrar soluciones completas de SOC, proporcionando las herramientas necesarias ante amenazas cibernéticas. Y es que, para la compañía, la creación de ciberresiliencia en sus clientes a través de la ciberseguridad OT es una de sus cinco áreas clave, en la que "desarrollamos capacidades especializadas para estos entornos, garantizando la seguridad y la continuidad de sus operaciones en la era digital", señaló **Eric Chalengeas**, Regional VP.

Bitdefender Global Leader In Cybersecurity

¡Detenga más ransomware y ciberataques avanzados!

Automatice, simplifique y centralice la seguridad en: endpoints, redes, nubes, identidades y aplicaciones de productividad.

Bitdefender ha sido nombrado líder en
The Forrester Wave™: Endpoint Security, Q4 2023

FORRESTER®
WAVE
LEADER 2023
Endpoint Security

Leer más:

Trusted. Always.

bitdefender.es

La autenticación sin contraseña, cada vez más usada, gracias al uso de factores de autenticación y biometría

Los ataques a la identidad se sitúan a la vanguardia, aprovechando que el 60% de las cuentas corporativas no tienen MFA

Durante el pasado año, los ciberdelincuentes lograron comprometer a algunas de las organizaciones más grandes del mundo aprovechando las vulnerabilidades de autenticación y acceso. De hecho, más del 26% de todas las respuestas frente a incidentes de Talos, la división de ciberinteligencia de **Cisco,** involucraron el uso de credenciales comprometidas en 2023.

Si bien la autenticación multifactor (MFA) sigue siendo una primera línea de defensa fundamental contra los ataques basados en identidad, los actores maliciosos están utilizando formas creativas de robar credenciales, destaca la multinacional. Y es que, a pesar de su creciente adopción, cuatro de cada diez cuentas de las empresas, de media, carecen de una MFA sólida, con el riesgo que supone.

Por ello, su informe 'Trusted Access Report 2024' destaca un cambio de paradigma que sitúa la identidad a la vanguardia de las ciberamenazas en un momento en el que prima el trabajo híbrido, aunque las autenticaciones de trabajadores en remoto están decreciendo desde 2020. Entre otros aspectos relevantes indica que la autenticación sin contraseña continúa aumentando: la adopción de factores habilitados por WebAuthn, incluidas claves de seguridad y tecnología biométrica como Touch ID, creció un 53% durante el pasado año.

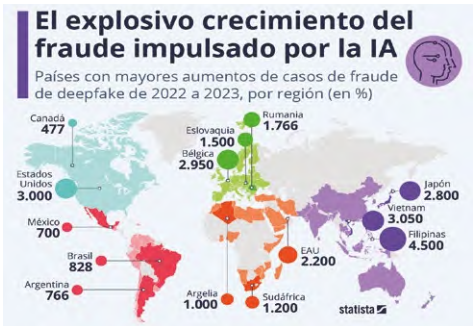
Falta de actualizaciones

En cuanto a la biometría y políticas, menos del 4% de las organizaciones implementan políticas explícitas de autorización o denegación basadas en la geografía. Es notable que, según la investigación, el porcentaje de fallos debido a dispositivos desactualizados aumentó un 75% en 2023.

"Cuando la gestión de identidades y accesos es deficiente o inadecuada, aumenta la superficie de ataque. A medida que se crean más relaciones entre dispositivos, identidades y permisos, resulta cada vez más difícil monitorizar qué usuarios están haciendo qué. Las organizaciones deben adoptar un enfoque de seguridad que priorice la identidad, combinando autenticación robusta con redes y seguridad en una solución completa", apunta **Ángel Ortiz,** director de Ciberseguridad en Cisco España.

Para 2026, el incremento de *deep fakes* hará que una de cada tres empresas que usan la biometría en ciberseguridad pierdan la confianza en ella

El problema de la confianza en lo digital puede suponer también un paso atrás a lo conseguido mediante biometría en autenticación y ciberprotección. Así lo destaca un informe de **Gartner** que avanza que los *deep fakes* con imágenes hiperrealistas generadas con Inteligencia Artificial (IA), pueden hacer que el 30% de las empresas pierdan la confianza en las soluciones de autenticación biométrica facial para 2026, según predice**.**



Y es que, a medida que las imitaciones de IA se vuelven más realistas y más fáciles de generar, también se reducirá la fiabilidad de los sistemas de autenticación y verificación a través del rostro, de acuerdo con la firma analista en su Cumbre de Gestión de Riesgos y Seguridad, celebrada en febrero, en Dubai.

Aunque ahora la mayoría de las soluciones biométricas faciales utilizan la detección de ataques de presentación (PAD) para determinar la "vivacidad" de un usuario que intenta autenticarse con su rostro, con el mayor realismo de los *deepfakes* y la complejidad de los ataques que los usan, se complica distinguir rostros falsos de verdaderos. Gartner ha alertado de que los 'ataques de inyección' de este tipo aumentaron un 200% en 2023.

Los equipos de TI y seguridad cada vez más unidos en la lucha contra las ciberamenazas, según COMMVAULT

Commvault ha dado a conocer un reciente informe en el que destaca que "los silos tradicionales entre los equipos de ITOps y de seguridad están empezando a romperse, a medida que las organizaciones se dan cuenta de la importancia de una mayor colaboración para combatir la avalancha de ciberataques más sofisticados".

Realizado junto a **The Futurum Group**, el estudio titulado 'Overcoming Data Protection Fragmentation for Cyber-Resiliency', contó con la opinión de más de 200 ejecutivos de TI de alto nivel y de C-Suite (más de la mitad de los cuales eran CIO, CSO y CISO) en América, EMEA y Asia-Pacífico. En él, casi todos los encuestados (99%) indicaron que la relación entre los departamentos de ITOps y de seguridad ha aumentado en los últimos 12 meses. Para aquellos que describieron la relación entre ITOps y seguridad como "conectada", el 64% declaró que ahora tienen objetivos compartidos para mantener la seguridad de la empresa y el 70% declaró que tienen procesos y procedimientos conjuntos para las operaciones diarias. Sin embargo, aún queda trabajo por hacer. Por ejemplo, sólo el 48% declaró haber establecido procesos y procedimientos conjuntos para mitigar o recuperarse de un incidente.

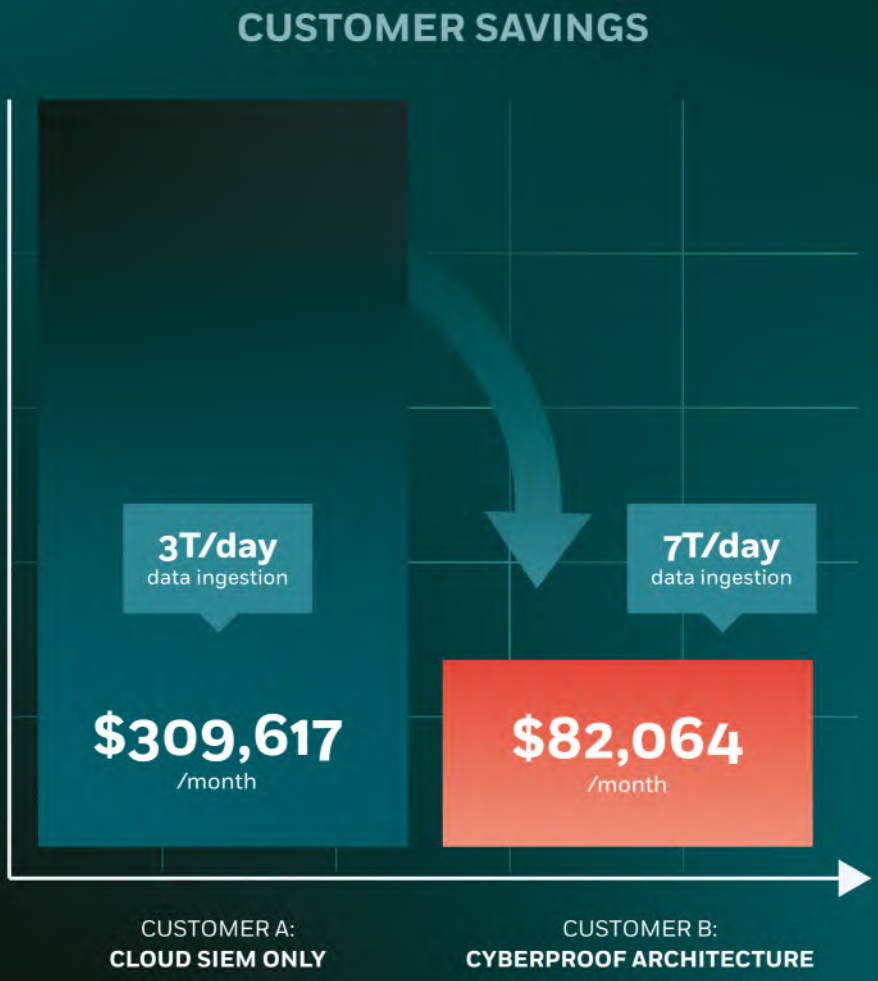

Melissa Hathaway

Fuerte apuesta

Además, la compañía ha fortalecido su Consejo de Ciberresiliencia con la incorporación de nuevos expertos. Presidido por **Melissa Hathaway**, una de las principales asesoras en materia de ciberseguridad de dos administraciones presidenciales en EE.UU., también forman parte de él **Roland Cloutier**, director de **The Business Protection Group**, exdirector de Seguridad de **Tik Tok**; **Shawn Henry**, director de Seguridad de **CrowdStrike; Mark Hughes**, presidente de Seguridad en **DXC Technology**; **Nancy Wang**, anterior directora general de Protección y Seguridad de datos de **AWS**; y, **John Zangardi**, CEO en **Redhorse Corp.** anterior CIO del Departamento de Seguridad Nacional de EE.UU., entre otros.

CUT YOUR SECURITY OPERATIONS SPEND

with CyberProof's cloud-native SecOps



VISIT US AT WWW.CYBERPROOF.ES

CyberProof®
A UST Company

PI Ernest Lluch i Martín 5, Edificio Telefónica 00, 7 planta
08019 Barcelona | Tel: +34 938 395 888 ext.: 400

También ha presentado la incorporación de Madrid como nueva región *core computing*, la quinta de Europa

Gecko es el nombre en clave de la nueva iniciativa de AKAMAI para ampliar su plataforma *cloud*, que ya es la de mayor distribución de todo el mundo

Akamai Technologies ha anunciado sus planes para integrar las capacidades de *cloud computing* en su red de Edge. Su nueva Generalized Edge Compute (Gecko) es capaz de ejecutar las cargas de trabajo de forma más próxima a los usuarios, los dispositivos y las fuentes de datos, ofreciendo al usuario mejores experiencias en la red. Se trata de dar respuesta a la inquietud de la alta dirección que considera que el uso de los servicios distribuidos en la nube aumentará en los próximos 12 meses, según un estudio de **ClearPath Strategies,** por sus ventajas

para procesar y analizar datos de inteligencia artificial (IA) y aprendizaje automático, de forma rápida y eficiente.

Una novedad que dio a conocer en Madrid, con la presencia de **Francisco Arnau,** Regional Vice President Spain & Portugal de la compañía, **Federico Dios,** Presales Director, y **Christian Scotti**, Senior Solutions Engineer, quienes explicaron cómo Gecko aspira a convertirse en una plataforma clave en entornos empresariales multinube. "Supone un paso más hacia un nuevo tipo de nube diseñada para satisfacer las necesidades de las aplicaciones modernas que requieren un mayor rendimiento, una latencia menor y una verdadera escalabilidad global, algo que las arquitecturas de nube actuales no pueden ofrecer", recuerda Arnau, a la vez que pone en valor que se aplicará en diferentes aspectos de ciberseguridad que gestiona la compañía.

De momento, la plataforma ya ha comenzado con pruebas iniciales con varios de sus clientes empresariales en sectores como la IA, los videojuegos multijugador y los contenidos sociales y multimedia, a los que seguirán otros nuevos para Akamai como *retail* inmersivo, la informática espacial, el análisis de datos y el IoT industrial y de consumo, que ya estudian las posibilidades que ofrece Gecko, comentó Dios.

Nuevos sectores

"Las actuales arquitecturas de la industria tratan la nube y las redes Edge por separado. Gecko está diseñado para permitir que la computación, de forma generalizada, se implemente sobre la red Edge mundial existente de Akamai, aprovechando las herramientas, procesos y capacidad de observación para proporcionar una experiencia coherente en todo el proceso de computación desde la nube hasta el Edge", destacaron los expertos de la compañía en su presentación. También, recordaron que "Gecko trasladará la computación tradicional más pesada, normalmente confinada a centros de datos centralizados, al *edge* de la red de Akamai. Esto llevará la computación integral a cientos de ubicaciones previamente difíciles de alcanzar, permitiendo a los clientes mover cargas de trabajo más cerca de sus usuarios".

Además, se dio a conocer que Madrid se ha incorporado como nueva región *core computing* de la compañía, convirtiéndose en la 25ª región en todo el mundo y la quinta en Europa, donde se pueden crear, implementar y escalar cargas de trabajo en la nube más distribuida. Akamai cuenta con su Connected Cloud, la plataforma en la nube más distribuida a nivel global con 4.100 puntos de presencia en todo el mundo, que será determinante en su nueva propuesta de Geck.

Por otro lado, la empresa ha dado a conocer sus nuevas funciones de App & API Protector, que vienen a reforzar y simplificar las defensas de seguridad.

VAR GROUP apuesta por España con una oferta centrada en ciberseguridad, *blockchain*, IA, *manufacturing* e industria 4.0 y *cloud journey*

Var Group, compañía perteneciente a **SeSa,** con sede en Italia, ha comenzado a trabajar en España a través de oficinas en Madrid y de la mano de sus socios locales como **Wise Security**, **Tech Value**, **Visualitics** y **Cadlog**. El objetivo de la firma es introducir sus productos y servicios, especializados principalmente en ciberseguridad, migración a la nube, aplicaciones de negocio, analítica, gestión de datos, IA y soluciones industriales.

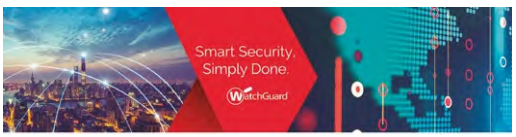
Con una facturación global de 703 millones de euros y una plantilla formada por más de 3.700 profesionales, el encargado de liderar la actividad de Var Group España será **Gorka Jiménez**, profesional con más de 20 años de experiencia y fundador de compañías referentes en el ámbito de la ciberprotección e identidad digital, que ocupará el puesto de CEO y que buscará impulsar sus áreas de negocios en

ámbitos tecnológicos tan variados como ciberseguridad, *blockchain*, *manufacturing* e industria 4.0, *data science,* IA y *cloud journey.*

"Nuestra intención es acompañar a las empresas del mercado español en su evolución digital simplificando la gestión tecnológica, consolidando las operaciones, y optimizando su eficiencia y gestión de recursos. Por eso, no nos vamos a limitar a proporcionar productos y servicios, sino que apostamos por entender continuamente las necesidades de sus clientes para ayudarles frente a los desafíos digitales", ha destacado Jiménez.

WATCHGUARD obtiene por segunda vez consecutiva el reconocimiento de Campeón en la Matriz de Liderazgo en Ciberseguridad 2023 de Canalys

WatchGuard Technologies ha sido reconocido como Campeón del Canal de Ciberseguridad en la Matriz Global de Liderazgo en Ciberseguridad 2023 de **Canalys,** que analiza diferentes aspectos de la propuesta de 30 proveedores. El informe anual evalúa el rendimiento de los proveedores en el canal durante los últimos 12 meses basándose en los comentarios de



los *partners,* las encuestas a los proveedores, las estimaciones de envíos de Canalys y la opinión de los analistas. Este reconocimiento marca el segundo año consecutivo en el que la compañía alcanza dicho estatus.

Canalys informó de que "el compromiso de WatchGuard con el canal quedó demostrado por su continua inversión en productos clave, programas e iniciativas de capacitación durante los últimos 12 meses, especialmente con los MSPs en los segmentos de las pymes y el mercado medio. Los *partners* valoraron muy positivamente la facilidad para hacer negocios y la calidad de la gestión de cuentas de la compañía".

"Todo lo que hacemos -desde las continuas mejoras de nuestro marco Unified Security Platform centrado en los MSP hasta los beneficios de habilitación y soporte para *partners* referentes en la industria que ofrecemos en nuestro programa de *partners* de canal WatchGuardONE- busca apoyar de la mejor forma a nuestros socios", destacó la CMO de WatchGuard y Vicepresidenta Senior de Estrategia de Negocio, **Michelle Welch.**


Audea
FEBRERO 2024...
22años
ofreciendo los mejores
servicios de Ciberseguridad
www.audea.com
info@audea.com

QUALYS amplía su alianza con ORANGE CYBERDEFENSE para fortalecer su oferta de servicios gestionados

Qualys ha anunciado una ampliación de su colaboración con **Orange Cyberdefense.** A través de ella, sus capacidades de gestión, detección y respuesta ante vulnerabilidades (VMDR) se incluirán en el servicio de inteligencia de vulnerabilidades gestionado por el área de ciberseguridad de la 'telco'.

Así, Orange Cyberdefense integrará las soluciones de Qualys, incluyendo VMDR, en su servicio Managed Vulnerability Intelligence, lo que proporcionará a sus clientes un mejor descubrimiento de activos, evaluación de riesgos y priorización gracias a la plataforma TruRisk.

"Orange Cyberdefense ofrece un servicio de seguridad integral y efectivo, y estamos encantados de que su Servicio Gestionado de Inteligencia de Vulnerabilidades sea ahora más preciso y escalable con la integración de nuestras capacidades VMDR", ha destacado el director de Ingresos (CRO) de Qualys, **Dino DiMarino.**

Además, esta asociación amplifica la integración actual BYOL (Bring Your Own License, o traiga su propia licencia) con OCI para la monitorización de vulnerabilidades, con el fin de ofrecer la plataforma completa de soluciones Qualys a través de Oracle Cloud Marketplace.

Por otra parte, Orange ha presentado su propuesta, 'Ciber Protección', un servicio para proteger a sus clientes frente a los riesgos en Internet, que se ofrece a través de su Centro de Seguridad, con propuestas exclusivas a través de alianzas con organizaciones como **Zurich** y **Mapfre**.

ACRONIS se une a la MICROSOFT INTELLIGENT SECURITY ASSOCIATION

Acronis se ha convertido en miembro de la **Microsoft Intelligent Security Association** (MISA), el ecosistema de proveedores de software independientes (ISV) y proveedores de servicios de seguridad gestionados (MSSP). Los miembros de MISA han integrado sus soluciones con la tecnología de seguridad de Microsoft para mejorar las defensas ante las crecientes amenazas.

La integración entre Acronis Cyber Protect Cloud y Microsoft Intune permitirá a los *partners* desplegar agentes de Acronis y aplicar planes de protección basados en grupos de Microsoft Entra ID, a través de Microsoft Intune, que se adhiere a las mejores prácticas de Microsoft. Ahora, los *partners* de Acronis pueden explorar con facilidad las opciones de integración directamente a través del catálogo de *partners* de MISA, con el objetivo de ofrecer a los MSP una experiencia más accesible para habilitar de forma eficaz un ecosistema integrado.

Acronis aboga por aplicaciones y servicios integrados de forma nativa que suelen utilizar los proveedores de servicios para impulsar la productividad y la eficacia.

Acronis Cyber Protect Cloud es una solución única, avanzada e integrada que reduce la complejidad y proporciona una protección integrada. También, engloba el ecosistema de Acronis de más de 200 integraciones con proveedores externos.

BREVES

■ **Revista SIC** ha actualizado en su web, con fecha de 1 de abril, el cuadro de CSIRT españoles registrados en distintos organismos. Destaca la aparición por primera vez en el listado del foro FIRST de **ITE-CSIRT**, la adición del **Centro de Seguridad y Vigilancia Digital** de **A3Sec** –que hasta ahora aparecía como CSIRT de Colombia– y la baja del CERT de **TIC Defense**. También entra en FIRST, por primera vez, **MyCloudDoor** que también aparece como candidato en la lista de Trusted Introducer. Otro nuevo candidato es **ACD-TRC**. **GTN-CERT** de **Getronics** y **GMV** (que culmina su entrada en todas las listas) pasan a estar "registrados" y el CSIRT de **Inetum** pasa a estar pendiente de volver a registrarse en la citada relación. Son novedad en ENISA los CSIRT de **Cyberzaintza**, **Innotec Security**, **Softeng** e **InnovaSur**. Este último también se incorpora a CSIRT.es.

■ En 2023 se produjo un aumento de más de 700 anuncios en la web oscura que ofrecen ataques de denegación de servicio distribuido (DDoS) a través de dispositivos de IoT, según un informe de **Kaspersky**. Estos servicios tienen diferentes precios, dependiendo de factores como la protección DDoS y la verificación por parte del objetivo, que van desde 20$ (18,5 euros) por día, hasta 10.000$ (9.300 euros) por mes. La web oscura también sirve como centro para *exploits* dirigidos a vulnerabilidades de día cero en dispositivos de IoT y paquetes de *malware* de IoT completos.

■ **Google** pagó 9,3 millones de euros en recompensas por errores, en 2023, en sus productos y servicios. Más de 600 hackers de 'sombrero blanco', en 68 países, fueron recompensados por el gigante tecnológico por descubrir fallos en sus sistemas. El pago único más alto otorgado fue 104.593 euros. Aunque las cifras parecen altas, son inferiores a las de 2022 cuando se pagaron más de 11 millones de euros por este concepto. Desde 2010, la compañía ha pagado casi 59 millones por vulnerabilidades.

■ La **Agencia para la Modernización Tecnológica de Galicia** ha suscrito un acuerdo de adhesión a la **Alianza Global de Ciberseguridad** (GCA), que le permitirá acercar la labor de esta organización internacional al ecosistema gallego concernido, agrupado en el Nodo Gallego de Ciberseguridad CIBER.gal. Además, reforzará su presencia internacional y la posición de Galicia como región pionera en la sensibilización, concienciación e investigación en este ámbito.

■ **IPM, a Ricoh Company,** obtuvo el premio al mejor *partner* de **VMware by Broadcom** en la categoría de capacitación técnica en la región de EMEA. El proveedor reconoce con estos premios el esfuerzo, el compromiso de sus socios clave en el mundo durante 2023.

■ **BeDisruptive** ha creado la línea de negocio Industrial Cybersecurity, con el objetivo de ofrecer servicios específicos para entornos industriales, la cual será dirigida por **David Marco**. Además, en su línea de *training & awareness,* ha puesto en marcha su Cyber Industrial Academy, un servicio que incluye cuatro planes formativos completos. Junto a ello, la compañía ha conseguido el Nivel Alto de la certificación del Esquema Nacional de Seguridad (ENS), y ha obtenido las nuevas certificaciones ISO 14001 e ISO 20000-1.

■ España estrena dos nuevos servicios como parte de la iniciativa Open Gateway, la propuesta que la GSMA anunció en el MWC 23 de Barcelona y que está orientada a crear un marco común y abierto entre operadoras cuyo fin es facilitar a desarrolladores y proveedores de servicios en la nube la creación de aplicaciones y servicios más seguros que se comuniquen entre sí de manera fluida.

■ El operador logístico **Bergé** obtuvo la ISO 27001 para los sistemas de gestión de la seguridad de la información, por la que se reconoce que la compañía ha implementado un conjunto de medidas técnicas, organizativas y legales para garantizar la confidencialidad, integridad y disponibilidad de la información. Además, compromete a la firma a evaluar de forma continua los riesgos a los que está expuesta y a mejorar constantemente el sistema de gestión.

ALLURITY, propietario de la española AIUKEN, refuerza su posición con la compra de la alemana SRLabs

Allurity, el grupo europeo de empresas referentes en ciberseguridad y propietaria de **Aiuken Cybersecurity**, ha cerrado la adquisición en Alemania de **Security Research Labs** (SRLabs), una consultora de ciberprotección con sede en Berlín y Hong Kong que presta sus servicios a clientes de 21 países en cuatro continentes, en los sectores de telecomunicaciones, banca, seguros, alta tecnología, servicios públicos y criptografía.

El Grupo considera esta operación como estratégica, ya que refuerza su posición geográfica y sus capacidades para ofrecer una oferta integral en el mercado global de la ciberseguridad. Esta adquisición le permite, además, avanzar en sus planes para liderar el sector en Europa donde, en la actualidad, es una de las 10 firmas más grandes del continente y genera aproximadamente 100 millones de euros en ingresos. Así, con SRLabs, Allurity da un paso significativo al potenciar su oferta con consultoría estratégica de ciberseguridad *premium*, conocimientos únicos y soluciones avanzadas en la industria.

Esta es la octava empresa que Allurity adquiere en el sector, en los últimos dos años. A SRLabs hay que añadir las suecas Arctic Group, ID North y Pulsen IAM, la danesa CSIS, la española Aiuken Cybersecurity, la portuguesa Cloud Computing y la suiza Securix.

"Con esta compra somos más fuertes a nivel europeo e internacional y nos abre las puertas sobre todo de Asia, un mercado en el que tenemos que estar, puesto que crecerá a tasas cercanas al 20% de aquí a 2028, y moverá una cantidad de dinero de aproximadamente 80.000 millones de euros en el mismo periodo", ha explicado **Juan Miguel Velasco,** CEO de Aiuken Cybersecurity y miembro del consejo de Allurity.

ORANGE BUSINESS, primera firma en ofrecer Prisma SASE con SP Interconnect, de PALO ALTO NETWORKS

Orange Business, Orange Cyberdefense y **Palo Alto Networks** han reforzado su asociación para ofrecer Prisma Secure Access Service Edge (SASE) con Service Provider (SP) Interconnect. Así la compañía francesa se convierte en el primer proveedor de servicios en todo el mundo que ofrece esta solución a través de su plataforma Evolution.

Este enfoque optimizado permitirá a sus clientes utilizar una oferta simplificada, que incluye conectividad más SASE administrado por un portal intuitivo de administración de nube multiusuario. También, se beneficiarán de una infraestructura de red global y escalada para impulsar ventajas comerciales SASE seguras y en tiempo real.

Además, desde una perspectiva de seguridad, la solución proporcionará acceso a la red Zero Trust (ZTNA) de extremo a extremo con visibilidad integral de la red de transporte para sucursales, nubes y centros de datos. Esto brindará, por ejemplo, a los clientes con estrategias multinube una mayor confiabilidad de la red.

Por otra parte, Palo Alto Networks ha firmado con un acuerdo con **Telefónica Tech,** "para ofrecer servicios gestionados de seguridad *cloud*, de red y puntos finales que faciliten a las empresas la aceleración de su transformación digital, asegurando que sus activos digitales están seguros en todo momento".

NOMBRAMIENTOS

El **Centro Europeo de Competencia en Ciberseguridad** (ECCC) ha elegido al que es ya su primer director oficial, el italiano **Luca Tagliaretti,** sucediendo así al interino que ha tenido el organismo desde su puesta en marcha, el español Miguel González Sancho. Cuenta con una amplia trayectoria habiendo ocupado roles de dirección en eu-Lisa y el Banco Central Europeo. Es ingeniero por el Politécnico de Milán.

Miguel González Sancho ha sido nombrado por la **Comisión Europea** como Responsable de la Unidad de 'New Connectivity Systems'. Hasta ahora al frente de la unidad de Head 'Cybersecurity technology and Capacity Building, de la D.G. Connect, es uno de los funcionarios de alto nivel españoles más destacados en la UE y ha ocupado durante tres años el puesto de Director Ejecutivo Interino del Centro Europeo de Competencia en Ciberseguridad.

La **Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales** (Seteleco) ha incorporado a **Andrés Ruiz** como Subdirector General de Integridad de las Telecomunicaciones. Ingeniero Informático por la Politécnica de Valencia (UPV), ha tenido un destacado papel con foco en la ciberprotección en los últimos 11 años en el Departamento de Seguridad Nacional (DSN), además de haber sido Oficial Nacional de Enlace de España con Enisa.

El Secretario General de la **OTAN,** Jens Stoltenberg, ha designado a **Farah Dakhlallah,** del Reino Unido, como portavoz de la Alianza, desde marzo. Cuenta con una amplia experiencia tanto en el sector público como en el privado, incluidas las Naciones Unidas, el gobierno del Reino Unido y AstraZeneca, así como en varias organizaciones de medios. Sucede a Oana Lungescu, que fue portavoz de 2010 a 2023.

Defensa ha nombrado jefe del Mando del Espacio (Mespa) al General de División, **Isaac Crespo.** Hasta ahora segundo jefe y jefe del Estado Mayor del organismo. Salió de teniente de la Academia General del Aire en 1988 y es piloto de caza y ataque, con F18 y Eurofighter, del que fue el primer jefe del primer escuadrón con el caza europeo. Cuenta con 73 misiones de guerra, entre ellas, la Operación ISAF en la BA de Herat (Afganistán).

Joanna Świątkowska ha sido elegida como Secretaria General Adjunta de la **Organización Europea de Seguridad Cibernética** (ECSO)/CYBERSEC. Ha trabajado para UBS y la Oficina Nacional de Seguridad Presidencial polaca, además de haber sido directora del European Cybersecurity Journal.

Incibe ha encomendado a **María Eugenia López Hernández** la dirección de Comunicación del organismo, habiendo sido hasta ahora Responsable de Conocimiento y Concienciación para empresas y profesionales. También coordinadora del Grupo de Trabajo del Foro Nacional de Ciberseguridad, es licenciada por la Pontificia de Salamanca en Periodismo, Publicidad y Relaciones Públicas, habiendo trabajado con anterioridad para Mnemo y talento Solutions, entre otras.

Oscar Díaz ha sido promocionado por la **Agencia de Ciberseguridad de Cataluña** a Director de Centros de Competencia e Innovación en Ciberseguridad**.** Previamente ha trabajado en Servihabitat, PwC, EY, Axa y Capgemini, entre otras. Es ingeniero en Informática por la Autónoma de Barcelona.

EAGLESIGHT | MNEMO

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

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

Solicita tu prueba gratuita

TF-CSIRT Trusted Introducer · CSIRT.es · Red Nacional de SOC

info@mnemo.com
Mnemo
mnemo.com

BBVA y CISCO suman fuerzas de nuevo para acelerar la transformación digital e impulsar la innovación

Cisco y **BBVA** han anunciado el refuerzo de su alianza, y han firmado un Acuerdo Estratégico que engloba todo su portafolio de software y servicios (WPA, Whole Portfolio Agreement), que proporciona a BBVA un acceso más rápido a la completa oferta de software de Cisco y a los servicios de Experiencia de Cliente (CX). BBVA es la primera institución de servicios financieros europea que firma un WPA con Cisco en Europa y América Latina.

Jordi García (BBVA) y Oliver Tuszik (Cisco), durante la firma del acuerdo

Este acuerdo de cinco años con BBVA incluye soluciones de ciberseguridad, colaboración, centro de datos, redes y servicios, abarcando operaciones en varios países e incluyendo servicios proporcionados por un equipo especializado de Cisco. Además, el acuerdo simplifica la gestión al consolidar 3.000 contratos individuales en un único acuerdo unificado, agilizando las operaciones globales de tecnología de BBVA y optimizando la eficiencia. "Durante la próxima etapa de nuestra asociación estratégica, aprovecharemos conjuntamente el poder de todo el portafolio de Cisco, incluyendo las últimas innovaciones impulsadas por la IA, para acelerar la transformación digital de BBVA", ha señalado **Oliver Tuszik**, presidente de Cisco para EMEA.

Desde 2016, BBVA y el equipo dedicado de Cisco han colaborado para crear el banco del futuro. Esta alianza digital estratégica, junto a acuerdos con otras empresas tecnológicas de referencia, ha acelerado la transformación de la entidad bancaria.

"La alianza de BBVA con Cisco es más que una relación proveedor-cliente. Después de ocho años trabajando juntos en asociación estratégica, las oficinas y los empleados de BBVA en todo el mundo tendrán acceso no sólo a los actuales desarrollos tecnológicos sino, también, futuros de Cisco", explica el director global de Ingeniería de BBVA, **José Luis Elechiguerra**. "Además, el acuerdo nos permite lograr importantes mejoras en eficiencia y productividad", añade el director global de Estrategia, Finanzas y Control de ingeniería de la entidad, **Jordi García.**

WISE SECURITY GLOBAL reafirma su apuesta por la Gestión de Identidades Digitales con su DID Authenticator, como avanzó en SECURMÁTICA

Wise DID Authenticator simboliza el comienzo de una nueva era en la que la seguridad se fusiona con la simplicidad, ofreciendo una solución robusta para la gestión de credenciales verificables de usuario, estableciendo un nuevo estándar en la gestión de identidades digitales. El proyecto con **Betmedia** ha sido seleccionado entre más de 300 propuestas como una iniciativa vanguardista, apoyada por Ceuta y acelerada por Ceuta Open Future.

En el foro del pabellón 'España', enseñó al público del MWC2024, en febrero, cómo superar uno de los mayores retos a los que se enfrentaba su cliente Betmedia: la verificación de identidades y la gestión de accesos. La solución Wise DID Authenticator busca garantizar el cumplimiento normativo y la seguridad, asegurando una experiencia de usuario sin precedentes.

"Wise DID Authenticator No es sólo una aplicación; es un guardián para la identidad digital en un mundo sin contraseñas", ha explicado el director de Digital Identity de la compañía, **Óscar Flor**, que también ha destacado la necesidad de este tipo de soluciones en un sector como el del *gambling*, con una alta regulación.

NOMBRAMIENTOS

● El **Grupo ING** ha promocionado a **Gustavo Lozano García** a Retail CISO, sumando esta responsabilidad a la de CISO para Iberia. Ha ocupado este rol en DIA, además de otros puestos destacados en Grupo Sia y Deloitte, entre otras. Es ingeniero en Informática por la Pontificia de Comillas.


● **Unicaja** ha promocionado a **Juan del Río** a Director de Ciberseguridad, y ha apostado por **Juan Carlos Valle** como Director de Operaciones de Seguridad. Del Río, con más de 15 años de experiencia, ha trabajado para S21sec, Fujitsu e Ingenia. Es ingeniero en informática por la Universidad de Málaga. Valle ha sido CISO de Liberbank y ha ocupado puestos de responsabilidad, entre otras, en Minsait, Accenture y Thales.

● **Cepsa** ha reconocido el buen trabajo de **Javier Galindo** ascendiéndole a Responsable de Seguridad de la Información (RSI). Con una amplia trayectoria en Westcon, Teléfonica, Tecnocom y Dimension Data Luxemburgo, entre otras. Es ingeniero en Informática por la Universidad Autónoma de Madrid.

● **Eduardo González,** hasta ahora CTO y CISO de **Maxam,** ha sido ascendido a Global CTO y CISO. Ingeniero en Informática por la UAX, ha trabajado previamente para Parkeon, Amper, Landata y Alcatel-Lucent.

● **Clariane** ha apostado como CISO por **Carmelo Zerpa.** Con una amplia trayectoria en dirección estratégica de ciberprotección, ha estado en Fujitsu, Viewnext, Dimension Data y Tecnocom, entre otras.

● **Roger Pablo Nevado** ha sido elegido por **Ifema** como Responsable de Ciberseguridad. Ha desempeñado roles de responsabilidad en SIA Group, MACC Residencial, Capgemini Engineering, Pullmantur, entre otras. Es ingeniero técnico de Sistemas por la Pontificia de Salamanca.

● **Guillermo Cordero** es el nuevo Head of Cybersecurity de **Gransolar Group**. Previamente ha trabajado para Seur, Media Markt e I-Joy Europe.

● **Grupo Bankinter** ha fichado a **José Ossuna** como Director de Soporte de Control de Riesgos TIC. Ha ocupado roles de responsabilidad en EY, PwC y Eurocontrol, entre otras. Es graduado en Ingeniería de Sistemas de Telecomunicaciones por la Universidad de Alcalá.

En ALSO estamos contigo para ayudarte a crecer en tu negocio

NUESTRA PROPUESTA DE VALOR

¿Cómo ayudamos a desarrollar tu negocio en Ciberseguridad?

- Formación y capacitación
- Desarrollo de negocio
- Generación de demanda
- Servicios profesionales

Porque somos expertos en desarrollar el negocio de ciberseguridad de nuestros partners

ALSO TE OFRECE:

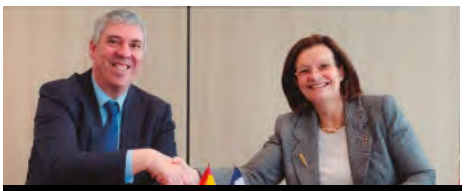
- Marcas líderes del mercado
- Migración de solución a Cloud
- Expertos en Ciberseguridad
- Automatización de la gestión de tu negocio con ALSO Cloud Marketplace
- Soluciones que se adaptan al mercado
- Consultoría adaptada a tus clientes

Contacta con un especialista de ALSO

comercial.es@also.com | +34-697172423

INDRA y THALES colaboran para impulsar el desarrollo y comercialización de sistemas de defensa de vanguardia

Indra y **Thales** han firmado un acuerdo para colaborar en materia de defensa con el objetivo de acelerar el desarrollo de tecnologías europeas de vanguardia y aprovechar sinergias para competir en el mercado español e internacional. Ambas empresas quieren sacar partido a las oportunidades de negocio relacionadas, especialmente, con sistemas radar, de ciberseguridad, sistemas de comunicaciones y simulación.


José Vicente de los Mozos (Indra) y Pascale Sourisse (Thales)

En el ámbito de la ciberdefensa, ambas aprovecharán sinergias en programas impulsados por la **UE,** como AIDA (Análisis de Datos con Inteligencia Artificial), así como otras iniciativas con clientes europeos e internacionales. En el área de sistemas de comunicaciones, en el que ya han trabajado juntas con anterioridad, aprovecharán las sinergias y complementariedades tecnológicas ya identificadas para reforzarse.

Para impulsar estas acciones se creará un Comité Directivo conjunto que definirá la estrategia y pondrá en marcha grupos de trabajo específicos, entre otros aspectos.

"La colaboración industrial es absolutamente crítica para que Europa mantenga su liderazgo y tenga voz a la hora de decidir hacia dónde va nuestro futuro. Este acuerdo sirve para encontrar sinergias, entregar mejores sistemas y desarrollar nuevas tecnologías en el estado del arte", ha destacado el consejero delegado de Indra, **José Vicente de los Mozos.**

El acuerdo, además, fortalece la base industrial de la defensa europea, uno de los objetivos declarados de la Política de Seguridad y Defensa de la UE.

Alianza entre CYBERMADRID y la ASOCIACIÓN ESPAÑOLA DE EMPRESAS CONTRA EL FRAUDE

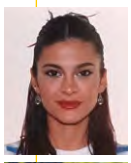
El **Clúster de Ciberseguridad de Madrid** (**CyberMadrid**), y la **Asociación Española de Empresas Contra el Fraude** (AEECF) han firmado un convenio marco de colaboración para promover y difundir la importancia de la lucha contra el ciberfraude y la promoción de la ciberseguridad entre sus respectivos colectivos.

Damián Ruiz y Jorge Hernández

La ciberestafa crece exponencialmente y existe una ingeniería social cada vez más sofisticada. Esto exige una respuesta holística y proactiva que consiste en una fuerte concienciación de la sociedad en su conjunto y en la implementación de medidas de seguridad en sistemas, esquemas de detección y equipos de respuesta para prevenir y mitigar todo tipo de delitos cibernéticos. Además, la colaboración público-privada contribuye a investigar a los ciberdelincuentes y a desarrollar leyes y regulaciones que aborden el ciberfraude de manera efectiva y a nivel global.

La AEECF elabora anualmente, desde 2016, el Informe sobre el estado del fraude en España, una valiosa recopilación de datos, análisis de tendencias y nuevos desafíos, que ayuda a las empresas a fortalecer sus defensas en su lucha contra el fraude. Según el último estudio, correspondiente a 2023, el 84% de las empresas encuestadas declara haber sufrido más intentos de fraude que el año anterior. Esto supone un importante incremento respecto al informe anterior (53%) y confirma que la proliferación de técnicas, sofisticación e impacto de la ciberestafa es exponencial. Otro dato revelador es el referido a la cuantía de las pérdidas ocasionadas por fraude, ya que un 47% de los encuestados apunta que éstas han sido superiores a las del ejercicio anterior. CyberMadrid celebrará el próximo 18 de abril el 'I Congreso Nacional de Ciberseguridad en Fraude Digital'.

NOMBRAMIENTOS



Cajamar tecnología ha incorporado por **Sonia Peinado** para su área de Control de Ciberseguridad. Con anterioridad, ha ocupado diferentes roles en compañías como Sothis, Layakk y F1-Connecting.

Attindas Hygiene Partners ha contratado como Information Security Risk & Governance a **Eduardo López Ruano.** Hasta ahora CISO de Cloud Worldwide Service, ha trabajado para Deloitte España e Indra, entre otras. Es ingeniero técnico de Telecomunicaciones por la Politécnica de Madrid.

Roberto Valencia ha sido fichado por **Orange España** como Cybersecurity Project Manager Senior. Ha desarrollado su labor profesional en Oesia, Indra, SIA y Deloitte, entre otras.

Ibercaja se ha reforzado, en el ámbito de la protección de la identidad, con **Eliseo Venegas** como Responsable de IAM. Ha desempeñado roles de responsabilidad en Aubay Spain, SegurCaixa Adeslas y NTT Data Europe y Latam. Es graduado en ingeniería por la Politécnica de Madrid.

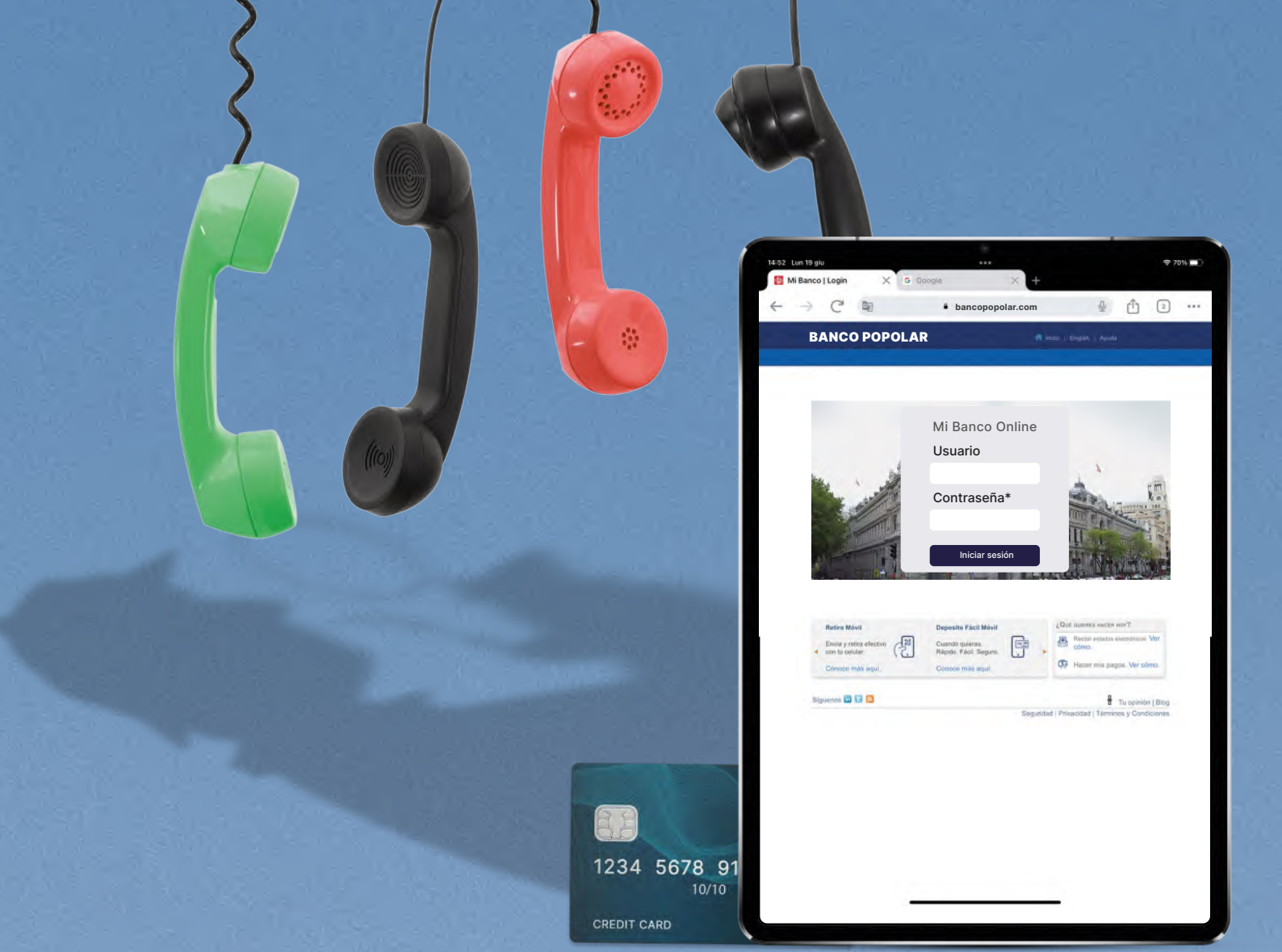
Iberdrola ha reconocido el buen trabajo de **Álvaro Gómez** nombrándole Responsable Global de GRA y Cultura de Ciberseguridad. Ingeniero de Telecomunicaciones por la Universidad de Cantabria ha trabajado en Everis, EY y PWC.

Jimena Sastre ha sido contrata por **PaynoPain** como Directora del Departamento Legal and Compliance Officer (CCO). Ha ocupado roles de responsabilidad en Easy Payment & Finance, Garrigues, Aliseda Inmobiliaria y es copresidenta del Capítulo España de la Association of Certified Financial Crime Specialists (ACFCS).

Fibratel ha contratado a **Jonatan Monroy** como SOC Manager. Con una amplia experiencia en este ámbito, ha trabajado en Línea Directa Aseguradora, InnoTec System y Bureau Veritas Formacion, entre otras.

BBVA Technology ha reconocido la pionera y solvente labor de **Franz Hassmann** promocionándole a Head of Enterprise Tech & Data. Con un gran bagaje en ciberprotección, es ingeniero en Informática por la UPM, ha trabajado para EY, Solium eService CFenter e Innovation 4Security, del Grupo BBVA.

Howden, bróker de seguros, ha promocionado a **Manuel Pérez** a Head of Cyber for South Europe and Latam. Es licenciado en ADE por Icade y se incorporó a Howden Londres en 2014. Tras varios años en la sede central del grupo, se trasladó a Tel Aviv (Israel), para seguir desarrollando su carrera. En 2018, regresó a España para crear el área de Ciberriesgos en Iberia que se ha convertido en uno de los pilares de las especialidades de la firma.



¿Entregarías tus códigos bancarios a un operador telefónico?

No te dejes engañar por aquellos que te contactan amenazando con el cierre inmediato de tu cuenta bancaria o el bloqueo de tu tarjeta de crédito. Transformar los comportamientos digitales de tus empleados es fundamental, pero para hacerlo necesitas una plataforma de capacitación completa, diseñada para maximizar la efectividad de los procesos de aprendizaje. Tres rutas de formación para desarrollar las tres principales características defensivas de cada individuo: el conocimiento, la percepción del peligro y la prontitud.

Cyber Guru

SECURITY AWARENESS TRAINING THAT WORKS!

www.cyberguru.io

ESTE ES UN QRCODE SEGURO

HORNETSECURITY GROUP se hace con VADE y renueva su certificación en el ENS

Hornetsecurity Group ha integrado a la compañía francesa **Vade**, especializada en protección del correo-e con más de 2.500 millones de mensajes analizados diariamente.

Hornetsecurity se ha consolidado como un aliado clave para las organizaciones a la hora de proteger su

infraestructura informática, sus comunicaciones digitales y sus datos gracias a sus servicios *cloud* y soluciones de última generación de seguridad, cumplimiento y *backup*. Por su parte, Vade siempre ha destacado por su solución de seguridad de correo-e basada en SaaS para Microsoft 365. Su herramienta cuenta con una tecnología de filtrado de correos basada en una API diferenciada y es eficaz para grandes empresas de telecomunicaciones e industriales.

En este sentido, Hornetsecurity ofrece diferentes servicios adicionales para Microsoft 365, como *backup*, gestión de permisos, formación en concienciación de seguridad automatizada y validación de destinatarios con inteligencia artificial. Con la unión de Hornetsecurity y Vade, los clientes y *partners* se beneficiarán de una oferta de servicios más amplia. En 2024, estarán disponibles productos adicionales, facilitados a través del centro de datos de Vade.

Por otro lado, **Hornetsecurity** ha renovado su acreditación de Conformidad por parte del Esquema Nacional de Seguridad (ENS), emitida por el **CCN-CERT**.

STORMSHIELD obtiene la Certificación Estándar de ANSSI, para la gama Network Security, y realiza un PoC ante ataques cuánticos

Stormshield ha sido reconocida con de la Certificación Estándar para su gama Stormshield Network Security (SNS).

Tras haber recibido la acreditación Common Criteria EAL4+ el pasado mes de diciembre, este nivel de confianza otorgado por la **Agencia de Ciberseguridad Nacional de Francia** (ANSSI) permite a los Operadores de Importancia Vital (OIV), Entidades Esenciales (EE) y Entidades Importantes (IE) utilizar soluciones que responden a sus retos de seguridad.

Eric Hohbauer, Sales Director and Managing Director en Stormshield, con la certificación de ANSSI

Al igual que con EAL4+ Common Criteria, se auditaron y analizaron todas las funciones del *firewall* (filtrado, detección de ataques, gestión de ancho de banda y políticas de seguridad, auditoría y autenticación fuerte del administrador), VPN (IPSec DR) y administración.

De forma paralela, la compañía ha completado con éxito una primera prueba de concepto (PoC) que incorpora algoritmos de cifrado con resistencia a los ciberataques cuánticos en modo híbrido en sus cortafuegos SNS. El planteamiento de la compañía en este ámbito está en línea con las recomendaciones de la ANSSI, publicadas en abril de 2022, para evolucionar de forma gradual a los algoritmos pos-cuánticos en previsión de su plena madurez. Así pues, este mecanismo híbrido tiene la ventaja de combinar "cálculos para un algoritmo de clave pública precuántico conocido y un algoritmo pos-cuántico adicional" y de "aprovechar la fuerte capacidad del primero para resistir a los atacantes tradicionales, y la capacidad conjeturada del segundo para resistir a los atacantes cuánticos", según sus responsables.

NOMBRAMIENTOS

● Tras una década como responsable de **Kaspersky** Iberia, **Alfonso Ramírez** ha sido promocionado a Director General para Europa. Con más de 20 años en el sector, ha ocupado puestos de responsabilidad previos en GTI Software y Bahlsen Group, entre otras. Es licenciado en Marketing y Gestión Comercial por el Esic.

● **WatchGuard Technologies** ha reconocido la eficaz labor de **Miguel Carrero** nombrándole Vice President Partner Ecosystem Growth & Strategic Accounts, habiendo ocupado, desde hace tres años, el cargo de Vice President, Managed Security Service Providers & Strategic Accounts. Con una amplia trayectoria, con claro enfoque estratégico, ha ocupado roles de responsabilidad en Siemplify, Mobilem y HPE. Es graduado en ADE por el ICADE y cuenta con un MBA por el IESE.

● **Salvador Sánchez Taboada** ha sido fichado por **CyberProof** como Head of Sales Iberia & Latam. Con más de 20 años de trayectoria, ha trabajado en roles de responsabilidad para Open Cloud Factory, Rohde & Schwarz Cybersecurity, ElevenPaths y Panda Security, entre otras. Es ingeniero en Informática por la UPM.

● **Netskope** ha promocionado a **Raphaël Bousquet** a Vicepresidente Ejecutivo Mundial Comercial, reemplazando así a Chris Andrews, que se retirará de la compañía. Veterano del sector de las redes y la seguridad, y reconocido directivo del área comercial, ha dirigido desde hace décadas y con gran éxito, equipos de ventas de tecnología altamente cualificados en empresas líderes del mercado. Desde su incorporación a Netskope en 2021 ha contribuido a la expansión de la presencia de la empresa, la captación de talento y la incorporación de clientes".

● **Gerard Cervelló** ha puesto en marcha la compañía **LTA Labs,** de la que también será CEO. Ha ocupado puestos de responsabilidad en Outpost24 (y en la etapa previa como Blueliv) y Scytl Secure Electronic Voting, donde ha desarrollado gran parte de su carrera.

● **Vesku Turtia** ha sido contratado por **BioCatch** como Senior Regional Sales Manager para Iberia. Con una solvente trayectoria en el mercado oferente tecnológico, ha desempeñado roles de responsabilidad en compañías como Armis, Cyberreason, Nozomi Networks y FireEye, entre otras. Es licenciado en ADE.

● **Ángel Ruiz Sánchez** ha sido contratado por **Facephi** como Director Regional para Iberia. Ha trabajado, entre otras, para Veridas, Uanataca y Bradndocs. Es licenciado en Derecho por la Complutense y cuenta con un PDD en ADE por el Iese.

● **Mikel Rufián** ha comenzado una nueva etapa, relanzando la compañía **Asint360,** fundada por él en 2015, en la que ejercerá como CEO. Con una amplia trayectoria, en la que ha llegado a ocupar el rol de Global CISO, ha trabajado en Bidaidea, Innotec y KPMG, además de ser un docente activo en varias universidades.

BABEL

Business Focused Cybersecurity

babelgroup.com

- Managed Cybersecurity
- Industry
- Governance, Risk & Compliance
- Infrastructure & Cloud Security
- Awareness

eSOC
Centro de Operaciones de Seguridad

eSOC
INDUSTRIAL

Red Nacional de SOC

CERTIFICACIÓN DE CONFORMIDAD CON EL ens
Categoría ALTA
RD 3/2010

FIRST
Improving Security Together

CSIRT.es

ISO 20000

ISO 27001-2

V-VALLEY pone en marcha un plan de inmersión en IA para el canal e incrementa su portafolio con TRILIO y WASABI

V-Valley ha puesto en marcha un programa de formación en Inteligencia Artificial para el canal de distribución.

Este ciclo formativo, denominado 'Inmersión en Inteligencia Artificial: cómo funciona y cómo usarla desde cero' contó, como primera iniciativa, con tres sesiones en marzo, que fueron desarrolladas en el centro de formación V-Valley Academy. En la primera de ellas, a cargo de **Enrique Serrano,** CEO de Tinámica y presidente de MBIT School, se analizó el escenario actual de la IA y cómo afecta al sector su evolución. La segunda fue dedicada a las soluciones que puede utilizar el canal, cuáles hay que posicionar en cada departamento del cliente y su uso, a cargo de **Guillermo Fernández**, AI Strategist y experto en el desarrollo modelos de comportamiento.

La última, con **José Luis Molina**, CEO de **Hispatec**, empresa de soluciones digitales de gestión para el sector agrícola, se centró en el impacto medioambiental de la IA. Además, participaron **Adobe, APC, Blackberry, Check Point, Dell Technologies, Eaton, Foxit** y **Zebra**.

Por otro lado, el mayorista ha firmado un acuerdo de distribución con **Trilio**, a través del cual, los clientes de V-Valley pueden completar sus proyectos de contenedores y máquinas virtuales y brindar resiliencia operativa al satisfacer los requisitos de Backup & Restore, Disaster Recovery, Ransomware Recovery, Portability, Mobility y Migration en sus implementaciones de multinube híbridas.

Además, ha sumado a su portafolio a **Wasabi Technologies,** especializada en *hot cloud storage* y con la que ofrecerá sus servicios de almacenamiento en la nube.

TIREA apuesta por LOGALTY y su firma digital

Grupo Logalty ha integrado su tecnología de firma digital en la plataforma abierta CIMA (Conectividad, Innovación y Servicios para la Mediación Aseguradora) de la **Sociedad Gestora de Tecnologías de la Información y Redes para las Entidades Aseguradoras** (**TIREA**). Su entrada permitirá a 39 entidades aseguradoras, 1.714 corredores y diferentes empresas de software adheridas a ella utilizar el servicio de contratación electrónica de Grupo Logalty. Un paso notable en un momento en el que el sector apuesta por la gestión digitalizada de las pólizas, asegurando el cumplimiento de la legislación y, también, lograr ratios adecuados de devolución de contratos firmados.

En concreto, Logalty ha sido seleccionada por CIMA como proveedor confiable durante los próximos tres años para la firma de pólizas en esta plataforma, gracias a la robustez jurídica que ofrece en el proceso de su firma electrónica y a su amplia experiencia en el sector asegurador.

La presidenta ejecutiva de Grupo Logalty, **María Dolores Pescador**, ha destacado "la importancia de esta colaboración como un paso significativo en la construcción de un ecosistema que garantice la confianza de todas las partes involucradas en el sector asegurador".

NOMBRAMIENTOS

SailPoint ha reconocido la buena labor de **Elena Cerrada** ascendiéndola a Sales Director STRAT Southern, que incluye a Iberia e Italia. Hasta ahora Country Manager para España y Portugal, ha ocupado roles de responsabilidad en Forcepoint, Check Point, Fluke Networks y Telindus, entre otras. Es ingeniera de Telecomunicaciones por la UPM.

Gorka Jiménez ha sido elegido como CEO de **Grupo VAR España,** además de continuar con su cargo de responsable de Wise Security Global -adquirida recientemente por la compañía italiana-. Con una amplia trayectoria, ha ocupados roles de responsabilidad en compañías como Incita.

Claroty ha incorporado a su Consejo Asesor a **Chris Inglis**, que entre 2021 y 2023 ejerció como el primer Director Nacional de Ciberseguridad de EE.UU. Veterano de las Fuerzas Aéreas de EE.UU. y exdirector adjunto de la NSA, llega para impulsar el desarrollo de las soluciones de seguridad de la multinacional. Es profesor visitante en las Academias Naval y de las Fuerzas Aéreas de Estados Unidos y Asesor Principal de Hakluyt and Company y un destacado miembro del consejo de Huntington Bancshares.

Soledad Antelada ha sido ascendida a Security Technical Program Manager Office of the CISO en **Google.** Graduada en Informática por la Universidad de Málaga, es una de las profesionales españolas de mayor proyección internacional habiendo trabajado casi una década en el Berkeley Lab y en el National Energy Research Scientific Computing Center (NERSC). Además, es fundadora de la iniciativa Girls Can Hack.

Innotec Security (part of Accenture) ha contratado a **Santiago Arellano y Nathali Oropeza,** como Service Manager de Seguridad Gestionada y como Cyber Security Consultant, respectivamente. Arellano cuenta con una amplia trayectoria en compañías como Datos101, Forensic & Security, SIRT, Ambar, Secure&IT y Exclusive, entre otras. Oropeza, con anterioridad, trabajó en Fujitsu con un rol similar. Es Graduada en Químicas por la Complutense y cuenta con un Máster en Ciberseguridad por el Icai-Icade.

Zerolynx ha fichado a **Alex Enríquez** y a **José Miguel Aranda**, como Senior Analyst y como Headhunting -experto en atracción y gestión de personas-, respectivamente. Enríquez ha trabajado para Solis Commercial, QCData y Secom Caribe, entre otras. Es ingeniero industrial por la Universidad de La Habana (Cuba) Cujae. Aranda ha desarrollado su carrera en Clictalent, Izertis, Sidertia Solutions e Indizen. Es graduado en Derecho por la Uned.

Cipher, a Prosegur Company, ha promocionado a **Juan Luis Meléndez** a GRC Practice Manager EMEA, y ha incorporado a **David Echarri** Senior Practice Manager, responsable para las prácticas, también para EMEA. Meléndez se ocupaba hasta ahora de esta área solo para España. Posee una amplia trayectoria, contribuyendo con su labor en PwC, Everis e Implemental, entre otras. Cuenta con un Master en Ingeniería de Sistemas por la Rey Juan Carlos. Echarri cuenta con cerca de dos décadas en el sector, habiendo desempeñado roles de responsabilidad en Grupo SIA, Minsait, Oesía y Aventia, entre otras.

CIBERSEGURIDAD

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

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

Todas las respuestas que buscas están en aenorciberseguridad.com

AENOR

www.aenor.com

VEEAM ofrece indemnizaciones de hasta 4,6 millones de euros por *ransomware* con su programa 'Cyber Secure', y suma fuerzas con KYNDRYL

Veeam Software ha presentado su programa 'Cyber Secure', que combina su tecnología creada específicamente con un equipo de expertos que ayudan a las empresas a prepararse, protegerse y recuperarse de los ataques de *ransomware*.

Con él, ofrece soporte previo a incidentes que incluye la planificación de la arquitectura, asistencia en la implementación y evaluaciones trimestrales de seguridad.

Y, cuando se produce un ataque, los clientes pueden ponerse en contacto con el equipo de respuesta ante *ransomware* de Veeam y el programa proporciona, a su vez, apoyo tras el incidente para permitir una rápida recuperación.

En concreto, su propuesta se basa en tres componentes clave: por un lado, la seguridad fiable –con la asistencia para el diseño e implementación que garantice las mejores prácticas de Veeam en la puesta en marcha de soluciones con los más altos estándares de seguridad–; por otro, una ayuda integral durante todo el proceso cuando se sufre un incidente cibernético; y, finalmente, una cobertura financiera en la que se ofrece la confianza de una rápida recuperación a partir de una copia limpia y fiable de los datos de su *backup*, así como Veeam Ransomware Recovery Warranty: un reembolso de hasta 4,6 millones de euros en gastos de recuperación de datos ante un ataque verificado.

Además, la compañía ha llegado a un acuerdo con **Kyndryl** para ofrecer servicios de resiliencia respaldados por tecnología innovadora, gestión experta de infraestructuras y servicios de recuperación ante incidentes. Gracias a este acuerdo, la primera será ahora un Veeam Accredited Service Partner (VASP).

LOGICALIS anuncia un aumento del 53% en su facturación de proyectos asociados a IBM por una apuesta de las compañías por la IA

Ante un escenario de crecimiento donde en 2023, las 300 empresas más grandes de España destinaron más de 46.898 millones de euros a TI, evidenciando un aumento del 24% respecto a 2022, la mitad de esta suma se ha invertido en servicios de TI externalizados, lo que representa un crecimiento del 20% en comparación con el año anterior. Específicamente, el sector industrial ha asignado un 35% de su inversión a soluciones de IA y Machine Learning, y un 37% a tecnologías de Big Data. Ante este escenario, desde **Logicalis** han dado a conocer un aumento del 25% del volumen de proyectos asociados a **IBM**, quienes reconocían a la entidad como 'Partner del Año en Data & IA', en el marco de su IBM Ecosystem Summit 2023.

"Esta colaboración, que se extiende durante más de dos décadas, se ha fortalecido con proyectos innovadores en IA, especialmente con Cloud Pak for Data o Watson X, plataforma de IA y datos desarrollada por IBM para empresas.

La formación y el acceso a tecnologías avanzadas han sido fundamentales para el éxito de este *partnership* donde, este año, hemos experimentado un aumento en la facturación del 53%", ha explicado el Head of Data de la empresa, **Raúl Hermosa.**

Así, desde Logicalis destacan una tendencia al alza entre las compañías españolas que buscan implementar e integrar fácilmente la IA en la totalidad del negocio.

NOMBRAMIENTOS


● El área de servicios de Seguridad de **IBM** cuenta con un nuevo responsable, **Carlos Creus,** quien ha sido promocionado al igual que **Liher Elgezaba** a WW Security QRadar SOAR Tech Sales Leader. Creus con más de una década en la compañía, ha trabajado para PwC. Elgezaba lleva casi dos décadas en la multinacional.

● En la nueva reestructuración de **Deloitte, Carmen Sánchez Tenorio,** hasta ahora Socia Directora de Risk Advisory en Deloitte España y miembro del Comité Asesor del CEO en España ha sido ascendida a responsable de una de las nuevas cuatro áreas de negocio de la firma, la de Tecnología y Transformación, que aglutinará todas sus capacidades –incluida la ciberprotección– y oferta para promover la transformación digital, además de impulsar la IA, con un inversión, ya en marcha, que rondará los 2.755 millones de euros.

● **Devoteam Cyber Trust** se ha reforzado con **Biel Camprubí** como Security Automations Lead. Hasta ahora, había desarrollado su trayectoria profesional en CyberProof y cuenta con un grado en Ingeniería Informática por la Autónoma de Barcelona.

● **Grant Thornton España** contará con **Raúl Manso** como Cybersecurity Director & Senior Manager. Ha desempeñado roles de responsabilidad en S2 Grupo, donde llegó a ser Subdirector Técnico GRC, así como en EY, Banco Santander y en la Universidad de Nebrija, en la que también estudió el grado de Ingeniería Informática.

● **Rhea Group** ha contratado a **César Peñacoba** como Senior Security Consultant. Ha ocupado puestos de responsabilidad en S2 Grupo, HP, Siemens y Add Servicios Informáticos. Es licenciado en Informática por la Politécnica de Madrid.

● **Halborn** ha promocionado a Lead Security Manager a **Antonio Carrillo**. En la compañía desde hace dos años, también ha destacado por su trabajo en Idom Consulting y Tecnimart. Es ingeniero de Telecomunicaciones por la UPM.

● **IriusRisk** ha ascendido a **Josué Encinar** a Responsable de Seguridad de Producto. En la compañía desde 2021, ha trabajado para Telefónica, Accenture y GMV, entre otras.

● **Sopra Steria** ha ascendido a **David González** a Director de su Agencia Gestión de Infraestructuras, Cloud y Ciberseguridad. En la empresa desde 2005, también ha trabajado para Cadtech, Sintel y Saint Gobain España, entre otras.

● La consultora **Abast** ha promocionado a **Mónica Maganto** a Business Manager Cybersecurity. Ha trabajado para Quint, Satec, HP y TCP Sistemas e Ingeniería. Es ingeniera técnica en Informática por la Politécnica de Madrid.

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.

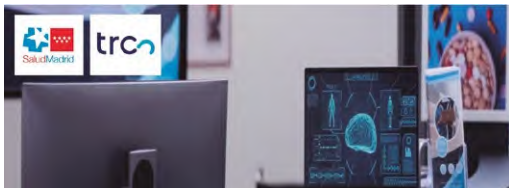
marketing.TIC@gmv.com

gmv.com

gmv®
INNOVATING SOLUTIONS

El SERVICIO MADRILEÑO DE SALUD apuesta por TRC y refuerza su ciberprotección con una inversión de casi cuatro millones de euros

La **Consejería de Digitalización** ha destinado recursos significativos para el desarrollo y mantenimiento de proyectos de ciberseguridad en el **Servicio Madrileño de Salud** (Sermas). En este sentido, se ha realizado una inversión de 3,5 millones de euros para la implementación de la tecnología Identity Threat Protection, con el objetivo de garantizar un nivel óptimo de seguridad.



Para llevar a cabo esta tarea, el Sermas ha confiado en el equipo de Ciberseguridad de **TRC** que llevará a cabo, durante los próximos cuatro años, un análisis continuo, proporcionando visibilidad del estado real de la seguridad del Directorio Activo, a través de la tecnología de **CrowdStrike.** Este informe incluye la evaluación del nivel de exposición a amenazas, la recomendación de prácticas de mejora y la definición de posibles riesgos. Además, se establecerán políticas de detección, cambio de contraseña, bloqueo y acceso condicional a recursos corporativos.

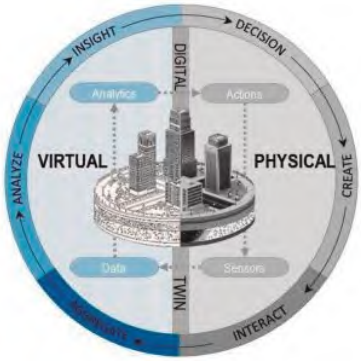
La adopción de esta tecnología puntera ha permitido proteger el Directorio Activo del Sermas de ataques basados en identidad y vulnerabilidades en los protocolos de autenticación.

Con un alcance que abarca aproximadamente a 113.000 usuarios corporativos, se ha logrado mantener un nivel óptimo de seguridad en un entorno crítico.

Desde la Consejería de Digitalización se enfatiza la importancia de proteger la gestión de accesos a los recursos IT corporativos, incluyendo cuentas de usuario, equipos y objetos de directorio relacionados con la infraestructura de la Consejería de Sanidad de la Comunidad de Madrid.

NUNSYS GROUP obtiene la concesión del proyecto Local Digital Twin de la UE para SmartCities

Nunsys Group será la compañía encargada de generar un Gemelo Digital en *SmartCities* con componentes para la ciberprotección que aseguren la privacidad y el cifrado de extremo a extremo. El proyecto de Gemelo Digital para Local Digital Twin (LTD) consiste en replicar de manera exacta una ciudad en formato digital, que sea actualizada constantemente con datos en tiempo real, como el tráfico, la calidad del aire, energía, etc. El objetivo estará centrado en mejorar la eficiencia y sostenibilidad, es decir, "tener una versión virtual de tu ciudad desde donde poder mejorarla", indican sus responsables. Se integran datos reales para simular, visualizar y predecir la dinámica urbana, ayudando con herramientas y tecnologías avanzadas como IoT, IA y análisis de datos, para predecir la dinámica urbana, la gestión y la planificación eficiente de la ciudad.



El proyecto LDT de la Unión Europea va dirigido al intercambio de conocimientos dentro de la comunidad para mejorar la sostenibilidad y resiliencia como requisitos de cumplimiento en el Pacto Verde.

NOMBRAMIENTOS


A3sec ha ascendido a **Alejandro Agudelo** a Director de Operaciones e incorporado como Project Manager a **Rubén Palazón.** Agudelo es ingeniero electrónico y ha desarrollado su carrera en la operadora de telecomunicaciones Claro. En 2016 se incorporó a la empresa como director técnico en Colombia desde donde ha asumido su nuevo rol para España. Palazón, ingeniero Industrial, ha desarrollado su trayectoria profesional en Siemens, Amazon y CaixaBank, entre otras.


GMV ha promocionado a director de la vertical de financiero en Secure e-Solutions de GMV a **José María Blanco** y ha incorporado a **Antonio Blanco Cedrón** como Responsable de Desarrollo de Negocio en GMV ITS. Blanco comenzó su trayectoria como emprendedor, fundando Texware Comunicaciones en 1991 y ha trabajado para Amper, Telesoft y Telefónica. Blanco Cedrón ha ocupado roles de responsabilidad en Inetum, Iecisa y Elecnor, Ibermática y Software AG, entre otras.

Andreia Cristina Castellan se ha incorporado a **Mnemo** como Sales Manager. Cuenta con más de 20 años de experiencia en ventas corporativas y gestión de canales en empresas nacionales y multinacionales de Brasil y España, en empresas como Botech, GH Crecemos, TechHeroX y VSI, entre otras.

Nunsys Group ha promocionado a **Mónica Franco** a Delegada en Madrid y Desarrollo de Negocio de Ciberseguridad en Sothis by Nunsys Group. En la compañía desde 2021, ha trabajado en Grupo SIA, Minsait, Exclusive Networks y AirOn, entre otras.

Wise Security Global ha promocionado a **Juan Pérez** a Cybersecurity Servives & Tools Director. Ha trabajado para IBM, IncitaSecurity y TB Security. Es ingeniero técnico en Informática por la Politécnica de Catalunya.

Reconociendo el buen trabajo realizado por **David Pastor, Recorded Future** le ha promocionado a Senior Account Manager/Team Lead para el Sur de Europa. Ha trabajado para RSA Security, Telefónica, Innotec Systems y Grupo Antea, entre otras.

Ackcent Cybersecurity ha contratado a **Iván Rodríguez** como Senior Account Executive. Ha trabajado para Evolutio, BT Group y Amena, entre otras. Es ingeniero de Telecomunicaciones de La Salle, en Barcelona.

Alaia Tellería se ha incorporado a **Opscura** como Customer Success Manager. Ha trabajado para Titanium Industrial Security, Évolo Consultores y el Icex, entre otras organizaciones.

iC Consult ha fichado como Sales Executive a **Davide Amato**. Ha desarrollado su carrera profesional en BlackBerry, One Identity y Amazon, entre otras. Es licenciado por la Universidad de Wales (Reino Unido) en Márketing.

Enrique Serrano se ha incorporado a **Qualys** como Enterprise Account Executive. Licenciado en Informática por la Universidad Nebrija, cuenta con más de 20 años de experiencia en compañías como Delinea, Palo Alto Networks, Veritas o Symantec.

kaspersky

¿Es el EDR un paso demasiado grande? Ya no.

Kaspersky Next EDR Optimum te ayuda a identificar, analizar y neutralizar las amenazas evasivas gracias a que proporciona capacidades de detección avanzada fácil de usar, investigación simplificada y respuesta automatizada.

Kaspersky Next
EDR Optimum

www.kaspersky.es

SOPHOS presenta Partner Care, una oferta de atención personalizada para los socios

Sophos ha ampliado su compromiso con el canal con la incorporación de Partner Care, una oferta de su programa global de *partners* que cuenta con un equipo de expertos dedicado que ofrecen asistencia operativa y atienden preguntas no relacionadas con ventas, las 24 horas del día, los siete días de la semana.

Así, entre otras novedades, Sophos Partner Care ofrece un único punto de contacto para realizar presupuestos, navegar por el portal de *partners,* resolver dudas sobre licencias y solicitudes de no reventa (NFR), entre otros. Con este alto nivel de servicio, los socios que trabajan con pymes pueden mejorar su productividad y aumentar la rentabilidad.

Para ayudar a los *partners* y MSPs a tomar conciencia de los problemas críticos del sector, la compañía ofrece inteligencia sobre amenazas desde su unidad Sophos X-Ops, con más de 500 expertos en ciberseguridad. Así, la inteligencia de Sophos X-Ops ayuda a los *partners* y MSPs a responder con confianza a las preguntas y preocupaciones de los clientes sobre los últimos *ransomware*, vulnerabilidades y ataques que circulan en las noticias. Para ayudar a optimizar las distintas tecnologías en los entornos de los clientes, también ha añadido a su oferta una integración de **Veeam** a sus soluciones MDR y XDR.

Además de Partner Care, Sophos ofrece varias mejoras a su programa global de *partners*, incluyendo una bonificación adicional del 5% y un descuento en el registro de acuerdos para los socios que vendan Sophos MDR, entre otras.

ISACA se asocia con AEINSE para lanzar el Certificado de Especialista en Ciberseguridad para los Sistemas de Seguridad Física

La **Asociación Española de Ingenieros de Seguridad** (**Aeinse)** en colaboración con **ISACA** han puesto en marcha el Certificado de Especialista en Ciberseguridad para los Sistemas de Seguridad Física (**ECSSF**), que "nace de la necesidad de cubrir la demanda por parte de los Ingenieros de Seguridad Física relativa a los conocimientos para la correcta implementación, gestión dentro de la red y buenas prácticas a la hora de implementar y mantener nuevas y existentes instalaciones", destacan ambas organizaciones.

En concreto, el ECSSF ofrece programas de formación y certificaciones en áreas alternativas como conocimientos y habilidades fundamentales de seguridad de TI, incluyendo protección en la nube, protocolos de seguridad, seguridad de la información, cifrado y seguridad de la red.

Así, a través de esta iniciativa, los socios de Aeinse podrán adquirir certificaciones, como ITCA (Networks and Infrastructure Fundamentals), ITCA (Cybersecurity Fundamentals), CET (IoT Fundamentals) y CET (Cloud Computing Fundamentals).

Este anuncio es el último realizado por Isaca en su esfuerzo por reducir el déficit de competencias, comprometiéndose a aumentar el alcance de su formación y credenciales en Europa para superar los 46.000 individuos certificados.

NOMBRAMIENTOS

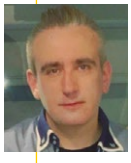
BeDisruptive ha contratado a **David Marco** como Global Industrial Cybersecurity Director, a **Myriam Sánchez**, como nueva CTEM Director y a **Fernando Aranda** como Head of DFIR. Marco ha trabajado para Accenture, Entelgy Innotec Security y Técnicas Reunidas, entre otras. Sánchez es ingeniera en Informática por la Pontificia de Salamanca y cuenta con más de 20 años en ciberseguridad, en compañías como Telefónica, TB-Security, InnoTec y Accenture. Aranda ha desarrollado su carrera en Ayesa-Ibermática, Minsait, Indra y France Telecom España, entre otras. Es ingeniero de Telecomunicaciones por la Universidad de Liverpool.

CrowdStrike ha apostado por **Juan Luis Garijo del Cura** promocionándole a Vicepresidente para el Sur de Europa. Ocupando roles de responsabilidad en la compañía desde 2020, también ha trabajado para Palo Alto Networks y Cisco.

Elena Miguel ha sido contratada por **Leet Security** como Audit Manager. Ha trabajado para Indra, ICA Informática y Quint Wellington Redwood Iberia. Es ingeniera técnica en Informática de Sistema por la UCLM.

Siemens ha incorporado a **Manuel Mendoza** como Cybersecurity Platform Lead Architect. Posee una amplia experiencia en este ámbito, en compañías como AWS, Eurofins y Nestlé, es graduado en Telecomunicaciones por la UPC.

Ignacio Gerez ha sido nombrado Director de la Unidad de Ciberseguridad y Networking de **Omega Peripherals.** Llega desde SIA (an Indra company). Anteriormente, trabajó en empresas como Inetum, Iecisa, Sener y Auding Intraesa, asumiendo posiciones de dirección en diferentes ámbitos. Es ingeniero de Telecomunicaciones y Electrónica por la Universidad de La Salle.



El CTO y fundador de eGarante, **Yago Jesús** ha comenzado en paralelo una nueva etapa en la que ocupará el mismo rol en **Aroki Security.** Con una destacada trayectoria técnica, ha trabajado para Indra, ISC Consultores y Da Vinci.

Laura Cotorruelo ha sido ascendida por **Capgemini** a Strategy Manager en Ciberseguridad. Ha desarrollado su trayectoria en KPMG y Mapfre, entre otras. Tiene un doble grado por la Carlos III de Madrid en ADE y Derecho.

Minsait ha promocionado a **Marta Camacho** a Cybersecurity Manager. Ingeniera en organización industrial por la Universidad de Málaga, ha ocupado roles de responsabilidad en Deloitte, donde comenzó su carrera.

Más de **20 años** anticipando un mundo ciberseguro

+700 **Trabajadores** expertos | **+1000** **Clientes** satisfechos | **+1500** **Auditorías** avanzadas | **+35** **Países** | **+7200** **Incidentes** tratados al año

S2 Grupo es la compañía de referencia en Europa y Latinoamérica en ciberseguridad. Llevamos a nuestras espaldas más de 20 años de experiencia y operamos en +35 países con un equipo de más de 700 expertos. A través de nuestras soluciones, los esfuerzos en concienciación a la sociedad y la inversión en innovación construimos el mundo ciberseguro en el que queremos vivir.

Síguenos en: @s2grupo s2grupo.es

S2 GRUPO 20 años
Anticipando un mundo ciberseguro

EXCLUSIVE NETWORKS y SENTINELONE aceleran la adopción de su estrategia XDR en EMEA

Exclusive Networks ha decidido potenciar su estrategia XDR con **SentinelOne,** para ofrecer las mejores soluciones de detección y respuesta ampliadas (XDR) en toda la región EMEA. A través de esta asociación, el mayorista ofrecerá a los *partners* acceso a Singularity XDR, la plataforma de SentinelOne que proporciona una visión unificada de las amenazas e incidentes en los *endpoints*, las identidades y la nube para proteger a toda la empresa.


Paul Eccleston

Exclusive Networks también aportará su experiencia en estrategia XDR, aceleración de ventas e implementación técnica para ayudar a los *partners* a gestionar la plataforma de forma eficaz. Con el portafolio aún más completo de fabricantes de ciberseguridad, Exclusive Networks hará realidad XDR como estrategia para los partners de canal. Junto con Netskope y Exabeam, las empresas obtienen una visibilidad amplia al adoptar soluciones integradas que se distinguen por ser las mejores.

"SentinelOne ha revolucionado el mercado con su pionera plataforma de seguridad impulsada por IA y continúa innovando en la protección del *endpoint* frente a las amenazas. Al estrechar nuestros lazos y combinar nuestra experiencia y un gran portafolio con la tecnología de SentinelOne, podemos permitir a nuestros *partners* llevar a cabo una estrategia XDR", ha explicado el SVP EMEA de Exclusive Networks, **Paul Eccleston.**

La Asociación @ASLAN comienza sus 35 años renovando su junta y con máximo histórico de socios

Tras cuatro años como presidente, **Ricardo Maté** (**Sophos**) ha cedido el testigo al frente de la asociación **@aslan** a **Alberto Pascual** (**Ingram Micro**) –como ya informó SIC 158–, que "toma el relevo para seguir impulsando la divulgación tecnológica en sectores clave de la economía nacional y los retos y oportunidades que generará la IA en los próximos años",

destacan desde la organización que presentó, en su Asamblea General Ordinaria, en enero, su Plan de Actividades –encabezado por la 31ª edición del Congreso & EXPO ASLAN 2024, el 17 y 18 de abril en Madrid bajo el título "IA. Todo cambia. Un gran avance en digitalización"–.

Además, dio a conocer que ha alcanzado su máximo histórico de socios con 45.458 profesionales, además de haber experimentado un crecimiento del 36%.

En su nombramiento, Pascual se marcó como principales retos "dar continuidad y mejorar las iniciativas de los últimos años, aprovechar los retos y oportunidades que ofrece la IA, seguir mejorando los servicios a empresas asociadas y reforzar la colaboración con entidades, como la CEOE, para impulsar la digitalización en grandes y pequeñas empresas". Le acompañarán, en la Junta Directiva, **Luis González** de **Allied,** de vicepresidente, **Francisco Verderas,** como secretario general, **D. Telesis**, como tesorero, además de ser vocales **Melchor Sanz**, de **HP, Julia Santos**, de **Dynatrace**, **Fernando Feliu**, de **Virtual Cable**, **Julia Castrillo**, de **Bechtle**, **Mario Medina de Ilunion**, **Adela de Toledo** de **PureStorage**, **Francisco Torres-Brizuela** de **NetApp**, **Ruth Velasco** de **Sophos**, **Santiago Campuzano** de **Veeam** y **Patricia Núñez** de **Lenovo.**

NOMBRAMIENTOS


Tarlogic ha promocionado a **Antonio Cuesta** a Cybersecurity Sales Executive, y ha fichado a **David Sanz** como Analista de Ciberinteligencia. Cuesta es Graduado en Telecomunicaciones por la Universidad de Sevilla y preiamente ha trabajado para Everis, Minsait y Grupo Sia, entre otras. Por su parte, Sanz es un reconocido profesional en el ámbito del Osint, habiendo trabajado con anteriporidad para The Aimery Group y Effect Group, además de ser fundador de la *start up* Hooptap y de la iniciativa 'Brigada Osint'.

Zscaler ha ampliado su equipo con la incorporación de **Federico Teti** como Global Solutions Architect. Ha ocupado roles de responsabilidad en Netskope, Forcepoint, Sophos y Synnex Westcon Comstor Latam. Es Licenciado en Sistemas e Informática por la Universidad de Kennedy (Buenos Aires).




Factum ha contratado a **Francisco Javier Santiago** como SOC Manager, a **Karen Carrizo** como Consultora de Ciberseguridad, a **Alberto Jiménez** como Senior Sales Account Manager y a **David Ibañez** como Senior Account Manager. Santiago ha trabajado para Synack Red Team, Bosonit, Open Spring, Telefónica, BBVA Next Technologies y Mnemo, entre otras. Carrizo ha desarrollado su labor profesional en Coval Servicios Financieros y Pretorian, entre otras. Jiménez cuenta una amplia trayectoria, habiendo ocupado puestos de responsabilidad en SealPath y Deyde Calidad de Datos, entre otras. Ibañez ha desempeñado roles de responsabilidad en SealPath, Lefebvre, Thomson Reuters y Positive Marketing.

Mateo Sánchez ha sido contratado por **S2 Grupo** como Cibersecurity Account Manager. Ha trabajado para Secure&IT, Seresco y Richoch, entre otras. Cuenta con un Master en Ciberseguridad por la Universidad de Barcelona.

FACTUM

Cybersecurity Services

Tu tranquilidad,
nuestra razón de ser.

No te pierdas nada
Síguenos en LinkedIn

cyberex_
Cyber Security Exercises

hackrocks | FACTUM
1° RANKING **ESPAÑA**

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

José Ángel Álvarez

Director del Centro de Ciberseguridad del Ayuntamiento de Madrid, CCMAD

En diciembre del año 2021, y en consonancia con lo planeado por su Oficina Digital, el Ayuntamiento de Madrid creó el CCMAD como unidad orgánica dentro de IAM (Informática del Ayuntamiento de Madrid). A su frente, en calidad de director, se encuentra José Ángel Álvarez, informático, empleado público con experiencia (INTA, Ministerio de Defensa…) y miembro de ProtAAPP. Su responsabilidad: gestionar junto a su equipo humano los riesgos asociados con la ciberseguridad de las áreas de gobierno, los organismos autónomos y el personal municipal de la capital de España, y, en última instancia, de quienes viven en ella.

“No hay transformación digital de las Administraciones Públicas sin ciberseguridad”

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

– ¿Qué modelo de gobernanza de la ciberseguridad está instaurado en el Ayuntamiento de Madrid?

– El máximo órgano de gobierno de la seguridad en el Ayuntamiento es el Comité Municipal de Seguridad de la Información (CMSI) cuyo presidente es el Director de la Oficina Digital, Fernando de Pablo, vicepresidente el Responsable de Seguridad de la Información, el gerente de Informática del Ayuntamiento de Madrid (IAM), Juan Corro y cuenta con un vocal por cada área de gobierno.

Este CMSI eleva para aprobación a la Junta de Gobierno la “Política de Seguridad de la Información del Ayuntamiento de Madrid y sus Organismos Públicos”, que establece los principios, directrices y responsabilidades para proteger la confidencialidad, integridad y disponibilidad de los servicios y activos de la información del Ayuntamiento.

Dentro de la estrategia de transformación digital de la ciudad, “Madrid, Capital Digital” se incluye como un aspecto esencial la “Estrategia de Ciberseguridad del Ayuntamiento” basada en cuatro pilares: Gobierno, Protección, Detección y Respuesta, y Cultura de Ciberseguridad.

Por último, el Centro de Ciberseguridad del Ayuntamiento de Madrid (CCMAD) es la unidad orgánica que despliega las capacidades y servicios de ciberseguridad para proteger las áreas de gobierno, los organismos autónomos y el personal municipal.

– ¿Cómo se gestó la creación del CCMAD y cómo está organizado el centro?

–En el verano de 2020 el alcalde creó la Oficina Digital, con Fernando de Pablo al frente, que a su vez nombró a Alfonso Castro como Gerente de IAM. En esta nueva etapa, se refuerza la importancia de la ciberseguridad hasta el punto de incluir en los compromisos de alcaldía para esa legislatura la creación del CCMAD.

Tras muchos esfuerzos, en diciembre 2021 se crea formalmente el CCMAD, como una unidad orgánica en IAM, para dar servicios de ciberseguridad a todo el Ayuntamiento.

En marzo de 2023, damos un paso más e inauguramos unas nuevas instalaciones con la presencia del alcalde, momento que aprovechamos para explicarle todo el trabajo que realizamos, junto a nuestros proveedores, 24x7, 365 días al año.

En el ámbito presupuestario, es importante destacar que, en los últimos años, el Ayuntamiento ha multiplicado por cuatro los recursos (tanto humanos como económicos) dedicados en exclusiva a la ciberseguridad, lo que demuestra el firme compromiso de la organización en esta materia.

En cuanto a cómo estamos organizados, CCMAD cuenta con un servicio de coordinación y 5 departamentos: GRC, Ingeniería, SOC, Auditorías y Cultura. Prestamos los servicios de Vigilancia Digital, Detección y Respuesta, Búsqueda de Amenazas, Asesoramiento Tecnológico, Seguridad en el Ciclo de Desarrollo, Escaneo automatizado de la superficie de ataque, Auditorías de Vulnerabilidades, Asesoramiento en cumplimiento TIC y Formación, Concienciación y Difusión de la ciberseguridad, a todas las áreas de gobierno, a los organismos autónomos y a los, aproximadamente, 30.000 empleados municipales.

– ¿Cómo está organizada la participación de la función de ciberseguridad en el ciclo de las iniciativas de IAM en el Ayuntamiento?

–La ventaja de que CCMAD sea una unidad orgánica de IAM es que nos permite estar muy pegados a los responsables de los servicios prestados a los empleados municipales y a los sistemas desarrollados para las unidades de negocio. Participamos activamente en todo el ciclo de vida de los servicios y sistemas: desde las fases de diseño e implementación, puesta en marcha y la supervisión continua de los servicios.

Somos afortunados porque el equipo de profesionales de IAM está especialmente concienciado de la importancia de la ciberseguridad en el diseño y operación de los servicios y sistemas, tenemos el apoyo incondicional del Comité de Dirección del organismo y, en especial, de nuestro gerente, Juan Corro.

En el caso de servicios gestionados directamente por las áreas de gobierno vía proveedores externos, nuestro objetivo es definir un modelo de contratación y supervisión, que permita a los proveedores prestar el servicio con garantías y a los responsables de los contratos tener mecanismos de supervisión adecuados.

–En el Ayuntamiento de Madrid, y además de la propia corporación municipal específica, hay entidades públicas del Ayuntamiento o en las que participa el Ayuntamiento con personalidad jurídica propia, que son infraestructura crítica y en su mayor parte servicio esencial. ¿En qué frentes colabora el CCMAD para ayudar a gestionar los riesgos de ciberseguridad en el complejo entramado de entidades y servicios, prestados por públicos y privados?

–Si pensamos en términos de ciberse-

guridad de la ciudad la palabra clave es COLABORACIÓN. A modo de ejemplo, hemos trabajado mucho con todas las empresas públicas del Ayuntamiento para establecer canales de comunicación, intercambiando información sobre posibles ciberamenazas y disponiendo de mecanismos preparados para reaccionar de forma coordinada en caso de ciberincidente crítico. También mantenemos una comunicación fluida con el CNPIC y la OCC, por razones obvias.

Conviene destacar que, desde finales de 2022, el Plan Territorial de Emergencia Municipal del Ayuntamiento de Madrid (PEMAM) incorpora las ciberamenazas como una posible causa de una emergencia en la ciudad, definiendo los equipos de respuesta y los mecanismos de coordinación necesarios para superar una posible cibercrisis.

–¿Cómo se plantean en el CCMAD ir abordando la transformación de Madrid en una ciudad "inteligente" en la que va a ir creciendo la OT y la IoT en prácticamente todos los espacios digitales y ciberfísicos de la Capital?

– Todas las grandes ciudades del mundo están desplegando miles de millones de dispositivos inteligentes y, los que nos dedicamos a ciberseguridad, enseguida asociamos: inteligente -> conectado -> vulnerable.

Ante un reto de semejantes dimensiones hemos pensado que la unión hace la fuerza y el Ayuntamiento de Madrid ha suscrito un convenio de colaboración con el Centro de Domótica Integral (CEDINT) de la Universidad Politécnica de Madrid, para crear el "Laboratorio IOT de Madrid" (IOT-MadLab). En este laboratorio se prueban los dispositivos de fabricantes que luego se instalarán en la ciudad, garantizando la debida interoperabilidad y su encaje en la nueva arquitectura de referencia IOT de la ciudad. El reto es incorporar pruebas de ciberseguridad a estos dispositivos. Esto nos permitirá acercarnos a la seguridad de los dispositivos IOT en primera persona.

Esta iniciativa ya ha despertado el interés de otras ciudades y comunidades autónomas que nos han pedido más información al respecto.

– En el reparto de tareas que se deduce de la legislación vigente sobre ciberseguridad en España, el CCN tiene encomendado, entre otros, el epígrafe de las Administraciones Públicas. ¿Mantienen ustedes relaciones fluidas con el Centro?

– En primer lugar, me gustaría destacar el excelente trabajo realizado por el CCN desde su constitución allá por el año 2004, con Luis Jiménez y Javier Candau a la cabeza.

La colaboración entre el CCN y el Ayuntamiento de Madrid lleva muchos años funcionando perfectamente pero todavía se ha reforzado más, desde la firma del convenio entre ambos organismos para el intercambio de información, la formación especializada y el desarrollo de proyectos tecnológicos conjuntos.

Además, el CCMAD fue uno de los primeros organismos en incorporarse a la Red Nacional de SOCs (RNS), iniciativa del CCN que consideramos esencial para compartir información sobre amenazas entre todas las AAPPs españolas y, en el futuro, con el resto de SOCs europeos.

"El Centro de Ciberseguridad del Ayuntamiento de Madrid (CCMAD) es la unidad orgánica que despliega las capacidades y servicios de ciberseguridad para proteger las áreas de gobierno, los organismos autónomos y el personal municipal".

Y, como dije en las pasadas jornadas del CCN-CERT, si CCN publica una guía para certificar SOCs, el CCMAD hará todo lo posible por cumplirla, con el objetivo de la mejora continua en la prestación de los servicios a nuestra comunidad de usuarios.

– ¿Le parece acertado que el CCN, en lo que se refiere a la RNS, en la que participan entidades públicas y MSSPs, vaya a dar luz verde a la incorporación en la misma de compañías del Ibex35?

– En alguna de mis conversaciones con CISOs del sector privado les he sugerido la incorporación de estas grandes empresas a la Red Nacional de SOC, por lo que creo que la decisión de CCN es un acierto y redundará en beneficio de los usuarios del sector público y privado, es decir, la ciudadanía.

– ¿También está de acuerdo en que, en un futuro, solo los proveedores en la RNS que mantengan la categoría Gold puedan optar a prestar servicios a las Administraciones Públicas?

– Los proveedores del sector privado están compartiendo información sobre ciberamenazas y ciberincidentes pero creo que todavía hay margen de mejora. Cualquier incentivo en esta línea me parece acertado y, sin duda, acabará como un requisito en los pliegos de contratación.

– ¿Mantienen ustedes relaciones de colaboración con Centros parecidos o similares que pudiera haber en otras ciudades españolas, en ciudades de la UE y urbes de otras zonas del mundo?

– Sí, compartir conocimientos y experiencias con otras ciudades es absolutamente esencial. Debemos recordar que todos nos enfrentamos a problemas muy similares y, las soluciones, también son muy parecidas. No reinventemos la rueda.

Varios ejemplos. A nivel nacional, Guillermo Obispo (alias "Willy"), nuestro coordinador del CCMAD, es a su vez el coordinador del subgrupo de ciberseguridad de la Red Española de Ciudades Inteligentes (RECI) y esto le permite estar en contacto con ciudades de toda España intercambiando información en materia de ciber.

Por ejemplo, hace unas semanas, con el apoyo de RECI, hemos organizado una sesión de trabajo muy interesante con responsables de ciberseguridad de grandes ciudades de la Comunidad de Madrid, junto con personal de la consejería de Digitalización. Esperamos realizar más reuniones de este tipo con otras ciudades de España. También mantenemos una comunicación muy fluida con responsables de ciberseguridad de varias comunidades autónomas, con los que compartimos dudas, inquietudes y experiencias.

"Desde finales de 2022, el Plan Territorial de Emergencia Municipal del Ayuntamiento de Madrid (PEMAM) incorpora las ciberamenazas como una posible causa de una emergencia en la ciudad, definiendo los equipos de respuesta y los mecanismos de coordinación necesarios para superar una posible cibercrisis".

A nivel europeo, en 2022 Madrid se unió a la comunidad Eurocities, 200 grandes ciudades europeas que colaboran en materia de tecnología e innovación y, participa muy activamente en la Cybersecurity Community of Practice formada en este momento por 21 grandes ciudades.

– ¿Y con la Comunidad de Madrid?

– La relación entre la Comunidad (Madrid Digital) y el Ayuntamiento (IAM) siempre ha sido fluida, compartiendo experiencias y conocimientos. Desde CCMAD mantenemos contactos frecuentes con el equipo ciber de Madrid Digital, encabezado por la magnífica Esther Muñoz, intercambiando experiencias, proyectos, lecciones aprendidas, pero también información sobre ciberamenazas o posibles incidentes.

En cuanto a la nueva Agencia de Ciberseguridad de la Comunidad de Madrid estamos impacientes por comenzar a trabajar conjuntamente buscando sinergias y mecanismos de colaboración.

– Usted trabaja en la Administración. ¿Cree que, a efectos de la función pública (funcionarios y empleados), deberían tomarse medidas para encauzar el futuro profesional de los expertos en ciberseguridad que hay en las Administraciones?

– En primer lugar, me apena que la palabra "funcionario" se utilice en ocasiones con connotaciones peyorativas, porque existen muchas personas que dedican su carrera profesional a servir a la ciudadanía en profesiones muy relevantes, como policías, bomberos, médicos, etc. En este sentido, me gustaría visibilizar el trabajo que muchos funcionarios realizan todos los días para sostener y evolucionar la tecnología de las AAPP con el objetivo de prestar mejores servicios a la ciudadanía.

Creo que es esencial que exista un cuerpo de empleados públicos realmente expertos en tecnología y digitalización para definir y liderar la estrategia de transformación digital de las AAPP, que no podremos completar sin el apoyo del sector privado.

Debemos encontrar fórmulas para simplificar el proceso de incorporación a la función pública, atrayendo talento joven y diverso, así como hacer atractiva la carrera profesional para retener ese talento, porque en la época de la automatización y la inteligencia artificial, las personas son el elemento clave de las organizaciones.

"Hemos suscrito un convenio de colaboración con el Centro de Domótica Integral (CEDINT) de la UPM para crear el "Laboratorio IOT de Madrid" (IOTMadLab), en el que se examinan los dispositivos de fabricantes que luego se instalarán en la ciudad. El reto es incorporar pruebas de ciberseguridad para estos dispositivos".

– ¿Qué papel juega y quiere jugar ProtAAPP en el ámbito de la mejora de la gestión de la ciberseguridad en el entorno público?

– En el año 2018, Miguel Ángel Rodríguez Ramos creó la Comunidad "Protege las Administraciones Públicas" (ProtAAPP) con una idea: que los empleados públicos pudiesen APRENDER, CONOCER y COMPARTIR en materia de ciber, de forma complementaria a la colaboración existente entre instituciones.

Seis años después, ya somos más de 470 empleados públicos, incluyendo personal civil tanto de la Administración General del Estado, Comunidades Autónomas y Entidades Locales, pero también personal militar de los ejércitos y guardia civil, en su condición de empleados públicos.

El objetivo no ha cambiado: compartir conocimientos y experiencias entre empleados públicos para enriquecer nuestras mentes, lo que beneficia a los organismos donde estamos destinados y, por ende, a la ciudadanía.

A modo de ejemplo, por tercer año consecutivo, el track de ProtAAPP dentro del congreso RootedCON, ha sido un éxito rotundo de asistencia y, lo más importante, punto de encuentro de los empleados públicos con interés en ciberseguridad.

– ¿Qué impacto va a tener la legislación que nos viene (pongamos que la NIS2, la ley de ciberresiliencia, la de ciber solidaridad,…, en el ámbito de la gestión de la ciberseguridad en las ciudades?

– Creo que la "buena" legislación tiene un impacto positivo en el sector, estableciendo marcos comunes y buenas prácticas que permiten incrementar el nivel de madurez de los procesos de las organizaciones. Sin embargo, debemos reflexionar sobre cada nueva normativa y entender cuánto de seguridad real puede aportar a las organizaciones, evitando crear normativas que aporten poco valor y puedan convertirse en un pesado lastre normativo que requiera destinar cantidades ingentes de recursos que podrían ser más útiles en otras tareas.

– Una última pregunta: ¿qué nota le pondría al alcalde de Madrid, José Luis Martínez-Almeida en materia de comprensión de la gestión de riesgos asociados con la ciberseguridad?

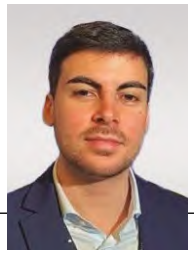
– Repasemos los hechos: el alcalde incluyó la creación del Centro de Ciberseguridad en la lista de compromisos de la alcaldía, eligió a las personas idóneas para liderar la transformación digital del Ayuntamiento y aprobó la inversión necesaria para el despliegue de las capacidades y servicios de CCMAD.

"Si el CCN publica una guía para certificar SOCs, el CCMAD hará todo lo posible por cumplirla, con el objetivo de la mejora continua en la prestación de los servicios a nuestra comunidad de usuarios".

Ahora es nuestro turno. Debemos gestionar adecuadamente estos recursos para reducir la probabilidad de que el Ayuntamiento sufra ciberincidentes, cuando sucedan (que lo harán) detectarlos y responder con rapidez, y minimizar el posible impacto negativo en los activos municipales, porque no hay transformación digital de las Administraciones Públicas sin ciberseguridad. ■

COMUNIDAD VALENCIANA: despliegue de capacidades avanzadas EDR para la mejora de seguridad en los equipos de su Servicio de Salud

La necesidad de reforzar en pandemia las medidas de seguridad en los equipos y accesos remotos de los usuarios a una infraestructura tan crítica como los hospitales y centros de salud en plena pandemia, obligó al servicio de Salud de la Comunidad Valenciana a abordar un primer proyecto de protección de equipos domésticos para profesionales que tuvieron que conectarse desde su domicilio. Con esto se obtuvo un control total de las conexiones remotas y se aseguró que no se propagara ningún *malware* desde los puestos de teletrabajo. Tras dicho éxito, y de la mano de Nunsys Group –con la ayuda tecnológica de Cytomic de Watchguard–, se aborda un nuevo proyecto de sustitución del EPP de Conselleria por el mismo EDPR con capacidades avanzadas de detección y respuesta a incidentes en todos los equipos del servicio de salud con 50.000 equipos.



Antonio Grimaltos / Jesús Díez

La imprevista llegada de la pandemia puso en jaque algunos de los sectores más críticos de la sociedad, los servicios autonómicos de salud se enfrentaron a uno de los mayores retos de los últimos años, modernizar y asegurar todo su sistema informático con una urgente cuenta atrás.

En un tiempo donde los ciberataques a hospitales eran más continuados que en ninguna otra industria la **Generalitat Valenciana** se encontró con más de 2.500 trabajadores obligados a cambiar su rutina por el teletrabajo, respetando todas las normas para no comprometer la información y los sistemas de la Consellería de Sanitat.

Sin recursos suficientes en hardware ni tiempo para el bastionado ni la correcta configuración de todos los equipos, los ataques de *malware* subían junto con las oleadas del Covid, se buscó, por tanto, una solución que reforzara dichas medidas de seguridad y permitiera control sobre las conexiones remotas desde una VPN.

La apuesta fue clara, la tecnología **Cytomic** de **Watchguard Technologies** permitió que los trabajadores volvieran a sus casas y no tuvieran la obligación de sustituir sus endpoint personales con el intrusismo que ello conlleva, esto no solo permitió una rápido despliegue gracias a su adaptabilidad en diferentes sistemas operativos, fueran Windows, Mac o Linux.

Además, se pudo realizar una prueba contra amenazas futuras o que los equipos tuvieran previamente, se identificaron 1.400 diferentes tipos de *malware*, una cifra que demuestra la magnitud de exposición de los dispositivos en el momento.

La adquisición de 5.000 licencias EPDR Cytomic permitió que cada vez más equipos domésticos pudieran sumarse al teletrabajo y conectarse a la Consellería asegurando la confidencialidad, disponibilidad e integridad de las comunicaciones.

En esta primera fase impulsada por el **CCN** y la distribución de Cytomic, Nunsys Group actúa como partner tecnológico, con el objetivo de realizar los diferentes pilotos de prueba contra amenazas y aportando su tecnología SafeCloud para el almacenamiento cloud del Esquema Nacional de Seguridad en nivel alto.

Tras el éxito con las 5.000 licencias en equipos externos, la Consellería se plantea mejorar también sus centros hospitalarios utilizando la misma tecnología de Cytomic, con más de 24 departamentos de salud críticos y un volumen de 50.000 equipos internos.

El trabajo de Nunsys Group consiste en definir grupos a nivel del departamento de salud, crear un grupo para cada hospital y cada departamento si hay varios hospitales, a su vez también se establecen diferentes grupos dentro de cada hospital a los que los equipos puedan ingresar.

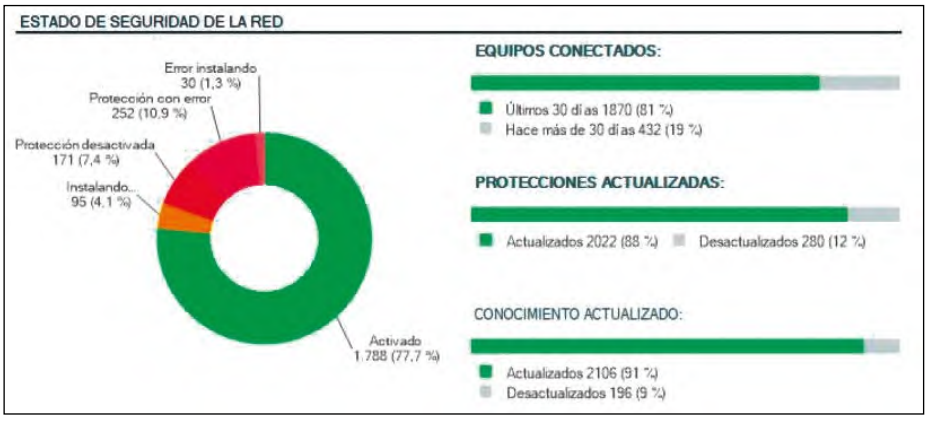
A modo de ejemplo y como grupos básicos podrían dividirse los equipos de un hospital en dos, 'equipos' y 'servidores'. Dentro de los equipos podrían definirse las diferentes secciones como 'administración', 'consultas externas', 'radiología', 'oncología', 'traumatología', etc.

Dado que actualmente la Consellería cuenta con otra solución en activo, la implementación inicial se realizó sin activar la opción de antivirus en las computadoras para que no ocurran conflictos, aunque posteriormente pueda activarse a nivel global con la propia licencia EPDR de Cytomic con tan solo dar luz verde a las opciones correspondientes.

Aparentemente, este plan de implementación primero pone el EPDR en modo Audit, para seguir con el modo Hardening y finalmente a modo Lock. Esto lleva a una implementación de mejoras en las capacidades de aprendizaje en la propia herramienta, un funcionamiento que también se implementará en otras unidades.

También se han creado roles para que cada UID de departamento solo pueda ver los dispositivos que administra, este enfoque también se utiliza en otras unidades de la Consellería de Sanitat, donde Nunsys Group se encarga de establecer planes de formación para los responsables.

Aunque el proyecto se encuentra en una fase temprana camino al aprovechamiento de las 50.000 licencias, alrededor de 2.500 equipos ya cuentan con la actualización de esta tecnología y cada semana nuevos departamentos se suman al despliegue, donde se espera que entre 3 y 6 meses como fecha establecida se complete el proyecto.



Cada semana, Nunsys Group ofrece informes de control de los datos recogidos en el análisis de la consola que incluye indicadores de ataque, urls sospechosas de *phishing*, acciones de los usuarios, altas de nuevos equipos y diferentes gráficos para controlar la seguridad. ■

Antonio Grimaltos
Técnico. Oficina de Seguridad de la Información
Consellería de Sanitat
GENERALITAT VALENCIANA

Jesús Díez
Inside Sales y Comunicación
NUNSYS GROUP

Luca Tagliaretti

Director Ejecutivo del Centro Europeo de Competencia en Ciberseguridad

"El ECCC es el motor de la implementación de la estrategia europea en investigación, innovación y política industrial, y para coordinar inversiones conjuntas en proyectos estratégicos"

Directo en su forma de hablar, apasionado por los retos y con más de 20 años de experiencia en transformación digital, ciberseguridad e investigación en organismos como eu-Lisa y el Banco Central Europeo, Luca Tagliaretti se ha convertido desde febrero pasado en el primer director del Centro Europeo de Competencia en Ciberseguridad. A pesar de su agenda 'imposible' para la puesta en marcha del ECCC, este ingeniero por la Universidad de Milán, hizo un hueco para responder a las cuestiones planteadas por Revista SIC, sobre los retos iniciales del organismo que está llamado a ser el abanderado de la innovación y el desarrollo de nuevas capacidades en este ámbito en Europa. ¿Su secreto? "Siempre considero que cada cambio trae nuevas oportunidades. Debemos aceptar y abrazarlos como parte de nuestra vida y aprovecharlos al máximo". Un buen ejemplo del buen hacer de este ejecutivo que, entre otras titulaciones, ha cursado el prestigioso Programa de Negociación de Harvard.

– Ha trabajado para dos organismos de referencia como eu-Lisa y el Banco Central Europeo. ¿Qué lecciones de ellos espera aplicar en el ECCC?

– No es fácil hacer una comparación entre una institución grande como el BCE, una agencia establecida como eu-LISA y una nueva como el Centro Europeo de Competencia en Ciber-Seguridad (ECCC). Todos los organismos de la UE son similares porque se basan en normas de personal semejantes (no siempre idénticas), pero también, todos son diferentes porque todos desarrollaron sus culturas internas.

Para una puesta en marcha como el ECCC es necesario evolucionar rápidamente hacia una organización más estructurada con procesos claros. El ECCC cuenta con un equipo altamente motivado y comprometido que comprende muy bien la importancia de su misión. He llegado a Bucarest apenas hace dos meses, pero estoy muy orgulloso del trabajo que estamos haciendo en la preparación para la autonomía financiera y para la implementación de los fondos del Digital Europe Programme (DEP).

– ¿Cuáles son sus tres prioridades como director del ECCC para 2024?

– En primer lugar, completar la instalación del Centro, trasladándonos a su sede definitiva y logrando independencia financiera y capacidad de gestionar nuestro propio presupuesto. En segundo, elaborar y gestionar el programa de trabajo estratégico para 2025-27, que definirá las principales áreas de inversión para el futuro. Por último, seguir cumpliendo con la evaluación y gestión de las convocatorias de subvenciones del DEP. Y si puedo agregar una más, sin duda, será completar en 2024 el registro de las empresas y entidades que formarán parte de nuestra cibercomunidad.

– En Europa se están implementando normativas de gran importancia como NIS2, DORA, CRA, CSA… ¿En qué les ayudará el ECCC?

– El panorama de la ciberseguridad de la UE vio un mayor enfoque en el desarrollo de políticas, regulaciones y directivas para abordar desafíos sin precedentes. La legislación de la UE sobre ciberseguridad es en general global, pero ahora lo importante es aplicarla en consecuencia. Aquí entra en juego el papel principal del ECCC, que es apoyar la implementación de políticas de ciberprotección ofreciendo las subvenciones necesarias y fomentando la creación de una cibercomunidad. Me gusta referirme al ECCC como el motor de la implementación de la estrategia europea en investigación, innovación y política industrial en el área de la protección cibernética al marcar una agenda europea común para el desarrollo tecnológico y coordinar inversiones conjuntas en proyectos estratégicos en esta materia.

Solo por dar algunos ejemplos: el Centro ayuda a implementar la legislación de la UE sobre ciberseguridad en el marco del DEP con varios

llamamientos para apoyar concretamente a los Estados miembros. Actualmente, tenemos una convocatoria en curso que dedica 30 millones de euros para apoyar la puesta en marcha de lo que supone la Ley de Resiliencia Cibernética (CRA). Esto incluye apoyar a las pymes europeas, centrándose en las micro y pequeñas empresas, para fortalecer sus capacidades en materia de ciberseguridad.

– ¿Y de cara al futuro?

– En términos de proyecciones futuras, el ECCC desempeñará un papel importante en la gestión de fondos dedicados al Sistema Europeo de Alerta de Ciberseguridad, consistente en una red de Cyber Hubs nacionales y transfronterizos, que están siendo creados por la Ley de Cibersolidaridad.

En cuanto a la importancia de fomentar una comunidad cibernética y el papel del ECCC, creo que podemos proporcionar un enfoque coherente y estructurado, dar instrucciones adoptando e implementando tecnologías existentes y, en general, financiando soluciones de ciberseguridad. Esto significa apoyar a las pymes –y, en términos más generales, a nuestra economía– para que estén mejor protegidas de los ciberataques y sean más competitivas en el mercado global, reforzando la protección de las infraestructuras críticas, manteniendo la excelencia en la investigación y aumentando la concienciación y los conocimientos técnicos a todos los niveles.

– ¿Cuál es el aspecto más desconocido del Centro que dirige?

– Yo diría que su modelo de gobernanza. Esto se debe a que el ECCC no trabaja solo sino en estrecha cooperación con una red de Centros Nacionales de Coordinación (uno de cada Estado miembro), que apoyan la implementación de la estrategia a nivel nacional. Este modelo de gobernanza en particular se adoptó porque es el más apropiado para abordar los desafíos de ciberseguridad que requieren una respuesta internacional y coordinada.

Por supuesto, los Estados miembros tienen un papel clave en el desarrollo de las prioridades para 2025-2027 en el próximo programa de trabajo. De momento, las propuestas han sido presentadas, sobre todo, por los Centros de Coordinación Nacional y se prevén más oportunidades desde ese ámbito en el futuro próximo. También, esperamos que sean muy importantes las contribuciones voluntarias de los Estados miembros para apoyar con fondos adicionales los programas implementados.

– ¿Cuáles son las áreas donde más se invertirá en ciberseguridad a través del ECCC, por qué son críticas y qué capacidades específicas se espera desarrollar?

– Hasta la fecha, el ECCC ha puesto en marcha más de 110 proyectos en toda Europa en el marco del Programa Europa Digital, por una inversión de casi 400 millones de euros. Los temas tratados van desde la resiliencia de la ciberseguridad, hasta la ciberprotección en Salud, aplicaciones novedosas de la IA, despliegue de la criptografía poscuántica y, también, seguridad en redes 5G. Estos proyectos representan aproximadamente a 500 organizaciones beneficiarias de los fondos. Para lo que queda de este año, y para 2025, la tendencia se mantendrá sin cambios con un equilibrio entre proyectos de alta visibilidad y alto impacto, y apoyo a todas las demás prioridades de la agenda estratégica. Si conseguimos llevar a cabo lo planeado, para finales del 2024, el ECCC gestionará un presupuesto general del DEP de más de 700 millones de euros.

"El ECCC desempeñará un papel importante en la gestión de fondos dedicados al Sistema Europeo de Alerta de Ciberseguridad, la red de Cyber Hubs nacionales y transfronterizos, que están siendo creados por la Ley de Cibersolidaridad"

– ¿De qué dependerá el éxito o el fracaso del ECCC?

– Yo diría que, aparte de la necesidad de seguir el ritmo de las tecnologías, el éxito del Centro dependerá en gran medida del esfuerzo conjunto de la red de Centros Nacionales de Coordinación (NCC). Su papel es fundamental para garantizar la implementación nacional de la estrategia y representa el primer punto de contacto para que la entidad forme parte del ecosistema nacional de empresas cibernéticas. La lucha contra los ciberataques requiere unidad y coordinación.

– En una entrevista en Revista SIC, Lorena Boix, directora de Sociedad Digital, Confianza y Ciberseguridad de la DG CONNECT de la Comisión Europea, destacó que "Es fundamental que cada país disponga de una autoridad nacional a cargo de la supervisión y el cumplimiento de las obligaciones de ciberseguridad derivadas de la NIS". ¿Existe alguna Agencia Nacional que considere que sería el modelo a seguir? Pocos países tienen una con plenas capacidades...

– Comparto la opinión de Lorena Boix al abogar por que las autoridades nacionales centrales se encarguen de garantizar que las obligaciones de NIS (y ahora NIS2) se apliquen de forma coherente. Esto será, simplemente, establecer la coordinación a nivel nacional. Tenemos que esforzarnos por conseguirlo, aunque aún debemos reconocer que no siempre es posible debido a la naturaleza amplia y horizontal de la Directiva NIS y al hecho de que los avances nacionales se producen a diferentes ritmos.

Volviendo a su pregunta, es difícil señalar un ejemplo específico de una autoridad nacional, dadas las diferencias que existen en términos de capacidad nacional, pero espero que, con el crecimiento en importancia de las diferentes agencias cibernéticas nacionales, pronto tomarán reforzar la función de coordinación para la implementación del NIS2 y el control del cumplimiento.

– ¿Qué papel jugarán tanto el ECCC como la NCC en nuevas tecnologías como la IA aplicada a ciberprotección?

– Tanto la ECCC como la NCC jugarán un papel clave en la implementación de la Ley de Cibersolidaridad y en el desarrollo de los Cyber Hubs. Ya se lanzaron convocatorias DEP dedicadas para el uso de IA en la configuración de los *hubs* y se pondrán en marcha más para conectar y operar la nueva infraestructura.

El sistema de alerta previsto en la nueva legislación aprovechará herramientas e infraestructuras de última generación, como la Inteligencia Artificial y el análisis avanzado de datos, para detectar rápidamente ciberamenazas e incidentes. En este sentido, España está muy bien posicionada para incrementar su papel y su implicación en este proyecto histórico.

– ¿Cómo analiza el estado de la gobernanza de la ciberseguridad en España y qué espera que aporte tanto al ECCC, como a la NCC?

– España es uno de los países de referencia en Europa en términos de preparación y respuesta a las ciberamenazas. Tanto Incibe como el Mº para la Transformación Digital y la Función Pública son ejemplo de profesionalidad y experiencia en la UE.

He visitado recientemente el Incibe en León y me impresionó especialmente el trabajo que está realizando su agencia nacional en educación y sensibilización, en el fomento de la cooperación en la cibercomunidad española y en la protección de los ciudadanos vulnerables a través de la iniciativa 017. Podríamos decir que es un buen modelo a seguir en muchos aspectos. ■

Texto: **José Manuel Vera**
Fotos: facilitadas por el entrevistado

Identi :: SiC

Identidad digital

cebo y salvoconducto

Organiza:

Revista SiC

www.revistasic.com/identisic

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

ágoraSIC
Centro de Conocimiento en Ciberseguridad

Gobierno | gestión | operación

Hora de afinar

Para los estados y entidades supranacionales está resultando ardua la tarea de fijar un modelo de referencia para la llevanza de la seguridad y la defensa del ciberespacio y de la tupida dimensión ciberfísica que se cierne sobre nosotros. Una de las razones estriba en las significativas diferencias de organización política y territorial de los países, algo que se evidencia incluso en la UE.

SIC propone en este reportaje especial un viaje por las distintas formas en las que el gobierno y la gestión de la ciberseguridad se están sustanciando en algunos estados no europeos, en estados europeos y en estados miembros de la UE, incluido el nuestro, que se encuentra actualmente enfrascado en alcanzar un texto consensuado de trasposición de la NIS2.

SUMARIO

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

El ciberespacio es un dominio geopolítico en el que los estados están experimentando con enfoques defensivos y ofensivos

Organización de la Ciberseguridad: Quién lleva la batuta

Hace más de 50 años que el NIST de EE.UU. se convirtió en el origen de los que hoy se denominan agencias nacionales de ciberseguridad, organismos con grandes capacidades, identificadas por las estrategias de ciberprotección de cada país, que buscan proteger, impulsar y desarrollar políticas de seguridad cibernética para proteger el estilo de vida de las personas, impulsar la economía y, también, hacer frente a actores estatales que buscan la hegemonía en el ciberespacio, como China o Rusia, frente a los países occidentales. Tan amplio objetivo plantea retos significativos y, al efecto, cada país está apostando por un modelo que, a su vez, pasa por la colaboración internacional. Normativas como NIS2 en Europa darán un paso de gigante en pro de unos grandes 'campeones nacionales' que permitan una mejor coordinación para un ciberespacio más seguro.

Ana Adeva y José Manuel Vera (Equipo SIC)

En 1983, tras ver la recién estrenada película 'Juegos de Guerra', el presidente de EE.UU., **Ronald Reagan,** preguntó a su jefe del Estado Mayor Conjunto, **John Vessey**, si "¿algo así podría ocurrir de verdad?". Y pocos días después la respuesta no pudo ser más preocupante: "presidente, el problema es mucho más grave de lo que usted cree". Así lo destacó **Fred Kaplan** en su libro 'Dark Territory: The Secret History of Cyber War' (2017), en el que recuerda que fue uno de los puntos de partida para que las agencias de inteligencia reforzaran sus estrategias ofensivas y defensivas en el ciberespacio.

Pocos años después, el país, a través de la **Carnegie Mellon** puso en marcha el primer equipo de respuestas a incidentes (CERT) tras sufrir el ataque del gusano Morris (1988), considerado el primer *malware* de la historia, diseñado por un estudiante de la **Universidad de Cornell, Robert Tappan Morris,** y liberado por accidente, infectando unos, aproximadamente, 6.000 de los 60.000 servidores conectados a la red.

Este hecho mostró que no había capacidades de respuesta ante incidentes de gran impacto y globales, actuándose de forma aislada y descoordinada tanto en EE.UU. como en el resto del mundo. Por ello, semanas después se creó el primer Centro de Coordinación de Respuesta ante Emergencias (CERT).

Sin embargo, a pesar de haber pasado más de dos décadas desde entonces y de la millonaria inversión en ciberseguridad nacional y todo tipo de esfuerzos, las cosas han cambiado menos de lo esperado. Un buen ejemplo de ello es el ciberataque sufrido por Estonia en 2007, contra numerosas infraestructuras críticas nacionales sembrando el caos y que dio pie a un intenso debate sobre si un incidente cibernético puede permitir invocar el artículo 5 del Tratado del Atlántico Norte, que obliga a los socios de la Alianza a acudir en ayuda de un país que es atacado.

Frente a un panorama de amenazas cibernéticas globales cada vez más complejo no hay país donde las políticas y capacidades cibernéticas no hayan pasado a ocupar, en la última década, un lugar central en la seguridad internacional, según destaca el **Instituto Internacional de Estudios Estratégicos** (IISS), en su informe 'Capacidades cibernéticas y poder nacional: una evaluación neta', de 2021. Un enfoque que pasa por establecer un marco de gobernanza, más o menos centralizado, más o menos militar, para abordar y gestionar las crecientes amenazas cibernéticas que afectan a la seguridad nacional, la infraestructura crítica y los ciudadanos, a partir de la publicación de su estrategia nacional de ciberseguridad y la colaboración con el resto de países que apuestan por el mismo estilo de vida.

Disparidad de estrategias y enfoques

Sin embargo, de puertas adentro cada país tiene su propio enfoque. Todas las estrategias nacionales de ciberseguridad (NCSS) cuentan con similitudes en la protección de activos, el compromiso con la investigación y el desarrollo y una mejor colaboración nacional e internacional, pero también se carece de un marco unificado de ciberseguridad subyacente, lo que se traduce en una gran disparidad en la estructura y el contenido de las estrategias, según destaca un estudio comparativo de varias de ellas de investiga-

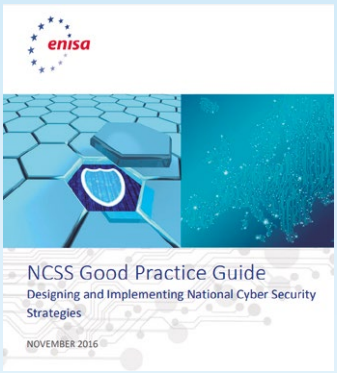
dores de la **Universidad de Staffordshire**, en Reino Unido.

"En algunos países, la atención puede centrarse en proteger el riesgo de infraestructura crítica, mientras que otros apuestan por proteger la propiedad intelectual y también los hay que se centran en mejorar la concienciación sobre la ciberseguridad de los recién conectados ciudadanos", destacaron **Goodwin** y **Nicholas,** en 2013, en un informe, recordando que "lo que constituye un riesgo significativo para un país puede no aplicarse a otro".

Por ejemplo, indica que en el caso de las estrategias de Canadá y el Reino Unido, estas se centran en la seguridad y la prosperidad económica en el mundo digital, mientras que las de Singapur y Estonia apuestan por la resiliencia y Australia y EE.UU. establecen su enfoque para una Internet abierta y segura. En otras, como la noruega, se considera la ciberseguridad parte de la apuesta por la transformación digital, o el caso español que fundamenta su estrategia en la seguridad y el crecimiento económico. Frente a ella, Lituania considera clave la concienciación y la resiliencia y en Estonia todo pasa por una "sociedad digital más resiliente".

Diferencia de enfoques en Europa

En Europa, **Enisa** publicó en 2012 y actualizó en 2016 una guía de buenas prácticas para diseñar e implementar una estrategia nacional de ciberseguridad (NCSS) en la que recomienda "establecer una estructura de gobernanza clara", proponiendo tres opciones de alto nivel para la estructura de gobernanza nacional, sin recomendar ninguno. De hecho, en su documento de 2023, 'Un marco de gobernanza para las estrategias nacionales de ciberseguridad', ya destaca que hay 31 países que cuentan con una. Entre otras recomendaciones, para llevarla a cabo aconseja "contar con un organismo que supervise el cumplimiento de las entidades reguladas con las normas europeas e internacionales" y "utilizar esquemas de certificación para productos, servicios y procesos TIC", entre otros aspectos, además de dotar a las autoridades concernidas con competencia sancionadora.



Por ello, actualmente, se vislumbra una tendencia a centralizar la gobernanza de la ciberseguridad. Un buen ejemplo es que los cuatro países más poblados de Europa –Alemania, Francia, Reino Unido e Italia– están apostando, desde hace tiempo, por centralizar cada vez más funciones este ámbito en un solo organismo. Sin embargo, a pesar de ello, cada agencia, centro o autoridad nacional de ciberseguridad en cada nación tiene su propia idiosincrasia. Ello hace que cada estado identifique su autoridad nacional encargada de transponer la directiva NIS2, de trabajar de forma conjunta en la red de CSIRT o de formar parte de la red de centros del Centro de Competencia en Ciberseguridad (ECCC).

Así, de momento, cada nación apuesta por un organigrama diferente. De momento, de los 27 países de la UE, más de 13 cuentan con una única autoridad nacional de ciberseguridad.

Eso sí, no hay unidad en el modelo de estructura de gobernanza. Mientras que una de las más veteranas, la **Agencia Nacional de Ciberseguridad** (NCSC), del Reino Unido (que no es UE), destaca por un enfoque muy proactivo en la gestión de amenazas cibernéticas y su capacidad para coordinar respuestas a incidentes a nivel nacional, otras como la **Agence Nationale de la Sécurité des Systèmes d'Information** (ANSSI) apuestan por un enfoque más integral en la protección de sistemas de información críticos. La alemana **Bundesamt für Sicherheit in der Informationstechnik** (BSI) es un referente en el desarrollo de estándares de seguridad cibernética y su papel en la protección de la infraestructura crítica en el país, entre otras. También, es de interés el caso de Italia que en 2021 creó su **Agencia Nacional de Ciberseguridad** (ANC), –la cual contará con 122 millones de presupuesto en 2026– aglutinando, entre otros aspectos, el trabajo de cinco organismos nacionales en este ámbito, que a partir de la puesta en marcha del Centro se convirtieron en sectoriales. Al igual que el caso de Irlanda que puso en marcha en 2011 su **National Cybersecurity Centre** (NCSC-IE) como autoridad nacional. Eso sí, existe una buena cooperación entre agencias y entes nacionales. En la reciente **Conferencia de Seguridad Cibernética de Múnich,** en febrero, varios de sus responsables mantuvieron reuniones para continuar con trabajos actuales por una Europa más cibersegura.

'Ciberejército' europeo

Incluso en la UE se valora, al margen del papel de las agencias nacionales de ciberseguridad, apostar por un enfoque más unificado en ciberdefensa, dependiente directamente de los mandos militares. En la última conferencia anual de la **Agencia Europea de Defensa** (AED), en noviembre de 2023, el responsable del **Consejo Europeo, Charles Michel**, propuso crear una "fuerza cibernética" a medida para reforzar sus capacidades defensivas en este ámbito y que debería ser un "componente fundamental" de la defensa de Europa. "Nos ayudaría a tomar

una posición de liderazgo en las operaciones de respuesta cibernética y superioridad de la información, y creo que debería estar dotado de capacidades ofensivas", explicó.

Enfoque poliédrico mundial

Fuera de Europa, el caso de EE.UU. es, sin duda, uno de los más interesantes por cuanto la ciberprotección es muy granular estableciéndose un CISO en la Casa Blanca, como encargado de aplicar la Estrategia Nacional de Ciberseguridad (cuya última edición es de 2023), y una asesora adjunta de seguridad nacional, **Anne Neuberger.** Y dos ramas: por un lado, la de Defensa, con la **Agencia Nacional de Seguridad** (NSA) y el Comando Cibernético, del DoD; y, por otro, para el sector público y privado, la **Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA),** dependiente del **Departamento de Seguridad Nacional** (DHS), encargada de "comprender, gestionar y reducir el riesgo de nuestra infraestructura física y cibernética". También, con una unidad de coordinación con la NSA.

Una arquitectura de gobernanza que, sin embargo, ha experimentado numerosas fricciones. Nadie olvida cuando, en mayo de 2009, el presidente **Barack Obama** identificó la ciberseguridad "como uno de los desafíos económicos y de seguridad nacional más graves que enfrentamos como nación, pero que nosotros, como gobierno o como país, no estamos preparados adecuadamente para contrarrestar", apostando por el "desarrollo de un enfoque integral para proteger la infraestructura digital de Estados Unidos", creando la figura del Coordinador de Ciberseguridad del Poder Ejecutivo, directamente bajo su mando para garantizar una respuesta organizada y unificada a futuros incidentes cibernéticos. Cargo para el que designó a **Rod A. Beckstrom.** Sin embargo, menos de un año después, renunció por falta de financiación y apoyo, además de por constatar una dependencia excesiva de la NSA y sus intentos de dominar los esfuerzos de seguridad cibernética por parte de la agencia.

Rusia

En cuanto a Rusia, la lista de ciberactores es larga y compleja. Incluye entidades privadas, no siempre legítimas, junto con los servicios de seguridad tradicionales, el ejército y el nivel político superior, donde se toman las decisiones siempre con carácter presidencial. Por ello, existe una coordinación estrecha entre diversos organismos gubernamentales, como el **Servicio Federal de Seguridad** (FSB), el principal organismo de seguridad nacional de Rusia, que incluye responsabilidades en ciberseguridad, el **Centro Nacional de Coordinación de Ciberseguridad** (NCC), encargado de coordinar la respuesta a incidentes cibernéticos y promover la seguridad cibernética, así como el **Ministerio de Defensa** y la Agencia de Seguridad de la **Información del Gobierno de Rusia** (FSTEC), para abordar las amenazas cibernéticas de manera integral. Además, también actúa tanto a través del **Servicio de Inteligencia Exterior de Rusia** (SVR) como de la **Dirección Principal de Inteligencia del Estado Mayor General** (GRU), la primera involucrada en actividades de ciberespionaje en el extranjero y la segunda con una participación más directa en operaciones cibernéticas ofensivas y defensivas.

China

En el caso de **China**, todo pasa por su apuesta de ser la primera "potencia cibernética" y a ello dirige todo tipo de recursos. Sin una agencia única, entre los organismos más importantes del país en este ámbito está la **Oficina de Ciberseguridad y Coordinación de la Información** (CNCERT), encargada de coordinar y supervisar la ciberseguridad en China, además de las competencias del **Ministerio de Seguridad Pública** (MSP), responsable de hacer cumplir las leyes en esta materia y combatir el cibercrimen. También, destaca su **Administración del Ciberespacio de China** (CAC), creada en 2011, que es el organismo regulador de internet en China. Por supuesto, cuenta con unidades de ciberdefensa muy activas en el **Ejército Popular de Liberación** (PLA). Como curiosidad, para desarrollar capacidades y profesionales cuenta con un **Centro Nacional de Ciberseguridad** –su nombre oficial es Base Nacional de Innovación y Talento en Ciberseguridad–, en una extensión de 40 km^2, con centros de investigación y emprendimiento, laboratorios y una Escuela Nacional de Ciberseguridad, y el apoyo de los niveles más altos del **Partido Comunista Chino** (PCC).

Israel

Tampoco hay que olvidarse de uno de los grandes referentes en el ámbito cibernético, **Israel**, para el que la ciberseguridad es una prioridad nacional debido a la importancia estratégica de la tecnología y la información en el país. Su gobernanza se centraliza a través de la denominada **Dirección Nacional Cibernética de Israel (INCD),** dentro del **Israel National Cyber Directorate (RIDC)**, responsable de coordinar esfuerzos, establecer políticas y directrices, y supervisar la implementación de medidas de seguridad cibernética en los sectores público y privado, y depende directamente de la Oficina del Primer Ministro. Entre sus funciones están desde la salvaguardia de la infraestructura crítica, la seguridad nacional y los avances tecnológicos del país, hasta la recopilación y el análisis de inteligencia y en la respuesta a las amenazas cibernéticas, así como su equipo Nacional de Respuesta a Incidentes Cibernéticos (CERT-IL).

¿Hace falta crear una Agencia Nacional en España?

Aprovechando el 'V Encuentro del Esquema Nacional de Seguridad (ENS)', en junio del año pasado, se celebró una mesa de debate sobre 'El gobierno de la ciberseguridad nacional, hacia dónde vamos'. Moderada por el editor de **SIC, Luis Fernández,** en ella intervinieron el subdirector general del **CCN**, **Luis Jiménez**, el por entonces comandante del **Mando Conjunto del Ciberespacio**, general **Rafael García**, el jefe de la **Oficina de Coordinación Cibernética, Álvaro de Lossada**, **Miguel Martín**, representando al **Incibe, Andrés Ruiz**, por aquel entonces asesor en ciberseguridad del **Departamento de Seguridad Nacional**, y **Tomás Roy**, director de la **Agencia de Ciberseguridad de Cataluña**.

Los participantes destacaron la necesidad de aprobar una tercera estrategia nacional de ciberseguridad y, también, la de establecer una Agencia Nacional. Así lo manifestó Ruiz, que consideró que "tarde o temprano la tendremos, ya que somos de los pocos países que no cuentan con una", resaltando al Reino Unido como el ejemplo a seguir. De Lossada apostilló que "somos un país descentralizado y la seguridad y la ciberseguridad deben ser corresponsabilidad de todos los actores implicados". Por su parte, el general Hernández recordó que siempre sería bienvenida pero con "un sistema de cogobernanza, que marque a cada uno en su sitio". Jiménez también consideró positiva "la coordinación de políticas y capacidades, centralizando muchas dispersas en organismos para tener más eficiencias e influencia en Europa". "Aunque para ello habrá que prestar atención a los detalles, al cómo se construye, dónde, qué y con qué responsabilidades, por lo que exige un debate sosegado entre los actores que estamos en ciberseguridad", respondió De Lossada. Lo que quedó claro, según el general Hernández es que, "salvando las distancias, necesitamos un 'director de orquesta'", "sin despedir a todos los músicos", añadió De Lossada.

Eso sí, no hubo unanimidad sobre de quién debería depender una agencia nacional. Mientras que Ruiz consideró que, igual que la Agencia Nacional italiana, debería depender del ministerio de Presidencia, Jiménez consideró que debería depender de la Secretaría de Estado del CNI...

En definitiva, la conclusión de la mayoría manifestó que España también contará con su Agencia Nacional, tras un debate profundo... "La pregunta es cuándo", dijeron los participantes. Quizá, sea una de las grandes novedades en esa esperada tercera versión de la Estrategia Nacional de Ciberseguridad que, tras la de 2019, debería ver la luz en breve.

Además, en el ámbito militar está la **Unidad 8200,** de inteligencia de las **Fuerzas de Defensa de Israel** (IDF), especializada en inteligencia de señales y operaciones cibernéticas. Muchos expertos en ciberseguridad de Israel, en el sector privado, provienen de esta unidad.

Ministra de ciberseguridad en Australia

Quizá el caso más emblemático sea el de Australia, que cuenta con una cartera ministerial de seguridad cibernética desde 2017, actualmente ocupada por **Clare O'Neil**. Bajo ella trabaja el **Centro Australiano de Seguridad Cibernética (ACSC**), fundado en 2014 y que depende también de la Dirección de Señales de Australia (ASD) y colabora con varias partes interesadas para abordar los desafíos de ciberseguridad.

En Oriente Próximo está, como referente, la **Autoridad Nacional de Ciberseguridad de Arabia Saudita** (NCA), creada en 2017, dependiente de las máximas autoridades, el Rey y el Príncipe heredero, con la misión de "impulsar la ciberseguridad del estado, proteger sus intereses, la seguridad nacional y la infraestructura sensible".

En Asia, destaca la **Agencia de Seguridad Cibernética (CSA), de Singapur**, de 2015, dependiente de la Oficina del Primer Ministro. Entre otras funciones, se encarga de desarrollar la estrategia de ciberseguridad, colaborar con otras agencias y supervisar los sectores críticos. Además, también tiene capacidades de respuesta.

Seis posibles modelos de gobernanza nacional en ciberseguridad

Entre los diferentes trabajos que analizan qué modelo de gobernanza en ciberseguridad nacional es mejor, destaca el estudio publicado hace dos años por **Todor Tagarev,** entonces miembro del **Instituto de Tecnologías de la Información y las Comunicaciones,** y hoy Ministro de Defensa de Bulgaria, y **Vasil Rizov**, miembro del **Colegio de Defensa Nacional GS Rakovski**, bajo el título **'**Modelos alternativos de organización nacional de ciberseguridad: evaluación comparativa', en la Revista de la 'Academia de Gestión Estratégica', integrada por expertos de todo el mundo.

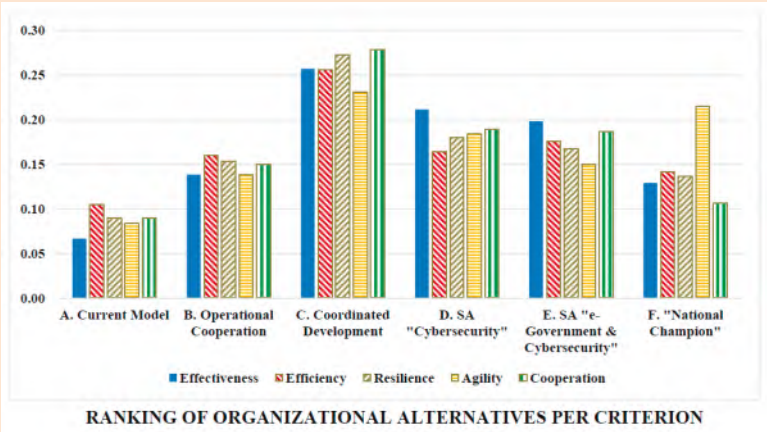
En él, "exploran formas alternativas de organizar estas capacidades a nivel nacional para intentar definir un 'mejor' modelo", en gobernanza nacional de la ciberseguridad. Y analizan cada uno según cinco criterios -efectividad, eficiencia, resiliencia, agilidad y cooperación-, proponiendo "seis modelos alternativos ubicados en dos dimensiones según el grado de coordinación entre los principales contribuyentes a la ciberseguridad y el grado de centralización".

Mas o menos centralización

Así, en su análisis considera que existe un primer tipo de organización, sin un claro líder en este ámbito, "con responsabilidades clave en materia de ciberseguridad asignadas a organizaciones existentes". El segundo tipo identificado, '**Modelo de cooperación operativa',** es la evolución del anterior con "mecanismos de coordinación operativa, previstos en la estrategia nacional de ciberseguridad y la ley de ciberseguridad", en el que "las organizaciones con responsabilidades clave para diferentes sectores de interés (defensa, aplicación de la ley, etc.) interactúan continuamente y coordinan sus actividades para monitorizar y mantener una imagen común del ciberespacio. Además, supone "crear un Centro Nacional de Situación Cibernética para apoyar la cooperación operativa". El tercero, '**Desarrollo coordinado de capacidades'**, a partir del anterior, suma "la cooperación operativa y el uso coordinado de agencia y recursos comunes para crear el espectro de capacidades de ciberseguridad necesarias". En este nivel, también se prevé el establecimiento de una Red Nacional de Coordinación de Ciberseguridad. En definitiva, en estos tres modelos, "la arquitectura de ciberseguridad a nivel nacional permanece distribuida, pero aumenta el grado de coordinación entre las agencias responsables".

Mayor centralización

Tanto en el cuarto modelo como en el quinto, se apuesta por una mayor centralización. En el denominado '**Agencia Estatal Ciberseguridad'** se configura la gobernanza en torno a la "creación de una nueva agencia estatal centrada íntegramente en la ciberseguridad", con "funciones tanto operativas como de supervisión en la provisión de ciberseguridad, incluida la lucha contra el ciberdelito y el ciberespionaje, las actividades de ciberdefensa y la protección de infraestructuras críticas y activos estratégicos, y la seguridad criptográfica", y posicionando a la agencia como "un componente del sistema de seguridad nacional". El quinto, bautizado como de **'Agencia Estatal e-Gobierno y Ciberseguridad'**, la Agencia también aglutina "responsabilidades *civiles*" para la protección de la seguridad nacional. Por último, el sexto, propone la **'Subcontratación a una empresa líder (campeona nacional)'**.



RANKING OF ORGANIZATIONAL ALTERNATIVES PER CRITERION

Cooperación y consolidación

Su conclusión es que hay una clara "preferencia por una sólida cooperación y coordinación operativa en el desarrollo de capacidades de ciberseguridad" pero "depende de cada país encontrar el modelo que mejor se adapte al panorama de amenazas y vulnerabilidades cibernéticas específicas, los acuerdos administrativos generales, las relaciones público-privadas y sociales, y la capacidad humana y tecnológica disponible", destacan los dos autores.

Europa: camino de un marco legislativo para impulsar la colaboración, la armonización y la acción común

Desde que en 2013 se diera un por primera vez un importante impulso a la ciberprotección en la UE con la elaboración de la Estrategia de Ciberseguridad, los avances regulatorios han dado forma a la coordinación y gobernanza del ecosistema en Europa, propiciando la creación de distintos organismos, grupos y redes para atajar las disparidades entre estados y las lagunas existentes a escala nacional en la materia. Normativas como NIS2, cuya implementación será obligatoria en 2025, marcarán un antes y un después en este ámbito cada vez más crítico por las constantes amenazas a la ciberseguridad nacional por parte de países como China y Rusia.

El panorama regulatorio y político de la ciberseguridad ha experimentado cambios sin precedentes en los últimos años, convirtiéndose en objeto de leyes, normativas y recomendaciones internacionales, así como en la asignación de recursos concretos. Muchos de estos avances tienen como fin impulsar una colaboración, coordinación, armonización y acción común, tanto en la UE como fuera de sus fronteras, dando forma, además, al entorno empresarial en todo el mundo, debiéndose adecuar a su cumplimiento.

Una cuestión clave en este sentido es el tipo de gobernanza en tales iniciativas. En el caso de la UE se presume, al menos, horizontal y colaborativa. Y es que la creciente digitalización e interdependencia entre los países, ha elevado la necesidad de una cooperación eficaz entre los Estados miembros y las instituciones para poder dar una respuesta más rápida y una coordinación adecuada en todos los niveles (estratégico, operativo, técnico y de comunicaciones). Especialmente, en una Europa que sigue fragmentada debido a la falta de soluciones interoperables y con un grado de madurez diferente entre países en este ámbito.

Dos décadas de trabajo

Así pues, existen importantes iniciativas que están repercutiendo directamente en la forma de cooperación, provisión, desarrollo de capacidades, gestión y supervisión de la seguridad. Entre ellas, destaca, sin duda, el papel central que, en 2019, se le otorgó a la **Agencia de Ciberseguridad de la UE** (**Enisa**), a través de la Ley de Ciberseguridad (*Cybersecurity Act*), con un mandato permanente, más recursos y nuevas tareas.

La Agencia, que este año cumple dos décadas, desempeña ahora un papel clave en el apoyo en la implementación de políticas, en el desarrollo de capacidades cibernéticas, en la divulgación coordinada de vulnerabilidades, así como en la creación y el mantenimiento del marco europeo de certificación de la ciberseguridad de productos, servicios y procesos de TIC. Además, está facultada para contribuir a intensificar tanto la cooperación operativa

(ayudando a los Estados miembros que deseen solicitarla a manejar sus incidentes de ciberseguridad), como a apoyar la coordinación de la UE en caso de ciberataques y crisis transfronterizas a gran escala.

Primer instrumento horizontal para la resiliencia

Junto a ello, cabe destacar, sin duda, la adopción en 2016 del "primer instrumento horizontal del mercado interno destinado a mejorar la resiliencia de las redes y los sistemas de información de la Unión frente a los riesgos de ciberseguridad", según definen desde la **Comisión Europea**. Se trata de la Directiva sobre redes y sistemas de información (NIS) de la UE que, si bien tuvo notables logros, mostró a su vez ciertas limitaciones, como un nivel inconsistente de resiliencia entre Estados miembros y en sectores, insuficiente comprensión común de las principales amenazas y desafíos, así como una falta de respuesta conjunta a la crisis. Esto dio lugar a la propuesta por parte de la Comisión, en diciembre de 2020, de un conjunto revisado de normas: la conocida como NIS2, la Directiva sobre medidas para un alto nivel común de ciberseguridad en toda la Unión, que entró en vigor en enero de 2023 y que la gran mayoría de los Estamos miembros están inmersos en su transposición, ya que el límite es el 17 de octubre de este año. El único país que a fecha de cierre de esta edición anunció su transposición fue Bélgica, el 27 de marzo, en un proyecto de ley para NIS2 que reemplaza completamente la Directiva NIS en el país y formará parte de su estrategia de ciberseguridad 2.0.

Aspectos clave de la NIS2

Entre otros aspectos, NIS2 amplía su ámbito de aplicación para abarcar a grandes y medianas entidades de más sectores críticos (con dos categorías: esenciales e importantes), refuerza los requisitos de seguridad y notificación para las empresas, introduce medidas de supervisión más estrictas para las autoridades nacionales, así como requisitos de aplicación más estrictos y pretende armonizar los regímenes de sanciones en todos los Estados miembros. También, mejora el papel del Grupo de Cooperación (*NIS Cooperation Group*) a la hora de dar forma a decisiones políticas estratégicas y aumenta el intercambio de información y la cooperación entre las

autoridades de los Estados miembros.

Además, impulsa la cooperación operativa dentro de la red CSIRT y establece una **Red Europea de Organizaciones de Enlace en crisis cibernéticas (EU-CyCLONe)**. Una iniciativa que se puso en marcha en 2023, con

representantes de las autoridades de gestión de cibercrisis de los Estados miembros, para apoyar a la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel operativo y garantizar el intercambio regular de información relevante entre los Estados miembros y las instituciones, órganos, oficinas y agencias de la Unión.

Marco de gobernanza

Eso sí, la Directiva deja a cada Estado miembro autonomía a la hora de estructurar sus órganos en esta materia, pero obliga a definir un marco de gobernanza que se coordine con las estructuras europeas para su aplicación. Por ello los Estados miembros deben de cumplir unos requisitos mínimos como son designar una o más autoridades competentes de ciberseguridad, un punto de contacto único, así como equipos de respuesta a incidentes de seguridad informática (CSIRT). Además, en cuanto a la supervisión y ejecución, busca garantizar que las autoridades competentes supervisen efectivamente y adopten las medidas necesarias, incluyendo un régimen sancionador.

Grupo de Cooperación NIS y Red de CSIRT

Como parte fundamental para mejorar y facilitar la coordinación y cooperación estratégica y el intercambio de información entre los Estados miembros, a raíz del artículo 14 de la NIS2 se ha establecido el Grupo de Cooperación NIS, que es relevante en el organigrama europeo. Lo preside el país que ostenta la Presidencia del Consejo de la UE (por tanto, hasta

el 30 de junio es Bélgica), y está compuesto por representantes de los Estados miembros, la Comisión y de Enisa. Entre otras funciones, intercambia información con la red EU-CyCLONe y, además, en el frente operativo, cuenta con el apoyo del trabajo de la **red de CSIRT** (*CSIRT Network*). Precisamente, esta red, establecida por la Directiva NIS y fortalecida por la NIS2, es un elemento importante de la resiliencia europea por cuanto busca "contribuir al desarrollo de la confianza y promover una cooperación operativa rápida y eficaz". Está compuesta por CSIRT designados por los Estados miembros y de CERT-EU y, aunque la NIS establece que cada país designe uno o más CSIRT, no en todos los casos los estados han designado solo uno, sino dos o incluso hasta tres, como en el caso de Austria, Polonia y España (CCN-CERT, INCIBE-CERT y ESP DEF CERT), según se muestra en el mapa de su página oficial (csirtsnetwork.eu).

CERT-EU

Junto a todo ello, cabe mencionar el papel del **CERT-EU**, creado en 2011, que se presenta como "una de las entidades de ciberdefensa más maduras de Europa y un engranaje central de ciberseguridad de la UE". Está formado por un equipo de expertos en seguridad informática de las instituciones y organismos de la UE. Además, coopera con CERT nacionales (tanto en países de la UE como fuera de la UE) y socios internacionales, para mejorar el nivel de intercambio de información. En diciembre de 2023 se publicó el Reglamento 2023/2841 que refuerza el objetivo del CERT-EU considerándolo como Servicio de la Ciberseguridad para las instituciones, órganos, oficinas y agencias de la Unión, aunque manteniendo su nombre.

Cibersolidaridad y la red transnacional de SOC

Entre otras iniciativas también cabe destacar que, el 20 de marzo, el **Parlamento Europeo** y la **Presidencia del Consejo** llegaron a un acuerdo provisional sobre la llamada 'Ley de Cibersolidaridad' (como se hace eco este número de SIC en sus Noticias). La propuesta incluye un nuevo mecanismo de cooperación en el ecosistema de ciberseguridad europeo al establecer la creación de un Escudo Europeo de Ciberseguridad y un Mecanismo de Ciberemergencia integrado para desarrollar un mejor método de ciberdefensa.

Estrategia de Ciberseguridad

Entre otras iniciativas, también hay que hacer referencia a la importancia de la Estrategia de Ciberseguridad (*EU Cybersecurity Strategy*) que, en su versión más reciente, de finales de 2020, sigue impulsando el desarrollo de capacidades colectivas para responder a los ciberataques y el trabajo con socios de todo el mundo. En ella, se indica que "las cuatro cibercomunidades (aquellas que se ocupan del mercado interno, de la aplicación de la ley, de la diplomacia y de la defensa) deben trabajar más estrechamente para lograr una conciencia compartida de las amenazas".

Una Unidad Cibernética Conjunta para la gestión de crisis

Fruto de la Estrategia de Ciberseguridad y de la Estrategia de una Unión de la Seguridad de la UE, en junio de 2021, la Comisión propuso la creación de una **Unidad Cibernética Conjunta** (*Joint Cyber Unit, JCU*), a escala de la UE, como "paso importante hacia la finalización del marco europeo de gestión de crisis de ciberseguridad".

En concreto, la Comisión destaca que la JCU es necesaria porque "la UE actualmente no dispone de espacios para facilitar una cooperación estructurada entre los Estados miembros y todas las instituciones, organismos y agencias pertinentes de la UE en materia de ciberseguridad".

La JCU se ubicará en las oficinas de Enisa y CERT-EU en Bruselas. Eso sí, los países de la UE han enfatizado "la importancia de racionalizar los procesos y estructuras existentes para reducir la complejidad", según Euractiv. Los gobiernos nacionales también reafirmaron sus prerrogativas nacionales, especialmente en competencias, mandatos y poderes legales, al tiempo que pidieron una estructura de gobernanza que considere "adecuadamente" a todos los países involucrados.

Aprovechar sinergias, establecer jerarquías y marcar un camino para actuar rápido ante crisis cibernéticas define la gobernanza de cada país

Entre la defensa y la protección de lo digital: el reto de apostar por agencias nacionales de ciberseguridad

Decía el polifacético Benjamin Franklin que "por cada minuto dedicado a la organización, se gana una hora". Y poco hay más acertado al proceso que está viviendo Europa con la transposición de la directiva NIS2 que, entre otros cambios notables, obliga a cada Estado miembro a designar los órganos necesarios para la coordinación de las políticas adoptadas para mantener un alto nivel de seguridad en toda la UE, aunque cada país adapta su modelo de gobernanza a sus necesidades.

"Es fundamental que cada país disponga de una autoridad nacional a cargo de la supervisión y el cumplimiento de las organizaciones de ciberseguridad derivadas de la NIS". Así lo destacaba en una amplia entrevista, en SIC 153, la directora para la Sociedad Digital, la Confianza y la Ciberseguridad de la **DG Connect** de la **Comisión Europea**, **Lorena Boix**. Se trata de un paso más hacia un ciberescudo europeo, aprovechando las sinergias nacionales. Un reto para el que Europa ofrece, a través de sus organismos, un papel de apoyo, coordinación y acción común en materia de ciberseguridad en todo el ámbito comunitario, además de abordar aquellos aspectos que tienen que ver con el desarrollo de capacidades y niveles mínimos de seguridad en cada Estado miembro.

Pero cada país materializa, de forma independiente, su estructura institucional y organismos nacionales a través de una estrategia de ciberprotección adaptada a sus necesidades y una gobernanza que, en algunos estados está vinculada al ámbito de la Defensa y, en otros, al de la transformación digital. Lo que nadie discute es la necesidad de contar con organismos que permitan ser eficientes y, también, actuar con rapidez ante amenazas cada vez más complejas.

En este sentido, en Europa encontramos muchos países que apuestan por autoridades nacionales de ciberseguridad bajo la denominación de 'agencias', 'centros' u 'oficinas'. Una apuesta que han hecho ya los cuatro países más poblados del Viejo Continente –Alemania, Francia, Italia y Reino Unido– centralizando el control y la gestión de la seguridad nacional en un único punto, que también actúa como contacto frente a la Red europea de CSIRT, entre otros casos.

De igual forma, Bélgica que ostenta la presidencia del Consejo de la UE se encuentra entre los que más centralizada tiene la gestión de su ciberprotección. En concreto a través de su **Centro de Ciberseguridad** (CCB), considerado la autoridad central del país en este ámbito que, entre otras, tiene como funciones implementar la política nacional en ciberprotección, con todos los departamentos gubernamentales, así como seguir, coordinar y supervisar la aplicación de su estrategia, además de garantizar la gestión de crisis, entre otros.

Optan también por este tipo de enfoques países como **Estonia** con su Information System Authority (NISA) y su National Cyber Security Centre (NCSC-EE) que, desde marzo de 2023, han pasado a denominarse **Centro Nacional de Seguridad Cibernética** (NCSC)**,** dependiente del Ministerio de Asuntos Económicos y Comunicaciones, y que otros países nórdicos como Letonia, Lituania, Finlandia, Suecia y Dinamarca también tienen en vigor a través de entidades similares. O **Chequia** con su **Agencia Nacional de Seguridad Cibernética y de la Información** (NÚKIB), desde 2017, englobando al Consejo de Seguridad del Estado (BRS), miembro del Comité de Seguridad Cibernética, encargado de coordinar y planificar la ciberseguridad nacional; y al Centro Nacional de Seguridad Cibernética (NCKB), así como a la División de Compromiso y Asuntos Estratégicos.

NIST, más de 50 años de... ¿la primera ciber 'agencia' nacional?

Aunque igual la primera agencia cibernética, como tal, podría ser considerada **Arpanet** (*Advanced Research Projects Agency Network*), que dio lugar a Internet, seguramente por méritos propios podría ser considerado el NIST (hasta 1988 denominado **Instituto de Ciencias y Tecnología Informática de la Oficina Nacional de Estándares** –NBS–). Se trata del organismo que, desde 1972, ha desarrollado todo tipo de investigaciones sobre ciberseguridad y publicado directrices sobre protección cibernética tanto para el sector privado, como el público, así como la Academia.

Entre sus hitos más destacados figura el haber establecido un programa de seguridad informática en 1985, hasta desarrollar el estándar del uso de la contraseña, en 1974, o haber publicado la primera guía ejecutiva de bolsillo de seguridad informática en 1976, cuando solo había 130.000 ordenadores en todo EE.UU. y que sirvió de base para que el Congreso aprobara la primera Ley de Seguridad Informática, en 1987.

También resulta de especial interés la evolución que ha experimentado el **Centro Nacional de Ciberseguridad** (NCSC) de **Suiza**, por la información crítica con la que cuenta el país. Para fortalecer sus capacidades, en 2022 el Consejo Federal decidió transformarlo en una Oficina Federal, a partir del 1 de enero de 2024, siendo dependiente del Departamento Federal de Defensa, Protección Civil y Deportes (DDPS).

Eslovenia, bajo la denominación de **Oficina Gubernamental de Seguridad de la Información** (URSIV) también tiene un modelo centralizado con una autoridad nacional competente en el campo de la seguridad. Conecta a las partes interesadas en el sistema nacional y coordina las capacidades operativas a un nivel estratégico. Es también el único punto de contacto para garantizar la cooperación transfronteriza con las autoridades pertinentes de otros Estados miembros de la UE y con la Red Europea CSIRT, junto con otras tareas de cooperación internacional. Además, supervisa la implementación de su Ley de Seguridad de la Información (ZInfV) y, debido a que tiene la tarea de informar al Gobierno y al Consejo de Seguridad Nacional (NSC) en caso de incidente crítico o ataque cibernético, la URSIV también se incluye dentro del sistema de seguridad nacional.

Asimismo, en **Eslovaquia** se denomina **Oficina de Seguridad Nacional** al organismo central de la administración estatal para la ciberseguridad del país. La creación de la oficina está históricamente relacionada con las negociaciones sobre la entrada de la República Eslovaca en la UE y la OTAN, en las que se exigía la creación de una institución independiente que se encargaría de la protección de los datos clasificados, del cifrado y la protección de la información. En enero de 2016, la oficina asumió la responsabilidad de la seguridad cibernética, siendo también punto de contacto nacional para la ciberseguridad ante la UE. Para fortalecer sus capacidades, también puso en marcha la Unidad Nacional SK-CERT (Equipo Eslovaco de Respuesta a Emergencias Informáticas) que desde 2019 se ha convertido en el Centro Nacional de Seguridad Cibernética SK-CERT, que forma parte de la red de CSIRT de la UE.

Autoridades bajo Defensa

Al igual que, en países como Francia, donde la autoridad nacional (ANSSI) depende de la secretaría general de Defensa, resulta interesante destacar que, en **Lituania**, el **Centro Nacional de Seguridad Cibernética** (NKSC), forma parte del Ministerio de Defensa. Por ello es "responsable de la gestión unificada de ciberincidentes, el seguimiento y control de la implementación de los requisitos de ciberseguridad y la seguridad de la información crítica, infraestructura y acreditación de recursos de información". Además, es punto de contacto en la implementación de la Directiva NIS y Centro Nacional de Coordinación (NCC) y tiene la función de CERT-LT. Pero, además, dentro de las ramas del NKSC, está el Centro Regional de Ciberdefensa, que inició sus operaciones en 2021.

Autoridades nacionales más recientes

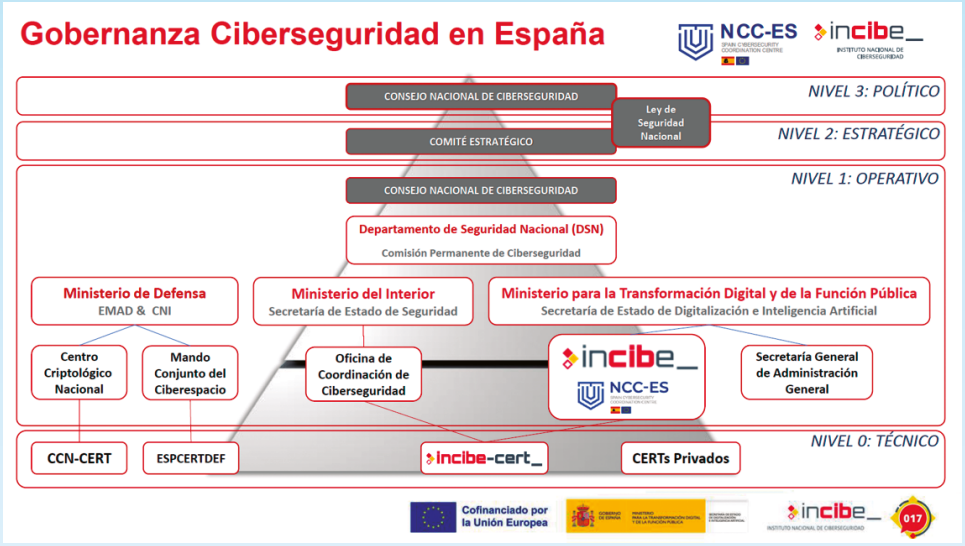
Entre las últimas en apostar por una agencia nacional está Grecia, cuyo **Ministerio de Gobernanza Digital** está poniendo en marcha su Autoridad de Ciberseguridad. El proyecto de ley para su creación finalizó su consulta pública en enero de este 2024. "El principal objetivo será la coordinación e implementación de la Estrategia Nacional de Seguridad Cibernética, así como la prevención y gestión efectiva de los ataques cibernéticos en Grecia, con el fin de lograr un alto nivel de seguridad de las redes y los sistemas de información en los sectores público y privado", se dice en su anuncio. Estructuralmente, será una evolución y actualización de la Dirección General de Ciberseguridad del Ministerio de Gobernanza Digital y estará supervisada, por tanto, por ésta última. Contará con una plantilla de 155 empleados.

Modelos más descentralizados

Frente a estos modelos centralizados llama la atención el caso de **Austria,** que es uno de los que más distribuida tienen su estructura de gobernanza en ciberseguridad, ya que muchos organismos del Gobierno son competentes en este ámbito. En menor medida, **Luxemburgo** cuenta con una **Agencia Nacional de Seguridad de los Sistemas de Información** para el sector público y las infraestructuras críticas, adscrita a su Alta Comisión para la Protección Nacional, pero ésta, por ejemplo, no aglutina los mismos cometidos que sus homólogas en otros países ya que, por ejemplo, el punto de contacto en el contexto de la implementación de Directiva NIS se establece en el Instituto Regulador de Luxemburgo, que depende del Ministerio de Asuntos Exteriores y Europeos. Y es su Centro Nacional de Competencia en Ciberseguridad (NC3), dependiente del Ministerio de Economía, el que actúa como Centro Nacional de Coordinación (CCN), según la Estrategia de Ciberseguridad 2021-2025 del país.

Cuenta atrás en 2024

España estaría en un punto medio, en este camino hacia la centralización con diferentes organismos competentes en diferentes ámbitos –**CCN, Incibe, OCC, MCCE, DSN**–, aunque ninguno con capacidad ejecutiva sobre el resto. Por ello, se espera con expectación la anunciada Ley de Ciberseguridad integral por parte del ministro de Transformación Digital y Función Pública, **José Luis Escrivá**, previéndose su eventual aprobación antes de finales de año, y que podría vincularse a la trasposición de la NIS2.



Entre otros aspectos se espera que sirva para reducir el riesgo cibernético español y ofrezca un nuevo marco de trabajo que permita reforzar los mecanismos actuales y la coordinación entre los diferentes agentes involucrados, en caso de incidentes, así como regular el uso de proveedores de riesgo, además de incentivar la innovación en este ámbito y la generación de profesionales, ante el déficit existente.

No sería raro que también España contará con un organismo nacional (quizá agencia o centro) en este ámbito, dado que se ha convertido en la enseña de identidad de la apuesta de cualquier país u organización por dar al tema que trata la máxima prioridad. Entre los ejemplos conocidos más destacados en nuestro país están desde la recientemente puesta en marcha de Agencia Espacial española, hasta la Agencia Estatal Antidopaje y la de Seguridad Aérea.

Cuatro agencias nacionales que marcan el camino...

CENTRO NACIONAL DE SEGURIDAD CIBERNÉTICA (NCSC)

Reino Unido es, sin duda, uno de los grandes referentes europeos por la madurez de su arquitectura de gobernanza en ciberseguridad, a través de su **Centro Nacional de Seguridad Cibernética** (NCSC), creado en 2015 y dependiente del **Cuartel General de Comunicaciones del Gobierno** (GCHQ), uno de los tres servicios de inteligencia del país. El organismo fue inaugurado dos años después y con él se centralizó el trabajo del CESG (la unidad de seguridad de la información del GCHQ), el Centro de Evaluación Cibernética (CCA), el Equipo de Respuesta a Emergencias Informáticas del Reino Unido (CERT UK), además de integrar las funciones del Centro para la Protección de la Infraestructura Nacional (CPNI).

Actualmente, con un presupuesto anual que ronda los 2.000 millones de euros, dentro de su Estrategia Nacional de Ciberseguridad y un millar de empleados, es un buen ejemplo de agencia nacional de ciberprotección por las capacidades que aglutina: desde supervisar la respuesta de la organización a incidentes cibernéticos hasta mejorar la resiliencia cibernética de la infraestructura nacional crítica, identificar los riesgos y oportunidades en tecnologías emergentes, entre otros aspectos. Además, es punto de contacto único para pymes, organizaciones más grandes, agencias gubernamentales, el público en general y departamentos de la Administración y colabora con fuerzas del orden, defensa, agencias de inteligencia y seguridad del país.

AGENCIA NACIONAL DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN (ANSSI)

Francia es otro de los grandes referentes en Europa con su **Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI),** creada en 2009 y que depende de la Secretaría General de Defensa y Seguridad Nacional (SGDSN) "para ayudar al primer ministro en el ejercicio de sus responsabilidades en materia de defensa y seguridad nacional".

Heredera de la Dirección Central de Seguridad Informática, cuenta con una plantilla de más de 700 personas y más de 100 millones de euros de presupuesto. Su misión es "garantizar la misión de la autoridad nacional en materia de seguridad de los sistemas de información. Como tal, le corresponde proponer normas para la protección de los sistemas de información estatales y verificar la implementación de las medidas adoptadas. Además, la ANSSI desempeña un papel clave en ciberdefensa y de orientación de la investigación francesa y europea en materia de ciberseguridad. Para consultas de alto nivel cuenta con un comité estratégico compuesto por altos funcionarios gubernamentales, para visiones estratégicas en este campo.

OFICINA FEDERAL DE SEGURIDAD DE LA INFORMACIÓN (BSI)

Alemania, junto a Francia, destaca por sus medios y por trayectoria. Cuenta con una estructura muy unificada a través de la **Oficina Federal de Seguridad de la Información** (BSI), dependiente del Ministerio Federal de Interior, Construcción y Comunidad, y dispone de una plantilla de casi 1.750 empleados y para este año 237,5 millones de presupuesto.

Fundada en 1991, y con una ley actualizada en 2009, su cometido inicial fue proteger las redes gubernamentales y asegurar las puertas de enlace de las redes centrales, aunque sucesivas normativas la han ido encomendando otros aspectos que van desde el desarrollo de estándares, hasta asesoramiento experto, consultoría, etc. También, se convirtió en la Oficina Central de Informes para la Seguridad de TI dentro de la administración federal, proporcionando información y análisis para garantizar la capacidad del gobierno federal para actuar durante crisis de TI de importancia nacional. En febrero de este año renovó su enfoque bajo el concepto de '**Cybernation Germany**', que se plasma en seis objetivos: impulsar la ciberseguridad a un lugar más alto en la agenda, la ciberresiliencia, hacer un uso específico de los conocimientos tecnológicos, avanzando constantemente en la digitalización, dar forma a la ciberseguridad con pragmatismo y promover un próspero mercado cibernético en Alemania".

AGENCIA POR LA CIBERSEGURIDAD NACIONAL (ACN)

En **Italia**, la **Agencia por la Ciberseguridad Nacional** (ACN) es la Autoridad Nacional de Ciberseguridad para proteger los intereses nacionales en este campo y la resiliencia, se sitúa bajo la Presidencia del Consejo de Ministros. Fue creada en junio de 2021 por Decreto Legislativo, que "redefinió la arquitectura nacional de ciberseguridad, con el objetivo de racionalizar y simplificar el sistema de competencias existente a nivel nacional", indican desde la propia Agencia. En 2022, contaba con una plantilla de más de 300 personas y su presupuesto para 2024 es de 84 millones de euros, aunque se espera que ascienda para 2026 a 122 millones de euros.

Entre sus cometidos, destaca el garantizar la implementación de la Estrategia Nacional de Ciberseguridad. También, se designa como autoridad nacional competente y punto de contacto en materia de la NIS2. Es la autoridad nacional de certificación de ciberseguridad y participa en las actividades internacionales del Grupo Europeo de Certificación de Ciberseguridad (ECCG). Bajo la ACN operan: el CSIRT Italia, el Centro Nacional de Evaluación y Certificación (CVCN), el Centro de Coordinación Nacional (CCN), así como el Organismo de Certificación de la Seguridad Informática. Además, es el elemento central del Perímetro Nacional de Ciberseguridad (PSNC). "Estas competencias se atribuían anteriormente a una pluralidad de actores institucionales", se cita en su Estrategia de Ciberseguridad 2022-2026.

España, dentro del 'Top 20' en los principales a pesar de no contar con una agencia nacional

Disponer de una autoridad nacional de ciberseguridad, uno de los aspectos siempre valorados en los principales rankings mundiales

Conocer el 'poder cibernético' y la madurez de los diferentes países del mundo es el reto de diferentes análisis mundiales por parte de asociaciones, organizaciones públicas y *think tanks*. Datos que son de interés por lo que aportan en sus diferentes enfoques y que, en general, contemplan de forma positiva en su apartado que mide la gobernanza nacional el hecho de contar con autoridades de ciberprotección.

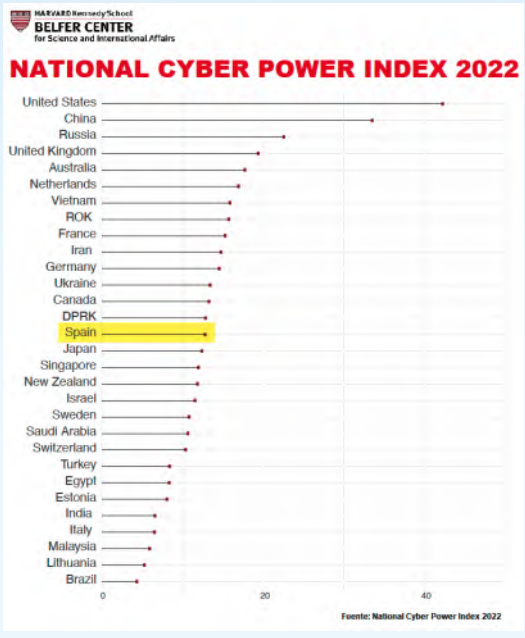
Así, entre los más conocidos está, sin duda, el Índice de Ciberseguridad Global (ICG) de la **Unión Internacional de Telecomunicaciones** (UIT), que comenzó a realizarse en 2007 y que, entre otros muchos aspectos (es el que más elementos valora, mucho más allá de la ciberseguridad, como el grado de conectividad de la población a Internet), puntúa la existencia de una agencia nacional responsable como parte del conjunto de "medidas institucionales" de naturaleza organizativa que promueve. De cualquier forma, su última edición, la cuarta, –al cierre de esta edición–, no ha sido actualizada desde 2020.

Otro de los rankings más valorados es el 'Índice Nacional de Ciberpoder' (NCPI), realizado por el **Centro Belfer para Ciencias y Asuntos Internacionales de la Escuela Kennedy de Harvard**, cuya última edición es de finales de 2022 –y la primera, de 2020– que muestra "una instantánea del estado actual" de las capacidades cibernéticas de 30 naciones -España queda la 15ª- a través de modelos de valoración, tanto cualitativos como cuantitativos, con más de 1.000 fuentes de datos existentes y con 29 indicadores que incluyen desde ataques cibernéticos atribuidos, estándares técnicos y de gobernanza, y que pretende ser el "mejor modelo holístico, hasta la fecha, para medir el poder cibernético". Por supuesto, uno de los aspectos más valorados es que el país cuente con una agencia nacional de ciberprotección, así como un ecosistema industrial notable.

En su última edición, los países con mayores capacidades cibernéticas son EE.UU., seguido de China, Rusia y Reino Unido -que pierde una posición respecto al análisis de 2020-. No obstante, el documento también advierte que los resultados pueden no ser totalmente concluyentes por cuanto "los países a menudo ocultan sus verdaderas capacidades cibernéticas, particularmente las capacidades destructivas, defensivas y de espionaje".

ITUPublications 2020

Nombre del país	Puntaje	Rango
Estados Unidos de América**	100	1
Reino Unido	99,54	2
Arabia Saudita	99,54	2
Estonia	99,48	3
Corea (República de)	98,52	4
Singapur	98,52	4
España	98,52	4
Federación Rusa	98.06	5
Emiratos Árabes Unidos	98.06	5
Malasia	98.06	5
Lituania	97,93	6
Japón	97,82	7
Canadá**	97,67	8
Francia	97,6	9
India	97,5	10
Pavo	97,49	11
Australia	97,47	12
Luxemburgo	97,41	13
Alemania	97,41	13
Portugal	97,32	14
Letonia	97,28	15
Países Bajos**	97.05	dieciséis
Noruega**	96,89	17
Mauricio	96,89	17
Brasil	96,6	18
Bélgica	96,25	19
Italia	96.13	20
Omán	96.04	21
Finlandia	95,78	22
Egipto	95,48	23
Indonesia	94,88	24
Vietnam	94,59	25
Suecia	94,55	26
Katar	94,5	27
Grecia	93,98	28
Austria	93,89	29
Polonia	93,86	30



Análisis 'en vivo'

También, destaca el Índice Nacional de Seguridad Cibernética (NCSI) que ofrece la **e-Governance Academy Foundation,** de Estonia, que busca medir "en vivo" la preparación de 39 países -aunque con la metodología anterior incluía 177-, para prevenir ciberamenazas y gestionar incidentes cibernéticos, así como su nivel de desarrollo digital. Precisamente, España es uno de los países que, con la nueva medición, ha desaparecido en el actual ranking -antes ocupaba el 10º lugar (ver imagen). En definitiva, pretende ser una "una base de datos con materiales de evidencia disponibles públicamente y una herramienta para el desarrollo de capacidades nacionales en seguridad cibernética". Por ello, está previsto que el equipo del NCSI también desarrolle en los próximos años diferentes aplicaciones para el análisis y desarrollo de la ciberseguridad a nivel nacional. Además, su enfoque de análisis del 'Desarrollo de Políticas de Ciberseguridad', también incluye como indicador la presencia de una autoridad nacional responsable en ciberprotección y un responsable de coordinación de la política sectorial.

Otro análisis de interés es el realizado por el **Instituto Internacional de Estudios Estratégicos** (IISS), que ha dado lugar a varios informes, bajo el título 'Capacidades cibernéticas y poder nacional: una evaluación neta', el primero de 2021, fruto de dos años de estudios y que aporta una "evaluación cualitativa del poder cibernético de 15 países –EE.UU., Reino Unido, Canadá, Australia, Francia, Israel, Japón, China, Rusia, etc.- clasificándolo en tres niveles. Curiosamente, sólo EE.UU. ocupó el primero. En 2023 volvió a realizar un estudio con 10 países más - Brasil, Estonia, Alemania, Países Bajos, Nigeria...-, sin considerar que ninguno se merece ese primer nivel, siendo los mejor valorados son Alemania y Países Bajos.

Entre los peor valorados, en el tercer nivel, están Brasil, Estonia, Nigeria, Arabia Saudita, Singapur, Sudáfrica, Turquía y los Emiratos Árabes Unidos, ya que, aunque tienen "fortalezas o fortalezas potenciales en algunas de las categorías", también presentan "debilidades significativas en otras".

HORA...

DE AFINAR

La UE y Europa perfilan su futuro

A instancias de SIC, diversos países de la Unión Europa y alguno más del continente se han avenido amablemente a responder –a través de la portavocía que en cada caso procediera o fuera viable–, a algunas preguntas formuladas para conocer, sucintamente, sus respectivas casuísticas de conformación de su gobernanza en la materia, sus hitos en ciberprotección más reseñables, así como el estado de situación de la aplicación de la directiva NIS2 que sobreviene. Sus inestimables aportaciones arrojan no poca luz sobre el grado de dificultad de la consolidación de la gobernanza y sobre qué senderos tomar.

OFICINA FEDERAL ALEMANA DE SEGURIDAD DE LA INFORMACIÓN (BSI)

ALEMANIA

FABIENNE TEGELER
Jefa de la Sección de Gestión de Clientes y Asuntos Jurídicos de la Oficina Federal Alemana de Seguridad de la Información (**BSI**)
Presidenta del Consejo de Administración de **ENISA**

– ¿Cuál es la característica principal que debe definir el desempeño de una agencia o autoridad nacional de ciberseguridad: gobernanza, gestión, control o supervisión? ¿Debería disponer de su propio presupuesto para llevarlo a cabo?

– Una agencia nacional de ciberseguridad debe tener experiencia técnica en los diferentes aspectos de la ciberseguridad, incluidas capacidades operativas internas (por ejemplo, un equipo nacional de respuesta a emergencias informáticas) y contar con su propio presupuesto.

– En la historia de la entidad a la que pertenece, ¿cuál ha sido el hito más importante que ha destacado y justificado su creación y asignación de capacidades y responsabilidades?

-Siempre que a BSI se le encomendaron medidas o tareas para mejorar eficazmente el nivel de ciberseguridad en el gobierno y la industria alemana (por ejemplo, la Ley de Seguridad de TI 2.0), estos fueron hitos importantes para BSI. A nivel técnico, cada vez que las medidas para reaccionar ante las amenazas cibernéticas tienen éxito, esto constituye un hito para BSI (por ejemplo, las contribuciones de BSI a la eliminación de infraestructuras de *botnets*).

– España está considerando el diseño de un nuevo modelo de gobernanza nacional en ciberseguridad. Según su experiencia, ¿cuál es el error a evitar al crear y asignar responsabilidades a una agencia o autoridad nacional de esta naturaleza?

– En general, las agencias de seguridad cibernética deben tener un mandato central y preciso, evitando posibles duplicaciones o competencia entre entidades gubernamentales, y actuar técnicamente de manera independiente. Los principales desafíos son los conflictos de intereses y las tareas y competencias redundantes en el ecosistema de las instituciones gubernamentales.

– ¿Cuál es el estado de la trasposición de la directiva NIS2 en su país?

-La implementación de la NIS2 es un tremendo desafío para los Estados miembros de la UE. BSI apoya al Ministerio Federal del Interior y de la Comunidad en sus esfuerzos por implementarla a nivel nacional.

CENTRO EUROPEO DE COMPETENCIA EN CIBERSEGURIDAD (ECCC)

LUCA TAGLIARETTI
Director Ejecutivo
ECCC

– En una entrevista en SIC, Lorena Boix, directora en la DG CONNECT de la Comisión Europea, destacó que "Es fundamental que cada país disponga de una autoridad nacional a cargo de la supervisión y el cumplimiento de las obligaciones de ciberseguridad derivadas de la NIS". ¿Existe alguna Agencia Nacional que considere que sería el modelo a seguir? Pocos países tienen una con plenas capacidades...

– Comparto su opinión de abogar por que las autoridades nacionales centrales se encarguen de garantizar que las obligaciones de NIS (y ahora NIS2) se apliquen de forma coherente. Esto será, simplemente, establecer la coordinación a nivel nacional. Tenemos que esforzarnos por conseguirlo, aunque aún debemos reconocer que no siempre es posible debido a la naturaleza amplia y horizontal de la Directiva NIS y al hecho de que los avances nacionales se producen a diferentes ritmos.

Volviendo a su pregunta, es difícil señalar un ejemplo específico de una autoridad nacional, dadas las diferencias que existen en términos de capacidad nacional, pero espero que, con el crecimiento en importancia de las diferentes agencias cibernéticas nacionales, pronto tomarán reforzar la función de coordinación para la implementación de la NIS2 y el control del cumplimiento.

CENTRO DE CIBERSEGURIDAD (CCB)

BÉLGICA

MIGUEL DE BRUYCKER
Director General

– ¿Cuál es la característica principal que debe definir el desempeño de una agencia o autoridad nacional de ciberseguridad: gobernanza, gestión, control o supervisión? ¿Debería disponer de su propio presupuesto para llevarlo a cabo?

– Gobernanza y sí, contar con un presupuesto propio.

– En la historia de la entidad a la que pertenece, ¿cuál ha sido el hito más importante que ha destacado y justificado su creación y asignación de capacidades y responsabilidades?

– Llevar a Bélgica a la cima en múltiples índices de ciberseguridad nos ha dado alas y presupuesto.

– España está considerando el diseño de un nuevo modelo de gobernanza nacional en ciberseguridad. Según su experiencia, ¿cuál es el error a evitar al crear y asignar responsabilidades a una agencia o autoridad nacional de esta naturaleza?

– Vincularla a servicios de Defensa o de Inteligencia.

– ¿Cuál es el estado de la transposición de la directiva NIS2 su país?

– Pasó por el parlamento a finales de marzo. Así que queda poco más de un mes más de trabajo pero se puede considerar completamente aprobada.

AGENCIA NACIONAL DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN (NÚKIB)

CHEQUIA

LUKÁŠ KINTR
Director
NÚKIB

– Dado su perfil, ¿cuál es la característica principal que debe definir el desempeño de una agencia o autoridad nacional de ciberseguridad: gobernanza, gestión, control o supervisión? ¿Debería disponer de su propio presupuesto para llevarlo a cabo?
– La Agencia Nacional de Seguridad Cibernética y de la Información (NÚKIB) es el organismo administrativo central para la seguridad cibernética de la República Checa y la protección de la información clasificada. NÚKIB también es responsable de la implementación del servicio público regulado en el marco del programa Galileo.
El Parlamento de la República Checa aprueba el presupuesto de NÚKIB como parte del presupuesto estatal. Para el año 2024, el presupuesto de NÚKIB fue fijado por el Parlamento en 610 millones de coronas checas (aprox. 24 millones de euros). NÚKIB se establece directamente bajo el gobierno y está sujeto al control parlamentario.
– En la historia de la entidad a la que pertenece, ¿cuál ha sido el hito más importante que ha destacado y justificado su creación y asignación de capacidades y responsabilidades?
– El motivo de la creación de NÚKIB fue la creciente importancia de proteger el ciberespacio de la República Checa y la necesidad de construir una institución especializada que cubriera las áreas mencionadas anteriormente y proporcionara las condiciones adecuadas para el cumplimiento de las agendas necesarias.
– España está considerando el diseño de un nuevo modelo de gobernanza nacional en ciberseguridad. Según su experiencia, ¿cuál es el error a evitar al crear y asignar responsabilidades a una agencia o autoridad nacional de esta naturaleza?
– Para NÚKIB desde el principio ha sido beneficioso que en la República Checa exista una ley escrita de calidad sobre ciberseguridad. Cuando se redactó la ley, se pensó, entre otras cosas, que la ciberseguridad no es sólo una disciplina puramente técnica de TI, sino que también son importantes las actividades políticas, la educación, la cooperación jurídica internacional, etc. Por lo tanto, recomendamos que se establezca bien la legislación.
– ¿Cuál es el estado de la trasposición de la directiva NIS2 en su país?
– NÚKIB ha preparado una nueva ley sobre ciberseguridad que, entre otras cosas, transpone la Directiva NIS2 a la legislación checa.
Es probable que la ley entre en vigor a partir del 1 de enero de 2025. También publicamos un informe anual sobre el estado de la ciberseguridad en la República Checa con datos, principalmente, de entidades reguladas por la Ley de Ciberseguridad.

AUTORIDAD NACIONAL DE SEGURIDAD

ESLOVAQUIA

ROMAN KONEČNÝ
Director

– ¿Cuál es la característica principal que debe definir el desempeño de una agencia o autoridad nacional de ciberseguridad: gobernanza, gestión, control o supervisión? ¿Debería de disponer de su propio presupuesto para llevarlo a cabo?
– Se podría comparar con una receta culinaria. Una agencia funcional siempre debe ser una combinación de una gran parte de independencia de la política con una buena combinación de expertos dedicados y trabajadores en la gerencia media y alta. Todo esto debe combinarse con requisitos legales claros para las entidades reguladas con un nivel adecuado de control.
– En la historia de la Autoridad de Seguridad Nacional, ¿cuál ha sido el hito más importante que ha destacado y justificado su creación y asignación de capacidades y responsabilidades?
– Un acontecimiento clave fue la adopción de la Ley de Ciberseguridad en 2018. Sin ella, no habríamos podido crear un sistema de ciberseguridad funcional en Eslovaquia y no habría estado claro quién y en qué medida debería contribuir en este complejo rompecabezas.
– España está considerando el diseño de un nuevo modelo de gobernanza nacional en ciberseguridad. Según su experiencia, ¿cuál es el error a evitar al crear y asignar responsabilidades a una agencia o autoridad nacional de ciberprotección?
– En este caso no hablaría tanto de errores sino de recomendaciones. Ciertamente, no subestime el aspecto financiero: calcule los costes tanto de las operaciones, como de las actualizaciones o innovaciones. Es necesario definir claramente los poderes legislativos y los órganos reguladores. Por último, pero no menos importante, un plan (a corto, medio y largo plazo) es sumamente esencial. Al final del día, necesita ver cómo está creciendo su organización, dónde tiene sus reservas y cómo está cumpliendo sus objetivos.
– ¿Cuál es el estado de la transposición de la directiva NIS2 en su país?
– La Autoridad Nacional de Seguridad está trabajando arduamente para modificar la Ley de Ciberseguridad con varios elementos nuevos de NIS2. En el pasado, Eslovaquia ha seguido estrictamente la Directiva NIS, por lo que tenemos una posición inicial un poco más fácil con respecto a la modificación de la Ley de Ciberseguridad mencionada anteriormente con respecto a NIS2. Esperamos cambios alrededor del verano.

OFICINA DE SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO (URSIV)

ESLOVENIA

– ¿Cuál es la característica principal que debe definir el desempeño de una agencia o autoridad nacional de ciberseguridad: gobernanza, gestión, control o supervisión? ¿Debería disponer de su propio presupuesto para llevarlo a cabo?

– La idea detrás de una agencia nacional de ciberseguridad es la centralización jerárquica de los esfuerzos de ciberseguridad en un estado. A lo largo de las últimas dos décadas hemos visto que uno tiene dificultades para brindar seguridad en el espacio digital si esos esfuerzos se dispersan. Sin embargo, una mayor centralización no significa usurpar todas las tareas y acciones de ciberseguridad. Lo que representa es una coordinación sistémica jerárquica de responsabilidades y tareas que deben ser realizadas por múltiples partes interesadas en múltiples niveles y puntos en una variedad de redes. Una organización coordinadora de este tipo puede desempeñar sus tareas de manera efectiva y exitosa si está estructuralmente ubicada de manera adecuada dentro de una burocracia y si cuenta con el apoyo de recursos financieros suficientes.

– En la historia de la URSIV, ¿cuál ha sido el hito más importante que ha destacado y justificado su creación y asignación de capacidades y responsabilidades?

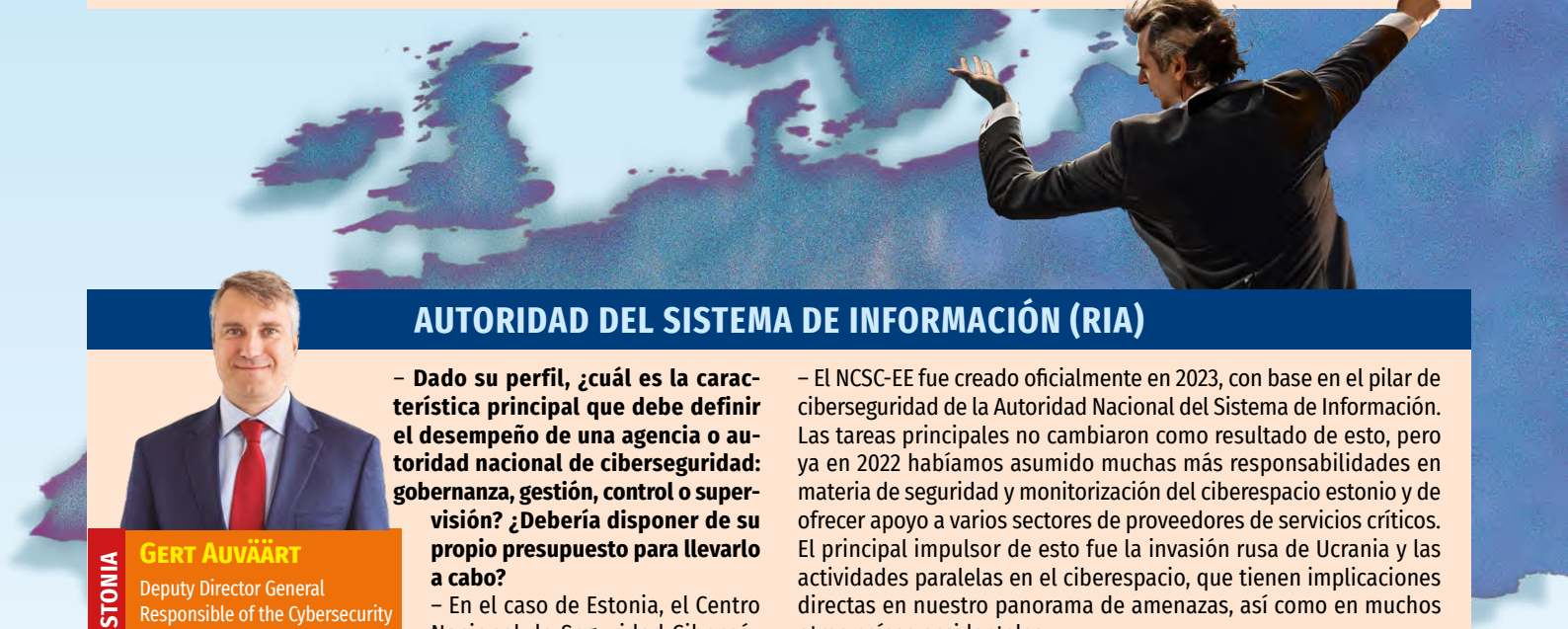
– El primer gran paso fue, por supuesto, la creación de URSIV en 2019 tras la adopción de la Ley de Seguridad de la Información en 2018. En aquel entonces, URSIV formaba parte del Ministerio de Administraciones Públicas, que era responsable de la cartera de Digitalización y Seguridad de la Información. Rápidamente se hizo evidente que, debido a la naturaleza de la ciberseguridad, la agencia recién creada necesitaba ser reposicionada para que pudiera realizar con éxito sus tareas de coordinación horizontal e interinstitucional. Esto ocurrió en 2021, cuando URSIV se posicionó como una agencia gubernamental responsable directamente ante el Primer Ministro.

– España está considerando el diseño de un nuevo modelo de gobernanza nacional en ciberseguridad. Según su experiencia, ¿cuál es el error a evitar al crear y asignar responsabilidades a una agencia o autoridad nacional de ciberseguridad?

– No nos dedicamos a asesorar a otras naciones soberanas. Lo que funciona en Eslovenia puede no ser apropiado para España y viceversa.

– ¿Cuál es el estado de la transposición de la directiva NIS2 en su país?

– Transpondremos NIS2 con una nueva Ley de Seguridad de la Información, cuyo borrador se encuentra en etapa de consulta pública y está previsto que se adopte hasta el momento designado en el otoño.



AUTORIDAD DEL SISTEMA DE INFORMACIÓN (RIA)

ESTONIA

GERT AUVÄÄRT
Deputy Director General
Responsible of the Cybersecurity in RIA

– Dado su perfil, ¿cuál es la característica principal que debe definir el desempeño de una agencia o autoridad nacional de ciberseguridad: gobernanza, gestión, control o supervisión? ¿Debería disponer de su propio presupuesto para llevarlo a cabo?

– En el caso de Estonia, el Centro Nacional de Seguridad Cibernética (NCSC-EE) es parte de una organización más grande: la Autoridad Nacional del Sistema de Información (NISA). El NCSC-EE es el pilar que alberga el equipo nacional de respuesta a incidentes (CERT-EE) y también desarrolla el estándar nacional de seguridad de la información, supervisa su implementación dentro del sector público y los proveedores de servicios esenciales, supervisa la protección de la infraestructura crítica y analiza el sistema estonio, el panorama de amenazas cibernéticas y planificación de campañas de concientización relacionadas con la cibernética dentro de la sociedad. Una parte del presupuesto de NISA se asigna al NCSC-EE para llevar a cabo sus tareas.

– En la historia de la entidad que dirige, ¿cuál ha sido el hito más importante que ha destacado y justificado su creación y asignación de capacidades y responsabilidades?

– El NCSC-EE fue creado oficialmente en 2023, con base en el pilar de ciberseguridad de la Autoridad Nacional del Sistema de Información. Las tareas principales no cambiaron como resultado de esto, pero ya en 2022 habíamos asumido muchas más responsabilidades en materia de seguridad y monitorización del ciberespacio estonio y de ofrecer apoyo a varios sectores de proveedores de servicios críticos. El principal impulsor de esto fue la invasión rusa de Ucrania y las actividades paralelas en el ciberespacio, que tienen implicaciones directas en nuestro panorama de amenazas, así como en muchos otros países occidentales.

– España está considerando el diseño de un nuevo modelo de gobernanza nacional en ciberseguridad. Según su experiencia, ¿cuál es el error a evitar al crear y asignar responsabilidades a una agencia o autoridad nacional de ciberseguridad?

– Creo que el error que se debe evitar es tener responsabilidades superpuestas o poco claras, por ejemplo, si la autoridad también participa o no en la formulación de políticas. Además, la ciberseguridad es un ámbito que afecta a todas las agencias, por lo que vale la pena considerar si la agencia nacional de ciberseguridad debería depender de la oficina del primer ministro, en lugar de cualquier ministerio.

– ¿Cuál es el estado de transposición de la directiva NIS2 en su país?

– En Estonia, el Ministerio de Asuntos Económicos y Comunicaciones es responsable de la implementación de la directiva NIS2 y todavía es un proceso en curso.

CENTRO NACIONAL DE SEGURIDAD CIBERNÉTICA (NCSC-IE)

IRLANDA

DARRAGH MCSWEENEY
Cyber Security Responder at National Cyber Security Centre, Ireland (**NCSC-IE**)

– Dado su perfil, ¿cuál es la característica principal que debe definir el desempeño de una agencia o autoridad nacional de ciberseguridad: gobernanza, gestión, control o supervisión? ¿Debería disponer de su propio presupuesto para llevarlo a cabo?
– No existe ningún elemento que defina o deba definir una agencia nacional de ciberseguridad en su conjunto. Recientemente hicimos una revisión de nuestra estrategia nacional de seguridad cibernética para evaluar el progreso y considerar nuevas iniciativas para garantizar el cumplimiento de todas las medidas descritas en ella. Las 18 nuevas acciones estratégicas abarcan las siete áreas temáticas de enfoque de la Estrategia, que incluyen, entre otras:

- Protección de la infraestructura nacional crítica: Desarrollar más redes sectoriales de intercambio de información con operadores relevantes de infraestructura nacional crítica y sectores industriales importantes, incluidos los sectores de infraestructura digital y energía.
- Habilidades: Facilitar el desarrollo continuo de un repositorio centralizado de cursos educativos y de aprendizaje en ciberseguridad en todos los niveles y en todo el país, y utilizar estos datos para desarrollar materiales para escuelas, orientadores y otros para crear conciencia sobre las carreras en ciberseguridad y aprendizaje.
- Desarrollo empresarial: implementar un programa de apoyo financiero para las pymes y otras partes interesadas de la sociedad, de conformidad con las disposiciones de la UE, para mejorar la resiliencia de la ciberseguridad y facilitar la innovación.
- Ciudadanos: Desarrollar y publicar con mayor frecuencia documentos de asesoramiento y orientación personalizados sobre las medidas que pueden tomar los ciudadanos, las pymes, las escuelas e instituciones educativas, y las organizaciones comunitarias y voluntarias para prevenir y mitigar los riesgos de seguridad cibernética.

Creemos que es fundamental no centrarse demasiado en un área, sino mejorar las medidas de protección que tenemos en todo el país.

– En la historia de su entidad, ¿cuál ha sido el hito más importante que ha destacado y justificado su creación y asignación de capacidades y responsabilidades?
– La primera Estrategia Nacional de Seguridad Cibernética de Irlanda fue acordada por el Gobierno y publicada en julio de 2015. Estableció una hoja de ruta para el desarrollo del NCSC y una serie de medidas para proteger mejor los datos y las redes del Gobierno, así como la infraestructura nacional crítica. En este período transcurrido desde entonces, el NCSC ha crecido significativamente en escala y capacidad, y se ha introducido la primera Directiva de seguridad de la información y las redes. Desde entonces, el fortalecimiento del NCSC ha sido un componente clave de la Estrategia Nacional de Seguridad Cibernética y un hito importante fue el acuerdo por parte del Gobierno en 2021 de una ampliación significativa de la dotación de personal y los recursos del NCSC, que desde entonces ha progresado significativamente. Se está desarrollando una instalación central exclusiva para el NCSC como parte de la nueva instalación central del Departamento de Medio Ambiente, Clima y Comunicaciones en Dublín.

– España está considerando el diseño de un nuevo modelo de gobernanza nacional en ciberseguridad. Según su experiencia, ¿cuál es el error a evitar al crear y asignar responsabilidades a una agencia o autoridad nacional de ciberseguridad?
– Como ya mencioné, la actual Estrategia Nacional de Seguridad Cibernética, que se publicó en 2019, es una estrategia gubernamental de cinco años de duración destinada a mejorar la seguridad y la resiliencia de los sistemas gubernamentales y la infraestructura nacional crítica. La Estrategia establece una serie de medidas de colaboración para mejorar la ciberseguridad y la resiliencia de los organismos públicos, los proveedores de servicios esenciales, las empresas y los hogares, para apoyar el desarrollo continuo de la industria de la ciberseguridad y la comunidad de investigación, y para garantizar que Irlanda desempeñe un papel importante en los debates internacionales sobre la seguridad y la estabilidad de un ciberespacio libre y abierto. Creemos que, al delinear todos nuestros objetivos dentro de esta estrategia, dar plazos claros sobre cuándo nos esforzamos por alcanzar esos objetivos y obtener el respaldo y el compromiso del gobierno fue esencial para el éxito que hemos tenido desde el lanzamiento de esa estrategia con respecto a la aumentar la resiliencia cibernética y las capacidades del país en su conjunto.

– ¿Cuál es el estado de transposición de la directiva NIS2 en su país?
– Se ha iniciado la elaboración de un esquema general, que será considerado por el Gobierno, de cara a cumplir el plazo de transposición del 17 de octubre de 2024.

CENTRO NACIONAL DE CIBERSEGURIDAD (NCSC)

SUIZA

FLORIAN SCHÜTZ
Director of the Swiss NCSC

– Dado su perfil, ¿cuál es la característica principal que debe definir el desempeño de una agencia o autoridad nacional de ciberseguridad: gobernanza, gestión, control o supervisión? ¿Debería disponer de su propio presupuesto para llevarlo a cabo?
– El Centro Nacional Suizo de Ciberseguridad (NCSC) se centra en la gobernanza y la gestión. El control y la supervisión son actividades clave de los reguladores. Dado su papel, la industria, los ciudadanos y el sector público confían en el NCSC suizo. Esto le permite no sólo ayudar, sino también generar recomendaciones de seguridad aplicables que, por otra parte, los reguladores pueden utilizar si es necesario. El NCSC tiene un presupuesto propio.

– En la historia de la entidad que dirige, ¿cuál ha sido el hito más importante que ha destacado y justificado su creación y asignación de capacidades y responsabilidades?
– El hito más importante fue la segunda versión de la Ciberestrategia Nacional Suiza (NCS), que por primera vez incluyó en una estrategia conjunta las fuerzas del orden, la inteligencia, la ciberseguridad militar y civil. La implementación de esta estrategia requirió una coordinación central de las diferentes entidades responsables de su parte, lo que fue el punto de partida para la discusión sobre la mejor estructura y responsabilidad para dicha entidad.

– España está considerando el diseño de un nuevo modelo de gobernanza nacional en ciberseguridad. Según su experiencia, ¿cuál es el error a evitar al crear y asignar responsabilidades a una agencia o autoridad nacional de ciberseguridad?
– En mi opinión, el mayor error sería pensar que una Agencia Nacional de Seguridad Cibernética puede proteger al país de forma independiente. La responsabilidad de la ciberseguridad se reparte entre diferentes actores del gobierno, la industria y la sociedad civil. Además, centrarse únicamente en la respuesta a incidentes sería un gran error. Una entidad nacional debe impulsar el aumento de la seguridad en todo el país considerando cuidadosamente el impacto potencial en el producto interior bruto.

– ¿Qué opina de la directiva NIS2?
– Suiza no es miembro de la UE y, por tanto, no se aplica la directiva NIS2. Sin embargo, el parlamento suizo aprobó recientemente una ley para la obligación de informar de ataques cibernéticos a infraestructuras críticas, que es compatible con las obligaciones de informar de incidentes en la legislación de la UE. Actualmente estamos trabajando en la ordenanza antes de que la ley entre en vigor, probablemente a principios del próximo año.

(Ciber)seguridad Nacional española

La cuestión: ¿instaurar una dirección operativa o afinar en la coordinación de lo existente?

La obligación de trasponer a nuestra legislación la Directiva NIS2, la Directiva relativa a la resiliencia de las entidades críticas y el cada vez más cercano cumplimiento efectivo de la ley DORA (resiliencia operativa para el sector financiero), han recrudecido en España el debate sobre cómo mejorar la actual organización de la ciberseguridad (principalmente civil) en el marco de la Seguridad Nacional.

No está resultando sencillo mantenerla en estructuras ya prexistentes (que es lo que se ha hecho hasta ahora) y menos todavía estabilizar un modelo específico para su llevanza, que por su alcance multidimensional e impacto en todo frente merece tener.

Así, nos encontramos con ideas encontradas entre los actores acerca de cómo debería llevarse la gestión de la ciberseguridad, de dónde debería ir dependiendo, si habría que crear una agencia o un centro coordinador, sus implicaciones con la seguridad privada clásica, la forma de mensurar el esfuerzo presupuestario estatal en la materia y la forma de aplicarlo, el apoyo a la industria y el fomento de la cultura...

Para mayor abundamiento, la vigente estrategia Nacional de Ciberseguridad, documento gubernamental que data de 2019, pide ya una revisión, que debe de partir de lo conseguido en estos cinco años, de lo aprendido y de lo que se nos viene encima con las iniciativas legales europeas y de otras partes del mundo a pleno gas, que amenazan con una sobrecarga de requisitorias de cumplimiento cruzado que pudiera dificultar, en algún momento, las acciones encaminadas a la gestión efectiva de los riesgos de ciberseguridad.

Ante esta circunstancia, SIC ha intentado pulsar la opinión de los principales actores de la (ciber) seguridad nacional: CCN, DSN, INCIBE, MAEC, MCCE y OCC (SES) formulándoles una única pregunta; la siguiente:

"**¿Qué ventajas comportaría –frente a la situación actual– crear una entidad administrativa de ciberseguridad con personalidad jurídica propia, que centralice competencias y recursos?**".

De estas seis entidades mencionadas, han considerado procedente contestar dos (hecho del que no debe deducirse que las que han desestimado responder no tengan una idea formada al respecto), el Centro Criptológico Nacional (CCN) y el Instituto Nacional de Ciberseguridad (INCIBE), por boca de sus responsables.

Sus opiniones, en calidad de gestores expertos de primer nivel en la materia, no es que sean poco coincidentes, sino que están, a todas luces, enfrentadas.

LA REFLEXIÓN DEL CCN

Luis Jiménez
Subdirector General
Centro Criptológico Nacional – CCN

"La gobernanza de la ciberseguridad en España se ha venido articulando a través de la arquitectura esbozada en el Sistema de Seguridad Nacional, arrancando, a nivel estratégico, en el Consejo de Seguridad Nacional (Consejo Nacional de Ciberseguridad) y concluyendo, a nivel táctico, en los denominados CSIRT de referencia.

Sin embargo, teniendo en cuenta que la ciberseguridad es una manifestación de la seguridad nacional –como así ha declarado el Tribunal Constitucional–, y pese a los beneficios derivados de la antedicha arquitectura, esbozada ya en la Estrategia Nacional de Ciberseguridad de 2013 y consolidada en la de 2019, la ausencia de una entidad nacional de ciberseguridad que lidere el nivel operativo provoca que el actual modelo resulte a todas luces insuficiente –y, en muchas ocasiones, ineficaz–, debiendo mejorarse, por las siguientes razones principales:

1. Se carece de una dirección operativa nacional de la ciberseguridad.
2. Se carece del imprescindible análisis del ecosistema de la ciberseguridad, comprensivo de todos los actores implicados: sector público, privado y ciudadanos.
3. Dispersión de la respuesta ante las amenazas y de los procedimientos de prevención, detección y respuesta.
4. Limitado intercambio de información.
5. Ausencia de métodos, procedimientos y herramientas comunes.
6. Debilidad en la defensa de los intereses de España.
7. Ineficacia en la asignación y gestión de los fondos públicos.

Una entidad como la que se menciona, a la que podríamos denominar Centro de Ciberseguridad Nacional, atendiendo a las directrices estratégicas del Consejo de Seguridad Nacional (Consejo Nacional de Ciberseguridad), y encuadrada orgánicamente en el departamento Ministerial adecuado –que, por motivos obvios, no debería coincidir con aquel que lidere la trasformación digital de nuestro país–, constituiría el punto focal de dirección operativa y coordinación de los esfuerzos para proteger el ciberespacio de España, puesto que tendría las siguientes funciones de primer nivel:

- Asumir la responsabilidad de constituir el punto focal de la ciberseguridad de España, desde el punto de vista operativo y de coordinación metodológica, jurídica, tecnológica, de investigación y de formación, ostentado el papel de Autoridad Nacional Operativa en materia de Ciberseguridad, Ciberinteligencia y Ciberdefensa.
- Determinar los mecanismos para materializar las directrices estratégicas establecidas por la Estrategia Nacional de Ciberseguridad y posibilitar la implantación de las actividades comprendidas en sus Líneas de Acción, en el ámbito de sus competencias.
- Proporcionar la capacidad nacional de dirección operativa y de coordinación frente a los incidentes provocados por los ciberataques de que puedan ser objeto los sistemas de información de las entidades de los sectores público, privado y ciudadanos (comunidad de ciberseguridad), a través de las diferentes Autoridades Competentes y CSIRT de referencia establecidos por la legislación vigente.
- Proporcionar a la comunidad de ciberseguridad el asesoramiento metodológico, jurídico, operativo y tecnológico para la gestión de programas de ciberseguridad.
- Trabajar con otras entidades, nacionales, e internacionales, organismos públicos y asociaciones, especialmente de la Unión Europea y de los países y organizaciones occidentales, civiles y militares, en el análisis de amenazas y vulnerabilidades, contribuyendo al desarrollo de mecanismos de protección, detección y respuesta adecuados.
- En su calidad de Autoridad Nacional Operativa en materia de ciberseguridad, participar en programas internacionales de la alerta temprana y cooperación, en representación de España, sin perjuicio de las competencias legalmente atribuidas a los departamentos ministeriales competentes.
- Atendiendo a las directrices del Consejo de Seguridad Nacional (Consejo Nacional de Ciberseguridad), liderar una I+D+i propia y en cooperación con otras agencias e instituciones, públicas y privadas, con el objetivo de desarrollar una nueva generación de tecnologías para la ciberseguridad.
- Dirección de la investigación de los riesgos de seguridad, de las medidas preventivas, detectivas y de respuesta, realización de pruebas y ejercicios, etc.
- Dirección de la cooperación con la industria en materia de productos y servicios de ciberseguridad.
- Dirección de la implantación de los esquemas de certificación de la seguridad de aplicación en España, así como, en su caso, del desarrollo de nuevos esquemas particulares o sectoriales.
- Participación en la elaboración de los medios de formación y sensibilización en materia de ciberseguridad, ciberinteligencia y ciberdefensa.

Como es fácil deducir, los beneficios derivados de la constitución de una entidad como la citada serían, entre otros, los siguientes:

- Mejora sustancial de la ciberseguridad y la resiliencia de los sistemas de información (públicos y privados) de España, en sus vertientes de prevención, detección, vigilancia, respuesta y disuasión.
- Optimización de los recursos económicos destinados a ciberseguridad.
- Mejora la posición internacional de España en materia de ciberseguridad.
- Coadyuvar en las responsabilidades de dirección estratégica del Consejo de Seguridad Nacional (Consejo Nacional de Ciberseguridad).
- Facilita la gobernabilidad de España en materia de ciberseguridad.
- Supervisar, desde el punto de vista de la (ciber)seguridad, las iniciativas de Transformación Digital del Estado.
- Sin que suponga un impacto legislativo significativo".

"Una entidad, a la que podríamos denominar Centro de Ciberseguridad Nacional, atendiendo a las directrices del Consejo de Seguridad Nacional (Consejo Nacional de Ciberseguridad), y encuadrada orgánicamente en el departamento Ministerial adecuado –que, por motivos obvios, no debería coincidir con aquel que lidere la trasformación digital de nuestro país–, constituiría el punto focal de dirección operativa y coordinación de los esfuerzos para proteger el ciberespacio de España".

LA REFLEXIÓN DE INCIBE

Félix Barrio
Director General
Instituto Nacional de Ciberseguridad INCIBE

"El planteamiento de centralización de competencias y recursos no presenta ventajas si atendemos a la complejidad del problema que tratamos de gestionar, y cómo cada autoridad o centro de respuesta realiza funciones complementarias a la vez que altamente especializadas.

En España las autoridades competentes son designadas por el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y van desde la Secretaría de Estado de Transportes hasta el Consejo de Seguridad Nuclear. En cuanto a los centros de respuesta a incidentes y crisis cibernéticas (CSIRT), el artículo 11.1 de Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, establece que son CSIRT de referencia en materia de seguridad de las redes y sistemas de información, el CCN-CERT para entidades del sector público y el INCIBE-CERT para las entidades del sector privado, con la cooperación del ESPDEF-CERT del Ministerio de Defensa, en situaciones y operadores que tengan incidencia en la Defensa Nacional.

Las competencias de las Autoridades competentes están reguladas en el artículo 10 del Real Decreto Ley 12/2018 y van más allá de la gestión de incidentes o crisis, debiendo regular, sancionar, adoptar estrategias y medidas de actuación en prevención y respuesta ante incidentes, en cooperación con los centros de respuesta.

"Lo que necesitamos es armonizar y coordinar la dispersa y abundante normativa de ciberseguridad bajo el paraguas de una Ley integral de ciberseguridad que, bajo el liderazgo de todo un Ministerio de Transformación Digital, puede impulsar mejoras en materia de coordinación, anticipación de necesidades regulatorias y de servicio público, y optimizar unos recursos públicos y privados que necesitan continuar siendo impulsados, con la participación, eso sí, de todas las autoridades gubernamentales implicadas".

La tentación de centralizar autoridades y centros de respuesta en un mando único, bajo la fórmula de agencia gubernamental o similar, nos situaría ante un escenario en el que la toma de decisiones puede crecer en complejidad, por más que se simplifique la toma de decisiones en una única institución, resultando improbable sustituir el preciso conocimiento o experiencia de las necesidades tanto de recursos como reglamentarias, la propia operativa o las condiciones de gestión de incidentes en ciberseguridad que tiene cada autoridad.

Un ejemplo claro de que concentrar autoridad puede dificultar la resolución de un problema complejo desde el punto de vista técnico como es el de la ciberseguridad, lo hemos visto recientemente cuando se adoptó por parte de un magistrado de la Audiencia Nacional el bloqueo de una red social como Telegram, en el curso de una investigación relativa a propiedad intelectual y derechos audiovisuales relacionados con el ocio electrónico, sin tener en cuenta que dicha herramienta era utilizada por numerosas organizaciones y colectivos como sistema de mensajería preferente, de diversos sectores, debiendo levantar la orden de bloqueo a raíz de las consecuencias no previstas de la medida.

Esta consideración a la complejidad técnica del problema de la ciberseguridad es también aplicable al debate sobre la conveniencia de agencias autonómicas que pueden monitorizar y resolver las necesidades de configuración, adecuación o intervención en activos informáticos, tales como computadoras, dispositivos móviles, servidores, portales de servicios web, bases de datos, aplicaciones de software, distribuidos por decenas de miles entre nuestros miles de centros hospitalarios y de salud, centros escolares, ayuntamientos, administraciones de ámbito autonómico y un enorme etcétera. Probablemente sean los departamentos de Tecnologías de la Información autonómicos y en algunos casos sus departamentos o agencias regionales los que puedan tener una mayor capacidad para coordinar las inversiones, formación técnica, despliegue de medidas de ciberseguridad en esa amplísima red, bajo una coordinación con las autoridades nacionales en materia de reporte y respuesta a incidentes, que encomendar a una macro autoridad nacional la gestión estratégica, de monitorización y de soporte a tan inmensa y heterogénea red de activos informáticos y de comunicaciones.

Lo que necesitamos en España es armonizar y coordinar la dispersa y abundante normativa de ciberseguridad bajo el paraguas de una Ley integral de ciberseguridad que, bajo el liderazgo de todo un Ministerio de Transformación Digital, puede impulsar mejoras en materia de coordinación, anticipación de necesidades regulatorias y de servicio público, y optimizar unos recursos públicos y privados que necesitan continuar siendo impulsados, con la participación, eso sí, de todas las autoridades gubernamentales implicadas en el compromiso hacia la ciberseguridad".

Retos en la seguridad y confiabilidad en la IA

Mirando hacia el futuro, existen múltiples razones para ser optimistas sobre el papel que la IA puede jugar como una fuerza positiva en la sociedad. Sin embargo, este futuro no está garantizado, requiere un compromiso consciente con la ética y la seguridad en cada paso del desarrollo tecnológico. Por ello, es preciso equilibrar la innovación con la responsabilidad social. En las siguientes páginas dos expertos reflexionan sobre estas tecnologías en asuntos como las requisitorias normativa y legislativa, enfoques confiables y controles a aplicar.

Irene Yusta / Antonio Requena

La revolución de la Inteligencia Artificial (IA) está reconfigurando el panorama global en múltiples sectores, desde la salud y la educación hasta la industria y la seguridad. A medida que la IA se integra cada vez más en la vida cotidiana, surge la necesidad imperativa de establecer marcos legislativos que no solo fomenten la innovación sino que también garanticen el uso ético y responsable de estas tecnologías. En este contexto, diversas iniciativas globales están emergiendo, pero es la Unión Europea (UE) la que destaca como pionera con su Reglamento de IA (IA Act), aprobado recientemente por el Parlamento.

El IA Act es un intento ambicioso de regular los sistemas de IA, estableciendo un marco para la gobernanza ética y segura de la tecnología en sus estados miembros. La propuesta clasifica las aplicaciones de IA según su nivel de riesgo, desde inaceptable hasta de bajo riesgo, y establece requisitos y restricciones específicas para cada categoría. Esto incluye la transparencia en el funcionamiento de los sistemas de IA, la adecuada supervisión humana, la precisión de los resultados y la seguridad de los datos utilizados.

Comparativamente, otras regiones y países están desarrollando sus propios enfoques hacia la regulación de la IA. Por ejemplo, en Estados Unidos, la estrategia está muy fragmentada, con iniciativas a nivel estatal y sin un marco unificado comparable al de la UE. En Asia, países como China han emitido directrices éticas para el desarrollo de la IA, promoviendo su uso para el bien social pero enfatizando también la importancia de la seguridad y la soberanía de los datos.

El Reglamento de IA de la UE establece un precedente significativo, no solo por su enfoque integral y detallado, sino también por su ambición de armonizar diferentes regulaciones. Esto representa un desafío a la vez que una oportunidad para las empresas internacionales que operan en múltiples jurisdicciones, las cuales deben navegar a través de un paisaje regulatorio en evolución mientras buscan aprovechar las ventajas competitivas que la IA ofrece.

El impacto del Reglamento va más allá de sus fronteras, ya que se posiciona como referencia para otros países y regiones que están en el proceso de desarrollar o actualizar sus propias regulaciones de IA. Al establecer altos estándares de transparencia, seguridad y ética, la UE está promoviendo un modelo global para el desarrollo y uso responsable de la IA. Esto no solo ayuda a mitigar los riesgos asociados con estas tecnologías, sino que también fomenta un entorno de innovación en el que la confianza del consumidor y la seguridad pública son prioritarias.

En definitiva, el IA Act representa uno de los primeros y más ambiciosos intentos de regular la IA a nivel global, lo que lo posiciona como un modelo potencial para futuras legislaciones en todo el mundo.

Clasificación de riesgos

El IA Act clasifica los sistemas de IA en cuatro categorías de riesgo: inaceptable, alto, limitado y mínimo. Esta clasificación se basa en el nivel de riesgo que los sistemas de IA presentan a la seguridad y los derechos fundamentales de las personas. Los sistemas considerados como un riesgo inaceptable están prohibidos debido a su potencial para violar los derechos humanos o socavar la democracia. Esto incluye, por ejemplo, la vigilancia masiva indiscriminada y los sistemas de puntuación social al estilo de ciertas distopías.

Figura 1.- Niveles de clasificación del riesgo según el IA Act.

Requisitos para sistemas de alto riesgo

Los sistemas de IA clasificados como de alto riesgo están sujetos a requisitos rigurosos antes de su implementación. Estos requisitos incluyen:

- **Transparencia y provisión de información:** Garantizar que los usuarios están plenamente informados sobre cómo funciona el sistema de IA, sus capacidades y limitaciones.
- **Calidad de los datos:** Asegurar que los conjuntos de datos utilizados para entrenar, probar y validar los sistemas de IA sean relevantes, representativos y libres de sesgos.
- **Documentación y registro:** Mantener registros detallados de la programación y entrenamiento del sistema de IA para facilitar la trazabilidad y la auditoría.
- **Supervisión humana:** Establecer mecanismos adecuados de supervisión humana para minimizar el riesgo de decisiones erróneas y garantizar el respeto por los derechos humanos.
- **Robustez, seguridad y precisión:** Desarrollar sistemas de IA que sean seguros, robustos y precisos, capaces de manejar errores o inconsistencias.

Potencial como modelo para futuras legislaciones

El IA Act tiene el potencial de servir como modelo para futuras legislaciones de IA a nivel global, por varias razones:

- **Enfoque basado en riesgos:** Su metodología para clasificar los sistemas de IA según el nivel de riesgo proporciona un marco flexible que puede adaptarse a la evolución de la tecnología y sus aplicaciones.
- **Equilibrio entre innovación y protección:** Al enfocarse en sistemas de alto riesgo, el IA Act busca proteger los derechos de los ciudadanos y la seguridad pública sin sofocar la innovación en el campo de la IA.
- **Promoción de la transparencia y la confianza:** Al establecer requisitos estrictos para la transparencia y la supervisión humana, fomenta un entorno de confianza y seguridad que es esencial para la aceptación y adopción generalizada de la IA.
- **Posible influencia global:** Dada la importancia económica de la UE, es probable que las empresas internacionales que deseen operar en el mercado europeo adopten las prácticas establecidas por el IA Act, promoviendo de facto un estándar global.

En conclusión, el IA Act no solo establece un marco legislativo para el uso ético y respon-

sable de la IA dentro de la UE, sino que también ofrece un modelo valioso para la regulación de la IA a nivel mundial. Al abordar proactivamente los riesgos y desafíos asociados con la IA, el Reglamento puede guiar el desarrollo de políticas y legislaciones que equilibren la innovación tecnológica con la protección de los derechos humanos y la seguridad pública.

PANORAMA DE LA LEGISLACIÓN DE IA A NIVEL MUNDIAL

El panorama de la legislación de IA a nivel mundial es tan diverso como los países que buscan regular esta tecnología disruptiva. Fuera de la UE, que se ha posicionado a la vanguardia con su Reglamento, otros países están adoptando enfoques variados, reflejando sus prioridades nacionales, culturales y económicas. Esta diversidad de estrategias subraya los múltiples desafíos éticos y de seguridad que la IA presenta, así como las diferentes filosofías sobre cómo la tecnología debe servir a la sociedad.

Mientras que la diversidad de enfoques presenta desafíos para la armonización de estándares y prácticas, también ofrece una oportunidad para aprender de las diferentes experiencias y fomentar un enfoque globalmente coherente y ético para la regulación de la IA.

Figura 2.- Organismos que están trabajando en regular la IA.

• **Estados Unidos** no ha implementado aún, a diferencia de la UE, un marco regulatorio federal unificado para la IA. Sin embargo, ha habido movimientos significativos a nivel estatal y sectorial, con directrices y políticas que abordan aspectos relevantes o aplicaciones específicas de la IA, como la privacidad de datos, el reconocimiento facial y los vehículos autónomos. A nivel federal, agencias como la Administración Nacional de Aeronáutica y del Espacio (NASA) y el Departamento de Defensa están desarrollando políticas para el uso ético de la IA en sus operaciones.

• **China** es otro actor importante en el escenario mundial de la IA, con ambiciones de convertirse en líder mundial para 2030. El gobierno chino ha emitido una serie de directrices con un fuerte enfoque en la seguridad, la ética y la promoción del bienestar público. Sin embargo, también hay preocupaciones sobre el uso de la IA para la vigilancia y el control social, lo que plantea cuestiones éticas significativas a nivel internacional.

• **Canadá** ha sido pionero en la adopción de una estrategia nacional que enfatiza la investigación ética y responsable en IA. A través del Instituto Canadiense de Investigaciones Avanzadas (CIFAR), Canadá ha invertido en programas que promueven la colaboración internacional y el desarrollo de IA responsable. Además, el gobierno canadiense ha establecido un Consejo Asesor de IA para guiar la implementación ética de la tecnología con políticas y prácticas gubernamentales.

• **Singapur** ha desarrollado un marco llamado "Model AI Governance Framework", que se centra en la transparencia y la equidad de los sistemas de IA. Este marco está diseñado para ser práctico y aplicable a una amplia gama de industrias, fomentando la innovación al tiempo que protege los derechos de los ciudadanos.

• **Reino Unido** ha adoptado un enfoque basado en principios para la regulación de la IA, a la vez que ha creado el Centro para Datos Éticos e Innovación que guía la implementación ética de la IA en el sector público y privado. Cabe destacar que el Reino Unido está invirtiendo en investigación y desarrollo de IA con una orientación respetuosa con la ética y la seguridad.

Estos enfoques nacionales varían significativamente, desde la promoción abierta de la innovación en IA hasta la implementación de estrictas regulaciones para abordar preocupaciones éticas y de seguridad. Lo que queda claro es que, mientras algunos países buscan liderar en el desarrollo de tecnología de IA, también hay un reconocimiento creciente de la necesidad de regulaciones que aseguren el uso ético y responsable de la IA.

A nivel global, hay un movimiento hacia la cooperación internacional y el intercambio de mejores prácticas en la regulación de la IA. Organizaciones internacionales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y las Naciones Unidas están facilitando el diálogo sobre principios éticos y directrices para la gobernanza de la IA, buscando establecer un consenso global sobre cómo abordar los desafíos que la tecnología presenta.

DESARROLLANDO IA CONFIABLE: UN ENFOQUE INTEGRAL

Desarrollar IA confiable es un imperativo ético y práctico para investigadores, desarrolladores y empresas en la era digital. Este enfoque integral abarca siete aspectos fundamentales: fiabilidad, seguridad, equidad, resistencia al mal uso, entendimiento y razonamiento, norma social y robustez. Incorporar estos principios desde el inicio del diseño y desarrollo de sistemas de IA no solo es crucial para ganar la confianza del usuario, sino también para mitigar riesgos y promover un impacto social positivo:

a. Fiabilidad. Implica que un sistema de IA funcione según lo previsto bajo diversas condiciones, produciendo resultados consistentes y precisos.

b. Seguridad. Se centra en proteger los sistemas de IA contra manipulaciones y ataques que podrían llevar a comportamientos no deseados o peligrosos.

c. Equidad. Busca asegurar que los sistemas de IA no perpetúen sesgos o discriminación.

d. Resistencia al mal uso. Se enfoca en controlar el potencial uso indebido por parte de atacantes maliciosos que quieren causar daños a los usuarios y las partes interesadas**.**

e. Entendimiento y razonamiento. Es la capacidad de explicar los resultados y el correcto razonamiento a los usuarios**.**

f. Norma social. E la capacidad de reflejar los valores humanos universalmente compartidos**.**

g. Robustez. Se refiere a la resiliencia frente a ataques adversarios y cambios en la distribución.

Estos siete aspectos fundamentales ofrecen un marco para desarrollar una IA confiable. A través de la implementación consciente de estos principios, los desarrolladores pueden crear sistemas de IA que no solo sean innovadores y eficientes, sino también éticos, seguros y beneficiosos para la sociedad. La adopción de las mejores prácticas en estas áreas es crucial para el futuro de la IA y su integración armoniosa en la vida cotidiana.

EL IMPERATIVO DEL CONTROL CONTINUO DE LA IA

El desarrollo y despliegue de sistemas de IA presentan retos únicos debido a su capacidad para aprender, evolucionar y, en algunos casos, operar de maneras que sus creadores no anticiparon completamente. Dada esta naturaleza dinámica, el control continuo de estos sistemas se convierte en un imperativo para asegurar que se mantengan alineados con principios éticos y de cumplimiento normativo a lo largo de su ciclo de vida. Este control continuo no solo implica monitorización y ajustes regulares, sino también la adaptación proactiva a cambios en el entorno operativo, avances tecnológicos y evolución de las expectativas sociales.

Importancia de los mecanismos de control continuo

• **Alineación ética:** Los sistemas de IA tienen el potencial de impactar significativamente en la sociedad, desde mejorar el acceso a la educación y la atención médica hasta influir en la

toma de decisiones judiciales y la privacidad. Un control continuo asegura que los sistemas se mantengan alineados con los valores éticos y no desvíen hacia comportamientos no deseados o discriminatorios.

• **Cumplimiento normativo:** Las regulaciones en torno a la IA están evolucionando constantemente a medida que gobiernos y organismos internacionales reconocen nuevos riesgos y oportunidades. Los mecanismos de control continuo permiten que los sistemas de IA se ajusten a estas normativas cambiantes, evitando sanciones y garantizando la protección de los usuarios.

• **Adaptabilidad y resiliencia:** Los entornos en los que opera la IA pueden cambiar rápidamente debido a factores externos como emergencias sanitarias, cambios económicos o avances tecnológicos. El control continuo facilita la adaptación a estos cambios, asegurando que los sistemas sigan siendo relevantes y efectivos.

• **Prevención de derivas en el aprendizaje:** A medida que los sistemas de IA interactúan con nuevos datos, existe el riesgo de que desarrollen comportamientos no anticipados o se desvíen de sus objetivos iniciales, un fenómeno conocido como deriva del modelo. La monitorización constante y la recalibración periódica ayudan a prevenir estas derivas, manteniendo la integridad del sistema.

Estrategias para el control continuo

• **Auditorías y revisiones periódicas:** Realizar auditorías regulares de los sistemas de IA, revisando tanto el comportamiento del sistema como los datos con los que interactúa, para identificar posibles desviaciones o áreas de mejora.

• **Marco de gobernanza de IA:** Establecer un marco de gobernanza robusto que defina claramente las responsabilidades, los procesos de toma de decisiones y los protocolos de intervención para los sistemas de IA.

• **Mecanismos de retroalimentación:** Implementar canales para recoger la retroalimentación de los usuarios y otras partes interesadas, permitiendo ajustes basados en experiencias reales y preocupaciones emergentes.

• **Entrenamiento continuo:** Asegurar que los sistemas de IA reciban entrenamiento continuo con datos actualizados y representativos para prevenir sesgos y mejorar su precisión y relevancia.

• **Transparencia y comunicación:** Mantener una comunicación abierta sobre cómo se monitorizan y controlan los sistemas de IA, aumentando la confianza de los usuarios y las partes interesadas.

Conclusión

El control continuo de los sistemas de IA es crucial para garantizar que permanezcan efectivos, éticos y en cumplimiento con las normativas a lo largo de su operación. Al adoptar un enfoque proactivo hacia la monitorización y ajuste de estos sistemas, las organizaciones pueden navegar con éxito los desafíos presentados por la naturaleza dinámica de la IA, asegurando que sus beneficios se maximicen mientras se minimizan los riesgos.

LA IA DEL FUTURO: ÉTICA Y SEGURIDAD EN EL DESARROLLO TECNOLÓGICO

El futuro de la IA se presenta como un horizonte lleno de promesas y potencialidades. Mientras nos adentramos en esta nueva era, el optimismo hacia el impacto positivo de la IA en la sociedad es tanto necesario como prudente. Sin embargo, para que este futuro sea tan brillante como esperamos, es imperativo que el desarrollo tecnológico de la IA se rija por fuertes consideraciones éticas y de seguridad. Esto requiere un delicado equilibrio entre fomentar la innovación tecnológica y mantener una firme responsabilidad social. Al hacerlo, podemos asegurar que la IA no solo avance en capacidades, sino que también promueva el bienestar colectivo y proteja los derechos fundamentales de todos los individuos.

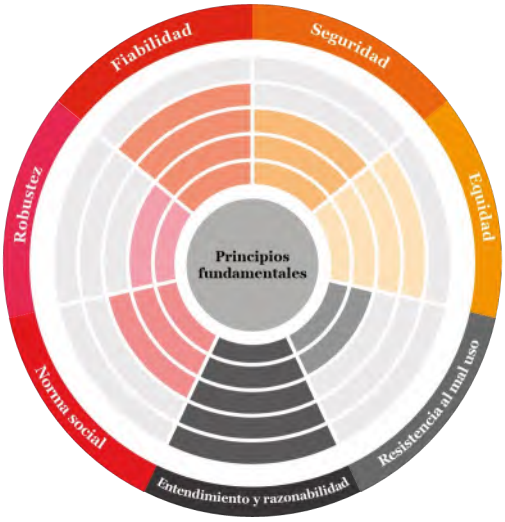


Fig. 3.- Principios para la gestión de riesgos en sistemas de IA.

Ética y seguridad: Pilares del desarrollo tecnológico

Para que la IA actúe como una fuerza positiva, los principios éticos y las medidas de seguridad deben ser integrados en el núcleo del proceso de diseño y desarrollo. Esto implica ir más allá del cumplimiento normativo, abrazando un compromiso profundo con la justicia, la equidad, la inclusión, y el respeto a la privacidad y la dignidad humana. El desarrollo de la IA debe ser guiado por un marco ético que considere el impacto a largo plazo de estas tecnologías en la sociedad y el medio ambiente.

Un equilibrio entre innovación y responsabilidad

La innovación tecnológica en el campo de la IA ofrece soluciones a algunos de los desafíos más complejos de nuestro tiempo, desde el cambio climático y la escasez de recursos hasta enfermedades globales y desigualdades sociales. Sin embargo, esta innovación debe ser equilibrada con la responsabilidad de garantizar que no se creen nuevos problemas o se exacerben las desigualdades existentes. Un enfoque responsable hacia el desarrollo de la IA incluye la transparencia en los procesos de toma de decisiones, el compromiso con la reducción de sesgos y la implementación de mecanismos de rendición de cuentas.

La colaboración multidisciplinaria como clave para el futuro

El futuro exitoso de la IA, fundamentado en la ética y la seguridad, requiere la colaboración entre disciplinas y sectores. Esto significa unir a ingenieros y desarrolladores de IA con expertos en ética, filosofía, sociología, derecho y política, así como con la sociedad en general. Este enfoque multidisciplinario puede fomentar una comprensión más profunda de las implicaciones sociales de la IA y promover el desarrollo de tecnologías que respeten y enriquezcan la vida humana.

Casos de éxito: Inspiración para el futuro

La historia reciente ya ha proporcionado ejemplos inspiradores de cómo la IA puede servir al bien común, desde sistemas de IA que ayudan en la diagnosis y tratamiento de enfermedades hasta algoritmos que optimizan la producción de energías renovables. Estos casos de éxito deben servir como modelos para el desarrollo futuro de la IA, demostrando que es posible alcanzar logros tecnológicos significativos mientras se protege y mejora la sociedad.

CONCLUSIÓN

Mirando hacia el futuro, existen múltiples razones para ser optimistas sobre el papel que la IA puede jugar como una fuerza positiva en la sociedad. Sin embargo, este futuro no está garantizado; requiere un compromiso consciente con la ética y la seguridad en cada paso del desarrollo tecnológico. Al equilibrar la innovación con la responsabilidad social, podemos asegurar que la IA no solo transforme nuestras capacidades tecnológicas, sino que también promueva una sociedad más justa, segura y próspera. Este equilibrio no es solo deseable, es esencial para garantizar que el futuro de la IA sea uno que todos deseemos habitar. ■

Irene Yusta
Head of Data and AI
MÁSMÓVIL

Antonio Requena
Socio en Business Security Solutions
PwC

Akamai

Akamai Connected Cloud

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

- Content Delivery
- Cyber Security
- Cloud Computing

www.akamai.com

>> Jorge Dávila

Frente al futuro, Camina o Revienta

A pesar de que "lo Cuántico" en criptografía puede acabar siendo una moda pasajera, la 'Paranoia Inducida' que ha traído ha espoleado el resurgir de lo Pos-cuántico y ya tenemos algoritmos administrativamente reconocidos que quieren desterrar a las antiguas glorias de lo asimétrico (RSA, ElGamal, Diffie-Hellman y Curvas Elípticas). Sin embargo, esa transición no se puede hacer ni a la ligera, ni de golpe, por lo que es momento de echarle un vistazo y ver qué podemos o debemos hacer.

"*Camina o revienta*" fue una de las aportaciones biográficas más sinceras de quien empezó siendo un pequeño delincuente que robó unas gallinas y que, con el paso del tiempo, se convirtió en un símbolo de lo que era nuestro país durante la década de los sesenta y setenta del siglo pasado. Ese título tan áspero viene a decir, entre otras cosas, que muchas veces en la vida **no hay más opción que avanzar para no desaparecer**, y es una expresión que se atribuye al que es un quinqui [1] salmantino llamado Eleuterio Sánchez Rodríguez [2].

En mayo de 1965 se produjo un atraco a mano armada en una joyería en la calle de Bravo Murillo de Madrid, y durante su desarrollo murió un vigilante de seguridad y robaron 120.000 pesetas (721,21 €). Eleuterio Sánchez fue acusado de ese robo y sometido a un juicio en el que se le declaró culpable. Se le condenó a la pena capital [3] (muy vigente en España en aquellas fechas [4]), aunque esa sentencia fue más tarde conmutada por la de cadena perpetua.

Tan pronto como tuvo ocasión, al año siguiente, Eleuterio Sánchez se fugó durante un traslado penitenciario saltando de un tren en marcha, al más puro estilo del Spaghetti Western [5] que por aquellos años se filmaba en Almería y Madrid [6]. Apenas dos semanas después fue detenido y llevado de nuevo a prisión, siendo su fuga objeto de una impresionante atención mediática que marcó una época.

Su fama mediática vino de la mano de sus fugas, la primera de ellas desde un tren en el que, custodiado por la Guardia Civil, participaba en un traslado penitenciario en 1966. Consiguió estar evadido durante trece días hasta ser arrestado. La segunda fuga fue del penal del Puerto de Santa María en la Nochevieja de 1970, tras el cual estuvo escondido y fugado durante un largo periodo de tiempo gracias a la ayuda de su grupo social. Su búsqueda fue seguida con gran interés por la prensa, lo que acrecentó su fama, hasta que finalmente el 2 de junio de 1973 fue detenido de nuevo y no se volvió a escapar. Desde el 20 de julio de 1981 está en libertad definitivamente al haber sido indultado por el gobierno español [7] de Calvo Sotelo después de una reinserción completa en la sociedad.

Entonces se contaron muchas versiones imprecisas, pero hoy la única historia de aquellos hechos y su contexto que nos vale quizás sea la del propio Eleuterio Sánchez contenida en su libro "*Camina o revienta*" (1977) [8] y que continuó con otro posterior, el titulado "*Mañana seré libre*" (1979). Ambas obras fueron escritas y publicadas mientras todavía su autor estaba en prisión.

El espíritu de supervivencia

Si algo tienen en común todos los sistemas vivos, independientemente de su complejidad, tanto los que van desde las humildes bacterias hasta las mismas élites económicas y sociales humanas, es una cualidad: el **espíritu de supervivencia** [9]. Todos los sistemas vivos, viven para **perpetuarse en el tiempo como colectivo** y eso lo hacen mediante la reproducción de sus individuos y el mantenimiento de la información cultural ("*el relato*"). Si las sociedades en el fondo **son las que den de sí sus tecnologías**, ese espíritu de supervivencia se manifiesta en una **necesaria actualización y renovación tecnológica**. Por ello, el escenario digital que cada día nos envuelve más, también debería actualizarse, pero queda por ver cómo lo hace.

Toda renovación o actualización tecnológica necesita **tiempo**, **previsión** y **planificación**, y bastante **esfuerzo de Investigación y Desarrollo**. Conocido esto, la cuestión que queda por dilucidar es cómo cada sociedad asigna recursos a ese proceso. En las sociedades capitalistas, esa "financiación" del proceso de modernización se le deja al "mercado", y éste sólo se pone en marcha si en ello ve el crecimiento de su misma riqueza. El Mercado no necesariamente se preocupa específicamente de su propia supervivencia aunque, indirectamente, el maximizar beneficios también es una forma de supervivencia, una perpetuación de *status quo* en la que sobrevive el Capital y no necesariamente los homínidos que lo adoran y personalizan.

Una forma que tiene el Capital de abordar las grandes operaciones que requieren gran cantidad de financiación es convencer a la ingenua población mundial de su absoluta necesidad. Ejemplo magnifico de ello fue la campaña "Átomos para la Paz" [10] que en el fondo fue una operación para justificar el uso civil de los materiales radiactivos y el establecimiento de la **Energía Nuclear de uso civil**. Realmente, esa operación lo que conseguía para los EEUU era un **mercado cautivo** [11] de ciudadanos europeos que **1)** le comprarían durante generaciones la tecnología que EEUU estuviera dispuesta a venderles y **2)** a consumir el uranio que tuvieran a bien venderles, eso sí **3)** con la condición de que los residuos de "combustión" volverían a manos americanas de modo que sólo ellos pudiesen extraer los materiales fisibles (el plutonio) de calidad e interés militar y que iba a requerir el inminente escalado de la Guerra Fría; no vaya ser que el **Club de Naciones con Armas Nucleares** [12] se pueble con más incontrolables de los que ya hay.

No es aconsejable utilizar y dar por seguro ningún algoritmo o procedimiento criptográfico que no haya sufrido (imbatido) el escrutinio público de los más hábiles criptoanalistas del planeta durante (al menos) un par de décadas.

Aunque la economía real de la Energía Nuclear sigue siendo un tema de debate y que la Historia ha puesto de manifiesto que el objetivo real de la misma era y es otro distinto del bienestar ciudadano de los que la pagan, la campaña de uso civil de los isotopos radioactivos logró engañar a muchos y terminar reclutando los intereses inconfesables de algunos [13].

Desde que existe Internet, sus muy publicitadas "tendencias" tienen como máximo **dos años de vida**. Para algunos los NFT habían llegado para quedarse y ahora están hundidos. Para algunos las criptomonedas iban a hacer desaparecer el dinero, las mondas y los bancos emisores, y sin embargo muchas de ellas han desaparecido, el "negocio Crypto" es sinónimo de fraude y estafa, y sólo siguen sobreviviendo algunas **por necesidades del blanqueo de capitales y la ciberdelincuencia** [14].

La Paranoia Inducida por la Amenaza Cuántica

En estos días las "*tendencias*" son la **Inteligencia Artificial** y todo **lo Cuántico**; la computación, el cifrado, las comunicaciones, los circuitos, etc. Dejando a un lado la IA, nos centraremos en algunos efectos que ha tenido lo que podríamos llamar la **Paranoia Inducida por la Amenaza Cuántica**. Igual que los ilustradores, músicos e intérpretes lamentan y preparan las exequias de su arte por el carácter tóxico que tienen las Inteligencias Artificiales llamadas "generativas", la paranoia [15] generada por los intereses cuánticos está teniendo efectos significativos en los tejidos digitales de nuestra sociedad.

Su primer y más renombrado efecto fue la iniciativa Pos-Quántica [16] de la administración estadounidense puesta en marcha en 2016. El objetivo de la misma era encontrar **nuevos algoritmos criptográficos asimétricos** [17] que pudieran resistir la amenaza cuántica que suponen los algoritmos de Shor [18] y Grover [19]. Es cierto que, de existir un ordenador cuántico confiable y tecnológicamente robusto, los problemas en los que se basa el algoritmo RSA [20] (**factorización**), ElGamal [21] y los protocolos Diffie-Hellman [22] (**logaritmo Discreto** [23]) y la Criptografía sobre Curvas Elípticas [24] (**estructura algebraica de las curvas elípticas sobre campos finitos** [25]) se verían simplificados significativamente, obligando a utilizar claves inmanejablemente grandes (si las comparamos con lo que estamos acostumbrados) y a tiempos de computación en su uso que hoy se nos antojan inaceptables.

Por este motivo, la comunidad académica mundial se volvió hacia viejos problemas que ya se conocían pero que, por distintas razones, no habían tenido mucho éxito (por ejemplo, el vetusto algoritmo de McEllice) como cuna para nuevos Criptosistemas Asimétricos. Los algoritmos Post-quantum se centran principalmente en seis aproximaciones distintas [26]: las basadas en **1) retículos** [27], **2) polinomios multivariantes sobre campos finitos** [28], **3)** la **seguridad de las funciones hash** [29], **4)** en **códigos correctores de errores** [30], **5)** las propiedades de algunas isogenias y otras **variedades abelianas** [31], **sobre curvas elípticas** operando **sobre cuerpos finitos** [32] y, por último, basándose en **6)** la **duplicación en el tamaño de claves** en sistemas simétricos [33].

No vamos a entrar en detalles técnicos sobre estas iniciativas ni sobre el éxito o no que se pueda esperar de algunas de ellas, sino que debemos centrarnos sobre **la conveniencia y la oportunidad de asumirlas actualmente como están y como han sido propuestas**, al estilo de lo que ha hecho la administración norteamericana a través de la iniciativa del NIST [34].

Dado que **1)** la seguridad de un algoritmo criptográfico está medida por la **complejidad computacional del ataque más efectivo conocido**, que **2)** los mecanismos de ataque **sólo se conocen cuando ya han sido descubiertos** (no podemos saber lo que depara el futuro), y **3)** que no hay herramientas generales que permitan atacar algoritmos criptográficos, por lo que **el criptoanálisis sigue siendo un arte**, NO es aconsejable utilizar y dar por seguro ningún algoritmo o procedimiento criptográfico que no haya sufrido (imbatido) el escrutinio público de los más hábiles criptoanalistas del planeta durante (al menos) un par de décadas. Por ello, **hoy** (y no antes) **podemos empezar a considerar razonablemente seguro el algoritmo AES** [35]; pero mejor que sea el de 256 bits de clave para que, de paso, sea *PQ resistant*.

Si no es razonable adoptar los algoritmos criptográficos recién llegados y seguimos creyendo la inminente llegada del Quinto Jinete (el cuántico, no el del apocalipsis) ¿Qué podemos hacer para sentirnos más seguros? Lo más razonable es adoptar una **estrategia mixta o híbrida** en la que se combinen de forma correcta los nuevos algoritmos pos-cuánticos y los mejores cifradores que hayamos estado utilizando los últimos cuarenta años (pre-cuánticos).

Hay una verdad ya establecida que viene a salvarnos y es que: *si mezclamos adecuadamente dos secuencias aleatorias y uniformemente distribuidas, y una de ellas permanece secreta, el resultado de la combinación reversible, sigue siendo secreta*. Eso ya lo demostró en 1948 Claude Shannon [36] con su **Teoría de la Información** [37] **aplicada A Sistemas Secretos** [38] y se conoce como **cifrado Vernam** [39] (1917) o cifrado **One Time Pad** [40] (OTP).

Es tiempo de encontrar y utilizar sabiamente nuevos algoritmos asimétricos pero no porque demos crédito a la paranoia inducida por los apóstoles de la amenaza cuántica, sino porque son pocas las cestas en las que estamos poniendo todos los huevos.

Así pues, lo lógico es **que generemos** (**bien**) **las claves simétricas** (secretas, aleatorias, uniformes, únicas y largas) que utilicemos para proteger la **confidencialidad** y/o **integridad** de la información utilizando tanto los nuevos (PQAs) como los viejos (PKAs) algoritmos y combinemos ambos de forma (OTP) que, **mientras uno permanezca secreto, la clave de cifrado siga siendo secreta**.

---

[1] Ver https://es.wikipedia.org/wiki/Merchero
[2] Ver https://es.wikipedia.org/wiki/Eleuterio_Sánchez
[3] Ver https://es.wikipedia.org/wiki/Pena_de_muerte_en_España
[4] Ver https://es.wikipedia.org/wiki/Antonio_López_Sierra
[5] Algunos ejemplos son, "Por un puñado de dólares" (1964), "La muerte tenía un precio" (1965) y "El bueno, el feo y el malo" (1966), todas ellas protagonizadas por un jovencísimo Clint Eastwood y acompañadas por la excepcional música de fondo de Ennio Morricone. Ver https://en.wikipedia.org/wiki/Spaghetti_Western
[6] Ver https://historias-matritenses.blogspot.com/2009/08/el-imperio-samuel-bronston-en-las-matas.html
[7] Ver https://www.boe.es/boe/dias/1981/10/07/pdfs/A23485-23485.pdf en su entrada 22810.
[8] "Camina o revienta" fue la historia que utilizó Vicente Aranda como argumento para su famosa película que lleva el mismo título. https://www.imdb.com/title/tt0093458/
[9] Ver https://en.wikipedia.org/wiki/The_Selfish_Gene
[10] "Atoms for Peace" fue el título de la conferencia que dio el Presidente de los EEUU Dwight D. Eisenhower ante la asamblea general de la Naciones Unidas en New York City el 8 de diciembre de 1953. Ver https://en.wikipedia.org/wiki/Atoms_for_Peace
[11] Ver https://en.wikipedia.org/wiki/Economics_of_nuclear_power_plants
[12] Ver https://en.wikipedia.org/wiki/List_of_states_with_nuclear_weapons
[13] Ver https://www.eldiario.es/sociedad/felipe-gonzalez-defiende-energia-nuclear-frente-renovables-son-energias-limpias-alguien-sacramento_1_10876945.html
[14] Ver https://cincodias.elpais.com/cincodias/2022/06/22/legal/1655914425_833391.html
[15] "Paranoia Megalomaníaca: el individuo cree poseer talentos o poderes superiores, se relaciona con seres divinos o personas famosas o poderosas, y está en el mundo porque le fue encomendada una alta misión." En https://www.significados.com/paranoia/
[16] Ver https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization
[17] Ver https://en.wikipedia.org/wiki/Public-key_cryptography
[18] Ver https://en.wikipedia.org/wiki/Shor's_algorithm
[19] Ver https://en.wikipedia.org/wiki/Grover's_algorithm
[20] Ver https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[21] Ver https://en.wikipedia.org/wiki/ElGamal_signature_scheme
[22] Ver https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
[23] Ver https://en.wikipedia.org/wiki/Discrete_logarithm
[24] Ver https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
[25] Ver "Resource analysis and modifications of quantum computing with noisy qubits for elliptic curve discrete logarithms" en https://www.nature.com/articles/s41598-024-54434-w.pdf
[26] Ver Daniel J. Bernstein : "Introduction to post-quantum cryptography" en https://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf
[27] Ver https://en.wikipedia.org/wiki/Lattice-based_cryptography
[28] Ver https://en.wikipedia.org/wiki/Multivariate_cryptography
[29] Ver https://en.wikipedia.org/wiki/Hash-based_cryptography
[30] Ver https://en.wikipedia.org/wiki/McEliece_cryptosystem
[31] Ver https://en.wikipedia.org/wiki/Abelian_variety
[32] Ver https://en.wikipedia.org/wiki/Supersingular_isogeny_graph
[33] Por ejemplo, el AES y los algoritmos SNOW 1.0, SNOW 2.0, y SNOW 3G que son cifradores de flujo sincrónicos basados en el uso de palabras. Ver https://en.wikipedia.org/wiki/SNOW
[34] Ver https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization
[35] Ver https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[36] Ver https://en.wikipedia.org/wiki/Claude_Shannon
[37] Shannon, Claude E: "A Mathematical Theory of Communication" Bell System Technical Journal. 27 (3): 379–423, 1948. Ver https://en.wikipedia.org/wiki/Information_theory
[38] Shannon, Claude E: "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol. 28(4), pages 656–715, 1949. Ver https://www.cs.virginia.edu/~evans/greatworks/shannon1949.pdf
[39] Ver https://en.wikipedia.org/wiki/Gilbert_Vernam
[40] Ver https://en.wikipedia.org/wiki/One-time_pad y https://patents.google.com/patent/US1310719

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

Aunque las cosas están claras, eso no significa que las cosas se vayan a hacer bien. La amenaza cuántica ha sabido convertirse en tendencia en Internet y eso ha hecho que todos pasemos por las **Horcas Caudinas**[41] y nos hinquemos de rodillas atemorizados de la llegada del **Quinto Jinete**[42]. Mientras tardan los desastres prometidos por "*influencers* de la amenaza cuántica", es cierto que **1)** el número de algoritmos criptográficos asimétricos era excesivamente reducido desde que en 1976 se imaginaron su existencia[43], y **2)** que no es bueno poner todos los huevos en la misma cesta (o algoritmo), por lo que **las estrategias hibridas son muy recomendables**. Por lo que podríamos concluir que "*no hay mal que por bien no venga*"[44].

Un algoritmo criptográfico puede ser perfecto, pero un atacante sólo necesita que su implementación, la que al final se utiliza, no lo sea.

La Post-Quantum Cryptography Alliance

Sin ánimo de alargarnos mucho más, conviene tener también en cuenta cómo se hacen esas migraciones y quienes la dirigen y capitalizan. Últimamente **The Linux Foundation**[45] ha puesto en marcha una iniciativa llamada **Post-Quantum Cryptography Alliance**[46] (**PQCA**), en la que algunos académicos pretenden "***dirigir el avance y adopción de la criptografía pos-cuántica***". En ese club se pretende reunir líderes industriales, investigadores académicos, y desarrolladores de todo tipo para dar respuesta a los retos planteados por la computación cuántica a la seguridad criptográfica, y hacerlo produciendo **implementaciones software "seguras" de algoritmos estandarizados**, a la vez que fomenten el continuo desarrollo y estandarización de nuevos algoritmos post-cuánticos.

Músculo no debería faltarle dada la lista de promotores declarados. Hay grandes empresas como Amazon Web Services (AWS), Cisco, Google, IBM, y Nvidia, con otras mucho más pequeñas y de nicho ontológicamente interesadas en que esto tire para delante como son IntellectEU, Keyfactor, Kudelski IoT, QuSecure, SandboxAQ y, curiosamente **en solitario aparece un laboratorio de la University of Waterloo**[47]. Aunque ya se sabe que son todos los que se apuntan para constar y luego ya veremos en que queda todo.

El objetivo de esta iniciativa la ponen sus promotores en la implementación de los nuevos algoritmos pos-cuánticos estandarizados dentro de librerías esenciales del sistema operativo en general y, en este caso, para el Linux en particular. Es inteligente centrarse en estas implementaciones porque ocupan un lugar privilegiado en la arquitectura de seguridad de todos los futuros sistemas y servicios. **Un algoritmo criptográfico puede ser perfecto, pero un atacante sólo necesita que su implementación, la que al final se utiliza, no lo sea**.

El Open Quantum Safe project

Uno de los primeros proyectos contenidos dentro de este paraguas en el **Open Quantum Safe project**[48], dentro de la University of Waterloo desde 2014, y que se presenta como un proyecto de software *open-source* centrado en la criptografía post-cuántica. Otro proyecto relacionado es el **PQ Code Package Project**[49] que se centra en implementaciones software del tipo "*llave en mano*", de los estándares pos-cuánticos que haya y vaya habiendo, empezando con el algoritmo ML-KEM[50].

Todas las aplicaciones de cifrado, almacenamiento, comunicaciones, terminales, etc., que corran por encima de esas nuevas librerías, de hacerlo, quedarían automáticamente "*actualizadas*" y "*securizadas*" al estilo pos-cuántico. En cualquier caso, aunque la intención declarada pueda ser buena, **siempre hay que participar activa y críticamente en el escrutinio de lo que se haga y proponga**. Más aun, las administraciones y empresas que luego dependen de la seguridad de esos sistemas operativos y servidores, **deberían dedicar recursos y esfuerzos para participar** (pero NO liderar) **y escrutar lo que** en ese sentido **se esté haciendo**.

Hay ejemplos de cómo algunas instituciones han intentado sabotear el establecimiento de estándares criptográficos con la esperanza de ganar secretas ventajas frente a todos los demás[51]. En 2013 los documentos publicados por **Edward Snowden**[52] sugerían que la NSA[53] participó muy activamente en la redacción del algoritmo **Dual Elliptic Curve Deterministic Random Bit generator**[54] (**Dual_EC_DRBG**) que se convertiría en estándar del NIST en 2006. Posteriormente se vio[55] que en ese estándar "*no era oro todo lo que relucía*" y se optó por retirarlo por defectuoso.

En resumen, es tiempo de encontrar y utilizar sabiamente nuevos algoritmos asimétricos pero no porque demos crédito a la paranoia inducida por los apóstoles de la amenaza cuántica, sino porque son pocas las cestas en las que estamos poniendo todos los huevos. Siempre debemos tomar con mucha cautela y desconfianza cualquier ofrecimiento, aparentemente desinteresado o ineludible, en actualizar, parchear, remozar o, en esencia, cambiar nuestros sistemas de seguridad y cualesquiera cosas en las que se apoyen, y comprometernos nosotros directa y activamente en el proceso de análisis y escrutinio ya que cualquier otra estrategia es como "*encomendar el alma al diablo*".

La estrategia hibrida de incluir nuevos algoritmos es una salida muy digna, y probablemente la más adecuada. Debe sin duda ser estudiada con detalle ya que en este mundo de lo digital no tiene sentido tirar o abandonar lo que, correctamente utilizado, sigue funcionando a pesar de los anuncios de los evangelistas de lo cuántico.

La estrategia hibrida de incluir nuevos algoritmos que ya se ha mencionado, es una salida muy digna, y probablemente la más adecuada. Debe sin duda ser estudiada con detalle ya que en este mundo de lo digital (como en muchos otros), no tiene sentido tirar o abandonar lo que, correctamente utilizado, sigue funcionando a pesar de los anuncios de los evangelistas de lo cuántico. ■

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

[41] Ver https://es.wikipedia.org/wiki/Batalla_de_las_Horcas_Caudinas Se refiere a la humillación de "pasar bajo el yugo", o cuando los samnitas humillaron a los romanos. Ver https://i.pinimg.com/originals/69/5e/d0/695ed0e7fbe6328c0ec515656631443b.jpg

[42] "El quinto jinete" (Le Cinquième Cavalier) es una muy recomendable novela de 1980 (tecno-thriller) escrita por Larry Collins y Dominique Lapierre.

[43] W. Diffie, M. Hellman: "New directions in cryptography" IEEE Transactions on Information Theory. Volume 22. Issue 6. November 1976, pp 644-654. Ver https://www-ee.stanford.edu/~hellman/publications/24.pdf

[44] "No hay mal que por bien no venga" es una comedia de Juan Ruiz de Alarcón. También se conoce con los nombres de "Don Domingo de don Blas" y "El acomodado don Domingo de don Blas". Ver https://es.wikipedia.org/wiki/Juan_Ruiz_de_Alarcón

[45] Ver https://www.linuxfoundation.org/

[46] Ver https://www.linuxfoundation.org/press/announcing-the-post-quantum-cryptography-alliance-pqca

[47] Ver https://uwaterloo.ca/institute-for-quantum-computing/

[48] Ver https://openquantumsafe.org/ y https://openquantumsafe.org/team/

[49] Ver https://github.com/pq-code-packageer https://github.com/pq-code-package

[50] Ver https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf

[51] Ver https://www.transcend.org/tms/2013/12/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer/ y https://arstechnica.com/information-technology/2015/12/unauthorized-code-in-juniper-firewalls-decrypts-encrypted-vpn-traffic/

[52] Ver https://www.itnews.com.au/news/nist-formally-chops-nsa-tainted-random-number-generator-405833

[53] Ver https://en.wikipedia.org/wiki/NOBUS

[54] Ver https://en.wikipedia.org/wiki/Dual_EC_DRBG

[55] Ver Thomas C. Hale: "The NSA Back Door to NIST" https://www.ams.org/notices/201402/rnoti-p190.pdf


Ayudándote a aprovechar todo el potencial de la tecnología, para construir un futuro en el que todos podamos confiar.
Ajoomal Asociados
Your Security, Our Responsibility
Alfonso.martinez@thalesgroup.com
Laura.fernandez@ajoomal.com
THALES
Building a future we can all trust

“Copilot for Security aprovecha nuestra experiencia en seguridad, inteligencia global de amenazas y las tecnologías para ganar en eficiencia en los casos más críticos”

Vasu Jakkal

Vicepresidenta Corporativa de Seguridad, Cumplimiento, Identidad y Privacidad de Microsoft

>Por **Ana Adeva**
>Fotografía: **Microsoft**

Con más de 20 años de trayectoria en todo tipo de frentes de TI, Vasu Jakkal se unió a Microsoft en 2020 como responsable del negocio de seguridad, cumplimiento, identidad, gestión y privacidad, valorado en 20.000 millones de dólares. Un área en la que tiene un peso especial la gran apuesta de la multinacional por la IA y que ocupa gran parte de su tiempo. Reconocida como una de las 25 principales mujeres líderes en ciberseguridad de 2019 por la firma Software Report, Jakkal desgranó para SIC algunas de las claves estratégicas de la compañía aprovechando la celebración del Microsoft AI & Innovation Summit en Madrid y los acuerdos suscritos con España.

– **Como Vicepresidenta Corporativa de Seguridad en Microsoft Corporation, que abarca un amplio portafolio de productos de Seguridad, Cumplimiento, Identidad y Privacidad, ¿por qué es tan importante unificarlos?**

– El panorama de amenazas al que nos enfrentamos no tiene precedentes y la velocidad, escala y sofisticación de los ciberataques está aumentando rápidamente. La importancia de una protección completa extremo a extremo radica en otorgar a los clientes la capacidad de abordar la seguridad desde todos los ángulos. Además, un portafolio integrado permite a los clientes cerrar puntos de fuga que suelen originarse al unir diferentes soluciones que no se complementan entre sí y aporta un mejor retorno de inversión. En la era de la IA, un conjunto integrado de soluciones facilita a la IA razonar a través de un conjunto de datos más unificado para una mejor visibilidad de las vulnerabilidades y comportamientos anómalos.

– **En su perfil destaca que usted “inspira el cambio liderando con una visión y una estrategia equilibrada con la generación de resultados medibles”, ¿Cómo se mide el éxito en ciberseguridad?**

– El éxito en ciberseguridad debe basarse en los resultados y, para ello, utilizamos muchas medidas, como la postura de seguridad, la resiliencia, los hitos de innovación y los marcos de confianza cero. También es importante contar con objetivos claros para que podamos estar orientados a la acción y ser ágiles en caso de ir por delante o por detrás. Por último, también es importante celebrar el éxito y al equipo.

Como ejemplo, veo y celebro los éxitos todos los días, a veces grandes logros y a veces pequeñas victorias. Cuando ayudamos a los clientes a prevenir un ataque devastador o a

adelantarnos a los malos actores, es un gran éxito para el equipo y para los defensores de todo el sector. Para mí, personalmente, cuando veo a las personas de mi equipo crecer en sus roles o expandir su liderazgo, eso es una gran victoria. Y que esté liderando nuestro negocio de seguridad en Microsoft en este increíble período de crecimiento y expansión, enfrentándome a este nuevo mundo de la Inteligencia Artificial con herramientas como Microsoft Copilot for Security, es también un éxito.

– ¿Cuál es el producto y servicio más desconocido -pero importante- del portafolio de seguridad reciente de Microsoft?

– Cada pieza de nuestro portfolio integral desempeña un papel fundamental en la seguridad de nuestros clientes. Sin embargo, estoy increíblemente orgullosa del trabajo que nuestro equipo ha realizado en Copilot for Security, nuestra solución de seguridad impulsada por IA. En la versión preliminar privada, nuestros clientes consiguieron ahorrar hasta un 40% del tiempo de sus analistas de seguridad en tareas fundamentales como investigación y respuesta, búsqueda avanzada de amenazas y análisis de inteligencia de amenazas. Actualmente, estamos en el punto de inflexión de la IA en la seguridad y estoy maravillada de ver cómo podemos continuar brindando avances de IA a toda la industria.

– Hace poco comentó en su LinkedIn que para ser exitosos los líderes deben aprender a "aceptar la incertidumbre y sentirse cómodos con lo inevitable". ¿Cómo practica eso en su día a día?

– Reconocer la incertidumbre y sentirse cómodo con lo inevitable es una tarea muy desafiante. En mi función, lo logro cuestionando y buscando respuestas constantemente. Incluso cuando las respuestas se me escapan, ampliar mis conocimientos me permite anticiparme a los resultados y tomar decisiones con mayor confianza.

– Además, usted destaca que "la seguridad es un deporte de equipo". ¿Quién -estado, empresa, organizaciones…- no está jugando como tal?

– Creemos firmemente que la seguridad es un deporte de equipo, y la industria debe trabajar en conjunto para protegerse contra las amenazas en evolución para ayudar a hacer del mundo un lugar más seguro. En seguridad, no se trata de lo que la tecnología puede hacer, sino de lo que las personas pueden hacer cuando están empoderadas por la tecnología. Utilizamos la frase de 'La seguridad es un deporte de equipo' como una llamada a la acción para todos los que pertenecen a la industria de la seguridad: somos más fuertes cuando nos mantenemos unidos que cuando estamos solos. A día de hoy, Microsoft cuenta con 15.000 *partners* y es maravilloso ver cómo el ecosistema trabaja conjuntamente.

– La industria de la ciberseguridad se encuentra en un momento de reestructuración –con operaciones destacables como la compra de Splunk por parte de Cisco o Juniper por parte de HPE, entre otras–. Ha participado en 15 operaciones de fusiones y adquisiciones… ¿Cómo impactan en la industria?

– La industria de la ciberseguridad está evolucionando rápidamente, en respuesta a un panorama de amenazas que cambia a una velocidad vertiginosa. Hoy hay más consolidación que nunca, pero lo importante es que también hay un reconocimiento esperanzador de que la industria tiene que trabajar unida, compartir información y, más allá de las diferencias competitivas, entender que, en última instancia, estamos del mismo lado frente a los actores que pretenden hacer daño.

– Uno de los grandes pilares en los que se cimienta el negocio de Microsoft, también en ciberseguridad, es la IA. ¿En qué se diferencia la aplicación de la IA de Microsoft a la hora de ofrecer seguridad y defensa cibernéticas?

– Microsoft Copilot for Security es más que un modelo de lenguaje grande (LLM) con IA que funciona con su tecnología de seguridad. Se basa en la última innovación en LLM, pero va más allá de eso: aprovecha todo el potencial de nuestra experiencia en seguridad, nuestra inteligencia global de amenazas y las tecnologías de Microsoft para ganar en eficiencia de forma masiva en los casos de uso de seguridad más críticos. Al enviar un *prompt*, Copilot for Security lo mejora con su sistema específico de seguridad basado en un profundo conocimiento de la seguridad de Microsoft y un aprendizaje continuo. El *prompt* se enriquece con nuestro portfolio de productos de seguridad de Microsoft extremo a extremo, con nuestra inteligencia de amenazas -informada por los 65 billones de señales que recogemos- y con el talento humano de Microsoft. Traduce la respuesta de acuerdo a tus instrucciones, tomando la forma de texto o código que te ayuda a ver y entender el contexto completo de un incidente de seguridad, el impacto y los próximos pasos que debes seguir para profundizar en la comprensión de lo que ha sucedido o tomar medidas inmediatas para la remediación y el fortalecimiento de la defensa de tu organización. Por último, Copilot for Security se integra con el portafolio de Microsoft de extremo a extremo, creando un efecto multiplicador para proporcionar una protección integral.

– Recientemente, el presidente de Microsoft, Brad Smith, y el presidente del Gobierno de España, Pedro Sánchez, firmaron un acuerdo de colaboración para la aplicación de la IA en la administración pública y el refuerzo de la ciberseguridad, con una inversión de 1.950 millones

"Estoy orgullosa del trabajo que nuestro equipo ha realizado en Copilot for Security. En la versión preliminar privada, nuestros clientes consiguieron ahorrar hasta un 40% del tiempo de sus analistas de seguridad en tareas fundamentales como investigación y respuesta, búsqueda avanzada de amenazas y análisis de inteligencia de amenazas"

"En Microsoft, vemos la Ley de IA de la UE no como un obstáculo regulatorio, sino como una oportunidad para predicar con el ejemplo en el desarrollo de soluciones de IA que no solo sean innovadoras, sino también éticas y responsables"

de euros. En materia de ciberseguridad, ¿qué supone esta inversión y qué acciones concretas esperan llevar a cabo a corto y medio plazo?

– Definitivamente, este ha sido un anuncio muy importante y relevante, y me complace ver las inversiones que se están realizando. Como parte de la colaboración entre Microsoft y el gobierno español, hemos acordado reforzar la ciberseguridad nacional de España. Microsoft abrirá próximamente una Región Cloud de Centros de Datos en la Comunidad de Madrid y anunciamos nuestra intención de construir un Campus de Centros de Datos en Aragón. Estas dos infraestructuras proporcionarán los servicios en la nube de Microsoft con las máximas garantías de seguridad, privacidad y soberanía del dato, y permitirán poner a disposición de las empresas y Administraciones públicas españolas y europeas toda la oferta de soluciones de IA de la compañía.

Además, con el objetivo de mejorar la seguridad de las empresas españolas y, especialmente, de las pymes, Microsoft colaborará con el Instituto Nacional de Ciberseguridad (Incibe), ofreciendo acceso a la telemetría e información global sobre potenciales amenazas y ciberataques que puedan afectar a las empresas y Administraciones públicas españolas. Asimismo, se establecerán acciones de divulgación conjuntas en el ámbito de la ciberseguridad, dirigidas a pymes y ciudadanos. Por otra parte, con el fin de reforzar, en concreto, la ciberresiliencia de las infraestructuras críticas, Microsoft y el Centro Criptológico Nacional del Centro Nacional de Inteligencia (CNI-CCN) explorarán conjuntamente la mejora de los mecanismos de alerta temprana y respuesta a incidentes de seguridad informática en las Administraciones públicas.

– Y, ¿qué opinión le merece la propuesta para crear un marco regulador de la IA en Europa, la primera del mundo en establecer reglas claras para su uso?

La introducción de la Ley de IA de la UE anuncia un período de transformación para la industria tecnológica. Al clasificar los sistemas de IA en función del riesgo que plantean y esbozar requisitos específicos para las aplicaciones de alto riesgo, la Ley garantiza que las tecnologías de IA se desarrollen y desplieguen de manera que se salvaguarden los derechos humanos y se promueva la transparencia y la responsabilidad. En Microsoft, vemos la Ley de IA de la UE no como un obstáculo regulatorio, sino como una oportunidad para predicar con el ejemplo en el desarrollo de soluciones de IA que no solo sean innovadoras, sino también éticas y responsables. La Ley se alinea con nuestra visión de un futuro en el que la IA permita a las personas y organizaciones lograr más mientras operan dentro de un marco de confianza y seguridad. Microsoft Copilot está a la vanguardia de nuestra respuesta a la Ley de IA de la UE, lo que demuestra nuestra dedicación en la creación de tecnologías de IA que respeten y mejoren la privacidad, la seguridad y el cumplimiento de los usuarios.

– La compañía, además, ha puesto en marcha la 'Iniciativa Futuro Seguro', un nuevo estándar de seguridad que avanza en la forma en que se diseña, construye, prueba y opera su tecnología. ¿De qué depende su éxito o fracaso?

– El éxito de la Iniciativa de Futuro Seguro (SFI) de Microsoft se basa en tres pilares cruciales. Uno de ellos son las defensas cibernéticas basadas en IA, donde aprovecharemos la IA para mejorar la protección contra todas las amenazas, incluso aquellas que están bien ocultas. Mediante el uso de avances impulsados por IA, nuestro objetivo es proporcionar una seguridad más rápida y eficaz. Otro pilar son los avances en ingeniería de software fundamental, donde planeamos lanzar funciones que mejoren la protección, introduzcan nuevos métodos de autenticación y fortalezcan la seguridad en la nube. Estos avances tecnológicos desempeñarán un papel fundamental para asegurar nuestro futuro. Y el tercer pilar reside en abogar por una aplicación más estricta de las normas internacionales para proteger a los civiles de las amenazas cibernéticas. En este sentido, al promover un comportamiento responsable y el cumplimiento de las normas, todos en la industria de la seguridad pueden contribuir a un entorno digital más seguro.

Esperamos que nuestro compromiso público con estos principios actúe como una llamada a la acción para la industria, y que las empresas y los gobiernos se unan a nosotros para tomar las medidas necesarias para darle al mundo el futuro seguro que se merece.

– Por último, usted participa en diferentes iniciativas a favor de la mujer en la ciberseguridad, ¿qué está provocando que el número de mujeres en el ámbito se quede en solo el 25%?

– Si bien estamos avanzando para cerrar esta brecha, es evidente que aún queda mucho trabajo por hacer para fomentar una industria más diversa. En una encuesta que realizamos en los últimos años, descubrimos que hay varios factores, entre ellos: estereotipos de las mujeres y sesgos de género; no hay suficientes mentoras y modelos a seguir en ciberseguridad; oportunidades insuficientes de capacitación y educación; e incertidumbre sobre las posibles trayectorias profesionales en el ámbito de la ciberseguridad. Juntos, el mundo académico, la industria tecnológica y las agencias gubernamentales estamos trabajando en programas y nuevas tecnologías para superar estos desafíos, a la vez que alientan a más niñas a imaginarse en carreras de ciberseguridad. En Microsoft, buscamos fomentar la tutoría, la educación y la participación comunitaria a través de diversas iniciativas tanto internas como externas con organizaciones como Women4Cyber Spain, o como Women in Cybersecurity (WiCyS) y Girl Security, en las que estoy involucrada personalmente. ■

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

+

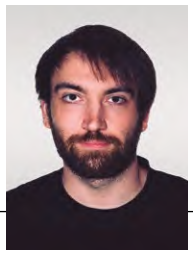
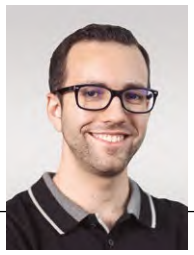
Netskope, líder global en ciberseguridad, está redefiniendo la seguridad de la nube, las redes y los datos, para ayudar a las organizaciones a aplicar principios de Zero Trust y proteger su información. La plataforma inteligente Netskope Security Service Edge (SSE) es rápida, fácil de usar y protege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

Tecnología disruptiva en el SOC: Desafíos de la IA en la Gestión de Incidentes

No cabe duda de que la Inteligencia Artificial ha transformado nuestras vidas, tanto en aspectos cotidianos, como la recomendación de películas y series en los principales servicios de *streaming*, así como en ámbitos profesionales, por ejemplo, en la preparación de informes utilizando servicios como ChatGPT. Dentro del Security Operation Center (SOC), como no podría ser de otra manera, la Inteligencia Artificial está presente, y desde el punto de vista de los autores, transformará de forma integral la manera en que los grupos de respuesta a incidentes trabajan, optimizando la identificación, detección y prevención de amenazas, ofreciendo un enfoque más proactivo y preciso en la gestión de la seguridad informática. Dados los beneficios, la pregunta es clara: ¿Están los actuales SOC preparados para esta tecnología disruptiva? ¿Qué cambios operacionales plantea esta nueva tecnología? A lo largo del artículo, intentaremos dar respuesta a la forma en que el SOC se beneficiará de la IA y a los actuales retos que esta tecnología plantea en términos de detección y predicción.


Nil Ortiz / Albert Calvo / Jordi Guijarro

En términos de detección y prevención, los Centros de Operaciones de Seguridad (SOC) históricamente han utilizado Indicadores de Compromiso (del inglés, *Indicators of Compromise*, IoC) como base para la monitorización, detección y prevención de amenazas. Estos indicadores de compromiso son evidencias obtenidas de forma forense de un ataque. Por ejemplo, si un actor malicioso ataca una infraestructura digital, este dejará trazas de un conjunto de dominios, direcciones IP y hashes, donde el SOC los etiquetará como maliciosos y los pondrá a disposición de la comunidad en forma de IoC a través de plataformas de *Threat Intelligence*. Sin embargo, trabajar con estos indicadores supone adoptar un enfoque reactivo, ya que solo se podrá detectar el ataque cuando ciertos indicadores estén presentes en la infraestructura.

En términos operacionales, esto se traduce en detectar el ataque una vez que ya ha sido iniciado a través de IoC, donde los actuales sistemas basados en reglas, como los sistemas de Detección de Intrusiones (IDS), ofrecen capacidades reactivas ante estos IoC en forma de alertas, ofreciendo capacidades de detección de amenazas en tiempo real. Finalmente, en términos de efectividad, utilizar estos indicadores como pilar del estudio presenta un gran esfuerzo de gestión de la información debido a su alta volatilidad. Los actores maliciosos cambian constantemente los IoC que utilizan para no ser detectados por IDS basados en esta información atómica, por lo que los indicadores suelen tener tiempos de vida cortos, lo cual añade una capa de complejidad extra a la gestión de incidentes y lleva a los operadores de seguridad a destinar muchos recursos en el triaje y evaluación de falsos positivos, aumentando la fatiga de los analistas en entornos de estrés constante.

El uso de datos no controlados para el entrenamiento de los modelos puede llevar a nuestros sistemas a ser vulnerables a ataques de exfiltración mediante puertas traseras insertadas por actores maliciosos, así como la ejecución de código arbitrario en nuestros sistemas, entre otras amenazas.

Con el fin de proporcionar mayor flexibilidad y un análisis más resiliente al tiempo, los analistas de seguridad y grupos de inteligencia de amenazas se centran en intentar capturar la actividad de los actores maliciosos en forma de comportamiento, ofreciendo capacidades analíticas al SOC. En este ámbito es donde la Inteligencia Artificial entra en juego, ofreciendo capacidades preventivas al SOC basadas en el análisis automático de la información. Esto se logra mediante la capacidad de generalizar un conjunto de patrones basados en algoritmos de IA, los cuales son utilizados para detectar y prevenir amenazas de forma proactiva. En este sentido, los sistemas basados en el análisis del comportamiento, conocidos como UEBA (del inglés *User and Entity Behavior Analytics*), se fundamentan en la utilización de algoritmos avanzados de análisis de datos para aprender patrones asociados a comportamientos anómalos, ofreciendo así mayor resiliencia que los sistemas tradicionales basados en reglas.

Los fundamentos de las herramientas UEBA se basan en la analítica del comportamiento en dominios como la psicología, marketing y biología, donde el comportamiento se modela para entender las interacciones entre el universo de estudio. En el ámbito de la ciberseguridad, los sistemas UEBA perfilan el comportamiento base de usuarios y entidades en la red, y señalan como posibles amenazas los comportamientos atípicos o anómalos. Estos sistemas se basan en el análisis exhaustivo de los datos que provienen de los diferentes usuarios y entidades de la organización con el fin de crear un perfilado del comportamiento de estos, generando un modelo de Aprendizaje Automático capaz de asociar ciertos patrones a comportamientos anómalos, como por ejem-

Los sistemas basados en UEBA están empezando a convertirse en una tendencia en los principales SOC a nivel mundial para gestionar los casos de uso más complejos, donde las reglas estáticas suelen producir más fallos.

X-OD

exclusive networks.
on demand.

Bienvenido a la economía de suscripción

www.x-od.com

Transición hacia el modelo as-a-service

El servicio que hará crecer tu modelo MSSP

Un modelo flexible que se adapta a tus necesidades

Cubbit FORTINET paloalto NETWORKS proofpoint. RPOST SentinelOne ThriveDX wasabi

Más información en **marketing_iberia@exclusive-networks.com**

plo un movimiento lateral o un ataque de *malware*. Finalmente, estos modelos se ponen en producción permitiendo la entrega continua de estas anomalías en la infraestructura, permitiendo al analista de seguridad tomar medidas de protección con el fin de reducir la superficie de ataque de amenazas latentes.

Los sistemas basados en UEBA están empezando a convertirse en una tendencia en los principales SOC a nivel mundial para gestionar los casos de uso más complejos, donde las reglas estáticas suelen producir más fallos. En este contexto, el centro de investigación **i2CAT**, enfocado en la investigación e innovación en tecnologías de internet, se ha destacado como pionero en la creación de sistemas UEBA capaces de ofrecer capacidades tanto reactivas como preventivas al SOC. En este sentido, la iniciativa por parte de i2CAT, denominada *detectUEBA* y presente en varios proyectos europeos, se basa en la integración de registros multimodales de aplicaciones con el fin de modelar las anomalías presentes causadas por un actor externo. En esta iniciativa, se utilizan algoritmos semisupervisados y del estado del arte en Deep Learning, siendo piezas fundamentales para la creación de perfiles de usuarios y entidades, permitiendo determinar rangos de normalidad en el comportamiento de los usuarios y detectar automáticamente desviaciones atípicas.

Otra vertiente de UEBA, también iniciativa del centro de investigación i2CAT en colaboración con la **Agencia de Ciberseguridad de Cataluña**, es *preventUEBA*, enfocada en comprender mejor las actividades y comportamientos de cada usuario y entidad. Tiene la capacidad de calcular el riesgo que cada usuario tiene de ser víctima de un ciberataque. Basándose, como no podría ser de otra manera, en el uso de algoritmos de aprendizaje automático, permite crear taxonomías de usuarios, resaltando los sesgos que tienen los usuarios y cuáles de ellos los hacen vulnerables a ataques latentes. No cabe duda que el uso de estas metodologías UEBA supone una gran ventaja de análisis, como se evaluó en el proyecto de *preventUEBA*, realizando un demostrador en una universidad española donde la herramienta fue capaz de dotar al equipo del SOC de capacidades preventivas ante ataques de phishing con una tasa de acierto de alrededor del 75%.

Sin embargo, estas herramientas basadas en algoritmos de IA también plantean retos durante la adopción por parte de los analistas. En primer lugar, está la cuestión de la explicabilidad. Se ha demostrado que si los algoritmos no cuentan con mecanismos suficientes para que el usuario final pueda entender qué predice el algoritmo, este quedará en desuso. Además, el uso no supervisado de estas herramientas puede acarrear resultados no deseados, como la introducción de falsos positivos en el sistema. Esta necesidad también es considerada por la Unión Europea con la IA Act, donde pone de manifiesto la necesidad de dotar a la IA de herramientas para que esta se pueda explicar.

Otro de los retos que introducen las nuevas tecnologías basadas en IA, es la aparición de una nueva superficie de ataque en el entorno a proteger. Dada la alta dependencia de los datos ingresados, al implementar tecnologías basadas en IA también debemos prestar atención al contenido que reciben los modelos tanto en la fase de entrenamiento como en la fase de analítica. El uso de datos no controlados para el entrenamiento de los modelos puede llevar a nuestros sistemas a ser vulnerables a ataques de exfiltración mediante puertas traseras insertadas por actores maliciosos, así como la ejecución de código arbitrario en nuestros sistemas, entre otras amenazas. También es importante vigilar la respuesta que producen los equipos de protección, dado que en

Frente a los retos del futuro SOC predictivo, aspectos estratégicos como la escalabilidad podrán cambiar el centro de gravedad en las arquitecturas de sistemas que han de dar respuesta a esa enorme necesidad de almacenamiento de datos y computación de altas prestaciones. ¿Es el cloud público, o en su derivada los servicios tipo SaaS, una apuesta sostenible?

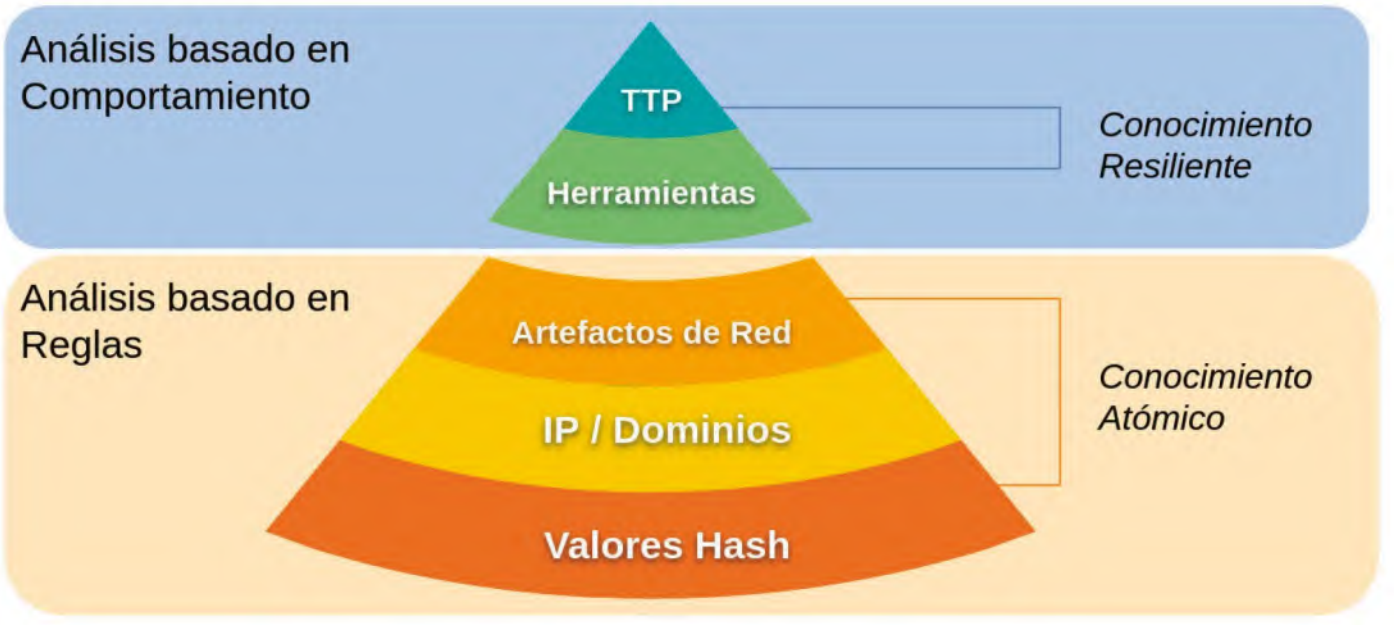


Figura 1.- El uso de sistemas predictivos permite generalizar comportamientos de entidades y usuarios, lo que posibilita obtener indicadores más resilientes en comparación con la utilización de indicadores atómicos, tales como valores hash, direcciones IP o dominios.

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

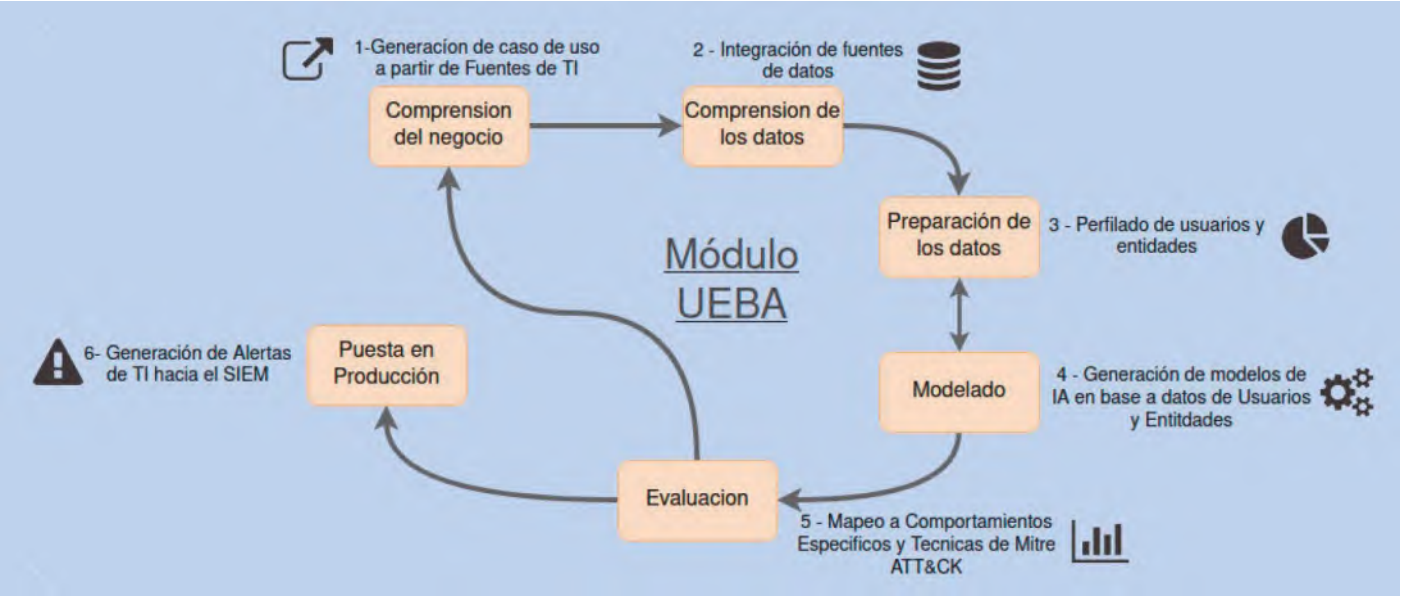


Figura 2.- Los sistemas predictivos se modelan de acuerdo a la metodología Cross Industry Standard Process for Data Mining (CRISP-DM).

los entornos donde se implementan este tipo de tecnologías suelen tener un alto nivel de automatización, sin que necesariamente los equipos responsables tengan visibilidad completa sobre todas las acciones que llevan a cabo las herramientas de respuesta automática.Por ejemplo, un actor externo podría atacar nuestros sistemas como una caja negra, monitorizando qué datos detectan los sistemas UEBA y son bloqueados por los sistemas SOAR, con el fin de desarrollar "payloads" específicos capaces de evadir los sistemas de detección.

Finalmente, el último reto latente es la necesidad de grandes recursos de cómputo que requieren estas aplicaciones basadas en analítica de datos, grandes consumidores de recursos. Hemos pasado de mainframes a PC y redes locales en el pasado, y durante la última década hemos visto una centralización y consolidación de servicios y aplicaciones en centros de datos y la nube pública. A día de hoy, cualquier SOC consolidado tiene unas necesidades crecientes de infraestructura para cubrir los requisitos de las plataformas de preservación de evidencias, de análisis y de detección temprana de anomalías de seguridad, entre otras. Frente a los retos del futuro SOC predictivo, estas necesidades se multiplicarán y es aquí dónde aspectos estratégicos como la escalabilidad podrán cambiar el centro de gravedad en las arquitecturas de sistemas que han de dar respuesta a esa enorme necesidad de almacenamiento de datos y computación de altas prestaciones. ¿Es el *cloud* público, o en su derivada los servicios tipo SaaS, una apuesta sostenible?

En Europa, alrededor de esta incertidumbre y frente a las necesidades crecientes de la digitalización, aparecen iniciativas como el proyecto de interés común europeo sobre infraestructura y servicios de computación en nube de próxima generación (IPCEI-CIS https://digital-strategy.ec.europa.eu/en/news/ipcei-next-generation-cloud-infrastructure-and-services-boost-europes-digital-decade) que permitirá el desarrollo de tecnologías europeas interoperables y accesibles de tratamiento de datos, lo que permitirá la construcción de una nube continua en múltiples proveedores. Dentro de los beneficios, permitirá una mayor eficiencia energética y de recursos. Por ejemplo, permitirá reducir la necesidad de transmitir grandes volúmenes de datos a los servidores cloud centralizados, enfocando una gestión necesaria de la infraestructura en el borde que permita mantener una arquitectura de TIERs en la capa de datos con una visión clara de evitar problemas como los de vendor-lock in.

Pero esto no se queda aquí, acompañar la certificación de esos servicios basados en *cloud computing* bajo paradigmas del "continuum" será vital, donde automatizar y simplificar el proceso de obtención de esos certificados de seguridad ha de ser también estratégico para el futuro SOC predictivo y su catálogo de servicios.

Acompañar la certificación de servicios basados en cloud computing bajo paradigmas del "continuum" será vital, donde automatizar y simplificar el proceso de obtención de esos certificados de seguridad ha de ser también estratégico para el futuro SOC predictivo y su catálogo de servicios.

En esta línea y bajo los futuros esquema de certificación de la Comisión Europea (EUCS) en los cuales ENISA trabaja, existen iniciativas como el proyecto **HE EMERALD** (https://www.emerald-he.eu/) financiado por la Comisión Europea con el objetivo de proporcionar un marco fácil de usar en el campo de la ciberseguridad para gestionar eficientemente las certificaciones, mejorando la seguridad y eficacia del uso de los servicios en la nube.

Las herramientas desarrolladas por EMERALD permitirán simplificar y dar soporte en el proceso de certificación, en el que se denomina Certificación como Servicio (CaaS) aportando la confianza necesaria en entornos de arquitecturas cloud híbridas o multi-nube. ■

Nil Ortiz
Senior Cybersecurity Researcher
i2CAT Foundation
nil.ortiz@i2cat.net

Albert Calvo
Senior AI Researcher
i2CAT Foundation
albert.calvo@i2cat.net

Jordi Guijarro Olivares
Principal Technologist Cloud-Edge Innovation
OPENNEBULA SYSTEMS
jguijarro@opennebula.io

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

PREMIOS 2017

25 referentes y cinco debates convirtieron esta edición de Espacio TiSEC en la gran cita anual sobre los Centros de Operaciones de Seguridad

Sectorización, regulación y certificación, ejes de la pujanza actual de los SOC y MSSP con la IA como pasajera innovadora hacia su futuro

Con casi 500 inscritos asistentes –en formato presencial y en remoto–, la segunda edición de Espacio TiSEC dedicada a los SOC y los MSSP mostró, en primicia, lo crucial de estos actores estelares de la ciberprotección actual. Notables iniciativas sectoriales, públicas y privadas, e internacionales –Red Nacional de SOC, las acciones acometidas en Europa y normativas como NIS2, DORA, CSA y la CRA, la innovación y apuesta por la IA y la especialización, por sectores…– junto con las solventes aportaciones de expertos del ámbito privado y público y de las entidades copatrocinadoras (de un lado, prestadores de servicio como Advens, Aiuken Cybersecurity, DXC Technology, EY, GMV, Innotec part of Accenture, S2 Grupo, SIA an Indra company y Telefónica Tech; y de otro, proveedores tecnológicos con foco en el tema como CrowdStrike, Eset, Sophos y WatchGuard) confirieron a este multitutinario congreso el rango de cita ineludible para desentrañar los nada triviales retos de la cibeprotección hoy.

En menos de un año, el transcurrido entre la anterior edición de TiSEC y ésta, con foco en los Centros de Operaciones de Ciberseguridad (SOC) y prestadores de servicios gestionados de ciberprotección (MSSP) se tiene la impresión, a la luz de las ponencias, de que ha transcurrido una década. El impacto de nuevas tecnologías como la Inteligencia Artificial generativa, la inminente llegada de las primeras certificaciones para este ámbito, tanto por parte del **CCN,** como de **Enisa,** y de otros agentes europeos, los cambios en la Red Nacional de SOC (RNS) o el impacto que tendrá la Ley de Ciberresiliencia, aprobada a finales de año, y la cada vez mayor exigencia sectorial por contar con una protección 'a medida' que entienda el negocio, entre otros muchos aspectos, han marcado las más de 25 intervenciones de esta edición bajo el sugerente lema 'A pleno SOC'.

Durante dos jornadas, el 12 y 13 de marzo, el público más especializado –se superaron los 500 inscritos agotándose las plazas en presencial– disfrutó de la edición y también planteó grandes retos e inquietudes que generaron varios debates de interés. Además, en remoto, se contó con una más que notable presencia de profesionales de Iberoamérica que también están trabajando en desarrollar SOCs públicos y privados y avanzar decididamente en la materia.

Abrió las jornadas el experto **Francisco Pérez Bes**, Socio de Derecho Digital de **Ecix**, quien en su exposición, destacó lo que supone la evolución que exige NIS2, tanto en la gobernanza empresarial como pública, que se aplica "en un momento de estabilidad en Europa" y que permite "incorporar nuevas obligaciones de seguridad y resiliencia, contemplar la ciberseguridad como un buen gobierno corporativo, imponer una responsabilidad personal del órgano de gobierno y garantizar la protección de la cadena de suministro, así como apostar por la colaboración público privada e intercambio de información".

Además, puso en valor los esfuerzos públicos por crear un ciberescudo europeo, legitimar las figuras del CSIRT/SOC ("que no tiene una figura legal como tal, pero sí mucha importancia en NIS2"), fomentar el rol proactivo de los equipos de respuesta sumando su trabajo a la infraestructura de los SOC (European Cybershield), así como reforzar la transparencia en la notificación de incidentes y el intercambio de información.

En cuanto a los prestadores de servicios de seguridad gestionada recordó que la normativa "los considera entidades esenciales o importantes pertenecientes a un sector de alta criticidad", entre otros aspectos, haciendo más complejos los procesos de contratación. Asimismo, destacó que la Ley de Cibersolidaridad pretende "reforzar las capacidades de la UE a través de CSIRT para responder a incidentes, a través de una infraestructura paneuropea para fomentar capacidades comunes", con SOCs nacionales y transfronterizos.

A modo de conclusión recordó que la ciberseguridad camina hacia su conversión en "un aspecto menos técnico para imbricarse en los aspectos de RSE-ESG de las organizaciones".


Francisco Pérez Bes


Vicente González


Miguel Ángel Cañada


Javier Ferre


José Luis Rojo

El papel de Enisa

A continuación, **Vicente González,** experto de la Unidad de Mercado, Certificación y Estandarización de Enisa (agencia que este año cumple 20 años), habló del 'Programa de trabajo evolutivo de la UE para la certificación de la ciberseguridad (URPW): MSSPs y Reserva de Ciberseguridad'. En su intervención, puso en valor la reciente modificación de la Ley de Ciberseguridad (CSA) que permitirá a la Agencia poner en marcha una certificación y esquema para MSSPs, "aunque va a llevar un tiempo" y, posiblemente, tenga mínimos y, también, varios niveles.

Además, repasó las últimas iniciativas del organismo, con importantes partidas dedicadas a la innovación en este ámbito, como la de 23 millones de euros, aprobada en 2022, para impulsar capacidades europeas de gestión y respuesta a incidentes, el esquema europeo de certificación basado en Common Criteria (*EUCC*), que entrará en vigor en 2025, –y que se estudia aplicar en todo tipo de entornos, desde la cartera digital a las eSIM–, hasta el valor de contar con unos perfiles definidos por Enisa en 2023 que buscan facilitar la contratación de los profesionales, con las capacidades adecuadas en este ámbito.

Terminó el primer bloque **Miguel Ángel Cañada**, del **Incibe,** responsable del Centro de Coordinación Nacional de España (NCC-ES) en el **Centro Europeo de Competencia en Ciberseguridad** (ECCC) qué habló del 'Programa Europa Digital: financiación para SOC con aplicaciones novedosas'. Tras mostrar el esquema de gobernanza de ciberseguridad en España, descentralizada, recordó que, entre otras misiones, el Incibe está centrado en apoyar la transformación digital, a partir de lo marcado por la 'Agenda España digital 2026', para generar y fortalecer capacidades de ciberprotección e impulsar el ecosistema en este ámbito, también, de cara a su internacionalización.

Además, mostró de forma pormenorizada las diferentes inversiones en innovación en SOC y MSSP que se están llevando a cabo en Europa a través de la Estrategia para la 'Década Digital' y en las que cobrará mucho peso el ECCC, en coordinación con todos los países.

"El Centro es una oportunidad para la I+D+i en ciberseguridad, ya que se prevé dedicar, hasta 2027, a través de Europa Digital, 1.650 millones para ciberprotección, además de estar incluido este aspecto en el Cluster III, con otros 1.600 millones y haber una partida importante de los 8.000 millones de los que invertirá el Fondo Europeo de Defensa. No faltó una referencia importante a la aplicación de nuevas tecnologías, como la IA, a los SOC que ya está plasmándose en los concursos convocados.

Exigencias de la sectorización

Le siguió un potente bloque focalizado en los 'Servicios gestionados: sectorización y entorno tecnológico'. Moderado por el director de **Revista SIC, José de la Peña**, que se inició con dos destacados socios de **EY** en la materia, **Javier Ferre,** Responsable Europeo de Servicios Gestionados de Ciberseguridad de la firma, y **José Luis Rojo**, al frente del Área de Ciberseguridad. Ambos realizaron una exposición en la que mostraron los retos de la movilidad en ciberprotección y la apuesta por servicios gestionados que hacen desde la firma con más de 200 profesionales dedicados y 10 SOCs. "Apostamos por un modelo de SOC

adaptado a cada cliente, con IA y automatización -para conseguir escalar- y constantemente actualizada", destacó el primero, quien subrayó la importancia de conocer al cliente y su sector específico para ofrecer el servicio que necesita. Además, Rojo expuso que desde EY se considera clave contar con este tipo de centros "para poder transformar la organización, ya que permite ver todo lo que sucede a nivel operativo". En definitiva, es un "modelo de transformación a través de la operación y focalizado en el valor del negocio", añadió, sin olvidar la importancia de "garantizar la resiliencia de procesos críticos con tres pilares como son poner a la persona en el centro, apostando por la tecnología y la innovación".

El valor de la Inteligencia

A continuación, intervinieron el responsable del CERT de la multinacional española **GMV** –que cumple 40 años–, **Oscar Riaño,** y **Raquel García Laguna,** Jefa de Proyecto de la compañía, para hablar de los retos en ciberprotección de los SOC en entornos portuarios. La segunda destacó, de forma especial, los principales ciberriesgos como son los ataques de denegación de servicio, así como los que buscan "el acceso a información crítica, a través de la cadena de suministro, y los que aprovechan vulnerabilidades en dispositivos y en un ámbito donde IT y OT están interrelacionados". Riaño mostró cómo está actuando ya su compañía ofreciendo protección a través de servicios gestionados en varias infraestructuras de este tipo, primando mucho el aspecto preventivo a través de herramientas como Zeek, para monitorización, o Yara, para evaluar posibles fallos y anticiparse a ellos. Además, destacó la necesidad de contar con "inteligencia de amenazas, un marco que permite monitorizar, como DETT&CT, adaptado a cada cliente".


Oscar Riaño


Raquel García Laguna


Óscar Navarro

Roberto Pérez


Vicente Segura

En el turno del sector ferroviario, el director del Área Industrial de **S2 Grupo, Óscar Navarro,** mostró la dificultad de proteger las diferentes infraestructuras que conforman este tipo de entornos –integrados por sistemas de distribución de energía, de gestión y, por supuesto, de los propios trenes–, aunque con muchos elementos compartidos con otros ámbitos OT e IT. De cualquier forma, centró su exposición en SOCs que permitan proteger el "material rodante", donde el reto es "definir los casos de uso", además de tener clara "la interpretación del contexto, una monitorización a través de sistemas embarcados, así como actuar a en el ciclo de operación", siendo necesario contar con "inteligencia y actuando de forma integrada a lo largo de la evolución de los vehículos", primando que los trenes no dejen de funcionar. A modo de conclusión destacó, como clave, la "unificación de la supervisión de todas las infraestructuras". Una ponencia que despertó gran interés por las dificultades técnicas para ofrecer una ciberseguridad gestionada adecuada.

Gestión continua de amenazas

También, la ciberprotección a través de servicios gestionados de las ciudades ocupó un lugar destacado en TiSEC. De la mano de **Roberto Pérez**, Head of Cybersecurity Services & Solutions Business de **SIA, an Indra company,** los asistentes conocieron las implicaciones en urbes conectadas de normativas como ENS 2.0 o NIS2, así como la recientemente aprobada Ley de IA.

En su conferencia, recordó que el reto para las grandes poblaciones es pasar del SOC IT, a uno para protección OT e IoT y que permita relacionar ambos mundos. Un reto complicado por cuanto sus infraestructuras digitales son objetivo en 2024 de "ciberataques potenciados por IA generativa, robo de identidad, incidentes que usan la cadena de suministro como potenciador y el *ransomware*". No faltó en su exposición un análisis a lo que supone la IA en detección y respuesta para maximizar la protección en los servicios gestionados.

Además de apostar por enfoques como el programa de Gestión Continua de la Exposición a Amenazas (CTEM), a modo de conclusión comentó la necesidad de que las administraciones públicas mejoren sus capacidades de prevención, protección, detección y respuesta a incidentes. Y todo ello teniendo claro que "la ciberseguridad no es un producto, es una solución que hay que gestionar y saber sacar partido, evolucionándola del modelo tradicional a uno multicapa en varios niveles".

Cuarta revolución

A continuación, **Vicente Segura,** Gerente de Producto de Ciberseguridad OT&IoT de **Telefónica Tech** abordó las "Infraestructuras OT modernizadas mediante convergencia IT/OT e infraestructuras OT ciberfísicas de nuevo diseño", con gran interés por parte de los asistentes por cuanto analizó las diferentes revoluciones tecnológicas, destacando que, la cuarta, la que ya vivimos, dependerá de los "sistemas ciber-físicos, materializado en fábricas y entornos inteligentes que toman decisiones de forma autónoma, utilizando diferentes tecnologías que se apoyan en la conectividad".

Así, destacó que es vital contar "con una matriz de ciberdefensa, como marco de referencia para identificar y planificar la construcción de contramedidas", además de establecer "una clara separación entre las funciones de seguridad que actúan antes y después de un incidente". Unos retos para los que propuso contar con lo que denominó 'Mission Critical SOC', ya que "para aumentar significativamente la resiliencia de los sistemas ciberfísicos" es vital "coordinar las diferentes contramedidas para que el conjunto actúe como un sistema con visión y capacidad E2E (automatización y orquestación de soluciones y servicios de ciberseguridad)", para mantener "un conocimiento actualizado del entorno y de la postura de seguridad y reaccionar satisfactoriamente".

Enfoque global

Como colofón a este apartado, se celebró un debate entre los ponentes en el que Rojo destacó la importancia de "no perder de vista la amenaza, ya que los cibercriminales no entienden de si la red IT y OT está segregada, por lo que hay que aprovechar sinergias y protegerlo todo", a lo que Pérez también añadió "la necesidad de identificar riesgos y medidas en función del entorno". Por su parte, García Laguna puso en valor las normativas sectoriales, como elemento de mejora, sumándose Segura en cuanto a que "son esenciales, pero no son el único aspecto que tener en cuenta". Navarro también recordó que, en los últimos dos

DEBATE

Evitar la comoditización del SOC, mostrando su valor al cliente

La sesión matinal terminó con un debate conducido y moderado por el Editor de Revista SIC, **Luis Fernández,** sobre 'Los retos en la relación cliente/proveedor de servicios para mejorar la respuesta ante incidentes', en el que participaron dos reconocidos profesionales como el SecArch & SOC Manager de **Admiral Europe Tech-Admiral Group**, **Jorge Hurtado,** e **Iván Sánchez,** CISO Global de **BUPA**.

Entre otros aspectos, Sánchez destacó la necesidad de que las empresas "entiendan y perciban el valor del SOC, midiendo lo que aporta, respondiendo a incidentes y entendiendo el modelo de negocio, "ya que no se puede vivir sin él". "Y si cuenta con un sello de certificación, mejor que mejor". Hurtado también consideró en este tipo de Centros que es fundamental contar con la empatía entre el cliente y proveedor, ya que "los 'SOC enlatados' no me gustan". De hecho, adelantó que está trabajado "en un modelo de SOC con IA generativa que permite ganar eficiencia a la hora de responder, generar casos de uso y reducir falsos positivos".


Jorge Hurtado e Iván Sánchez

También, destacaron la importancia del cambio de la Ley de Ciberseguridad que recientemente ha incluido los servicios gestionados y de las nuevas certificaciones que llegarán para SOCs, "aunque no es lo vital", añadió Hurtado, porque "hay que desterrar el 'concepto de centro de operaciones de ciberseguridad de talla única", dijo Sánchez. Ambos apostaron por disponer de este tipo de servicios "creando un valor tangible" y huyendo de la "industrialización", evitando "la comoditización", recordando que "cada vez se pide más con el mismo presupuesto".

o tres años, cada vez hay más demanda de servicios de ciberseguridad y más concienciación en las empresas.

Todos destacaron la necesidad de adecuar el grado de ciberprotección a la madurez de cada organización, aprender de lo hecho y ganar madurez, incluso, a partir de errores, apostando por una mayor monitorización en la que se prime lo crítico y relevante. Igualmente destacaron la necesidad de mejorar la compartición de información, aunque "aún hay camino por recorrer", ya que consideran que "muchas situaciones se basan en la confianza de las partes", que sigue siendo determinante.

La visión de los fabricantes

La sesión vespertina se centró en las tecnologías orientadas a la ciberseguridad gestionada, de mano de algunos de los fabricantes de referencia, como es **CrowdStrike**. Su Senior Sales Engineer para Iberia, **Álvaro García**, subió al estrado para explicar la propuesta de la compañía a través de dos 'olas' de innovación. La primera llegó con un cambio de visión en un momento en el que "se diseñaban las cosas por silos", para pasar a una estrategia fundamental: "el incidente es lo primero", explicó. Para ello, se pusieron todas las herramientas funcionales para poder entender y responder al incidente. Esto se tradujo, entre otros aspectos, en el desarrollo de su reconocida plataforma CrowdStrike Falcon, "que representa muy bien el mantra de la empresa: si tienes un incidente tienes que ser capaz de detectarlo en un minuto, de entenderlo y responderlo en 10 minutos y de procesarlo en 60", destacó.

Para hacer eso posible, en 2013, se dio paso a una segunda ola (2nd Wave), que consistió en hacer una plataforma abierta, abarcando todo el contexto que pueda proporcionar, también, el ecosistema del cliente e industrializarlo. Es decir, "coger esa telemetría e incorporarla al ciclo de la detección que nosotros ya hacíamos muy bien con el *endpoint*".

Terminó resumiendo, entre otros aspectos que, "al final, hay veces que hay que trabajar e innovar mucho para seguir manteniendo constante tu objetivo, y el nuestro es y siempre ha sido el mismo: detectar lo antes posible un incidente y gestionarlo lo mejor posible: el mantra 1-10-60", concluyó.


Álvaro García


Carlos Tortosa


Alberto Ruiz Rodas


Miguel Carrero

A continuación, **Carlos Tortosa**, director de Grandes Cuentas de **Eset España**, cogió el testigo para profundizar en la propuesta de la firma dirigida a los SOC. El directivo recordó que, en 1992, la multinacional lanzó la primera solución de ciberseguridad y, que, en la actualidad, posee 13 centros de I+D, "consiguiendo una red neuronal que nos provee de mucha información y que gestionamos de cara al cliente final, en este caso, también como servicio dentro de cualquier SOC, a nivel de inteligencia", puntualizó.

Entre otros aspectos, resaltó que el enfoque de seguridad de la compañía se basa en varios niveles y en cuatro principios: confianza, alta detección, bajo impacto en el rendimiento y facilidad de uso. Con todo esto, "fabricamos Eset LiveSense, que se nutre de tres partes principales; Eset LiveGrid, el *machine learning* y la experiencia de nuestros expertos". Y, precisamente, basada en LiveSense destacó la herramienta Eset Threat Intelligence, en la que Tortosa centró su ponencia, ya que, con ella, "generamos una serie de *feeds (botnets*, dominios, URLs, archivos maliciosos, IPs y APTs) que facilitamos a los SOC en un formato servicio para ser proactivo frente a las amenazas. También, puso en valor las capacidades de gestión y terminó subrayando que "lo más importante, no es sólo contar con herramientas potentes con alto ratio de detección y de protección, sino también, contar con el talento necesario".

Acto seguido, **Alberto Ruiz Rodas**, director de Ingeniería Preventa para España y Portugal de **Sophos**, ahondó en la visión de la compañía, indicando que "está bien tener un sistema XDR, pero de nada sirve si los pilares fundamentales no son fuertes, si no tenemos un buen sistema que reduzca la superficie de exposición, si no podemos bloquear la actividad maliciosa o que el propio *endpoint*, de forma autónoma, pueda realizar acciones de mitigación adaptando el nivel de severidad en relación a lo que el *endpoint* interpreta que está sucediendo". "Es importante hacer la distinción de que detección no es protección", resaltó poniendo en valor el *marketplace* de la compañía, "con el que recibimos telemetría de terceros".

No se quiso olvidar del "Notebook para que en los SOC puedan escribir sus notas, enriquecer los datos y, sobre todo, para que también puedan contar con una visión que les permita entender qué está sucediendo para realizar una acción". Además, "estamos añadiendo IA para detectar, por ejemplo, líneas en PowerShell que puedan ser maliciosas, entre otras funcionalidades". Y, "por supuesto, un SOC necesita automatizaciones y tenemos una API muy potente para automatizar lo máximo posible ese día a día en el SOC", puntualizó.

Para finalizar este bloque, **Miguel Carrero**, vicepresidente Secure Service Providers and Strategic Accounts de **WatchGuard,** expuso su propuesta de valor a través de la reflexión sobre las cosas que cambian y las que no, en este ámbito. Para ello, empezó por lo segundo, "lo que no ha variado es la función del SOC". Para el directivo, lo que sí ha cambiado son "las capacidades de ciertas tecnologías de habilitar y facilitar la labor de los profesionales". En este sentido, destacó el concepto de NDR (*Network Detection and Response*). Y es que, para la compañía, "la red no ha desaparecido, sino que ha cambiado, y es donde sigue habiendo mucha riqueza en esa telemetría".


Pablo Fernández

Así, y para potenciar sus capacidades, WatchGuard compró la firma CyGlass en septiembre pasado, que amplía la detección y respuesta de red basadas en IA y Open XDR. Esta operación permitió el impulso de la solución WatchGuard NDR.

Junto a ello, recordó la importancia de la Plataforma de Seguridad Unificada de la compañía, "donde la adquisición aporta elementos en la parte de gestión, seguridad de red, en la que no solo es protección sino también telemetría para detección y respuesta, y, además, nos permite abrirnos a terceros ya que se basa en protocolos de red conocidos".

Carrero también destacó la propuesta de la compañía en XDR, girando especialmente en torno a la red, identidad y el *endpoint*.

Red Nacional de SOC y retos

El comienzo de la segunda jornada se inició con la aportación de **Pablo Fernández,** Experto del Área de Centro de Operaciones de Ciberseguridad del **CCN**, quien disertó sobre la 'RNS: la herramienta de colaboración e intercambio del sector público y sus proveedores que no para de crecer'. En su intervención destacó que esta red de SOC ha supuesto un "cambio de enfoque" porque "hay tantos ataques que no damos abasto: sólo en 2023 se gestionaron más de 105.000 incidentes, siendo 120 críticos, aunque menos que los 139.000 de 2021".

Fernández repasó las diferentes iniciativas del CCN en este ámbito y mostró, en primicia, los cambios que desde marzo experimenta-

DEBATE

La importancia del conocimiento experto, la cercanía al cliente y al entorno que se protege en un SOC

La primera jornada del evento se completó con un postrer y dinámico debate, moderado por **José Manuel Vera**, redactor de **SIC**, que contó con los cuatro representantes de las empresas fabricantes. Una de las preguntas que generó más interés fue conocer cuál es la fórmula secreta que marca la diferencia entre un SOC que funciona y uno que vende humo. El primero en contestar fue **Álvaro García** (**CrowdStrike**), quien señaló que "la eficiencia de un SOC se demuestra, especialmente, cuando tienes un incidente", añadiendo, tras una reflexión, que "quizá reside en hacer un paquete de tecnologías y capital humano con gran conocimiento". De igual forma opinó **Miguel Carrero** (**WatchGuard**), quién apuntó que "lo complicado es el conocimiento profundo de las tecnologías, pero, también es la cercanía del entorno que estás protegiendo". **Carlos Tortosa** (**Eset España**) manifestó, de igual forma, que "es necesario conocer muy bien las tecnologías que estamos manejando y conocer muy bien las necesidades del cliente". "Hay que encontrar ese equilibrio", matizó. Por su parte, **Alberto Ruiz Rodas** (**Sophos**) dijo "no sé la fórmula secreta, pero los ingredientes al menos están claros. En nuestro caso, la telemetría de Sophos que nutre nuestros sistemas, aderezada con IA, más nuestros expertos que nos permiten dar el apoyo que los SOC necesitan".

Álvaro García, Carlos Tortosa, Alberto Ruiz Rodas y Miguel Carrero

Además, entre otras cuestiones se ahondó en lo que se puede automatizar o no se puede delegar a la IA, destacando que, a día de hoy, se sigue requiriendo la labor humana para ciertas tareas. Para concluir, se pidió a los cuatro que, desde su visión de fabricantes, dijeran cuáles son sus supersticiones que habría que desterrar. Para García claramente fue "no vas a conocerme como yo me conozco". Para Tortosa, más que superstición, "sería más una cuestión de criterios, necesito conocer bien aquello que voy a contratar porque al final voy a dar mis datos". Ruiz Rodas explicó que "más bien nuestra pata de conejo es que, en vez que nosotros tomemos acción, te decimos lo que tienes que hacer". Carrero habló sobre si se está colaborando o no se está colaborando de verdad entre cliente y proveedor. Así, respondió que "es más bien un mito, ya que esa colaboración se ve –y es de verdad–, con muy buenos resultados… pero no se percibe tanto como se debería".

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

DEBATE

La IA como potenciador, ante el déficit de profesionales y la necesidad de especialización

La segunda jornada de TiSEC también contó con un clarificador debate orbitando alrededor de la cuestión 'Hacia dónde se dirige la especialización en ciberseguridad gestionada: personas, sistemas IA y SOCs', en el que participaron **David Marqués**, Jefe de Operaciones de **Advens Iberia** –compañía que próximamente se sumará a la RNS–, **Mikel Salazar,** Director de Ciberseguridad de **DXC Technology**, y **Javier Sevillano,** SOC Director de **Innotec Security part of Accenture**.

Conducido por Luis Fernández, editor de SIC, en él, todos los participantes destacaron la importancia de la certificación en este ámbito, "aunque también nos obsesiona poner al cliente en el centro para entender sus riesgos y que el SOC sea el brazo armado de los equipos de ciberseguridad, del CISO, de los clientes, para poder responder y proteger", comentó Salazar. Sevillano sí quiso reconocer que los SOC viven ya en un "proceso de madurez", coincidiendo con Marqués, "aunque hay que huir del concepto de comprar 'SOC a kilos', que citó Roy en la anterior intervención".


David Marqués, Mikel Salazar y Javier Sevillano

Tras coincidir en que el sector público les supone en torno al 20% aproximadamente de su negocio todos destacaron la necesidad de apostar por la especialización. "Ya no hay 'Leonardos da Vinci' que saben hacer de todo porque cada sector exige saber de unas técnicas de trabajo, de monitorizar, de superficie de ataque", dijo Sevillano reconociendo Salazar que, por esa variedad de profesionales, "los SOC son factorías increíbles de formar profesionales". Además, destacaron a la IA como un potenciador de los diferentes roles que trabajan en estos Centros y, también, para paliar el déficit de profesionales que hay en el mercado.

Marqués, además, intervino poniendo en valor "la empatía con los empleados, cuidándoles para mantenerlos, además de facilitar su formación y crear vínculos basados en los valores de la empresa", más allá del aspecto económico en el que coincidieron que "se debería pagar más". Y también corroboraron todos que las certificaciones de los SOC no harán que se pueda pedir más por sus servicios y que la clave, en imparable *crescendo* "es la sectorialización, así como la cercanía con el cliente local".

rá la Red, permitiendo el acceso a entidades que no dan servicio al sector público, como es el caso de muchos SOCs de empresas del Ibex, ya que se apostará por integrar en ella a "cualquier compañía que proteja activos españoles". También, se abrirá la participación a proveedores que no den este servicio como tal, "como **Google** o **Microsoft**".

Además, se "ha creado una sección de proveedores, divididos en categoría Oro y Plata", según la cantidad de indicadores de calidad que compartan. Y, recordó el éxito de la RNS, que está siendo muy seguida en Europa, y que ya cuenta con 168 SOCs adheridos y con 57 proveedores (42 de oro y 11 de plata), aunque también hizo énfasis en que se va a echar a cuatro empresas -que denominó socios 'inhabilitados'-. "Si no se comparte nada, es mejor irse de la RNS".

Certificación de los MSSP y los SOCs

Fernández, también acometió la siguiente ponencia sobre el camino "hacia un esquema de certificación de Centros de Operaciones de Ciberseguridad". "Esto va de ser o no ser: si ser un SOC o no". En este sentido, recordó que "no es un SOC: no basta tener un EDR o un antivirus, ni con certificaciones como ISO 27001 o ENS; si no tienes personas a cargo de mirar los eventos y de hacerles frente, no tienes un SOC". Por ello, el CCN está poniendo en marcha una certificación que, de momento, tendrá el carácter de validación -denominada CCN-STIC 896-, con dos niveles de reconocimiento 'Básico' y 'Avanzado', y que espera que sea admitida en toda Europa acorde a la que haga Enisa u otras entidades públicas. Eso sí: será, posiblemente, la primera en este ámbito (esperan que se pueda obtener desde abril), y permitirá "medir las capacidades básicas de los servicios gestionados". Su objetivo es que "cualquier administración que quiera contratar con un proveedor de servicios de ciberseguridad pueda tener la certeza de unos mínimos". Además, adelantó que estará basada en disponer de 31 controles generales –que no habrá que demostrar si se tiene el ENS medio– y validar unos servicios concretos.


Tomás Roy

Le siguió el Director de la **Agencia de Ciberseguridad de Cataluña, Tomás Roy,** con una ponencia sobre las 'Implicaciones de la observabilidad en los servicios de ciberseguridad gestionada' que comenzó recordando que su organismo de ciberprotección autonómica anunció en marzo la convocatoria del nuevo modelo de aprovisionamiento y contratación pública de ciberseguridad, por 230 millones a cuatro años, para servicios externalizados. A continuación, centró su exposición en la importancia de disponer de un SOC de aplicaciones, basándose ya en una experiencia piloto que ha acometido junto con **Factum,** porque es "vital contar con capacidades de detección y respuesta a nivel de aplicación, que es uno de los principales vectores de ataque y cada vez será mayor". Así, entre sus conclusiones, subrayó la importancia de acometer las "evidencias que tenemos de problemas en el código de la aplicación, que no se han podido reducir por su complejidad y apostar por la monitorización". También, señaló la necesidad de ampliar el catálogo de amenazas de ciberseguridad, de acuerdo con los nuevos casos que se producen en la capa de aplicación y reducir el riesgo de uso de librerías vulnerables", entre otros aspectos, apostando por implicar a todos los actores en "los procesos para implantar en el SOC de aplicaciones".

'Autonomous SOC'

La jornada prtosiguió con una exposición del CEO de **Aiuken Cybersecurity, Juan Miguel Velasco,** sobre los 'MSSP+SOCs y el ecosistema de ciberseguridad tecnológica: sinergias y fricciones', en la que se mostró convencido de que la IA "no va a sustituirnos", pero sí será un multiplicador. De hecho, su apuesta es por la verticalización en ciberseguridad,

"El 44% de los directivos españoles no prioriza la ciberseguridad porque el lenguaje empleado en el sector es confuso"

europa press *30 de Mayo de 2023*

¿Le parece confuso?

Si puede entender esta imagen, no tiene excusa.

Dele a la ciberseguridad la prioridad que se merece

- para su **organización**
- para gestionar los **riesgos de proveedores**

Descubra los servicios de calificación de ciberseguridad de **LEET Security**.

LEET SECURITY info@leetsecurity.com www.leetsecurity.com 91 579 81 87

DEBATE

Compartición de información, para hacer frente al cibercrimen, basada en la confianza y siempre condicionada al negocio

Como culminación final de esta edición, TiSEC albergó un debate –moderado por José de la Peña–, sobre las 'Alternativas para aumentar la velocidad y la escala de intercambio de inteligencia de amenazas entre todos los actores concernidos', a cargo de **Julia Perea,** Directora de Seguridad digital de **Telefónica España**, y **Everson Nunes,** Head of Cyber Threat Detection en **Santander Digital Services**.


Julia Perea y Everson Nunes

En él, Perea comenzó explicando que para profundizar en el tema propuesto había hecho una 'batida de preguntas' a grandes expertos del sector, habiendo "unanimidad en la necesidad de colaboración". Así puso en valor la Inteligencia en el ámbito cibernético "apostando por la automatización" para "favorecer la toma de decisiones". Nunes recordó que, sectorialmente, ya se hace de forma intensa "a través, por ejemplo, de nuestro ISAC financiero", resaltando ambos la importancia de la calidad de lo que se intercambia "evitando que sea 'a granel". También, destacaron que frente a esta apuesta por compartir hay, en muchas ocasiones, limitaciones del negocio, legales, temor a multas por dar a conocer un incidente, etc. Además, se destacó que para muchas compañías y MSSP la inteligencia tiene un coste en fuentes, analistas, servicios para ofrecer el máximo valor a sus clientes y se mide lo que se da gratis como tal. "Se trata de un equilibrio que, a veces, es complicado", destacaron.

Perea recordó iniciativas privadas como la **Cyber Threat Alliance**, de la que forma Telefónica "y en la que hay un ranking de quién comparte y quién no". También se destacó que, en ciertos sectores, como banca y 'telco', sí hay un nivel alto de compartición para hacer frente a las ciberamenazas que afectan a varias empresas "porque toda la gente sabe que vamos en el mismo barco", destacaron recordando que normativas como DORA incentivan este aspecto.

"huyendo de la tiranía de los fabricantes" y enfocándose en la denominada *Cybersecurity Mesh Architecture* (CSMA).

Así, también destacó cómo su compañía está probando diferentes aplicaciones de IA generativas comerciales, como Microsoft Copilot, "que si se entrenan van ganando calidad de respuesta". Y recordó que ante el déficit de profesionales "hay que automatizar" e intensificar el uso de SOAR. Sí se mostró convencido de que ciertos roles en el SOC desaparecerán por la IA "como el nivel 1", y que esta tecnología, que permite ir ganando fiabilidad cuando se entrena, suple el problema de la "rotación de empleados", los cuales, se llevan un *know-how* que de esta forma se queda. "La IA igual no reduce personas, pero sí nos hará más fácil y eficiente trabajar, por ejemplo, reduciendo los falsos positivos". En definitiva, mostró su apuesta por el 'Autonomous SOC', capaz de automatizar muchas tareas de detección, triaje, mitigación, escalabilidad, y todo desde la nube.

Respuesta autónoma

Continuó una exposición el repetidas veces empredendor y hoy fundador y CEO de **Onum, Pedro Castillo** sobre el 'SOCless: Nube, automatización, IA y analítica avanzada. Verdades y mentiras' quien comenzó destacando "lo que hay en común entre todas las aplicaciones: el dato", recordando que ello hace que "la ciberseguridad tenga que estar en todo lo que rodea a los dispositivos".


Juan Miguel Velasco


Pedro Castillo

Con una divertida exposición, basada en la conocida película 'El bueno, el feo y el malo', mostró la necesidad de centrarse en los datos críticos, "los que realmente importan para el negocio" y alertó de que la IA vive un momento "de *hype* y luego puede llegar la decepción, porque lo que pasará es que estará integrada, de forma natural, en todo lo que nos rodea. Aunque falta tiempo". Además, alertó de la cantidad de recursos para desarrollarla y entrenarla que está invirtiendo el cibercrimen en ella. También, de que puede "quitar profesionales de las ocupaciones más básicas, pero hará que se demanden otros de las más especializadas, por lo que la cuenta de resultados igual no cambie tanto". Frente a todo ello, apostó por la concienciación, la formación y la colaboración para reforzar el trabajo de los SOC.

Concluyó mostrando labores que la IA permitirá hacer mejor, tales como responder a las amenazas, y "contar con una mitigación y detección proactivas", además de todas que reforzarán el trabajo actual de los profesionales. ■

En los tres últimos años la presencia femenina se ha mantenido estable en un 15%, según un estudio de Cybershark Recruitment

Los salarios de ciberseguridad, en Reino Unido, crecen más de un 9%, reduciéndose el trabajo en remoto y apostándose más por la promoción interna

"Decir que el futuro y la economía son inciertos en este momento es quedarse corto; sin embargo, creemos que las necesidades de las empresas deben satisfacerse con un nuevo enfoque de contratación". Así lo destaca el gerente de la compañía de contratación de perfiles de alto nivel **Cybershark Recruitment, Daniel Murray,** en la presentación del informe anual que realiza sobre los salarios en Reino Unido en el sector, a partir de un cuestionario confidencial a más de 2.300 profesionales, de ellos 14% mujeres.

Crecen los sueldos

La investigación destaca que el crecimiento medio de los sueldos ha sido de un 9,7% en el último año, así como que la antigüedad media de las personas en un mismo puesto se redujo de 24,05 meses a 23,25 este año.

Por distribución de la fuerza laboral, el sector de servicios bancarios/financieros ha pasado del 21,97% al 23,12%, las empresas tecnológicas del 30,94% al 25,58% en contraposición a las consultoras que crecen del 9,42% al 11,24%.

En cuanto a las áreas que más incrementaron los salarios de sus expertos, las cuatro más llamativas fueron las de Infraestructura Nacional Crítica, forensía digital, gestión de identidad y acceso, y gestión de continuidad de negocio. Además, tras la pandemia, el informe destaca que cada vez más gente apuesta por el trabajo presencial, "ya sea en modo híbrido o totalmente *in situ*".

Presencia femenina

En cuanto a la presencia femenina, el informe destaca que en los tres últimos años, se ha mantenido constante rondado el 15%, aunque también pone en valor que se constata que muchas empresas "están implementando programas de inclusión y

Salarios y evolución, según el área profesional, en ciberseguridad en Reino Unido (en euros)

• (Datos insuficientes)

	1-3 AÑOS	DIF. ANUAL	4-6 AÑOS	DIF. ANUAL	7-9 AÑOS	DIF. ANUAL	10-12 AÑOS	DIF. AÑOS	13-15 AÑOS	DIF. ANUAL	16-18 AÑOS	DIF. ANUAL	19-21 AÑOS	DIF. ANUAL	21+ AÑOS	DIF. ANUAL	DIF. ANUAL PROMEDIO
GOBERNANZA, RIESGO Y CUMPLIMIENTO	43.203 65.388	-2.56%	72.978 89.617	-5.00%	85.822 103.337	0.00%	87.574 100.126	-2.33%	122.603 145.956	17.65%	122.603 145.956	5.26%	134.279 163.471	0.00%	186.824 274.397	7.14%	2.52%
ARQUITECTURA DE CIBERSEGURIDAD	66.556 84.071	0.00%	78.816 96.331	0.00%	105.088 122.603	-11.76%	113.262 137.782	7.69%	131.360 151.794	-12.50%	134.863 164.054	0.00%	178.066 204.338	12.50%	204.338 256.882	0.00%	-0.51%
INGENIERO DE CIBERSEGURIDAD	58.382 70.059	17.65%	70.059 87.574	0.00%	87.282 105.088	-6.15%	99.834 119.100	10.00%	122.603 140.118	0.00%	134.279 157.632	0.00%	140.118 163.471	0.00%	•	•	3.07%
RESPUESTA A INCIDENTES	51.960 72.978	-2.70%	68.307 85.822	0.00%	93.412 116.765	14.29%	104.504 126.690	5.56%	122.603 145.956	14.29%	131.360 157.632	0.00%	151.794 186.824	0.00%	•	•	4.49%
ANÁLISTA DE CIBERSEGURIDAD	43.787 61.301	-6.67%	55.463 70.059	-7.37%	75.897 93.412	-0.80%	84.654 99.250	-5.86%	96.331 110.926	+5.00%	105.088 122.603	+0.00%	116.765 140.118	-12.00%	•	•	4.49%
e-DISCOVERY	40.868 52.544	•	62.761 80.276	•	74.437 91.952	•	84.071 100.126	•	113.262 136.615	•	121.435 143.621	•	•	•	•	•	•
SEGURIDAD DE RED	40.868 55.463	0.00%	56.631 72.394	8.00%	72.978 89.909	-3.33%	85.238 99.250	20.00%	90.493 108.007	0.00%	101.585 122.603	2.35%	110.926 134.279	0.00%	140.701 163.471	11.43%	4.81%
INTERNET DE LAS COSAS	46.122 61.885	-10.00%	62.469 75.313	10.00%	72.978 89.909	0.00%	88.157 103.337	4.00%	108.591 134.279	10.00%	•	•	•	•		•	
INFRAESTRUCTURA NACIONAL CRÍTICA	43.787 61.301	15.38%	58.382 72.978	25.00%	72.394 89.909	3.45%	93.412 108.007	25.00%	105.672 125.522	-2.86%	119.684 140.118	0.00%	130.776 148.875	3.33%	134.279 157.632	0.00%	8.66%

diversidad étnica y de género en sus negocios". De cualquier forma, aún hay "una disparidad entre los salarios de hombres y mujeres", aunque, "como el año pasado, la brecha se está reduciendo": mientras que los de las mujeres han crecido un 11,5%, el de los hombres ha subido un 8,9%.

En cuanto a las razones para lograr un incremento salarial, continúa en primer lugar la de cambiarse de trabajo, aunque se ha reducido. En concreto, los candidatos que lograron un aumento salarial de más del 26% bajaron del 25,71% al 19,89%.

Asimismo, el número de personas que reciben aumentos salariales de hasta el 10% dentro de su organización, ha crecido del 36,8% al 41,7%. También, es llamativo que los profesionales "sin aumento salarial" han pasado del 19,3% al 23,5%. Dicho de otra forma: casi una cuarta parte del mercado no obtuvo un aumento salarial alguno.

Cambio de empresa

El documento también analiza las causas que puede llevar a los profesionales a cambiar de empresa y destaca que el dinero no es una prioridad. "Las estadísticas muestran que cualquiera que acepte una contraoferta tiene un 50% más de probabilidades de regresar al mercado dentro de tres meses y un 75% más de probabilidades de regresar al mercado dentro de seis meses. Esto se debe al hecho de que los problemas, que podrían ser la falta de progresión, de responsabilidades, problemas con la dirección, un colega, el sector, el equilibrio entre vida personal y laboral, no cambian cuando se acepta una contraoferta".

En cuanto a la apuesta por el trabajo completamente en remoto volvió a bajar este año del 49,7% al 44,6% –especialmente en el formato de 'cuatro días desde casa' que pasó del 49,7% al 20,02%– "lo que indica que se está apostando por tres días en la oficina y dos desde casa o viceversa". En cuanto a las vacaciones, los profesionales del sector tuvieron de media 26,14 días excluyendo festivos y este año se ha producido un ligero incremento hasta los 26,64 días.

También es de interés que el 60,24% de los profesionales reciben una bonificación relacionada con el desempeño. Si también incluimos el bono garantizado, el 75,38% sigue recibiendo bonos, lo que representa una parte considerable del mercado. Destaca, eso sí, que se han reducido algunos incentivos como los coches de empresa o la cantidad dedicada para pensiones no contributivas, apartados que el informe considera que irán decreciendo año tras año.

Búsqueda de nuevo rol

El documento explica que, en lo relativo a personas dispuestas a cambiar de rol, se pasó del 22,42 % el año pasado al 31,52 % y que la promoción interna se redujo del 10,31% al 8,99%. Además, por primera vez en las tres ediciones de este estudio, se aprecia 'un aumento del salario básico' pasando del 23,77% de los encuestados que exigían un aumento al 24,98%. Asimismo, es revelador que el 49,32% de los encuestados cambió de rol en el último año, frente al 75% del anterior, lo que da crédito a la "gran dimisión" del año pasado que se hizo pública. Así, según los participantes, la permanencia en la empresa se está acortando pasando de un 24,6% el año pasado, los que llevan más de cuatro años en la compañía, a un 20,48%.

Así, el informe, como conclusión, apuesta por un año con menos cambios que otros en este sector por cuanto "el clima económico parece haberse calmado" tras un mercado que ha vivido muchas fusiones y compras buscando la eficiencia. ■

Salarios y evolución, según el área profesional, en ciberseguridad en Reino Unido (en euros)

• (Datos insuficientes)

	1-3 AÑOS	DIF. ANUAL	4-6 AÑOS	DIF. ANUAL	7-9 AÑOS	DIF. ANUAL	10-12 AÑOS	DIF. AÑOS	13-15 AÑOS	DIF. ANUAL	16-18 AÑOS	DIF. ANUAL	19-21 AÑOS	DIF. ANUAL	21+ AÑOS	DIF. ANUAL	DIF. ANUAL PROMEDIO
INTELIGENCIA DE AMENAZAS	46.122 64.221	3.33%	64.221 81.735	20.00%	84.071 102.169	3.33%	99.250 116.765	20.00%	108.007 134.279	0.00%	122.603 143.037	0.00%	128.441 145.956	0.00%	140.118 163.471	0.00%	5.83%
TEST DE INTRUSIÓN	57.799 72.978	4.00%	70.643 84.946	-12.50%	105.672 128.441	11.43%	128.441 145.956	0.00%	140.118 163.471	0.00%	•	•	•	•	•	•	0.59%
AUDITORÍA DE RIESGO Y TI	40.868 55.463	-7.41%	58.382 75.897	0.00%	76.481 96.331	13.33%	87.574 105.088	0.00%	99.250 116.765	-9.09%	108.007 128.441	0.00%	116.765 134.279	-14.29%	128.441 150.043	0.00%	-2.18%
GESTIÓN DE IDENTIDAD Y ACCESOS	49.041 64.221	30.00%	66.556 82.319	8.00%	78.816 96.331	20.00%	89.909 110.926	20.00%	105.088 128.441	0.00%	111.510 137.199	10.00%	122.603 140.118	-25.00%	140.118 169.309	25.00%	11.00%
CIBERRESILIENCIA	40.868 55.463	0.00%	52.544 70.059	20.00%	75.897 93.412	3.45%	81.735 96.331	25.00%	105.088 122.603	-21.05%	113.846 131.360	0.00%	122.603 140.118	0.00%	140.118 175.147	-14.29%	1.64%
GESTIÓN DE CONTINUIDAD DE NEGOCIO	37.949 55.463	20.00%	54.879 64.804	13.33%	66.556 81.735	30.00%	82.319 99.250	0.00%	87.574 105.088	0.00%	113.262 134.279	-10.00%	122.603 140.118	0.00%	140.118 169.309	25.00%	9.79%
CIBERSEGURIDAD EN NUBE	47.290 67.724	9.38%	67.140 89.909	11.43%	83.487 108.007	5.00%	100.418 126.106	10.00%	122.603 140.118	-25.00%	145.956 163.471	0.00%	151.794 186.824	20.00%	210.176 262.721	12.50%	5.41%
SEGURIDAD DE APLICACIONES	52.544 71.226	6.67%	66.556 82.319	8.00%	81.735 99.250	0.00%	96.915 122.603	10.00%	108.007 134.279	12.50%	134.279 157.632	0.00%	145.956 175.147	0.00%	180.985 216.015	0.00%	4.65%
DEVSECOPS	49.625 66.556	3.57%	70.059 87.574	0.00%	84.654 105.088	16.67%	110.926 124.938	20.00%	136.615 158.800	-5.00%	166.390 188.575	-5.00%	•	•	•	•	5.04%
FORENSÍA DIGITAL	47.290 67.724	16.67%	67.140 81.735	25.00%	83.487 108.007	40.00%	100.418 123.771	33.33%	122.603 140.118	-25.00%	145.956 163.471	-25.00%	151.794 186.824	0.00%	•	•	9.29%

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]

La necesidad de las organizaciones de ciberprotegerse les da más peso para influir en las juntas, según Ians Research y Artico Search

La presión regulatoria y la ansiedad socavan la satisfacción laboral de los CISO, planteándose, una gran parte, un cambio de trabajo

El 75% de los CISOs de EE.UU. y Canadá están abiertos a un cambio de trabajo oprimidos por los crecientes requisitos financieros y legales, así como la ampliación de responsabilidades en un panorama donde la IA también amplía la superficie de ataque. Así lo destaca un estudio realizado por Ians Research y Artico Search en el que, además, se subraya que solo la mitad interactúa con su junta directiva de forma frecuente.

La reducción del gasto en ciberseguridad y el aumento de las infracciones cibernéticas, junto con la popularización de las herramientas de Inteligencia Artificial (IA) y normativas más estrictas que obligan, entre otros aspectos, a la notificación de incidentes, están provocando que los CISOs hayan comenzado 2024 con una mezcla de ansiedad y, también, de oportunidades.

Así se desprende del informe sobre 'El estado del CISO 2023-2024', elaborado por **Ians Research** y **Artico Search**, en el que, por un lado, pone de manifiesto las crecientes exigencias de sus puestos de trabajo, donde tienen que lidiar con un día a día excepcionalmente complejo que les obliga a hacer más con menos, y en el que se arriesgan, además, a una exposición legal, incluso, de carácter personal. Esto está provocando que un número creciente de CISOs se esté planteando un cambio de trabajo. A su vez, el estudio destaca que existe "una oportunidad sin precedentes" de defender un lugar en las filas ejecutivas, debido a la mayor presión a la que se ven sometidas las organizaciones con respecto a la ciberseguridad de sus negocios.

En concreto, el objetivo de la investigación es tratar de comprender mejor las condiciones que afectan a este rol en la actualidad y, para ello, contó con los datos proporcionados por más de 660 directores de seguridad de la información de EE.UU. y Canadá, además de las respuestas, a través de entrevistas, de más de 100 CISOs de una variedad de industrias y tamaños de empresas.

Menor satisfacción laboral

El porcentaje de CISOs satisfechos en su trabajo y con su empresa cayó 10 puntos, hasta el 64%, de 2022 a 2023. Además, el 75% está abierto a un cambio laboral, lo que supone un incremento de ocho puntos con respecto al período anterior. El problema es que la ansiedad afecta, cada vez más, a estos profesionales. Un trastorno que también sufren sus homólogos españoles, según el estudio publicado en este mismo número de SIC, 'Factores críticos en la generación del estrés de los CISOs y cómo evitarlos', realizado por Advens.

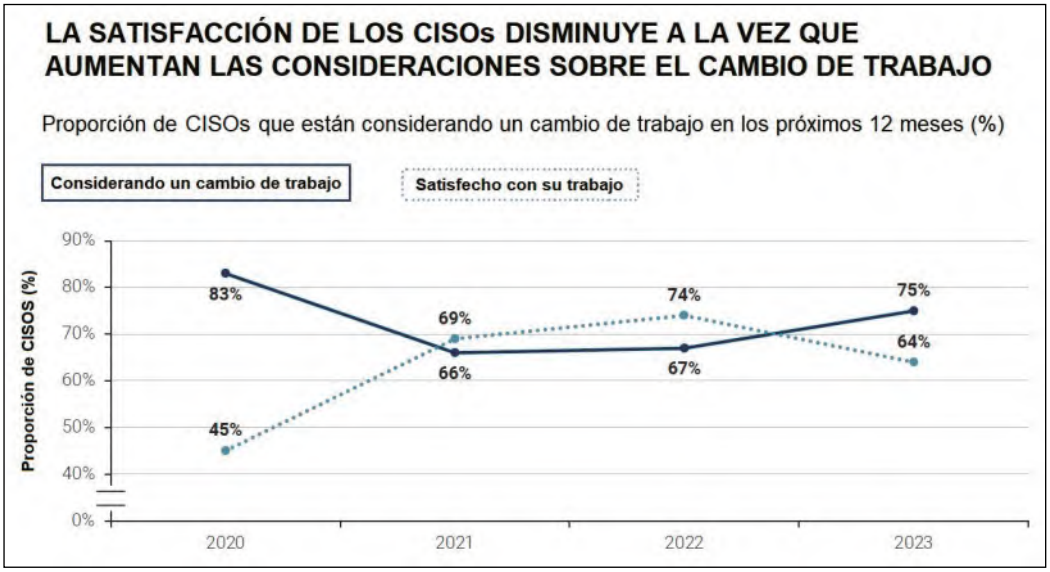
Entre los principales factores que afectan a esta situación, destacan, como otros años, los presupuestos ajustados y la creciente evolución de las ciberamenazas pero, ahora, también se suma un hecho más: "el aumento sin precedentes de herramientas de IA generativa que ofrecen a los CISOs nuevas oportunidades con capacidades de detección avanzada, automatización y defensas adaptativas pero, al mismo tiempo, plantean nuevas amenazas en sí mismas, con una superficie de ataque ampliada", se explica en el documento de Ians y Artico.

Junto a ello, se resalta que estos profesionales tienen que hacer frente a una mayor presión provocada por las nuevas obligaciones de los reguladores. Y es que, "ahora responsabilizan a los CISOs por la falta de transparencia, incluso el fraude, en nombre de su organización". Por ejemplo, en el caso concreto que concierne a los participantes en esta investigación, la **Comisión de Bolsa y Valores** (SEC) estadounidense "adoptó una firme postura de aplicación de la ley para las empresas públicas y privadas, y lo ha demostrado con acusaciones de fraude contra CISOs", puntualiza el informe, cuyos responsables añaden que "fueron considerados personalmente culpables de las infracciones".

Necesidad de colaboración

"Este tipo de normas y la mayor exposición a la que se enfrentan los directores de seguridad de la información exigen una fuerte colaboración entre éstos y el liderazgo de la empresa, incluida la junta directiva", subraya el estudio. Sin embargo, los datos de la encuesta demuestran que existe una desconexión en la mayoría de las empresas. Prueba de ello es que, únicamente la mitad (50%) interactúa con la junta directiva cada trimestre. De hecho, para el 25% se limita solo a una o dos veces al año, mientras que el 12% se reúne puramente *ad hoc* y el 13% no tiene ninguna participación.

Incluso, "entre las empresas con ingresos anuales que superan los 10.000 millones de dólares (la mayoría de las cuales cotizan en bolsa), sólo el 60% de los CISOs se reúnen con la junta directiva con regularidad y el 40% sólo una o dos veces al año", puntualiza. Señala, además, que a pesar de tener responsabilidades de nivel C, los directores de seguridad de



WISE SECURITY
a vargroup company

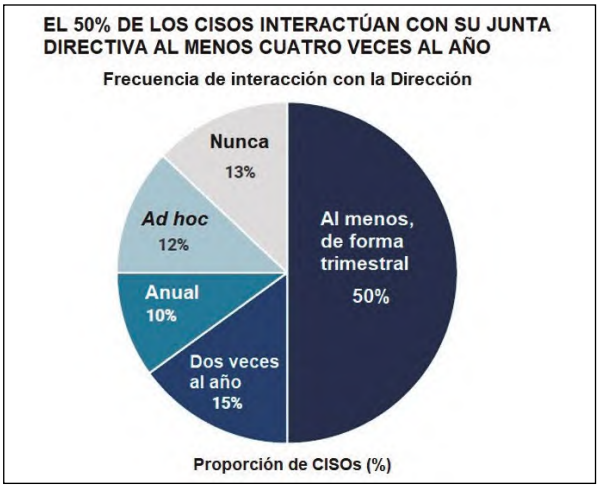
WISERTHANEVER

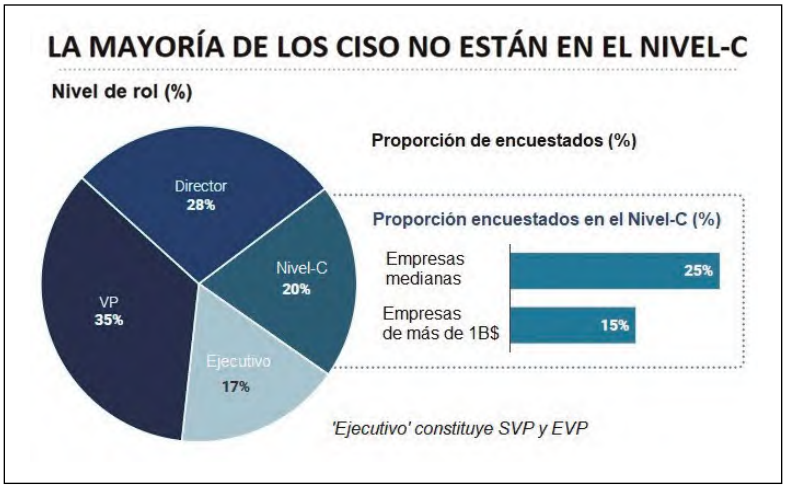
+CyberTrust +CyberSecurity

A Var Group company

wsg127.com

hello@wsg127.com | +34 910 700 549





la información tienen problemas para lograr ese tipo de reconocimiento dentro de sus organizaciones. Y es que, solo el 20% de todos los CISOs preguntados, y el 15% de los de empresas públicas, son considerados ejecutivos de nivel C. En concreto, el porcentaje de aquellos que se encuentran en dicho rango aumenta a medida que disminuye el tamaño de la empresa.

Más implicación, mayor satisfacción

La investigación también destaca que la satisfacción de estos profesionales aumenta con el acceso a la junta directiva, especialmente, cuando se tratan temas como los presupuestos y el riesgo. "Los que tienen una fuerte relación se sienten más valorados y, en general, indican que son 'escuchados', incluso cuando existen desacuerdos sobre el presupuesto", explican los responsables del estudio.

A pesar de ello, los CISOs tratan de buscar una indicación clara sobre los riesgos por parte de la dirección de sus empresas, pero a menudo no la encuentran. El 85% indicó que su junta directiva debería ofrecer una orientación clara sobre la tolerancia al riesgo de su organización para que puedan actuar. Sólo el 36% de los participantes considera que sí que lo hacen. Sin embargo, según el informe "la gestión del riesgo corporativo no es sólo responsabilidad empresarial y operativa del equipo directivo de una compañía: es una cuestión estratégica y de gobierno que está directamente dentro de la responsabilidad de supervisión de la junta directiva". Incluso, "en las empresas que cotizan en bolsa, sólo el 41% de los CISOs están de acuerdo en que la Dirección les proporciona una guía clara de tolerancia al riesgo", concretan.

Resulta también llamativo que solo un tercio informa a un cargo de negocio como el CEO, el COO (director de operaciones), el CFO (director financiero) o a un asesor legal. En el 42% de los casos, lo hace a un gerente directo de una función tecnológica, generalmente el CIO, y un 17% reporta al CTO (director técnico). Unos porcentajes que se han mantenido estables desde 2022, de acuerdo con la investigación.

Mejores oportunidades

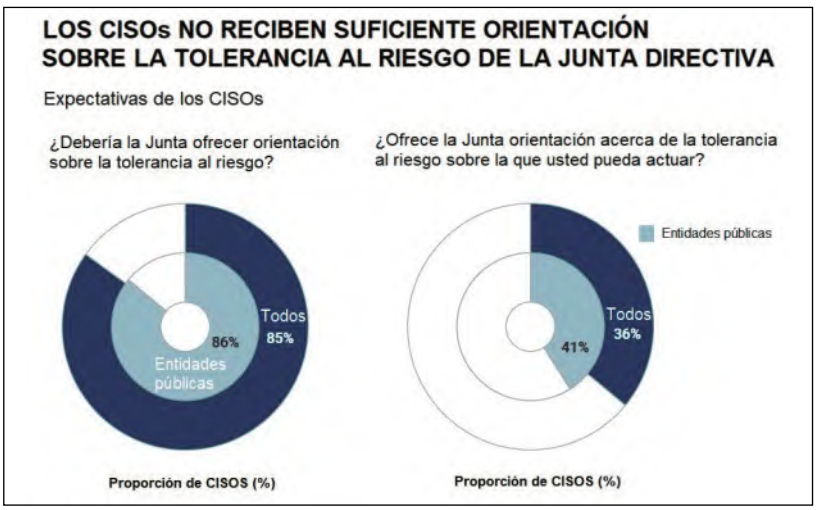
El dato positivo es que el aumento de las ciberamenazas "les da a los CISOs más capacidad para influir en los líderes fuera de su esfera de control directa", aunque un asiento en la mesa requiere mayores habilidades comerciales, según el informe. "Los CISOs deben poder comunicarse de manera efectiva con su junta directiva para cumplir con los requisitos en la presentación de informes, mejorar la alineación del presupuesto e impulsar una guía clara de tolerancia al riesgo", se destaca.

Para ello, necesitan, según se explica en el documento, "perspicacia para los negocios" y "presencia ejecutiva". La primera comprende "habilidades que permiten a los CISOs hablar el idioma de la junta directiva, incluida una sólida comprensión de la estrategia corporativa y la comercialización, así como de la financiera, además de tener la capacidad de encuadrar los riesgos en términos de impacto económico y costes de oportunidad, en lugar de limitarse a vulnerabilidades técnicas", especifica. La segunda implica la capacidad de ser persuasivo, directo y decisivo en las interacciones.

Desarrollo profesional

Dentro de este contexto, la investigación también ahonda en la formación que poseen los responsables de seguridad de la información preguntados, en los cuales, son las competencias tecnológicas las que dominan sus años de formación. En los años previos al puesto más alto, las dos trayectorias profesionales principales son la técnica y la de riesgo y cumplimiento.

También, apunta que la mayoría desarrolla sus capacidades de liderazgo a través del *coaching* ejecutivo y la formación externa. Eso sí, "los CISOs que participan en dichos programas o los han completado anteriormente reciben salarios más altos", señala el estudio. De hecho, la remuneración total de aquellos que actualmente participan o han completado un programa de *coaching* ejecutivo supera a aquellos que no han realizado un programa de desarrollo de habilidades de liderazgo en más de 200.000 dólares (182.850 euros).



Trabajo en remoto

Como dato adicional, y al igual que el año pasado, la investigación refleja que el 54% de los encuestados trabaja principalmente desde su casa, el 22% se encuentra en una situación híbrida y el 24% trabaja, generalmente, *in situ* en las oficinas de su empresa. ■

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

www.eset.es

ESET®
Digital Security
Progress. Protected.

Los participantes del estudio, realizado en España, consideran que una crisis cibernética les puede hacer perder su trabajo, según Advens

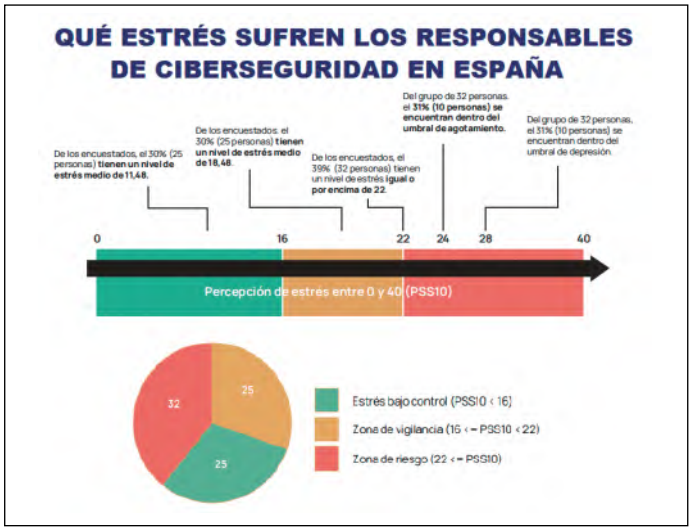
Casi cuatro de cada 10 CISOs confiesan vivir con unos niveles muy elevados de estrés por la dificultad e incertidumbre para ofrecer la máxima protección

Desde que **Steven Katz** fuera contratado en 1995 bajo el rol de Chief Information Security Officers (CISO) por **Citicorp,** este puesto profesional ha evolucionado mucho. Y no todo siempre para bien: el 40% de los profesionales que trabajan en España en este puesto considera que "vive una situación crítica de salud física y mental", y a más del 60% le preocupa poder perder su puesto de trabajo tras una crisis relacionada con la ciberseguridad. Así lo ha destacado el estudio 'Factores críticos en la generación del estrés de los CISOs y cómo evitarlos', realizado por **Advens,** junto a **ISMS Forum**. En él, 80 responsables de seguridad destacan que "la frustración, la incapacidad para desconectar y la sensación de estar siempre alerta, son los rasgos principales del cargo". Además, un 61% resalta que también se convive con el miedo a perder el trabajo por una crisis cibernética. Eso sí, el informe destaca que, analizando todas las respuestas, "los CISOs demuestran haber encontrado un equilibrio que les permita adaptarse al medio y evolucionar con él a la vez que el panorama va cambiando, así como una predisposición y proactividad por parte de la mayoría de los encuestados a nutrirse diariamente, y no dejar de aprender y adquirir conocimientos".

El análisis de la situación de los CISOs se ha realizado a través de dos conjuntos de preguntas: uno para analizar el nivel de estrés al que están sometidos y otro para comprender los detalles que podrían desencadenarlo. Para ello, se ha utilizado el modelo de la Escala de Estrés Percibido (PSS), que tiene como meta evaluar el grado en que los encuestados sienten que sus vidas son impredecibles, incontrolables y sobrecargadas, y que permite evaluar de forma global si una persona se siente o no capacitada para afrontar acontecimientos o momentos difíciles.

Salud mental

Así, entre otros aspectos de interés, el 75% de los encuestados confirma el estrés derivado del contexto de adversidad ante enemigos que a menudo son invisibles, el 61% se siente permanentemente alerta, casi una cuarta parte de los participantes no se acostumbra a los peligros e imprevistos del trabajo y el 42% se siente desanimado por el aumento de la frecuencia y potencia de los ciberataques.



De cualquier forma, es preocupante que el grupo más numeroso (39%), en concreto 32 de los 80 CISOs preguntados, sea el de más profesionales sobrepasados por su día a día en cuanto a su salud físico-mental y un malestar general que deriva en riesgos de amenaza y situaciones constantes de impotencia.

Competencias suficientes

En cuanto a las competencias, el 76% cree que tiene los conocimientos técnicos y metodológicos necesarios, pero solo algo más de la mitad de ellos cree que tiene la capacidad de adaptarse al contexto tan cambiante de la profesión. La gestión del riesgo de ciberseguridad, antes de las acciones de los CISOs, se considera un ejercicio difícil para el 89% de los encuestados, pero el 74% de ellos experimenta bastante bien la gestión de crisis. Por último, el 74% afirma que su trabajo "todavía" adolece de una idea preconcebida bastante negativa, el 75% sigue sintiéndose incomprendido, o incluso a veces considerado excesivo, y el 62% cree que una crisis importante podría costarle su trabajo.

Recomendaciones finales

En su parte final, el estudio recuerda que, dado el alto nivel de estrés detectado entre este rol profesional, esta situación debe "ser abordada con más profundidad por profesionales de la salud". Además, Advens e ISMS Forum también dan algunas recomendaciones con doble función: continuar con la concienciación y el reconocimiento del problema, y elaborar y poner en marcha una serie de prácticas para reducir el estrés.

De hecho, en cuanto a la incertidumbre con la que trabajan los responsables de ciberseguridad, "el contexto de adversidad es una fuente de estrés muy conocida, acentuada por la intensidad de la agresión potencial y la dificultad de afrontarla. Pero este contexto también puede crear empatía en la relación con los empleados de la empresa, lo que puede aliviar o suavizar la presión percibida", por lo que los responsables del informe recomiendan invitar "a los empleados a contribuir a la defensa, bajo el lema de que 'la seguridad es asunto de todos'", poniendo en marcha una defensa de doble sentido: "los trabajadores de la compañía confían en el equipo de ciberseguridad para que los defienda, y este equipo a su vez los invita a participar en esta actividad de defensa".

Además, aconseja poner en marcha desde seminarios web sobre resiliencia al estrés, hasta organizar talleres en profundidad para trabajar con grupos más pequeños, así como jornadas presenciales para sensibilizar e integrar a las profesiones de ciberseguridad en el pensamiento. Por supuesto, también recomienda mantener un trabajo continuo sobre la gestión del estrés, retratos y experiencias con otros CISOs, así como su integración a través de cursos de formación y divulgación orientada a la acción, entre otros aspectos. ■

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.

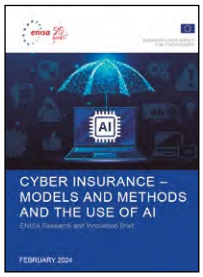
- **Una protección que no afecta al rendimiento.**
- **Despliegue flexible y gestión sencilla.**
- **La seguridad para aplicaciones que sí querrán tus desarrolladores.**

Más información en:

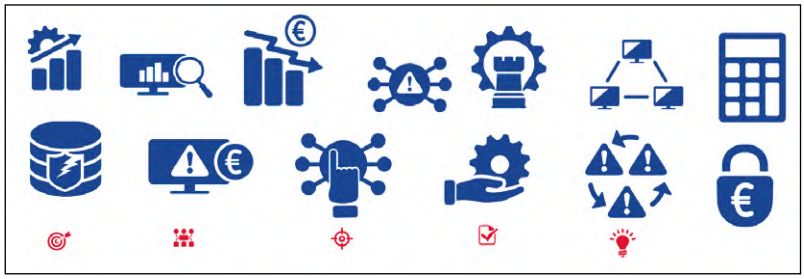
fastly.com/es/products/cloud-security

Considera importante también buscar enfoques que permitan contar con una póliza cibernética estandarizada para el sector privado

Ciberseguros: ENISA considera vital la inversión pública y la apuesta por el I+D para calcular mapas de ciberriesgos con datos de calidad a través de IA y ML



"Los riesgos cibernéticos presentan características complejas. No son estacionarios y evolucionan con el tiempo en sistemas técnicos y sociales que interactúan". Así lo destaca la **Agencia de Ciberseguridad de la UE** (**Enisa**) en su informe 'Cyber insurance: models and methods and the use of AI', con el que pretende ofrecer una descripción general de los enfoques de investigación y modelado existentes en identificar brechas a través de proyectos de investigación. Este documento complementa el ya elaborado en 2023, sobre las perspectivas y desafíos actuales de los operadores de servicios esenciales (OES) en relación con la suscripción de servicios de ciberseguros, destacando que ambos buscan facilitar una "mejor comprensión de cómo se puede hacer que el seguro cibernético sea más eficaz como herramienta para mitigar los ciberriesgos". Por ello, en esta nueva publicación pone en valor que "el seguro cibernético, especialmente cuando se combina con servicios de asistencia cibernética adecuados, puede mejorar tanto los beneficios para las empresas individuales como la resiliencia de la infraestructura de TI global".



Métodos estadísticos

El documento comienza con un capítulo de presentación no técnica, poniendo de manifiesto el problema del riesgo cibernético desde la perspectiva de las empresas que están expuestas a él y las compañías de seguros que están dispuestas a aceptarlo (parcialmente) mediante la suscripción de pólizas de seguro cibernético adecuadas. Además, hace énfasis en los métodos estadísticos avanzados de aprendizaje automático (ML) y de IA que ya se están usando en el contexto del análisis y la mitigación de riesgos cibernéticos o que tienen el potencial de proporcionar tales beneficios en el futuro.

Pasa en un segundo apartado a ofrecer un repaso detallado, por un lado, a las diversas facetas del riesgo cibernético; y, por otro, al seguro cibernético y sus requisitos. Con ello, proporciona los antecedentes académicos, ilustra las aplicaciones y los desafíos requeridos desde la perspectiva de la industria de seguros y, finalmente, ofrece la taxonomía del riesgo cibernético que se utiliza en el documento.

En su tercer capítulo analiza qué datos hay sobre riesgos cibernéticos, mostrando las principales investigaciones académicas al respecto y cómo se acomete el modelado. Así, destaca de forma especial sus consejos y recomendaciones para "crear mejores conjuntos de datos que estén disponibles para investigaciones que son esenciales para futuras investigaciones; especialmente para aplicaciones de ML/AI".

A continuación, dedica un cuarto apartado a los diferentes enfoques de modelado para el dominio cibernético que pueden usarse en el sector del seguro, destacando la importancia de "una separación en riesgos individuales, sistémicos y sistemáticos. En el ámbito de la modelización aún quedan muchos desafíos para el futuro".

Un análisis al que suma una interesante muestra de cómo se está aplicando el ML y la IA a los riesgos actuales -y futuros- en la ciencia actuarial y la industria de seguros, evidenciando el camino que queda por recorrer para que muchos de estos análisis puedan ser empleados por los seguros cibernéticos. De hecho, en su capítulo sexto ofrece una larga lista de problemas de investigación importantes y prometedores que se está acometiendo y superando.

Seguro vs riesgo

De hecho, es de especial interés el hecho de que explica que los "riesgos pueden examinarse desde diferentes perspectivas, como las causas de los eventos cibernéticos, el tipo de pérdidas que ocurren, los enfoques adoptados para evaluar los riesgos y las acciones tomadas para mejorar la ciberseguridad o mitigar las consecuencias negativas de los eventos cibernéticos". En este sentido, compañías como **MunichRe** consideran que habrá un "fuerte aumento de los ataques a medio y largo plazo, ya que las tecnologías de ataque se siguen desarrollando, entre otros, en el ámbito del crimen organizado, pero también por parte de los Estados". Y frente a esto "un actor clave en la gestión del riesgo ciber es la industria de seguros".

En cuanto a los actuales modelos utilizados por el sector asegurador, el estudio destaca que "es necesario seguir desarrollando nuevos enfoques de riesgos cibernéticos, que también sean la base para el análisis actuarial y la viabilidad de las soluciones de gestión de riesgos", así como "analizar los datos y desarrollar o adaptar más los métodos estadísticos. Esto incluye métodos de las áreas de ML y de IA". Es especialmente notable que el estudio considera una "cuestión importante" el "cómo diseñar con éxito un ciberseguro estandarizado para el segmento de clientes privados".

Así, Enisa destaca la necesidad del sector de apostar por la inversión en I+D+i en el ámbito de las pólizas cibernéticas para contar con mejores modelos de riesgos que permiten tener una "comprensión sólida de la vulnerabilidad específica de una empresa individual, por un lado, y las interrelaciones entre empresas, por otro lado, lo último que resulta en riesgos sistémicos y sistemáticos".

Datos insuficientes

Eso sí, alerta de que existe un importante obstáculo para "un mayor desarrollo y uso de herramientas estadísticas avanzadas y es la falta de datos disponibles públicamente", por lo que desde Enisa se aboga por "la creación de conjuntos de datos relacionados con la ciberseguridad disponibles públicamente para fomentar la investigación". La Agencia pide "incentivos gubernamentales e intervenciones regulatorias para habilitar una base de datos que permita a Europa ser competitiva en ciberseguridad".

Mayor inversión estatal

Como conclusión de los principales retos a acometer para crear herramientas con I+D, que permitan contar con datos fiables y concluyentes en el sector del seguro cibernético y que deberían involucrar, recuerda el informe, tanto a "miembros de la comunidad de I+i en general (académicos, investigadores e innovadores), la industria, la **Comisión Europea,** el **Centro Europeo de Competencia en Seguridad Cibernética** (ECCC) y los **Centros Nacionales de Coordinación** (NCC)". ■

xMDR

powered by cipher
a Prosegur company

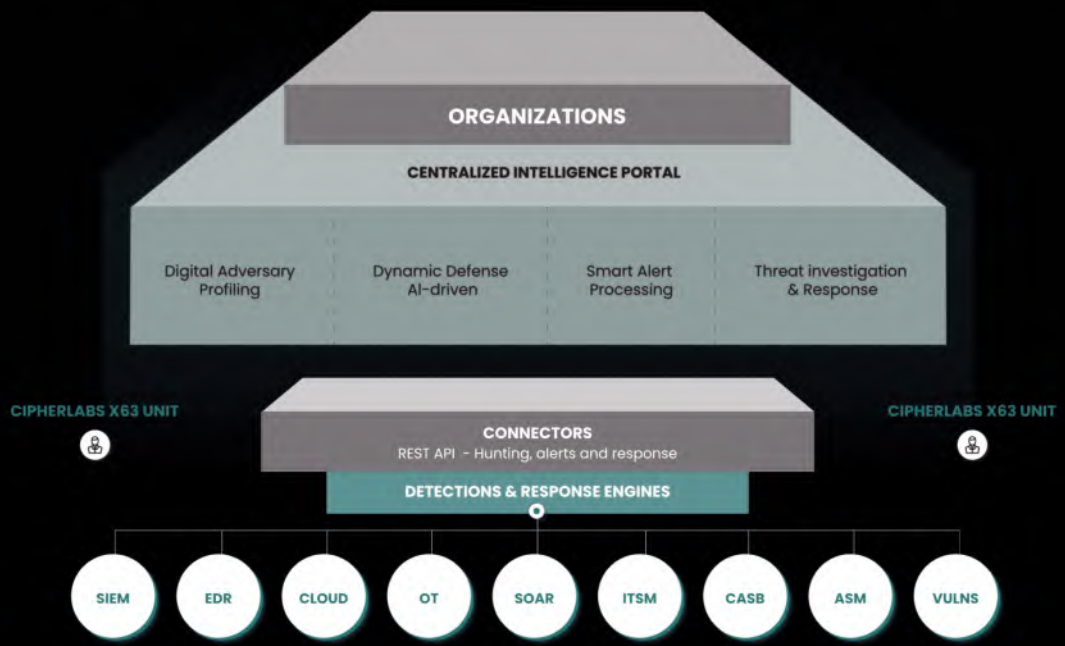
Modelado digital del adversario y aplicación de procesos cognitivos

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 in cipher ciphersec ciphersec

Alerta también del rápido uso de la IA generativa, tanto para ataques como para defensa, adaptándose rápido a las nuevas amenazas, según Tokio Marine HCC

Ataques patrocinados por estados a la cadena de suministro, y de *ransomware*, protagonizaron el 'panorama de amenazas' de 2023

Coincidiendo con sus 50 años de vida, **Tokio Marine HCC International** (TMHCCI) publicó un informe sobre los 'Top 10 Cyber Incidents 2023', en el que repasa y analiza, a través de dos de sus reconocidos expertos en este ámbito, **Isaac Guasch** y **Marc Pujol**, los principales ciberincidentes del año pasado. Una selección de interés por cuanto está hecha con la visión de uno de los referentes en riesgo cibernético y su aseguramiento, primando también su impacto financiero y daño reputacional.

El documento recuerda en su prólogo que "2023 será recordado por el continuo aumento de los ataques de *ransomware*, en gravedad y número", además de lamentar que "los ataques de los Estados-nación también hayan continuado debido a la persistente invasión rusa de Ucrania y al conflicto armado entre Israel y los grupos militantes palestinos liderados por Hamas en Gaza. Esto ha demostrado que los ciberataques sean un elemento importante en la guerra moderna", comentan sus responsables.

Ataques patrocinados

Por segundo año consecutivo, un ataque a un Estado-nación ocupa un lugar destacado en la lista: el realizado por Hamas contra Israel al comienzo del conflicto. Según **Cloudfare,** pocos minutos después de que comenzara la operación militar, se detectó un gran ataque DDoS contra sitios web que proporcionaban información crítica y alertas a civiles sobre ataques con cohetes. Además, el grupo cibercriminal, **AnonGhost** también –aprovechando una vulnerabilidad– intoxicó el sistema móvil de alertas, enviando, entre otras, notificaciones falsas o anulando las verdaderas. Le sigue en importancia, en segundo y tercer lugar, dos incidentes contra la cadena de suministro. El primero es el sufrido a principios de año por **ION Cleared Derivatives**, una división de **ION Markets** (un proveedor de soluciones de gestión de riesgos, activos, financiación y comercio ampliamente utilizado en el sector financiero), que informó de un ataque que "provocó la interrupción del negocio en ION y, también, de algunos de los bancos más grandes del mundo, interrumpiendo las operaciones de millones de clientes como efecto en cadena", destaca el documento, que recuerda que esta situación también afectó a los reguladores, ya que la **Comisión de Comercio de Futuros de Productos Básicos** (el principal organismo de control de derivados de EE. UU.) no pudo publicar su informe semanal sobre los Compromisos de los Comerciantes.

En tercer lugar, figura el ataque contra el proveedor de software **Progress,** cuya aplicación de transferencia de archivos MOVEi sufrió una vulnerabilidad aprovechada por los atacantes para, a través de la técnica de 'inyección SQL', permitirles sin autenticarse acceder a la base de datos de MOVEit Transfer. Una situación que les permitió hacerse con datos relevantes de **Ofcom, Transport for London, BBC, Boots** y **British Airways,** entre otras.

Completan este 'Top10', otras brechas de datos como la experimentada por **Air Europa**, a la que robaron información de las tarjetas de crédito de sus clientes, o la experimentada por **Marina Bay Sands.** También, forman parte de la lista ataques de *ransomware* varios realizados por la organización criminal **Lockbit** contra **ICBC,** además de contra el **Royal Mail** del Reino Unido y **Boeing**; y, también, el de **Scattered Spider** contra **Caesars** y **MGM Casinos,** uno de los más mediáticos del año por cuanto las dos cadenas de casinos apostaron por estrategias de mitigación distintas.

Como curiosidad, cierra el ranking el que es considerado el mayor ataque de DDoS registrado hasta ahora. Fue sufrido por **Google,** aunque sin éxito, y llegó a suponer hacer frente a 398 millones de solicitudes por segundo, siete veces más que el registrado el año anterior de este tipo.

Mayor velocidad

"La normalización de los ciberataques ha significado que estas historias no aparezcan en los titulares tanto como lo harían en el pasado, pero las empresas deben estar muy atentas a los principales vectores, como el *ransomware,* que continúa siendo muy rentable y eficaz. Y con la llegada de nuevas tecnologías esta tendencia no hará más que acelerarse", recuerda Guasch.

Además, en su parte final, el documento analiza el impacto que está teniendo en los ciberriesgos, la IA, su posible evolución y su diversificación, además de su potencial para los profesionales de ciberseguridad. "Como ya se comenta a menudo, la IA va viento en popa. En una industria que ya es muy dinámica, los especialistas en ciberseguridad experimentarán nuevas oleadas de ataques innovadores posibles gracias a la IA generativa. Sin embargo, al aprovechar estas nuevas herramientas -como Microsoft Security Copilot-, las empresas también podrán generar nuevas soluciones innovadoras de ciberseguridad, lo que conducirá a una posible carrera armamentista entre las bandas criminales y quienes intentan detenerlas", destaca el documento.

En concreto, pone en valor la capacidad de la herramienta de la multinacional para "aprender continuamente de las interacciones de los usuarios y ajustar sus respuestas para brindar respuestas más coherentes, relevantes y útiles a lo largo del tiempo. Este enfoque de aprendizaje adaptativo garantiza una mejora constante de las capacidades del sistema". De hecho, señala que "en el mundo de la ciberseguridad, donde cada minuto cuenta, herramientas como MS Security Copilot se están volviendo cruciales. Su capacidad para detectar amenazas priorizadas en tiempo real y anticipar los movimientos de los actores de amenazas basándose en un razonamiento continuo establece un nuevo estándar para las capacidades de seguridad de la IA". ■

Recuerda la importancia de estas iniacitivas que, en el caso de Criterios Comunes, cuentan en la UE con el 44% de sus laboratorios

ENISA aglutina en un solo informe todas las certificaciones de referencia en ciberseguridad en la UE, tanto en productos TIC como en nube

Se dice que lo que no se puede medir no se puede mejorar. Y precisamente ahí reside el valor de las certificaciones en todo tipo de ámbito. En el caso de la ciberprotección, la **Agencia de Ciberseguridad de la UE** (**Enisa**), ha publicado el informe 'Cybersecurity Certification Statistics', en el que hace un análisis cuantitativo del mercado de evaluaciones de la protección cibernética de los productos de TIC, servicios en la nube, así como las entidades que las realizan. Un ámbito que atañe de forma especial al organismo por cuanto la Ley de Ciberseguridad (Reglamento (UE) 2019/881) le encomienda crear un marco de certificación de la ciberseguridad de la UE y promover su aplicación.

Incremento notable

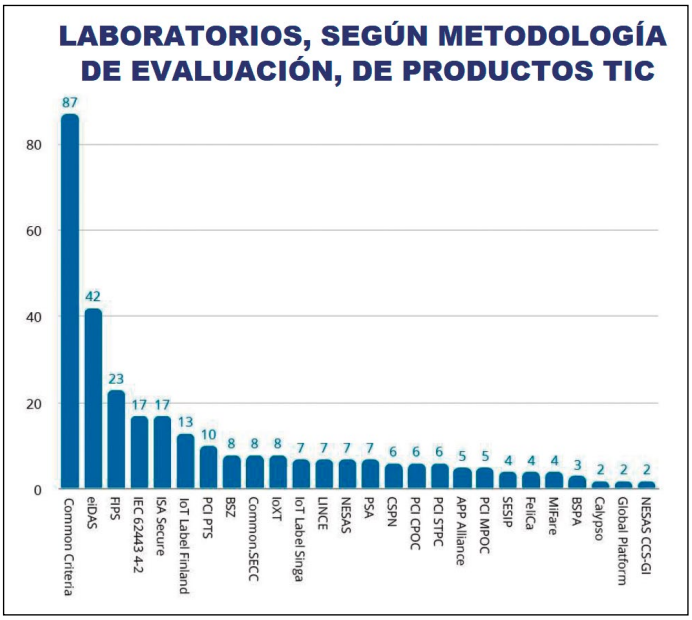
Así, el estudio tiene como objetivo analizar y comprender la evolución del mercado de la evaluación de la ciberseguridad, así como el impacto que tendrán los futuros esquemas en estudio en la UE; en particular, cuando se han establecido regímenes privados o se han simplificado metodologías para compensar algunas cuestiones, como los certificados de tiempo de comercialización, con regímenes nacionales existentes que serán sustituidos por los de la UE. Eso sí, no tiene en cuenta los esquemas con impacto local o en falta de uso, así como aquellos que no implican una evaluación de ciberseguridad centrada en el producto, como las 'Etiqueta de Ciberseguridad' de Francia o la de 'Made in Europe', ni los que no tienen un impacto europeo.

Escrito por **Chloé Blondeau,** de Enisa, y el reconocido especialista español, **José Ruiz,** Cybersecurity Business Unit Director de **Applus+ Laboratories,** el documento se centra en la evolución del número de soluciones TIC evaluadas y organismos de evaluación en los últimos cinco años. Así, tiene en cuenta las diversas formas de evaluar la ciberseguridad de las soluciones TIC, como estándares, nacionales y privadas, esquemas de certificación y metodologías seleccionados tras consultar a las partes interesadas que participan en los grupos de trabajo *ad hoc* sobre certificación de la ciberseguridad de la UE.

Así, en cuanto a los productos de las TIC, se puede observar que el número de sistemas y metodologías de evaluación está creciendo a lo largo de los años. "El mercado de la evaluación de la ciberseguridad para productos TIC no solo se basa en criterios comunes. En los últimos años, han nacido nuevos esquemas para responder a necesidades sectoriales como el pago, las telecomunicaciones o el transporte, pero también tecnológicas, por ejemplo, con el auge de los dispositivos conectados", destaca el estudio, que recuerda que, "además, con la aparición de nuevas metodologías de evaluación a tiempo fijo están surgiendo algunos sistemas y una nueva norma europea adoptada que apunta a plazos a priori limitados, generalmente más cortos".

Productos TIC

El informe comienza repasando las certificaciones para productos TIC, desde la de los CC, con el enfoque de la UE, hasta las metodologías ligeras como la Lince, de España, la BSZ, de Alemania, BSPA, de Países Bajos y CSPN de Francia, además de las que hay para productos criptográficos, identidad digital y firma, control de acceso –como FIDO–, comunicaciones móviles y de pago. También, referencia las 'etiquetas IoT' de ciberseguridad, como las que se ya ofrecen en Alemania, Finlandia o Singapur, entre otras. De hecho, recuerda que las etiquetas IoT (*Internet of Things*) son la nueva familia de metodologías de evaluación nacidas en los últimos años. Si bien siguen siendo voluntarios, estos esquemas tienen como objetivo aportar algo de claridad en el diverso ecosistema de dispositivos IoT.



Nuevos riesgos

En cuanto a los servicios en la nube de las TIC, hay menos marcos de evaluación debido a que la tecnología es más reciente. Sin embargo, por número de certificaciones realizadas, la norma ISO/IEC 27001 es la más empleada. Si bien aparecen nuevos esquemas que demuestran la necesidad de abordar la seguridad en la nube, su adopción sigue siendo lenta. Las certificaciones para servicios en la nube que "traen por su naturaleza una nueva capa de riesgos requieren un enfoque diferente en términos de evaluación de la seguridad". En este sentido, resalta que "si bien la mayoría de las metodologías de evaluación son bastante jóvenes y conocen una tímida adopción, ISO/IEC 27001 se erige como el estándar inevitable para abordar los sistemas de gestión de la seguridad de la información". Además, se pone en valor que "la cuestión de los datos gestionados que se plantea mediante el uso de servicios en la nube, llevó a varios países a construir su propio esquema de evaluación".

Organizaciones de certificación

Asimismo, dedica un amplio apartado a certificaciones de servicios en la nube repasando las más innovadoras, como el ENS de España (ver cuadro con número de empresas que ya la han superado), el C5 de Alemania, Secnumcloud de Francia, Zeker Online de Países Bajos o Fedramp de EE.UU.

Por último, termina con una pormenorizada lista de laboratorios acreditados, por países, de evaluación, así como organismos autorizados de evaluación de la conformidad. ■

Un 25% han experimentado accesos no autorizados en el último año, según Uptime Institute y Leet Security

La complejidad de la red aumenta el riesgo cibernético para los centros de datos, muy preocupados por su confidencialidad e integridad

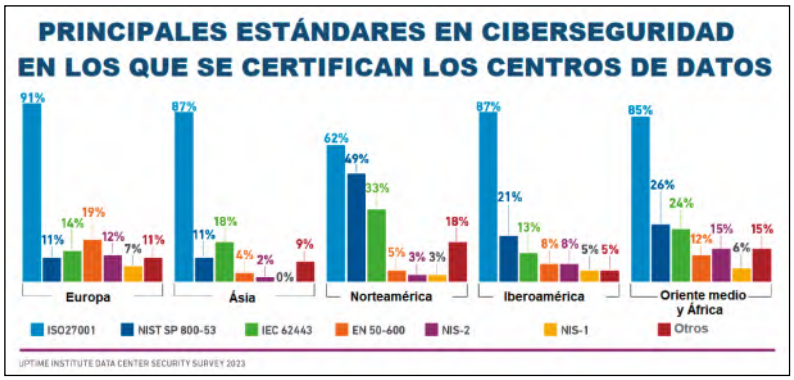
La infraestructura digital está más interconectada que nunca, tanto dentro como entre los centros de datos. Este es el resultado de las estrategias de virtualización, nube e híbridas a nivel de TI, y de los avances en monitorización remota, telemetría y sensores y gestión inteligente a nivel de instalaciones. Estos avances hacen que las redes de los centros de datos sean más complejas y amplían la gama de amenazas cibernéticas. Si bien seguir los estándares de seguridad de la industria puede mejorar la resiliencia digital, los ciberataques se están volviendo más sofisticados y a menudo superan el lanzamiento de actualizaciones de software y otras medidas defensivas.

Por ello, **Uptime Institute,** propietaria de la compañía española **Leet Security,** ha realizado una ilustrativa investigación, bajo el título 'Encuesta de seguridad de centros de datos', en la que preguntó a más de 300 profesionales que trabajan en este entorno, ya sea como propietarios o como clientes corporativos, sobre sus principales preocupaciones relacionadas con la ciberseguridad y sus estrategias para mitigar y responder a los riesgos digitales. De hecho, en ella se destaca que el 93% de los clientes de centros de datos empresariales solicitan activamente "más" información sobre la postura de ciberseguridad y cómo se han reforzado aspectos específicos.

El estudio ha desvelado que una de cada cuatro empresas del sector de centros de datos ha experimentado un ciberataque o acceso no autorizado a sus sistemas de TI o de tecnología operativa (OT), durante el último año. "A medida que estén cada vez más conectados, estos incidentes pueden volverse más frecuentes", destaca el documento. Además, es llamativo que los enfoques para las evaluaciones de ciberseguridad varían dependiendo de factores regulatorios y de sus costes. De hecho, otra investigación reciente de Uptime Institute encontró que los ciberataques representaban el 11% de cortes reportados públicamente en 2022, frente al 8% del año anterior.

Riesgos

En cuanto a la principal preocupación, la confidencialidad de los datos de los clientes es la primera, con diferencia. También está entre ellas, el *ransomware*, ampliamente percibido como peligroso y una amenaza considerable, ya que "se puede utilizar para cifrar o robar datos privados de clientes". Una situación preocupante por cuanto "la mayoría de los sistemas de TI y OT se pueden gestionar de forma remota, lo que puede mejorar la eficiencia, pero también introduce más vulnerabilidades de ciberseguridad", recuerda el estudio que, junto a ello, ha constatado que "si bien la mayoría de las organizaciones evalúan periódicamente la ciberresiliencia de sus terceros, muchas no lo hacen". Un total del 35% de este grupo permite el acceso de terceros a las redes internas.



Problemas de ciberseguridad

El documento también explica que la mayoría de los problemas de ciberseguridad están relacionados con la gestión de parches: casi dos tercios de las organizaciones de centros de datos dicen haber tenido problemas con este aspecto en los últimos tres años, aunque lo consideran "crucial" "para mantener la resiliencia digital". Y es que, a su complejidad se suma que los sistemas de TI, incluidos algunos equipos de las instalaciones, deban estar fuera de línea durante las actualizaciones, y requieren una coordinación cuidadosa para minimizar el riesgo de interrupciones en el servicio. Por ello, los responsables de su ciberprotección han mostrado su preocupación, por que la hiperconectividad de los centros de datos también hace que "la superficie de ataque sea cada vez más amplia", con el desafío que supone.

Revisiones semanales

En cuanto a la evaluación de las estrategias de ciberseguridad, el 90% de las empresas lo hace cada menos de seis meses, aunque algunas las lleva más que otras: llama la atención que, incluso, un 13% las acomete de forma semanal, a través de métodos menos invasivos como el escaneo de vulnerabilidades, análisis de registros y revisiones de listas de control de acceso. Eso sí, los preguntados destacaron que su periodicidad también depende de factores específicos del sitio, incluida la sensibilidad de la carga de trabajo de TI y complejidad de la red. Precisamente, su seguridad es la máxima prioridad en las revisiones que se acometen, apostando por estrategias que permiten "agregar capas de defensa contra los riesgos cibernéticos".

Estándares reconocidos

Además, los preguntados también resaltaron su apuesta por los marcos más sólidos para la seguridad de los datos, como los que utilizan cifrado resistente a los cuánticos, ya que consideran que "los algoritmos a menudo pueden compensar las vulnerabilidades de la red. Sin embargo, las debilidades del control de acceso pueden socavar incluso las redes más resistentes al permitir la entrada no autorizada a conexiones Ethernet o dispositivos". ■

NOVARED

Innovación en CiberSeguridad

EXPERTOS EN CIBERSEGURIDAD

PARA MITIGAR LOS RIEGOS DE SU NEGOCIO

28 AÑOS EN IBEROAMÉRICA

PROTEGIENDO A NUESTROS CLIENTES

www.novared.net

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

comunixgroup.com
Escuela de Hacking Ético de Novared

Enfoque de EY SOC: Transformación desde la Operación

Es habitual confundir un servicio gestionado con un servicio "comoditizado" y de poco valor. Precisamente, y a las pruebas me remito y con la regulación en la mano, los servicios SOC se están convirtiendo progresivamente en un elemento importante dentro del gobierno corporativo de las organizaciones. La propuesta de EY se centra en un modelo de SOC que debe ser flexible y personalizado para cada cliente. El principal enfoque de este modelo es proporcionar valor al negocio utilizando la transformación y la evolución integral desde las operaciones como eje central.

Nuestra visión de la situación actual de los servicios SOC

Nos encontramos servicios de SOC que están muy lejos de la cadena de valor de las organizaciones y se enfrentan a los siguientes desafíos:

1. Poca visibilidad de lo que hace el SOC y el valor que aporta a negocio. Los servicios SOC (incluyendo CSIRT) están totalmente justificados y valorados cuando existen incidentes que afectan al negocio. Es irónico que, cuanto más eficiente es un SOC, menos se le valora debido a la reducción de los incidentes. Para nosotros en EY, creemos que los servicios SOC deben esforzarse más en resaltar su contribución y valor para las organizaciones.

2. Falta de conocimiento y adaptación a cliente. Una talla única no funciona cuando se trata de SOC. Los servicios que son extremadamente estandarizados en N2 y CSIRT a menudo fracasan en caso de un ataque debido a la falta de personalización. Es esencial un profundo conocimiento del cliente para mejorar tanto la detección como la respuesta a los ataques cibernéticos.

Los servicios "caja negra" suelen provocar una dependencia del proveedor y la pérdida de conocimientos específicos para el cliente en términos de organización, procesamiento y tecnología.

3. No detectar o detectar en fases tardías de un ataque y demasiado falso positivo. Un alto nivel de falsos positivos puede ser un obstáculo para la eficacia de un SOC. Es un problema doble: no solo estaremos dedicando recursos y esfuerzos donde no toca, sino que también enmascararemos comportamientos sospechosos en fases iniciales de potenciales ataques.

Detectar en fases tempranas es vital para evitar impacto en la organización. Desafortunadamente, muchos SOC carecen de este enfoque en su organización, arquitectura de seguridad y procesos de gestión de alertas. Surge la pregunta, ¿conocemos los actores y sus técnicas que nos atacan o nos atacarán para poder detectarlos?

4. No evoluciona y pierde eficacia con el tiempo. ¿Nos imaginamos una solución de antivirus sin actualizar durante un año? Con las ciberamenazas y la tecnología del cliente en constante cambio, es crucial que los SOC se adapten y evolucionen para seguir siendo efectivos. De lo contrario, su eficacia se deteriorará con el tiempo. Un ejemplo de esto es el encaja en la seguridad OT/IoT.

Adicionalmente, los SOCs deben escalar. A medida que el alcance de estos servicios aumenta, muchos SOC aún dependen demasiado de la actividad manual, lo que limita su capacidad para escalar.

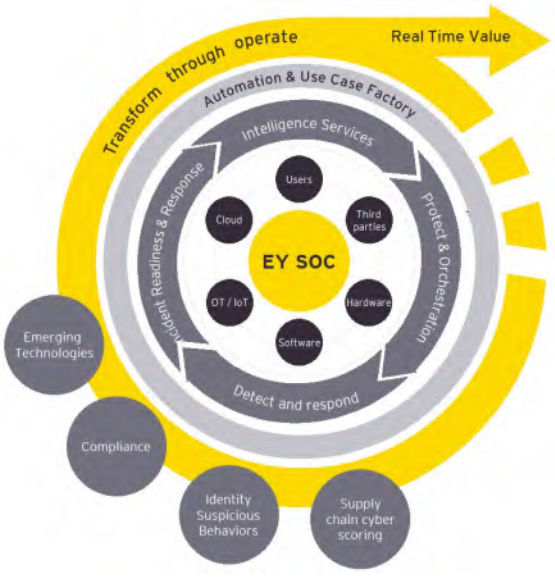


Figura 1.- Modelo EY SOC

Un modelo focalizado en el valor a negocio transformando a través de la operación de ciberseguridad

Desde EY entendemos que el valor que un SOC puede ofrecer al negocio de cualquier compañía es aquel que sea relativo a **impulsar la confianza digital y conseguir la resiliencia de los procesos críticos**. En muchas ocasiones confundimos el valor de negocio con valor tangible (por ej. Crecimiento de ingresos o ventas). En cambio, desde EY consideramos que el valor SOC para la organización no solo se rige en estos parámetros sino que el concepto de confianza y resiliencia digital va dirigido a todas las partes interesadas en la organización (empleados, clientes, accionistas, proveedores, etc) y por tanto se debe medir a través de indicadores representativos para cada uno de los colectivos.

En nuestro ADN tenemos grabado a fuego que **cada organización tiene unas necesidades particulares de SOC en cada momento** en función de múltiples factores tanto internos como externos. Algunos de estos factores hacen referencia a sus características de negocio, a su nivel de madurez en ciberseguridad, a su nivel de exposición pública, a su estrategia, etc. Por ese motivo no creemos en modelos de SOC "talla única" para todos los clientes. Nosotros apostamos por **servicios gestionados flexibles que sean capaz de adaptarse** a las necesidades particulares de cada cliente en cada momento. En línea con lo anterior, nuestro SOC deberá evolucionar de manera continua, a través de planes específicos de evolución, para continuar adaptándose a cambios tanto en la propia organización (por ej. Cambios tecnológicos en IT / OT), en el estado del arte de las amenazas (por ej. Nuevos actores) y la madurez de ciberseguridad del cliente (por ej. evolución del MFA / EDR).

Nuestro gran objetivo es **transformar desde la operación**. Vemos al SOC como la punta de lanza para el despliegue de la estrategia de ciberseguridad de una organización. Con una visión privilegiada, el SOC identifica las amenazas y riesgos actuales desde una perspectiva integrada y constante. Esto nos permite impulsar procesos de mejora continua que potencien la evolución y madurez organizativa a lo largo del tiempo.

En EY, enriquecemos nuestros servicios de SOC con una **capa analítica y estratégica** para aprovechar todos los datos disponibles. Con una serie de activos y aceleradores implementados desde EY, podemos aportar valor en una variedad de áreas, que pueden variar dependiendo de la compañía. Algunos ejemplos incluyen la cadena de suministro, el cumplimiento normativo, la gestión de identidades, la nube, e informes que realzan el valor del SOC.

Nuestra estrategia se centra en proporcionar centros de operaciones de seguridad sectoriales específicos. Actualmente contamos con ocho sectores definidos, además del SOC transversal.

A continuación, se recogen los principales aspectos diferenciales de nuestro modelo:

1. Transformación, evolución y personalización. A través de los servicios SOC se consigue una gran información de los entresijos organizativos y tecnológicos de las compañías. Una buena "digestión" de esta información permite identificar oportunidades de mejora y evolución en varios ámbitos:

• Evolución y adaptación del servicio SOC a las necesidades de la organización de manera continua (por ej. casos de uso, procesos, herra-

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

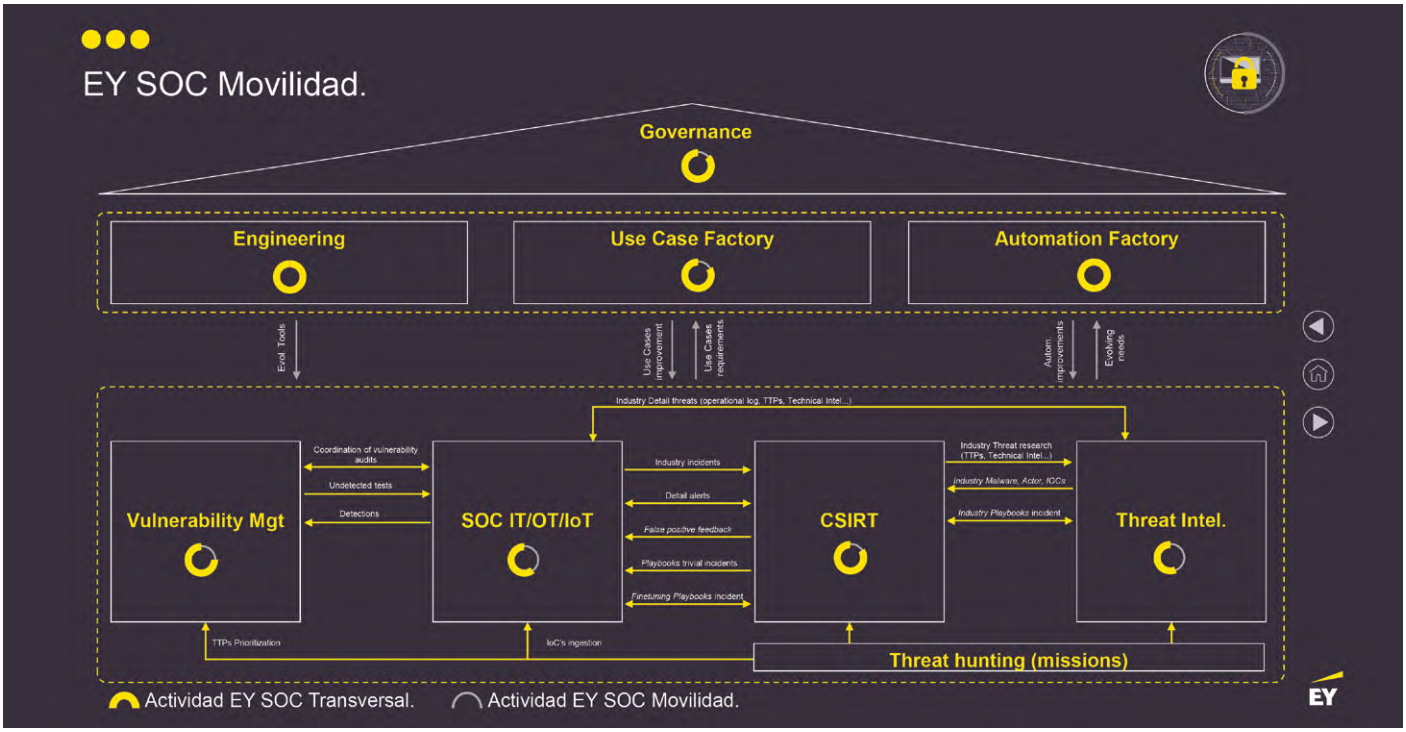


Figura 2.- Ejemplo de sectorización: Movilidad (presentado en TiSEC 2024 – A pleno SOC)

mientas, automatizaciones, etc.).

• Transformar el modelo de ciberseguridad y su integración con la organización (por ej. cumplimiento con regulaciones, medidas de protección de OT / IoT, desarrollo seguro, gestión de cambios, seguridad de proveedores, etc.).

• Evolucionar y mejorar el gobierno IT (por ej. inventario, procesos, mantenimiento, evolutivos, etc).

2. Reporting de valor. La generación mensual de informes del SOC, aunque es necesario, se configura insuficiente en el contexto actual. Las organizaciones, desde CISOs a CxO, necesitan mensajes de valor en tiempo real acerca de la actividad del SOC. Es decir, si el equipo está investigando un ataque en un ámbito de negocio, es necesario que se informe en tiempo real de la situación y de los resultados obtenidos en un lenguaje ejecutivo y entendible por el negocio.

3. Optimización con nuevas tecnologías. Con el objetivo de escalar y de poder llegar a todo el alcance de manera escalable, el modelo de SOC de cualquier entidad debe evolucionar hacia un entorno automatizado. Para conseguirlo desde EY identificamos 3 factorías:

• Factoría para automatizar toda la operación del Nivel 1.

• Factoría para priorizar, diseñar y desplegar los casos de uso y los *playbooks*/*runbooks*.

• Factorías de nuevas tecnologías autónomas e innovación (por ej. IA).

4. Sectorización. Como cualquier servicio gestionado existen múltiples tareas o elementos SOC transversales que son comunes a cualquier cliente. No obstante, cada vez más se requiere más especialización a cada cliente y sector (por ej. equipos de N2, análisis de amenazas y actores, integración de OT, etc). Por este motivo se plantea un SOC de SOCs compuesto por un SOC transversal común a todos los sectores y ocho SOCs verticales organizados por sector.

5. Supply Chain Scoring. Dada la importancia de la seguridad de terceras empresas que participan en el ecosistema de una organización y, teniendo en cuenta la visibilidad y la capacidad de transformación de un SOC, consideramos clave que el SOC sea un actor activo en la evaluación de proveedores a través de la monitorización de ataques y amenazas.

6. Servicios de Inteligencia. Los servicios de inteligencia se configuran como una pieza fundamental en la orquestación y priorización de las actividades del SOC. Conocer las TTPs de los actores que pueden atacarnos permitirá desplegar los casos de uso adecuados, priorizar la mitigación de la exposición por vulnerabilidad y establecer los entrenamientos necesarios a nuestro equipo de respuesta a Incidentes.

7. Casos de uso y *Playbooks*. Este es un elemento clave en el plano operativo del SOC. Hoy día se configura clave disponer de un conjunto casos de uso y *runbooks*/*playbooks* aque permitan detectar de manera efectiva en fases tempranas de ataque. Igualmente importante será minimizar los falsos positivos a través de metodologías de ajuste y mantenimiento (por ej. técnicas de *health check*).

8. *Compliance* desde la Operación. La visibilidad del SOC debe permitir dar visión del cumplimiento de normativas y regulaciones específicas de sector o ámbito (por ej. NIS2).

9. Risky Identity Management. La gran mayoría de ataques residen en la utilización ilícita de accesos e identidades. Por este motivo consideramos clave integrar procesos de gestión de identidades y accesos para detectar y actuar ante identidades con comportamientos de riesgo.

Conclusiones

Nuestra visión del SOC es que debe ser dinámico dentro de la organización, caracterizado por su flexibilidad y capacidad para adaptarse a los cambios de contexto relevantes y perceptibles desde la operación generando mensajes de valor en tiempo real. No puede seguir un modelo estático de "caja negra", sino que debe transformarse y evolucionar con las circunstancias cambiantes de amenazas y entorno tecnológico/organizativo para seguir siendo efectivo.

Las actividades del SOC deben seguir una estrategia de defensa activa, basada en un conocimiento profundo y actualizado de las amenazas potenciales. En este ámbito, la automatización debe ser una parte integral del SOC para permitir operaciones de seguridad escalables y efectivas.

Finalmente, el SOC puede jugar un papel integral en la mejora de la madurez de la ciberseguridad de las organizaciones. El SOC puede ayudar a las organizaciones a transformar y conseguir una postura de seguridad más fuerte y resiliente. ■

Javier Ferre
Socio Responsable Europeo
de Servicios Gestionados de Ciberseguridad
franciscojavier.ferrecabre@es.ey.com

José Luis Rojo de Luque
Socio Ciberseguridad
joseluis.rojodeluque@es.ey.com

EY

Enséñale los dientes al ransomware.

OBTÉN LA DEFENSA MÁS FEROZ CONTRA AMENAZAS COMPLEJAS.

Barracuda®

CTI de CYBERPROOF: Inteligencia de amenazas cibernéticas, un enfoque estratégico para la ciberseguridad

En el ámbito de la ciberseguridad, el servicio de Inteligencia de Amenazas Personalizada (CTI) de Cyberproof se destaca como una solución líder para organizaciones que buscan fortalecer sus activos digitales contra sofisticadas amenazas cibernéticas. El servicio abarca una metodología integral para monitorear a los adversarios por sector industrial, examinando aspectos como motivación, regiones de operación, objetivos y tácticas.

Introducción al servicio CTI

El servicio CTI es una combinación de recopilación de inteligencia continua, análisis minucioso e investigación específicamente adaptada al entorno del cliente. Su enfoque principal es detectar campañas dirigidas, identificar vulnerabilidades explotables, identificar indicadores de ataque y rastrear fugas de datos sensibles. Este servicio proactivo está diseñado para proporcionar a los clientes información procesable, lo que les permite ajustarse previamente al panorama de amenazas cambiante y administrar eficazmente los riesgos.

Metodologías y experiencia

El equipo de inteligencia de CyberProof está compuesto por veteranos experimentados de las unidades de inteligencia de élite de las Fuerzas de Defensa de Israel, con más de dos décadas de experiencia en ciberseguridad de Estado-nación. Nuestras herramientas de análisis únicas y desarrolladas en casa, que cuentan con algoritmos para evaluaciones más eficientes, trabajan en conjunto con los eventos internos del cliente para generar inteligencia adaptada. El módulo de Administración de Seguridad Automatizada (ASM) se integra sin problemas con la infraestructura del cliente, lo que permite una vigilancia constante de su presencia digital.

Monitoreo integral

A través de nuestro servicio, los incidentes basados en inteligencia procesable se categorizan en observaciones del panorama de amenazas y alertas de inteligencia personalizadas, que se entregan rápidamente para mejorar la preparación de seguridad del cliente. Nuestros servicios CTI incluyen monitoreo de actividades en la web oscura, fugas de datos, ataques de *phishing* dirigidos y protección de marca, combinados con técnicas avanzadas de análisis de inteligencia. Al realizar investigaciones específicas de la industria sobre amenazas, empoderamos a los equipos de seguridad de nuestros clientes con información procesable que les permite centrarse y neutralizar los riesgos más significativos para su negocio. Este enfoque proactivo garantiza una comprensión más amplia del panorama de amenazas y una detección temprana de posibles vulnerabilidades.

Servicios y reportes especializados

Los servicios complementarios como la Inteligencia de la Cadena de Suministro (SCI) permiten obtener información en tiempo real sobre posibles amenazas cibernéticas relacionadas con socios de la cadena de suministro. Nuestro servicio de Eliminación elimina rápidamente el contenido en línea malicioso, lo que reduce la exposición a la amenaza. Además, los clientes reciben informes exclusivos de CTI que ofrecen información profunda sobre amenazas emergentes con un enfoque en inteligencia específica de la industria y evaluaciones avanzadas de reconocimiento.

Excelencia operativa y soporte

CyberProof mantiene una estricta adhesión a los Acuerdos de Nivel de Servicio, brindando soporte operativo las 24 horas del día, los 7 días de la semana y garantizando tiempos de respuesta rápidos. Cada cliente se beneficia de un analista de CTI dedicado respaldado por un robusto equipo de soporte y protocolos de escalación. Las investigaciones ad hoc y las respuestas estratégicas a los ciberataques y vulnerabilidades de alto perfil son un testimonio de nuestro compromiso con la ciberseguridad de nuestros clientes.

Herramientas y técnicas avanzadas

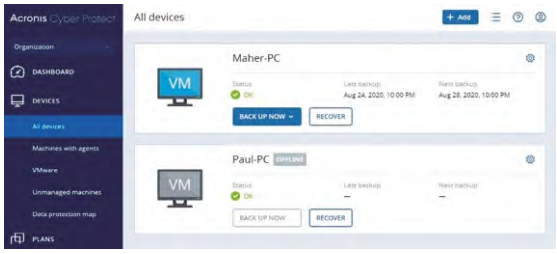
Nuestras metodologías utilizan una poderosa combinación de herramientas de investigación sofisticadas, que examinan la web clara, profunda y oscura en busca de señales de amenaza. Las herramientas también brindan una vista dinámica de la infraestructura externa del cliente, identificando continuamente nuevas vulnerabilidades y posibles riesgos de seguridad. A su vez, esto informa nuestro monitoreo dedicado de las huellas digitales de nuestros clientes, brindando una perspectiva holística de su postura de ciberseguridad.

El servicio de Inteligencia de Amenazas Personalizada de CyberProof no es simplemente una medida protectora; es una extensión estratégica del equipo de seguridad de una organización. Con monitoreo avanzado, metodologías sofisticadas y análisis de inteligencia experto, CyberProof empodera a los clientes para mantenerse un paso adelante de los ciberatacantes, salvaguardando así sus valiosos activos digitales y garantizando una postura de ciberseguridad resistente." ■

NETHANIEL RIBCO
Head of Cyber Threat Intelligence
CYBERPROOF

ACRONIS CYBER PROTECT 16 PERMITE RECUPERAR DATOS DE FORMA MÁS RÁPIDA Y SENCILLA

Acronis ha actualizado su producto estrella: **Cyber Protect,** que ya alcanza la versión 16. Con él, la compañía proporciona una integración única de copia de seguridad, recuperación ante desastres, ciberseguridad y gestión remota de puntos finales, a través de una única plataforma rentable y eficaz.



Entre otras novedades, la solución incorpora un nuevo panel de control centralizado, que mejora y simplifica aún más la gestión desde una única interfaz y proporciona una mayor visibilidad. Integra, además, funciones entre las que se encuentra seguridad frente a ciberamenazas, mediante el uso de inteligencia artificial (IA) y aprendizaje automático (ML), protegiendo de forma proactiva los datos, las aplicaciones y los sistemas frente a ciberataques avanzados. Ofrece recuperación rápida, permitiendo que los usuarios dependan mucho menos de la ayuda del equipo de TI central, ya que pueden iniciar con un solo clic las funciones de recuperación de *endpoints* distribuidos. También, la recuperación desde cero de cargas de trabajo físicas.

Además, permite un menor coste total de propiedad, una gestión centralizada y la integración con herramientas de terceros existentes, entre otros aspectos.

ACRONIS
www.acronis.com/es-es

CISCO Y KYNDRYL DESARROLLAN SERVICIOS DE SEGURIDAD DE *EDGE*

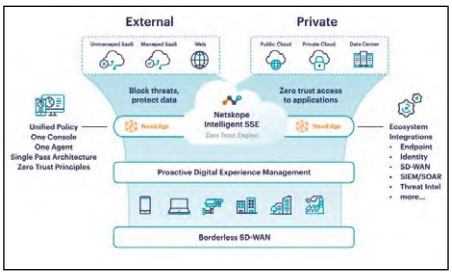
Cisco y **Kyndryl** han desarrollado dos servicios de seguridad de *edge*, de forma conjunta, para ayudar a los clientes a mejorar sus controles de seguridad y responder de forma proactiva a los incidentes cibernéticos.

Uno de ellos, denominado **Kyndryl Consult Security Services Edge (SSE)** con **Cisco Secure Access**, está diseñado para proporcionar un enfoque modular y unificado para la consultoría e implementación de una arquitectura SSE con la tecnología de Cisco.

El segundo, bajo el nombre de **Kyndryl Managed SSE** con **Cisco Secure Access**, presenta una nueva categoría de servicios de protección de red que integra la seguridad en un modelo de servicio en la nube. También, ofrece una solución de extremo a extremo para la transición, la implementación y los servicios gestionados de la solución SSE con la cartera de productos y servicios de Cisco. Este anuncio se basa en la asociación de Kyndryl con Cisco, a través de la cual las compañías han invertido conjuntamente y colaborado en un proceso de desarrollo para crear ofertas de seguridad escalables.

CISCO
www.cisco.com/c/es_es
KYNDRYL
www.kyndryl.com

NETSKOPE PONE EN MARCHA UNA OFERTA SASE ADAPTADA A LA MEDIANA EMPRESA Y FÁCIL DE USAR POR LOS MSPs



Para dar respuesta a los retos en ciberprotección y conectividad, especialmente en cuanto al trabajo híbrido, a los que se enfrentan las organizaciones medianas, muchos similares a los de las grandes empresas, **Netskope** ha desarrollado una solución SASE para el mercado medio, ofreciendo el mismo rendimiento y capacidades idénticas de seguridad avanzada de su propuesta para gran empresa.

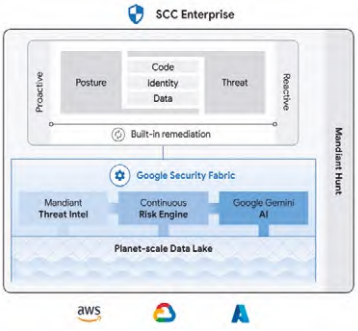
La solución se ofrece como un paquete fácil de gestionar, con capacidades de protección de datos y amenazas de nivel empresarial, "que se entregan listas para usar nada más sacarlas de la caja", explican sus responsables. Además, proporciona un despliegue y una administración simplificados de las políticas de red y seguridad, a través de una consola de gestión unificada y fácil de usar. También, dispone de conocimiento del contexto para Borderless SD-WAN y la cobertura de red global proporcionada por Netskope NewEdge, para una mayor agilidad y rendimiento de la red desde cualquier lugar. La multinacional, además, ha diseñado esta oferta SASE pensando en sus principales socios MSPs, con un diseño que facilita su despliegue y la gestión de Netskope SASE a escala para múltiples clientes.

NETSKOPE
www.netskope.com/es

GOOGLE SECURITY COMMAND CENTER ENTERPRISE FUSIONA LA PROTECCIÓN EN LA NUBE CON OPERACIONES ASISTIDAS POR IA

Con el objetivo de ayudar a sus clientes a gestionar y mitigar los riesgos en entornos multi*cloud*, **Google Cloud** ha presentado **Security Command Center Enterprise** (SCC Enterprise), una solución de gestión de riesgos en la nube que fusiona una seguridad proactiva *cloud* con operaciones de protección de nivel empresarial, y con un extra: la experiencia de **Mandiant**.

Una de sus principales características es que permite eliminar los silos



de herramientas, equipos y datos que crean barreras entre la protección en la nube y las operaciones de seguridad de las empresas. Además, "con nuestra nueva solución, las organizaciones pueden empezar a pensar en una nueva realidad: la de una seguridad en la nube con visibilidad SIEM y capacidades SOAR", afirman desde la compañía. Por un lado, los equipos de seguridad pueden acceder a una vista unificada de sus controles de estado, las amenazas activas, las identidades en la nube, los datos, etc.

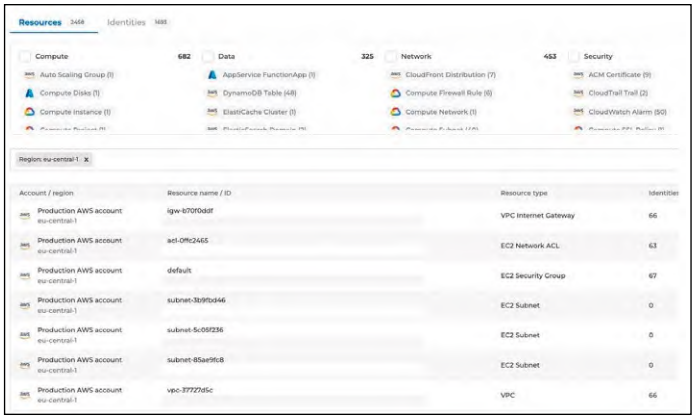
Por supuesto, también se apoya en la estructura de seguridad de Google, que a su vez utiliza un lago de datos para captar y analizar datos de la nube a la escala necesaria. Como resultado, genera gráficos dinámicos y permite entender las complejas relaciones existentes en los entornos multinube. Además, cuenta con la inteligencia de amenazas de Mandiant y su servicio **Hunt**, que ofrece asesoramiento humano a demanda, así como la integración de su IA **Gemini** para Google Cloud, entre otras funcionalidades.

GOOGLE
https://cloud.google.com

BITDEFENDER DIRIGE SUS NUEVAS SOLUCIONES A LOS MSP, LA GESTIÓN DE LA POSTURA DE SEGURIDAD CLOUD Y LA PROTECCIÓN DEL CORREO ELECTRÓNICO

Bitdefender ha puesto a disposición del mercado varias soluciones como **GravityZone CSPM+**, para la gestión de la postura de seguridad en la nube (CSPM), **GravityZone Cloud MSP Security Solutions**, una iniciativa dirigida a proveedores de servicios gestionados (MSPs) y a sus clientes corporativos, así como la funcionalidad **Email Protection,** de análisis e identificación de contenidos potencialmente peligrosos, ante intentos de *phishing* y fraudes en línea, presentes en el correo web.

Con la primera, la compañía busca supervisar y gestionar configuraciones de infraestructuras en la nube, incluidas Amazon Web Services (AWS), Google Cloud Platform (GCP) y Microsoft Azure, entre otras. Además, GravityZone CSPM+ incorpora la detección y respuesta a amenazas junto con las capacidades de gestión de derechos de infraestructura en la nube (CIEM), lo que permite a las empresas aplicar de forma fácil las políticas de gestión de identidad y acceso (IAM) y las mejores prácticas de configuración, especialmente en la búsqueda del cumplimiento, en entornos multinube. Con la segunda, ofrece protección avanzada para el *endpoint* y servicios gestionados de detección y respuesta (MDR) para identificar y erradicar las ciberamenazas en cualquier entorno el momento en el que se producen y para fortalecer la resiliencia contra los ciberataques. GravityZone Cloud MSP Security Solutions dispone de diferentes niveles: Secure, Secure Plus y Secure Extra, adaptados a las necesidades, requisitos (incluyendo *compliance*) y presupuestos específicos de cada cliente de los MSPs.



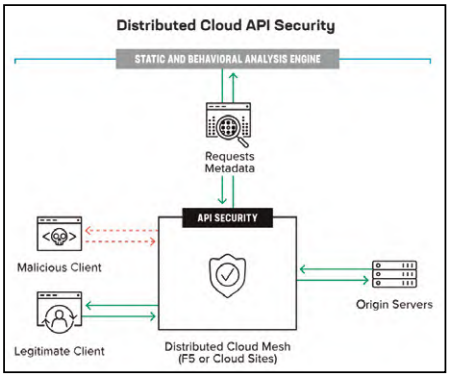
Mayor seguridad para Gmail y Outlook

Además, ha presentado su Email Protection, una potente funcionalidad que analiza e identifica, entre otros, intentos de *phishing* y fraudes *online*, presentes en el correo web de Gmail y Outlook al que se accede desde cualquier dispositivo.

BITDEFENDER
www.bitdefender.es

F5 AÑADE CAPACIDADES AUTOMATIZADAS DE RECONOCIMIENTO Y PENTESTING, Y DE IA Y SEGURIDAD *END-TO-END* PARA APIs PARA DETECTAR VULNERABILIDADES Y MEJORAR LA OBSERVABILIDAD

F5 ha enriquecido su propuesta **Distributed Cloud Services** con una solución automatizada de reconocimiento de seguridad y tests de intrusión. Además, para afrontar el crecimiento de las aplicaciones y de las APIs que las conectan debido al uso de la IA, ha sumado capacidades de prueba de código API y análisis de telemetría. Y es que, F5 también está haciendo que los beneficios de la IA estén presentes en todo su portafolio.



La incorporación de nuevas capacidades automatizadas de reconocimiento y *pentesting* es fruto de la reciente adquisición de la compañía **Heyhack.** Gracias a ellas, los clientes de F5 Distributed Cloud Services pueden escanear y descubrir fácilmente vulnerabilidades que afectan a sus aplicaciones web. Dependiendo de los resultados del análisis automatizado, la solución recomendará reglas para el cortafuegos de aplicaciones web y las soluciones de remediación más adecuadas.

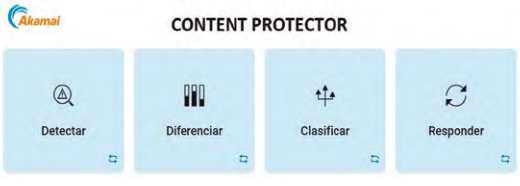
Estas funcionalidades automatizadas complementan el reciente anuncio de **F5 Distributed Cloud API Security**, que aprovecha la compra de **Wib**, experta en seguridad para APIs, permitiendo la detección de vulnerabilidades y la observabilidad en los procesos de desarrollo de aplicaciones, lo que hace que se identifiquen los riesgos y se implementen políticas antes de que las APIs entren en producción.

Así pues, Distributed Cloud Services ofrece los beneficios de una solución de seguridad API de ciclo de vida completo, entre los que se encuentran: una ventana de riesgo muy reducida para las nuevas APIs, mediante la identificación de vulnerabilidades y la aplicación de especificaciones estrictas y precisas antes de que entren en producción; orientación clara sobre gobernanza, con estándares en tiempo real e informes de cumplimiento normativo; así como descubrimiento de API, entre otros aspectos.

F5
www.f5.com/es_es

CONTENT PROTECTOR, EL PRIMER PRODUCTO DE AKAMAI ESPECÍFICO PARA DETENER LOS ATAQUES DE *SCRAPING*

Bajo el nombre de **Content Protector, Akamai** ha creado un producto que detiene los ataques de *scraping* sin bloquear el tráfico legítimo que las empresas necesitan para desarrollar su actividad comercial. "Los *bots* de *scrapers* son una parte esencial y a menudo productiva del ecosistema comercial, ya que se encargan de buscar contenido nuevo, destacar los productos en los comparadores y recopilar información actualizada sobre productos para compartirla con los clientes", explican desde la compañía. "Lamentablemente, los *scrapers* también se utilizan con fines perjudiciales, como la subcotización competitiva, la vigilancia que precede a los ataques de almacenamiento de inventario, así como la falsificación de bienes y sitios web". Lo peor es que "su especialización dificulta la detección", por lo que, "requiere detecciones diferentes para cada tipo de bot especializado", destacan.



Para evitarlo, la solución ayuda a detectar y mitigar los *scrapers* evasivos que roban contenido con fines maliciosos, permite mejorar el rendimiento del sitio y la experiencia del usuario, así como proteger la propiedad intelectual, al tiempo que proporciona mejores detecciones y menor número de falsos negativos.

Para ello, ofrece detecciones personalizadas, donde realiza unas evaluaciones a nivel de protocolo y de aplicación. A ello, se le une la capacidad de analizar las interacciones de los usuarios para distinguir entre el tráfico humano y el de *bots*, además de supervisar el comportamiento de los visitantes en su sitio web para identificar patrones inusuales.

AKAMAI TECHNOLOGIES
www.akamai.com/es

CHECK POINT PRESENTA INFINITY AI COPILOT, LA SERIE QUANTUM FORCE GATEWAY Y HARMONY SAAS

Check Point ha dado a conocer su primera generación de **Infinity AI Copilot**, en la que une la Inteligencia Artifical y tecnología de nube, en una solución "basada en 30 años de inteligencia en ciberseguridad *end-to-end*", según la compañía. Además, ha presentado **Quantum Force Gateway Series**, una innovadora serie de 10 cortafuegos de alto rendimiento para centros de datos y perímetros de red, y la solución **Harmony SaaS** de prevención de amenazas.

Integrada dentro de la plataforma Check Point Infinity, y sacando provecho al potencial de la IA Generativa (GenAI), Infinity AI Copilot actúa como un asistente administrativo y analítico que automatiza tareas de seguridad complejas y proporciona soluciones proactivas a las ciberamenazas. Además, reduce significativamente los tiempos de tareas rutinarias. De hecho, según la compañía, "ahorra hasta un 90% del tiempo que se invierte en tareas administrativas de seguridad, incluidos el análisis de eventos, la implementación y la resolución de problemas".

La solución también gestiona, modifica y despliega de forma automática reglas de acceso y controles de seguridad específicos para la política de cada cliente; aprovecha la IA en la búsqueda, análisis y resolución de amenazas; y supervisa todos los productos en toda la plataforma Infinity, entre otros aspectos.

Cortafuegos de alto rendimiento

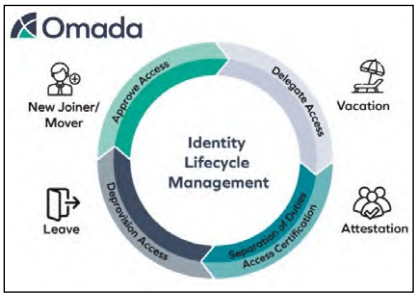
También como parte de la plataforma Infinity, Check Point ha desarrollado la Serie Quantum Force Gateway Series, que incluye 10 cortafuegos que pueden ofrecer un rendimiento de prevención de amenazas hasta 63,5 Gbps, respuesta automatizada a los ciberataques, inteligencia global en tiempo real y más de 50 motores de IA, además de una seguridad consolidada y gestión de políticas en entornos locales, en la nube y FWaaS (Firewall-as-a-Service).

Además, ha lanzado Harmony SaaS, una solución con la que las empresas pueden proteger su ecosistema SaaS contra amenazas como el robo de datos y cuentas.

CHECK POINT SOFTWARE
www.checkpoint.com

OMADA OFRECE MAYOR VELOCIDAD, INTELIGENCIA, CONECTIVIDAD Y EFICIENCIA CON LA NUEVA VERSIÓN DE IDENTITY CLOUD

Construida sobre una arquitectura moderna basada en microservicios y nativa de la nube, **Omada** ha presentado su nueva generación de **Identity Cloud**, con la que ofrece más velocidad, soporte inteligente para la toma de decisiones, conectividad y una mayor eficiencia operativa.



Entre sus características, destaca su mayor rendimiento para importar y procesar datos de identidad. Además, aumenta la frecuencia de importación de datos para reflejar los cambios organizativos en tiempo real.

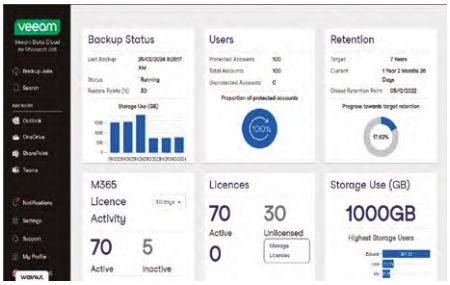
Con la introducción de esta versión, Omada Identity Cloud también ofrece a los clientes una mejora de la toma de decisiones basada en IA. Junto a ello, les permite configurar fácilmente cualquier aplicación y sistema para garantizar el Gobierno de Identidades de principio a fin en todo el conjunto de aplicaciones y el ecosistema más amplio de soluciones de seguridad e identidad digital. Así se ofrece "una gestión coherente de políticas y accesos en despliegues *on-premise*, híbridos y en la nube", indican desde la compañía. Además, su eficiencia operativa hace que los usuarios puedan aprovechar una experiencia del *workflow* optimizado que proporciona cuadros de mandos e informes específicos para el cumplimiento normativo.

OMADA
www.omadaidentity.com

VEEAM DATA CLOUD OFRECE COMO SERVICIO *BACKUP* PARA ENTORNOS MICROSOFT Y CAPACIDADES ADICIONALES DE IA

Veeam Software ha presentado su **Data Cloud**, desarrollado sobre Microsoft Azure. La solución ofrece en la actualidad *backup as a service* (BaaS) para Microsoft 365 y Microsoft Azure. Además, anunció en marzo una alianza ampliada a cinco años con Microsoft que permitirá la integración de la familia de productos de Veeam con los servicios **Microsoft Copilot y AI**.

En concreto, **Veeam Data Cloud para Microsoft 365** se ofrece como servicio de *backup* para proporcionar protección y recuperación de datos para Exchange Online, SharePoint Online, OneDrive for Business y Teams. Se trata, además, de un servicio 'todo en uno', que incluye: software, infraestructura de copia de seguridad y almacenamiento ilimitado en un paquete con mantenimiento continuo ofrecido por expertos. Por su parte, **Veeam Data Cloud para Microsoft Azure** es la primera oferta SaaS de la compañía para *backup* para este entorno. Proporciona protección de datos integral y recuperación de datos para Azure VMs, Azure SQL y Azure Files.



Capacidades de IA

Entre los aspectos más destacados de la colaboración entre Veeam y Microsoft, cabe señalar el desarrollo conjunto para aportar capacidades adicionales de IA a los productos de Veeam, como la integración de Copilot para el análisis automatizado de datos, *insights* rentables impulsados por IA y una visualización de datos más sencilla. Además, tiene soporte integrado de las últimas APIs para Microsoft 365 Backup Storage y aceleración de la migración de clientes *on-premises* a Veeam Data Cloud alojado en Azure, entre otros aspectos.

VEEAM SOFTWARE
www.veeam.com

PALO ALTO NETWORKS LANZA SOLUCIONES DE SEGURIDAD PARA REDES 5G PRIVADAS CON SU ECOSISTEMA DE SOCIOS

Palo Alto Networks ha dado a conocer su propuesta para redes 5G privadas con protección de extremo a extremo, en colaboración con varios de los *partners* más importantes del sector.

Impulsada por una convergencia de IA, Zero Trust, normativas y mandatos, **Palo Alto Networks 5G Security** se presenta así como una combinación de herramientas de seguridad de referencia con tecnologías y servicios de socios de redes 5G privadas, permitiendo a los clientes incorporar la seguridad a sus redes desde cero, protegiendo toda la infraestructura 5G y el tráfico de misión crítica que transporta.

Entre estos primeros *partners* de 5G privada se encuentran **Celona, Druid, Ataya, Netscout, Nvidia** y **NTT Data.**

Así, las organizaciones que construyen nuevas redes 5G privadas con Celona, Druid y Ataya pueden asegurar fácilmente las redes de radio a través de integraciones con Palo Alto Networks 5G Security. Además, con Netscout, la visibilidad de red omnipresente a nivel de paquetes se combinará a escala con Palo Alto Networks 5G Security, ayudando a los equipos de seguridad a obtener una gran visibilidad para tomar decisiones de política

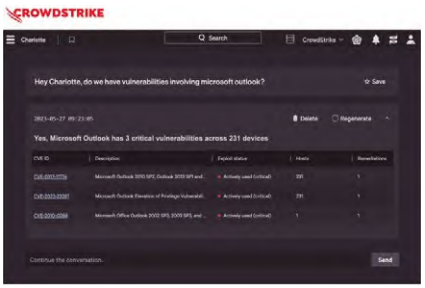
inteligentes. Por su parte, Nvidia, permite disponer de seguridad 5G escalable y asegura que las aplicaciones impulsadas por IA estén optimizadas.

Y, gracias a NTT Data, se podrá disponer de capacidades de infraestructura de red y servicios de consultoría de TI e integración de sistemas globales de confianza que ayudarán a los clientes a desplegar, gestionar y proteger sus redes 5G privadas.

PALO ALTO NETWORKS
www.paloaltonetworks.es

CROWDSTRIKE PROSIGUE CON SU APUESTA POR LA IA CON MÁS FUNCIONES DE CHARLOTTE AI, FALCON FOR IT Y FALCON DATA PROTECTION

CrowdStrike ha anunciado la disponibilidad de **Charlotte AI** y de **Falcon for IT**, así como la incorporación de nuevas tecnologías en la solución **Falcon Data Protection** para ayudar a los equipos de tecnología y de seguridad a sacar el máximo potencial de la IA generativa y minimizar la exposición a los riesgos asociados a ella.



Charlotte AI es capaz de reducir las rutinas, que tradicionalmente podían requerir horas, a minutos o segundos. En este sentido, mediante conversaciones naturales, el profesional puede preguntar dudas sobre cualquier evento relacionado con la protección de la organización y recibir respuestas antes de tomar decisiones dentro del flujo de trabajo automatizado. Además, reduce los tiempos de investigación y respuesta, y ofrece una gestión simplificada gracias a innovaciones basadas en IA, con acceso transparente a las fuentes de datos, controles de acceso basados en roles y salvaguardas avanzadas.

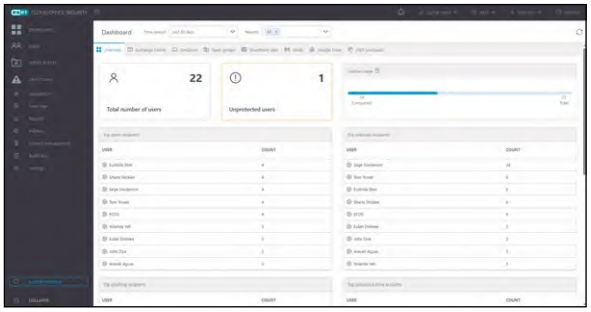
Por su parte, Falcon for IT es el primer producto desarrollado desde cero para aprovechar los flujos de trabajo basados en IA generativa en Charlotte AI. La solución consolida múltiples casos que afectan a los equipos de seguridad y de TI para que las organizaciones puedan reemplazar los productos heredados con una arquitectura de agente sencillo en la plataforma Falcon. Desde una misma plataforma, los clientes mejoran en visibilidad, comprensión de los riesgos y en la consolidación de los agentes y productos.

Finalmente, Falcon Data Protection "ayuda a las organizaciones a adoptar tecnologías de IA sin tener que preocuparse por filtraciones de datos cuando se cargan datos sensibles en herramientas comerciales de IA", explican desde la compañía.

CROWDSTRIKE
www.crowdstrike.com/sites/es

PROTEGER LAS COMUNICACIONES EN LA NUBE, OBJETIVO DE ESET CLOUD OFFICE SECURITY PARA MSPs

Con la creciente demanda de servicios gestionados en la nube, el mercado de MSPs se expande constantemente, pero este crecimiento también ha creado un nuevo terreno de reproducción para el *malware* sofisticado, según **Eset**.



Y es que, "con su acceso privilegiado a las redes empresariales, los proveedores de servicios comprometidos también pueden ser peligrosos para sus clientes al desencadenar un ataque a la cadena de suministro", indica el director de Investigación y Concienciación de Eset España, **Josep Albors**.

Para evitarlo, la compañía dispone de su **Programa MSP**, el cual se basa en la solución Eset Protect, que proporciona protección multicapa y, en sus niveles superiores integran **Eset Cloud Office Security** (ECOS), para proteger las aplicaciones de Microsoft 365 y Google Workspace. De hecho, estas soluciones de seguridad pueden interrumpir los procesos maliciosos que contactan con C&C controlados por los atacantes.

En concreto, ECOS ofrece protección anti*phishing,* bloqueando el acceso a páginas web conocidas por *phishing*, previniendo que los usuarios hagan clic en enlaces fraudulentos dentro de correos electrónicos. También, proporciona funcionalidades anti*malware.* En este sentido, escanea todos los archivos nuevos y modificados en OneDrive, Google Drive, Microsoft Teams y SharePoint Online.

A estas capacidades, se les une las de **Eset LiveGuard Advanced.** Con ellas, por ejemplo, si los motores de detección de *malware* identifican un nuevo tipo de amenaza, el archivo se envía a esta herramienta de análisis basada en la nube para una evaluación más detallada. Por último, también cabe señalar la funcionalidad multi-*tenant* de ECOS, para proteger y gestionar múltiples instancias de Microsoft 365 y Google Workspace desde una consola de Eset Cloud Office Security.

ESET
www.eset.com/es

Del 10 al 12 de abril de 2024, en formato presencial y en remoto

IV JORNADAS STIC & Congreso RootedCON Capítulo Panamá: "Gobernar y compartir, las claves del éxito en ciberseguridad"

Las **Jornadas STIC** y el **Congreso técnico RootedCON**, han aunado esfuerzos para organizar conjuntamente un nuevo capítulo internacional de sus encuentros, en esta ocasión en Panamá, del 10 al 12 de abril de 2024. Ambas han escogido a la ciudad panameña como lugar estratégico para celebrar uno de los mayores eventos de ciberseguridad de Iberoamérica, precedido por el éxito de las tres ediciones anteriores, celebradas en Colombia (2020 y 2021 en Bogotá y Medellín, respectivamente) y en República Dominicana (2022), para continuar promoviendo las alianzas en este sector.

El **Centro Criptológico Nacional** (**CCN**), el **Instituto Nacional de Ciberseguridad** (**Incibe**), el **Mando Conjunto del Ciberespacio** (**MCCE**) y **RootedCON,** por parte española, y la **Autoridad Nacional para la Innovación Gubernamental** (**AIG**) de Panamá organizan esta edición, con la colaboración de las principales autoridades e instituciones del país panameño, así como el apoyo institucional de la **Organización de los Estados Americanos** (OEA), **la red CSIRTAmericas** y el **Banco Interamericano de Desarrollo** (BID).

Así, durante tres días, y bajo el lema 'Gobernar y compartir, las claves del éxito en ciberseguridad', los asistentes podrán disfrutar de un completo programa de ponencias, talleres y laboratorios. En concreto, habrá una sala 'Jornadas STIC', presencial y en remoto, que se dividirá en tres módulos temáticos: uno Internacional, a cargo del CCN y el MCCE; otro de Cooperación, organizado por la OEA y el BID; y otro Institucional, en el que se podrá conocer la visión de la ciberseguridad del Gobierno de Panamá y sus instituciones. También, habrá otro módulo, para la sala CCN (sólo presencial), con sesiones impartidas por el organismo del CNI, para compartir su experiencia en la gestión de proyectos y actividades para mejorar las capacidades de prevención, detección y respuesta a ciberamenazas.

Según lo previsto, **Revista SIC**, a través de una ponencia conjunta de su editor y director –**Luis Fernández** y **José de la Peña**, respectivamente– aportará conocimiento y reflexiones de su dilatada y pionera experiencia de 32 años en el ámbito de la ciberprotección.

Congreso hacker español

En paralelo, del 10 al 12 de abril, también se celebrará la primera edición iberoamericana del congreso técnico RootedCON, en presencial y en remoto, que ofrecerá actividades más prácticas y técnicas, así como formativas de nivel avanzado. El acceso a este evento será gratuito para usuarios registrados, siendo de pago los laboratorios que se celebrarán también esos días.

Del 21 al 23 de mayo en Espacio Gran Vía (Barcelona)

El V CONGRESO DE CIBERSEGURIDAD DE BARCELONA reunirá a más de 60 referentes sobre los grandes retos del sector

La quinta edición del **Barcelona Cybersecurity Congress** (**BCC**), que tendrá lugar del 21 al 23 de mayo, presentará todo tipo de soluciones con el objetivo de incrementar la protección digital de la industria. El evento, organizado por **Fira de Barcelona,** con la colaboración de la **Agència de Ciberseguretat de Catalunya**, prepara una nueva edición con la participación de empresas y expertos que han desarrollado herramientas para construir un mundo digital más seguro, en un momento en el que el aumento del número de dispositivos IoT conectados y la adopción de la tecnología 5G también han provocado un aumento de riesgos y amenazas.

Con el lema 'Asegure hoy, proteja mañana', el BCC contará con una amplia gama de contenidos agrupados bajo los ejes temáticos de: Capacitación y Concienciación de Empleados, Medidas de Seguridad Robustas, Inteligencia y Monitorización de Amenazas, Soluciones de Gestión de Cumplimiento, Gobernanza y Privacidad de Datos, y Tecnología Regulatoria. Además, incluirá una zona de exposición comercial.

Entre los más de 60 ponentes que participarán, con la dirección técnica de la **Sociedad Internacional de Automatización** (**ISA**), destacan desde **Tom Liston**, autor del primer sistema tarpit de código abierto, hasta **Francisco Luis de Andrés**, Global CISO de **IriusRisk**, **Andreu Sancho**, Cybersecurity Senior Specialist de **Nestlé** o **David Andrés Hurtado**, Responsable de ciberseguridad OT y Ciberresiliencia en **Naturgy**, entre otros. También, se habilitará una Hacking Village, donde expertos pondrán en práctica sus habilidades. En paralelo, se celebrará el **ECSO** Cyber Investor Days.

El 18 de abril, en los Jardines de Cecilio Rodríguez (Madrid)

CYBERMADRID organiza el evento 'Nacional de Ciberseguridad en Fraude Digital', con apoyo público-privado

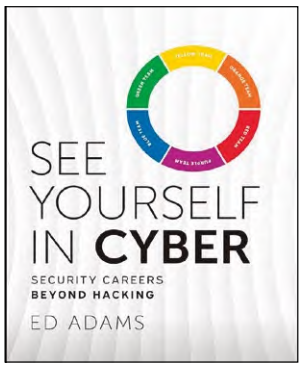
CyberMadrid, Clúster de Ciberseguridad de Madrid, organizará el 'I Congreso Nacional de Ciberseguridad en Fraude Digital', el 18 de abril, en el pabellón de los Jardines de Cecilio Rodríguez del madrileño parque de El Retiro.

Con esta iniciativa, la organización presidida por **Damián Ruiz**, pretende posicionar a la capital como referente nacional en ciberprotección en fraude digital y dar a conocer en profundidad los elementos que intervienen en las actividades de protección, detección y respuesta dicho ámbito.

Es intención asociativa que el encuentro se articule en torno a una tríada de bloques temáticos que plantearán la situación, protección e innovación del fraude digital y en los que se podrán conocer destacadas propuestas aplicando las nuevas tecnologías.

A fecha de cierre de esta edición, el Congreso cuenta con el apoyo institucional del **Ayuntamiento de Madrid**, **Comunidad de Madrid** e **Incibe,** junto a asociaciones, instituciones u organizaciones afines al Sector como la **Asociación Española de Empresas Contra el Fraude** (AEECF), **FrauDfense**, el **Centro de Cooperación Interbancaria, Banco Caminos** (CBNK) e **Isaca Madrid,** entre otros, así como de fabricantes con foco en el tema.

SEE YOURSELF IN CYBER: SECURITY CAREERS BEYOND HACKING

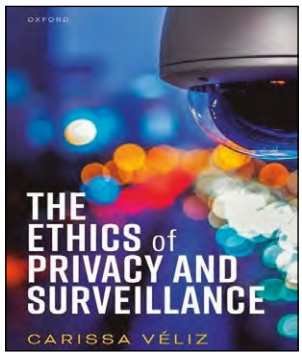


Autor: Ed Adams
Editorial: Wiley
Año: 2024 – 256 páginas
ISBN: 978-1-394-22560-6
www.wiley.com

Fundador y director ejecutivo de la compañía Security Innovation, **Ed Adams** ofrece una interesante aportación a través de un ensayo en el que analiza los diferentes roles que hay en las empresas y que no están necesariamente en el departamento de ciberseguridad pero que contribuyen de forma notable a ella. A lo largo de sus capítulos, pone en valor la aportación de profesionales como desarrolladores, expertos en DevOps, la alta dirección, los directores generales y cómo todos, con concienciación y formación, pueden impulsar la madurez de la compañía en ciberprotección.

Así, utilizando la conocida analogía de la rueda cromática, el autor explica los roles y responsabilidades modernos de los profesionales que operan dentro de cada 'porción', con abundantes ejemplos y estudios de casos de éxito que evidencian la importancia de aplicar el enfoque que plantea Adams en su obra. Además, cuenta con la aportación, a través de entrevistas, de destacados referentes para, en definitiva, proponer una estrategia viable y una metodología específica para que todos los que están en cualquier empresa aporten su 'granito' en ciberprotección.

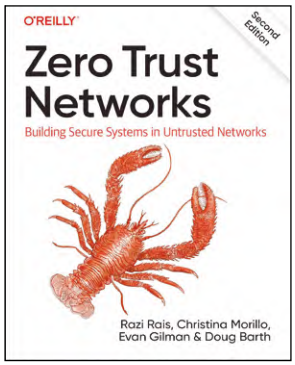
THE ETHICS OF PRIVACY AND SURVEILLANCE



Autora: Carissa Véliz
Editorial: OUP Oxford
Año: 2024 – 256páginas
ISBN: 978-0198870173
www.oup.es/es

Tras su interesante 'Privacidad es poder: Datos, vigilancia y libertad en la era digital', **Carissa Véliz** vuelve en este reciente volumen a poner el foco en la importancia de la ética y la privacidad en una época donde la vigilancia digital se ha exacerbado por el uso intensivo de las nuevas tecnologías. Por ello, la especialista de Oxford, propone esta obra, con la que pretende contribuir a una mejor comprensión de la privacidad desde un punto de vista filosófico: qué es, qué está en juego en su pérdida y cómo se relaciona con otros derechos y valores. Así, las cinco partes que componen este libro responden a preguntas básicas sobre privacidad: ¿De dónde viene la privacidad? ¿Qué es la privacidad? ¿Por qué es importante? ¿Qué debemos hacer con ella? ¿Dónde estamos? Por la escasez de obras sobre ética en el ámbito digital, ésta resulta de gran interés ya que, sin duda, es una de las pioneras en profundizar en ella ante los riesgos que supone la IA y la demanda de datos de todo tipo que precisa para su entrenamiento, vinculado a todo tipo de modelos de negocio. Por ello, "es hora de que la filosofía mire más de cerca la privacidad", comenta Véliz.

ZERO TRUST NETWORKS: BUILDING SECURE SYSTEMS IN UNTRUSTED

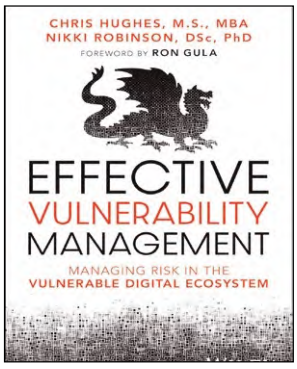


Autores: Razi Rais, Christina Morillo, Evan Gilman y Doug Barth
Editorial: Oreilly & Associates
Año: 2024 – 332 páginas
ISBN: 978-1492096597
www.oreilly.com

Excelente obra para profundizar en este enfoque a través de cuatro profesionales de reconocido prestigio en este ámbito. A lo largo de sus páginas, el lector, de carácter eminentemente profesional, podrá conocer diferentes recomendaciones y aproximaciones a la Confianza Cero, dando especial protagonismo a aspectos como la autenticación, la autorización y el cifrado en todo momento, además de disponer de acceso compartimentado y agilidad operativa. Aspectos que permitirán poner en marcha una arquitectura de una red de Confianza Cero, a partir de las tecnologías actuales. Además, incluye varios casos prácticos que permiten conocer aproximaciones de compañías que ya apuestan por Zero Trust, a través de conceptos como motores de confianza, de política y agentes de contexto. "Este modelo incorpora la seguridad dentro del funcionamiento del sistema, en lugar de superponerla", resaltan sus autores, que analizan las diferentes arquitecturas, estándares y marcos en está área.

EFFECTIVE VULNERABILITY MANAGEMENT

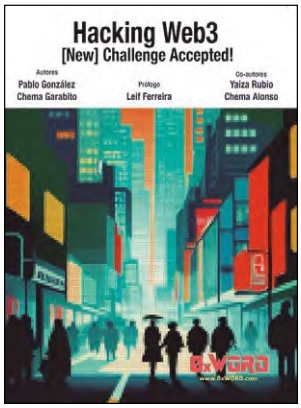
Managing Risk in the Vulnerable Digital Ecosystem



Autores: Chris Hughes, Nikki Robinson
Editorial: Wiley
Año: 2024 – 288 páginas
ISBN: 978-1394221202
www.amazon.com

Las organizaciones dedican una enorme cantidad de tiempo y recursos a abordar las vulnerabilidades de su tecnología, software y organizaciones. Pero, ¿están bien invertidos ese tiempo y esos recursos? Bajo esta premisa, los coautores Hughes y Robinson ofrecen una obra, eminentemente práctica, que permite tener un excelente conocimiento sobre cómo aplicar una gestión eficaz de vulnerabilidades a través de prácticas, procesos y herramientas que buscan permitir a las organizaciones actuales mitigar el riesgo de manera eficiente y oportuna en la era de la nube, DevSecOps y Zero Trust. Además, describe de forma exhaustiva las tareas de evaluación, planificación, monitorización y asignación de recursos para evitar este tipo de fallos de seguridad, "permitiendo a los lectores eliminar pasos innecesarios, simplificando el proceso de protección de los datos y las operaciones de la organización". Asimismo, el libro "cubre dominios emergentes clave, como la seguridad de la cadena de suministro de software y los factores humanos en la ciberseguridad". Desde luego, una interesante aportación de un tema que, cada año, continúa siendo foco de muchos de los grandes ciberincidentes.

HACKING WEB3: [NEW] CHALLENGE ACCEPTED!



Autores: Pablo González, Chema Garabito, Prologo Leif Ferreira; coautores: Yaiza Rubio y Chema Alonso
Editorial: 0xWord
Año: 2024 – 254 páginas
ISBN: 978-84-09-53983-3
https://0xword.com

Interesante aproximación para aplicar la ciberseguridad al denominado 'mundo de la Web3', la nueva Internet, descentralizada y basada en *blockchain*, que por muchos ya es considerada el nuevo paradigma técnico-económico. Y, como sus posibilidades son casi infinitas, ya hay notables proyectos con ella en todo tipo de ámbitos. Precisamente, para aportar la capa de protección cibernética, los autores y coatores de esta obra que es pionera en el panorama técnico bibliográfico en castellano, buscan a lo largo de sus siete capítulos ofrecer una valiosa información sobre cómo auditar, desarrollar de forma segura y conocer las vulnerabilidades a las que se enfrentan los proyectos de Web3. En definitiva, permiten entender, de forma didáctica, sus diferentes elementos, para aplicar la lógica a proyectos en ella, por ejemplo, implementando *smartcontracts* y evitando muchas de las vulnerabilidades frecuentes en este ámbito. Además, ofrece abundante información de herramientas para mejorar el desarrollo y la calidad del código, así como para proteger e identificar tus proyectos. Incluso se propone aprender con un CTF en Web3.

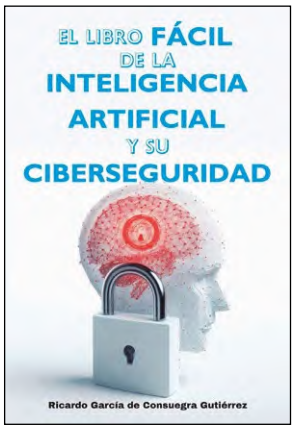
SECURITY IN THE CYBER AGE

An Introduction to Policy and Technology

Autor: Derek S. Reveron
Editorial: Cambridge University Press
Año: 2023 – 412 páginas
ISBN: 978-1009308588
www.cambridge.org

El ciberespacio es esencial para socializar, aprender, comprar y, en definitiva, realizar numerosas actividades en la vida moderna. Sin embargo, también tiene un lado oscuro: actores subnacionales, transnacionales e internacionales están desafiando la capacidad de los gobiernos soberanos de proporcionar un entorno seguro para sus ciudadanos. Según explica el autor de este libro, "los grupos criminales mantienen como rehenes a empresas y gobiernos locales mediante *ransomware*, los servicios de inteligencia extranjeros roban propiedad intelectual y realizan operaciones de influencia, los gobiernos intentan reescribir los protocolos de Internet para facilitar la censura y los ejércitos se preparan para utilizar operaciones en el ciberespacio en guerras". Por ello, con esta obra, busca ofrecer unas claves para entender cómo funciona el ciberespacio, así como el *modus operandi* de los actores estatales y no estatales aprovechándose de vulnerabilidades. Una obra, de carácter científico, que permite profundizar en formas tecnológicas, políticas y éticas de proteger el ciberespacio con un enfoque interdisciplinario.

EL LIBRO FÁCIL DE LA INTELIGENCIA ARTIFICIAL Y SU CIBERSEGURIDAD



Autor: Ricardo García de Consuegra Gutiérrez
Editorial: Publicación independiente
Año: 2024 – 150 páginas
ISBN: 979-8875701023
www.amazon.es

Curiosa aproximación a la Inteligencia Artificial desde un punto de vista de la ciberprotección, para los que busquen una obra sencilla de entender, aunque muy práctica. A lo largo de sus seis capítulos García de Consuegra, profesional con una amplia trayectoria en ciberseguridad, repasa desde qué cambios conlleva la IA, qué supone para la seguridad cibernética y cómo está impactando en el trabajo de los están en este sector.

Con un estilo ameno, abundantes ejemplos e historias curiosas, permite ir profundizando en los conceptos que hay que tener sobre esta tecnología y cómo se está aplicando, para bien y mal, a la ciberseguridad. Además, cuenta con un apartado final lleno de reseñas bibliográficas y enlaces con muchas aplicaciones y herramientas recientes, también, para protegerse de los ataques que ya la usan en el día a día.

LA TRANSFORMACIÓN DE LA GUERRA EN EL SIGLO XXI

Estudios estratégicos para su comprensión

Coordinadores: Carlos A. Bueno y Guillem Colom
Editorial: UNED
Año: 2024 – 212 páginas
ISBN: 978-84-362-7878-1
https://portal.uned.es

Este libro coral aborda algunas de las cuestiones más relevantes para comprender un fenómeno político, la guerra, que marca de forma radical las agendas nacionales e internacionales en la actualidad. Desde la asunción de que la naturaleza del conflicto armado permanece constante, se observa que muchos de sus elementos definitorios están experimentando en el siglo XXI un profundo proceso de transformación tecnológica, social, organizativa o informativa.

Por ello, según destacan sus autores, "el impacto multidimensional de la guerra exige la adecuada comprensión de sus dimensiones estratégica y militar. Así, los Estudios Estratégicos son el campo de conocimiento preocupado por el análisis en profundidad de conceptos y procesos vinculados con el empleo de la fuerza armada". Esa es la razón de esta obra, en la que participan grandes especialistas en este ámbito, como **Alberto Guerrero, Beatriz Cózar, Christian Villanueva, Rocío Vales, Jesus Román, Samuel Morales** y **Javier Miguel Gil,** quien, precisamente, es el autor del capítulo dedicado a la ciberguerra y sus implicaciones estratégicas.

DOCUMENTOS SiC
Nº 41
ABRIL 2024

V-Valley | Lidera

Protección de la cadena de suministro: Lidera Cloud plataforma de contratación de servicios de ciberseguridad para el canal

Conxi Palmero
Directora de Alianzas Estratégicas del Grupo Esprinet

Dámaso Ramos
Gerente de la Unidad de Negocio de Servicios de Ciberseguridad en V-Valley | Lidera

Servicios de valor orientados a acompañar al *partner* en todo el ciclo de vida de sus proyectos

Talento, con conocimiento, de un equipo experto con un portafolio innovador

Punto de encuentro entre fabricantes, revendedores y usuarios de tecnología

V-Valley I Lidera: Soluciones avanzadas de ciberseguridad basadas en la confiabilidad, la innovación, la excelencia y la capacitación

Desde que naciera en Italia, en 2011, el Grupo Esprinet se ha convertido en uno de los distribuidores de tecnología de referencia en Europa. Su apuesta por la ciberseguridad a través de V-Valley I Lidera también se ha visto refrendada por un crecimiento constante y la cada vez mayor demanda de sus productos y servicios por parte de grandes y medianas empresas, así como en múltiples sectores. Fruto de su buen hacer fue reconocida, en 2023, como mejor mayorista en ciberprotección por Context.

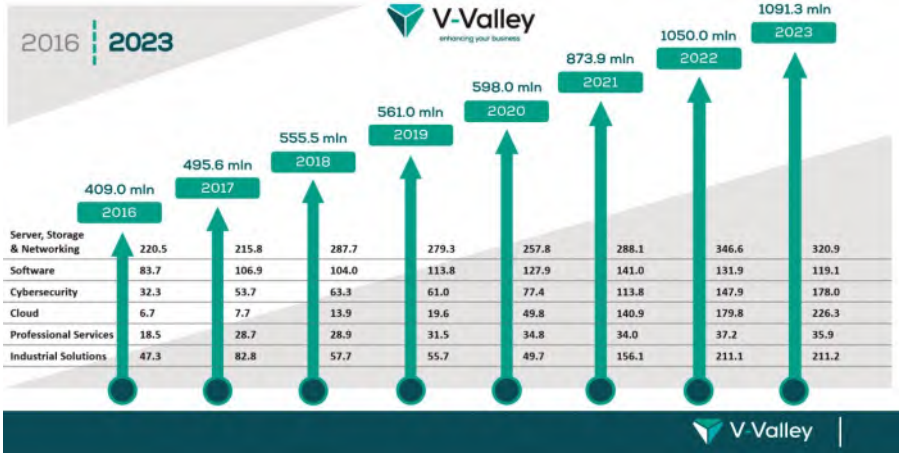
Con el objetivo de "promover la democracia tecnológica y guiar a las personas y las empresas hacia la digitalización", **Grupo Esprinet**, fundado hace más de 20 años en Italia, se ha convertido en poco más de una década en una referencia para el mercado del sur de Europa. En su éxito reside una clara apuesta por "ofrecer la experiencia de una multinacional, financieramente sólida, con un conocimiento preciso del mercado local, que la ha convertido en un socio de confianza para todo tipo de clientes que apuestan por impulsar su negocio a través de la transformación digital segura", destacan desde la compañía que, en 2023, facturó casi 4.000 millones de euros, tiene hoy más de 31.000 clientes, 650 marcas distribuidas, una plantilla superior a 1.800 especialistas, y oficinas en Italia, España, Portugal y Norte de África.

Unas cifras que, según ha señalado su director general, **Alessandro Cattani**, crecerán en 2024 por la recuperación de mercados en los que son una referencia, como el de pantallas y dispositivos, además de cuatro áreas en la que tiene una presencia más que notable como son la IA generativa, Ciberseguridad, 'Todo como Servicio' y Sostenibilidad. Y, en ellas, jugará un papel protagonista su división de ciberseguridad, nube y *data center*, **V-Valley I Lidera**, cuya plantilla ya roza los 670 empleados (más de un centenar en Iberia), y que el pasado año alcanzó una facturación de casi 1.100 millones de euros sumando sus áreas de ciberprotección, servidores, almacenamiento, redes, software, *cloud*, servicios profesionales y soluciones industriales.

David Gasca, Director Marketing Enterprise Security; Alberto López, Director Enterprise Security; y Dámaso Ramos, Business Unit Manager de Lidera Cloud.

Enfoque local, tecnología global

Decía el cofundador de **Apple**, **Steve Jobs**, que para tener éxito aconsejaba estar tan cerca de los clientes "que puedas decirles qué necesitan antes de que lo sepan por sí mismos". Y se trata de una máxima que también define el trabajo y enfoque tanto del Grupo como del área de protección de V-Valley I Lidera, uno de los grandes referentes en el mercado de *Advanced Solutions*. Con el lema '*Enhancing Your Business*' –'Mejorando tu negocio'–, la compañía acompaña a los clientes en su apuesta por la transformación digital segura ofreciendo una excelente simbiosis entre la experiencia de una multinacional y la agilidad y el conocimiento del mercado local de un mayorista con vocación ibérica, que centra su trabajo en servir de manera eficiente y personalizada a sus *partners*.



"El principal valor diferencial de la compañía radica en su equipo de expertos, integrado por más de 70 especialistas en ciberprotección con foco en todas las áreas comerciales, independientemente del tamaño de empresa y con todo tipo de perfiles técnicos"

El valor del talento

Por ello, V-Valley destaca que su reto es "ser el punto de contacto clave entre fabricantes, revendedores y usuarios de tecnología". Desde que llegara en 2018, el director de Enterprise Security de V-Valley, **Alberto López**, ha basado su éxito en "potenciar las capacidades técnicas y de servicios de la compañía, sumado al equipo comercial enfocado en el área de SMB en ciberseguridad". Precisamente, el talento y el conocimiento es uno de los grandes pilares de la compañía. "Nuestro valor diferencial es nuestro equipo, integrado por más de 70 especialistas en ciberprotección con foco en todas las áreas comerciales, independientemente del tamaño de empresa y con todo tipo de perfiles técnicos".

Oficinas de V-Valley | Lidera en Madrid

Por eso, para 2024, la compañía se ha marcado como objetivo "potenciar los servicios a los *partners*, desarrollar el mercado de mediana y pequeña empresa (SMB) y seguir trabajando en el catálogo de soluciones", una estrategia que, sumada a su buen hacer, le ha permitido en menos de una década multiplicar su facturación de los 32 millones de euros de 2016, a 178 millones el año pasado y ser reconocida en 2023 como mejor mayorista en ciberprotección por la reconocida **Context**. En 2024, su apuesta será ir más allá de la gran empresa a través de servicios para pymes, con una plataforma innovadora y pionera en este ámbito, como es Lidera Cloud. Con ella, quiere llevar las mejores soluciones a un sector cuya demanda de seguridad cibernética no deja de crecer por su apuesta por entornos como la nube y las nuevas tecnologías. A ello se suma una variada oferta de servicios y un portafolio de casi 35 fabricantes "con la máxima especialización y pensadas para cubrir todo tipo de necesidades y capacidades de última generación", explica el director de Marketing Enterprise Security, **David Gasca.**

"Trabajar con equipos con elevado *know-how* técnico y una gran empatía para entender las necesidades del canal y de nuestros clientes, es crucial en nuestras alianzas"

Economista por la Pompeu Fabra, Palmero cuenta con una dilatada trayectoria en tecnología, donde comenzó en el área de Control de Gestión y Auditoría, habiendo desempeñado roles de responsabilidad en PwC, Computer Gross y Sesa Spa. Desde hace un año, está a cargo de las alianzas de valor del Grupo Esprinet y, por supuesto, en V-Valley | Lidera.

Conxi Palmero
Directora de Alianzas Estratégicas del Grupo Esprinet

– Cuenta con más de 25 años en el sector Tech. ¿De qué depende que una alianza, en ciberseguridad, sea un fracaso o un éxito?
– Sobre todo del factor humano. Trabajar con buenos equipos con elevado *know-how* técnico y, a su vez, una gran empatía orientada a entender las necesidades del canal, de nuestros clientes, es crucial para el éxito de nuestras alianzas estratégicas.

– ¿En qué ha evolucionado la forma de acometer alianzas en ciberprotección en los últimos años?
– El rol de los mayoristas de soluciones ha cambiado mucho, los grandes *vendors* tecnológicos globales no buscan sólo *partners* tácticos y operativos en un territorio, sino socios estratégicos que sean capaces de comprender dinámicamente las necesidades del canal y sepan gestionarlas proactivamente, buscan agregadores de competencias, educadores en nuevos *trends*, orquestadores de la gran complejidad del mundo de la ciberseguridad. En un contexto muy dinámico como el que vivimos, con amenazas exponenciales, ser un *partner* estratégico para el *vendor* y para tu clientela significa crear verdadero valor añadido.

– ¿En qué áreas se va a apostar más por alianzas para crecer en este ámbito?
– V-Valley en *cyber* es un proyecto de éxito que ya cuenta con una cartera de soluciones muy innovadoras. Nos gusta trabajar con líderes por *trend* tecnológico, que resuelvan los problemas concretos, con una clara política de canal y que no pierdan el contacto con las necesidades evolutivas de los ecosistemas a los que nuestros clientes se dirigen. Con estos ingredientes se crea un proceso virtuoso de '*demand generation*' al que todos juntos contribuimos, cada uno con su rol. Este es el perfil de alianzas que buscamos. Tenemos que tener claro que jugamos un rol estratégico, que no somos solo un *partner* táctico.

– ¿Sus principales retos en materia de alianzas para 2024 en V-Valley | Lidera?
– ¡Muchos! La racionalización de la cartera de oferta de la compañía que se ha enriquecido ampliamente con la adquisición de Lidera; extender nuestra capacidad para ofrecer servicios especializados para el canal, ayudando a nuestros clientes en su actividad, así como crear nuevos servicios habilitadores que soporten a nuestros clientes ante un número creciente de amenazas.

– ¿Qué papel juega la IA en ciberseguridad y cómo espera acometer su integración en la oferta de V-Valley?
– La introducción de la IA es una tendencia clave en toda nuestra oferta, no solo en la de ciberseguridad, pero entendámonos: la IA tiene que ser un medio y no un fin para mejorar y ayudar a nuestros clientes de manera más inteligente y adaptativa. En el centro de nuestras decisiones están y estarán nuestros clientes y sus necesidades evolutivas. Nuestro Grupo cuenta ya con un equipo de data *scientists* que ayudan a construir las ofertas y adaptarlas, además de haber invertido desde hace años en uno de los *automated marketplaces* propietarios más a la vanguardia del mercado, colaborando con nuestros *vendors* de referencia para soportar las nuevas modalidades de oferta tecnológica '*as a service*'. Creo que pocos mayoristas poseen este tipo de recursos en ciberseguridad.

Dámaso Ramos

Gerente de la Unidad de Negocio de Servicios de Ciberseguridad en V-Valley | Lidera

Ingeniero, apasionado por la ciberseguridad y firme creyente de que el esfuerzo y el talento son la mejor forma de ofrecer productos y servicios de calidad, Dámaso Ramos es el responsable de una de las áreas más innovadoras de V-Valley | Lidera, con una firme apuesta por los servicios para las pymes. En las oficinas de la compañía, en Madrid, desvela las claves de esta nueva propuesta que aspira a ser una referencia, también en Europa.

"Lidera Cloud permite a los *partners* convertirse en proveedores de ciberseguridad gestionada para pymes sin realizar una inversión inicial"

– ¿Qué ha supuesto para Lidera su integración en V-Valley? Y viceversa.

– Lo mejor que se puede decir de esta integración es que no ha habido fricciones. Todas las piezas han encajado a la perfección, ya que disponemos de dos portafolios complementarios. Con ello, el éxito que viene cosechando el equipo de ciberseguridad de V-Valley en la gran cuenta se ve complementado por los que integramos Lidera que, históricamente, hemos destacado por aportar un valor diferencial en otros segmentos de mercado. Así que, para los que formamos parte de Lidera, esta integración supone pasar a formar parte de una gran organización, con todo lo que ello supone en términos de proyecto y de retos profesionales.

– Cada vez es más complicado diferenciarse en un mercado como el de la ciberseguridad en Iberia, ¿cuál es la clave para que los clientes perciban el valor de una propuesta?

– Sí, cada vez hay más actores en nuestro sector y, también, cada vez más especializados. En nuestro caso, tenemos claro que la mejor forma de diferenciarnos es aportar al canal aquello que demanda. Nuestro sector lleva tiempo orientándose hacia los servicios gestionados, y con la nueva área de Lidera Cloud ofrecemos una plataforma que permite al *partner* entregar este tipo de servicios sin realizar una inversión costosa en infraestructura.

– ¿Cuáles son los problemas técnicos y tecnológicos con los que se encuentran los CISOs y las empresas para estar actualizados en un panorama de amenazas cada vez más complejo y cambiante?

– Resiliencia, IA y tecnologías cuánticas son temas de actualidad para todas las empresas. Sabemos que cualquier estrategia debe apoyarse en tres pilares: tecnología, personas y procesos. En las grandes organizaciones esto es algo que está asumido y se aplica con excelencia. A medida que vamos bajando en la pirámide empresarial, el acceso a los dos últimos pilares, personas y procesos, se hace más complicado. Es aquí donde nuestro canal y herramientas –como Lidera Cloud– van a jugar un papel fundamental.

– Acaban de poner en marcha la plataforma Lidera Cloud, como una de las grandes áreas de negocio de V-Valley, de la que es responsable. ¿Qué ha sido lo más complejo y lo que más valor aporta?

–Lidera Cloud es el resultado de más de 20 años de experiencia ofreciendo ciberseguridad como servicio a nuestros socios. La pusimos en marcha en junio del año

pasado, con el objetivo de consolidar el conjunto de servicios que ya ofrecíamos. Esto quiere decir que nuestro canal ya está concienciado para ofrecer servicios de ciberseguridad a clientes pequeños y medianos apoyándose en nuestra plataforma.

– **¿Cuáles son los pilares en los que basarán su éxito?**

– A través de esta plataforma ofrecemos a nuestros *partners* la posibilidad de hacer provisión automática de servicios, pero lo que más valoran los clientes es el acompañamiento que realizan nuestros equipos comerciales y técnicos. Nuestros consultores acompañan al cliente durante todo el proceso de *onboarding* en la plataforma capacitándoles en cada una de las tecnologías que van a utilizar. Una vez en producción, ofrecemos un servicio de soporte de nivel I y II con ingenieros y procesos certificados por nuestros fabricantes.

– **Dar servicio 24x7 a miles de clientes finales también exigirá un esfuerzo importante…**

– Sin duda. Por ello, lo que intentamos es buscar la excelencia, no solo en la capacitación de nuestro equipo y en el trato hacia los clientes, sino también en las herramientas y procesos que utilizamos para soportar el servicio.

“Lidera Cloud ofrece servicios de protección del *endpoint*, *backup* y recuperación de desastres, gestión de parches, cifrado de dispositivos, control de datos y protección de correo electrónico. Próximamente, añadiremos soluciones de concienciación”.

– **¿Cuál será la solución más innovadora que se podrán disfrutar a través de ella? ¿También van a ofrecer el hardware como servicio?**

–Intentamos construir un portafolio de soluciones que incluya todas las tecnologías que nuestros clientes necesitan. Eso significa que sí: estamos trabajando para añadir hardware como servicio. El hecho de formar parte del Grupo Esprinet con una plataforma logística capaz de realizar más de 5.000 expediciones al día y con el soporte financiero necesario, nos facilita mucho para ofrecer el hardware en Lidera Cloud.

– **¿Cuáles son las áreas de la ciberprotección con las que comenzarán y hacia cuáles aspiran a que sean sus grandes protagonistas?**

– Actualmente, Lidera Cloud ofrece servicios de protección del *endpoint*, *backup* y recuperación de desastres, gestión de parches, cifrado de dispositivos, control de datos y protección del correo electrónico. Próximamente, añadiremos soluciones de concienciación, un elemento crítico en cualquier estrategia de seguridad. En cuanto al *roadmap*, en el corto plazo tenemos planes para incorporar hardware como comentábamos anteriormente y soluciones de protección de entornos *cloud*. En paralelo, seguiremos añadiendo funcionalidades a la plataforma para que los *partners* tengan la posibilidad de hacer una gestión completa de las suscripciones de sus clientes, desde la venta y provisión hasta la facturación.

– **Para el sector público, ¿cómo garantizarán que cumplen con el Esquema Nacional de Seguridad (ENS) en la cadena de valor del servicio, algo que les afecta a ustedes, a sus integradores y a sus fabricantes?**

“Aprovechamos nuestra experiencia, capacidades y la cercanía con nuestros clientes para escuchar sus demandas y poder dotar a nuestra plataforma de las tecnologías, funcionalidades y servicios que demandan”.

– Siempre intentamos aplicar el concepto de *security by default* en nuestros desarrollos. Todos nuestros programadores tienen una amplia experiencia en el desarrollo de plataformas y en la integración con las interfaces de programación que nos ofrecen nuestros fabricantes. Adicionalmente, seleccionamos siempre tecnologías que cumplan con las normativas existentes, con *data centers* en la Unión Europea, cumplimiento del ENS y, a aquellos fabricantes que aún no lo han hecho, les ayudamos a incorporar sus soluciones al Catálogo CCN-STIC.

– **¿Qué plataforma similar toman como referencia en otros países…?**

– Sinceramente, no nos hemos fijado en otras plataformas.

– **¿Cómo evitarán hacer la competencia a otras empresas que pueden ofrecer, por ejemplo, SOC virtuales a sus clientes?**

– Por supuesto, no queremos ser competencia de nuestros *partners* y, de hecho, no lo somos. Más bien todo lo contrario, somos su complemento perfecto. Lidera Cloud es un vehículo para llegar a una tipología de clientes para los que probablemente no sea rentable desplegar los recursos que requiere un servicio de SOC.

– **Su objetivo para 2024…**

– De puertas hacia dentro, crecer, por supuesto y evolucionar la plataforma añadiendo nuevas funcionalidades y servicios. De puertas hacia afuera, dar visibilidad al mercado de la existencia de Lidera Cloud hasta convertirla en una referencia en el sector. También, tenemos el objetivo de consolidar y hacer crecer el negocio de servicios profesionales. Para ello, estamos invirtiendo en recursos propios que nos permitan ser capaces de ofrecer a nuestros socios unos servicios de calidad.

– **Una frase con la que le guste resumir las capacidades y bondades de Lidera Cloud…**

– Lidera Cloud es una plataforma que permite a los *partners* convertirse en proveedores de servicio sin realizar una inversión inicial y con un portafolio de soluciones que cubre las necesidades de la mayoría de los clientes. ●

Lidera Cloud, la propuesta de V-Valley a su canal para prestar servicios avanzados y automatizados de ciberseguridad a cliente final pyme

En marcha desde mediados de 2023, la pionera plataforma Lidera Cloud, la gran novedad de V-Valley en ciberseguridad, se está convirtiendo en referente nacional. A través de ella, las pymes pueden disponer de la tecnología de nueva generación de cerca, de momento, de una decena de grandes especialistas como Acronis, Kaspersky, WatchGuard y Check Point, con sólo un clic. Incluso, de hardware que también se ofrece como servicio. Con esta nueva área de negocio, amplía las capacidades del portafolio de V-Valley | Lidera con cerca de 35 firmas para disponer de productos de ciberprotección, servicios, formación e, incluso, financiación, pilares que le convierten en uno de los grandes mayoristas en este ámbito en Iberia y sur de Europa.

"La plataforma de gestión de servicios de suscripción, Lidera Cloud, ofrece la posibilidad de provisionar servicios de ciberseguridad de manera automática y desatendida. Nuestros *partners* pueden acceder a su espacio de trabajo unificado, donde tienen la posibilidad de contratar y gestionar las soluciones de distintos fabricantes ofrecidos en ella, así como administrar sus usuarios". Buscando la simplicidad de uso, capacidades avanzadas y basada en la gran experiencia en la mediana y pequeña empresa de Lidera (desde 2023, integrada en V-Valley | Lidera), esta nueva área de negocio del mayorista no deja de crecer, ya que responde a las inquietudes de socios y, sobre todo, de usuarios finales que encuentran en ella su propio espacio de trabajo desde donde pueden acceder a todos los servicios contratados.

Por supuesto, se suma al conjunto de servicios orientados a acompañar al socio en todo el ciclo de vida de sus proyectos. Una idea que surgió tras ver que el proceso de negocio tradicional de reventa de licencias "era largo, con muchos actores, acciones y poco automatizado, lo que convertía la contratación en un asunto que se prolongaba durante días". Estos aspectos se simplifican ofreciendo la ciberprotección desde una plataforma, apostando por la sencillez y rapidez, ya que, a través de ella, se puede "proporcionar al *reseller* las herramientas necesarias para la venta, administración y facturación de servicios y clientes a través de un único portal de gestión, dando a nuestros *resellers* la posibilidad de suscribir un servicio de forma autónoma 24x7".

Apuesta por la facilidad

Entre las razones de su éxito, en poco más de un año, también destaca que Lidera Cloud reúne fabricantes mundialmente reconocidos en una plataforma de gestión que ofrece soluciones de protección del *endpoint, backup* y recuperación de desastres, gestión de parches, cifrado de dispositivos, control de datos y protección del correo electrónico. Así, a través de Lidera Cloud ya se puede disponer de las capacidades de **Acronis, BlackBerry, Hornetsecurity, Kaspersky** y **WatchGuard.** Además, estarán en breve referentes como **Check Point, Cloudflare** y **Trend Micro.**

Junto a ello, el equipo especializado de Lidera Cloud acompaña al socio de canal durante todo el proceso de adopción de la plataforma, además de asesorarle en la elección de las soluciones más adecuadas para cubrir las necesidades de sus clientes. Comprende, incluso, el paso a paso de capacitación en el uso de la plataforma, así como en cada una de las tecnologías elegidas, tanto con sesiones formativas como con apoyo en los primeros despliegues. Y, asimismo, con un seguimiento para "asegurar que todo está funcionando de la manera esperada a través de, entre otros aspectos, un servicio de soporte de nivel I, II y III para todas las tecnologías", además de mantener al corriente a los socios de todas las novedades que se incorporan. "Se trata de ser un compañero, más que un socio comercial", recuerdan sus impulsores.

En cuanto al coste de esta propuesta, la plataforma está pensada para que los "*partners* se vean beneficiados de mejores condiciones económicas a medida que van creciendo". ●

V-Valley I Lidera: Productos y servicios innovadores con el cliente en el centro y con protección y respuesta frente a amenazas avanzadas

Basando su éxito en un modelo de referencia en XaaS, *cloud* y suscripción, con un exhaustivo conocimiento del ecosistema de ciberprotección para adaptarlo a las necesidades reales de cada cliente, tanto en tecnologías, como beneficios, tiempo y recursos, la propuesta de V-Valley cuenta con cerca de 35 firmas en su portafolio. Todas centradas en ofrecer capacidades de prevención, protección y fiabilidad como servicio de valor, a través de un equipo de grandes especialistas y referentes del mercado.

Además, cuenta con un enfoque de consultoría para que el *partner* y el cliente tengan una solución a medida, siendo apoyados en todas las fases del proyecto: desde la identificación de amenazas, hasta la superficie de ataque, selección de las mejores tecnologías para ser resilientes, así como el proceso de capacitación y certificación del canal "para sacar su máximo potencial". Todo ello, con una firme apuesta por un enfoque de confianza cero mediante soluciones de gestión de vulnerabilidades, de accesos e identidad segura, punto final, protección *cloud*, de red, así como seguridad avanzada contra amenazas de nueva generación, y monitorización automática.

Formación y certificación

Además en su sede de Madrid dispone de su **'V-Valley Academy',** con más de 200 m^2, donde los *partners* pueden acceder a equipos con la última tecnología, para ayudarles en su negocio, así como a formación, certificaciones oficiales, eventos y *testing* de Advanved Solutions.

Para profundizar en sus novedades –como su plataforma Lidera Cloud–, V-Valley I Lidera celebró, en marzo, su III 'Cybersecurity Summit', en La Granja de San Ildefonso (Segovia), con los responsables de los fabricantes que componen su portafolio de ciberseguridad para compartir con sus *partners* la estrategia para 2024 y sus principales focos.

Capacidades de servicios en ciberseguridad de V-Valley

Cybersecurity	Presales	Demo/ Lab	Demo Unit Available	POC	Standard Training	Authorized Training Center	Help Desk I - II	Installation	Operational Support
A10	•	•	•	•	•	•		•	•
ACRONIS	•	•	•	•	•	•	•	•	•
BROADCOM	•								
CYBERARK	•	•	•	•	•				
CHECK POINT	•	•	•	•	•	•	•	•	•
CLOUDFLARE	•	•	•	•	•				•
ENTRUST	•	•			•				
IVANTI	•	•	•	•	•		•	•	•
KASPERSKY	•	•	•	•	•	•			
OPENTEXT	•								
SAILPOINT	•	•	•	•	•			•	•
SONICWALL	•	•	•	•	•	•	•	•	•
TRELLIX	•	•	•	•	•	•	•	•	•
TREND MICRO	•	•	•	•	•			•	•
WATCHGUARD	•	•	•	•	•	•	•	•	•
ARMIS	•	•	•	•	•				
AREXDATA	•	•							
BLACKBERRY	•	•	•	•	•		•	•	•
BACKBOX	•	•	•	•	•				
ELASTIC	•								
FORTANIX	•	•	•	•					
INVICTI	•	•	•	•	•			•	•
REDSIFT	•	•	•	•					
SECURONIX	•								
SKYHIGH	•	•	•	•	•			•	•
XMCYBER	•	•	•		•				

Portafolio de ciberprotección de V-Valley I Lidera

A10 · Acronis · AREXDATA · ARMIS · BACKBOX · BlackBerry · CA Technologies · CHECK POINT · CLOUDFLARE · CYBERARK · Cyber Guru · elastic · ENTRUST · iberlayer · invicti · ivanti · Kaseya · kaspersky · Lidera cloud · NETWITNESS · Omada · opentext Cybersecurity · REDCARBON · RED SIFT · SailPoint · securonix · Skyhigh Security · SONICWALL · sumo logic · Trellix · TREND · WatchGuard · XM Cyber

Lidera cloud

Powered by V-Valley

TU PLATAFORMA MSSP AUTOMÁTICA Y DESATENDIDA

La plataforma de gestión de servicios de suscripción MSSP que ofrece la posibilidad de provisionar servicios de ciberseguridad de fabricantes mundialmente reconocidos, de manera automática y desatendida.

ÚNETE A LAS VENTAJAS DE LIDERA CLOUD

- Modelo de suscripción
- Pago por uso
- Mayor margen por volumen
- API de provisión
- Atención comercial
- Proceso de onboarding
- Servicio integral de soporte
- Beneficios económicos

¿Quieres saber cómo integrar nuestras soluciones para acelerar tu negocio?
¡Contacta con nuestros especialistas!

www.v-valley.com

ACTOS y CONVOCATORIAS

Ignite on tour
Cybersecurity for the AI Era
Organiza: Palo Alto Networks
Fecha: 9-4-2024
Lugar: Espacio Ventas. Madrid.
Correo-e: igniteontour-emea@paloaltonetworks.com
Sitio: register.paloaltonetworks.com/igniteontourmadrid24

IV Jornadas STIC & Congreso ROOTEDCon. Capítulo Panamá
Organizan: CCN-CERT, Incibe, AIG-Panamá, RootedCon y ESPDEF-CERT
Fechas: 10/12-4-2024
Lugar: Centro de Convenciones de Panamá
Sitio: jornadas.ccn-cert.cni.es/es/ivjornada-panama

ViCon
Congreso de Ciberseguridad de Vigo
Fechas: 12/13-4-2024
Lugar: Círculo de Empresarios de Galicia. Vigo. Pontevedra.
Correo-e: vicon@galicia.com
Sitio: vicon.gal

Encuentros CCI-La voz de la industria
Toledo, 16-4-2024
Madrid, 18-4-2024
Valladolid, 9-5-2024
Organiza: CCI.
Tel.: 910 910 751
Correo-e: info@cci-es.org
Sitio: cci-es.org

Congreso ASLAN 2024
Organiza: Asociación @ASLAN
Fechas: 17/18-4-2024
Lugar: Palacio de Congresos IFEMA. Madrid.
Sitio: aslan.es

VII Congreso Auditoría & GRC 2024
Digital Trust con los Riesgos Emergentes
Organiza: ISACA Capítulo de Madrid
Fecha: 18-4-2024
Lugar: Meeting Place Castellana 81. Madrid.
Correo-e: administracion@isacamadrid.es
Sitio: isaca.madrid

I Congreso Nacional de Ciberseguridad en Fraude Digital
Organiza: Cyber Madrid
Fecha: 18-4-2024
Lugar: Pabellón de los Jardines de Cecilio Rodríguez. Parque del Buen Retiro. Madrid
Correo-e: asociados@cybermadrid.org
Sitio: congresocyberfraude.com

RSA Conference 2024
The Art of Possible
Fechas: 6/9-5-2024
Lugar: Moscone Center. San Francisco. EE. UU.
Correo-e: information@rsaconference.com
Sitio: rsaconference.com

Osintomático Conference 2024
Fechas: 17/18-5-2024
Lugar: La Nave Villaverde. Madrid
Sitio: osintomatico.com

Hack-én
Fechas: 17/18-5-2024
Lugar: Palacio de Congresos IFEJA. Jaén
Correo-e: hackencon@gmail.com
Sitio: hacken.es

Barcelona Cybersecurity Congress
Secure today, safeguard tomorrow
Organiza: Fira de Barcelona
Fechas: 21/23-5-2024
Lugar: Fira de Barcelona-Gran Vía.
Sitio: barcelonacybersecuritycongress.com

Espacio TISEC
Los ciberriesgos, en la encrucijada. El Ransomware tiene un precio.
Organiza: Revista SIC
Fechas: 19/20-6-2024
Lugar: Hotel Novotel Campo de las Naciones. Madrid.
Tel.: 91 575 83 24
Correo-e: info@codasic.com
Sitio: revistasic.com/tisec

SECURMÁTICA 2024
Manos a la obra y bien acompañados
Organiza: Revista SIC
Fechas: 8/10-10-2024
Lugar: Hotel Novotel Campo de las Naciones. Madrid.
Tel.: 91 575 83 24
Correo-e: info@securmatica.com
Sitio: securmatica.com

Identi::SIC
Identidad digital: Cebo y salvoconducto
Organiza: Revista SIC
Fechas: 20/21-11-2024
Lugar: Hotel Novotel Campo de las Naciones. Madrid.
Tel.: 91 575 83 24
Fax: 91 577 70 47
Correo-e: info@revistasic.com
Sitio: revistasic.com/identisic

JNIC 2024
IX Jornadas Nacionales de Investigación en Ciberseguridad
Organizan: Incibe y Univ. de Sevilla
Fechas: 27/29-5-2024
Lugar: ETS Ingeniería Informática
Sitio: 2024.jnic.es

FORMACIÓN CONTINUA

- **Campus Aenor**
  Tel: 91 432 61 25
  Sitio: aenorciberseguridad.com
- **Es-Ciber**
  Escuela Superior de Ciberseguridad
  Correo-e: info@es-ciber.com
  Sitio: es-ciber.com
- **Exclusive Networks**
  Tel.: 91 197 66 01
  Sitio: training.exclusive-networks.com/es-ES
- **M2i**
  Tel: 91 578 23 57
  Correo-e: info@m2iformacion.com
  Sitio: m2iformacion.com
- **One eSecurity**
  Tel.: 911 011 000
  Correo-e: info@one-esecurity.com
  Sitio: one-esecurity.com
- **Sans Institute**
  Sitio: sans.org
- **Westcon-Comstor**
  Tel: 91 419 61 00
  Correo-e: academy.es@westcon.com
  Sitio: https://academy.westconcomstor.com/es/

INDICE DE ANUNCIANTES

(one) eSecurity

Readiness · Detection · Response

¿Preparado para afrontar un ciberataque?

Confía en los mejores expertos

Readiness

- Cyber Consulting (CyCon)
- Cyber Exercises (CybEx)
- Cyber Insurance (Cybins)
- Cyber Threat Intelligence

Detection

- Deception
- Threat Hunting (TH)
- Compromise Assessment
- Managed Threat Hunting (MTH)

Response

- Emergency Incident Response (EIR)
- Digital Forensics (DFIR)

Detection & Response

- Managed Detection and Response

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

espacio tiSec

LOS CIBERRIESGOS, EN LA ENCRUCIJADA

EL RANSOMWARE TIENE UN PRECIO

Organiza: Revista SIC

Madrid
19 y 20 de junio _2024
www.revistasic.com/tisec