



30 años sic

Revista

www.revistasic.com

Ciberseguridad, seguridad de la información y privacidad

ENTREVISTA



Domingo Cardona

CEO y Cofundador
WISE SECURITY

AUTONOMÍAS

- CIC4Cyber en Cataluña
- Estrategia de Andalucía

ESTÁNDAR

La ISO/IEC 27002,
actualizada

DESINFORMACIÓN

Combatirla desde
la ciberseguridad

ESTRATEGIA

DEVO: Seguridad
analítica

PROYECTOS

- EMASA
- MUSEO DEL PRADO

EN CONSTRUCCIÓN

La Ciberguerra
entre escombros

Gemelos cibernéticos

2022, una odisea digital

MAYOR RENTABILIDAD Y VALOR

Ciberseguridad Corporativa



Descubre nuestra propuesta XaaS de última generación.

PROPUESTAS DE

XaaS

DE ÚLTIMA GENERACIÓN

Seleccionamos e introducimos en el mercado las soluciones más innovadoras para ayudar a las compañías en el crecimiento tecnológico y acelerar su transformación digital.

Equipo experto

Tecnologías punteras

Soluciones adaptativas

Capacidad financiera

Network

Cloud

Workplace

Aplicación

Dato

Gestión



BARCELONA

BILBAO

MADRID

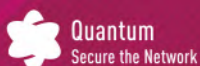
LISBOA

SEVILLA

ZARAGOZA

YOU DESERVE THE BEST SECURITY

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



MÁS INFORMACIÓN: www.checkpoint.com/es

info_iberia@checkpoint.com

>> Sumario



DOCUMENTOS



118 DOMINGO CARDONA,
CEO de Wise Security

6	EDITORIAL	156	PROPUESTAS
8	DOBLE FONDO	164	NOVEDADES
10	SIN COMENTARIOS	172	EVENTOS Y FORMACIÓN
12	NOTICIAS	174	BIBLIOGRAFÍA
102	PROYECTOS	178	ACTOS Y CONVOCATORIAS
140	INFORMES Y TENDENCIAS		

>> en este número

- 108** El mundo ha cambiado. El estándar internacional ISO/IEC 27002, también, por BORIS DELGADO y CARLOS MANUEL FERNÁNDEZ
- 112** CIC4CYBER en Cataluña: conocimiento, innovación y ecosistema, la apuesta consciente, por TOMÁS ROY
- 116** Estrategia de Ciberseguridad de Andalucía 2022–2025, por RAÚL JIMÉNEZ y ANTONIO REQUENA
- 122** La Ciberguerra entre los escombros, por JORGE DÁVILA
- 125** Ciberseguridad en Gemelos Digitales, por JAVIER LÓPEZ y CRISTINA ALCARAZ
- 132** Combatir la desinformación desde la ciberseguridad, por ALFONSO FRANCO
- 134** Teletrabajo: Reto técnico, reto humano, por ANTONIO DELGADO
- 138** ESTRATEGIA: DEVO: la seguridad analítica en la empresa llevada a un nuevo nivel, por MARC VAN ZADELHOFF

• **Plan Nacional de Ciberseguridad.** No se ha hecho público oficialmente el contenido del Plan Nacional de Ciberseguridad (PNC), aprobado por el Consejo de Ministros el pasado 29 de marzo del presente. Sí se ha indicado que dicho Plan se presentó al Consejo de Seguridad Nacional a mediados de noviembre de 2021, y que este informó favorablemente. Con posterioridad, y tras la publicación en diciembre de la Estrategia de Seguridad Nacional 2021, el texto se actualizó.

Parece ser que el PNC “contiene más de 130 actuaciones, cuya implementación asciende a un importe total de 1.000 millones de euros. Una parte importante de ellas ya tienen adjudicada su financiación. El resto se ejecutarán en años próximos, una vez se disponga de los recursos económicos necesarios. Una gran parte de las medidas incluidas en el plan están vinculadas al Plan de Recuperación, Transformación y Resiliencia”.

Algunas de esas actuaciones ya son antiguas conocidas (alguna muy antigua): SOC de la AGE, plataforma nacional de notificación, sistema nacional de indicadores de ciberseguridad...

Según se ha indicado a SIC, el documento es de difusión limitada y su publicación y/o publicidad supondría poner en riesgo el diseño y arquitectura de la ciberseguridad en España..., y dar publicidad al detalle del Plan, más allá de su contenido genérico, sería contraproducente.

Obviamente, entre decir lo que se ha dicho del Plan y dar información detallada hay un termino medio razonable. Incluso convendría aclarar si la pieza contiene más de 150 medidas, más de 130 o más de 100. Esperemos que lo de los 1.000 millones no tenga fluctuaciones.

Ya sabe, lector: la ciberseguridad es cosa de todos. Pero de algunos más que de otros.

• **Espacio TiSEC 2022.** Los días 27 y 28 de abril, en Madrid, tendrá lugar una nueva edición de este evento de SIC, que en esta ocasión se denomina: **Ransomware: ¿quién paga la fiesta?** Aunque hoy este tipo de *malware* es el que más quebrantos está causando a ciberatacados, a aseguradoras y a los que forman parte de la lucha contra la cibercriminalidad, lo cierto es que hay que hablar de toda una cadena de delito, bien organizada, en la que se ataca por varios frentes para sacar beneficio económico utilizando las TIC contra las TIC y contra las personas físicas y jurídicas.

La invasión e intento de fragmentación de Ucrania por Rusia es una guerra y no una “operación militar especial”, eufemismo del gusto del presidente Putin. Y tiene una vertiente digital en la que arrecian las escaramuzas. Y esto no hace sino enriquecer los distintos colores que se esconden tras un ciberataque, y genera incertidumbres en las competencias de privados y públicos en el tratamiento de eventos y necesidades de determinar claramente si cuando acontecen, estos pueden calificarse exclusivamente como presuntos delitos económicos o tiene, además, algún otro sabor, más allá que el que pudiera estar vinculado a la legislación sobre datos personales. Y eso, como bien saben las administraciones públicas, los administrados y las aseguradoras, se puede convertir en un problemón.

• **Ciberseguridad y partidos políticos.** Desde que el Gobierno dijo que las nuevas entidades de la AGE que se creasen se ubicarían fuera de Madrid, anda todo el mundo revuelto. Y como la Ciberseguridad es ya un asunto de Estado, ha empezado a formar parte del arsenal guerrero de los partidos políticos. Si juntamos estas dos ideas, y nos vamos a León, nos encontramos con un caso curioso: allí está Incibe desde sus orígenes como Inteco y, por tanto, libre del yugo centralista del Gobierno de España. Nació, deslocalizado. Pero para la Unión del Pueblo Leonés (UPL) esto no es suficiente, sino una razón para que allí se ponga el SOC de la AGE.

No solo eso, sino que teme que la existencia del SOC de la AGE pueda restar competencias a Incibe.

Ya sabe, lector, que para hacer política barata no es necesario leerse y entender la legislación vigente. Aunque, si lo miramos desde otro punto de vista, qué es la política sino el arte de cambiar la legislación.

Edita: Ediciones CODA, S.L. Goya, 39. 28001 Madrid (España) Tels.: 91 575 83 24 / 25 Fax: 91 577 70 47 **Correo-e:** info@revistasic.com www.revistasic.com **Editor:** Luis Fernández Delgado **Director:** José de la Peña Muñoz **Redacción:** Ana Adeva, José Manuel Vera **Sección Laboratorio SIC:** Javier Areitio Bertolín **Colaboran en este número:** Cristina Alcaraz, Juan Miguel Auñón, Pablo Borchas, Alberto Cañadas, Jorge Dávila, Antonio Delgado, Boris Delgado, Jesús Doña, Carlos M. Fernández, Carlos Frago, Alfonso Franco, Karen Gaines, Jess García, Luis Grañana, Raúl Jiménez, Javier Larrea, Javier López, Pedro Martín, Félix Muñoz, Alberto Partida, Antonio Requena, Tomás Roy, Héctor Sánchez, Jesús Sánchez, Juan Miguel Velasco, Pablo Velázquez, Marc van Zadelhoff **Departamento de Marketing/Publicidad:** Rafael Armisen Gil, Fernando Revilla Guijarro **Administración y suscripciones:** Susana Montero, Maite Montero, Mercedes Casares **Fotografía:** Jesús A. de Lucas **Ilustración:** Fernando Halcón **Diseño y producción:** MSGráfica | Miguel Salgueiro **Imprime:** Monterreina **ISSN:** 1136-0623

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

SECURMÁTICA

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

**Pensar la
ciberseguridad.**

Y repensarla.

4 • 5 • 6
OCTUBRE
2022

www.securmatica.com



JOSÉ DE LA PEÑA MUÑOZ
Director
jpm@codasic.com

Plan Nacional de Ciberseguridad: menos secretitos

La sociedad ha empezado a metabolizar la presencia informativa diaria de ciberataques. Llegará un momento en que su detección y efectos dejen de tener interés en la conformación periodística de la actualidad, como en cierto modo pasa con los accidentes de tráfico.

Pero las personas físicas y las jurídicas seguirán siendo ciberatacadas mientras así se les pueda sacar la pasta –ya directa ya indirectamente– o conseguir alguna ventaja.

Digo esto porque nos encontramos hoy en una especie de cambio de fase en el contexto de la “digitalización”, en la que ya no se demoniza a la empresa que sufre un ciberataque por presuponer automáticamente que sus gestores no han hecho los deberes, al menos los legalmente exigibles. Precisamente, uno de estos deberes exigibles es, en líneas generales, el de denunciar, notificar y, en determinadas

Frente a esto, nos encontramos hoy con un Plan de Choque antiPutín, en cuyo contexto se ha aprobado un Plan Nacional de Ciberseguridad con nadie sabe qué número y naturaleza de actuaciones, dotado con 1.000 millones de euros y cuyo contenido es de difusión limitada. Al tiempo, se ha publicado un Real Decreto-ley, el 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación. Lo curioso de esta pieza, sin duda necesaria, es que casi todo lo que pudiera ser polémico lo declara confidencial, y todo lo que interesa de verdad lo fía al desarrollo de un Esquema Nacional de Seguridad de redes y servicios 5G, que se publicará en forma de Real Decreto. Recordemos que todavía no ha visto la luz el Real Decreto del “nuevo” Esquema Nacional de Seguridad, el ENS. La cosa va de esquemas.

En el mundo de hoy, en el que la seguridad de un país es la de usted, la mía, la de la vecina del quinto, la de la panadería, la del Ibex, la de un pequeño ayuntamiento... no se puede concebir una Ciberseguridad Nacional de perímetro desmesurado y sobre la base de lo secreto, lo confidencial, lo reservado, lo restringido...

Menos lobos

En el mundo de hoy, en el que la ciberseguridad de un país es la de usted, la mía, la de la vecina del quinto, la de la panadería, la del Ibex, la de un pequeño ayuntamiento... no se puede ir montando una Ciberseguridad Nacional de perímetro desmesurado y sobre la base de lo secreto, lo confidencial, lo reservado, lo restringido... cuando a los

circunstancias, comunicar el hecho también a los que se hayan podido ver afectados.

Sin embargo, la superficie de ataque no hace sino crecer y la dificultad de desenmarañar eventos que afectan a varios sectores y a las cadenas de suministro resulta francamente compleja.

Ante esta situación, que viene produciéndose desde hace tiempo, algunas organizaciones de cierto porte, especialmente privadas, se han quejado de la escasa ciberprotección que brinda el Estado a la sociedad. Es más, algunos empiezan a estar hartos de los pocos resultados que dan las denuncias, hecho que, desde luego no es culpa de las policías ni de los tribunales, sino de todo el sistema en su conjunto. Y también hay quien, con razón, se queja de las exigencias de cumplimiento al sector privado y de la calamitosa situación de la gestión de la ciberseguridad en las administraciones públicas, que no es culpa de esos servidores públicos y contratados que llevan intentando desde hace años que la cosa mejore, sino de la cuestionable calidad de la clase política que nos viene gobernando desde hace más de una década.

demás se les pide transparencia, denuncia, notificación e inspecciones. No va con los tiempos. En fin, hasta el patriotismo evoluciona.

Los ciberataques son cosa seria; pero están dejando de ser percibidos así socialmente. Tenía que pasar. Y para sentir la cotidianeidad de este fenómeno, nada mejor que leerse la Sentencia 37/2022, de 14 de marzo del presente, de la Sala de lo Social de la Audiencia Nacional sobre la petición de ERTE por fuerza mayor que solicitó Ilunion tras haber sufrido una infección motivada por un *ransomware* de la familia Ryuk. La demanda la ganó la compañía y la perdió el Ministerio de Trabajo y Economía Social. Pero eso, con ser importante, no es lo que quiero destacar aquí. Lo que interesa es cómo se especifican los hechos probados (entre otros la existencia del ciberataque), los actores que se mencionan en la sentencia (clientes y proveedores), el papel que juega el estado de madurez de la gestión de ciberseguridad de la organización afectada y la activación de una póliza de seguros ante el hecho acontecido. Sinceramente, el texto es de obligada lectura para un profesional de la ciberseguridad. ●



Experiencia Simplificada

La plataforma Cisco SecureX proporciona una experiencia integrada que simplifica la gestión de su entorno de seguridad

Descubra cómo la plataforma XDR de Cisco puede elevar sus objetivos de seguridad en <https://www.cisco.es/securex>





LUIS FERNÁNDEZ DELGADO
Editor
lfernandez@codasic.com

GRU, mi cibervillano favorito

Irónicamente ha querido la casualidad que la denominación del personaje estelar de la franquicia de animación cinematográfica, **GRU** –tan gamberrete y ladronzuelo él como bien apañado técnicamente– responda al mismo acrónimo que Rusia tiene para su servicio de inteligencia exterior con más pegada: el **Glavnoe Razvedytalnoe Upravlenie**.

Esta potente unidad –de corte militar– es, según todos los indicios más plausibles de ‘atribución’, el emisor y, al tiempo, generoso contratante de hordas de villanos digitales que desde tiempo ha vienen hostigando a los perversos lares occidentales. Entre sus envenenados ‘regalitos’ figuran APT28, CyberBerkut, CyberCaliphate y Sandworm.

Las acciones cometidas por esta facción y otras de cuño similar retratan a Rusia como un incisivo actor muy tempranamente consciente de la importancia de manosear las redes en beneficio propio, ya destruyendo ya distorsionando el normal fluir informativo y digital desafecto con su sentir.

Ciberbrigadistas internacionales

–sean *Hackerberry Finns*, *chiquilihackers*, *hackerveydiles* o *hackermanitas*–, enarbolando causas pretendidamente justas y al margen de coordinarse con el ciberejército de su propio bando, no paran de adentrarse en la tundra ‘cibersovietzarista’

Sus trapacerías digitales –y las de sus hermanos de propósito FSB y SVR–, que se remontan ya a un par de décadas, cobran recientemente importancia decisiva por el conflicto de esta ‘tropa’ con Ucrania y, por derivada, con el bando occidental que sintoniza con el estado soberano ubicado en Europa oriental.

Rememorando el mítico libro de Erich Maria Remarque “Sin novedad en el frente”, cabe decir que, paradójica y dolorosamente, ahora sí las hay en esta nueva guerra del siglo XXI. Y no pocas. El conflicto ruso-ucraniano ha desatado, ya desde sus prolegómenos, que la actividad ciberbélica ‘oficial’ se posicionara madrugadoramente desde todos los frentes y bandos, erigiéndose en perfecto pretexto para probar un descomunal surtido de ciberacciones y arsenal digital emplazado a causar el mayor impacto posible en el contrario y, por otro lado, también a ensayar acciones inéditas de control, rastreo y destrucción cibernéticas.

La realidad percibida –en lo que ha trascendido– muestra que el resultado viene siendo desigual. Junto a mediáticos golpes de efecto con sonadas interrupciones DDoS, acciones de hackeo a ‘targets’ financieros e IC, sustracción y publicación de archivos, interposición de información y periodistas reivindicativos en telediarios..., también muestra la otra cara, mucho menos exótica. Me refiero al intento, *fake* mediante, de hacer colar que el presidente Zelenski pedía en línea la

rendición de su país. Sin duda, el bodrioso intento de servirse de imágenes del mandatario adulteradas por parte de los Josef Goteras y Otiliov, quedará para los anales de la ciberchapuceria.

Por otro lado, junto a la panoplia de acciones ‘cyberarmy style’ por parte de los contendientes –y agentes aliados– esperables en esta poliguerra dimensional, han convergido también otros tipos de respuesta, mucho más informales cuando no frikis, de consecuencias impredecibles. Este hecho, realmente inédito en la historia de las contiendas, hace referencia al protagonizado por hordas de ‘hackers’ bienintencionados y venidos arriba –ya en grupeto ya en solitario– que en plan despendole estampídico, cibervolando caóticamente por libre con ciberquincallería barata y al son emulador del himno rockero “We will, we will hack you...”, se han estado abalanzando sobre los activos digitales del enemigo para causar el mayor estropicio posible y, si suena la flauta, también para tratar de pillar alguna de las succulentas recompensas aireadas para identificar artífices rusos de actividades maliciosas.

Lo cierto es que estos ciberbrigadistas internacionales –sean *Hackerberry Finns*, *chiquilihackers*, *hackerveydiles* o *hackermanitas*–, enarbolando sin duda causas pretendidamente justas y al margen de coordinarse con el ciberejército de su propio bando, no paran de adentrarse en la tundra ‘cibersovietzarista’ sin mensurar las consecuencias derivadas de sus inconscientes e impulsivas incursiones –no siempre adecuadamente anónimas– por las que, por su rastro, podría colegirse las ubicaciones y su país de origen. Y como fruto de ello sobre-

viniesen contundentes respuestas a fin de causar escarmiento y disuasión a futuro.

Bien está que aflore el talento lateral de la pericia hacker y que coadyuve a la causa. Sin ir más lejos, esta destreza quedó patente en la reciente RootedCON cuando algunos de sus más insignes ponentes mostraron las triquiñuelas para con la app Telegram –casualmente muy usada por la resistencia ucraniana– o las debilidades de IC eléctricas, evidenciadas por espabilados expertos de Tarlogic, ambos dos perfectos ejemplos de aplicabilidad al asunto que nos trae.

Sirva pues como reflexión final que ante los daños colaterales provocados por la oleada de ciberagresiones al por mayor –y por libre– al imperio autárquico ciberzarista, este opte por repelerlas a machete como actos de guerra o más arteramente introduzca topes prorrusos en las filas occidentales, por ejemplo en aquellas empresas de ciberprotección que, tan generosas ellas, con los brazos abiertos se han mostrado dispuestas a acoger a expertos/as ucranianos huidos...

En el sofisticado tablero digital planetario en el que nos hayamos, ¿basta con cambiar a granel las contraseñas a nivel local y anunciar mesnadas de planes de choque sin concretar o nos pertrechamos de ciberseguridad adulta? A fin de cuentas, se trata de que nosotros también juguemos o de que jueguen con nosotros. Quilósá. ●

A woman with short brown hair, wearing a blue button-down shirt, is looking down at a tablet computer she is holding with both hands. She is standing in a factory or industrial setting, with blurred machinery and lights in the background.

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



© 2021 PricewaterhouseCoopers, S.L. Todos los derechos reservados. "PwC" se refiere a PricewaterhouseCoopers, S.L., firma miembro de PricewaterhouseCoopers International Limited; cada una de las cuales es una entidad legal separada e independiente.

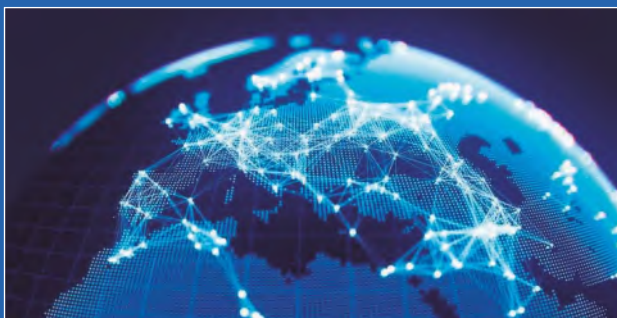
El CSIRT-EU, que cumple 10 años, cambiará su denominación a 'Centro de Ciberseguridad'

La Unión Europea creará un fondo para hacer frente a posibles crisis cibernéticas de alguno de sus estados miembro e impulsar su ciberresiliencia

La UE continúa dando pasos para fortalecer su hegemonía digital, también en ciberseguridad. En marzo, los gobiernos europeos aprobaron una declaración apostando por reforzar las capacidades del territorio comunitario a través de la creación del 'Fondo de Respuesta de Emergencia para Ciberseguridad', para hacer frente a posibles crisis cibernéticas, y el incremento de la financiación de los programas nacionales que permitan crear un mercado para proveedores de servicios de ciberseguridad confiables.

"Los recientes ataques cibernéticos dirigidos a Ucrania en un contexto de crecientes tensiones geopolíticas han demostrado cuán importante es la dimensión cibernética en los conflictos actuales", destaca el documento que, también, recuerda la necesidad de "que la UE avance con un plan ambicioso e integral para su ciberseguridad" a expensas de que, a causa de la guerra en Ucrania, se viva un ciberataque en el Viejo Continente contra infraestructuras críticas. En definitiva, se trata de reforzar la resiliencia de los operadores críticos y con más riesgo y que podrían ser uno de los principales objetivos en caso de que el conflicto escalara, además de permitir el desarrollo de un ecosistema de ciberseguridad. "Fomentar el desarrollo de tales proveedores debería ser una prioridad de la política industrial de la UE en el campo de la ciberseguridad", destacó la declaración.

Además, el documento pide a autoridades europeas como la Comisión, los reguladores nacionales de telecomunicaciones, la **Agencia de Ciberseguridad de la Unión Europea** (Enisa) y el **Grupo de Cooperación de Seguridad de Redes e Información** (NIS) que se involucren más y presenten recomendaciones concretas de pasos que se deberían de llevar a cabo para fortalecer la infraestructura digital de Europa frente a ciberataques, así como en las redes. También, lamenta la dependencia de la infraestructura de Europa, desde las conexiones globales de Internet hasta los cables submarinos, propiedad principalmente de empresas estadounidenses y chinas.



Nuevas regulaciones

Además, a finales de marzo, la Comisión propuso nuevas regulaciones de ciberseguridad para los 27 países para mejorar la protección de la administración pública de la UE. Así, se pide que el Reglamento de Ciberseguridad extienda las capacidades del **Equipo de Respuesta a Emergencias Infor-**



máticas (CSIRT-EU), cambiando su denominación a "Centro de Ciberseguridad", así como crear un **Grupo de Coordinación de Seguridad de la Información interinstitucional**, responsable de coordinar a dicho equipo y ayudar a implantar el Reglamento. Sobre todo, en aspectos como la obligación de implementar marcos de ciberseguridad para la gobernanza, la gestión y el control de riesgos, siendo sometidos a evaluaciones periódicas y notificando incidentes "sin demoras indebidas", por parte de todos los organismos públicos de la UE. También, se contempla aplicar un enfoque común para la categorización de la información basada en el nivel de confidencialidad.

Estrategia de normalización

La **Comisión** también ha dado a conocer su nueva estrategia de normalización acompañada de una propuesta de modificación

del Reglamento sobre este aspecto, un informe de cómo aplicarlo y un programa de trabajo para 2022 para poderla desarrollar. La iniciativa tiene como objetivo "fortalecer la competitividad global de la UE, permitir una economía verde, digital y resiliente, y consagrar los valores democráticos en las aplicaciones tecnológicas". En este sentido, recuerda que "las normas

son la base silenciosa del mercado único de la UE y la competitividad global. Ayudan a los fabricantes a garantizar la interoperabilidad de productos y servicios, reducir costes, mejorar la seguridad y fomentar la innovación".

Por eso, sus impulsores creen que este tipo de estándares son fundamentales para salvaguardar la seguridad y calidad de todo tipo de dispositivos conectados y redes, como en las *wifi*, que usamos en nuestro día a día.

En concreto, la estrategia propone cinco acciones: anticipar, priorizar y atender las necesidades de estandarización en áreas estratégicas, mejorar la gobernanza y la integridad del sistema de normalización europeo, así como el liderazgo europeo en estándares globales, apoyar más la innovación y formar a expertos en normalización a través de la organización de 'Días Universitarios' en la UE y contenidos específicos para investigadores.

Declaración de derechos digitales

Así mismo, a finales de enero, la Comisión también publicó su propuesta para una 'Declaración Europea sobre Derechos Digitales y Principios para la Década Digital'. En ella, transpone los derechos fundamentales de los ciudadanos de la UE a la esfera digital, basándose en su mayoría en declaraciones anteriores y en la Carta de los Derechos Fundamentales en Europa. Se espera que, tras ser debatida en el Parlamento y el Consejo, sea aprobada a mediados de año.





DETENGA LOS ATAQUES AUTOMÁTICOS Y LOS BOTS MALICIOSOS.

Las aplicaciones son el negocio. La automatización permite que las organizaciones sean las primeras en salir al mercado, en obtener beneficios y en innovar con aplicaciones que puedan cambiar el mundo.

f5.com/es_es/solutions/application-security/bot-management

```
.then((results) => {
  let patchedItem;
  results.forEach((currentItem, index) => {
    const schemaClass = this.configItems[index].schemaClass;
    if (!schemaClass) {
      // Simple item that is just key:value - not a larger object
      Object.keys(currentItem).forEach((key) => {
        currentConfig[key] = currentItem[key];
      });
    } else if (Array.isArray(currentItem)) {
      currentConfig[schemaClass] = {};
      currentItem.forEach((item) => {
        patchedItem = removeUnusedKeys.call(this, item);
        patchedItem = mapProperties.call(this, patchedItem, index);
        // if schemaClass is oddball, don't try to handle the
        // item as a schemaClass
        if (this.configItems[index].name !== 'f5') {
          currentConfig[schemaClass][item.name] = patchedItem;
        } else {
          currentConfig[schemaClass][index] = patchedItem;
        }
      });
    } else {
      currentConfig[schemaClass] = {};
      patchedItem = removeUnusedKeys.call(
        this,
        currentItem,
        this.configItems[index].name);
      patchedItem = mapProperties.call(this, patchedItem, index);
      currentConfig[schemaClass][currentItem.name] = patchedItem;
      getReferencePaths.call(this, currentItem, index, referencePromises, re
    }
  });
});
// get any objects that were referenced from the ones we already got
return Promise.all(referencePromises);
}).then((referencesResults) => {
```


EN BREVE

La COMISIÓN propone una 'Ley de Datos' buscando defender a empresas y personas frente a su mal uso por parte de las organizaciones

A finales de febrero, la **Comisión Europea**, dentro de su Estrategia Europea de Datos, publicó su propuesta de Reglamento de normas armonizadas sobre el acceso y uso justos de los datos, denominada Ley de Datos o 'Data Act'. Se trata de un texto con el que se quiere posicionar al Viejo Continente como la referencia en la llamada 'economía de datos'. Por ello, su principal objetivo es marcar unas reglas sobre el intercambio de datos, el acceso y su reutilización, así como los términos contractuales que deben darse, entre otros aspectos. Esta norma se aplicará en todos los sectores y afectará, especialmente, a las empresas y organizaciones basadas en datos que dependen de los que generan los productos conectados. Por eso, en el borrador la Comisión también propone abordar la concentración del mercado y limitar la dependencia excesiva de la UE de compañías extranjeras en esta área.

Entre sus principales novedades, destaca que busca establecer medidas para reforzar el control sobre sus datos por parte de personas y de empresas —permitiendo el acceso a los que cada uno genere—, además se tendrá en cuenta el abuso de desequilibrio a la hora de negociar los contratos de intercambio de datos —sobre todo, por parte de las pymes respecto a las grandes compañías—. También,

se permitirá al sector público, en casos excepcionales como catástrofes naturales o emergencias, poder acceder a datos de compañías del sector privado.

Restricciones

Un dato de especial interés, en lo que atañe a los proveedores de servicios en la nube, es que el texto propone varias restricciones respecto a un posible intercambio internacional de datos (sin importar si son de carácter personal a los efectos de la normativa de protección de datos).

Tanto la 'Data Act' como la 'Data Governance Act', que también está en proceso de tramitación, complementarán el actual Reglamento General de Protección de Datos (RGPD). Según ha explicado la propia Comisión, si la primera determina quiénes pueden generar valor a partir de los datos y en qué condiciones, la segunda crea procesos y estructuras para facilitar el intercambio de datos por parte de empresas, particulares y el sector público. En cuanto al régimen sancionador, se permite que cada estado miembro ponga en marcha el suyo, permitiendo designar o no una autoridad de supervisión, ya sea a partir de una existente o creando una nueva.

De cualquier forma, aún queda para su aprobación definitiva, ya que ahora se establecerá un periodo de debate, pero es un paso importante para impulsar la agenda de soberanía digital en la UE. Y todas las empresas, aprobadas ambas normativas, deberán acatarlas.



La OFICINA DE CÓDIGO ABIERTO de la COMISIÓN pone en marcha su programa de bug bounty

La **Oficina del Programa de Código Abierto de la Comisión Europea** (EC OSPO) presentó, a principios de año, un nuevo programa de recompensas por errores



utilizando la plataforma de la empresa **Intigriti**. A través de ella, se invita a los investigadores a encontrar vulnerabilidades de seguridad, fugas de datos personales, escalada de privilegios horizontales y/o verticales y SQLi. La recompensa más alta será de 5.000 euros para vulnerabilidades excepcionales y una bonificación del 20 % si también se proporciona la corrección tanto en LibreOffice,

LEOS, Mastodon, Odoos como CryptPad, soluciones de código abierto utilizadas por los

servicios públicos en toda la UE. Además, EC OSPO decidió incluir posibles

fallos en LEOS, un editor legal utilizado por la Comisión, el Parlamento, el Consejo y varios estados miembro. En total, el programa tiene un presupuesto de 200.000 euros.

Como se sabe, la **Oficina del Programa de Código Abierto de la Comisión Europea** se creó en 2020 como la primera acción concreta de la última Estrategia de Software de Código Abierto para 2020-2023.

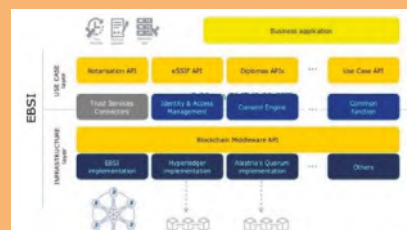
Primer llamamiento para contar con propuestas para una identidad digital basada en blockchain

El Programa Europa Digital reforzará las capacidades digitales críticas de la UE centrándose en áreas clave como la inteligencia artificial (IA), la ciberseguridad, la informática avanzada, la infraestructura de datos, la gobernanza y el procesamiento, así como el despliegue

de estas tecnologías y su mejor uso para sectores críticos.

Su objetivo es mejorar las habilidades para proporcionar una fuerza laboral para estas tecnologías digitales avanzadas. También, apoya al sector privado, las pymes y la administración pública en su transformación digital con una red reforzada de **European Digital Innovation Hubs (EDIH)**.

Ahora, ha celebrado su primera convocatoria que cubrirá el "Despliegue de servicios,



Estandarización de Blockchain (EBSI), Soporte para la implementación del Marco Europeo de Identidad Digital y la implementación del Sistema Once Only bajo la Regulación y Seguridad del Portal Digital Único". Precisamente, en este último aspecto, la convocatoria tiene como objetivo facilitar la implementación del Marco Europeo de Identidad Digital.

¿Qué es más perjudicial para tu estrategia de ciberseguridad, la pérdida de datos o de confianza?

Un ciberataque puede destruir intangibles tan valiosos para tu organización como la confianza. Para salvaguardarla, las estrategias de ciberseguridad deben enfocarse en la prevención de forma proactiva.

Descubre cómo desde EY podemos ayudarte.



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



Building a better
working world

El Senado da 'luz verde' al proyecto de Ley de Divulgación de Ciberincidentes y Biden da instrucciones para regular criptoactivos

ESTADOS UNIDOS redobla sus esfuerzos por mejorar sus capacidades nacionales en ciberseguridad incrementando su presupuesto de TI en un 11%

La invasión de Ucrania viene generando que las diferentes agencias de ciberseguridad del gobierno estadounidense hayan activado la alerta máxima ante la posibilidad de sufrir ciberataques por su apoyo al gobierno de Zelenski.



Joe Biden

Precisamente, la posibilidad de un gran ciberataque por parte de Rusia a los países de la OTAN que están apoyando a Ucrania está motivando que la Alianza considere la posibilidad de desarrollar una nueva doctrina para el uso apropiado de la fuerza en ámbitos cibernéticos. Fuentes del Senado y del Congreso de EE.UU. han apostado por ello recordando que el informe de la **Comisión Solarium**, de 2019, describió la doctrina estadounidense actual sobre el uso de la fuerza como "ambigua, tanto política como legalmente". "Nuestros adversarios claramente están explotando el umbral actual para realizar una variedad de actividades maliciosas, pero no alcanzan un nivel que justifique una respuesta de represalia importante", escribió la Comisión. "El gobierno estadounidense debe declarar públicamente que defenderá y combinará su declaración con una acción decisiva y consistente en todos los elementos del poder nacional", recomendaba el documento.

Además, para mejorar la coordinación con sus socios internacionales, **Anne Neuberger**, Asesora Adjunta de **Seguridad Nacional**, realizó en febrero una gira por Europa para "elevar la ciberseguridad y situarla como una prioridad de primer nivel de la OTAN, junto a socios internacionales". Su objetivo fue debatir sobre cómo "disuadir, interrumpir y responder a un posible incremento de la agresión rusa contra Ucrania, los estados vecinos y nuestros países", destacaron fuentes cercanas a Neuberger.

Presupuesto cibernético 2023

Precisamente, a raíz de las debilidades detectadas durante la guerra de Ucrania y de la política de hace ya un lustro de fortalecer la ciberseguridad de sus agencias federales, el presidente de EE.UU., **Joe Biden**, ha pedido en el presupuesto de 2023 un incremento significativo en la inver-

sión en ciberprotección. Entre otras partidas de interés ha pedido 11,6 millones de euros, para la investigación de comunicaciones avanzadas, y 168 millones para que el **Instituto Nacional de Estándares y Tecnología** (NIST) se concentre en la elaboración de nuevos estándares para la adopción de tecnologías críticas y emergentes como inteligencia artificial, ciencias cuánticas y biotecnologías.

Además, destacan los 9.793 millones de euros para ciberprotección para las agencias civiles federales, los 10.063 millones para operaciones cibernéticas no clasificadas del Departamento de Defensa, los 2.336 millones para el Departamento de Seguridad Nacional, así como 2.246 millones para la **Agencia de Seguridad de Infraestructura y Cibersegu-**



ridad (CISA), que depende del Departamento de **Seguridad Nacional** (DHS).

"La seguridad cibernética sigue siendo una prioridad principal para esta Administración, ya que nuestros adversarios continúan buscando medios nuevos y creativos para comprometer los sistemas federales", explica la propuesta presupuestaria. "La Administración ha contratado a los mejores expertos de todo el país para identificar las principales prácticas de protección y establecer un nuevo curso audaz para revisar el enfoque del Gobierno para asegurar la TI federal".

Cibercrimen y criptomonedas

Por otro lado, también ha sido notable la propuesta de la **Casa Blanca** para hacer frente a las amenazas que pueden suponer los activos digitales, incluidas las criptomonedas, que "han experimentado un crecimiento explosivo en los últimos años, superando una capitalización de mercado de 2,7 billones de euros cuando, en

2017, rondaban los 12.700 millones de euros. De hecho, se calcula que el 16% de la población, unos 40 millones de personas, ha invertido en ellas.

Ante esta situación, la Casa Blanca anunció una nueva Orden Ejecutiva "para abordar los riesgos y aprovechar los beneficios potenciales de los activos digitales y su tecnología subyacente". La orden establece una política nacional con seis prioridades clave: protección de consumidores e inversores; estabilidad financiera; financiación ilícita; liderazgo de EE.UU. en el sistema financiero global y competitividad económica; inclusión financiera; e innovación responsable.

Además, el **FBI** anunció a finales de febrero, a través de la Fiscal General Adjunta, **Lisa Monaco**, varias iniciativas para luchar contra la ciberdelincuencia, entre las que destacó la creación de la **Unidad de Explotación de Activos Virtuales**, especializada en la cadena de bloques, incautación de activos virtuales y formación al resto de la Agencia, así como la puesta en marcha del **Equipo Nacional de Aplicación de Criptomonedas** (NCET) del Departamento de Justicia que ya ha incautado de más de 3.500 millones de euros en criptomonedas.

Ley de divulgación de incidentes

Por otra parte, el Senado aprobó en marzo el proyecto de 'Ley de divulgación de ciberincidentes', junto a varias propuestas más para "fortalecer la seguridad cibernética de la infraestructura crítica y las redes gubernamentales", destacaron sus impulsores. Con ello, se da un paso más hacia la regulación que obliga a los propietarios y operadores de infraestructuras críticas, así como las agencias federales civiles, a informar a la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) sobre cualquier ataque cibernético significativo dentro de las 72 horas. También, tendrán que hacerlo casi todas las entidades cuando realicen cualquier pago de *ransomware*, dentro de las 24 horas siguientes a realizarlo.

Además, el Comité de Seguridad Nacional de la Cámara de Representantes aprobó la 'Ley del Consorcio Nacional de Preparación' para la Ciberseguridad de 2021, que ordena al Departamento de Seguridad Nacional (DHS) que desarrollen y analicen planes de capacitación en ciberprotección para los funcionarios públicos.



VMware Carbon Black Cloud Workload

Protección avanzada de cargas de trabajo para entornos virtualizados, privados y de nube híbrida.



Características clave

Solución de evaluación y gestión de vulnerabilidades sin rastreos

- Gestión del ciclo de vida y del inventario de cargas de trabajo.
- Integrado en Carbon Black Cloud y el complemento de vCenter.
- Monitorización conductual, que aprovecha los datos recopilados en la nube.
- Consulta miles de elementos de carga de trabajo a petición.
- Antivirus de última generación (NGAV).
- Realiza evaluaciones continuas para mitigar los riesgos de TI de forma permanente.

EN BREVE

La AGENCIA DE PROTECCIÓN AMBIENTAL apuesta por mayores capacidades de detección temprana para reducir el riesgo de incidentes en el sector de gestión del agua

La **Agencia de Protección Ambiental** (EPA) de EE.UU. ha presentado una propuesta para mejorar la protección de los sistemas de suministro de agua del país. La iniciativa, titulada 'Plan de Acción del Sector de Agua y Aguas Residuales' busca que el sector realice, en un centenar de días, un esfuerzo para mejorar sus capacidades en este ámbito,



sobre todo, en lo que atañe a la detección temprana y el intercambio rápido de datos en todo el gobierno.

Además, el plan aboga por el establecimiento de un grupo de trabajo de seguridad cibernética

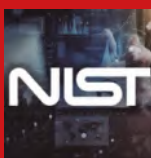
compuesto por líderes del sector del agua. También, se exige la implementación de proyectos piloto para demostrar y acelerar la adopción de la monitorización de incidentes.

El programa, al que se ha dado la máxima prioridad, ha sido apoyado también por el **Consejo de Seguridad Nacional** (NSC), la **Agencia de Seguridad de Infraestructura y Ciberseguridad** (CISA) y el **Consejo Coordinador del Sector del Agua y el Consejo Coordinador del Gobierno del Agua** (WSCC/GCC).

El NIST propone un modelo para evaluar estrategias de inversión en seguridad de redes y revisa su Marco de Ciberseguridad

El **Instituto Nacional de Estándares y Tecnología** (NIST) presentó, junto a investigadores universitarios, un estudio para desarrollar un nuevo modelo computacional que permita evaluar con detalle el coste de la protección de redes, aplicando tecnología de aprendizaje automático. La idea, plasmada en un artículo titulado 'Inversiones óptimas en ciberseguridad en redes grandes usando el modelo SIS: diseño de algoritmos', firmado por **Van Sy Mai**, **Richard La** y **Abdella Battou**, se inspira en un algoritmo diseñado para el seguimiento de pandemias. Así, su modelo "Susceptible-Infectado-Susceptible" (SIS) tiene en cuenta las inversiones, las pérdidas económicas y los requisitos de recuperación causados por infecciones de *malware*. En total, propone emplear cuatro algoritmos capaces de evaluar las probabilidades de que una red sea infectada, las tasas probables de propagación, cuánto tiempo y cuánto costaría reparar el daño y el gasto asociado con la recuperación total.

Además, el NIST ha anunciado una revisión de su reconocido Marco de Seguridad Cibernética (CSF) para que esté más alineado con otras iniciativas del organismo como sus marcos de privacidad, de desarrollo de software seguro, de gestión de riesgos, de fuerza laboral para la ciberseguridad (NICE) y sus distintas guías sobre ciberprotección IoT.



La OFICINA DE RESPONSABILIDAD GUBERNAMENTAL lamenta que las agencias federales no midan el riesgo de las infraestructuras críticas

Algunas de las nueve agencias federales de EE.UU. que, entre otras responsabilidades, son las que se ocupan de medir y evaluar los estándares de ciberseguridad, en 16 sectores críticos, han descuidado sus funciones. Así lo destaca en un nuevo informe la **Oficina de Responsabilidad Gubernamental** (GAO). En concreto, la crítica es hacia las que velan por la ciberprotección de 13 sectores, a los que se han realizado auditorías incompletas, según la GAO, sin confirmar que cumplen los marcados por el NIST. Y nueve de ellos no contaban con los planes de ciberseguridad que deberían. Algo especialmente preocupante, ya que entre ellos están desde el de servicios de emergencia química, hasta el de atención médica y salud pública, el de servicios financieros, el de instalaciones comerciales e, incluso, el de reactores nucleares, entre otros.



CISA ofrece un listado de un centenar de herramientas y servicios gratuitos de ciberseguridad para empresas

La **Agencia de Seguridad de Infraestructura y Ciberseguridad** de EE.UU. (CISA) publicó en febrero, a través de su web, una lista con un centenar de herramientas y servicios gratuitos de ciberseguridad que pueden ayudar a las organizaciones a reducir el riesgo, mejorar la resiliencia y que ofrecen sin coste compañías como **Microsoft**, **Google**, **Cloudflare**, **Cisco**, **Center for Internet Security**, **CrowdStrike**, **Tenable**, **AT&T Cybersecurity**, **IBM**, **Mandiant**, **Splunk**, **VMware**, **SANS**, **Secureworks** y **Palo Alto**, entre otras.

Así, en su propuesta hay desde herramientas de código abierto, no relacionadas con proveedores, hasta recursos proporcionados por el sector privado y organizaciones gubernamentales. Así mismo, recuerda que cualquier empresa puede inscribirse en su servicio gratuito de 'Escaneo de vulnerabilidades', que proporciona informes semanales.



La SEC exigirá más transparencia y planes de seguridad a los fondos de inversión y sus asesores

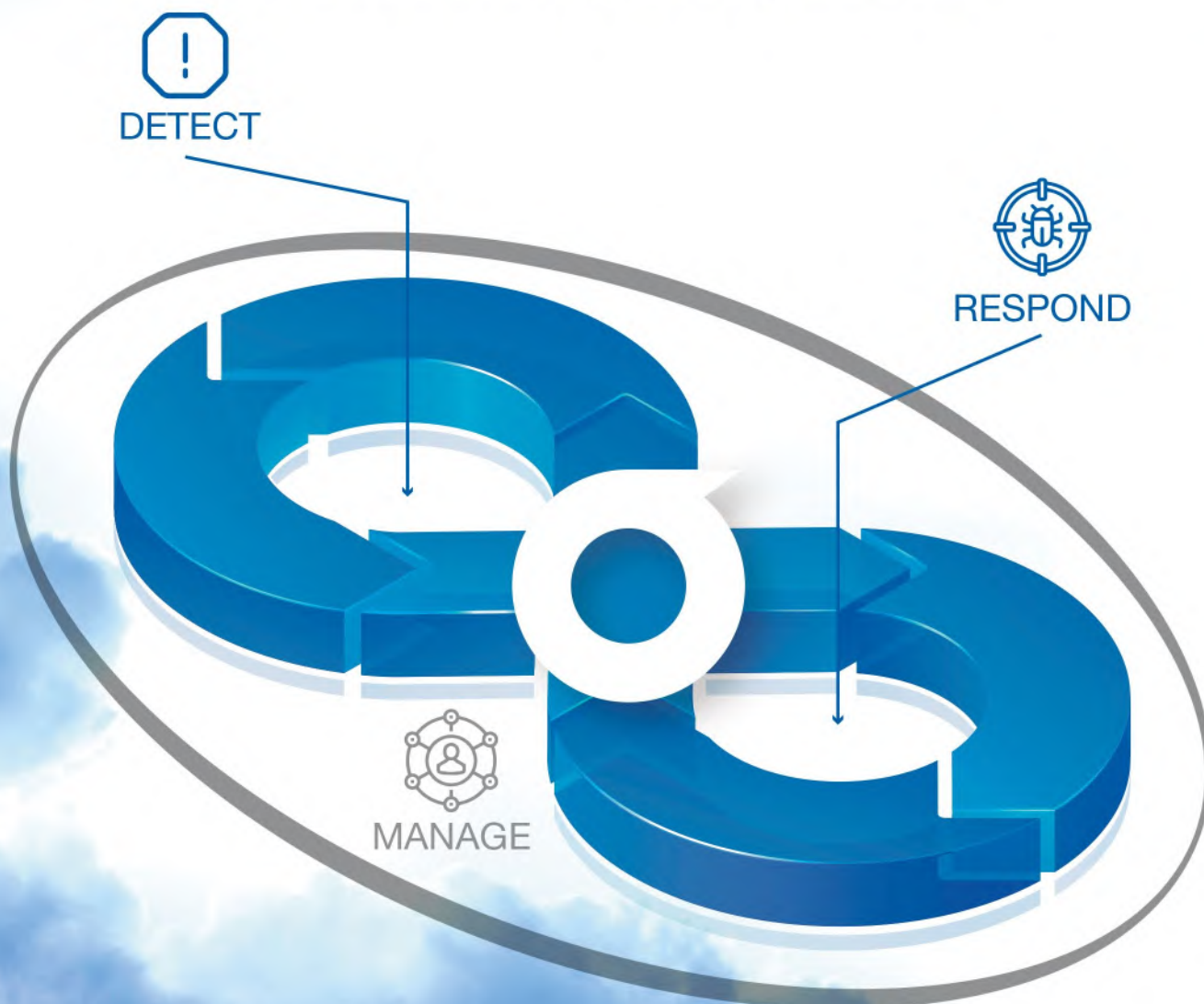
La **Comisión de Bolsa y Valores** (SEC) ha anunciado que está estudiando un plan para exigir que las compañías públicas sean más transparentes en lo que atañe a sus planes de ciberseguridad y en la notificación de incidentes, sobre todo de cara a sus inversores. De aprobarse, las compañías tendrían que dar a conocer el rol de la gerencia y la junta y la supervisión de los riesgos de seguridad cibernética, si cuentan con políticas y procedimientos de ciberseguridad y cómo de probable puede impactar en las finanzas de la compañía un ciberataque.

Se trata del tercer proyecto de ciberseguridad que la SEC anuncia en lo que va de año, ya que, a principios, propuso incrementar el Cumplimiento e integridad de los sistemas de regulación (SCI) a ciertas plataformas de negociación de valores gubernamentales y en febrero se planteó que asesores de inversiones registrados y los fondos de inversión también mejoraran su ciberseguridad.





**a la vanguardia en
Detección y Respuesta**



Aiuken Cybersecurity de
nuevo presente en la lista de
Top Vendor MDRS 2021 por

Gartner®

www.aiuken.com

Se dará especial protagonismo a nuevas entidades, como el Centro de Coordinación Cibernético del Gobierno o la 'ciber' Fuerza Nacional

REINO UNIDO aprueba su Estrategia de Ciberseguridad 2022-2030 para salvaguardar las "funciones críticas" del Gobierno

A principios de año, el **Reino Unido** aprobó y publicó su primera estrategia de ciberseguridad, que está focalizada en mejorar la protección de los servicios públicos de la nación. Entre otros aspectos de interés, el documento contempla la creación del **Centro de Coordinación Cibernética del Gobierno (GCCC)** para poder coordinar mejor las respuestas a los ataques al sector público, así como poner en marcha un servicio de informes de vulnerabilidades entre gobiernos, para permitir que los investigadores de seguridad y el público informen fácilmente de los problemas que identifican con el sector público. También, se apuesta por implantar una política de ciberseguridad común tanto en servicios digitales públicos, como en los diferentes departamentos de la Administración.

La estrategia se sustenta en dos pilares fundamentales: el primero,



centrado en construir una base sólida de resiliencia organizacional; y el segundo, tiene como objetivo "permitir que el gobierno se 'defienda como uno', aprovechando el valor de compartir datos, experiencia y capacidades", destacó

el Director de Seguridad del Go-

bierno, **Vincent Devine**. Además, contempla invertir 45,9 millones de euros para mejorar la ciberseguridad de las autoridades locales y proteger los servicios y datos esenciales —desde subvenciones a la vivienda, hasta la gestión electoral o las becas escolares—.

Eso sí, también ha sido puesta en tela de juicio por considerar que este presupuesto se quedará corto. De cualquier forma, en líneas generales, la nueva estrategia ha

sido bien recibida tanto por la industria, como por el sector británico de ciberseguridad, por su apuesta por mejores prácticas, controles y gestión de la seguridad en estas instituciones, además de conllevar un presupuesto concreto y en consonancia con otras iniciativas recientes como fue en 2021 la creación de una **Fuerza Cibernética Nacional** para incrementar sus capacidades ofensivas en el ciberespacio.

Impulso a la creación de la primera Oficina de Identidades Digitales

Fruto de su ya demostrado interés por la identidad digital, el Reino Unido anunció que está estudiando crear una **Oficina de Identidades Digitales (ODIA)**, tras la consulta pública realizada por el **Departamento de Digital, Cultura, Medios y Deporte (DCMS)**. Su objetivo es lograr que las identidades digitales sean tan seguras y confiables como las basadas en documentos oficiales en papel. Para ello generará un ecosistema de identidades y atributos digitales, siguiendo las propuestas del año pasado para un marco de confianza y un órgano de gobierno. Una iniciativa que también está acometiendo la UE.

De momento, la ODIA se integrará en el DCMS para supervisar los estándares de seguridad y privacidad



pertinentes. Así entre sus objetivos destaca el poner en marcha un proceso de acreditación y certificación sólido y seguro junto

con una marca de confianza, crear una 'puerta de enlace legal' para que las empresas de confianza realicen controles de verificación de los datos en manos de los organismos públicos, para validar la identidad de una persona y confirmar la validez legal de las formas digitales de identificación.

RUSIA y CHINA suman más fuerzas en operaciones militares ofensivas que EE.UU., según el Military Balance

Desde hace décadas, el **Military Balance**, publicado por el **Instituto Internacional de Estudios Estratégicos (IISS)**, de Londres, se ha convertido en una especie de 'Biblia' de la capacidad bélica de cada país, con una información detallada de las fuerzas y medios de cada nación. En su edición de 2022, la obra ha destacado que la suma de unidades militares cibernéticas de Rusia y China es significativamente mayor que las de EE.UU., contando como tal, fuerzas militares en activo con responsabilidad directa en el ciberespacio. Según la obra, el 33% de las ciberfuerzas militares rusas están especializadas en acciones



ofensivas, en comparación con el 18,2% de las chinas y el 2,8% de las estadounidenses, de acuerdo a los roles asignados a cada una.

Entre sus capacidades están desde denegar, degradar, perturbar o destruir activos hasta la investigación de vulnerabilidades, la creación de *malware* o tomar el control de un sistema a través de *exploits*.

Además, destaca las acciones en este aspecto de Rusia que, en julio de 2021, actualizó su Estrategia de Seguridad Nacional, dedicando una sección a la seguridad de la información y enfatizando el desarrollo adicional de las fuerzas y capacidades cibernéticas militares.

PASCAL STEICHEN, nuevo Presidente del CENTRO de COMPETENCIA EN CIBERSEGURIDAD de la UE

El Consejo de Administración del **Centro Europeo de Competencia en Ciberseguridad (ECCC)**, constituido en junio de 2021, nombró, por un mandato de cuatro años, al luxemburgués **Pascal Steichen**, Presidente del Consejo de administración y de los centros nacionales de coordinación del **Centro y Red Europeos de Competencia en Ciberseguridad**. En total, el Consejo de Administración está compuesto por representantes de los 27 Estados miembro, la Comisión Europea (dos) y Enisa (uno). La reunión, celebrada a finales de febrero, también aprobó la lista de los Centros Nacionales de Coordinación

designados oficialmente por los 27 países —en el caso de España, es el **Incibe**—.



El encuentro también permitió avanzar en la puesta en marcha del Centro, que gestionará parte de la financiación que se dedica a la ciberseguridad desde el programa Europa Digital, con 1.980 millones de euros y Horizonte Europa, orientado a la investigación y la innovación, con 95.500 millones.

También se adelantó que la convocatoria cibernética de Europa Digital, tendrá una primera inversión de 55 millones dedicada al despliegue de los Centros Nacionales de Coordinación (CNC).

Fortinet Security Fabric

Broad

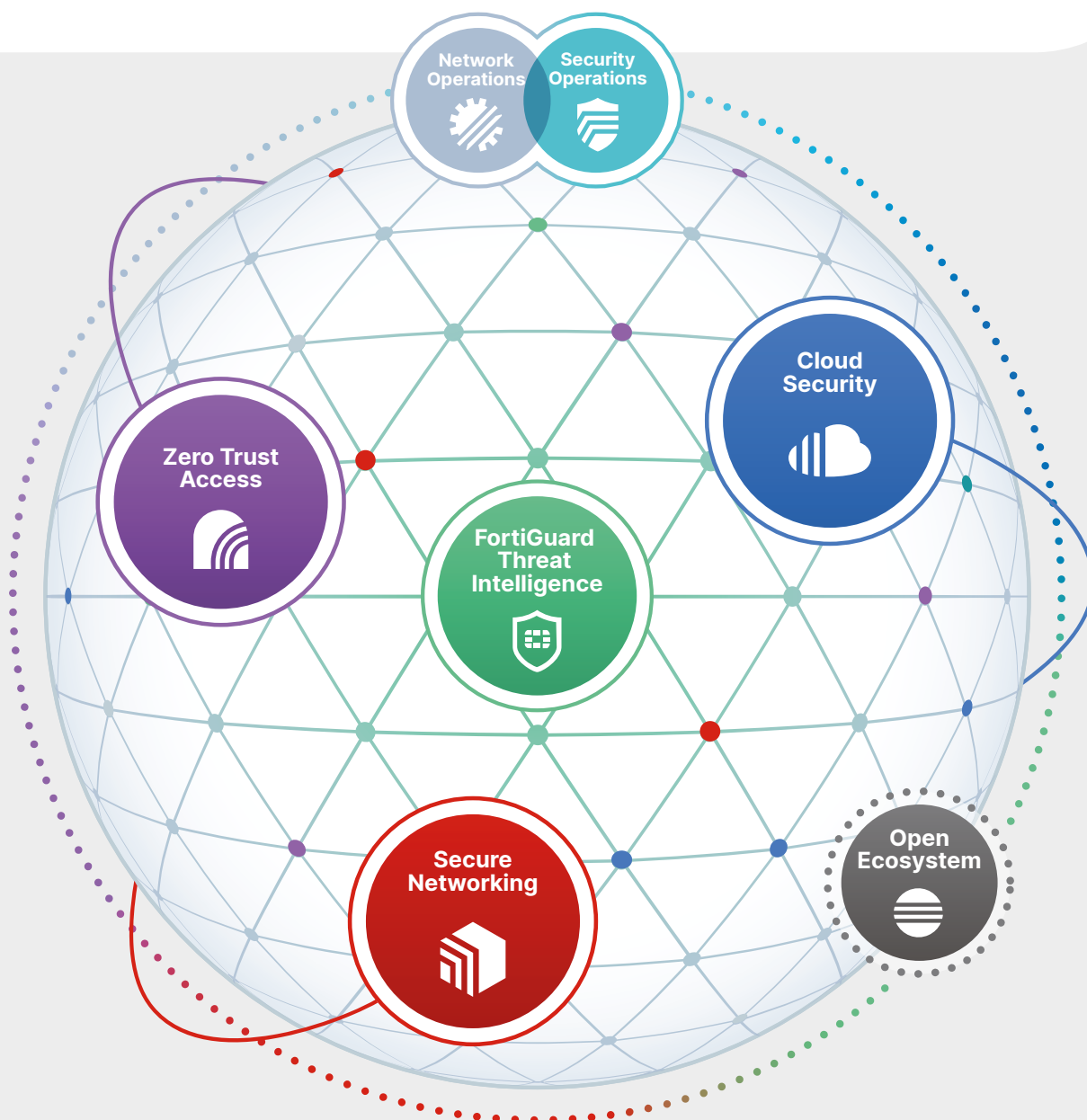
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with AI-driven security for fast and efficient operations



El presidente SÁNCHEZ anunció en el acto de agradecimiento al FNC en La Moncloa la creación del Plan Nacional de Ciberseguridad

El pasado 9 de marzo del presente, tuvo lugar en La Moncloa, un acto de reconocimiento y agradecimiento a los miembros del **Foro Nacional de Ciberseguridad (FNC)** por la realización de los primeros trabajos llevados a cabo en el seno de esta organización orientada a la colaboración público-privada, cuya creación estaba prevista en la ENCS 2019 y que se constituyó en julio del año 2020.

En el acto participaron el Presidente del Gobierno, **Pedro Sánchez**; la Secretaria de Estado Directora del CNI y del CCN –y Presidenta del Consejo nacional de Ciberseguridad–, **Paz Esteban**; la Secretaria de Estado de Digitalización e Inteligencia Artificial, **Carme Artigas**; el Director del Departamento de Seguridad Nacional (DSN), **Miguel Ángel Ballesteros**; el embajador en Misión Especial para la Ciberseguridad y Amenazas Híbridas, **Nicolás Pascual de la Parte**, así como otros cargos

públicos vinculados con las TIC y la ciberseguridad: la SGAD, el CCN, el MCCE y la empresa pública Incibe.

La parte privada estuvo integrada por representantes de asociaciones, empresas especializadas y expertos que forman parte del FNC, como es el caso de la revista **SIC**, vocal del Foro a través de su compañía editora, **Ediciones CODA**.

En el encuentro intervinieron el presidente del Gobierno, la secretaria de estado directora del CNI y el CCN, y Presidenta del Consejo

Nacional de Ciberseguridad, la Secretaria de Estado de Digitalización e IA, el Director del DSN, y la Presidenta de la Fundación Borredá, esta última en representación del sector privado.

En su discurso, el presidente del Gobierno ya avanzó la intención del Ejecutivo de aprobar el Plan Nacional de Ciberseguridad, que incluye, entre otras actuaciones, “la creación de un sistema

integrado de indicadores de ciberseguridad a nivel estatal; la constitución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus organismos públicos y, finalmente, la implementación de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes y de amenazas”.

El presidente concluyó agradeciendo la labor realizada desde el sector público, así como por los 117 expertos, tanto de este sector como del privado, que han tomado parte

España: la Ciberseguridad ya es también Política de Estado



El Foro Nacional de Ciberseguridad, en La Moncloa



Alocución del Presidente a las autoridades y miembros del FNC asistentes

CIENCIA E INNOVACIÓN destina 54 millones al 'Plan Complementario de Comunicación Cuántica' para reforzar la protección cibernética

La Ministra de **Ciencia e Innovación**, **Diana Morant**, presentó en marzo el Plan Complementario en Comunicación Cuántica, que movilizará un total de 73 millones de euros. A través de él, el Ministerio trabajará con el País Vasco, Cataluña, Galicia, Madrid, Castilla y León y el **Consejo Superior de Investigaciones Científicas (CSIC)** para crear una infraestructura de comunicación de alta seguridad, apoyar la industria cuántica europea e impulsar un sector industrial con nuevas empresas en los ámbitos digital y de ciberseguridad.

La ministra ha remarcado que este pro-

yecto se alinea con el reto de salvaguardar la seguridad de las comunicaciones ante amenazas múltiples, como la invasión rusa a Ucrania.

Este Plan Complementario se dirige a un sector estratégico dentro de las tecnologías

cuánticas de segunda generación, que se basa en la capacidad de manipular sistemas cuánticos individualmente, alineándose de esta manera con algunas de las iniciativas de I+D+i de la UE, como el Quantum Flagship y la creación de una red cuántica paneuropea, EuroQCI.

Precisamente, el **Centro de Seguridad Cibernética de la OTAN (NCSC)** anunció en marzo que ha probado con éxito los flujos de comunicación seguros en un mundo postcuántico, utilizando una red privada virtual (VPN) proporcionada por la empresa británica **Post-Quantum**.

Presentación del Plan Complementario de Comunicación Cuántica

SE ACABARON LOS ERRORES



#CURAPENTESTING

Ciberseguridad, Ciberinteligencia, BlackArrow, Innovación

www.tarlogic.com

El FNC hace públicos los primeros entregables de sus Grupos de Trabajo iniciales

El Foro Nacional de Ciberseguridad (FNC), el espacio de colaboración público-privada impulsado por el Consejo de Seguridad Nacional, publicó a finales de febrero los primeros entregables elaborados por sus diferentes grupos de trabajo. Estos informes se centran en el estudio de la cultura de la ciberseguridad en España, el apoyo a la Industria e I+D+i y la definición de un Esquema Nacional de Certificación para responsables de esta materia.

Para la elaboración de estos trabajos, los tres grupos, formados por **117 expertos** en la materia pertenecientes a **74 organizaciones públicas y privadas**, han conseguido materializar esta colaboración basándose en la búsqueda de acuerdos y el posicionamiento común en beneficio de los objetivos del FNC. Así, las sinergias entre representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organizaciones sin ánimo de lucro y el esfuerzo de profesionales de reconocido prestigio, han permitido la consecución de los primeros retos encomendados por el Consejo Nacional de Ciberseguridad.



Esquema Nacional de Certificación de Responsables de ciberseguridad

Este grupo de trabajo, coliderado por el **Centro Criptológico Nacional (CCN)** y la **Comisión Sectorial de TIC de la Crue Universidades Españolas (Crue-TIC)** se ha encargado de establecer las condiciones y requisitos para la certificación de los profesionales de la ciberseguridad en el Esquema Nacional de Certificación de Responsables de Ciberseguridad. Su promoción y desarrollo es responsabilidad del CCN, la **Secretaría de Estado de Digitalización e IA**, así como la **Secretaría de Estado**

de Seguridad. Este sistema permitirá certificar a la figura del responsable de la seguridad del Esquema Nacional de Seguridad, al responsable de seguridad y enlace de las infraestructuras críticas, al responsable de la seguridad de la información y a los responsables de seguridad de servicios o productos TIC de empresas proveedoras de infraestructuras críticas o de servicios esenciales. Así, se generará un Registro de Entidades de Certificación ya acreditadas y un Registro de Personas Certificadas.

Informe sobre la cultura de la ciberseguridad en España

El proceso de digitalización y transformación digital de nuestra sociedad, acelerado por la pandemia, exige mejorar el conocimiento de los riesgos asociados. Por ello, el primer documento elaborado por el grupo de trabajo de cultura de ciberseguridad, coliderado por el **Departamento de Seguridad Nacional**, la asociación **ISMS Forum** y la **Fundación Borredá**, es el Informe sobre la Cultura de la ciberseguridad en España.

Entre las conclusiones de este trabajo destacan el desconocimiento generalizado de los ciberriesgos entre autónomos y pymes o la carencia de competencias en ciberseguridad en los trabajadores. Por este motivo, se proponen actuaciones dirigidas a incrementar la eficacia y la eficiencia de la cultura de ciberseguridad y promocionar una conciencia social compartida, así como la creación de un Observatorio para la elaboración y seguimiento del Barómetro Integral de Ciberseguridad (OBIC).

Informe sobre la industria y la investigación españolas en ciberseguridad

El ecosistema español de ciberseguridad se ha desarrollado durante los últimos 20 años a partir de unas sólidas bases legislativas y con el liderazgo de organismos gubernamentales, centros tecnológicos, universidades y del sector privado. Estos antecedentes han posicionado a España como uno de los países de referencia en nivel de madurez en algunos aspectos de la ciberseguridad a nivel global. Sin embargo, el Informe elaborado por este grupo de trabajo, coliderado por el **Instituto Nacional de Ciberseguridad (INCIBE)** y la **Cámara de Comercio de España**, establece que los resultados de la red de investigación nacional no están siendo transferidos a la industria.

Por este motivo, el informe marca la necesidad de diseñar un mapa que armonice y certifique las competencias y establezca las capacidades de I+D+i del sector. Para ello, urge definir un ecosistema de ciberseguridad que lidere el desarrollo de la industria y la investigación nacional y una agenda estratégica de investigación e innovación para España que mejore su identidad digital, los laboratorios de 5G, la seguridad en IA o las tecnologías cuánticas.

Próximos pasos del FNC

El FNC quiere señalar que estos trabajos son un primer paso para seguir avanzando en el aumento de la colaboración público-privada. En este sentido, las nuevas líneas de trabajo irán centradas en acciones dirigidas a aumentar la concienciación del ciudadano en ciberseguridad, así como fomentar su corresponsabilidad; la incorporación de la ciberseguridad en el buen gobierno corporativo de las empresas; y la internacionalización de la industria, la I+D+i y el talento. Asimismo, se trabajará en la elaboración de una agenda estratégica de I+D+i; en el análisis de las propuestas formativas y de capacitación existentes y *gaps* respecto al Esquema y Competencias para fomentar una Formación y Capacitación de mayor calidad; en el estudio del mercado de ámbito nacional en el sector de la Ciberseguridad para conocer; analizar las capacidades actuales ante las necesidades genéricas de ciberdefensa y mejorar la colaboración público-privada en el ámbito regulatorio de ciberseguridad.

Qué es el Foro Nacional de Ciberseguridad

Como ya informara SIC, el Foro Nacional de Ciberseguridad se constituyó en 2020 bajo el paraguas del Consejo de Seguridad Nacional, y está presidido por el Departamento de Seguridad Nacional, constando igualmente de dos vicepresidencias a cargo del CCN e INCIBE. Está compuesto, además, por los organismos públicos con competencia en la materia y por 16 organizaciones representantes de la sociedad civil y el sector privado. Actualmente el Foro cuenta con cinco grupos de trabajo activos: grupo de cultura de ciberseguridad; grupo de apoyo a la Industria e I+D+i; grupo de formación, capacitación y talento en ciberseguridad; grupo de análisis e impulso a la industria de ciberdefensa y grupo de trabajo sobre regulación.

Más información: <https://foronacionalciberseguridad.es>



CROWDSTRIKE

Stop Cozy Bear

We Stop Breaches

Consigue una capacidad de protección inigualable de la plataforma cloud-native líder del mercado.



Alerta del aumento de ataques de *ransomware* contra infraestructuras críticas en un informe conjunto con el CERT-EU

ENISA actualiza su modelo de madurez para CSIRT e inaugura su nueva sede en ATENAS

La **Agencia de Ciberseguridad de la UE (Enisa)** publicó en febrero una nueva versión del marco de madurez de los Equipos de Respuesta a Incidentes de Ciberseguridad (CSIRT), para mejorar sus capacidades a través de una metodología de evaluación personalizada. Basado en el desarrollado en 2019 por la Agencia y, al igual que su predecesor, "pretende contribuir a la mejora de la capacidad de gestión de ciberincidentes, con un enfoque en los CSIRT nacionales", destacan desde Enisa. Así, la nueva versión incluye un parámetro adicional de 'Política de medios públicos', además de

revisar los 44 parámetros restantes del estándar 'SIM3' de la Open CSIRT Foundation. Se trata del Modelo de Madurez de Gestión de Incidentes de Seguridad usado desde 2008 por las diferentes comunidades de CSIRT. Enisa utiliza este estándar como referencia para el marco que desarrolló. Los parámetros consisten en atributos relevantes para la organización, operación o funcionamiento de un CSIRT y se clasifican en las siguientes categorías: organizacionales,

humanos, herramientas y procesos.

En la UE, se alienta a los CSIRT nacionales a desarrollar su madurez sobre la base del enfoque de madurez de tres niveles de ENISA CSIRT, que se basa en SIM3. La



evolución del marco también obedece a la necesidad de cumplir con los requisitos de la Directiva sobre seguridad de las redes y sistemas

de la información (NIS) sobre las capacidades de los CSIRT y tiene en cuenta los requisitos propuestos para estos equi-

pos en la actual revisión de la Directiva NIS, conocida como NIS2.

No obstante, Enisa recuerda que "el marco también es adecuado para otro tipo de CSIRT, como organizaciones multinacionales



Aumento de las amenazas

Además, la Agencia publicó un informe de amenazas, bajo el título 'Threat Landscape Report Volumen 1', junto con el **CERT-EU** que este año cumple una década desde

que comenzara a funcionar. En él se alerta de un "aumento sustancial de las ciberamenazas para las organizaciones públicas y privadas en toda la UE", a través de ataques de *ransomware* y de otros dirigidos contra infraestructuras críticas.

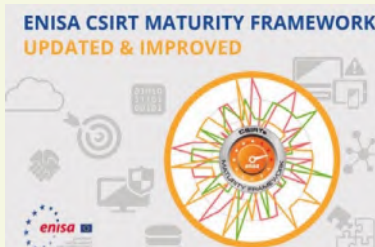
o sectoriales, universidades, hospitales o agencias gubernamentales".

Al mismo tiempo, Enisa inauguró, también en febrero, su nueva sede en Atenas, en un encuentro que corrió a cargo del Ministro griego de Gobernanza Digital, **Kyriakos Pierrakakis**, y la Vicepresidenta de la Comisión Europea, **Margaritis Schinas**.

Copa del mundo cibernética

Además, impulsada por Enisa, en septiembre se celebrará la primera 'Copa del Mundo Cibernética' (ICC), junto con otras organizaciones regionales e internacionales.

Comprenderá una serie de desafíos de ciberseguridad y se espera que participen más de 4.000 jóvenes talentos de Europa, América del Norte, Asia, África y Oceanía, con más de 64 países involucrados. Cada región geográfica estará representada por un equipo de jóvenes talentos.



Más de la mitad de los analistas de los SOC's se plantean renunciar por agotamiento

Las organizaciones podrían enfrentarse en 2023 a un año difícil después de que una investigación de la *startup* irlandesa **Tines** pusiera de manifiesto que es probable que el 64% de los analistas de los Centros de Operaciones de Seguridad (SOC) cambien de trabajo el próximo año. La compañía, que encuestó a 468 analistas de operaciones de seguridad (SecOps) que trabajan a tiempo completo en empresas con 500 o más empleados, desveló que el 71% está experimentando cierto nivel de agotamiento, "debido a que el 69% no tiene suficiente personal y a que el 60% ha visto aumentar su carga de trabajo durante el



último año", cita el informe. Casi dos tercios (64%) afirmó que dedican más de la mitad

de su tiempo al "tedioso trabajo manual" y aproximadamente el mismo número (66%) cree que la mitad de sus tareas podrían automatizarse.

El exceso de herramientas también parece estar contribuyendo a las ineficiencias en el SOC, según el estudio. Y es que, más de la mitad (53%) destacó que utiliza entre 11 y 30 productos relacionados con la ciberseguridad. Los encuestados indicaron, asimismo, que la elaboración de informes (50%) es la tarea que les consume más tiempo, seguida de la supervisión de amenazas (47%), la detección de intrusos (38%), el trabajo de detección general (32%) y las operaciones (31%).



Cyber
Guardian



La **ciberseguridad** de los
grandes, al alcance de todos.

Casi todas las Comunidades están dedicando partidas específicas para proteger sus redes y sistemas y poner en marcha su SOC, en coordinación con el Centro Criptológico Nacional

La puesta en marcha del COCs de la AGE y la Red Nacional de SOC impulsan la ciberseguridad en comunidades y ayuntamientos

España, que cuantitativamente es uno de los grandes referentes europeos en equipos de respuesta a incidentes (CERT/CSIRT), y en titulaciones de grado y postgrado en ciberprotección, también lo quiere ser en Centros de Operaciones de Ciberseguridad (SOC). A la iniciativa de la Administración Pública de contar con un Centro de Operaciones (COCs), que liderará el **Centro Criptológico Nacional (CCN)**, junto a una Red Nacional de SOC (RNS), y actuará en coordinación con un 'Super SOC' europeo (actualmente en estudio), se vienen sumando en estos últimos meses el anuncio de una 'lluvia' continua de SOC locales y autonómicos con vocación de integrarse con el COCs para disponer de una visibilidad granular y en tiempo real de lo que ocurre en las redes españolas, sobre todo, de los servicios públicos.

En este contexto, de momento se ha adjudicado ya la puesta en marcha del Centro de Operaciones a una UTE (unión temporal de empresas), integrada por **Indra** y **Telefónica**, con un presupuesto de 46,4 millones de euros, con una duración de dos años (hasta diciembre de 2023). Esta cantidad se suma a los 5,2 millones que ya se invirtieron en 2021 a través del **Ministerio de Defensa**

para este proyecto. Previsiblemente, otros servicios y tecnologías de terceros subyacentes se sumarían, de un modo u otro, a esta ambiciosa y nada trivial iniciativa.

En paralelo, desde el CCN se está trabajando para que comunidades y administraciones locales

pongan en marcha sus SOC. Así, en marzo, en la XXIII reunión de Ciberseguridad de la Comisión Sectorial de Seguridad, organizada por el CCN, se presentó el 'Modelo Valenciano de Ciberseguridad' como el 'camino a seguir' para comunidades autónomas, diputaciones y entidades locales.

Tanto comunidades, como ayuntamientos, prevén financiar sus proyectos con fondos europeos de los programas de recuperación. Por ejemplo, a la madurez en protección digital de muchos actores en comunidades como Madrid —que prevé poner en marcha, al fin y a no mucho tardar su propia Agencia de Ciberseguridad en 2022—, Valencia o Galicia se suman al fuerte impulso de otras como Andalucía, Aragón y Canarias, entre otras.

Centro de Excelencia y Estrategia de Galicia

Entre las grandes novedades de este primer trimestre destaca el anuncio de la **Xunta gallega** de una inversión de 3,5 millones de euros



Parque Tecnológico de Galicia, en Ourense

para poner en marcha un Centro de Excelencia para fortalecer la lucha contra la ciberdelincuencia. Situado en el **Parque Tecnológico de Galicia** (Tecnópole, en la imagen) ourensano, también, estará dedicado a I+D+i en ciberprotección y para potenciar el talento especializado en este campo.

Por otro lado, la nueva Estrategia Gallega de Ciberseguridad 2022-2027, ya en camino, reforzará las líneas de trabajo y recursos en ciberseguridad para garantizar la expansión de las políticas digitales de la Xunta y recogerá las acciones para ejecutar las obligaciones de gobernanza y cumplimiento del nuevo ENS

Plan de choque de la Generalitat

En Valencia, también ha sido significativo el denominado 'Modelo Valenciano de Ciberseguridad', una evolución del plan de choque de entidades locales puesto en marcha en 2021 por su **Conselleria de Hacienda** y que se ha convertido, según han destacado sus responsables, en "modelo de excelencia para implementar por el resto de las autonomías". Así lo resaltó en una intervención, en marzo, el Director General de las TIC, **José Manuel García Duarte**, en la que destacó que "el esfuerzo realizado por la Generalitat en los últimos meses a través del plan de choque nos ha convertido en un ejemplo a seguir para el CCN-CERT, dependiente del Gobierno central, que ahora busca expandirlo al resto de comunidades autónomas". De hecho, tras el desarrollo de dicho plan y en coordinación con las tres diputaciones provinciales, "se ha delegado en el CSIRT-CV los servicios de seguridad que presta el CCN-CERT como máximo organismo competente en materia de ciberseguridad a nivel nacional y que permitirá que las entidades locales de la Comunidad sean de las primeras en integrarse 'de facto' en la Red Nacional de SOC".

Agencia y estrategia andaluza

En Andalucía, el Consejero de la Presidencia, **Elías Bendodo**, anunció en febrero que en el Pal-



I Congreso de Ciberseguridad de Andalucía

meral de las Sorpresas de Málaga se ubicará la **Agencia Digital de Andalucía**, que ya cuenta con una sede en Sevilla, y el nuevo **Centro de Ciberseguridad** de la comunidad. Éste último, con un presupuesto de 60 millones de euros a tres años y que espera estar operativo en 2022.

De hecho, los pasados 23, 24 y 25 de marzo, la Agencia Digital de Andalucía celebró su primer Congreso de Ciberseguridad, un evento multitudinario en el que se dieron a conocer aportaciones que se tendrán en cuenta para la Estrategia andaluza de Ciberseguridad 2022-2025, que hizo su puesta de largo en dicho evento y de la que SIC detalla en otras páginas de esta edición.

Ecosistema robusto para Aragón

Por su parte, **Aragón** anunció una inversión de más de 20 millones de euros en el 'cerebro informático' de la Administración autonómica, como parte de un ecosistema robusto en torno a la ciberseguridad nacional, teniendo como ejemplo a países como Israel, Finlandia o Suecia y tomando como punto de partida diferentes

thycotic y **Centrify** son ahora Delinea.

Delinea™

Definiendo los límites de los accesos privilegiados.

En un mundo híbrido y sin perímetro, lo contrario de lo complejo no es simple, es precisión.



delinea.com

actuaciones en Huesca, con el apoyo del Gobierno autonómico y

la **Universidad de Zaragoza**, entre otros. Y es que, el **Ayuntamiento de Huesca**, que pondrá en marcha un SOC y una oficina virtual, con una partida de 200.000 euros, quiere pugnar por ganar 'imagen de marca' como referente en ciberprotección. Además, la comunidad ha anunciado una inversión de 4,5 millones para poner en marcha su SOC, que se ubicará en el parque tecnológico Walqa.

Castilla y León redobla esfuerzos

Castilla y León, que cuenta con el Servicio de Seguridad de la Información de la **Dirección General de Telecomunicaciones y Transformación Digital**, también está redoblando sus esfuerzos en este ámbito, aunque la Junta ya tiene un SOC, que gestiona la Dirección General a través de **GMV**. Entre otros, ha publicado un Decreto regulador de la política de seguridad de la información y ha puesto en marcha varios proyectos relacionados con la ciberseguridad dentro del Componente 11 del Plan de Recuperación, Transformación y Resiliencia.



Navarra evoluciona

Navarra, que dispone de un SOC con una década de experiencia y con un carácter horizontal -presta servicio a todos los departamentos y organismos autónomos del Gobierno de Navarra, incluido Salud, Hacienda Foral de Navarra, Policía Foral, etc - continuará su evolución en ciberseguridad con importantes mejoras, fruto de su madurez y trayectoria. Entre otros aspectos, este año acometerá la implementación de protección anti-*ransomware* a nivel de sistemas de almacenamiento, se contará con detección de ciberamenazas en tiempo real y *threat hunting* mediante la evolución del SIEM actual a un producto nuevo (IBM QRadar), además de mejorar las capacidades de su Red Team, para realizar simulaciones de ciberataques avanzados y persistentes, y dirigidos (APTs), y aumentar la interconexión con fuentes de inteligencia de reconocido prestigio. También, está previsto la certificación en el Sistema de Gestión de Seguridad de la Información ISO27001 del área completa de Infraestructuras, Telecomunicaciones, Centros de Datos, etc., y la implantación de un Sistema de Gestión de Continuidad de Negocio, basado en ISO22301.

SOC / CSIRT en Murcia

Por su parte, **Murcia** tiene en vigor un contrato centralizado de Comunicaciones y Seguridad informática de la Comunidad 2018-2021 (prorrogado hasta 2023), con una partida para ciberseguridad, a través de la que se tiene un servicio de SOC y CSIRT, además de contar con cumplimiento normativo y la



adecuación al ENS de las diferentes consejerías, organismos autónomos y entes públicos adheridos de la Comunidad. "Adicionalmente, y en colaboración con el CCN-CERT, hemos participado en la creación de un vSOC para extender este servicio a diversos ayuntamientos de la región", explican desde el gobierno regional a la vez que adelantan que en este 2022, "está previsto licitar un nuevo SOC que amplíe los servicios actuales y los complementa con concienciación sobre ciberseguridad para usuarios, que dé servicio no sólo a los organismos y consejerías de la administración regional sino, también, a los ayuntamientos de menos de 20.000 habitantes". El presupuesto previsto ronda los 2,8 millones de euros anuales.

Canarias licita CSIRT-CERT

El **gobierno canario**, que desde hace dos años tiene su propio SOC, también tiene previsto licitar un CSIRT-CERT (se denominará CSIRT-CAN), "cuyo ámbito irá más allá del propio Gobierno de Canarias. El propósito es dar servicio a las entidades locales, además de permitir la instalación de equipos para la recolección de datos (sondas), servicios profesionales para asistencia e, incluso, integrar a la administración de Justicia (que tiene financiación finalista al respecto)", han explicado desde el gobierno canario a SIC.

Otras autonomías

Baleares, por su parte, según ha explicado a SIC, también contará con un SOC, dependiente del departamento de **Modernització i Administració Digital**, al que destinará cerca de 1,5 millones de euros, en tanto que desde el gobierno de **La Rioja** se ha comunicado que "también está apostando por mejorar su ciberprotección y que el gobierno cuenta un SOC que será renovado a través de una licitación (NEOTEC)".

Ciudades inteligentes: los ayuntamientos invierten en proteger sus dispositivos conectados, en IA y en sus SOC's

En cuanto a las iniciativas locales, se registra una vibrante actividad. Dentro de ella, reseñar que **Barcelona** —dentro del Proyecto Europeo IRIS para desarrollar las bases de ciudades inteligentes seguras—, haya sido elegida como una de las tres grandes ciudades europeas seleccionadas por **Cisco** para probar la plataforma de ciberseguridad IRIS en su red urbana de IoT y de Inteligencia Artificial.

En **Madrid**, el organismo autónomo de **Informática del Ayuntamiento (IAM)** creó en 2021 un Centro de Ciberseguridad, como elemento vertebrador de la actividad y protección de **Madrid Digital**. Y en 2022 continuará experimentando mejoras en capacidades y medio para dar soporte a lo que busca ser la estrategia de la capital como 'ciudad inteligente'. Para ello, también se ha puesto en marcha el **Comité Municipal de Seguridad de la Información** y se espera aprobar, el 23 de



junio, la Ley para la creación de su **Agencia de Ciberseguridad** —en abril se quiere dar 'luz verde' a su anteproyecto—.

En **Bilbao** también se podrá en marcha un SOC, a través de una licitación de más de 250.000 euros, con los fondos Next Generation, además de acometerse otras mejoras en protección digital, como la renovación de la infraestructura de *backup* para garantizar las copias WORM, la detección de amenazas en la capa DNS y DHCP o el proyecto de Ciberseguridad para la Ciudadanía.

Vigo también está poniendo en marcha un SOC, complementando lo que ya tiene en este ámbito para integrarse en la Red Nacional de SOC. Y **Alicante**, a través de la concejalía de Nuevas Tecnologías, prevé poner en marcha un centro de operaciones, además de renovar los servidores e implementar una capa de IA. Para ello, dedicará 1,3 millones de euros.

Burgos, por su parte, destinará una partida, que rondará los 650.000 euros, a reforzar su ciberprotección y fomentar el teletrabajo, con dinero de los fondos europeos. Igual que **Oviedo**, que pondrá en marcha su propio SOC, con una inversión de 800.000 euros.

Por su parte, el **Cabildo de Tenerife** presentó su 'Plan de Modernización Municipal' correspondiente a 2022, que distribuirá dos millones de euros entre los ayuntamientos tinerfeños para el despliegue de proyectos en ámbitos como la ciberseguridad.

SEIDOR

Human focused
Technology experts



seidor.com



[/seidor](https://www.linkedin.com/company/seidor)

ANDALUCÍA se suma a las iniciativas autonómicas y presenta también su estrategia de ciberseguridad

Como puesta de largo de sus acciones encaminadas a la ciberprotección, Andalucía celebró en Málaga los pasados 23, 24 y 25 de marzo, a instancias de su gobierno regional a través de la **Agencia Digital de Andalucía**, su I Congreso de Ciberseguridad en cuyo marco se confirmó la ubicación en la pujante ciudad costera anfitriona del **Centro de Ciberseguridad de Andalucía** y se presentaron las líneas maestras de desarrollo de la **Estrategia Andaluza de Ciberseguridad 2022-2025**, llevada a cabo por el Director Gerente de la ADA **Raúl Jiménez**.

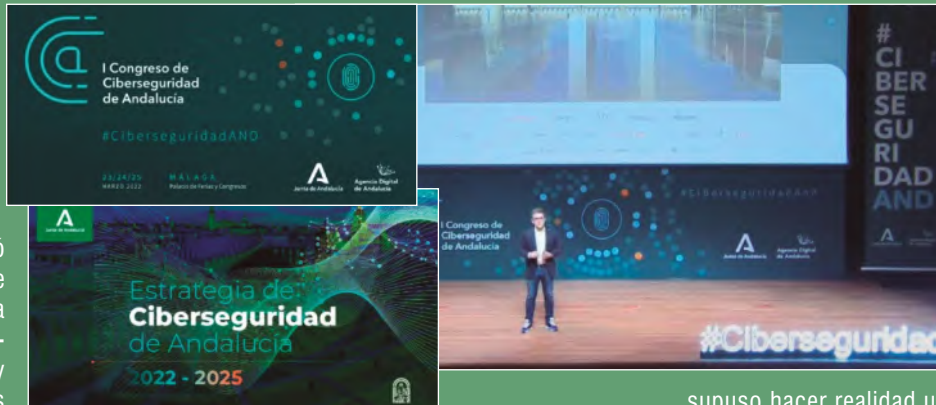
En la sesión matinal de apertura tomaron parte, de un lado, la experta europea de re-

ferencia en el ámbito **Lorena Boix**, Directora para la Sociedad Digital, la Confianza y la Ciber-

El evento, que registró la asistencia presencial de varios centenares de interesados, ofreció una oportunidad única para la presentación oficial de esta estrategia –de la cual SIC ofrece un detallado resumen en otras páginas de esta edición de abril– que

supuso hacer realidad una experiencia de trabajo colaborativo entre la Administración Pública y muchos actores de ciberprotección del sector TIC con intereses en la región.

El congreso incluyó mesas de debate, área expositiva y zona para *networking*.



seguridad en la Dirección General CONNECT de la **Comisión Europea**, e institucionalmente **Francisco de la Torre**, Alcalde de Málaga, y **Antonio Sanz**, Viceconsejero de Presidencia, Administración Pública e Interior de la Junta de Andalucía.

IMDA, ICEX e INCIBE muestran industria española al mercado Asia/Pacífico



ICEX España Exportación e Inversiones, en colaboración con **Incibe** y la **Oficina Económica y Comercial de España** en Singapur, organizaron el pasado 25 de marzo, en Madrid y por primera vez, una reunión –privada no abierta al público general– sobre empresas españolas para la protección de la seguridad y la privacidad del dato y/o el desarrollo de seguridad en la nube con interés en el mercado Asia/Pacífico al objeto de favorecer la internacionalización de nuestras empresas en el mercado oriental.

En dicha reunión y de la mano del **Infocomm Media Development Authority (IMDA)** de Singapur, **Alastria** e **Incibe**, se ana-

lizaron las soluciones de cadena de bloques y ciberseguridad enfocadas en la protección del dato y de la nube por parte de empresas españolas y ante un público perteneciente a las entidades anteriormente mencionadas.

En la reunión, realizada en el auditorio de ICEX en Madrid, tras la pertinente invitación pública, participaron cinco empresas españolas especializadas en la materia (**AuthUSB**, **eSignus**, **Fractalia**, **Leet Security** y **One eSecurity**), que mostraron, en sus respectivos segmentos de ciberprotección, las claves principales para cubrir las necesidades que este sector demanda a día de hoy.

Empresas vascas trabajan en el desarrollo de mecanismos avanzados para proteger la red eléctrica

La red eléctrica es uno de los sistemas más críticos de cualquier país y cada vez cuenta con más elementos conectados. Para mejorar su ciberprotección, en el País Vasco se ha puesto en marcha el proyecto **TrueValSec (Trust Technologies for Smart Grid value chain Cybersecurity)**, bajo el programa **I+D Hazitek 2021**, y en el que participan desde **Ikerlan** hasta el **Clúster GAIA**, así como otras organizaciones como **Inge-**

team Power Technology, como líder del proyecto; **Electrotécnica Artech Smart Grid**, **Enigma Media**, **Iberdrola**, **Ormazabal Protection & Automation**, **PwC**, **Zigor**, y **ZIV Aplicaciones y Tecnologías**.

Su objetivo es la generación de tecnologías de ciberseguridad innovadoras, verificables y esca-

lables, “que permitan construir soluciones a largo plazo para cumplir con los retos de negocio y competitividad del sector electrónico en las redes inteligentes del futuro”. “Lo que hemos estado trabajando en TrueValSec es una ciberseguridad defensiva teniendo en cuenta todos los elementos que forman la cadena de valor.

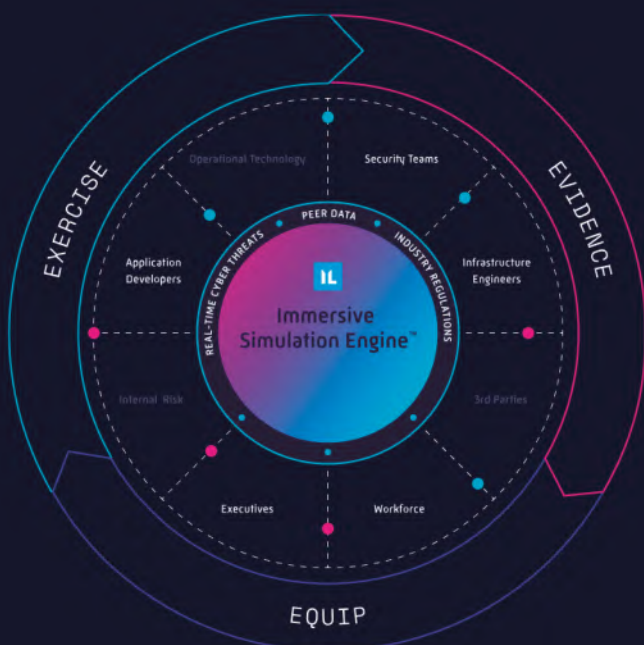
Es decir: establecer mecanismos de defensa más avanzados para tratar que la red eléctrica

sea impenetrable. Este tipo de medidas, orientadas a evitar cualquier tipo de ataque son, sin duda, las más importantes en un mundo cambiante, por lo que debemos invertir en ellas”, ha destacado el Responsable de Ciberseguridad en la UN Power Grid Automation de Ingeteam, **Imanol García**.





La plataforma que impulsa las capacidades de ciberseguridad a equipos técnicos y no técnicos



Cansado de enseñar ciberseguridad de manera tradicional en la Inteligencia británica, James Hadley — CEO de Immersive Labs— ha creado una plataforma con más de 1600 laboratorios para que equipos técnicos y no técnicos aprendan de la única forma posible: a través de la experiencia en un entorno totalmente real. Immersive Labs cuenta con la primera plataforma de preparación cibernética que permite evidenciar la capacidad en ciberseguridad y el nivel de riesgo y resiliencia. Además, brinda métricas precisas de las habilidades, conocimiento y juicio de los equipos para que, posteriormente, se pueda reportar con facilidad y precisión.

Cyber Workforce Optimization ofrece laboratorios dinámicos basados en ejercicios desarrollados por expertos en la materia y con la tecnología de inteligencia de amenazas más reciente del sector — proporcionando, a su vez, créditos CPE. Asimismo, disponemos de un contenido actualizado, por lo que cualquier amenaza estaría disponible en nuestra plataforma en cuestión de minutos tras su descubrimiento. Con el objetivo de ejercitar, evidenciar lo aprendido y, posteriormente, proporcionar las herramientas adecuadas para mejorar y demostrar dónde estábamos, estamos y queremos llegar en nuestro trayecto. De forma que CWO permite justificar toda la estrategia de ciberseguridad.

Para Immersive Labs el eslabón más fuerte somos las personas y, por ello, creemos firmemente en formar, fomentar el desarrollo interno, retener el talento y proporcionar resiliencia a todo el equipo que conforma la organización. ¿Es posible medir la ciber-resiliencia? Nosotros podemos hacerlo y queremos que nos acompañes en este viaje.

Resilience
you can prove.

Readiness
you can
measure.

Confidence
you can trust.



Un nuevo informe, que actualiza el ecosistema, destaca que cuenta ya con más de 430 empresas en este ámbito

CATALUÑA presenta su nueva Comunidad de Ciberseguridad con foco en el talento, el emprendimiento y la internacionalización

En un acto en la Universidad Pompeu Fabra, el pasado 16 de marzo se presentó la 'Comunidad de Ciberseguridad de Cataluña', en un encuentro en el que se destacó la importancia de esta iniciativa, así como sus objetivos y el catálogo de servicios. Además, se dieron a conocer sus grupos de trabajo vinculados a los ámbitos de transformación operativa, internacionalización, startups e inversión y talento.

Esta 'Comunidad de Ciberseguridad' es una de las cinco comunidades tecnológicas que integran la denominada -curiosamente en inglés- **Digital Catalonia Alliance (DCA)**, una coalición sectorial con cerca de 360 miembros que busca el impulso y la dinamización del ecosistema tecnológico emergente. Está impulsada por el **Departamento**



de la Vicepresidencia y Políticas Digitales y Territorio de la Generalitat y la Fundación i2CAT y cuenta con la coorganización de la **Agencia de Ciberseguridad de Cataluña**. El evento que fue inaugurado por el Director de esta última, **Oriol Torruella**, también contó con la participación de **Tomàs Roy**, Director de Estrategia de Seguridad e Internet Segura en el organismo de ciberprotección catalán, así como con **Xavier Galcerán**, Responsable de la Comunidad de Ciberseguridad de la DCA en la Fundación i2CAT.

Además, se presentó, en este ámbito, el Grupo de trabajo en Transformación Operativa, con **Olga Forné**, Global CISO en Mediapro Group y **Genís Margarit**, vocal y representante de **Telecos.cat**, el de Trabajo en Internacionalización, con **Meri-**

txell Pineda, CEO en **Outlier Consulting** y **Lluís Vera**, CEO en **Ackcent**, el de *startups* e Inversión, con **Mónica Espinosa**, Cofundadora de **WERock Capital** y **Daniel Solís**, CEO de **Blueliv**, así como el de Trabajo en Talento, con **Helena Rifà**, Directora Académica del Máster Universitario de Ciberseguridad y Privacidad (MISTIC) en la **Universidad Abierta de Cataluña (UOC)** y **Manel Medina**, Coordinador del Nodo de Ciberseguridad del **DIH4CAT** y Catedrático de la **Politécnica de Cataluña (UPC)**.

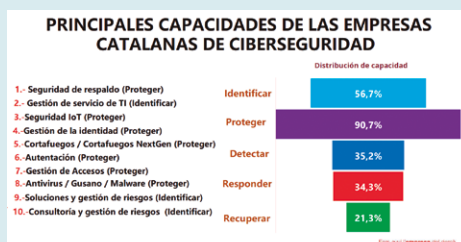
Congreso catalán de ciberseguridad

Por otro lado, del 10 al 12 de mayo la Ciudad Condal acogerá el **Barcelona Cybersecurity Congress**, que contará con conocidos expertos y que debatirá, entre otros aspectos, sobre la importancia de la ciberseguridad en el teletrabajo.

El ecosistema catalán recoge los frutos de su esfuerzo

Cataluña está haciendo un importante esfuerzo por ser un destacado agente en el panorama de ciberseguridad nacional. Su **Agencia de Ciberseguridad** y **ACCIÓ** presentaron en marzo una nueva edición de su informe en el que se destaca que la región ya cuenta con 432 empresas que trabajan en este ámbito, el cual genera más de 8.000 puestos de trabajo. Además, se recuerda que "la consolidación de las herramientas digitales a raíz de la pandemia de la Covid-19 también ha impulsado la facturación del sector en un 11% en el último año", estimándose una superación de los 900 millones de euros.

Se destaca como especialmente positivo que el número de empresas dedicadas a la ciberseguridad creció un 20% durante el 2021 en Cataluña y, en total, alcanzan más de cuatro centenares de actores. Con todo, ha de precisarse que las locales específicas son las menos y, mayoritariamente, las delegaciones y filiales estatales en el territorio. El sector también vio aumentada la facturación en un 11%, alcanzándose los 912,9 millones de euros; y el empleo en un 19% hasta los 8.188 puestos de trabajo (datos de 2020, los últimos dispo-



Valor de mercado de ciberseguridad	% Creación anual 2021-2026
1 Estados Unidos	7,6%
2 China	19,5%
3 Reino Unido	9,5%
4 Japón	8,1%
5 Alemania	7,8%
6 Francia	8,1%
7 Australia	9,2%
8 Corea del Sur	12,7%
9 Canadá	9,2%
10 India	17,7%
11 Países Bajos	8,0%
12 Italia	7,3%
13 España	9,2%
14 Brasil	8,9%
15 Suiza	8,5%

Países ordenados por valor de mercado el 2021

Fuente

nibles). Éstas son algunas de las conclusiones destacadas del estudio 'La ciberseguridad en Cataluña, elaborado al alimón por ACCIÓ -la Agencia para la competitividad de la empresa del Departamento de Empresa y Trabajo- y la Agencia de Ciberseguridad de Cataluña.

En cuanto a cómo es este eco-

sistema, las empresas dedicadas a la ciberseguridad son pymes en su gran mayoría (85%). Asimismo, casi un 30% de los actores del sector son exportadores y hasta un 22% facturan más de 10 millones de euros. Por capacidades, de acuerdo con la taxonomía de la **European Cyber Security Organization (ECSO)**, destacan las empresas dedicadas a la protección, identificación y detección de ataques cibernéticos.

El estudio también apunta la importancia de la ciberseguridad para el tejido industrial dado que el entorno cada vez más conectado permite generar nuevas empresas que desarrollan tecnologías para determinados tipos de ataques y nuevos modelos de negocio basados en el estudio de vulnerabilidades. En esta línea, la ciberseguridad puede contribuir al

pleno desarrollo de otras tecnologías innovadoras como la Internet de las Cosas, el vehículo conectado, la industria 4.0, la salud digital o el comercio electrónico.

Ecosistema catalán

La gran mayoría de las empresas catalanas dedicadas a la ciberseguridad también forman parte del **Catalonia Industry Suppliers**. Se trata de la plataforma en línea para encontrar proveedores industriales y tecnológicos en Cataluña, que en el pasado marzo actualizó su base de datos y ya reúne a más de 4.600 empresas catalanas. Esta herramienta, creada en marzo de 2020, incorpora desde este año nuevas empresas tecnológicas y de servicios consolidándose como el espacio de referencia para posicionar internacionalmente el potencial industrial de Cataluña.

El documento también destaca la buena labor para dar a conocer las tendencias y alertas de ciberseguridad a través de la web oficial ciberseguretat.cat.





Entelgy·Innotec

SECURITY

The (Cybest) Security Company

innotec.security

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

 Entelgy Innotec Security |  @InnotecSecurity |  Entelgy Innotec Security |  @innotec.security



COUNTERCRAFT, en la lista de productos aprobados de mitigación y diagnóstico continuo del DHS de EE.UU.

La Plataforma de engaño cibernético de la donostiarra **CounterCraft** y sus servicios expertos de inteligencia de amenazas han sido incluidos por el **Departamento de Seguridad Nacional (DHS)** de EE.UU. en su 'Lista de productos aprobados (APL)', en la categoría de diagnóstico y mitigación continuos (CDM). El programa



Counter Craft

CDM, desarrollado en 2012, se creó para proporcionar un enfoque dinámico para fortalecer la ciberseguridad de las redes y sistemas gubernamentales. Así, a través de él, se ofrecen herramientas de protección, servicios de integración y paneles que ayudan a las agencias gubernamentales participantes a mejorar su postura de seguridad.

La plataforma de inteligencia de amenazas de engaño distribuida de CounterCraft permite a los operadores diseñar, implementar, monitorizar y mantener campañas de engaño para recopilar inteligencia de amenaza

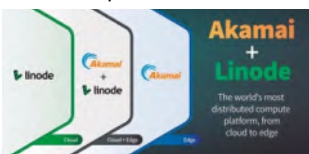
zas procesable en tiempo real, específica para sus misiones y evitar adversarios. Esta tecnología aborda algunos de los casos de uso más difíciles, como la detección de amenazas internas, la búsqueda proactiva de amenazas y la participación activa de atacantes.

El programa CDM apoya los esfuerzos de todo el gobierno y específicos de la agencia para proporcionar soluciones basadas en riesgos, consistentes y rentables para proteger las redes civiles federales. Los operadores cibernéticos de EE. UU. recurren cada vez más al engaño cibernético como contramedida a la creciente ola de ciberataques novedosos y complejos. Desde 2016, la tecnología de CounterCraft ha sido considerada una de las soluciones más valoradas por el DHS y otras agencias federales estadounidenses, frente a notables competidores.

AKAMAI adquiere LINODE por 791 millones de euros, incorporando una plataforma IaaS para desarrollar, ejecutar y proteger las aplicaciones

En febrero, **Akamai Technologies** compró **Linode**, proveedor de una plataforma IaaS (*Infrastructure as a Service*), con la que ofrecerá a las empresas una solución "más fácil de desarrollar y masivamente distribuida para construir, ejecutar y asegurar las aplicaciones", destacan desde la compañía. Junto con Linode, Akamai se convertirá así en una de las plataformas informáticas más usadas del mundo, desde la nube hasta el **Edge**. "La compañía ha sido pionera en el negocio de Edge Computing durante más de 20 años, y hoy estamos entusiasmados de comenzar un nuevo

capítulo en nuestra evolución mediante la creación de una plataforma en la nube única para crear, ejecutar y proteger aplicaciones desde la nube hasta el perímetro. Esta es una gran noticia para los desarrolladores



que ahora podrán crear aplicaciones en una plataforma que ofrece una escala, un alcance, un rendimiento, una fiabilidad y una seguridad sin precedentes", dijo **Tom Leighton**, Director Ejecutivo y Cofundador de Akamai.

AIUKEN Cybersecurity: 10 años de tecnología "Made in Spain" exportada al mundo

De compañía de "garaje" a líder Global. Los comienzos son siempre duros, pero en España para una empresa de tecnología, aún más. Para aquellos que lo estén pensando, que sepan que montar aquí una compañía es una odisea como la novela griega de Homero, y te hace sentir como el verdadero Ulises, y los argonautas.

Garaje hubo poco —el de mi casa del Pardillo—. La realidad es que, como buenos españoles, las horas de diseño y trabajo en la terraza del Lizarrán del Diversia de Alcobendas son nuestro verdadero origen, que nunca hubiera sido posible sin los servicios en la Nube de un Arsys o la wifi gratis del Lizarrán... Ya solo quedamos cuatro o cinco de los de entonces, y somos más de 100. ¡Cómo pasa el tiempo!

Ahora, contamos con orgullo, que somos una compañía de seguridad con SOC virtuales basados en Cloud y que protegemos a los clientes en el Cloud y desde el Cloud, y los analistas te dicen "qué bien, qué correcto, bla, bla, etc."; pero en 2012 todos opinaban que estábamos locos y que la nube no sería adoptada por las grandes empresas y menos para ciberseguridad... Éramos unos visionarios... Y aún lo somos: ahora estamos en Blockchain, Nube, SOAR, MESH y OT 5G; es increíble lo dinámico que es el mercado de tecnología. Y el de ciberseguridad, aún más.



10 Aiuken Cybersecurity

Con el desarrollo en 2016 de la tecnología de nuestro SOC Virtual multifabricante basado en Cloud, adoptamos estándares como Kubernetes e "Infraestructura as code", lo que nos permitió desplegar nuestros SOC en Latinoamérica, Europa, GCC, África, y ahora Norteamérica y Asia. La innovación ha sido la clave, el motor, y el valor de demostrar al mundo que en España hay grandes innovadores, personas con ideas nuevas y que lo único que faltan son recursos y entidades que apuesten por ellos. Nosotros lo hicimos y aquí estamos.

La Ciberseguridad 2012 a 2022. La evolución de Aiuken ha sido la de la ciberseguridad. Desde 2012-2013 las compañías han ido tomando conciencia de que sin la última no es posible el negocio; todo ello, claro está, admitiendo que hasta 2019-2020 con el

Cóvid y la explosión del *ransomware* había muchos que no se habían enterado. Nuestra evolución ha pasado por cuatro etapas claramente diferenciadas: 1) Aiuken como integrador y consultora; 2) Aiuken MSSP y los primeros SOC globales; 3) Aiuken MDR Global; y 4) Aiuken SOAR e IA. La primera es la más natural, al ser una compañía pequeña con necesidad de ingresos, la consultoría y el *reselling* resultan una combinación de rápido crecimiento. La etapa 2 trajo el primer SOC en el centro de Madrid, apenas 100 m², pero ya contábamos con 15 personas y rápidamente pasamos al nuevo del aeropuerto con 300 m² y una capacidad de 50 profesionales. Después vino el de Chile, luego los de Marruecos y Barcelona, más tarde Dubai, Arabia Saudí, Puerto Rico y Costa de Marfil. En 2020 en plena pandemia, inauguramos nuestro nuevo edificio propio, 2.000 m² en Boadilla con dos SOC, uno de IT y otro de OT, con 500 m² de superficie cada uno en un edificio de tres plantas, con laboratorios, salas de 'Demo', de formación, etc.

CLOUDSOC basado en ASIP (Aiuken Security Integrated Platform) 2017. 2017 marcó un hito importante con el nacimiento de la versión 1.0 de nuestra plataforma de SOC. Mereció invertir todo el beneficio de la compañía para el desarrollo, ya que después de tres años, conseguimos tener un software único a nivel mundial que nos posicionó como líderes de plataformas de SOC, encontrándonos hoy en el SOC 5.0 + IA + 5G, un hito en fuentes de inteligencia, orquestación y automatización.

Aiuken 2032. Estos 10 años han sido de vértigo, con crecimientos de más del 25% anuales, cambios tecnológicos increíbles, digitalización tremenda de todos los sectores, incluso pandemias globales y guerras. El futuro nos trae más digitalización, el avance de las Criptomonedas, el Metaverso, Blockchain, 5G, IA, robotización, viajes espaciales e incluso la colonización de la Luna y Marte. Será una nueva década apasionante. Y Aiuken estará ahí para proteger y hacer que los nuevos avances sean seguros para todos.



JUAN MIGUEL VELASCO
CEO
AIUKEN



Cambiando la forma de asegurar las aplicaciones web

¿Miles de activos web que asegurar?
No hay problema. Incorpore la automatización de la seguridad en cada paso de su ciclo de desarrollo y consiga más seguridad con menos esfuerzo manual.



Creado por expertos en seguridad



Innovador y orientado a la investigación



Escalable y adaptable



Los mejores estándares de su clase

Lidera, distribuidor oficial de Invicti

 (+34) 91 837 58 80

 info@lidera.com

 www.lidera.com



Áudea: una propuesta consolidada de 360° de ciberseguridad, riesgos, privacidad y cumplimiento normativo

La verdad es que parece que fue ayer cuando abrimos la primera carpeta en el servidor con el nombre de **Áudea** y ya han pasado 20 años, quién nos lo iba a decir. Nació en 2002, como consecuencia de la segregación de un departamento de nuevas tecnologías de un despacho de abogados; empezamos como cualquier *startup*, con muy pocos medios y recursos y sin ningún cliente, pero con mucha ilusión.

Desde el inicio tuvimos clara la visión de que la seguridad de la información sería clave a medio plazo aún, por lo que, al año de iniciar nuestras operaciones, empezamos a incorporar otra serie de perfiles a la organización (lo que en la actualidad se conoce como consultores GRC, especialistas de ciberseguridad...), para poco a poco convertirnos en lo que somos ahora una consultora especializada en ciberseguridad, riesgos, privacidad y cumplimiento normativo, capaz de prestar servicios transversales en las organizaciones como único proveedor.

En 2006, dimos otro gran paso –parece que no equivocado– y que ha sido y es parte fundamental de la idiosincrasia de la compañía, estableciendo la posibilidad de teletrabajar, convirtiéndonos en una empresa flexible, moderna y con la clara visión de que la dedicación al trabajo no tenía que estar reñida con la conciliación. Estos aspectos junto con el esfuerzo, la humildad, la orientación, la cercanía y el compromiso con el cliente han formado y forman parte de los valores que nos han regido desde el principio y poco a poco nos ha permitido tener nuestro espacio en esta industria tan compleja.

Otro aspecto que creo que merece ser resaltado es que, en 2012, continuando con el afán de innovar, creamos un área formada por pedagogos y especialistas en *e-learning* para desarrollar la línea de negocio de concienciación y formación, siendo en la actualidad proveedores de referencia para grandes compañías en el desarrollo de programas directores de concienciación.



Durante muchos años hemos liderado la compañía, cuatro socios, dos de los cuales surgieron de nuestra propia plantilla, como consecuencia de su trabajo e involucración; pero como todo modelo, ha de estar en continuo movimiento, hace un año decidimos dar un paso más, uniéndonos al **Grupo Logicalis**, con la idea de continuar creciendo y dotar a Áudea de una presencia internacional y, adicionalmente, nos está permitiendo cerrar el círculo en materia de ciberseguridad y seguridad de la información, ofreciendo a nuestros clientes una solución 360° que combina productos y servicios en este ámbito.

Aparte de los valores mencionados anteriormente, sin duda el pilar fundamental de los éxitos de estos 20 años, son todas y cada una de las personas que han contribuido con su esfuerzo y trabajo a que esto haya sido posible manteniendo la misma ilusión, profesionalidad y exigencia que el primer día. Asimismo, nos sentimos agradecidos a todos los clientes, *partners* y colaboradores por su fidelidad y confianza, porque sin ellos no hubiéramos podido llegar hasta aquí.

Si me preguntan por el futuro, lo veo siempre apasionante. Tras 20 años, tenemos las mismas ganas que el primer día, sentimos que seguimos siendo una *startup* llena de retos y oportunidades, nos queda toda una vida por delante y muchos sueños por cumplir.



JESÚS SÁNCHEZ
CEO
ÁUDEA

APPLUS+ adquiere LIGHTSHIP SECURITY para certificación de productos conectados

Applus+, especializada en inspección, ensayos y certificación, compró en febrero el proveedor estadounidense de certificación de productos, **Lightship Security**. Se trata de un laboratorio de ciberseguridad acreditado y especializado en la certificación de productos conectados para grandes fabricantes de Norteamérica y a nivel internacional.

“Los fundadores de Lightship cuentan con una gran trayectoria profesional en el sector y están modernizando la forma en que se enfoca la certificación de productos relacionados con las tecnologías de la información. Y se espera que Lightship mantenga un crecimiento superior al 20% anual durante los próximos años”, destacan desde Applus+.

La operación se enmarca dentro del plan estratégico de la firma catalana para reforzarse en las

tecnologías clave necesarias para apoyar a sus clientes en el cambio tecnológico global derivado de la transición energética, la electrificación y la conectividad. “Esta incorporación añade diversos esquemas norteamericanos reconocidos por la industria a nuestras certificaciones de ciberseguridad en Europa y Asia, de manera que

podemos ofrecer a nuestros clientes un portafolio muy completo de certificaciones para la comercialización de sus productos en todo el mundo”, destacó el Vicepresidente Ejecutivo de la División Laboratories, **Jordi Brufau**. “La oferta conjunta de la certificación europea y norteamericana aportará gran valor a nuestros clientes, al convertirnos en una ‘ventanilla única’ para todas sus necesidades de certificación de producto”, añadió **Jason Lawlor**, Presidente de Lightship.



HORNETSECURITY se certifica en el ENS y alerta de que el 40% de los correos-e entrantes son potenciales amenazas

Hornetsecurity ha logrado la certificación de Conformidad por parte del Esquema Nacional de Seguridad (ENS), que abarca los sistemas de información que dan soporte al desarrollo, servicio y aplicación en el entorno de protección del correo electrónico, de los datos y servicios de *backup* del puesto de trabajo.

En concreto, la compañía ha logrado la acreditación del ENS de categoría Media, dado que su aproximación al mercado es a través del canal, en un proceso que ha llevado a cabo **Oca CERT**. A partir de ahora, Hornetsecurity pone a disposición de sus *partners* una certificación que les otorga un distintivo de calidad, lo que proporciona a la marca una ventaja competitiva para dar servicio a empresas privadas o entidades públicas que decidan contratar a un proveedor en este entorno.

Además, la compañía presentó su ‘Informe sobre amenazas cibernéticas 2021/2022’, centrándose en la comunicación por correo-e. Entre otros datos de interés, destaca que el 40% de todos los correos-e entrantes

representan una potencial amenaza. “Al ser el principal medio de comunicación de las empresas, el correo-e es una de las principales puertas de entrada de la ciberdelincuencia y sigue siendo un importante vector de ataque”, destacan desde la compañía. El *phishing*, los enlaces maliciosos y el *ransomware* se encuentran entre las tácticas de ataque más utilizadas, junto con la “suplantación de marca”, especialmente común también.



¿PROTEGERTE DE LAS
CIBERAMENAZAS TE QUITA
EL SUEÑO?

... ¿O TE DIFERENCIA DE LA
COMPETENCIA?

Generamos confianza, transformamos la
seguridad en una fuente de fortaleza y
ventaja competitiva

| GET THE FUTURE
YOU WANT

Un centenar de grandes compañías se unen para pedir que se exijan cinco estándares básicos de protección en dispositivos IoT

Más de un centenar de multinacionales, entre las que figuran **Google, Microsoft o Deloitte** y organizaciones como **Consumer Reports, Center for Internet Security y Cyber Threat Alliance**, se han unido para pedir a los gobiernos, en una carta publicada en febrero, que se implemen-

ten unos estándares universales para la seguridad básica en dispositivos del Internet de las Cosas (IoT) y que deberían abordarse a través de normativas de ámbito internacional y el apoyo del sector privado.

En concreto, los integrantes de esta petición reclaman que los dispositivos conectados traigan, por defecto, actualizaciones regulares de software, no tengan contraseñas predeterminadas, dispongan de política de divulgación de vulnerabilidades del producto por parte del fabricante, además de datos y comunicaciones

seguras. De hecho, recuerdan que estas ya se encuentran recogidas en más de un centenar de estándares de seguridad y privacidad que se han publicado en todo el mundo.

“Si bien todas las partes interesadas (fabricantes, distribuidores, proveedores, reguladores e incluso los propios con-

sumidores) tienen roles respectivos que desempeñar en el desarrollo, la implementación y el uso seguros de los productos de IoT, la seguridad de los dispositivos requiere que los fabricantes y proveedores que colocan dispositivos en el mercado se adhieran a las mejores prácticas para garantizar que los productos estén diseñados teniendo en cuenta la seguridad”, escribe el grupo. Eso sí, reconocen que “implementar estas capacidades plantea diferentes desafíos para los fabricantes y proveedores de todo el mundo”.



POLONIA impulsa la ciberprotección nacional creando su FUERZA DE DEFENSA CIBERNÉTICA

El Ministro de Defensa de Polonia, **Mariusz Blaszczak**, nombró en febrero a un General del Ejército, **Karol Molenda**, para dirigir la recién creada unidad Fuerza de Defensa Cibernética. Contará con capacidades de defensa, reconocimiento e, incluso, de acciones ofensivas para proteger a las Fuerzas Armadas del país ante ciberataques. “Somos conscientes de que, en el siglo XXI, los ciberataques se han convertido en una de las herramientas de la política más agresiva,

también utilizada por nuestro vecino”, destacó Blaszczak, aparentemente refiriéndose a Rusia. “Por esa razón, estas



capacidades son de naturaleza fundamental y clave para las Fuerzas Armadas de Polonia”. La unidad también trabajará en colaboración con el Centro Nacional de Seguridad Cibernética, iniciada en 2019.

Entelgy Innotec Security: 20 años Having a good time

Parece que fue ayer cuando empecé con este proyecto empresarial y, la verdad, después de 20 años sigo con la misma ilusión y ganas de construir un proyecto importante de ciberseguridad español. Hace dos décadas, cuando la sociedad empezaba a experimentar un desarrollo tecnológico sin precedentes, como consecuencia del creciente uso de internet y de la evolución de las TIC, yo ya me había formado como ingeniero informático y trabajaba como consultor de seguridad de la información. Ahí, cuando todavía ni siquiera existía el término de ciberseguridad, empecé a ser consciente de los riesgos y amenazas que este cambio suponía y, por tanto, del futuro que este sector tendría.

Fue entonces cuando decidí dejar de trabajar en compañías cuyo modelo no encajaba con mi filosofía de empresa y abrir la mía propia. Y con una clara vocación de ayudar y proteger lo más valioso de una organización nació, en septiembre de 2002, Innotec Security.

Con un equipo de solo cuatro personas, nos especializamos en seguridad de la información y gestión del riesgo, convirtiéndonos en una de las primeras empresas en España completamente dedicada a esta materia. Así llegaron nuestros primeros clientes, como Telefónica España, Caja Duero, Caja España y Caixa Galicia, quienes también fueron, en cierto modo, adelantados a su época. Y digo esto porque en aquel momento las organizaciones consideraban la ciberseguridad más como un

gasto prescindible que como una necesidad presente y futura y, por tanto, una inversión ineludible para la continuidad de su negocio.

Con el transcurso de los años y el auge de los ciberataques, sin embargo, cada vez más empresas y organismos fueron reconociendo que debían tener sus sistemas y redes protegidos. De este modo, nuestros clientes fueron aumentando y, como consecuencia de ello, el volumen de la compañía.

Así, decidimos iniciar un proceso de internacionalización, abriendo en 2007 una sede en Chile, a la que siguieron otras oficinas en Brasil, Colombia, México, Perú y Estados Unidos, convirtiéndonos actualmente en una de las principales compañías de ciberseguridad en España y un referente en Latinoamérica.

Pero este impulso no habría sido tal de no ser por el gran salto cualitativo que dimos cuando el 28 de marzo de 2011 el grupo tecnológico Entelgy entró a formar parte de nuestro capital. Un momento clave en la historia de la compañía que, ya bajo el nombre de Entelgy Innotec Security, ha propiciado que hayamos pasado de 60 empleados a más de 550. Fue un acierto estratégico ya que Innotec Security ha conseguido mantener su filosofía de trabajo y su carácter de empresa de nicho dedicada a ciberseguridad.

Actualmente, gracias a todos estos profesionales, con un grado de conocimiento y especialización difícilmente superables, y a nuestros SOC de Madrid, Sevilla y Vitoria, en 2021 pudimos dar servicio a 45 nuevos clientes, superando las 250 organizaciones que confían su seguridad en nosotros. Entre otras, las principales compañías del IBEX 35 y los organismos públicos españoles e internacionales de referencia: OTAN, ONU, OEA, Agencia Europea de Ciberseguridad (ENISA), Centro Criptológico Nacional y Centro Nacional de Inteligencia (CCN/CNI), INCIBE, Centro Vasco de Ciberseguridad (BCSC), etc.

En definitiva, unas cifras que nos permitirán de cara al futuro ofrecer unos servicios cada vez más avanzados, con foco en la inteligencia de amenazas, y mejorar la resiliencia de nuestros clientes.

Por el momento, y echando la vista atrás, tengo claro que este éxito ha sido, sigue siendo y será, sin duda alguna, mérito de las personas. Un equipo humano que ha sabido entender el objetivo de esta empresa, trabajando todos al mismo compás y disfrutando del camino como grandes amigos. Por esto, el lema escogido para este vigésimo aniversario va por ellas y por nuestros clientes: 20 años *Having a good time*.



FÉLIX MUÑOZ
CEO
ENTELGY INNOTEC SECURITY



Symantec™ Data-Centric SASE

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

Contacto:

🌐 westconcomstor.com/es/es

✉️ symantec.es@westcon.com

🌐 broadcom.com

TEHTRIS, con una plataforma europea de XDR, toma altura en España

Tehtris, especializada en neutralización automática de ciberamenazas a través de su plataforma europea XDR (eXtended Detection and Response), anunció a principios de año su expansión en Europa con la apertura durante este año de filiales en España y Alemania, la creación de equipos comerciales en nuevos territorios, así como

con el cierre de nuevas alianzas europeas, que ya se encuentran activas en Suiza, Bélgica y Luxemburgo. De momento, en 2021 contrató a más de 160 personas y en 2020 realizó con éxito una ronda de financiación de Serie A récord, por valor de más de 20 millones de euros.

Este año, Tehtris espera alcanzar los 200 profesionales, "para apoyar a las empresas y administraciones europeas en su carrera tecnológica, destinada a proteger el mundo cibernético, que se ha convertido en

un complejo campo de batalla", destacan desde la compañía, y por ello ha vuelto a destacar su apuesta por mercados como el ibérico o el germano. Además, resaltó que sus tecnologías han sido elegidas e implementadas por los socios europeos de la compañía, como **Cappgemini**,

TEHTRIS XDR Platform

Open interfacing with your security solutions

Orange CyberDefense, **Nomios**, **Expleo Group**, **Sopra Steria**, **Post** (Luxemburgo), **Approach** (Bélgica) y **Eyra Group** (Suiza), entre otros.

La compañía ha desarrollado la plataforma Tehtris XDR, una solución de Respuesta de Detección Extendida, "diseñada en Europa y programada de forma nativa", según la firma, que busca facilitar la detección, el análisis y la neutralización de ciberataques, como el *ransomware*, y comportamientos inusuales o maliciosos.

TORQ inicia sus actividades en Europa y España apostando por la automatización

La compañía **Torq** ha comenzado su actividad en Europa, incluyendo España, contando para ello desde el inicio con el *expertise* de uno de los especialistas técnicos más solventes, el español **Alberto Cita**, quien ha sido fichado en calidad de Arquitecto de Soluciones Senior,

Con una aproximación a la ciberprotección disruptiva, Torq fue fundada por los creadores de Luminare (adquirida por Symantec) y Twistlock (adquirida por Palo Alto) y dispone de una plataforma de automatización "no-code" que está diseñada específicamente para la automatización de la operación de seguridad, y que no tiene asociada ni la complejidad y ni las grandes inversiones asociadas a otras alternativas como las plataformas SOAR, que son viables para muy pocos.

En declaraciones a SIC, Cita precisa que "Con Torq, además

de que se presta como un servicio en nube (SaaS), se necesitan literalmente minutos y cero líneas de código para tener automatizados flujos de operación que permiten aliviar la carga de trabajo de los equipos de operación, reducir la fatiga de alertas, responder más rápido ante incidentes de seguridad, incluyendo, si se estima necesario, validación humana de la automatización, gracias a la integración de *chatbots* con múltiples plataformas de colaboración como Teams, Slack o Webex, simplificar el *threat hunting*, responder de forma automática y sencilla a comportamientos sospechosos de usuarios, incluso estableciendo de forma automática diálogo con los propios usuarios afectados para darles la opción de justificar/validar su comportamiento..., los casos de uso son muchísimos y no paran de crecer", afirma.

ONE eSECURITY: "Together as ONE" con el sueño de ser aún mejores

El pasado 9 de febrero **One eSecurity (ONE)** cumplía 15 años. Han sido 15 intensos años llenos de aventuras luchando codo con codo con nuestros clientes contra infinidad de adversarios avanzados en decenas de países. 15 años que sin duda han constituido una experiencia humana y profesional de valor incalculable para todos nosotros.

ONE empezó siendo solo un ambicioso sueño: crear un equipo de respuesta de élite que fuera capaz de hacer frente a los mayores incidentes. Haríamos así lo que nos apasionaba mientras poníamos nuestro granito de arena para contribuir a un mundo mejor. 15 años e infinidad de incidentes y proyectos después es increíble ver que ese sueño se ha convertido en realidad.

ONE está hoy presente en tres continentes, proporciona todos los servicios imaginables alrededor del ciclo de vida del incidente, cuenta con un equipo humano extraordinario y tecnología propia de vanguardia que nos permiten jugar en la Liga de Campeones de las empresas de nuestro sector a nivel mundial. A pesar de que nuestro sueño ya apuntaba muy alto, no adivinamos que conseguiríamos llegar tan lejos.

Si me preguntasen cuáles han sido las claves de nuestro éxito, les diría que han sido la pasión, las ganas de aprender, el trabajo duro y, sobre todo, las personas.

Como dijo el gran Walt Disney, "se necesitan personas para hacer un sueño realidad". Y el gran reto a lo largo de tantos años ha sido "subir a nuestro sueño" a tantas y tantas personas, clientes y equipo, que han

creído en él y que han ayudado a convertirlo en realidad.

Hace unas semanas uno de nuestros clientes nos decía, tras haber tenido a tiempo un incidente de enormes proporciones, que había sido un placer trabajar con nosotros, tanto por nuestra calidad técnica como, sobre todo, por la humana. Creo que pocas palabras me podían haber llenado de mayor orgullo.

Hace años que adoptamos "Together as ONE" como nuestro lema, y es que desde siempre hemos apostado por el compañerismo y el equipo. Seguramente les resulte curioso saber que es nuestro equipo al completo, desde el más veterano hasta el más junior, quien decide quién se sube a bordo y quién no, ellos eligen quiénes quieren que sean sus compañeros. Y la verdad es que rara vez fallan. Y ese equipo es capaz de empatizar con los equipos humanos de nuestros clientes, ampliando nuestra potencia de fuego y consiguiendo resolver situaciones e investigaciones que a menudo se antojaban imposibles. Raro ha sido el caso en el que, gracias a esta estrategia y capacidades, no hayamos conseguido nuestros objetivos.

Pero el sueño no acaba aquí. Seguimos tremendamente ilusionados por ser aún mejores, por poder seguir ayudando más y mejor a nuestros actuales y futuros clientes a prepararse, detectar y responder a cualquier amenaza, incluso las más sofisticadas, en cualquier parte del mundo, físico y cibernético, un mundo que cada vez resulta más hostil. En definitiva, seguimos, como el primer día, deseando contribuir a hacer este mundo un poquito mejor, un lugar más seguro.

Desde estas páginas quiero mandar un afectuoso saludo a todos los clientes que han confiado en nosotros durante estos 15 años, a todos nuestros compañeros, y en general a todos los que de una u otra forma han contribuido a convertir a ONE en la realidad que es hoy. Gracias.



JESS GARCIA
Fundador y Director
One eSecurity



ISO 27701

Gestión sostenible de la privacidad

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

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

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

marketing@gmv.com

gmv.com

El crecimiento previsto anual, estimado entre el 12% y el 14%, podría aumentar más por el impacto del conflicto bélico internacional

El mercado corporativo de ciberseguridad en España, en constante ascenso, podría aproximarse a los 2.000 millones de euros

Según estimaciones de Revista SIC, que lleva realizando desde el año 2000, referidas exclusivamente a la actividad del mercado corporativo de ciberseguridad -no directamente residencial- en España y algunas áreas de influencia, el sector facturó en 2021 la cifra de 1.710 millones de euros, experimentando un crecimiento promediado del 11% respecto del año anterior, en tanto que su proyección estimada para este 2022 experimentaría un incremento de entre el 12% y el 14% promediado, situando la facturación en órdenes de los 1.932 millones de euros previsto para este año. Con todo, esta previsión aún podría ir al alza derivada del conflicto internacional por la guerra ruso-ucraniana.

La inestabilidad digital, los conflictos y escaramuzas cibernéticas y la intensa amenaza de chantajes y extorsiones por la proliferación de *ransomware* muy agresivos, así como unas administraciones públicas espoleadas por su precariedad defensiva y con el viento a favor de

la eclosión de SOC's y agencias de ciberprotección territoriales, podría disparar estas estimaciones.

El normal devenir del sector, en continua pujanza y crecimiento desde hace dos décadas, y que se vio afectado hace dos años por la llegada de la Covid-19, detonante de que varias áreas de actividad, mayormente referidas a dotar de confidencialidad a las actividades laborales en remoto,

registraran parámetros de crecimiento inusitados (con aumentos de más del 35%) y otras, con foco en proyectos más sofisticados e innovadores, sufrieran retraso o se aplazaran coyunturalmente.

Asimismo, el mercado laboral viene registrando en este periodo una importante convulsión propiciando un inusitado trasiego de profesionales en el sector oferente y

demandante. De la misma manera, continúa causando serias distorsiones en el capítulo de salarios y remuneraciones ante la acusada falta de especialistas en algunas funciones.

Cabe precisar que estas estimaciones de SIC hacen referencia exclusivamente a las actividades mercantiles del sector con clientes empresariales (privados y públicos) que aglutinarían las actividades de consultoría/asesoría, prescripción, implantación de herramientas y soluciones, licencias/mantenimiento/actualización, externalización de servicios (mayormente MSSPs) y en la nube, auditoría, personal externo, formación y seguros (en fase de encarecimiento).

De este conjunto de actividades quedan excluidas las referidas a las estrictamente jurídicas de protección de datos personales (que no las TIC) y a la I+D+i de laboratorios, centros de investigación y universidades.



LOGALTY se convierte en prestador de servicios de Confianza eIDAS con la máxima certificación del ENS y se hace con la compañía SMARTBIOMETRIK

Logalty ha sido el primer prestador de servicios de Confianza eIDAS en obtener la máxima certificación del Esquema Nacional de Seguridad (ENS), emitido por **Aenor**. En concreto, lo ha logrado en 'Categoría Alta' para sus servicios de notificación y contratación electrónica prestados en modalidad *cloud*. Así, esta certificación se suma al resto de acreditaciones que la empresa tiene, como la ISO 27001 e ISO 22301, que certifican la eficacia y adecuación de los sistemas de gestión de la seguridad de la información y continuidad del negocio, dotando a la organización de niveles adecuados de fortaleza, y otorgando confianza a los clientes que sustentan una parte de sus procesos en los servicios que proveen.

Con esta certificación, la empresa se diferencia del resto de prestadores de servicios de confianza, siendo uno de los pocos que ha apostado por su obtención. Esto permite optar, de forma efectiva, a la prestación de servicios en el ámbito de la administración pública, así como reducir la exposición al riesgo de incumplimiento del Re-



glamento General de Protección de Datos, en tanto que la implantación de las medidas del ENS permite satisfacer el artículo 32 del reglamento. Aunque esta certificación tiene una validez de dos años, Logalty ha destacado que ya trabaja para aumentar su alcance y se espera que a lo largo de los próximos meses se incorporen nuevos servicios y capacidades.

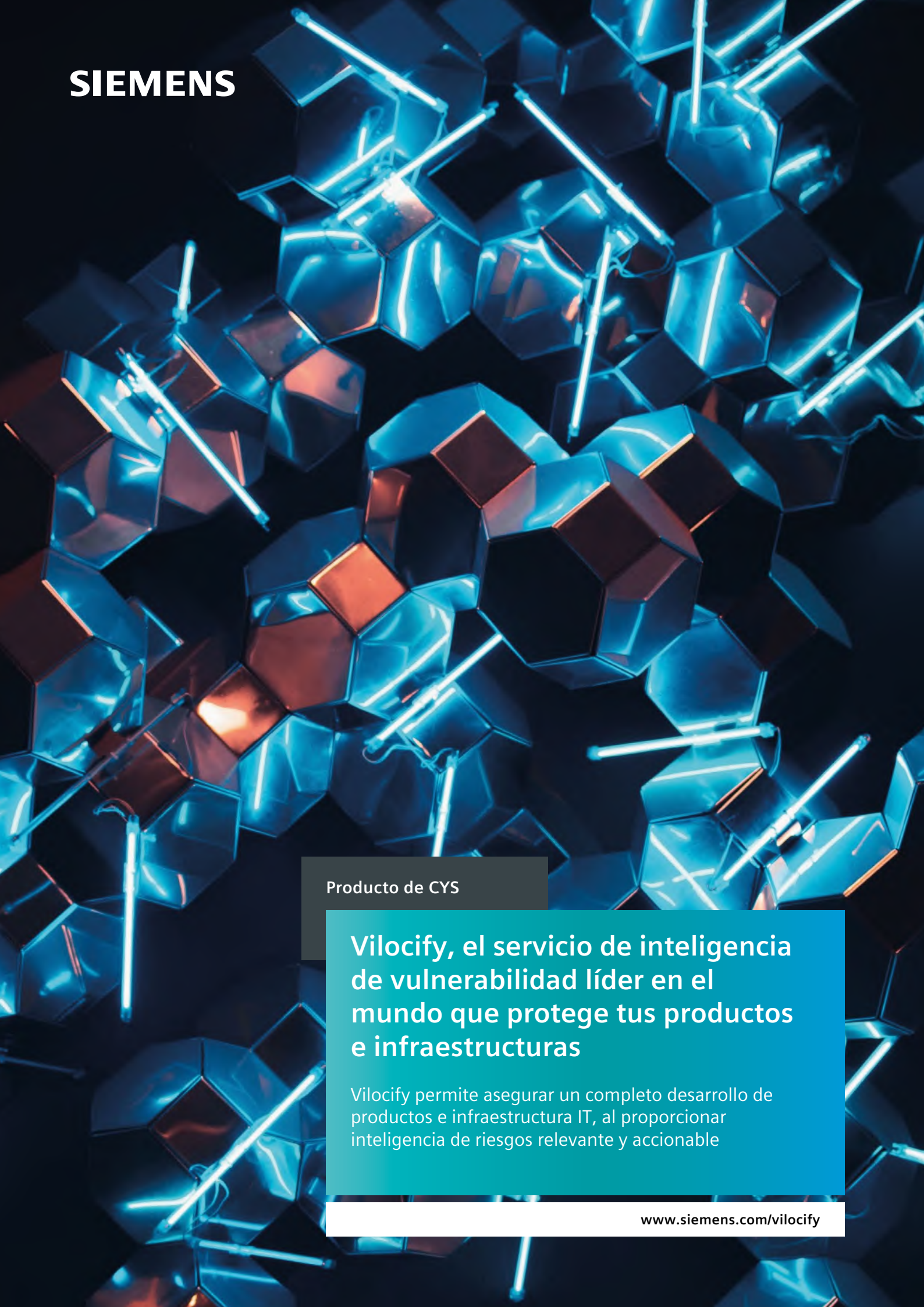
Compra estratégica

Por otro lado, a través de los fondos de capital privado **Ardian Growth**, **MCH Private Equity** y **Swen Capital Partners**, **Logalty** ha incrementado su portafolio tecnológico con la compra de la compañía

Smart [] Biometrik

de verificación de identidad **SmartBiometrik**, que cuenta con soluciones innovadoras en el campo de la identificación y seguridad digital.

Cabe reseñar que esta operación es la segunda adquisición que ha llevado a cabo la compañía, en menos de un año, tras hacerse previamente con **RegTech Solutions**.



SIEMENS

Producto de CYS

Vilocify, el servicio de inteligencia de vulnerabilidad líder en el mundo que protege tus productos e infraestructuras

Vilocify permite asegurar un completo desarrollo de productos e infraestructura IT, al proporcionar inteligencia de riesgos relevante y accionable

www.siemens.com/vilocify



Gigantes tecnológicos, como GOOGLE, se hacen con referentes, como MANDIANT, para ganar negocio en ciberprotección

2021 fue un año récord de inversiones y movimientos en el sector con 430 operaciones y fusiones, según SecurityWeek. En total, se movieron más de 70.000 millones de euros, un 294% más que en 2020, según datos de Momentum Cyber. Una efervescencia que, según los analistas, vino motivada por el incremento de presupuesto dirigido a ciberseguridad ante el mayor riesgo de amenazas, más graves y complejas, destacando la compra de pequeñas empresas de ciberprotección con tecnologías muy específicas. Así, entre los protagonistas de estas compras y ventas estuvieron grandes referentes como Accenture, Cisco, Deloitte, IBM, Mastercard, Microsoft y Schwarz Group, entre otras.

El mercado continúa con muchos movimientos. Diversos analistas han adelantado que los principales en 2022 estarán relacionados con compañías que cuenten con propuestas de protección del hardware y el software de los sistemas de control industrial (ICS) y de tecnología operativa (OT), presentes en todo tipo de instalaciones, desde hospitales

y con las que la ampliará su solución en la nube, CloudGuard. Por su parte, **Forescout** adquirió el proveedor de ciberprotección para el cuidado de la salud **CyberMDX**. La canadiense **Trulioo** se hizo con **HelloFlow**, que ofrece una solución de orquestación sin código, y **Vectra** adquirió **Sirius Security** para ampliar su portafolio para gestionar de amenazas a las

soluciones de monitorización de integridad de archivos (FIM), por 316 millones de euros, por parte de su propietario **Belden** a **HelpSystems**. Un movimiento llamativo por cuanto en 2015 la adquirió a **Thoma Bravo** por casi el doble, unos 640 millones de euros. Precisamente, **HelpSystems** se hizo con **Alert Logic**, un proveedor de seguridad de detección y respues-

han faltado rumores en el mercado, como la posible compra de la división de ciberseguridad de **Atos**, por parte de **Airbus**, después de desistir de la de **Thales**, o la posibilidad de que **Cisco** se haga con **Splunk**.

Mercado ibérico

En nuestro país, **Applus+** se hizo la compañía **Lightship Security**. Se trata de un laboratorio de ciberseguridad acreditado y especializado en la certificación de productos conectados para los fabricantes más importantes tanto de EE.UU. como a nivel internacional. Además, la consultora **Seidor** aterrizó en el mercado galo con la adquisición de **Work Well**, centrada en soluciones informáticas para la pequeña y mediana empresa.

Asimismo, la empresa tecnológica catalana **Firmaprofesional**, que celebra este año su 20 aniversario en el sector de la identidad digital y la firma-e, anunció la adquisición de **biid**, una plataforma de firma electrónica a través del móvil. **Logalty**, por su parte, compró **SmartBiometrik** para añadir la verificación biométrica de identidad a su cartera.

Rondas de financiación

En esta área, la operación más llamativa fue la de **Securonix**, que obtuvo más de 900 millones de euros en una nueva ronda de financiación. Además, la firma de verificación de identidad **Veriff**, recaudó 90 millones de euros. **Cynomi**, una *startup* israelí con una plataforma de 'CISO virtual' para pymes y proveedores de servicios, recaudó 3,1 millones de euros. **Beyon Identity** también se hizo con una nueva inyección de capital, en su caso de 90,3 millones, en una ronda de financiación de la Serie C.

BlueVoyant, además, participó con éxito en otra ronda consiguiendo 225 millones de euros.



Finaliza la adquisición de McAfee, Google compra Mandiant, Check Point se hace con Spectral, Forescout con CyberMDX, Vectra con Sirux, SentinelOne con Attivo, Akamai con Linode, Logalty con Smart Biometrik, HelpSystems adquiere Alert Logic, Micro Focus a Debricked. En España, Applus+ adquiere a Lightship, Seidor a Work Well y Firmaprofesional compra biid, entre otras operaciones.

a fábricas. Así las cosas, durante el primer trimestre, sin duda, la operación de mayor calado fue la compra de **Mandiant** por parte de **Google**, por más de 4.880 millones de euros, y que sumará a su filial **Google Cloud** para "complementar sus capacidades de protección", destacan desde la compañía, ya que desde ella se ofrecen algunos de sus servicios más avanzados en este ámbito, como **Zero Trust**. Con esta incorporación, mejorará su oferta "de operaciones de seguridad de extremo a extremo con capacidades aún mayores para ayudar a los clientes en sus entornos locales y en la nube". También, fue significativa la ejecución de la compra anunciada en 2021 del área de **McAfee** dedicada al consumidor, por más de 12.655 millones de euros, por parte de un grupo inversor formado por **Advent**, **Permira**, **Crosspoint Capital**, **CPP Investments**, **GIC** y **ADIA**.

Además, **Check Point** se hizo con **Spectral**, una *startup* israelí innovadora en herramientas 'developer-first' diseñadas por y para desarrolladores,

identidades y plataformas SaaS. **Tenable** compró **Cymptom**, especializada en gestión de 'rutas' de ataque que podrían ser aprovechadas por los cibercriminales. **Avast** adquirió **Secukey**, proveedor de identidad digital, y **Mitek** compró **HooYu**, especializada en tecnología **KYC**.

SentinelOne se hizo con **Attivo Networks**, para mejorar su oferta de XDR con seguridad de identidad y acelerar el cambio a **Zero Trust**, en una operación que ronda los 556 millones de euros. También, ha sido notable la operación de **Appalachia Technologies**, uno de los principales MSSP en EE.UU., que adquirió **Cyber Protection Group (CPG)**, una empresa de ciberseguridad y cumplimiento. Asimismo, **Akamai Technologies** compró, por algo más de 790 millones de euros, **Linode**, proveedor de una plataforma IaaS (*Infrastructure as a Service*) para desarrollar, ejecutar y proteger aplicaciones.

Pero no todo han sido grandes operaciones. Sirva como ejemplo la venta de **Tripwire**, especializada en

ta gestionadas (MDR). **CyberRes**, la empresa de ciberresiliencia propiedad de **Micro Focus**, compró **Debricked**, una compañía que ayuda a las organizaciones a proteger su cadena de suministro de software. La adquisición permitirá que **CyberRes** ampliar la resiliencia de su software y las capacidades de DevSecOps.

Por su parte, la empresa de administración de vulnerabilidades y superficies de ataque **Cyber Security Works (CSW)** adquirió **CYR3CON IP**. Asimismo, el proveedor de soluciones de redes especializadas, **Belden**, anunció la compra de **Macmon Secure**, con sede en Alemania, de software de control de acceso a la red. La británica **Crossword Cybersecurity**, de desarrollo de software de gestión de riesgos y ciberseguridad, compró la empresa de inteligencia de amenazas **Threat Status**. Además, la firma de capital privado **Crosspoint Capital Partners** adquirió una participación significativa de la Conferencia RSA, que se convertirá en un negocio independiente de **RSA Security**. Tampoco





Compartir es de sabios

En 1998, el presidente de los Estados Unidos, Bill Clinton, firmó la directiva presidencial 63, en la que llamaba al sector público y al privado a compartir información sobre amenazas y vulnerabilidades, tanto físicas como digitales, para proteger las infraestructuras críticas de EE.UU. Acuñaba en esa directiva el término de "Information Sharing and Analysis Center" (centro de análisis y de compartición de información), conocido por las siglas ISAC. En 1999 se creó el **ISAC** para servicios financieros (FS-ISAC). Actualmente, el FS-ISAC reúne a miembros de más de 70 países y ofrece servicios de inteligencia, eventos y formación en ciberseguridad.



"Enseña lo que sabes hacer bien y mejora aún más mientras lo enseñas".

Esta sería la expresión que añadiría a la visión de los mosqueteros para la ciberseguridad en España.

En España, la Línea de Acción 4 de la Estrategia Nacional de Ciberseguridad 2019, orientada a impulsar la ciberseguridad de ciudadanos y empresas, menciona que "... la ciberseguridad es una responsabilidad compartida con los actores privados..." y alude a la "necesaria cooperación para la seguridad común". En esta línea, en julio de 2020 se crea el **Foro Nacional de Ciberseguridad**, liderado por el **Consejo de Seguridad Nacional**.

Recientemente, este foro ha publicado tres trabajos de investigación con valiosa información. En especial, quiero destacar, por un lado, los objetivos y las conclusiones sobre la cultura de la ciberseguridad en España, y por otro, las propuestas para la industria e investigación españolas en ciberseguridad. Es más, el pasado 9 de marzo, el propio presidente del Gobierno anunció el nuevo Plan Nacional de Ciberseguridad. La relevancia de la ciberseguridad sigue creciendo. Desde esta humilde columna, quería compartir una visión y algunas propuestas, muy prácticas, para que tanto la administración española como el sector privado, puedan beneficiarse de esta colaboración entre sectores.

Compartir información no puede limitarse a compartir un formulario a rellenar por cada miembro del foro cada vez que sufra un incidente, ni a una reunión multitudinaria y altamente politizada cada trimestre. Compartir, hoy en día, con las actuales amenazas geopolíticas, está cerca de la visión de antaño de los tres mosqueteros: "uno para todos y todos para uno". ¿Suenan infantil? Bien, no está muy alejada del artículo

5 del tratado de Washington de la **OTAN**. "Enseña lo que sabes hacer bien y mejora aún más mientras lo enseñas". Esta sería la expresión que añadiría a la visión de los mosqueteros para la ciberseguridad en España.

Concretamente, en relación a los ciberincidentes, una posible forma de dividir en trocitos esa colaboración sería tratar la prevención, la reacción y la preparación de modo enfocado y pasito a pasito. Comenzando con la prevención, la inteligencia sobre posibles amenazas es esencial. Las fuentes de la administración y las del sector privado, en especial las de las grandes empresas, suelen ser complementarias. Las pequeñas y medianas empresas apenas tienen acceso efectivo a esta inteligencia. Necesitamos un modo sencillo, atractivo y altamente configurable de hacer llegar a todos los partícipes, administraciones y sector privado, pymes incluidas, información práctica sobre qué deben proteger, por qué y cómo.

En relación a la reacción, es esencial transmitir la importancia de realizar simulacros. Los equipos de respuesta frente a incidentes de aquellas empresas con mejores recursos y amplia experiencia, generalmente en las multinacionales del sector privado, podrían encontrar algo de tiempo para compartir conocimiento con las pequeñas empresas con las que trabajan día a día, sus proveedores, y con las administraciones con las que interactúan. Recordemos que actualmente los incidentes más inesperados, y devastadores, en grandes empresas, proceden de su cadena de valor y no de sus propias redes. "Si les hacemos más seguros, nos hacemos más seguros nosotros también".

Finalmente, con respecto a la preparación, ¿podemos imaginar posibilidades de rotación de profesionales especializados en la detección y respuesta a incidentes, de modo ágil y voluntario, entre pymes, grandes corporaciones y administración? ¿o manuales de reacción frente a típicos ataques de ransomware, ya seguidos con éxito en producción, que puedan ser compartidos, y enseñados, entre los integrantes del foro?

Como ven, son puntos prácticos que pueden colocarnos, como país, en una posición más resiliente que la actual. Como decía una gran amiga, "no esperemos a que caiga un avión comercial para poner radares en todas las aeronaves."

Alberto Partida

Experto en Ciberseguridad

Sígueme en LinkedIn:

<https://linkedin.com/in/albertopartida>



RISKRECON, de MASTERCARD, impulsa la CYBERSECURITY ALLIANCE para reducir el ciberriesgo de terceros a través de su valoración

RiskRecon, una empresa de **Mastercard**, ha creado y puesto en marcha una iniciativa global, la **Cybersecurity Alliance**, para facilitar el acceso a calificaciones de riesgo cibernético en software y herramientas, especialmente, para controlar cualquier posible riesgo a través de la cadena de suministro. Así, a través de la alianza sus asociados tendrán acceso a información de calidad para limitar el riesgo que asumen cuando tienen

acuerdos con otras compañías. De momento, a ella se han sumado **Aravo, Archer, Argos Risk, ComplyScore, CyberGRX, Deloitte, EY, HSB / Munich Re, Interos, Kroll, LogicGate, OneTrust, Privva, ProccesUnity, Standard Fusion, TealBook, Tech Mahindra, Venminder, Whistic y Wipro**, entre otras.

Y es que el riesgo que se asume

a través de negocios con terceros es cada vez mayor, según varios estudios. El analista **Forrester**

Research espera que el denominado 'riesgo de parte enésima'

(vulnerabilidades de proveedores con grados de separación aún mayores) facilitará el 60% de los incidentes de seguridad cibernética en 2022.

Datos de RiskRecon y el Instituto **Cyentia** también destacan que las infracciones cibernéticas de múltiples partes pueden causar 26 veces más daño financiero en comparación con un ataque que afecta a un solo objetivo. Una situación a la que se quiere hacer frente ofreciendo, a través de la alianza, acceso a información de puntuación de gestión de riesgos cibernéticos para que las compañías puedan protegerse mejor del riesgo de terceros.





Hay otra forma
de protegerse del
RANSOMWARE
sin sobresaltos:

LA VACUNA

SI TU ORGANIZACIÓN ES
GRUPO DE RIESGO, **EL RIESGO**
ES NO VACUNARSE.



Le presentamos la solución más sencilla para que todos los equipos de su organización estén siempre protegidos de las principales y más activas familias de ransomware: microCLAUDIA. Se trata de una VACUNA que entra en funcionamiento cuando un usuario decide abrir un archivo que resulta ser dañino y frena su ejecución, previniendo así una posible infección en su compañía. Con ella, estará protegiendo a miles de usuarios y equipos contra este tipo de ciberataque tan frecuente.

microCLAUDIA es compatible con todas las versiones de WINDOWS desde WINDOWS XP y su instalación es muy fácil, así podrá “vacunar” a todos aquellos equipos personales que estén trabajando en remoto.

No deje a su organización expuesta a riesgos innecesarios, participe en nuestra campaña de vacunación.

Si necesita más información, escribanos a clientes@s2grupo.es

Síguenos en:



• [@s2grupo](https://twitter.com/s2grupo) • [s2grupo.es](https://www.s2grupo.es)



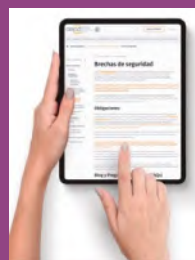
GRUPO

Anticipando un mundo
ciberseguro

El registro de Delegados de Protección de Datos crece más de un 26% llegando a los 82.000

Las reclamaciones presentadas ante la AEPD aumentaron un 35% en 2021, aunque las notificaciones por brechas de datos apenas supusieron un 4%

La Agencia Española de Protección de Datos (AEPD) publicó en marzo su 'Memoria 2021', en la que constata que recibió casi 14.000 reclamaciones (un 35% más), a las que hay que sumar los casos transfronterizos, aquellos en los que la Agencia actúa por iniciativa propia y las quejas de seguridad trasladadas a inspección. En cuanto a las reclamaciones ordinarias, las planteadas con mayor frecuencia por los ciudadanos en 2021 correspondieron a servicios de internet (16%), videovigilancia (12%), recepción de publicidad (excepto spam) (11%), e inserción indebida en ficheros de morosidad (9%). Y en procedimientos sancionadores, se finalizaron 585, un 49% más que en 2021. Las áreas más frecuentes en estos procedimientos son videovigilancia (25%), servicios de internet (22%), y publicidad a través de correo-e o teléfono móvil (9%).



Brechas de datos

En cuanto a las notificaciones de brechas de datos personales realizadas ante la Agencia, estas son inicialmente recibidas por la División de Innovación Tecnológica (DIT), que realiza un primer análisis. La DIT recibió y analizó 1.647 notificaciones en 2021, de las que poco más del 4% (76) se remitieron a la Subdirección de Inspección por requerir de una investigación en profundidad. Las brechas de datos personales

más frecuentes son las causadas por ciberincidentes de origen externo/malintencionado y, dentro de este tipo de incidentes, el ransomware es el más repetido. En paralelo, siguen en aumento los casos en los que el cifrado de los datos y/o los sistemas van precedidos de una filtración de información y su puesta a la venta en internet y darkweb.

En lo relativo a las cifras de Delegados de Protección de Datos (DPD) notificados ante la Agencia, 2021 se cerró con 82.249 DPD, frente a los 65.040 de 2020, más de un 26%. De la cifra del año pasado, 74.033 corresponden al sector privado y 8.396 al sector público. La Agencia también ha recordado el hito que ha supuesto la puesta en marcha del 'Pacto Digital para la Protección de las Personas', una iniciativa que ya cuenta con casi 400 entidades adheridas.

Por otro lado, la AEPD y el Ministerio de Consumo han presentado una campaña en redes sociales para difundir entre la ciudadanía qué pasos deben seguir si sufren una suplantación de identidad en estos servicios. En España, más de 27 millones de personas poseen perfil en redes sociales, según el último Estudio de redes sociales de IAB, en el que incluyen datos como su nombre, fotografías y otro tipo de información personal.

Además, la AEPD participará en la primera acción coordinada de autoridades europeas de protección de datos para analizar el uso de servicios en la nube por parte del sector público, dentro del marco de actuaciones coordinadas del Comité Eu-



ropeo de Protección de Datos (EDPB, por sus siglas en inglés). El objetivo es obtener una visión integral que permita identificar y fomentar las mejores prácticas, detectar posibles deficiencias y realizar recomendaciones en la contratación y el uso de servicios en la nube. Esta iniciativa busca así conocer y, en

su caso, contribuir a elevar el nivel de cumplimiento y la protección de los datos personales de los ciudadanos, no sólo a nivel nacional sino, también, en el conjunto de la UE. Las 22 autoridades participantes analizarán más de 80 organismos e instituciones públicas europeas de un amplio abanico de sectores como la salud, las finanzas, la educación, las compras centralizadas o los proveedores de servicios informáticos. La AEPD analizará las prácticas de 12 de ellos correspondientes al sector público español y publicará sus conclusiones antes de final de año.

Evaluaciones de impacto

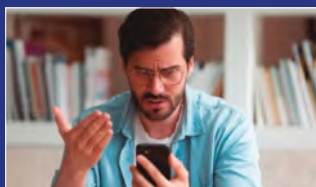
Además, la AEPD dio a conocer una lista de verificación para ayudar a los responsables del tratamiento a identificar y determinar de una forma rápida si el proceso y la documentación que están siguiendo para llevar a cabo una Evaluación de Impacto en la Protección de Datos (EIPD) contiene los elementos exigibles. La lista permite realizar una comprobación rápida de que se han tenido en cuenta todos los aspectos necesarios al realizar y documentar una evaluación de impacto (EIPD).

La biometría, garante de la seguridad del usuario frente a ataques con técnicas de SIM Swapping

El SIM Swapping es un tipo de fraude en el que se obtiene un duplicado de una tarjeta SIM asociada a una línea de teléfono sin el consentimiento de su titular y teniendo como fin suplantar la identidad del mismo y acceder a información confidencial (aplicaciones bancarias, correos-e, redes sociales...). Recientemente, se han impuesto 5,8 millones en multas a varias operadoras de telecomunicaciones por duplicados fraudulentos de tarjetas SIM al considerar la Agencia Española de Protección de Datos (AEPD) que sus políticas de seguridad son insuficientes para evitar duplicados fraudulentos. Y, en EE.UU., el FBI ha alertado que este tipo de ataques se ha multipli-

cado por cinco en los últimos tres años.

Frente a ello, la compañía Veridas, una empresa SaaS que ofrece soluciones para verificar la



identidad real de las personas en el espacio digital y físico, ha destacado que "se podrían hacer más esfuerzos por parte de las empre-

sas para evitar este fraude, ya sea implementando el doble factor de autenticación (2FA), usando algo que tienes, que sabes o que eres y complementándolo con factores biométricos (voz o cara), incapaces de ser suplantados, lo que los hace altamente seguros".

Freno a la autenticación facial en EE.UU. por los riesgos de privacidad que plantea

La agencia gubernamental IRS (Internal Revenue Service) anunció en febrero que no usaría tecnología biométrica de reconocimiento para facilitar la autenticación de los usuarios con la Administración.

Una decisión que se produjo después de la presión del Congreso para limitar el uso de esta tecnología por los problemas para



la privacidad que supone. Así, IRS anunció que dejará de usar servicios de verificación de identidad de terceros que usan reconocimiento facial, un cambio de rumbo importante ya que había anunciado su intención de emplear 'video selfies' para que los contribuyentes accedieran a su IRS.gov a finales de este año.

Proteja su futuro digital

WALLIX PAM4ALL*

¡Recupere el control de sus accesos!

El teletrabajo y los nuevos usos digitales han provocado que el número de accesos a las infraestructuras de las empresas haya crecido exponencialmente. Con WALLIX PAM4ALL, solución de gestión unificada de privilegios, podrá gestionar los accesos de forma granular al definir rigurosamente los objetivos, usos y duraciones, minimizando los riesgos asociados a las conexiones y los privilegios. PAM4ALL reduce su superficie de ataque sin afectar a la productividad y en conformidad con la normativa.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED

*PAM4ALL : Privileged Access Management / Gestión del Acceso Privilegiado para todos

MAPFRE obtiene la certificación PCI DSS en todos sus centros de datos

Mapfre ha ampliado a sus Centros de Procesamiento de Datos (CPD), de Alcalá de Henares, la certificación PCI DSS, que acredita que cumple con todas las medidas de seguridad requeridas por el 'Payment Card Industry Security Standards Council', que regula internacionalmente las condiciones en que las tarjetas de crédito deben custodiarse por las entidades que las admiten como medio de pago.

El uso de tarjetas de crédito por particulares, tanto en formato físico como digital, está cada vez más extendido. Esto hace que sean objeto de interés por parte de los ciberdelincuentes, por lo que las empresas emisoras de estas tarjetas son más exigentes con

los requisitos que imponen a las compañías que, como Mapfre, posibilita el uso de estas tarjetas para la adquisición de productos. Así pues, es relevante el hecho de que Mapfre haya logrado ampliar



Vanessa Escrivá (Mapfre) (izquierda), y Guillermo Llorente (Mapfre), recogen el certificado de manos de Daniel Fernández (Internet Security Auditors).

la certificación PCI DSS a sus dos CPDs de Alcalá de Henares (Madrid), acreditando que cumplen con las medidas de seguridad necesarias para garantizar el cumplimiento de los requisitos del PCI SSC. El certificado fue llevado a cabo por el equipo auditor de la compañía española Internet Security Auditors.

NOTARIADO logra el ENS nivel Alto, gestionado por ANCERT

Los sistemas de información del Notariado han obtenido la certificación del Esquema Nacional de Seguridad (ENS), de nivel alto, gestionado por



Ancert, la Agencia Notarial de Certificación y el centro tecnológico del Consejo General del Notariado.

Esta certificación reconoce la seguridad de todos los sistemas de información, procesos, bases de datos, sedes, plataformas y portales del Notariado para el ejercicio de su función pública.

El sello ENS de nivel alto ha certificado, entre otros aspectos,

la circulación por canales seguros de más de 30 millones de copias electrónicas de documentos notariales al año. Sólo en 2020, la plataforma de servicios telemáticos del Notariado permitió el envío de ocho millones de copias electrónicas de documentos notariales a las Administraciones. De hecho, la sede aloja la segunda mayor base de datos de España.

El alcance del ENS incluye los dos centros de procesamiento de datos de Ancert, el entorno Signo de las notarías, el Portal Notarial del Ciudadano y todos los sistemas de información que dan soporte a los servicios del Índice Único Informatizado, la prevención del blanqueo de capitales, la tramitación telemática con la Administración Pública y servicios con entidades financieras.

Desde la cibertrinchera

¿Y tú de quién eres?

Respiración agitada, pupilas dilatadas y cansancio hasta la médula. Agazapados en nuestra cibertrinchera evitando el fuego cruzado, con una mano en el corazón y otra en el teclado, con mil ojos y pestañas en lo que acontece, pero con la cabeza gacha refugiado en el calor de una pantalla. ¿Qué está sucediendo? ¿Cómo diantres hemos llegado hasta aquí? y lo más importante, ¿cómo salimos de está?

Apenas ya recuerdas tu vida de hace meses. Un buen donut y cafeína, y tus incidentes de rutina. Amenazas con nombres de animales o códigos indescifrables, ¿hoy tocan los pandas tuertos o los osos amorosos? Rusos, chinos o norcoreanos... poco importa la verdad, dale a la ruleta de los playbooks compañero: más vulnerabilidades que cerrar, 'forensicadores' a currar, máquinas que replanchar, e indicadores que rastrear. Viviendo la "vida loca" de la ciberseguridad, entre phishing, brechas y los famosos "ramonwares". ¿Una pandemia mundial? ¡Sin problema amigo! Somos los mismos guerreros con distinta capa, ahora con batín y zapatillas de Homer, luchando sin horario, esperando las provisiones y gadgets del próximo pedido.

Sin embargo, para esto no estabas preparado. La ciberguerra te sonaba a cuento "ruso", carne de películas de domingo tarde y series de streaming nocturnas. Reconoces que la geopolítica te pilló un poco lejos, casi desde los cuadernos de secundaria,

Llega el momento de la ciberdefensa, ahora sí hay un claro adversario, un arrogante y potencial destructivo enemigo. Sea por ciber-patriotismo, hacktivismo devoto o supervivencia empresarial, no hay vuelta atrás, nada será igual.

un poco de Wikipedia y listo para ser un experto. Ahora llega el momento de la ciberdefensa, ahora sí hay un claro adversario, un arrogante y potencial destructivo enemigo. Sea por ciber-patriotismo, hacktivismo devoto o supervivencia

empresarial, no hay vuelta atrás, nada será igual. ¿Con quiénes trabajas? ¿Qué software utilizas? ¿Dónde te conectas? Se instala la paranoia, la desconfianza extrema, se levantan nuevos muros que jamás imaginabas. Miras a los ojos, red social o chat más cercano, esperando que tu interlocutor tome partido, ¿rojo o azul? Nunca esos colores tan "ciber" habían cobrado tanto sentido. Gobiernos, grupos criminales, empresas... todos toman posiciones, no hay lugar a ambigüedades, no es momento de cobardes. El que antes era compañero, compartiendo penas y confidencias, es ahora tu enemigo y deja al descubierto vuestras vergüenzas, ¿verdad amigo Conti? El que antes era tu socio comercial, reputado y respetado, se encuentra enjaulado y estrangulado por sanciones y expuesto al escrutinio constante. Aunque también otros muchos buitres y gañanes de Internet aprovecharán la coyuntura para abusar de un lado y del otro, con el dinero como única bandera. Hacktivista con motivaciones legítimas, por favor también reflexiona, no todo vale y quizás esa empresa que se pone entre ceja y ceja no es tan oscura como pintas.

Tras pestañear volvemos a aterrizar de nuevo en nuestra cibertrinchera. Con la resaca de una gran pandemia, ahora vivimos una "nueva normalidad", un mundo interconectado en plena desconexión física y virtual. Un escalado que nos asienta en un estado de alerta constante, esperando lo peor, que ahora no solo es posible sino incluso probable. Acopio de provisiones, interconexión de banda ancha y nervios de acero. No hay que mirar atrás, sino adelante. Racionalizar esta nueva etapa, dejar pasar la tormenta, soñando que el mundo recobre la cordura y volvamos a dar pasos adelante. Mientras tanto seguiremos mirando al lado y preguntando, ¿y tú de quién eres?

Deseo que estas líneas nos encuentren a todos no más allá de una tensa espera, y los malos augurios se desvanescan volviendo a una senda racional. Seas Ruso, Ucraniano, Griego o Romano... no importa de dónde vienes sino quién eres. Nuestro más sincero y fuerte abrazo para aquellas personas que creen en un mundo global y trabajan por y para la defensa de las víctimas.

REFERENCIAS

- <https://github.com/curated-intel/Ukraine-Cyber-Operations>
- <https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/>
- <https://cyberknow.medium.com/update-10-2022-russia-ukraine-war-cyber-group-tracker-march-20-d667afd5aff>

CARLOS FRAGOSO

carlos@fragoso.eu



Descubre nuestro valor



Potenciamos tu negocio con las mejores soluciones IT



www.westconcomstor.com



Considera la ciberprotección uno de sus tres grandes ejes estratégicos

La AGENCIA ESPACIAL EUROPEA contará con su primer Centro de Operaciones (C-SOC) para 2024

La **Agencia Espacial Europea** (ESA) está poniendo en marcha un nuevo centro de seguridad cibernética que protegerá todos los sistemas de la Agencia contra interferencias externas, desde su infraestructura terrestre hasta los satélites en órbita. "Garantizar la 'ciberresiliencia' de nuestros sistemas espaciales y terrestres es parte de los deberes diarios de la ESA", destacó el organismo que, también, avanzó que el Centro estará operativo en 2024 y proporcionará "capacidad de gestión y monitorización".

Para ponerlo en marcha, ha firmado un contrato de 'fase 2' con un consorcio de 19 empresas europeas de Italia, Bélgica, Francia, Alemania, Reino Unido, Estonia y Rumanía. Liderado por la italiana **Leonardo**, el consorcio diseñará, implementará, construirá, validará y operará el C-SOC bajo la responsabilidad técnica de la Oficina de Seguridad de la ESA. El establecimiento del C-SOC está en línea con la 'Agenda 2025' del Director General de la ESA, **Josef Aschbacher**, que enfati-

za la importancia de proteger los activos espaciales europeos para que los ciudadanos puedan confiar en los sistemas y servicios que necesitan. Operando sobre una base de arquitectura distribuida, el C-SOC podrá dar cobertura



de seguridad robusta y redundante a toda la infraestructura de la ESA, monitorizando y administrando sus vulnerabilidades las 24 horas del día y los 365 días del año, mejorando también la protección para los Estados miembros de la ESA y sus socios.

Además, el C-SOC tendrá nodos e interconexiones distribuidas en todos los sitios principales de la Agencia mientras que, para permitir una cobertura generalizada en todo el territorio europeo, las estaciones móviles (platafor-

mas operativas ciberportátiles) se implementarán según sea necesario, en principio, extendiendo la protección a los socios involucrados en las misiones de la ESA. El centro forma parte del esfuerzo por mejorar su ciberseguridad de la Agencia que también cuenta con el Centro de Excelencia de Seguridad.

Cumbre Espacial 2022

Por otro lado, la ESA celebró su cumbre anual en Toulouse (Francia), en la que identificó tres líneas de acción estratégicas para abordar desafíos, desde la crisis provocada por el cambio climático y sus consecuencias a las amenazas para la infraestructura europea crucial en el espacio y en la Tierra. Precisamente, la ciberseguridad cobró un especial protagonismo dentro de esta apuesta de futuro por cuanto los aceleradores de la ESA complementan la iniciativa de 'Conectividad Segura' de la UE en la que también se incluye una propuesta sobre la gestión del tráfico espacial.

CHARTER OF TRUST y DIGITAL TRUST FORUM se fusionan para impulsar una mayor protección en las pymes

El **Charter of Trust** (CoT) o Carta de Confianza y el **Digital Trust Forum** (DTF) o Foro de la Confianza Digital van a unir sus fuerzas y fusionarse bajo el marco del 'Charter of Trust' para formar una iniciativa conjunta que impulse una mayor ciberseguridad y confianza digital. Con este paso, el 'Charter of Trust' también pretende dedicar más atención a la inteligencia artificial confiable en el futuro. El 'Charter of Trust' fue lanzado en la Conferencia de Seguridad de Múnich en febrero de 2018 por **Siemens** y ocho socios del sector industrial.

El DTF, por otro lado, se constituyó en Berlín en mayo de 2019 como una iniciativa de **Bosch**. Con ello, Bosch se unirá al CoT. La empresa de logística, **Deutsche Post DHL Group**, también ha decidido unirse a la iniciativa, con lo que el número de miembros del 'Charter of Trust' asciende a 17 cuatro años después de su firma.

Digital Trust Forum



Además, el CoT ha creado el **Foro de Socios Asociados**, al que se han unido instituciones como la **Oficina Federal de Seguridad de la Información** (BSI) de Alemania, el **Centro Criptológico Nacional** (CCN), la **Universidad de Graz** y el **Instituto Hasso Plattner for Digital Engineering GmbH** (HPI). El **Centro Canadiense de Ciberseguridad**, **Cyber Readiness Institute**, **CyberNB**, **Cyber Peace Institute**, **Global Cyber Alliance** y el **Ministerio de Economía, Comercio e Industria** (METI) y el **Ministerio de Asuntos Internos y Comunicación** (MIC) de Japón también se han sumado recientemente como socios.

Además de Siemens y la Conferencia de Seguridad de Múnich, componen el CoT actualmente: **AES**, **Airbus**, **Allianz**, **Atos**, **Bosch**, **Dell Technologies**, **Deutsche Post DHL Group**, **IBM**, **Infineon AG**, **Mitsubishi Heavy Industries**, **NTT**, **NXP Semiconductors**, **SGS**, **TotalEnergies** y **TÜV SÜD**.

Nace 'NONPROFIT CYBER' con el apoyo de 22 organizaciones de ciberseguridad para colaborar y mejorar la protección corporativa

Un numeroso grupo de entidades especializadas, sin ánimo de lucro, entre las que están desde el **Center for Internet Security** hasta la **Cloud Security Alliance**, **Cyber Threat Alliance**, **Cyber Peace Institute**, **Global Cyber Alliance**, **MITRE's Engenuity Center for Threat Informed Defense**, **SAFE Code** y el **Consumer Reports**, entre otras, han dado un paso adelante para formar una coalición que combinará y alineará su investigación, herramientas y recursos colectivos para ayudar a proteger a las empresas vulnerables de los ciberataques.

El enfoque inicial de 'Nonprofit Cyber' será

impulsar la conciencia de ciberseguridad y dar mayor visibilidad al trabajo que desarrollan sus integrantes, así como aprovechar sinergias.

En definitiva, la organización busca "proporcionar una vía de comunicación unificada al público sobre algunas de las mejores prácticas o recursos de ciberseguridad disponibles. Es parte de un esfuerzo más amplio para eliminar la exageración del marketing y FUD (o "Miedo a la incertidumbre y la duda"). De momento, no hay ninguna entidad española de este perfil que se haya sumado a ella —aunque sí hay organizaciones nacionales que están presentes en algunos de sus miembros fundadores—.



Seguridad Avanzada WatchGuard for SOC

En busca de lo desconocido con Threat Hunting



Servicios de
Threat Hunting



Detección, investigación
y respuesta



Ciber
Resiliencia

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



SEGURIDAD
ENDPOINT AVANZADA



AUTENTICACIÓN
MULTIFACTOR



NUBE SEGURA
WI-FI



SEGURIDAD
DE RED

Smart Security, Simply Done.

Contacto: 900 840 407

Email: strategic.accounts@watchguard.com

www.watchguard.com

Afirman que "mantenerse un paso por delante de los atacantes tiene un coste insostenible", según un estudio de Accenture

Los CISO piden más alineación con el negocio y aún consideran la protección de la nube "compleja"

Accenture ha presentado la nueva edición de su informe 'Estado de la ciberresiliencia 2021', con la opinión de 4.700 ejecutivos de países de todo el mundo, entre ellos España, en el que destaca que más de la mitad (55%) de las grandes empresas no están deteniendo eficazmente los ciberataques, detectando y solucionando los fallos rápidamente o reduciendo su impacto. El estudio también revela que el 81% cree que "adelantarse a los atacantes es una batalla constante y el coste es insostenible", un aumento notable respecto al 69% que tenía esa creencia en 2020. En cuanto al gasto en ciberseguridad, el 82% de los encuestados, tanto a nivel global como en España, afirmó haberlo incrementado en el último año.

El documento destaca, asimismo, la necesidad de extender los esfuerzos de ciberseguridad más allá de los propios límites de la empresa, a todo su ecosistema, señalando que los ataques indirectos —es decir, aquellos que se producen a través de la cadena de suministro— siguen creciendo. Por ejemplo, a pesar de que dos tercios (67%) de las organizaciones creen que su

CUATRO NIVELES DE CIBERRESILIENCIA



ecosistema es seguro, los ataques indirectos representan el 61% de todos los sufridos el año pasado, frente al 44% del año anterior.

En cuanto a la migración a la nube del sistema de protección, el 38% de la muestra española asegura que este entorno todavía no forma parte de la discusión en torno a la seguridad, seis puntos por encima del resultado arrojado en la encuesta global (32%). Entre los principales motivos que impiden la adopción de la nube, alrededor de un tercio destaca un gobierno y unas normativas deficientes,

asimismo, los encuestados subrayaron que la seguridad en la nube es demasiado compleja y que no tienen, a nivel interno, las habilidades para estructurar un marco adecuado de protección en este entorno.

También, es notable que el 85% de los CISO consultados están de acuerdo o muy de acuerdo con que la estrategia de ciberseguridad está desarrollada teniendo en cuenta objetivos empresariales, como el crecimiento o la cuota de mercado.

Ciberamenazas

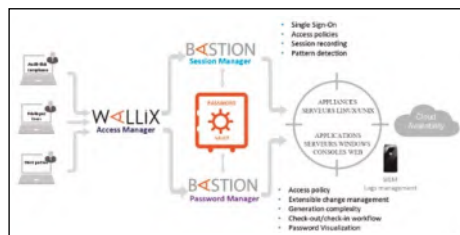
El informe destaca, además, que en 2021 se vivió una media de 270 ataques por compañía a lo largo del año, lo que supone un aumento del 31% respecto al año anterior. Si se observan los resultados de la muestra efectuada en España, el incremento de los ciberataques fue de un 260%, respecto a 2020.

Por último, el estudio recomienda, para mejorar la ciberprotección corporativa, dar a los CISO un puesto en la 'mesa de decisiones' de la compañía, así como integrar la seguridad dentro de las prioridades empresariales.

WALLIX refuerza su inversión en innovación para seguir creciendo con su visión de 'PAM para todos'

Wallix ha dado a conocer su nueva estrategia para este año marcada por su apuesta por el I+D de producto y su apertura en nuevos mercados, como en España, para continuar con su crecimiento. Así, también ha destacado su visión estratégica 'PAM para todos' con el objetivo de posicionarla como un actor principal en la constitución de un mundo digital de confianza. En este sentido, "el actual contexto de transformación digital y el auge de los

En cuanto a sus cifras de negocio, dentro de su plan estratégico para el periodo 2022-2025, ha destacado una inversión orgánica de 10 millones de euros, destinados tanto a reforzar su innovación en producto como a la expansión de actividades de marketing y ventas. Con ello, este plan de desarrollo, denominado 'Unicorn 25', prevé alcanzar una facturación de 100 millones de euros en tres años, con un margen operativo superior al 15%, manteniendo una media de crecimiento del 30% anual a lo largo de todo el plan. La estrategia corporativa actual de la compañía parte de unas bases implementadas por su anterior plan de crecimiento 'Ambition 21': una oferta PAM referente en el



nuevos usos digitales ofrecen a Wallix una perspectiva de crecimiento seguro en un mercado en evolución, en el que se prevé que el Application Performance Management (APM) duplique su tamaño de aquí a 2025", destacan desde la compañía.

mercado, una fuerte base de clientes y una amplia huella geográfica de actuación. Con ello, la compañía se ganó la confianza de cerca de 600 nuevos clientes a nivel global y generó un volumen de negocio de 23,2 millones de euros en 2021, facturando un 15% más.

La IA ayudará a combatir el ransomware y los agujeros de seguridad de la nube en 2022

En 2021, el ransomware fue un tema candente en la industria después de una serie de incidentes de alto perfil que involucraron a organizaciones como el **Servicio Público de Empleo Estatal (SEPE)** y la **Sanidad del Principado de Asturias**, que fueron víctimas. En este contexto, el responsable para España y Portugal de **Vectra AI**, **Ricardo Hernández**, destacó cuatro áreas de la ciberprotección que evolucionarán en 2022: la se-



guridad en la nube, que se verá sometida a una presión creciente; la proactividad para minimizar los ataques de ransomware; la creciente demanda por parte las organizaciones de servicios de detección y respuesta gestionados y de automatización; y el incremento de la IA para

contrarrestar el uso malicioso de la MFA.

"Dado que 2022 planteará su propio conjunto de obstáculos relacionados con la seguridad, es fundamental que las organizaciones se adelanten a los acontecimientos para garantizar la mejor protección posible contra las posibles amenazas. Para lograrlo, las organizaciones deben tratar de implementar una estrategia de detección y respuesta. Para ello, suelen emplear combinaciones de IA y aprendizaje automático (ML) para buscar cruces entre actividades autorizadas pero sospechosas, y el tipo de comportamientos que un adversario mostrará como parte de un ataque en desarrollo. Si las empresas asumen que han sido comprometidas y buscan activamente las señales, estarán en una posición mucho más fuerte para detectar todo tipo de ataques a tiempo y detenerlos antes de que se conviertan en brechas de seguridad", subrayó.

Identifica las brechas de seguridad en minutos

con la Validación Continua de Seguridad

01

Simula

Simula ataques a través de cualquier vector

02

Evalúa

Conoce tus puntos de exposición

03

Remedia

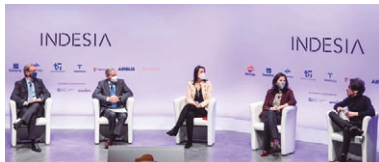
Soluciona tus problemas de seguridad



Más información:



El I FORO INDESIA analiza el impacto de la IA y la iniciativa ODISEIA presenta su primera 'Guía ética' española



La inteligencia artificial (IA) es una de las mejores oportunidades para el crecimiento de la economía española. Solamente su aplicación tendrá un impacto estimado en el PIB español de 16.500 millones de euros en 2025, según han avanzado los expertos que se reunieron en el 'I Foro Indesia: el impacto de la Inteligencia Artificial en la industria'. El encuentro fue organizado por Indesia, asociación para la aplicación de la inteligencia artificial en la industria, integrada por Repsol, Gestamp, Navantia, Técnicas Reunidas, Telefónica, Microsoft, Airbus y Ferrovial y que cuenta con el apoyo del Basque Artificial Intelligence Center (BAIC) y Accenture.

En él, los principales directivos de las entidades asociadas compartieron sus reflexiones sobre el papel de la IA en el impulso económico, la mejora de la competitividad y el futuro de la industria española y europea. Así, destacaron la posición privilegiada con la que cuenta España para avanzar en ella, al tener ya disponible una infraestructura sólida y sofisticada para la conexión de banda ancha, fibra y 5G. Algo que permite que el impulso de la inteligencia artificial se lleve a cabo en mejores condiciones que en otros países de la UE.

Además, en febrero, Odisia –el Observatorio Del Impacto Social y Ético de la Inteligencia Artificial–, en colaboración con PwC, Google, Microsoft, IBM y Telefónica presentaron la primera 'Guía de buenas prácticas para el uso de la Inteligencia Artificial ética' elaborada en España. El documento ha sido realizado por un equipo multidisciplinar de más de 30 de profesionales integrado por tecnólogos, juristas y expertos en distintos campos, y recoge un

detallado informe y un análisis jurídico de los principios éticos que aplican a la IA, a partir del estudio de 27 iniciativas en todo el mundo.



GOOGLE: SOBERANÍA DIGITAL

La soberanía digital no es un concepto sencillo de fijar porque escapa a una definición estándar que pudiera implementarse fácilmente con requisitos operativos o de ingeniería. Cada Estado, cada segmento de mercado, cada industria lo describe de diferentes maneras y, a menudo, manifiestan expectativas que exceden los requisitos meramente legales o regulatorios.

Para determinados clientes la expectativa de soberanía reside fundamentalmente en asegurar que el proceso de sus datos, o de sus clientes/usuarios/ciudadanos, se desarrolla dentro de un área geográfica determinada. Otros, en respuesta mayormente a alguna regulación sectorial, esperan disponer además de una mayor precisión en la localización exacta de los datos. Algunos otros entienden la Soberanía como una garantía de inmunidad a leyes extranjeras que pudieran demandar acceso a sus datos, mientras que para otro tipo de clientes resulta más importante que las operaciones administrativas y de soporte sobre sus datos, sean realizadas por personal ubicado dentro de su área geográfica.

Para no pocos clientes la expectativa de soberanía se asocia más al cumplimiento de requerimientos de seguridad nacionales o regionales altamente prescriptivos, como es el caso de C5 en Alemania, SecnumCloud en Francia o ENS en España, mientras que, en el caso más demandante, normalmente asociado a la seguridad nacional o a la protección de infraestructuras críticas, la expectativa de soberanía se asocia a una autonomía total y autosuficiencia en un estado de desconexión absoluta.

En definitiva, no existe una única expectativa y parece que la soberanía se puede concebir de maneras diferentes, por lo que debemos entender y responder a todas y cada una de ellas porque cada escenario tendrá unas consecuencias diferentes sobre la ingeniería, las operaciones y el ámbito legal.

Google Cloud

Su aproximación a los escenarios soberanos anteriormente descritos es considerada muy

innovadora. La arquitectura abierta de la propia plataforma permite no tener que sacrificar capacidades de la nube pública en detrimento de la opción soberana. Los clientes utilizarán las cargas de trabajo que deseen, con el nivel de control deseado, sin perder por ello los beneficios transformadores de la nube pública.

Desarrollamos estas capacidades a través de un conjunto de controles de soberanía de datos que los clientes pueden implementar directamente o en colaboración con socios locales sobre los que se delegan las operaciones de aquellos controles de soberanía más sensibles o estratégicos.

Esto es posible hacerlo por la forma en que la infraestructura de Google Cloud está construida, y más específicamente en cómo funciona el mecanismo de cifrado de GCP (Servicio de administración de claves en la nube). La arquitectura de cifrado nos permite delegar controles a socios confiables de una manera única. De esta forma las cargas de trabajo permanecen conectadas a la estructura de la nube mientras los socios locales las segregan y controlan completamente.

En este sentido, Google Cloud construye la Soberanía digital en tres niveles, en función de los controles sobre los datos e infraestructura que decidamos otorgar al proveedor. Además de los controles administrados por el proveedor, es decir, aquellos controles de acceso a los datos que son administrados por el cliente, pero que el proveedor hace cumplir, tendremos estos niveles de soberanía:

- **Soberanía de datos:** los clientes tienen mecanismos para ejercer un control independiente sobre el acceso del proveedor a los datos descifrados.

- **Soberanía operativa:** los clientes pueden controlar la capacidad del proveedor para acceder a la infraestructura de software y hardware para proporcionar gestión operativa.

- **Soberanía del software:** los clientes obtienen independencia de los proveedores para que no tengan que depender de una relación continua con ninguna empresa extranjera para ejecutar las cargas de trabajo.

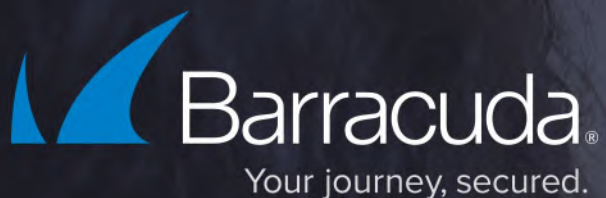
Así, a través de la soberanía del software, las organizaciones alcanzan autonomía completa en un estado de desconexión del proveedor de nube o software. Se garantiza, entonces, su autonomía tecnológica ante cualquier escenario geopolítico complejo.



HÉCTOR SÁNCHEZ MONTENEGRO
National Technology Officer para España

JAVIER MARTÍNEZ
Sales Engineer Manager

GOOGLE CLOUD



El 91 % de los ciberataques comienzan con un correo electrónico.

Bloquee el phishing, el ransomware y otras innumerables amenazas de correo electrónico con **Barracuda Email Protection.**

Más información:
iberia_team@barracuda.com | barracuda.com

SANTANDER y FACTUM lanzan Cyber Guardian, una plataforma innovadora para ayudar a proteger a las pymes

Santander ha puesto en marcha **Cyber Guardian**, una innovadora solución para que las pymes puedan defenderse de las amenazas del mundo digital y fortalecer la protección de su negocio, con la misma capacidad que tienen ya las grandes corporaciones. Cyber Guardian, creada en colaboración con **Factum**, empresa participada por el banco a través de Tresmares, permite a las pymes proteger su negocio de las ciberamenazas, con soluciones punteras y servicios innovadores.

El servicio Cyber Guardian les ofrece a las pymes la capacidad de evaluar su riesgo de ciberseguridad; proteger sus dispositivos, *emails* y navegación, así como formar a sus empleados, entrenándolos con pruebas de *phishing* y mensajes de concienciación, para convertirlos así en la primera barrera de defensa. Esta solución incorpora, además, monitorización proactiva de alertas de seguridad 24/7 y permite responder a las amenazas más avanzadas y emergentes. Todo ello, sin necesidad de conocimientos previos y de forma fácil e intuitiva.

Otra innovadora función que incorpora es la herramienta de puntuación de Ciberseguridad. Con ella, los usuarios mantienen un seguimiento continuo del nivel de su negocio y pueden gestionar sus riesgos. Además, el servicio de monitorización permanente y automático evalúa la gravedad de los riesgos.

Al mismo tiempo, la herramienta ofrece protección para todos los dispositivos de la compañía, ya que monitoriza, detecta y elimina virus, *ransomware*, caballos de Troya y *spyware*, conocidos o no. Asimismo, ayuda a detectar

eventuales fallos de seguridad en las webs de la pyme.

La solución del Santander y Factum también ayuda a las empresas en una tarea fundamental: la concienciación de los trabajadores de la importancia de la ciberseguridad. Así, por ejemplo, permite el envío de simulaciones de *phishing* a los empleados, para que aprendan a reconocer los correos maliciosos y sepan cómo actuar frente a ellos, a través de una formación específica.

Las pymes que contraten el servicio se beneficiarán de un descuento permanente del 50% ofrecido por Santander, con un precio final de 125 euros por año y dispositivo. Cyber Guardian, además, puede ser financiado el primer año con los fondos europeos NextGenEU, dentro de la categoría Ciberseguridad en el ámbito del Kit Digital, un programa impulsado por el Gobierno a través del Ministerio de Asuntos Económicos y Transformación Digital. Empresas entre 11 y 49 empleados pueden solicitar a un importe máximo de 6.000 euros, para categorías de

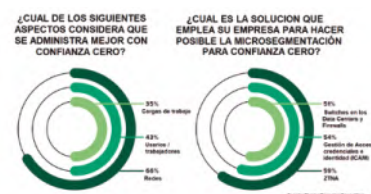
ciberseguridad como Cyber Guardian. Las pymes que obtengan el bono digital pueden tener la herramienta a coste cero durante el primer año.

Cyber Guardian se puede contratar a través de todos los canales del banco, desde la oficina a la APP Santander o la web, así como en la web de Factum. Además, el banco, a través de su plataforma de asesoramiento a las pymes para obtener los fondos europeos, ofrece ayuda para la tramitación de la petición del bono digital de forma gratuita, agilizando así los trámites para recibir esta subvención.



Confianza Cero: aún inmaduro, pero crucial para proteger la nube y la transformación

Forrester Consulting, junto a **Illumio**, publicó en febrero un informe sobre el estado de adopción del enfoque de Confianza Cero en 2022, preguntando a más de 330 profesionales de ciberseguridad de EE.UU., EMEA y Asia-Pacífico. Entre otros aspectos de interés, el 75% destacó su utilidad para combatir las crecientes ciberamenazas, aunque también mostró que aún queda mucho por hacer. Sirva como ejemplo que más del 60% reconoció no estar preparado para el rápido ritmo que exigen las empresas para su evolución digital, migrando muchos de



sus sistemas e información a la nube, y con la popularización de los entornos híbridos de trabajo.

Además, un 52% subrayó que los programas de Confianza Cero presentan beneficios organizacionales claros, ya que permiten una mayor agilidad que otros enfoques (52%), migraciones más seguras a la nube (50%) y ofrecen un alto grado de protección a la transformación digital (48%).

De hecho, el 78% resaltó que sus empresas esperan invertir más medios en Zero Trust este año para abordar las brechas de seguridad emergentes, aunque su estado de adopción aún está en sus primeras etapas. Eso sí, solo el 36% de las organizaciones ha comenzado a implementar soluciones de Confianza Cero y, de esa cifra, sólo un 6% ha desarrollado totalmente un proyecto de este tipo.

En este sentido, un 73% destacó que aspectos como la microsegmentación son uno de los pilares que sustentan Zero Trust, así como apostar por una arquitectura de red de confianza cero (ZTNA). Sin embargo, "las tasas de adopción de estos dos conceptos aún están rezagadas", recuerda el informe. Asimismo, explica que entre los grandes problemas para implementar este enfoque está la falta de experiencia de la fuerza laboral y la incapacidad para identificar el 'piloto de microsegmentación' de confianza cero correcto.

EY, TANIUM y la EMBAJADA DE EE.UU. abordan la ciberamenaza global y ponen foco en la visibilidad, el control y la protección

EY, Tanium y la **Embajada de Estados Unidos** celebraron en **Madrid** el pasado 10 de marzo un acto centrado en "Los retos para operar la tecnología de forma segura en el actual contexto de transformación digital", durante el cual se abordó la problemática actual en el ámbito de la visibilidad, control y protección de los activos e información corporativos y cómo la solución ofrecida en el marco de la alianza de EY y Tanium está en disposición de cambiar las reglas del juego.

Tras la bienvenida y apertura del evento por parte de la Emba-



jada, se expuso la visión del Gobierno de EE.UU. sobre el actual panorama de ciberamenaza global, dando paso a continuación a la firma, que expuso de la mano de su socio de Consultoría Tecnológica y Ciberseguridad, **Jordi Juan**, el enfoque de EY para la

gestión y protección de los activos e información corporativos, en la cual la tecnología de Tanium juega un papel crucial, hecho cuyo director de cuentas estratégicas para España, **Alvaro Exteverry**, corroboró pormenorizando las capacidades de visibilidad y control de la plataforma para parcheo eficiente de sistemas en tanto factor crítico para la seguridad digital de los negocios.



Unificar la seguridad de la identidad

Proteja a las personas, las aplicaciones y los datos esenciales para su negocio

Si la seguridad de TI es su responsabilidad, aprenda cómo puede implementar un modelo de Zero Trust para reducir vulnerabilidades de las violaciones de datos, las amenazas internas y externas, y cerrar las brechas de exposición a la ciberseguridad.

Nuestras soluciones PAM, IGA, Access Management y AD le permiten consolidar en un solo proveedor de seguridad todas las ramas de la identidad, simplificar la administración del acceso de los usuarios y brindar una seguridad eficiente a su empresa desde el perímetro de la identidad.

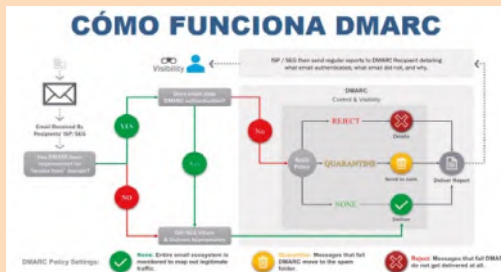
www.oneidentity.com

A pesar de su eficacia, una década después de publicarse, este protocolo de autenticación aún no se ha popularizado, según Proofpoint

Las instituciones públicas españolas no protegen adecuadamente a los usuarios contra el fraude por correo-e a través de la implementación de DMARC

A finales de enero de 2012 se publicaron las primeras especificaciones de DMARC (*Domain-based Message Authentication, Reporting and Conformance*), un protocolo de autenticación de correo-e de código abierto que ha resultado muy eficaz frente al *phishing* o suplantación de correos-e. A pesar de ello, una década después de darse a conocer su empleo como parte de las estrategias de seguridad de administraciones públicas y empresas, todavía no está tan generalizado como debiera.

Así lo destaca **Proofpoint** que, con motivo de su décimo aniversario, realizó un interesante análisis para examinar el uso del protocolo por parte de las principales administraciones públicas españolas. En concreto, se centró en las páginas web de los ministerios y la Presidencia del Gobierno, así como



en los portales de Internet de las 17 comunidades autónomas y los principales organismos gubernamentales. Entre sus conclusiones más relevantes destaca que el 83% de los sitios web de los Ministerios y de la Presidencia no tienen implantada ninguna política de DMARC, lo que significa que no están tomando ninguna medida para proteger proactivamente a los ciudadanos contra los riesgos del fraude por correo electrónico.

Además, sólo cuatro (17%) de los 23 dominios analizados a nivel estatal han implementado el nivel

recomendado y más estricto de protección DMARC (*reject*), que realmente bloquea los correos-e fraudulentos para que no lleguen a sus destinatarios, lo que significa que el 83% está dejando a los usuarios expuestos al fraude a través de este canal.

En cuanto a las comunidades autónomas, sólo 10 de las 17 (59%) han publicado registros DMARC, lo que significa que el 41% no protege proactivamente a los ciudadanos de este riesgo. Sólo tres (18%) han implementado el grado más alto de protección.

Amenazas internas

La compañía también dio a conocer los resultados de su 'Estudio Global de Ciberseguridad', realizado junto con **Ponemon Institute**, en el que destaca que las amenazas in-

ternas cuestan a las organizaciones 13,4 millones de euros anuales, un 34% más que en 2020. Además, se recuerda que el 56% de los incidentes se deben a la negligencia de personal interno, mientras que los robos de credenciales casi se han duplicado y son los más que más cuesta remediar, con una media de casi 700.000 euros por incidente. También es llamativo que, según la encuesta, el número total de incidentes haya aumentado un 44% en solo dos años.

El número de incidentes por empresa también ha subido, ya que el 67% de las empresas experimentaron entre 21 y más de 40 incidentes al año, frente al 60% en 2020. Los robos de credenciales casi se han duplicado desde el último estudio. Además, se calcula que un 62% de las organizaciones españolas sufrieron al menos una infección de *ransomware*, y cuatro de cada 10 (39%) optaron por pagar, al menos, el rescate.

THYCOTICCENTRIFY cambia su denominación a DELINEA

Delinea se estrenó en enero como proveedor de referencia de soluciones de gestión de acceso privilegiado (PAM). Con el respaldo de **TPG Capital**, Delinea se formó en abril de 2021 tras la fusión de dos compañías ya consolidadas en el área de PAM, **Thycotic** y **Centrify**.

Así, la firma acaba de lanzar una nueva identidad de marca, en la que destaca por su importante progreso como compañía fusionada y su compromiso de ofrecer soluciones integrales preparadas para la nube, que sitúan los accesos privilegiados en el centro de las estrategias de ciberseguridad.

"En Delinea, creemos que lo opuesto a lo complejo no es ser simple, sino ser adecuado. Nuestra misión es ofrecer una seguridad invisible para el usuario y, al mismo tiempo, proporcionar a los equipos de TI la seguridad y el control que necesitan", destacó **Art Gilliland**, su Director Ejecutivo. "Con Delinea, definimos los límites del acceso de forma clara y fácil con el objetivo de ayudar a las empresas a reducir el riesgo, garantizar el cumplimiento y optimizar la seguridad. Ofrecemos un acceso privilegiado sin excesos", añadió.

El escaso compromiso de TI y de los directivos pone en riesgo las inversiones en ciberprotección

Trend Micro ha publicado un estudio en el que destaca que el bajo compromiso persistente de los responsables de TI y de los directivos puede poner en peligro las inversiones y exponer a las organizaciones a las ciberamenazas. De hecho, más del 90% de los responsables de la toma de decisiones empresariales y de TI encuestados expresaron su especial preocupación por los ataques de *ransomware*. Curiosamente, a pesar de esta preocupación, poco más de la mitad de los equipos de TI (57%) debaten sobre los ciberriesgos con los directivos, al menos, una vez a la semana.

Afortunadamente, la inversión actual en iniciativas cibernéticas no es baja. Algo menos de la mitad (42%) de los encuestados afirmó que su organización es la que más gasta en reducir la posibilidad 'ciberataques' para mitigar el riesgo empresarial. Esta fue la respuesta más popular, por encima de proyectos más típicos como la trans-

formación digital (36%) y la transformación de la plantilla (27%). Alrededor de la mitad (49%) afirmó haber aumentado las inversiones para mitigar los riesgos del *ransomware*.

"Sin embargo, el escaso compromiso de los directivos, combinado con el aumento de la inversión, sugiere una tendencia a 'tirar el dinero' en lugar de desarrollar una labor de comprensión de los desafíos de la ciberseguridad e invertir adecuadamente", destaca el informe.

Acuerdo en Cataluña

Por otro lado, **Trend Micro** se ha unido a **Cercle Tecnològic**, organización sin ánimo de lucro para el

fomento de las TI en Cataluña, con el fin de fortalecer y estrechar las relaciones con *partners* y empresas del sector, además de su utilización como vehículo en la divulgación de sus conocimientos y tecnología para hacer más seguro el intercambio de información digital.



No sea la próxima víctima de un ciberataque

Tome medidas contra las amenazas con un equipo de expertos en respuesta



Con Sophos MTR, su empresa cuenta con el respaldo de un equipo de expertos que ofrece un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas las 24 horas.

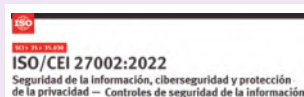
www.sophos.com/es-es

© Copyright 2022, Sophos Ltd. All rights reserved. Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK. Sophos is the registered trademark of Sophos Ltd.

SOPHOS
Cybersecurity delivered.

Publicada la nueva ISO 27002:2022 que actualiza su estándar de controles de seguridad

En febrero, se publicó la nueva ISO 27002 que simplifica la implementación de la normativa pasando de 114 controles a 93, a pesar de que hay más, ya que se ha procedido a su agrupación en cuatro dominios -Controles Organizacionales, Relativos al Personal, Físico y Tecnológicos-, por 14 secciones de su predecesora. De cualquier forma, es de interés que ahora se incluyen 11 controles nuevos relativos a gestión en la nube (como también refleja el borrador del Esquema Nacional



de Seguridad) y controles para mitigar las amenazas actuales. Además, se incluyen dos nuevos elementos: uno sobre el uso de atributos asociados a cada control, incluidos en el marco NIST, y otro sobre por qué es necesario aplicar cada control.

La adaptación de las empresas que ya estén certificadas en la

ISO 27001 no requerirán un gran esfuerzo, en principio, ya que se limitará sólo al cumplimiento de 11 controles nuevos y a la reorganización de los que ya se tienen para adaptarlos a la norma, así como alineándolos en la declaración de aplicabilidad (SOA), y actualizando las políticas y procedimientos con dichas referencias. Asimismo, está previsto un periodo de transición, durante el que la entidad certificadora no exigirá los cambios, aunque sí podrá confirmar que la empresa está en proceso de abordar esa novedad.

En definitiva, “para las empresas que estén actualmente en proceso de implementación de la certificación ISO 27001 o estén pensando en certificarse cuanto antes, aunque todavía no se conoce la fecha de publicación de la nueva ISO 27001, y, por tanto, se certificarán con la estructura de la actual ISO 27001, se puede dejar preparado y mapeado los cambios y agrupaciones que van a sufrir los controles”, destacaron desde Aenor.

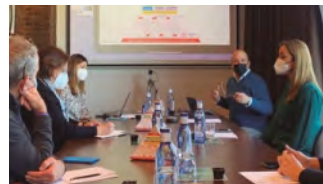
El CCI continúa sus esfuerzos por facilitar la labor de los responsables de ciberseguridad industrial con nuevas guías y dos plataformas

El Centro de Ciberseguridad Industrial (CCI) ha presentado dos prácticas guías para facilitar el trabajo de los profesionales del sector. Una destacando los tres mayores desafíos de estos profesionales en un proyecto y otra con los retos que encaran los proveedores en este tipo de trabajos. En ambas, destaca el problema de evaluar las ofertas de proveedores y seleccionar el adecuado, aunque todos tengan que cumplir la IEC-62443. En este sentido, desde la asociación recomiendan apostar por soluciones que sean ágiles de desplegar, con la adecuada funcionalidad y calidad de soporte, entre otros aspectos. Además, indica que la importancia de “la gestión de actualizaciones y el modelo de confianza cero: no son un camino opcional por recorrer, son del que debemos intentar no desviarnos”.

Por otro parte, con la colaboración de profesionales de organizaciones industriales y proveedores

del ecosistema CCI presentó en febrero de forma oficial (SIC 148 ya se hizo eco de ello) dos plataformas. Por un lado, RECIN que facilita el diseño de arquitecturas seguras en los proyectos industriales y la incorporación de requisitos de ciberseguridad en infraestructuras críticas industriales según el estándar IEC-62443-3-3. Por otro, la de ‘Catálogo Activo’, que ofrece buscar qué proveedores tienen capacidades de ciberseguridad para cumplir con los requisitos de los principales estándares, permitiendo filtrar por múltiples condiciones.

Asimismo, Freddy Macho, Presidente del Centro de Investigación de Ciberseguridad IoT – IIoT, y José Valiente, Director del CCI, firmaron un convenio para desarrollar iniciativas comunes de actividades de divulgación y formación en ciberseguridad industrial y en entornos del Internet de las Cosas (IoT) e Internet de las Cosas Industrial (IIoT).



ESPAÑA, uno de los países más afectados por los robos de credenciales

El robo de información sigue siendo una de las motivaciones principales de los cibercriminales, y España es uno de los países más afectados por esa actividad delictiva, según el último informe de amenazas de la compañía Eset. Entre las catalogadas dentro de esta categoría destacan los incidentes relacionados con robo de credenciales, principalmente, porque permiten preparar y realizar ataques más dirigidos y mucho más graves. De hecho, la investigación considera que “el robo de credenciales en empresas y organizaciones españolas sigue a unos niveles preocupantes”. “Además, se produce una monopolización por parte de dos familias de spyware, como son Agent Tesla y Formbook, copando más del 60% de las de-



tecciones de info-stealers (caballos de Troya) en España”, destacó Josep Albers, Director de Investigación y Concienciación de

la compañía.

En este sentido, recordó que “independientemente de la técnica que utilicen, los delincuentes han ido perfeccionando sus estrategias para obtener mejores resultados”. Prueba de ello, es que en una reciente campaña analizada “pudimos comprobar cómo, en unas pocas horas, los delincuentes obtuvieron cientos de registros”.

Eset, además, se ha asociado con Intel para mejorar la seguridad de los endpoints a través de la detección de ransomware. La colaboración busca aprovechar la GPU para la seguridad y cribar este tipo de amenazas en la telemetría de la capa de silicio.

TANIUM abre oficina en España para ofrecer su plataforma de defensa contra el ransomware, cumplimiento normativo y análisis de riesgos

Tanium, proveedor de gestión de puntos finales convergentes (XEM), ha puesto en marcha su centro de operaciones en España desde el que proporcionará a empresas y organizaciones visibilidad y control de todos los servidores, estaciones de

ofrecerá las capacidades de nivel ‘Enterprise’ de la plataforma, sin la necesidad de contar con nuevas infraestructuras físicas de TI, proporcionando soluciones sencillas, cost-effective y muy fáciles de desplegar y de gestionar.



trabajo, máquinas virtuales, dispositivos de red, contenedores y flujos de trabajo, para aumentar la resiliencia y disminuir el riesgo.

A medida que crezcan las operaciones, Tanium trabajará estrechamente con su red de partners para establecer un ecosistema fiable de productos, servicios y soporte. Su programa de MSP ofrecerá las soluciones de su plataforma tanto a compañías de gran tamaño, como a medianas empresas. Asimismo,

“Las empresas y organizaciones españolas quieren mejorar su higiene cibernética en áreas como la aplicación de parches, el cumplimiento normativo o la monitorización de datos sensibles, entre otros. Sin embargo, ninguna de estas disciplinas se puede gestionar eficazmente, si no se tiene total visibilidad y control de todos los endpoints”, ha destacado su Country Manager en España, Álvaro Etcheverry. Desde un panel único, la plataforma de Tanium proporciona a las organizaciones una fuente compartida de certeza y visibilidad de la situación.

CyberRes



ArcSight

Operación de la Seguridad

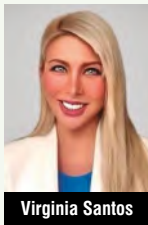
Obtenga una detección más rápida y precisa de amenazas conocidas y desconocidas con un SOC resiliente, basado en el análisis adaptativo de la seguridad que de manera inteligente, resuelve la escasez de talento disponible en el mercado.

CyberRes es una línea de negocio de Micro Focus. Con uno de los portafolios de seguridad más grandes del mundo, ayudamos a nuestros clientes a navegar en el cambiante panorama de amenazas del mundo actual, creando resiliencia empresarial y cibernética dentro de sus equipos y organizaciones. Estamos aquí para ayudar a las empresas a acelerar la confianza, la fiabilidad y la supervivencia en tiempos de adversidad, crisis y volatilidad empresarial.

cyberres.com

IMMERSIVE LABS desembarca en España con su innovadora plataforma de preparación cibernética

Fundada en 2017 en Gran Bretaña por **James Hadley**, actual CEO, **Immersive Labs** se ha convertido en una de las empresas tecnológicas con más crecimiento a nivel europeo. Ahora, la pujante compañía llega a España de la mano de **Virginia Santos** como Directora de Ventas y **Jorge Ortiz** como Ingeniero de Preventa.



Virginia Santos

Immersive Labs cuenta con una solución de referencia en el mercado: la primera plataforma de preparación cibernética destinada a profesionales técnicos y no técnicos, ofreciendo contenido basado en desafíos 'gamificados' desarrollados por expertos en ciberseguridad y con la tecnología de inteligencia de amenazas más

reciente del sector. Utilizando un enfoque totalmente diferencial, permitiendo a las organizaciones ponerse a prueba en entornos totalmente reales y demostrar la preparación de sus usuarios a la hora de enfrentarse a ciberamenazas emergentes,



Immersive Labs permite demostrar no sólo la capacidad en ciberseguridad sino, además, el nivel de riesgo y de resiliencia de la organización y de todos los usuarios que la componen, aportando métricas y una visión mucho más estratégica.

Sectores sensibles, como Transporte e Infraestructuras Críticas, los más afectados por la falta de agilidad para identificar y bloquear amenazas

Como es sabido, los atacantes, generalmente, tardan días o semanas en explotar nuevas vulnerabilidades, pero a los equipos de ciberseguridad les lleva una media de tres meses (96 días) en identificar y bloquear las ciberamenazas más recientes, según el informe 'Cyber Workforce Benchmark Report 2022', de **Immersive Labs**.



Mitre ATT&CK, prioridad formativa

El documento también destaca las técnicas de ataque que más priorizan las organizaciones en su formación. La gran mayoría se centra en el marco Mitre ATT&CK.

"Esto lleva a pensar que las empresas tratan de

prevenir los ataques, concentrándose en 'cómo puedo evitar ser comprometido', más que en saber 'cómo reaccionar si ya he sido atacado', explican sus responsables.

Cabe reseñar, además, que los equipos de seguridad de aplicaciones (AppSec) son capaces de desarrollar habilidades en menos tiempo que los equipos de ciberseguridad. Según el informe, el 78% de las habilidades de protección de aplicaciones se desarrollaron más rápido de lo esperado, en comparación con el 11% de los equipos de ciberseguridad.

La investigación también señala que, cuando los ciberataques aparecen en los medios de comunicación, los expertos en ciberseguridad aprenden lo necesario para lidiar con ellos con más agilidad. Así, las cinco habilidades desarrolladas más rápido, completadas en tan solo cinco días, incluyen módulos que cubren la conocida vulnerabilidad Log4j y el *exploit*

Log4Shell, así como el *exploit* InstallerFile-TakeOver para Windows. El *ransomware*, por su parte, es la amenaza que genera la mayor incertidumbre para los equipos de respuesta dificultando, en gran medida, la decisión que hay que tomar, aunque finalmente un 83% de las empresas del estudio se decantó por no pagar el rescate.

TIEMPO DEDICADO A APRENDER A IDENTIFICAR Y RESPONDER A LAS AMENAZAS MÁS RECIENTES

Sector	Media días
• Ocio/Entretenimiento	65
• eCommerce y Retail	68
• Medios y Publicidad	69
• Gobierno	88
• Tecnología	92
• Servicios financieros	97
• Educación	100
• Fabricación	108
• Salud	116
• Consultoría	118
• Infraestructura crítica	128
• Transporte	145

Fuente: Cyber Workforce Benchmark Report 2022, Immersive Labs.



LA CONFIANZA COMIENZA DESDE **CERO**

Acelere su traslado a la nube con
la plataforma Zscaler Zero Trust Exchange.

Más información en [zscaler.com](https://www.zscaler.com)



©2021 Zscaler, Inc. All rights reserved. Zscaler and Zero Trust Exchange are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

España, segundo país del mundo, por víctimas de 'caballos de Troya bancarios', según Kaspersky

Tres de cada cinco empresas ya utilizan dispositivos IoT, pero menos de la mitad los protegen de forma adecuada

Dos de cada cinco (43%) empresas no protegen sus infraestructuras IoT de forma completa, según revela el informe 'Superar los límites: Cómo abordar las demandas específicas de ciberseguridad y proteger el IoT', realizado por **Kaspersky**. La investigación pone de manifiesto que los riesgos de ciberseguridad y las filtraciones de datos son la principal barrera para la implementación de proyectos IoT para muchas empresas. El informe adelanta que, a pesar de que se espera que el número mundial de dispositivos IoT conectados crezca un 9%, hasta alcanzar los 27.000 millones de conexiones en 2025, no se está invirtiendo con la misma fuerza en su seguridad. Sirva como ejemplo que, en los últimos tres años, casi el 20% de las organizaciones ya han observado ciberataques en los dispositivos IoT de su red, según **Gartner**.

En este sentido, el documento destaca que, "aunque dos tercios de las organizaciones (64%) en todo el mundo utilizan soluciones

de IoT, el 43% no las protege completamente. Esto significa que para algunos de sus proyectos -que pueden ser desde una estación de carga de vehículos eléctricos, hasta equipos médicos conectados-, las empresas no utilizan ninguna herramienta de protección". Los motivos pueden deberse a la gran diversidad de dispositivos y sistemas IoT, que no siempre son compatibles con las soluciones de seguridad. Casi la mitad (46%) de las empresas encuestadas a nivel global temen que los productos de ciberseguridad puedan afectar al rendimiento del IoT o pueda ser demasiado difícil encontrar una solución adecuada

(40%). Por otra parte, los riesgos de ciberseguridad son considerados la principal barrera para la implementación de IoT por más de la mitad de las organizaciones (57%).

Amenazas móviles

La compañía también ha publicado su análisis anual sobre las amenazas móviles en el que ha destacado que el número de ataques a los usuarios en todo el mundo ha disminuido, con 46 millones en 2021, frente a los 63 millones en 2020. Sin embargo, sus analistas destacan su preocupación por que "el nuevo *malware*

para móviles se ha vuelto cada vez más complejo, con nuevas formas de robar las credenciales bancarias y de juegos de los usuarios, así como otro tipo de datos personales". Durante el año pasado, Kaspersky detectó más de 95.000 nuevos 'caballos de Troya' bancarios para *smartphones*, siendo España el segundo país, por detrás de Japón, con mayor porcentaje de usuarios atacados, sobre todo, por *software* malicioso bancario.

Proyecto CONSENT

Por otro lado, la compañía ha anunciado su participación en el 'Proyecto CONSENT' para concienciar a jóvenes, padres, profesores e instituciones sobre el impacto negativo de la pornografía, para prevenir todas las formas de violencia de género, con especial atención a la violencia sexual, así como frenar los efectos que causa la sexualización prematura y la hipersexualización entre niños y los más jóvenes.



INGENIA, el movimiento estratégico del GRUPO BABEL para afianzar su posición en el mercado

Como ya informara SIC de la operación, en julio de 2021, **Babel** integró el **Grupo Ingenia**, especializado en ciberseguridad, soluciones digitales y servicios eLearning, dentro de su estrategia de crecimiento inorgánico. Este proceso de integración finalizó con éxito



en enero, incorporando un equipo de 400 profesionales muy especializados y competencias tecnológicas complementarias a las ya existentes en la compañía. De entre esos servicios, y dada la creciente demanda, Babel ha decidido poner foco sobre su nuevo *expertise* en ciberseguridad, y mantener la marca Ingenia. Eso sí, sale al mercado con una nueva identidad y logo. Su propuesta cubre un amplio abanico de áreas que permiten salvaguardar la seguridad de la información: cumplimiento

y gestión de riesgos, despliegue de tecnologías de protección, seguridad gestionada y desarrollo seguro.

Además, en el ámbito de la seguridad gestionada destaca su Centro de Operaciones de Seguridad, eSOC, repartido entre España y Chile, y en expansión a Portugal, Marruecos y México. Este centro es miembro de **First** y **CSIRT.es**.

Alrededor del eSOC se dan servicios de *Blue Team*, *Red Team*, respuesta a incidentes, *threat hunting*, ciberseguridad industrial y ciberinteligencia. Además, Ingenia tiene una herramienta propia para la gestión de GRC, ePULPO, muy extendida entre los organismos públicos nacionales. Todos los servicios de ciberseguridad de la marca cuentan con las certificaciones ISO27000, ISO20000 y ENS de nivel Alto.

EVOLUTIO continúa con su expansión en Iberia con un nuevo centro de trabajo en LINARES

Evolutio, empresa de integración de servicios *cloud*, inauguró oficialmente en febrero su



nuevo centro de trabajo en Linares (Jaén). Se espera que genere 150 puestos cualificados en los próximos dos años, fomentando el talento local y su permanencia en Jaén, apostando por nuevos acuerdos e itinerarios de formación con centros educativos locales y administraciones públicas. La compañía tecnológica, con sede en Madrid, ya inició en 2021 la contratación de los primeros alumnos formados en centros educativos linarenses en áreas tecnológicas de gran demanda, incorporándolos al nuevo centro dentro de su plan de

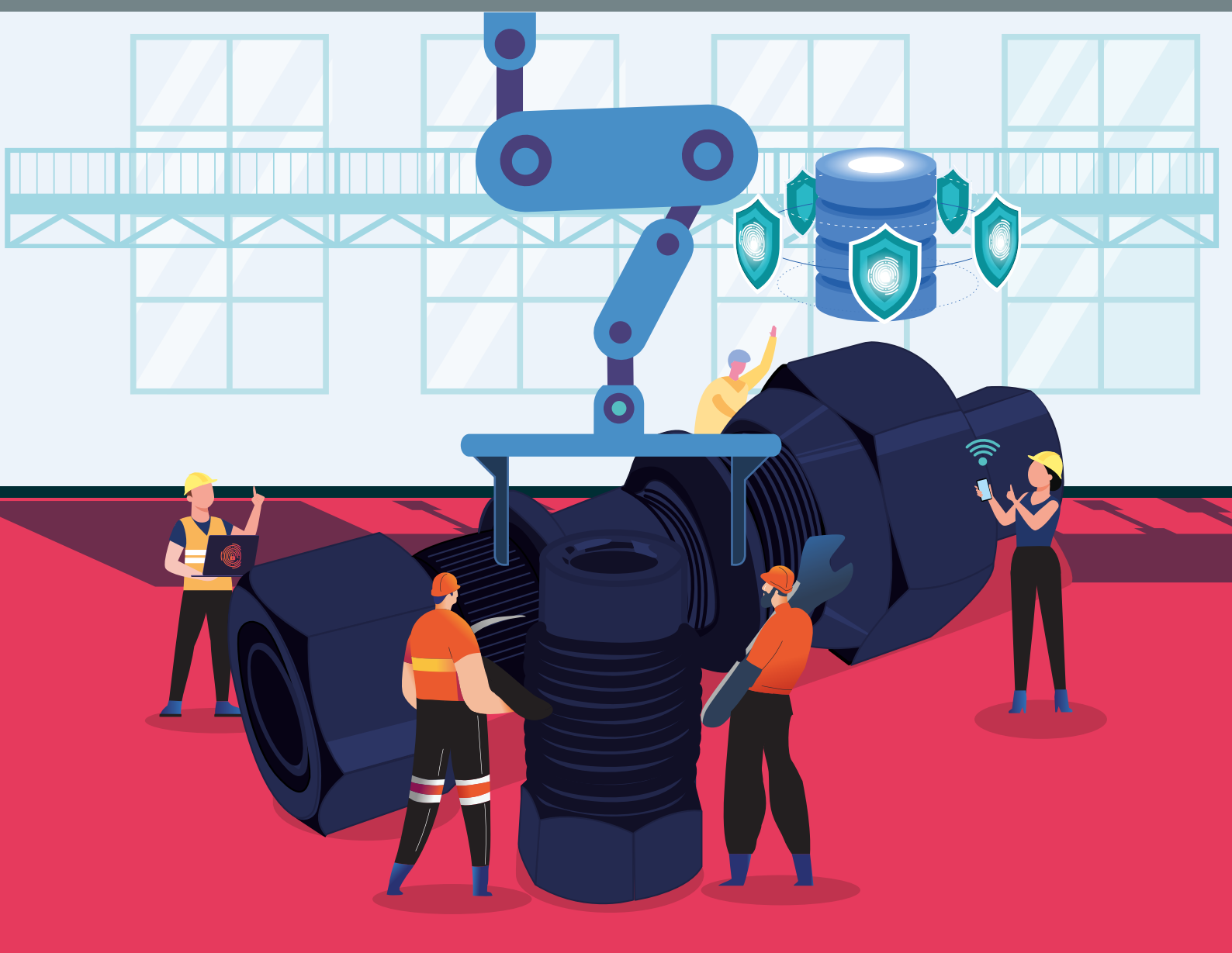
acuerdos para fomentar el talento local y su permanencia en Jaén mediante empleo estable en la compañía.

Entre los nuevos puestos de trabajo que reforzarán el servicio prestado a los clientes de Evolutio en ciberseguridad, entornos *cloud*, experiencia de usuario y *contact center*, se encuentran técnicos de administración y soporte de redes, técnicos de seguridad perimetral y desarrolladores de software e IT.

De forma paralela, **MA Seguros**, la mutua de los profesionales sanitarios, ha confiado en Evolutio la actualización de sus sistemas y procesos para impulsar la modernización de su modelo de negocio.

En un sistema industrial, cada pieza es clave.

PRIMER LABORATORIO ESPAÑOL
acreditado para evaluar la ciberseguridad
de componentes industriales con el esquema
IEC 62443 4 -1 / IEC 62443 4 -2



Laboratorio acreditado para
evaluaciones:



Se une a la Alianza LACChain, de *blockchain*, y a la iniciativa francesa Campus Cyber, para ser un referente en el país

TELEFÓNICA TECH amplía sus alianzas, con VU y ZSCALER, y establece un nuevo Consejo Asesor para potenciar su crecimiento orgánico

Telefónica Tech continua con su crecimiento a través de alianzas como la realizada con **Zscaler**, con la que anunció un acuerdo "para potenciar el servicio Security Edge", que consolida las funciones de seguridad SASE-SSE (*Security Service Edge*), ofrecidas desde la nube, con la gestión de la seguridad proporcionada desde sus SOC's globales. Además, firmó un acuerdo con **VU**, compañía experta en fraude digital y en la protección de identidad del usuario, por el cual, lanzan el servicio global Access & Authentication para proteger del robo o mal uso de las credenciales corporativas mediante mecanismos de Confianza Cero, con tecnología de múltiple factor de autenticación adaptativo y sistemas biométricos de reconocimiento facial y voz, entre otras capacidades.

Apuesta por *blockchain*

La compañía también se ha sumado a dos iniciativas. Por un lado, a la alianza global **LACChain**, para promover el desarrollo del ecosistema de la cadena de bloques en América Latina y Caribe. Integrada por diferentes actores del entorno *blockchain* y liderada por el Laboratorio de Innovación del **Grupo del Banco Interamericano de Desarrollo (BID Lab)**, con la incorporación de Telefónica Tech, la alianza suma 57 miembros. En ella,



actualmente, se están desarrollando 38 proyectos con impacto en inclusión, con 136 nodos y 81 entidades que ejecutan nodos en un histórico de más de 35 millones de bloques.

Además, la compañía se ha sumado, como parte de su proceso de internacionalización, a la iniciativa gala '**Campus Cyber**', para colaborar contra las nuevas ciberamenazas, y en el refuerzo de la estabilidad y la seguridad internacional del ciberespacio. Se trata de una iniciativa que forma parte de un plan de 1.000 millones de euros que el presidente francés, **Macron**, presentó en febrero de 2021, con el objetivo de reforzar la ciberseguridad del país de aquí a 2025. De la cuantía, 150 millones se destinarán a impulsar el ecosistema francés para favorecer una mejor colaboración entre las distintas empresas e ins-

tituciones, en particular, mediante la creación del Campus Cyber en el barrio de la Défense, en París. Con esta membresía, Telefónica Tech busca convertirse también en un actor de referencia en el país vecino.

Nuevo Consejo Asesor

De forma paralela, Telefónica Tech constituyó su Consejo Asesor, presidido por su CEO, **José Cerdán**, que ayudará a potenciar el crecimiento orgánico e inorgánico de la compañía y a impulsar el liderazgo de sus propuestas de valor para la transformación digital. Formado por profesionales de reconocido prestigio y experiencia en el mundo tecnológico entre sus integrantes están desde **Juan Ignacio Cirac**, Director en el **Instituto Max Planck** de Óptica Cuántica, hasta **Chema Alonso**, Chief Digital Officer de Telefónica; **María Jesús Almazor**, CEO de Ciberseguridad y Cloud de Telefónica Tech; y **Gonzalo Martín-Villa**, CEO de IoT y Big Data de T-Tech, entre otros. También, forman parte de él **Alejandro Romero**, fundador y CEO de **Alto Analytics** y ahora Chief Operations Officer de **Constella Intelligence**, e **Isabel Fernández**, doctora en Computación e IA y actualmente rectora de la **Universidad Alfonso X El Sabio**.



NETSKOPE amplía su nube privada de seguridad, crea un nuevo programa de canal y consigue el ENS de Nivel Alto

Netskope ha anunciado un importante hito en la expansión de su nube privada de seguridad



NewEdge, que ahora cuenta con centros de datos de cómputo completo en más de 50 regiones de todo el mundo. Todos, accesibles para sus clientes sin tasas ni recargos adicionales, con los servicios de Netskope Security Cloud, como cortafuegos en la nube, pasarela web segura, agente de seguridad de acceso a la nube, acceso a la red de confianza cero, etc.

La compañía, además, ha creado un nuevo programa de *partners* denominado **Evolve Partner Program**, en el que introduce tres niveles de socios (Autorizado, Oro y Platino) y más descuentos e incentivos, además de am-

pliar las vías de certificación técnica y lanzar una nueva especialización de servicios.

Asimismo, y para ofrecer un mejor servicio a sus *partners* en EMEA, ha ampliado su plantilla de canal en esta región.

ENS Alto

Por otra parte, como adelantó SIC, Netskope superó un proceso de rigurosa evaluación, por **Appius+**, para la consecución del Esquema Nacional de Seguridad (ENS) de Nivel Alto. Así, queda acreditada como proveedor externo de servicios tecnológicos a las Administraciones Públicas y está certificado respecto a las disposiciones del ENS.

JUAN ROIG vende a NUNSYS su participación en SOTHIS, reconocida por SIEMENS como Gold Partner en las categorías MOM y Cloud

Angels, el vehículo inversor del presidente de **Mercadona**, **Juan Roig**, ha cerrado la venta del grupo tecnológico **Sothis** a **Nunsys**, conformando una compañía de

1.400 empleados y una facturación esperada en 2022 de 140 millones de euros.

De forma paralela, **Siemens Digital Industries Software** ha otorgado a Sothis el estatus de Gold Partner, siendo la primera empresa española en lograr dicho reconocimiento como especialista en sistemas MOM. Los sistemas MOM se componen de un conjunto de soluciones tecnológicas que, integradas, dotan



Joaquín Guerra (Sothis) recoge el premio acompañado de Luis Beltrán director comercial de la misma unidad de negocio

a los usuarios de funcionalidades orientadas a la gestión de la información en el ámbito de los procesos de fabricación y producción industrial. En paralelo, la empresa también fue reconocida como

el mejor socio en EMEA en la implantación de soluciones de Digital Industries Software en la categoría MOM y Cloud de los premios Siemens TOP Partner EMEA 2021. Entre los clientes que ya confían en la compañía valenciana para la implantación de este tipo de soluciones se encuentran referentes, como **Mercadona**, **Heineken España**, **Acesur**, **Deoleo**, **Covap**, **Lactiber**, **Huevos Guillén**, **Porminho** o **Bardinet**.



Redefiniendo DLP

En el 85 % de las fugas interviene el factor humano*

Porque las organizaciones actuales necesitan un enfoque más moderno para la prevención de la pérdida de datos

**Proteger la información. Reducir el riesgo.
Sin compromiso**

Más información en proofpoint.com/es
o contacte con nosotros info-spain@proofpoint.com

proofpoint.

*2020 Data Breach Investigations Report

© 2021 Proofpoint, Inc. All rights reserved.

Su CEO, Gil Shwed, destacó la necesidad de repensar la ciberseguridad para hacer frente a los ataques de 'V Generación'

CHECK POINT anuncia su nueva estrategia de negocio en su evento CPX 360, presentando su cortafuegos más rápido

La multinacional israelí celebró, en febrero, su evento anual para clientes y socios, **CPX 360**, en el que presentó su nueva tecnología *Quantum Lightspeed* con la que, según la compañía, ofrece "el cortafuegos más rápido del mundo, con un rendimiento 20 veces superior a su competencia". Además, aprovechó para dar a conocer sus innovaciones previstas para 2022. Así, durante la jornada se destacó el nivel de sofisticación de las amenazas de nueva generación, que se han plasmado en ataques a la cadena de suministro y vulnerabilidades como la de Log4j, entre otras en las que el *ransomware* ha sido el claro protagonista. "Si miramos a 2021, fue uno de los años más desafiantes en términos de ciberataques", destacó el fundador y CEO de la compañía, **Gil Shwed**, quien aprovechó el evento para dar a conocer su nuevo eslogan, 'You Deserve the Best Security' (Te mereces la mejor seguridad) y su logotipo (referenciado en SIC 148), con los que se pretende marcar un nuevo impulso estratégico para animar a las organizaciones a que implementen soluciones integrales 'prevent first' (prevenir primero) capaces de hacer frente a la 'ciberpandemia'.



Arquitectura Check Point Infinity

Además, se resaltó que la arquitectura Check Point Infinity es la base de todo lo que hace la compañía. Proporciona una solución unificada para las amenazas, basada en tres pilares: Quantum, para asegurar la red; CloudGuard, para una completa seguridad en la nube; y Harmony, para asegurar a los usuarios y sus accesos.

Todo ello se basa en el software de gestión Infinity Vision y en ThreatCloud, que es el "cerebro" que conecta todos los elementos y permite la protección contra las amenazas en tiempo real y desde todos los vectores.

El Director de Gestión de Producto, **Itai Greenberg**, destacó las capacidades de las nuevas familias de productos para 2022 entre las que están desde los que encuadrados en la categoría Quantum, como los Quantum Lightspeed, "con un ren-



dimiento cinco veces superior al de la generación anterior de gateways", así como los que están dentro de CloudGuard, que han permitido que Check Point fuera "el único proveedor que ha dado protección preventiva contra la vulnerabilidad Log4j en diciembre de 2021", según la propia compañía. Además de los de acceso

para usuario final, en Harmony, con 'cinco soluciones en una' y facilitando la gestión de la ciberseguridad.

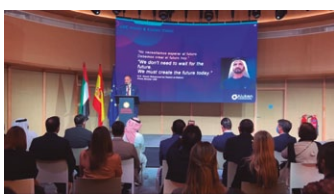
Buenos resultados

Check Point también aprovechó para dar a conocer su buena evolución, ya que en 2021 logró unos ingresos de 2.167 millones de dólares (1.976 millones de euros), que supone un incremento del 5% en comparación con el año anterior. Como curiosidad, para destacar la importancia de la rapidez, contó como invitado con el atleta **Usain Bolt**.

AIUKEN presenta en Expo 2020 Dubai su primera plataforma de ciberseguridad con IA para el 5G

La multinacional española, **Aiukén**, presentó en la Expo Dubai 2020, ante un auditorio que registró un lleno absoluto, su Plataforma de orquestación, automatización y respuesta frente a ciberamenazas, ASIP 5.0, que utiliza un avanzado motor de Inteligencia Artificial (IA), "el primero de su clase cien por cien español", según la compañía. El evento, que fue celebrado en el pabellón de España junto al **Spanish Business Council** de los Emiratos Árabes Unidos (UAE), buscó ofrecer un 'plus' de ciberprotección frente a amenazas en los entornos 5G.

Para ello, la nueva plataforma ASIP 5.0 realiza tareas de orquestación, automatización y respuesta 24x7 para proporcionar una defensa más completa frente a los ciberataques, especialmente a medida que avance



la implantación del 5G. Desde la compañía destacan que "ASIP 5.0 ha sido desarrollada para combinar la automatización total de la gestión de procesos y defensa ante amenazas gracias a su motor de IA que incorpora SOAR 2.0. Un modelo predictivo en tiempo real capaz de analizar más de un millón de amenazas por segundo y definir acciones automáticas frente a cualquier ciberataque". "Estamos orgullosos de haber desarrollado el primer motor de orquestación de ciberseguridad que utiliza 100% Inteligencia Artificial en España y Europa gracias al CDTI y a nuestros inversores", resaltó el CEO de la empresa, **Juan Miguel Velasco**, recordando que "iniciamos una nueva era tecnológica para la ciberprotección en el transformador mundial digital del 5G".

FACTUM, con el apoyo del BANCO SANTANDER, desarrolla un nuevo MDR y crea una división de identidad y firma-e

Tras la entrada del **Banco Santander** en su accionariado, **Factum** está potenciando el área de ciberseguridad, especialmente en el ámbito de los servicios gestionados donde ha crecido un 25% respecto al año anterior. Además, está poniendo en marcha diferentes iniciativas junto con la entidad bancaria, con soluciones como la puesta en marcha de un MDR (Managed Detection and Response) que estará operativo a lo largo de este año.

De igual modo, la organización está poniendo especial foco en soluciones de identidad y firma electrónica, con el despliegue de una división específica para desarrollar esta línea de negocio y que va a contar con personal especializado. En esta línea, la compañía está desplegando Factum Labs, un área de innovación donde se desarrollan soluciones propias dentro del área de ciberseguri-



dad. Asimismo, pretende fortalecer su propuesta de ciberseguridad tanto en Europa, como en Latinoamérica, y abre la puerta a importantes acuerdos con fabricantes de referencia globales.

Además, Factum ha reforzado su posición como *partner* estratégico, gracias a la renovación de acuerdos con socios como **Forrescout**, **CrowdStrike** y **Netskope**; así como la diversificación de proyectos hacia sectores, como el de la industria alimentaria, de la salud o de la moda.

En cuanto a la proyección del equipo humano, durante 2021 tuvo un crecimiento importante, alcanzando los 100 profesionales y prevé llegar a 130 personas en plantilla este año. Asimismo, la compañía anunció en 2021 un crecimiento de un 15% y la previsión de alcanzar una facturación de 17 millones a finales de 2022.

We turn
threat intelligence
into proactive
actions

Detecta, analiza y responde a las últimas ciberamenazas más rápido con nuestra plataforma Threat Compass. Su diseño modular único te permite utilizar la protección más adecuada para tu negocio e invertir sólo en las opciones de ciberinteligencia que necesitas.

Visita blueliv.com para obtener más detalles y empezar a tomar una aproximación más proactiva ante las ciberamenazas.

La ciberseguridad de S2 Grupo crepita en Fallas

Tras el forzado parón pandémico, la actividad de las populares Fallas por fin pudo recobrar todo su vigor en la pasada edición de marzo, en la cual —y como ya venía sucediendo en las dos ediciones precedentes—, la ciberseguridad tuvo su protagonismo merced a la compañía **S2 Grupo**, cuya sede central se ubica en la ciudad levantina.

Al amparo de la denominada *Falla Cibersegura* adscrita a su sede en Francisco de Llano, el monumento estuvo dedicado, como en ocasiones anteriores, a distintas dimensiones de la ciberprotección desde una óptica divulgadora, claramente enfocada a concienciar sobre ciberseguridad a la sociedad valenciana.

La compañía anfitriona, precisamente con un bagaje diferenciador en las tareas de concienciación, aludió en la falla de este año —denominada ‘Conectados’— a representar me-



25 millones de facturación

Por otro lado, los resultados de la compañía especializada en ciberseguridad y gestión de sistemas críticos, que co-dirigen sus socios fundadores **José Miguel Rosell** y **Miguel Juan**, registraron un crecimiento de su volumen de negocio del 27%, ascendiendo la facturación de su último ejercicio a 25 millones de euros, frente a los 19,5 logrados en 2020, siendo de resaltar que de dicha facturación 1,8 millones se encuadran en su actividad de I+D+i. Asimismo, la compañía valenciana cerró el pasado año con una plantilla de 459 especialistas, esto es, un 10% más que en el ejercicio previo.

Además, S2 Grupo ha firmado una alianza estratégica con **Euskaltel** para permitir que el operador amplíe sus servicios de ciberseguridad para clientes corporativos, convirtiendo a la firma valenciana en su operador principal para este tipo de proyectos.

tafóricamente los principales aspectos derivados de los riesgos de la actividad de internet, incluyendo alusiones a algunas de sus más conocidas herramientas. Su atinada plasmación en el monumento fue acreedora del 2º Premio de la Categoría Segunda.

NETSKOPE pone foco en proteger el dato sin degradación donde quiera que esté y abrirá en este semestre un centro de datos en Barcelona

El pasado 24 de marzo **Netskope** celebró su Summit Barcelona en donde comunicó al centenar de asistentes presenciales al acto, sus ascendentes resultados como compañía, tanto en España como específicamente en Cataluña. Su primer ejecutivo español, **Miguel Martos** y el homónimo para el área catalana, Andorra y Baleares, **David Maciá**, se congratularon de anunciar que Barcelona acogerá antes de que acabe este primer semestre de 2022 un centro de datos, el segundo en España de la multinacional tras el de Madrid, sumando así más de 60 en todo el mundo.

En esta edición se mostraron todas las novedades de Netskope y por qué la propuesta *Security Service*

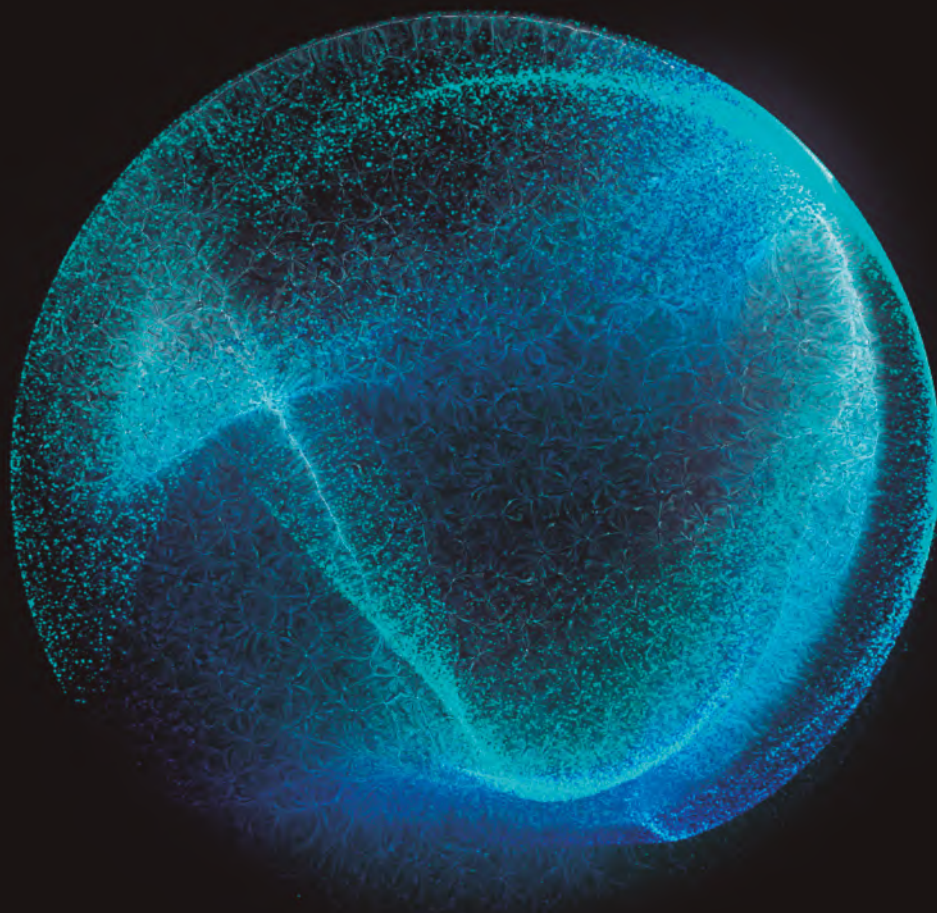
Edge (SSE) supone un punto de inflexión en la evolución de la seguridad de la nube, los datos y las redes, remarcándose el hecho de que el foco de Netskope estará centrado en proteger el dato sin degradación donde quiera que se encuentre o vaya.

La sesión se completó con aportaciones cla-

rificadoras de cómo la propuesta SSE protege al dato y las personas —impartida por **Yaroslav Rosomakho**, Field CTO—, y se mostró una ‘demo’ de alto impacto en la que se desvelaban las debilidades inherentes al ecosistema TI en su conexión con todos los variopintos escenarios de nube y de conexión con las mismas, a cargo del experto **Ignacio Franzoni**.

La sesión se completó con la visión ofrecida por la CIO de EMEA de Netskope, **Ilona Simpson**, quien enfatizó cómo la ciberseguridad inteligente facilita la agilidad del negocio y el CISO de **Puig**, **Oscar Sánchez**, ilustró, con alusiones metafóricas cinematográficas, cómo Netskope y sus tecnologías ayudan en los objetivos de ciberprotección de la multinacional.





ArrowSphere

La plataforma de gestión y servicios
en la nube líder del mercado.

Otorgó el premio 'Raúl Jover' a la labor del CCN y repartió 16.000 euros en *bug bounty*

Regresa ROOTEDCON batiendo récord de asistencia, con un público más profesional y abundantes novedades técnicas

El regreso presencial del congreso técnico de ciberseguridad más multitudinario de España, **RootedCON**, fue una de las buenas noticias que trajo marzo, mes que auguraba la progresiva remisión de lo peor de la pandemia. Durante tres días, con más de 3.100 asistentes, en su tradicional sede —el Kinépolis madrileño— más de 30 ponentes de alto nivel, incluidos representantes de Fuerzas y Cuerpos de Seguridad del Estado e instituciones públicas, impartieron conferencias en las que no faltaron un buen número de investigaciones inéditas, algunas muy polémicas y mediáticas, como la de 'Hacking Smart Meters' de **Jesús María Gómez**, de **Tarlogic**.

En ella, mostró una herramienta, **PLCTool**, que permite *hackear* infraestructuras eléctricas fruto del trabajo de la investigación de la compañía de servicios de ciberseguridad, que detectó un problema en los contadores inteligentes de electricidad, comunes en la mayoría de las infraestructuras, comunicándose de forma poco segura, por lo que son fácilmente manipulables. Desde **Tarlogic** se denunció que, en los dos años pasados desde que comenzase la investigación, se han puesto en contacto en numerosas ocasiones con las distribuidoras, los fabricantes de los contadores, diversas empresas implicadas, como la que se encarga de la gestión del protocolo Prime, y hasta con las instituciones. Sin embargo, hasta ahora los investigadores de la compañía gallega no son conocedores de que nadie esté liderando la resolución de este crucial problema.

También, despertaron interés otras ponencias relevantes, como la de **David Meléndez** sobre cómo usar los marcadores biométricos del ritmo cardíaco para autenticarse; las



nuevas técnicas de ataques desconocidas a través de contenedores de Docker, mostradas por **Carlos Polop**; o cómo se puede exfiltrar información a través dispositivos hardware como el desarrollado por **David Reguera**. Incluso, se dio a conocer cómo es posible inyectar *malware* en las gafas de realidad virtual Oculus. También, fueron notables la de **Pedro Cabrera** y **Miguel Gallego** sobre posibles ataques a redes 5G y la que impartió el Jefe del Departamento de Delitos Telemáticos de la **Guardia Civil**, **Juan Sotomayor**, con los pormenores sobre cómo se realizan investigaciones cibernéticas, basándose en una recientemente cerrada operación contra un robo de criptomonedas o la de **Chema Alonso** sobre la IA aplicada a la ciberseguridad.

Como colofón, **Alfonso Muñoz** —todo un clásico del evento—, analizó la privacidad y criptografía de la conocida red social **Telegram**. Y es que, “estas aplicaciones saben

Por su parte, **Pablo San Emeterio** presentó una serie de medidas de protección que se pueden añadir dentro de las aplicaciones de IM para impedir que personas ajenas puedan husmear en las conversaciones que tenemos. Concretamente, se trata de incluir una capa extra de cifrado gracias al uso de técnicas de introspección y de instrumentación dinámica. Estas técnicas permiten modificar el comportamiento de aplicaciones y SOs, en este caso, de la citada **Telegram**.

Esta edición contó, además, con una sala dedicada a ponencias elegidas por la asociación **ProtAAPP** y en la que se dieron a conocer desde el trabajo de la Comunidad de Madrid en la materia, por parte de **Esther Muñoz**, hasta cómo se aprovechan fallos de configuración en **Microsoft Azure** que pueden suponer problemas de seguridad, por parte de **Juan Garrido**.

Noche hacker

más de nosotros, por ejemplo, por con quién hablamos y a la hora que lo hacemos, que por lo que hablamos”. Durante su ponencia, se analizaron “los enormes problemas asociados con el conocimiento de metadatos de los usuarios por parte de **Telegram**”, recordó el experto que, a su vez, destacó que “la mayor parte de la información y ficheros intercambiados solo tiene cifrado cliente-servidor. Así que, esta red social conoce en claro la mayor parte de la información intercambiada”.

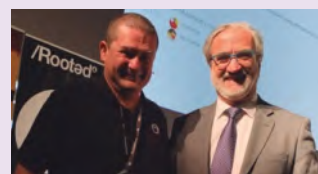
No faltó la ‘noche hacker’, en la que medio centenar de expertos en *bug bounty* consiguieron dar con numerosas vulnerabilidades reportadas que fueron recompensadas con 16.000 euros, alcanzando por su gravedad, una de ellas, los 3.000.

Reconocimiento al Centro Criptológico Nacional

Por otra parte, el congreso cedió espacio para visibilizar el proyecto **#Include** de la **Fundación Goodjob** y quiso reconocer la labor de un destacado agente en el ecosistema español —galardón que ya recibiera *Revisa SIC* en 2019—.

En esta ocasión, el premio ‘**Raúl Jover**’, cofundador del congreso fallecido en 2021, fue para el **Centro Criptológico Nacional**,

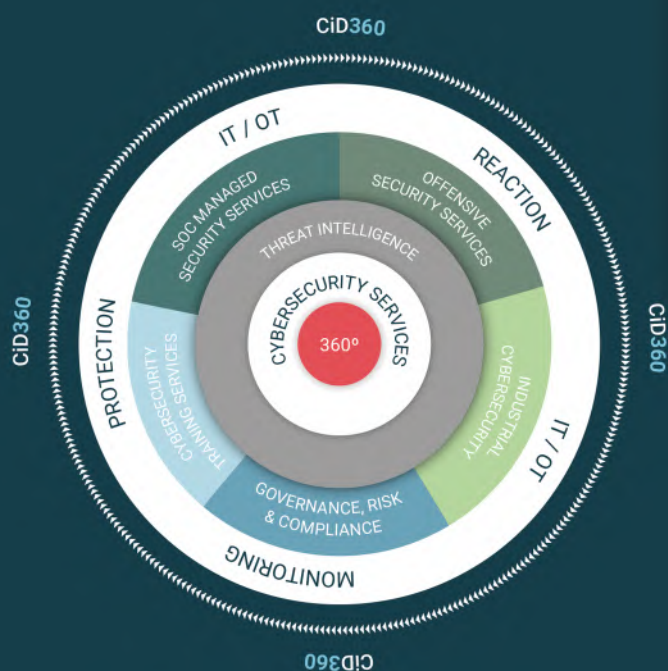
del **CNI**, por su labor en pro de la ciberseguridad nacional y que recogió su Subdirector General, **Luis Jiménez** —en la imagen, con



Román Ramírez, cofundador de **Rooted**. Cabe recordar que, hasta ahora, este galardón

se denominaba ‘Antonio Ropero’, pero éste pasará a quedarse para las ediciones de **Rooted Málaga**, de donde era conocido experto.

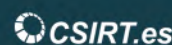
No seas presa fácil ante ciberataques



its⁺ by Ibermática

Soluciones y servicios escalables que brindan inteligencia, detección, administración y respuesta integral contra amenazas, asegurando su negocio.

Nuestro **SOC CERT** es miembro de pleno derecho del FIRST, así como de los foros TF-CSIRT y CSIRT.es



CONTACTA
CON NOSOTROS

+34 902 102 655
+34 902 413 500

marketing@its-security.es
info@ibermatica.com

Durante la celebración del multitudinario congreso técnico sus impulsores explicaron las claves de su éxito

FUNDACIÓN GOODJOB pone en marcha la 5ª Edición del Programa #include y muestra su 'saber hacer' en ROOTEDCON

El multitudinario congreso técnico, **RootedCON**, quiso apoyar la iniciativa **#Include**, de la **Fundación GoodJob**, aprovechando su XII edición en marzo, totalmente presencial, ofreciendo distintas actuaciones de visibilidad. Así, junto a alguna ponencia impartida por un emotivo y resuelto especialista de origen **#include**, se celebró una vistosa sesión titulada 'Impact #include: Hackeando la relación Empleo y Discapacidad', moderada por el Editor de **Revista SIC**, **Luis Fernández**, —entidad co-impulsora junto al congreso en dar el pistoletazo de salida de esta pujante iniciativa— en la que distintos actores de la misma —impulsores, coordinadores, formadores y alumnos ya colocados— dieron a conocer sus casuísticas en pro de este singular y ejemplarizante proyecto llevado a cabo por la fundación para formar a personas con discapacidad e incorporarlas al ecosistema laboral de ciberseguridad.

Un reto que, según el Director General de la organización, **César López**, se ha plasmado ya en cuatro ediciones y más de 250 alumnos formados, con el apoyo de entidades como el **Instituto Nacional de Ciberseguridad (INCIBE)**, el **Centro Criptológico Nacional (CCN)**, la **Consejería de Economía, Empleo y Competitividad de la Comunidad de Madrid**, el **Nodo Gallego-Cibergal**, la **Agencia Catalana de Ciberseguridad**, **Revista SIC**, **RootedCON** y la colaboración de más de 35 empresas, entre las están: **Telefónica Cybersecurity Cloud & Tech**, **AtoS**, **Entelgy Innotec**, **Axians**, **Botech**, **Capgemini**, **CSA**, **DXC Technology**, **Evolutio**, **Mnemo**, **S2 Grupo**, **Seidor**, **Siemens**, **Tarlogic**, **Thales** y **Wise Security Global**, entre otras.

En la mesa participaron grandes impulsores de



esta iniciativa, como **Román Ramírez**, responsable académico del programa, **Pablo Sanemeterio**, de **Telefónica Tech**, **Jorge Sanz**, de **Sidertia**, dos de sus tutores, así como **Ana Gómez** y **Patricia Rey**, ambas de la Fundación. Todos resaltaron el talento y el esfuerzo de todos los alumnos y cómo, gracias a él y a los buenos profesionales que de forma altruista imparten la formación, se consigue capacitar e incorporar al mercado de trabajo a personas con discapacidad capaces de realizar un trabajo de alta cualificación en las empresas colaboradoras.

Prueba de ello fue uno de los momentos más emotivos de la mesa en la que participaron **Borja Reina** y **Alejandro Yébenes**, dos alumnos del programa que actualmente trabajan en **S21sec** y **OneseQ**, el área de ciberseguridad del **Grupo Alhambra**, respectivamente. Ambos explicaron cómo una discapacidad relacionada con la vista les había limitado el acceso al mercado. Una limitación que gracias a la cualificación adquirida en el programa de GoodJob no fue impedimento para trabajar en el sector de ciberseguridad.

Así, hasta el momento, a través de esta iniciativa, se han formado cerca de 250 personas con discapacidad de diferentes áreas geográficas de España (Madrid, Cataluña, Castilla y León, Valencia, etc.), con un porcentaje de empleabilidad del 85%. A comienzos de este mes de abril, concretamente el día 4, se pone en marcha la 5ª Edición del Programa **#include**, y en paralelo la realización del Programa **#cloud**, un programa piloto en **cloud computing** dirigido en esta primera edición a 30 participantes.

Acuerdo con Telefónica Tech



Por otro lado, la **Fundación Telefónica** y la **Fundación GoodJob** firmaron un acuerdo para impulsar la empleabilidad de las personas con discapacidad a través de los Programas **#Impact**, en los que participarán profesionales voluntarios del **Grupo Telefónica**. El objetivo es formar, tutorizar o 'mentorizar' a participantes con discapacidad en competencias digitales. Inicialmente, esta colaboración se desarrolla en el Programa **#cero** de capacitación en competencias digitales y el Programa **#include** de empleabilidad en ciberseguridad. No obstante, ambas organizaciones extenderán esta colaboración a otros programas de empleabilidad, como **#cloud**, **#understand**, de análisis de datos e IA, y otros orientados a la programación, como **#dev** y **#denarius**, y también para el programa **#redes**, relacionado con el soporte de redes.

AENOR certifica en la ISO/IEC 27701 a INBENTA y en gestión de la digitalización, UNE 0060, a CONTAZARA, especializada en nuevas tecnologías para la gestión del agua

Inbenta, compañía internacional referente en el desarrollo de IA y Procesamiento de Lenguaje Natural, se ha convertido en una de las primeras empresas en obtener la certificación de **Aenor** en ISO/IEC

27701, de Gestión de Privacidad de la Información, una extensión de las normas ISO/IEC 27001 de Gestión de Seguridad de la Información,



e ISO/IEC 27002 de Controles de Seguridad.

La certificación ISO/IEC 27701 ayuda al cumplimiento con los principios y obligaciones que impone la legislación en materia de protección de datos y privacidad como, por ejemplo, el Reglamento Europeo de Protección de Datos (RGDP)

y la LOPDGDD. "Unirnos al reducido grupo de pioneros que gozan de esta certificación supone una mejora sustancial de nuestro

inbenta Sistema Integrado de Gestión, que aúna Calidad (ISO 9001), Seguridad de la Información (ISO/IEC 27001 e ISO/IEC 27017) y ahora también Privacidad (ISO/IEC 27701)", destacan desde la compañía.

Certificación 4.0

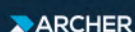
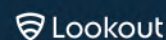
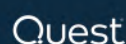
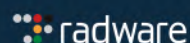
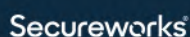
Además, la pyme industrial **ConTAZARA**, dedicada a las nuevas tecnologías para la gestión del agua, recibió el certificado Aenor de sistema de gestión para la digitalización, según la Especificación UNE 0060. Esta certificación ayuda a las organizaciones industriales a su digitalización, a través de un sistema de gestión eficaz, orientado específicamente para las pymes.

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

 ARCHER aruba
a Hewlett Packard
Enterprise company CISCO
Partner
Distributor IBM
Distributor Lookout MICRO
FOCUS NETWITNESS
An RSA Business OUTSEER
An RSA Company Quest radware SecurID
An RSA Business Secureworks® SONICWALL™ STORMSHIELD VERACODE vmware® WALLIX
CYBERSECURITY SIMPLIFIED

Las II Jornadas STIC Capítulo Colombia reunieron en Medellín a profesionales de 31 países aliados por una Iberoamérica cibersegura

El **Centro Criptológico Nacional (CCN)** y el **Instituto Nacional de Ciberseguridad (Incibe)**, celebraron sus segundas Jornadas STIC en Medellín (Colombia), con la asistencia de más de 500 profesionales y una audiencia en línea de 2.500 usuarios de 31 países. El evento contó con el apoyo del CSIRT Américas Network del Comité Interamericano contra el Terrorismo de la **Organización de los Estados Americanos (OEA)**. Bajo el lema 'Aliados por una Iberoamérica cibersegura', esta iniciativa ha congregado a los principales expertos en ciberseguridad en una clara apuesta por estrechar la cooperación público-privada, a través de tres días



de ponencias y mesas redondas.

Las jornadas fueron inauguradas por la Directora del **CNI, Paz Esteban**, quien destacó "la importancia de seguir colaborando y compartiendo información entre todos los actores implicados" y añadió que "queremos contribuir al fortalecimiento del ciberespacio en cada uno de nues-



tros países, porque somos conscientes de que debemos forjar un escudo protector, capaz de proporcionar seguridad y tranquilidad a nuestro sector público, ciudadanos y empresas".

Durante las jornadas, el Ministro de Defensa de Colombia, **Diego Molano**, también quiso expresar la satisfacción de celebrar este encuentro destacando las iniciativas nacionales en ciberseguridad.

Reconocimiento a CSIRTAméricas

Aprovechando el congreso, dentro del espacio dedicado a CSIRTAméricas, **Alison August Treppe**, Secretaria Ejecutiva del **Comité Interamericano contra el Terrorismo (CICTE)** de la OEA;

Javier Candau, Jefe del Departamento de Ciberseguridad del CCN, y **Rosa Díaz**, Directora General del **Incibe**, entregaron un galardón a **Roberto Lemaitre**, Coordinador de CSIRT-CR, de Costa Rica, además de premiar por su trabajo a **Diego Subero**, Oficial del Programa de Ciberseguridad del CICTE/OEA.

Actualización de Rocío y guías CCN-STIC

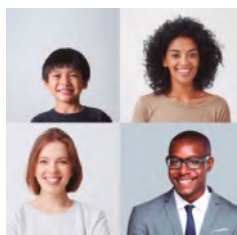
En paralelo, el Equipo de Respuesta ante Incidentes de Seguridad de la Información del CCN-CERT anunció la publicación de una nueva versión de Rocío, la solución de auditoría de cumplimiento con el ENS/STIC en dispositivos de red. Gracias a las funcionalidades incorporadas, Rocío permite ahora realizar auditorías sobre dos nuevas familias de equipos de comunicaciones: HP Comware y Aruba-CX.

Además, en febrero se publicó la Guía CCN-STIC 881, de adecuación al Esquema Nacional de Seguridad (ENS) para universidades y, en marzo, se actualizó la Guía CCN-STIC 140, sobre taxonomía de referencia para productos de seguridad TIC, entre otras novedades.

VERIDOS da a conocer la nueva generación de soluciones de verificación en la Cumbre Mundial de la Policía, basada en el ADN

La compañía **Veridos**, proveedora de soluciones de identidad integrales, dio a conocer en la Cumbre Mundial de la Policía, a mediados de marzo, su nueva generación de soluciones de seguridad y de verificación con tres productos innovadores: VeriDNA, VeriGO Drive ID y el kit de inspección Veridos.

"Estas soluciones habilitarán a los estados a confeccionar documentos oficiales aún más seguros e identificar a las personas con mayor rapidez", destacaron desde la empresa. En concreto, se mostró las



VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient
and Bundesdruckerei

capacidades de VeriDNA como solución para determinar la identidad, basada en el reconocimiento del patrón del ADN y su singular identificación. Además, a través de ella, se ofrece a las administraciones públicas un paquete de tecnología integral para la verificación de las personas, salvaguardando también la privacidad. De hecho, es una de las primeras soluciones para crear identificadores a prueba de falsificaciones basados en la biometría del ADN humano e integrados en la gestión del ciclo de vida de los documentos de identidad.

Priorizar vulnerabilidades con código de explotación es más efectivo que las puntuaciones CVSS

"2021 marcó un récord en vulnerabilidades de software conocidas. Las organizaciones informaron de 20.130, 55 al día, de media. Y aunque sólo el 4% suponen un riesgo alto, incluso los departamentos de TI con más recursos y personal no pueden solucionar todas estas 'brechas' en sus infraestructuras". Así lo expone **Kenna Security**, ahora parte de **Cisco**, que ha presentado un informe, en colaboración con **Cyentia Institute**, en el que muestra cómo evitar daños mayores y gestionar con mayor éxito las vulnerabilidades, mostrando la probabilidad relativa de que éstas sean explotadas.

En su estudio destaca que, para ello, es necesario "priorizar de forma adecuada las vulnerabilidades que hay que subsanar centrándose en las de alto riesgo con código de explotación público", lo que "es más eficaz que aumentar la capacidad de las organizaciones para par-



chearlas". "Pero si además se consiguen ambas metas -priorizar y remediar-, se puede lograr una reducción de hasta 29 veces en la probabilidad de explotación", explican desde la compañía.

La investigación confirma, además, una directiva de la **Agencia estadounidense de Seguridad de Infraestructuras y Ciberseguridad (CISA)** que sugiere dejar de priorizar la reparación de vulnerabilidades basándose en las puntuaciones CVSS (Common Vulnerability Scoring System) para centrarse en las que suponen un riesgo inminente.

La ciberseguridad integral, aquí y ahora

IBM Security Guardium

Las organizaciones tienen que sortear un ambiente digital cada vez más peligroso. Las posibilidades de sufrir un ataque aumentan cada día y los riesgos que afrontan sus sistemas y datos también.

Una protección convencional ya no resuelve el problema e, incluso, lo agrava por la falsa sensación de seguridad que proporciona. Por eso, **los especialistas en ciberseguridad de IBM tienen la solución: una seguridad informática completa, analítica e inteligente.**

Los negocios modernos, con entornos cada vez más complejos e híbridos, deben abordar este reto en toda su complejidad, con una estrategia integral que englobe datos, personas, procesos y herramientas.

IBM® Security Guardium® es la plataforma más completa de seguridad que resuelve esta necesidad. Una solución inteligente y flexible que protege los datos críticos de negocio.

La respuesta más eficaz que garantiza que ningún ciberdelincuente pondrá en peligro el presente y futuro del negocio.

Aquí y ahora.

¿Qué podemos hacer por su organización?

Contacte con Logicalis y conozca cómo podemos ayudarle.

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

Email
marketing-es@es.logicalis.com

Para conocer más sobre cómo orquestar su seguridad TI, escanee el código QR



El riesgo de los proveedores de servicios: el 90% reconoce haber sufrido ataques en 2021

El cibercrimen cada vez se centra más en los proveedores de servicio, por el impacto que tiene un ataque, tanto en la empresa como en sus clientes. Buena prueba de ello es que, según una investigación de la compañía **N-able**, el 90% de los MSP han reconocido haber sufrido un ciberataque con éxito en el último año y medio. De hecho, los participantes destacaron que la cantidad de ataques que

28% experimentó la pérdida de confianza en ellos por parte de sus clientes.

Los métodos de ataque más comunes detectados por los MSP, según el estudio, fueron el *phishing* (75 %), los de DDoS (56 %) y de *ransomware* (42 %).

Lo que es bastante llamativo es que, a pesar de esta situación y cifras, los investigadores de N-able constataron que los proveedores de servicios no están

INVERSIONES DE LOS MSP PARA MANTENER SEGUROS LOS NEGOCIOS DE CLIENTES



han sido repelidos durante este período casi se duplicó, pasando de una media de seis a 11.

El informe, que ha contado con la opinión de 500 ejecutivos de TI en MSP, también constató la eficacia de este tipo de servicios, ya que el 82% reconoció haber alertado a sus clientes de posibles ataques, evitando una media de 18 por mes.

En cuanto a los efectos de los ciberataques contra los MSP, más de la mitad de los encuestados confesaron pérdidas financieras e interrupciones comerciales, el 46% también sufrió pérdida de negocio, el 45 % efectos reputacionales y el

acometiendo grandes inversiones en su ciberseguridad —rondan únicamente el 5%—, ni están implementando muchas medidas básicas que deberían tener, como es la autenticación de dos factores y que sólo el 40% ha introducido de forma interna.

Prueba de la preocupación existente por la ciberseguridad de los proveedores, entre otras iniciativas, se ha hecho patente en la consulta que ha llevado a cabo el Reino Unido para estudiar la posibilidad de que los proveedores estén obligados, por Ley, a cumplir unos mínimos estándares de ciberseguridad en el país.

GMV incrementa su plantilla apostando por la innovación, también, en ciberseguridad en infraestructuras y TI

GMV ha incrementado su plantilla en un 17,5%, con más de 250 puestos tanto de perfiles *junior*, como *senior*, en las diferentes áreas en las que es un referente como espacio, transporte y, también, ciberseguridad. Esta especialización, unida a la experiencia alcanzada en sus áreas de actividad, han permitido a GMV mantener una dinámica de crecimiento, seguir generando puestos de trabajo y, también, convertirse en una reconocida marca empleadora.

Su buen hacer se plasma en “el desarrollo de productos y servicios innovadores en los sectores en los que está presente, le ha permitido continuar tanto con su actividad productiva como afrontar nuevos proyectos de mayor relevancia e impacto internacional”, destacan desde la compañía.

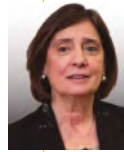
Entre dichos proyectos destaca la adjudicación del contrato para la evolución y mantenimiento del segmento terreno de control

de **Galileo**, la participación en el desarrollo de la nueva generación de vehículos autónomos de **BMW** y el despliegue del nuevo sistema tarifario integrado y multimodal en la red de transporte público de las **Islas Baleares** con tecnología EMV.

En concreto, en ciberseguridad, lleva tres décadas protegiendo las infraestructuras y los sistemas tecnológicos de grandes organizaciones y administraciones públicas en todo el mundo. Cuenta con un equipo altamente cualificado que ofrece servicios y soluciones específicas para distintos sectores, como el financiero, el industrial o de la salud.



NOMBRAMIENTOS



● La **Fiscalía General del Estado** ha renovado en el cargo a **Elvira Tejada de la Fuente** como Fiscal de Sala del Servicio de Criminalidad Informática. Ingresó en la Carrera Fiscal en 1981 y en 2011 obtuvo su destino como Fiscal de Sala responsable de esta unidad centrada en los delitos informáticos, cuya creación, precisamente, fue objeto en su momento de un Premio SIC.



● Interior ha nombrado al comisario principal, **Tomás Vicente Riquelme**, Jefe de la **División de Operaciones y Transformación Digital** de la **Policía Nacional**, Área a la que corresponde la coordinación, gestión y supervisión en el ámbito de la operatividad policial, así como la planificación estratégica en materia de transformación digital. Ingresó en el Cuerpo en 1983 y ha ocupado distintos destinos en la Comisaría General de Información, en Logística e Innovación, así como en la Comisaría General de Policía Judicial y la Dirección Adjunta Operativa. Cuenta con la encomienda de la Orden del Mérito Civil y la Cruz al Mérito Policial con distintivo rojo.



● El **Consortio de Compensación de Seguros** ha ascendido a **Adrián Macías** a Jefe de la Oficina Técnica de Seguridad Informática, siendo hasta ahora Responsable Coordinador de Ciberseguridad. Licenciado en Informática por la Universidad de Alcalá, ha trabajado para S2 Grupo y el Ayuntamiento de Daganzo de Arriba, entre otras organizaciones.



● La **Agencia de Ciberseguridad de Cataluña** ha encomendado a **Tomás Roy** la dirección del denominado Centro de Innovación y Competencia en Ciberseguridad (CIC4Cyber). Con anterioridad, Roy venía siendo Director del Área de Estrategia y en la antigua etapa del ente, bajo la denominación de Cesisat, fue Director del mismo.



● **Entelgy, The BusinessTech Consultancy** ha incorporado a **Pablo Echevarría** como CEO Global Business y a **José Antonio Rocha** como

Managing Director de su división de negocio Digital Business Process. Echevarría, con más de 30 años de experiencia, será el encargado de dirigir los equipos de EMEA y LATAM, así como la gestión de las divisiones de Ciberseguridad y Digital Business Process. Ha trabajado para empresas como Telefónica, tanto en España como en el Reino Unido, o Axent, en cargos de alta dirección. Rocha, también con tres décadas de experiencia, es experto en la implementación de soluciones basadas en RPA, Inteligencia Artificial, Hyperscalers, IoT, y metodologías Design Thinking y Agile. Ha trabajado, entre otras, en AT&T, Ericsson, Telefónica, Etisalat o Fractalia.

CipherTrust Data Security Platform

Localice, proteja y controle los datos sensibles de su organización en cualquier lugar gracias a la protección de datos unificada de última generación.

Localizar



Proteger



Controlar



EXCLUSIVE NETWORKS sigue creciendo con alianzas con JUNIPER, WASABI, NETSKOPE Y SALT SECURITY, y supera los 1.000 millones de euros en un trimestre

Exclusive Networks continúa con su estrategia de alianzas con una importante asociación con **Guardia Cybersecurity School** (Quest Education Group), para abordar la creciente escasez de habilidades en el sector. Con su lanzamiento en septiembre de 2022, Guardia Cybersecurity School se convertirá en la primera escuela de TI completamente dedicada a ciberseguridad en Francia. También, ha sido significativo el anuncio de la multinacional extendiendo la propuesta de **Ignition Technology**, el distribuidor especializado de valor añadido de la compañía, “para proveedores emergentes de ciberseguridad disruptiva” a EMEA. Así, comercializará su portafolio en mercados estratégicos clave en el sur de Europa (Francia), Oriente Medio y África subsahariana, estando ya presente en norte de Europa, Reino Unido y países nórdicos, entre otros.

También ha sido notable la alianza con **Juniper**, una compañía global con productos de conectividad avanzados, y de **Wasabi**, que ofrece almacenamiento en la nube de manera simple, predecible y asequible para empresas de todo el mundo, además de la ampliación de la alianza con **Netskope**. Asimismo, se



ha asociado con **Salt Security** “para combatir la creciente amenaza contra la seguridad de las APIs”, convirtiéndose en su primer distribuidor de valor añadido en la región de PAN-EMEA. El acuerdo se circunscribirá inicialmente a España, el Reino Unido, Francia, DACH, Benelux, países nórdicos e Italia. También, ha presentado su **Centro de Formación Exclusive** (ETC, por sus siglas en inglés). Se trata de una nueva plataforma de formación con la que el distribuidor ofrece una amplia selección de cursos acreditados por sus fabricantes.

Buen momento

Asimismo, la compañía ha destacado la buena marcha de su negocio tras lograr “superar, por primera vez en su historia, los 1.000 millones de euros de ventas brutas en un trimestre. Este no es solo un hito simbólico en nuestro viaje, sino que también demuestra nuevamente nuestro éxito al abordar la demanda convincente de soluciones de ciberseguridad y ofrecer la plataforma de comercialización óptima”, han destacado desde Exclusive.

THREATQUOTIENT suma fuerzas con MNEMO para mejorar, con automatización, la ciberprotección

ThreatQuotient, proveedor de inteligencia contra amenazas (TIP), y **Mnemo**, especializada en servicios gestionados de ciberseguridad, han alcanzado un acuerdo por el cual, ésta se beneficiará de las ventajas de la plataforma ThreatQ para acelerar todos los procesos de operaciones necesarios para proveer servicios a sus clientes, automatizando muchos de ellos y mejorando por tanto su eficiencia. Además, de este nuevo uso de su plataforma, ThreatQuotient también ofrece la oportunidad a Mnemo de poner en marcha nuevos servicios de manera más ágil.

Esta alianza permitirá dotar al equipo de *Cyber Threat Intelligence* de Mnemo



de capacidad de gestión y orquestación de amenazas, eventos y análisis de incidentes de seguridad, integrando de manera homogénea la capacidad de análisis, investigación, enriquecimiento, generación respuesta y aplicación de planes de acción. Todo desde un sistema central que ofrezca retrospectiva en tiempo real y modelos de tratamiento diseñados aplicables a las amenazas cargadas, con resultados operables por las infraestructuras de detección y prevención de forma directa.

Por otro lado, ThreatQuotient ha llegado a un acuerdo con **Ingecom**, que distribuirá sus soluciones en España, Italia y Portugal.

NOMBRAMIENTOS



● **Pascal Steichen** ha sido designado Presidente y Coordinador del **Centro de Competencia en Ciberseguridad de la UE (ECCC)**, en un mandato que tendrá una duración de cuatro años. Este alto ejecutivo luxemburgués participó en la fundación de la *European Cyber Security Organisation (ECSO)*, es miembro activo del consejo consultivo de la FIC, forma parte del jurado de la *IFSEC Global Influencers in Security and Fire Award* y, desde hace poco, representa a su país en el Consejo de Administración del ECCC.



● **Banco Sabadell** ha fichado como Director de Auditoría Interna de Ciberseguridad a **Manel Cantos**. Con una dilatada experiencia, ha desempeñado roles de responsabilidad en Capgemini Engineering, Altran, Telindus y Schneider Electric, entre otras. Es ingeniero de telecomunicaciones por la Politécnica de Cataluña y cuenta con una decena de certificaciones.



● La multinacional aseguradora **Axa** se ha reforzado con **Salvador Esteve** como SOC Project Manager. Ingeniero Informático, ha desempeñado roles de responsabilidad en Sothis, BT y la Comunidad Valenciana, entre otras.



● **Javier Macías Blanco** ha sido contratado como Especialista en Ciberseguridad por **Urbaser**. Con una dilatada trayectoria profesional, ha trabajado para organizaciones como Seur, donde venía siendo CISO, Oesia, AirOn Group y Tieto, entre otras.



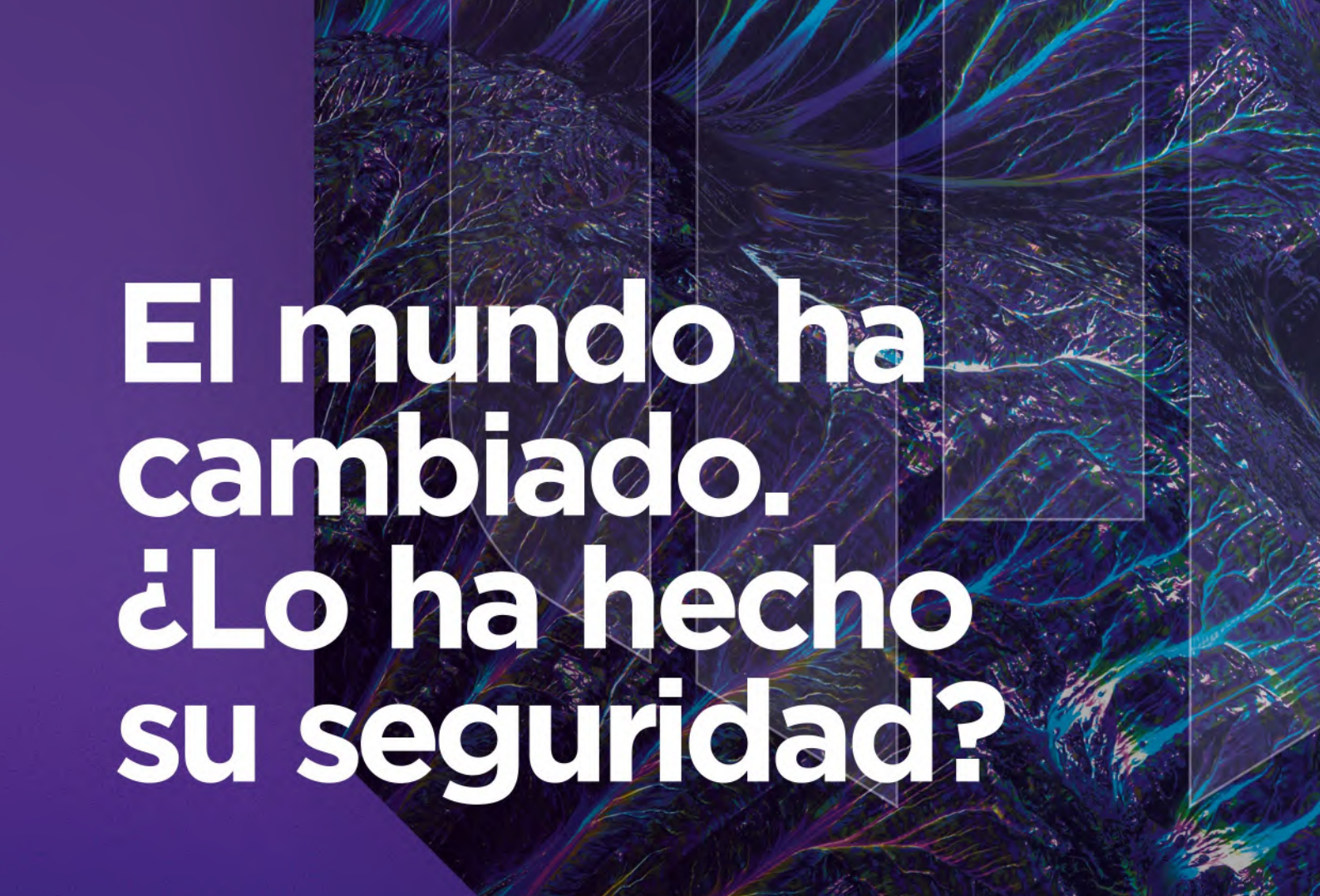
● **Francisco Javier Sucunza** ha sido contratado por **Repsol** como Especialista en Ciberinteligencia. Con más de 20 años de experiencia, con foco intenso en la ciberprotección industrial, ha estado en compañías como Siemens, Capgemini, Telefónica y Entelgy Innotec, entre otras. Es Matemático por la Universidad de Zaragoza.



● **Tranxfer** ha encomendado a **Julio Prada** el cargo de CEO. Con una amplia experiencia en el área del software como servicio, llega a la compañía tras 15 años en Inbenta, donde fue Director General. Ahora, además de ayudar a la compañía en su crecimiento en España y en países de habla hispana, también participará en su internacionalización, sobre todo, en Alemania y Francia. En paralelo, a lo largo de su trayectoria profesional, ha compaginado su carrera como profesor asociado en la EADA Business School.



● **Willis Towers Watson** ha contratado a **Carmen Segovia** como Directora de Ciberriesgos. Con gran experiencia en el sector, ha ostentado cargos de responsabilidad en Aon Risk Solutions y Marsh, entre otras. Es Licenciada en Ciencias Políticas y Sociología por la Autónoma de Barcelona.



El mundo ha cambiado. ¿Lo ha hecho su seguridad?

**SentinelOne,
el fin de la
seguridad pasiva**

El malware no necesita una conexión para atacar, y su ciberseguridad tampoco debería hacerlo. SentinelOne ofrece protección online/offline en cualquier plataforma o sistema operativo. Si su seguridad solo funciona online, entonces no funciona.

Los mejores ya confían en nosotros

ASTON MARTIN

norwegian 

flex

McKESSON

 **SentinelOne®**

sentinelone.com

FACEPHI obtiene la certificación PINAKES para mejorar con verificación la protección bancaria

FacePhi ha logrado la certificación **Pinakes**, un reconocimiento que distingue a la compañía como proveedor tecnológico homologado frente a cualquier entidad bancaria nacional. Con ella, su tecnología de verificación de identidad digital pasa a formar parte de la cadena de suministros del Centro de Cooperación Interbancaria, una asociación bancaria que promueve y desarrolla ideas de interés para el sector, y que depende del **Banco de España**.

Como bien es sabido, el nuevo marco regulatorio europeo EBA/GL/2019/02 obliga a las entidades financieras europeas a realizar auditorías de seguridad a todos aquellos proveedores tecnológicos a los que se les externalizan tareas críticas para el desarrollo de su actividad, a nivel operacional y en funciones de control. Con la certificación **Pinakes**,

estos proveedores pasan de tener que realizar una auditoría por cliente a obtener una única certificación que sirve para todos los bancos españoles.

Así pues, para lograr este reconocimiento, se ha evaluado el nivel de seguridad de FacePhi en tres aspectos: integridad, confidencialidad y disponibilidad, alcanzando un *rating* AAA que implica que se ha logrado la máxima puntuación posible.

La certificación ofrece facilidades a la hora de aplicar las soluciones de la compañía en todo tipo de entidades financieras españolas, desde las más grandes a las más pequeñas, como las cajas rurales. Un uso que se vuelve más sencillo gracias al lanzamiento de la Plataforma de Identidad Digital de FacePhi, que permite la implementación de su tecnología en todo tipo de empresas, sin importar su tamaño.



AWS se convierte en el primer fabricante en refrendar un servicio en la nube con ENS Alto, con Lince, y realizada por JTSEC

Amazon Web Services (AWS) ha sido el primer fabricante en obtener la primera certificación Lince y cualificar un servicio en la nube, siendo **Jtsec** el laboratorio que ha realizado la evaluación. "Esto supone un hito para el catálogo CPSTIC, ya que nos encontramos que muchos proveedores están cambiando la tendencia a evaluar servicios en la nube, lo que muestra además la aceptación del catálogo y su evolución, y también los laboratorios hemos de estar actualizados", destacan desde la empresa granadina.

Como se sabe, AWS Key Management Service (KMS) facilita la creación y la administración de claves criptográficas y el control de su uso en una amplia gama de servicios de

AWS y en sus aplicaciones. Utiliza módulos de seguridad de hardware que se han validado según FIPS 140-2 para proteger sus claves. El servicio está integrado con otros servicios de AWS, lo que facilita el cifrado de los datos que almacena en estos servicios y el control del acceso a las claves que los descifran.

Con esta nueva certificación e inclusión en el catálogo, "AWS da un paso más en garantizar la seguridad, contrastada por Jtsec, y el departamento de Productos y Tecnologías del CCN, siendo el primer proveedor en acreditar un servicio de seguridad en la nube, bajo la metodología Lince", ha destacado el Security Assurance para Iberia de AWS, **Borja Larrumbide**.



NOMBRAMIENTOS

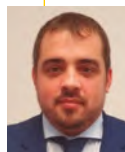


● **Aenor** ha reconocido la buena labor de **Boris Delgado**, hasta ahora Manager de Certificación TIC, ascendiéndole a Director de Soluciones de Digitalización y Tecnología. Es ingeniero Superior en Informática por la Pontificia de Salamanca y ha realizado gran parte de su trayectoria profesional en Aenor donde comenzó como Lead IT Auditor.



● La multinacional distribuidora **Arrow**, en reconocimiento a su solvente trayectoria, ha ascendido a **Iñaki López Monje** a Director Regional de la división de negocio Enterprise Computing Solutions

para el Sur de Europa, añadiendo Italia y Marruecos a su anterior responsabilidad en la región de Iberia. Además, la compañía ha reforzado su equipo con la llegada de **Pablo Alarcón** como Strategic Account Director para la región de EMEA. López Monje venía siendo Director Regional de la compañía en España, en la que comenzó en 2012. Con anterioridad, trabajó en Altimate, Mambo Technology y Sofecom, entre otras. Por su parte, Alarcón fue Responsable de Alianzas en Telefónica Tech, en la que ha desarrollado casi dos décadas de labor, además de trabajar para otras entidades, como la Agencia de Certificación Electrónica (ACE).



● **Juan Tárrega** ha sido promocionado para convertirse en Responsable del departamento GRC (Gobierno Riesgo y Cumplimiento) de **Audea Seguridad de la Información**. Ha ejercido, durante más de una década, como consultor de seguridad y jefe de proyecto en el ámbito de la seguridad de la información, gestión del riesgo tecnológico, continuidad de negocio y cumplimiento normativo a nivel internacional. Ha trabajado para compañías como Auren y Pwc.



● **Daniel Romero** ha sido contratado por F5 como Ingeniero Preventa. Ha trabajado para empresas como Westcon-Comstor Spain, Grupo Antea, Itway y Razona, entre otras, y es ingeniero de Telecomunicaciones por la Politécnica de Madrid.



● **Botech** ha fichado a **Alberto Moro** y **Andréia Castellan** como Manager en el área de Cybersecurity Services y Business Development Manager, respectivamente, reforzando su área de

desarrollo de negocio de productos tecnológicos para pymes. Moro cuenta con más de 15 años de experiencia, en los que ha trabajado para compañías como Panda Security o Telefónica, destacando por su amplio conocimiento en *threat hunting*, análisis forense, *pentesting*, auditorías de seguridad y *reversing*. Por su parte, Castellan cuenta con más de tres décadas de experiencia liderando proyectos en TI, centrándose en los últimos años en ciberseguridad para compañías como GH Crecemos o TechHero X.



● **Disruptive Consulting** ha elegido a **Javier Navarro** para el puesto de Director de Ciberseguridad y Defensa. Con anterioridad ha trabajado en organizaciones como NTT Data Europa y Latinoamérica, Deloitte, Logitek y KPMG, entre otras.

Predecir lo que importa

La alianza líder que garantiza
la **gestión de vulnerabilidades**
y compliance técnico



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

ARROW cierra un acuerdo exclusivo como Symantec Cybersecurity Aggregator con BROADCOM

El distribuidor **Arrow** ha firmado un acuerdo con **Broadcom** para posicionarse como 'Cybersecurity Aggregator' para el catálogo de software de **Symantec**, para su base de clientes europeos de pequeñas y medianas empresas (pymes).



el lanzamiento de un programa de socios de canal, herramientas de venta, un programa de prueba y compra, y opciones de precios basadas en el valor, lo

que permite a los *partners* enfocarse y aumentar la inversión en sus negocios de ciberseguridad de Symantec.

Tras este nuevo acuerdo de Aggregator, a partir de febrero, Arrow se posiciona como distribuidor exclusivo de las soluciones de Symantec para los socios de canal y, en última instancia, para los clientes, dentro del segmento de las pymes, también en España. Arrow ofrecerá una serie de iniciativas que permitirán a su canal de ciberseguridad crear y obtener beneficios económicos por ofrecer experiencias de cliente excepcionales, aumentar la retención y ayudarles a crecer.

Con el apoyo de Broadcom, las nuevas iniciativas de Arrow incluyen

"Este es un desarrollo emocionante para Arrow en Europa, ya que el segmento de las pymes sigue ofreciendo una importante oportunidad para nosotros y nuestros socios *resellers*. Estamos comprometidos con ayudar a impulsar el crecimiento continuo de Symantec invirtiendo en recursos que ayuden a nuestros distribuidores a aumentar sus ventas de soluciones de Symantec y a equiparlos con todo lo que necesiten", ha destacado el Presidente de EMEA para la división de negocio Enterprise Computing Solutions de Arrow, **Eric Nowak**.

V-VALLEY potencia su catálogo incorporando a BITDEFENDER y DEEP INSTINCT

V-Valley distribuirá los productos y servicios de ciberseguridad de **Bitdefender** para la detección, protección y respuesta ante amenazas, con una amplia

propuesta para el mercado empresarial. Con este acuerdo, los *partners* de **V-Valley** podrán acceder a la tecnología de Bitdefender, especializada en la eliminación de amenazas, protección de la privacidad y los datos y facilitar la resiliencia informática.

Entre todas sus soluciones destaca la plataforma GravityZone, para la defensa de los activos de las empresas frente a ciberamenazas, desde las más comunes hasta las más sofisticadas. También, son reseñables sus tecnologías EDR y MDR, que ofrecen servicios de prevención, detección y respuesta en puntos finales, red, nube y usuarios finales, y que están diseñadas para ayudar a organizaciones y a los proveedores de servicios gestionados a mejorar su capacidad en la detección y erradicación de amenazas en tiempo real, reforzando su resiliencia frente a los ciberataques. A ello se unen

sus soluciones avanzadas de *threat hunting*, que ayudan a las empresas a identificar y eliminar las amenazas ocultas en su red.

Además, el mayorista ha incorporado en su portafolio de ciberseguridad a **Deep Instinct**, empresa que aplica el aprendizaje profundo de extremo a extremo aplicado a ciberprotección, para empezar a distribuir sus soluciones en el mercado español. Fundada en 2015, Deep Instinct cuenta con una plataforma de prevención de amenazas construida sobre un marco de aprendizaje

profundo integral de IA patentado, lo que la convierte en una de las organizaciones con mayor proyección en un panorama en el que los ciberataques crecen exponencialmente.

"V-Valley ha demostrado una gran capacidad para abrir nuevos mercados con tecnologías pioneras y, por su profundo conocimiento del mercado y flexibilidad para adaptarse a las necesidades locales, se convierte en el aliado perfecto", afirmó **Noelle Margiotta**, Channel Manager para el Sur de Europa de Deep Instinct.



NOMBRAMIENTOS



● **Cipher** ha ascendido a **Jorge Hurtado** a Global CTO de la compañía perteneciente al

Grupo Prosegur, y ha incorporado a **Frank Costa** y **Yago Gómez-Trenor**, ambos como Sales Manager. Hurtado hasta ahora, era Vicepresidente para la región de EMEA de la compañía. Con más de 20 años de contrastada experiencia –13 de ellos reportando a la alta dirección– trabajó con anterioridad para Capgemini, CGI y Gesfor, entre otras. Por su parte, Costa posee más de tres décadas de experiencia, especializado en venta consultiva y gestión comercial en IT, OT e IoT, así como en desarrollo de negocio e Industria 4.0, habiendo trabajado en empresas como Grupo SIA, S2 Grupo, Logitek, S21sec, Spamina y Fujitsu, entre otras. Gómez-Trenor es Ingeniero Técnico en Informática por la Politécnica de Valencia y lleva más de 14 años en desarrollo de negocio en compañías como S2 Grupo, Vintegris, Sothis, Mapfre Prevención, Alliance Footwear o Grupo Alulac, entre otras.



● **Stormshield** ha promocionado a **Sébastien Viou** a Director de Producto de Seguridad. El directivo, que se incorporó en 2020 como Consultor de Ciberseguridad, continuará ejerciendo esta función en la empresa, además de hacerse cargo de la gestión de un equipo cualificado compuesto por 18 personas, entre los que destacan expertos en ciberamenazas, *pentesters* y consultores dedicados a mejorar la seguridad de las soluciones de Stormshield.



● **BlueVoyant** ha reforzado su equipo con **Ángel Otermin** como Regional Sales Manager para España, Portugal e Italia. Con anterioridad, trabajó en diversos puestos de responsabilidad en T-Systems, donde lideraba la unidad de negocio para Iberia, y en HP Enterprise, entre otras. Es titulado en Informática por la Universidad de Northumbria (Reino Unido), además de contar con un Máster por la IE Business School.



● **Syneto** ha ascendido a **Alessandro Freddi** como Sales Director para España, siendo así el máximo responsable de la compañía en nuestro territorio y ampliando sus funciones, hasta ahora en Italia. Ingeniero mecánico, se unió a la compañía hace una década como Director Asociado, siendo nombrado responsable del país alpino en 2016. Con anterioridad, trabajó para compañías como Antedata SRL, Nuovamacut Nord Ovest y CF Gomma SPA, entre otras.



● **Arsenio Pérez Gavira** ha sido contratado como Cybersecurity Manager/Digital Platform Services por **Sopra Steria**. Posee una amplia experiencia, habiendo trabajado en compañías como Castroalonso Let, 11Paths y Telefónica Digital, entre otras. Es Ingeniero en Informática por la Universidad de Alicante.

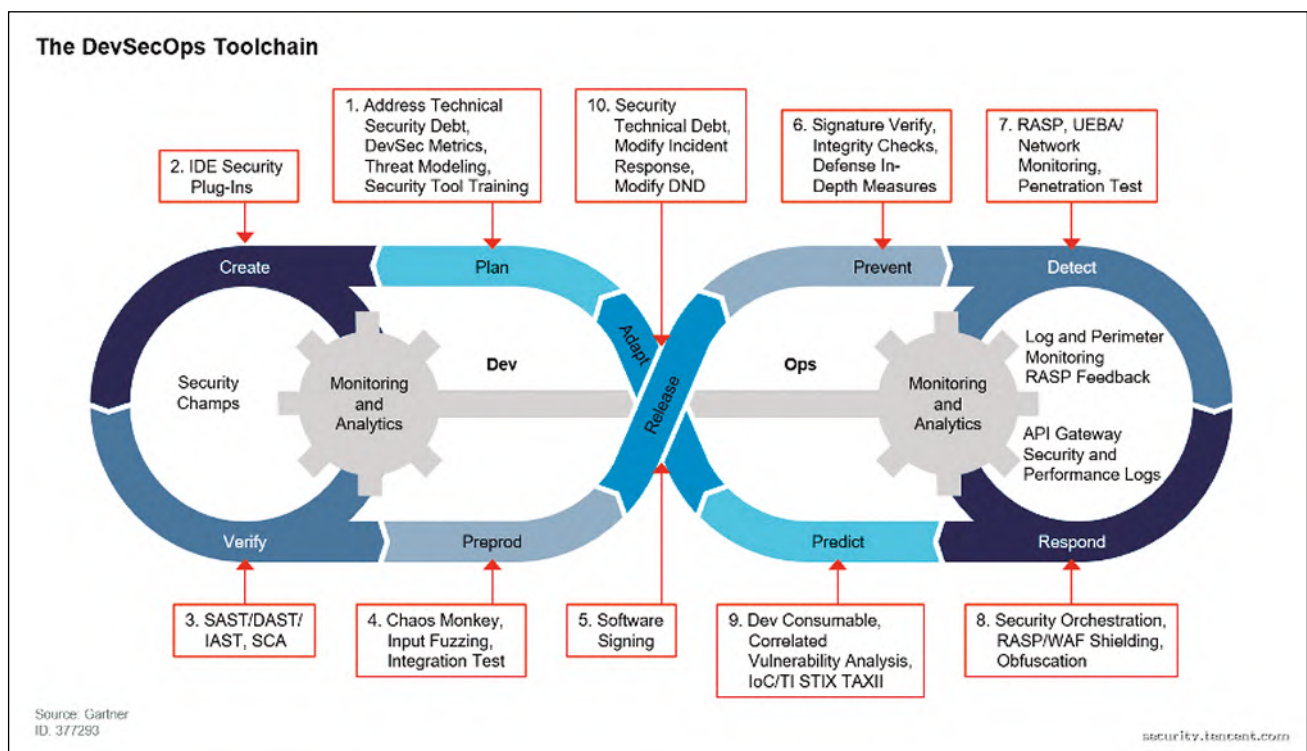


Un portfolio completo de
Seguridad de Aplicaciones

SYNOPSYS[®]
Silicon to Software[™]

tufin

ROHDE & SCHWARZ



www.cefiros.net – comercial@cefiros.net

SEIDOR estrena imagen corporativa, compra WORK WELL y logra el ENS en categoría Alta

Seidor ha obtenido el Certificado del Esquema Nacional de Seguridad (ENS), en categoría Alta, para sus servicios del Centro de Monitorización, Operación de la Ciberseguridad, Servicios de Análisis y Respuesta Ante Incidentes de Seguridad (Seidor CSIRT) y los de asistencia, soporte y consultoría profesional TI.

“Este nuevo éxito nace del esfuerzo y el compromiso de la organización, a través de la Oficina de Ciberseguridad Corporativa, dirigida por **Rubén Mora**, CSO/CISO de Seidor, y del departamento de Calidad y Protección de Datos, al frente del que está **Francisco Naranjo**”, destacan desde la compañía.

Así, desde ahora, el Seidor CSIRT, acreditado y miembro de los foros **FIRST.org**, **IT-CSIRT Trusted Introducer** y **CSIRT.es**, dispone de la máxima categoría del ENS acreditando la seguridad de sus sistemas de la información y los datos personales que custodia y trata en sus servicios a entidades y organismos



Nueva imagen y lema

Además, coincidiendo con su 40 aniversario, la compañía ha estrenado nueva identidad e imagen de marca global, así como nuevo lema ‘Human focused Technology experts’, que plasma su sentir como ‘activistas tecnológicos’.

También, ha sido notable la compra, por parte de la consultora, de la empresa gala **Work Well**, especializada en soluciones informáticas para la pequeña y mediana empresa y, desde hace 20 años, *partner* de SAP Business One, con la que ha aterrizado en el mercado de Francia. Con esta compra, la empresa española amplía su presencia geográfica, continuando su proceso de internacionalización. De esta manera, ya son 40 los países en los que tiene presencia gracias a un equipo humano formado por más de 6.000 profesionales.



que pertenecen a la administración pública, y de todos sus clientes.

NOMBRAMIENTOS



● **Alberto Cita** ha sido contratado por **Torq**, firma especializada en software como servicio, como Senior Solutions Architect. Con amplia experiencia, este reconocido profesional ha trabajado en compañías como Zscaler, Symantec y Brocade, entre otras. Es ingeniero de Telecomunicaciones por la Politécnica de Madrid.



● **Cyberbit** ha fichado a **Blas Simarro** como Regional Sales Manager para Iberia. Pionero del sector en nuestro país, con más de dos décadas en este ámbito, ha desempeñado diversos roles de responsabilidad en empresas como BlackBerry-Cylance, Lidera Network, Buguroo, S21sec y McAfee, entre otras.



● **IBM Security** ha contratado como Associate Partner a **Daniel Zapico** y **Roberto Peña**. Zapico ha sido CISO de Globalia y Air Europa y ha trabajado para firmas como EY, SIA, Prohuban y Fundación Pablo VI, entre otras. Por su parte, Peña cuenta con más de 20 años de experiencia de trayectoria forjada en empresas como Mnemo, PwC y Protiviti, entre otras.



● **Pedro García Milicua** ha sido fichado por **Kyndryl** como Security Technical Solution Manager (TSM). Ingeniero Técnico en Informática de Sistemas por la Politécnica de Madrid, cuenta con una dilatada trayectoria profesional en empresas como Twilio, DXC Technology y Deloitte España, entre otras.



● **Lacework** ha confiado en **Joan García** para desempeñar el puesto de ‘Solving Cloud Security Challenges with AI’ para España y Portugal. Con más de una década de experiencia, ha trabajado para empresas como Splunk, HashiCorp, Pure Storage y Veritas Technologies, entre otras. Es ingeniero de Telecomunicaciones por la Politécnica de Cataluña.



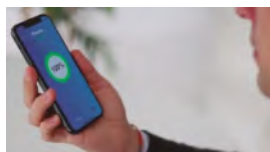
● **Vectra AI** ha promocionado a **Willem Hendrickx** como Chief Revenue Officer (CRO), habiendo ocupado hasta ahora el puesto de Vicepresidente Senior Internacional. Con más de 25 años de experiencia en ventas de software, ocupó con anterioridad roles de responsabilidad en EMC/Dell, Nokia, Alcatel-Lucent y Riverbed Technology.

VERIDAS se une al Pacto Digital para la protección de las personas de la AEPD



Veridas, especializada en soluciones para la verificación de la identidad real de las personas, se ha adherido al Pacto Digital para la protección de las personas de la **Agencia Española de Protección de Datos (AEPD)**, proyecto por el que la compañía española se suma al compromiso por la responsabilidad en el ámbito digital. Con la adhesión a este Pacto, Veridas quiere hacer más patente su compromiso con la protección de datos y con la creación de un entorno digital sano y libre de contenidos que atenten contra la integridad y el honor de las personas.

“Dada la importancia que, para Veridas, tiene el cumplimiento de la



normativa de protección de datos, la adhesión a este Pacto es un paso natural, ya que supone afianzar las políticas y buenas prácticas que ya viene aplicando, al tiempo que permite participar más activamente en la divulgación de una cultura digital saludable”, han destacado desde la compañía. Además, recuerdan que sus “soluciones persiguen que todas las personas puedan ser ellas mismas también en el entorno digital, por lo que resulta esencial la protección de la identidad y el libre acceso al mismo por todos”.

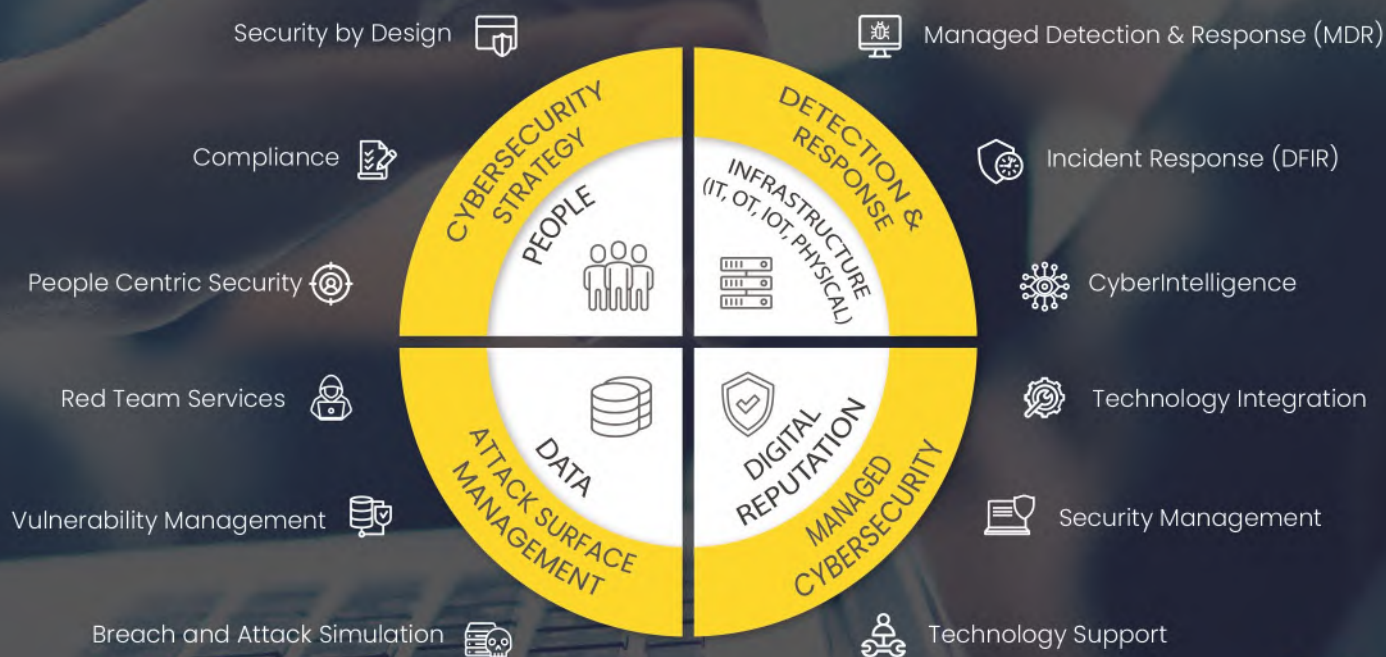
Cabe recordar que el Pacto Digital, promovido por la AEPD, cuenta con la participación de una gran cantidad de organizaciones y entidades profesionales (más de 300), especialmente del entorno tecnológico.



**UN LÍDER MSSP GLOBAL, 100% COMPROMETIDO CON NUESTROS CLIENTES
PARA AYUDARLES A MITIGAR TODOS SUS RIESGOS DE SEGURIDAD
EN SU PROCESO DE TRANSFORMACIÓN DIGITAL**

Cipher es una empresa del grupo Prosegur, fundada en el año 2000 y centrada en la seguridad de la información, con presencia en 15 países, más de 400 especialistas en seguridad certificados y 6 centros de operaciones de Ciberseguridad (SOC/CERTs).

Cipher presta una gran variedad de servicios, destacando el área de Seguridad Gestionada y Detección y Respuesta de incidentes (MSSP/MDR).



PEOPLE CENTRIC
SECURITY

CYBERSECURITY
COMPLIANCE

CYBERSECURITY
STRATEGY

CYBERSECURITY STRATEGY AND CULTURE

ORANGE BUSINESS SERVICES y FORTINET suman fuerzas en SASE para crear una red de nube nativa segura y escalable

Orange Business Services y Fortinet se han asociado para ofrecer un enfoque disruptivo de Secure Access Service Edge (SASE) mediante la integración de las tecnologías de red orientadas a la seguridad de Fortinet en la infraestructura cloud de telecomunicaciones de Orange.



“Esto refuerza la convergencia de la seguridad y la red, al tiempo que optimiza el rendimiento independientemente de la ubicación del usuario”, destacan desde las entidades. “A diferencia de otras ofertas de prestación

de servicios SASE en el mercado, este enfoque sin fisuras –con integración y automatización incorporadas– garantiza la actualización de los servicios en tiempo real y una experiencia de usuario inigualable”, añaden.

Con este paso entre Orange y Fortinet, que también ha dado lugar a ‘Flexible SD-WAN’ basado en ‘Fortinet Secure SD-WAN’, se proporciona la base para las transformaciones nativas de la nube a escala para mejorar la agilidad y la resiliencia del negocio. El resultado es una solución SASE controlada de extremo a extremo y disponible a nivel global que busca cerrar la brecha entre el usuario y la aplicación.

SIEMENS lanza el ‘PCS neo’ para convertirse en referente en España de la transformación segura de la industria de proceso

Con el objetivo de ayudar a la industria de proceso a competir, Siemens ha anunciado el lanzamiento del ‘PCS neo’, el nuevo sistema de control de la compañía con la que apoyará a las empresas españolas a afrontar su transformación digital. Con el lema “neo Era”, esta plataforma de software se presentó el pasado mes de marzo en sendos eventos, en Madrid y en Barcelona.

La solución destaca por una accesibilidad sencilla, ya que el cliente puede trabajar con ella desde un navegador sin necesidad de tener un programa instalado, lo que facilita que cualquier usuario pueda conectarse de una manera remota e inmediata con la simple utilización de una infraestructura segura.

Otra característica del ‘PCS

neo’, reside en su escalabilidad, ya que al no necesitarse tener instalado el programa en cada ordenador es mucho más fácil adaptar esta plataforma de software al crecimiento y nuevos requerimientos de una planta de procesos. A ello se suma su capacidad colaborativa, puesto que varios miembros de un equipo pueden trabajar a la vez con esta aplicación en paralelo y se agiliza la puesta en marcha de los proyectos y la sensible reducción del *time to market*.

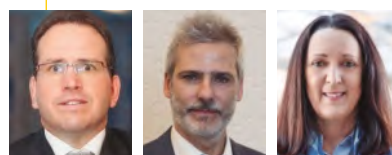
El sistema también cumple con los requerimientos en materia de ciberseguridad en el terreno de la defensa en profundidad y está preparado para poder asignar diferentes permisos a los usuarios en función de sus necesidades.



NOMBRAMIENTOS



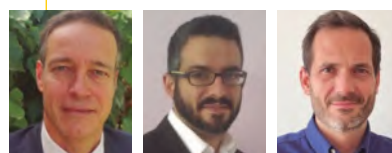
● **Zerolynx** ha ascendido a *Team Leaders* a **Jorge Escabias**, hasta ahora Cyber Security Analyst, y **Francisco Antonio Megía**, que ocupaba el puesto de consultor senior de ciberseguridad. Escabias, matemático, cuenta con una labrada experiencia en el sector, habiendo trabajado para S2 Grupo y Redsys España, entre otras, e impartiendo talleres en RootedCon, HackOn y las Jornadas STIC CCN-CERT. Megía es ingeniero técnico en Informática de Sistemas y Graduado en Ingeniería de Computadores con una amplia experiencia, habiendo formado parte de los equipos de PwC, Eulen Seguridad y SIA.



● **Netskope** ha incorporado a **Manuel Lorenzo** y **Raúl Gordillo**, ambos como Regional Sales Manager, y a **Marilyn Miller**, como Chief People Officer, cargo de reciente creación en la compañía. Lorenzo posee más de una década de experiencia y ha desempeñado diferentes roles comerciales en FireEye, RSA Security, Mercury y EMC, entre otras, y es ingeniero superior en Informática por la Universidad de Málaga. Por su parte, Gordillo cuenta con más de 25 años de experiencia y ha desempeñado roles de responsabilidad en Pentera, CrowdStrike, Forcepoint, Blue Coat y Siemens España, entre otras. Miller, con gran trayectoria en el área de recursos humanos, aporta más de 20 años de experiencia adquirida en empresas como Anaplan, Alfresco, Quotient Technology, Aecom, BMC Software y Cisco Systems, entre otras.



● El distribuidor **Cefiros** se ha reforzado con el fichaje de **Maribel Poyato** como Business Development Manager y Account Manager de Cataluña, Comunidad Valenciana y Baleares. Profesional de reconocida solvencia, ha trabajado para compañías como Tixeo y BlueBottleBiz, entre otras.



● **Ivanti** ha ampliado su equipo incorporando a **Kamel Karabelli**, **Enric Cortés** y **Sacha Muñoz**, como Solutions Architect para España y Portugal, Account Manager y Sales Specialist ESM, respectivamente. Karabelli ha formado parte del equipo de la compañía en el Sur de Europa y ha ocupado diferentes funciones técnicas en las áreas de gestión y ciberseguridad en empresas como Qualys, y en mayoristas como GTI y TowersIT, entre otros, en tanto que Cortés ha ocupado puestos de responsabilidad en Pulse Secure (adquirida por Ivanti), Dell, HP y Deloitte, entre otras. Por su parte, Muñoz ha desempeñado roles de responsabilidad en fabricantes como Nortel Networks, donde desarrolló toda la estrategia de marketing y ventas corporativas para España.



STORMSHIELD

La opción europea de ciberseguridad

¡No pague un ransomware!

Descubra nuestra solución
multicapa de protección
contra el ransomware.



STORMSHIELD
Endpoint Security
Evolution

www.stormshield.com

ENTELGY INNOTECH SECURITY celebra sus dos décadas con más de 250 clientes, entre ellos las principales compañías del IBEX35

En septiembre de 2002, **Félix Muñoz**, actual CEO de **Entelgy Innotech Security**, decidió crear una empresa especializada en la gestión del riesgo y en la seguridad de los sistemas. Con el transcurso de los años, la empresa fue creciendo y con ella el número de organizaciones que reclamaban sus servicios. Su gran salto cualitativo fue el 28 de marzo de 2011, cuando el grupo tecnológico Entelgy entró a formar parte de su capital y comenzó un crecimiento notable.

Así, y ya con la denominación de Entelgy Innotech Security, inició su proceso de internacionalización, estando presente en Argentina, Brasil, Chile, Colombia, México, Perú y Estados Unidos. Ahora, bajo el lema 'Having a good time. The (Cybest) Security Company', celebra su vigésimo cumpleaños "convertida en un referente en el mundo de la ciberseguridad, tanto en España como en Latinoamérica", destacan desde la empresa.

Fruto de su buena salud, la compañía ha pasado de una plantilla inicial de cua-

tro personas a más de 500 empleados altamente cualificados.

Asimismo, tan solo en el ejercicio anterior, dio servicio, a través de su Centro Avanzado de Operaciones de Seguridad (SmartSOC), a 45 nuevos clientes, ascendiendo a más de 250 las organizaciones que confían su seguridad a esta empresa. Entre otras, las principales compañías del IBEX

35 y los organismos públicos españoles e internacionales de referencia, como la OTAN, ONU, OEA, la Agencia Europea de Ciberseguridad (ENISA), CCN y CNI, INCIBE y el Centro Vasco de Ciberseguridad (BCSC).

Es miembro, asimismo, de los principales foros y asociaciones del sector, tanto a nivel nacional como internacional, entre los que destacan el FIRST y CSIRT.es, entre otros. Asimismo, recientemente, entró a formar parte de un proyecto piloto, promovido por el CCN, y que constituye el primer hito del despliegue de la Red Nacional de SOC (Centros de Operaciones de Seguridad).



NOMBRAMIENTOS



● **HomeServe Iberia** ha contratado a **Judit Closa** como Directora de Seguridad de la Información. Con anterioridad ha desempeñado roles de responsabilidad en Habitissimo, Volotea y Deloitte España, entre otras compañías. Es ingeniera de Telecomunicaciones por la Autónoma de Barcelona.



● **Zscaler** ha nombrado a **Paul Eccleston** como Vicepresidente Internacional de Partners y Alianzas, asumiendo la responsabilidad de todos los segmentos del canal. Previamente CEO de Nuvias Group, ha trabajado para empresas como Microsoft, IBM, Cisco, HP, Dell, Symantec, Juniper, Fortinet, VMware, Citrix y Zoom, entre otras.



● **Exclusive Networks** ha ampliado su equipo con la llegada de **Carlos Trinidad** como Business Development Manager para Fortinet, de **Mariana Urreiztieta**, como Directora de RR.HH. para el Sur de Europa, de **Miguel Fernández Pavia** como Business Development Manager y de **Juan Fernando Romero**, en calidad de Account Manager de la zona Este. Trinidad posee una dilatada experiencia de más de 12 años y ha desempeñado roles de distinta responsabilidad en empresas como Factum, Secura, Iseo y Suptratecnología, entre otras. Urreiztieta, licenciada en Derecho, ha trabajado en Criterio, VistaPrint y GetYourHero. Fernández Pavia, ha estado dedicado desde hace más de una década a la seguridad, primero como responsable de la explotación de servicios del SOC y más tarde en la implantación de proyectos de seguridad. Fernando Romero, ha trabajado para Open35 en la parte de desarrollo de negocio y en los últimos años como Key Account Manager.

BABEL anuncia nuevas inversiones en big data, analytics, ciberseguridad, hiper automatización, nube e inteligencia artificial

Tras la adquisición del grupo **Ingenia**, en 2021, incorporando a 400 profesionales, **Babel** ha anunciado nuevas inversiones para 2022 para "mantener un crecimiento orgánico por encima del 20% y alcanzar los

125 millones de euros de cifra de negocio, así como una plantilla en torno a los 2.500 profesionales". Para ello, reforzará de forma notable su apuesta por "aquellas tecnologías que consideramos que son estratégicas y que nos están dando resultados muy positivos, como big data, analytics, ciberseguridad, hiper automatización, nube e inteligencia artificial".

Además, ha anunciado que "si se con-

cretan varias operaciones inorgánicas que la compañía está estudiando de cara a 2022, la cifra de negocio podría incrementarse notablemente, pudiendo alcanzar un crecimiento del 30% con respecto a 2021".

De cualquier forma, su CEO, **Tony Olivero**, ha destacado que la compañía "está alcanzando, año tras año, un mayor conocimiento vertical de los principales sectores de actividad, lo que nos sitúa como el socio tecnológico de preferencia para las grandes compañías. Un proceso de reposicionamiento que, en 2022, queremos hacer tangible con el reciente cambio de marca".

El grupo tecnológico experimentó en 2021 un importante incremento de su negocio: al 20% obtenido en España hay que sumar un crecimiento muy relevante en el resto de las geografías donde opera Babel: 51% en Marruecos, 41% en Portugal, 12% en México y 4% en Chile.

Con el objetivo de fortalecer su canal de partners, **SealPath** ha incorporado a **Sandrine Roux**, como Directora de Canal para el Sur de Europa y a **Patricia Alfaro**, que estará al frente del departamento para Iberia. Roux cuenta con más de 20 años de experiencia en el área comercial y de canal, habiendo trabajado en compañías como Nortel Network, Newell, NTR y Oxford University Press. Por su parte, Alfaro cuenta con más de 23 años de experiencia, habiendo formado parte de empresas como Sage, ADL Technology, SAP y Microsoft.



Con el objetivo de fortalecer su canal de partners, **SealPath** ha incorporado a **Sandrine Roux**, como Directora de Canal para el Sur de Europa y a **Patricia Alfaro**, que estará al frente del departamento para Iberia. Roux cuenta con más de 20 años de experiencia en el área comercial y de canal, habiendo trabajado en compañías como Nortel Network, Newell, NTR y Oxford University Press. Por su parte, Alfaro cuenta con más de 23 años de experiencia, habiendo formado parte de empresas como Sage, ADL Technology, SAP y Microsoft.

Con el objetivo de fortalecer su canal de partners, **SealPath** ha incorporado a **Sandrine Roux**, como Directora de Canal para el Sur de Europa y a **Patricia Alfaro**, que estará al frente del departamento para Iberia. Roux cuenta con más de 20 años de experiencia en el área comercial y de canal, habiendo trabajado en compañías como Nortel Network, Newell, NTR y Oxford University Press. Por su parte, Alfaro cuenta con más de 23 años de experiencia, habiendo formado parte de empresas como Sage, ADL Technology, SAP y Microsoft.



**Inicio de sesión
único SSO**



**Autenticación Multifactor
Adaptativa**



**Gestión del
Ciclo de Vida**



**Acceso al
Sevidor Avanzado**



**Gestión de
Acceso a Apis**



Directorio Universal



Proxy inverso

Okta es una plataforma confiable para proteger todas las identidades. Más de 10.650 organizaciones confían en el software y las API de Okta para iniciar sesión, autorizar y administrar usuarios.

Okta se distribuye en Iberia a través de Ingecom, Value Added Distributor (VAD) especializado en soluciones de ciberseguridad y ciberinteligencia.

Para mayor información sobre las soluciones de identidad de Okta, contáctenos aquí: **info_spain@okta.com**

SYNOPSIS elige a CÉFIROS para potenciar su estrategia en Iberia a través del canal

La compañía **Synopsis** ha cerrado un acuerdo de distribución con **Céfiros** para potenciar su apuesta por el canal y poder tener presencia en todas las regiones de España y Portugal. Para lograrlo, la compañía se apoyará en la red de *resellers* e integradores de Céfiros y empresas desarrolladoras de software. Para Céfiros, la incorporación de Synopsis supone poder completar su portafolio en un área que considera básica con una solución completa para el ciclo de vida del desarrollo software. Asimismo, a través de esta alianza, Synopsis espera poder alcanzar con este acuerdo unas cifras que permitan ayudar a la compañía a alcanzar sus objetivos globales, aportando un equipo comercial y técnico dedicado al territorio, y poder dar soporte y apoyo a los numerosos proyectos que actualmente está desarrollando Synopsis en la región.

Synopsis, reconocida en soluciones de seguridad de aplicaciones (AST),



proporciona herramientas de análisis estático/dinámico/interactivo (SAST, DAST, IAST) y soluciones de análisis de composición de software (SCA) y Fuzz Testing que permiten

a los equipos encontrar y reparar rápidamente vulnerabilidades y defectos en código propietario, componentes de código abierto y comportamiento de la aplicación.

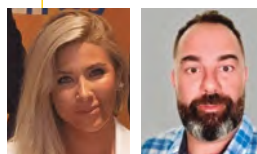
Prueba del buen hacer de Synopsis es que ha sido reconocida como 'líder' en el Cuadrante Mágico de Gartner para pruebas de seguridad de aplicaciones (AST) por quinto año consecutivo. Según la capacidad de ejecución y la visión completa, están posicionados en lo más alto y más a la derecha en el Cuadrante de líderes, siendo pioneros en el desarrollo de la siguiente categoría en la seguridad de aplicaciones: ASOC (*Application Security Orchestration and Correlation*) implementada por nuestro producto único en el mercado CodeDX.

NOMBRAMIENTOS



● **Logicalis** ha promocionado a **Mar Pacheco** como nueva responsable de la Business Unit de Seguridad, y contratado a **Vicente Alcaraz** como

Sales Manager. Pacheco, con una asentada trayectoria en la compañía desde los tiempos de Morse, con anterioridad ha trabajado en Al-Pi e IBM. Por su parte, Alcaraz, licenciado en Geografía e Historia por la Autónoma de Madrid, cuenta con una amplia experiencia y ha trabajado en compañías como Insight, Comsoft Direct, Dell EMC y Hewlett Packard Enterprise, entre otras.



● **Immersive Labs**, la plataforma de preparación cibernética destinada a profesionales técnicos y no técnicos desembarca en España, de la mano de **Virginia**

Santos como Directora de Ventas y **Jorge Ortiz** como Ingeniero de Preventa. Santos, grado en Derecho y Filología, hasta su incorporación venía siendo responsable de ventas de Cipher para el Reino Unido y con anterioridad estuvo en Darkrace. Por su parte, Ortiz cuenta con una sólida trayectoria en formación y responsabilidades técnicas en compañías como CyberReason, Blue Coat (Symantec) y AlienVault.



● **Bitdefender** ha ascendido a Director de Ventas para Iberia a **Sergio Bravo**. Es ingeniero de Telecomunicaciones por la Politécnica de Madrid y ha trabajado en compañías como Kaspersky Lab, HPE, MicroStrategy y McAfee, entre otras.



● **RSA Netwitness** ha fichado a **Vicente Gozalbo** como Enterprise Sales Account Manager para Iberia. Con más de 16 años de solvente experiencia ha trabajado para compañías como Splunk, IBM, Bull, Selestia, BMC

Software y en la empresa matriz de su actual entidad, entre otras.



● **Luis Suárez** ha sido contratado por **Splunk** como Sales Engineer y **Juan Carlos Peña** como Regional Sales Manager. Suárez, reconocido ponente en eventos de ciberprotección, ha trabajado para compañías como Kaspersky, DXC Technology, Symantec y Thomson Reuters, entre otras. Peña, con más de 20 años en el sector, ha trabajado para Zscaler, Symantec y Nortel Networks, entre otras.



● **Lookout** se ha reforzado con **Daniel Villaseñor** como Sales Engineer para Iberia. Es Ingeniero de Telecomunicaciones y posee más de 15 años de experiencia en Networking, IT y Ciberseguridad, desarrollando su carrera en consultoría tecnológica en empresas como Ricoh y Telefónica.

EUROCYBCAR y CENTRO ZARAGOZA suman fuerzas para impulsar certificaciones aplicadas al automóvil

"En 2021 se batió el récord de ciberataques a vehículos de todas las marcas y en todos los países. Es



algo que está sucediendo desde el año 2012: de manera remota -es decir, sin tener contacto directo-, se han robado coches, acelerado y frenado vehículos en marcha o alterado los sistemas y tecnologías incluidos en todo tipo de automóviles", han resaltado desde **Eurocybcar**, que ha firmado un acuerdo con el **Centro Zaragoza**, un instituto de investigación de vehículos participado por 19 entidades aseguradoras. Gracias a esta colaboración, ambas unen sus respectivas áreas de conocimiento para trabajar en favor de la mejora de la seguridad vial y la ciberseguridad de los vehículos. "El convenio se enmarca en esta nueva coyuntura para la automoción y movilidad y supone un gran paso adelante para la

protección de todos, ya que la ciberseguridad entra en el foco de los proyectos de I+D+i en materia

de seguridad vial y seguridad de los vehículos", destacan ambas entidades.

Normativa UNECE/R155

La entrada en vigor de la normativa UNECE/R155, impulsada por la **ONU**, exigirá que todos los vehículos que se homologuen en la **UE** desde el próximo mes de julio sean ciberseguros por ley (debiendo demostrarlo mediante un certificado de ciberseguridad) y, a partir de julio de 2024, todos los que estén en la venta. Por eso, este convenio de colaboración "supone un paso de gigante hacia nuestro objetivo de lograr una ciberseguridad vial", ha destacado la CEO de Eurocybcar, **Azucena Hernández**.

Trend Micro Cloud One™

SEGURIDAD CLOUD SIMPLIFICADA.

No todas las soluciones cloud son iguales. Ayude a sus clientes potenciales a superar la complejidad y genere informes personalizados del valor proyectado de Trend Micro Cloud One con el estudio Forrester Economic Impact.

Conozca más en: trendmicro.com/ForresterTEI



Primer puesto en el informe de IDC global de cuotas de mercado Hybrid Cloud Workload Security de junio de 2021

Con una cuota de mercado del 27,5 %, Trend Micro triplica la del segundo proveedor.



Guía de mercado de Gartner para plataformas de protección de cargas de trabajo en la nube, julio de 2021

En nuestra evaluación del informe, Trend Micro ha determinado que cumplimos con 8 de las 8 recomendaciones.

IBERMÁTICA suma IA a los SOC, junto con VICOMTECH, e impulsa la digitalización de CONSTRUCTORA LOS ÁLAMOS

Ibermática ha elevado, según destaca la compañía “el nivel de los sistemas de ciberdefensa gracias a tecnología de Inteligencia Artificial”. En colaboración con Vicomtech, y a través del proyec-

to IT(SIA)², ha logrado añadir un componente crítico para cualquier Centro de Operaciones de Seguridad (SOC) empresarial, ya que aprovecha el Aprendizaje Automático y el Análisis del Comportamiento para detectar amenazas en toda la cadena de ataques, investigando automáticamente cada alerta y creando un mapa de inteligencia para capacitar a los analistas de seguridad y acelerar la remediación. Así, la compañía aporta a través de este sistema un importante aumento de la capacidad de detección, de comprensión del entorno, de un filtrado del ruido y de la toma de contramedidas oportunas cuando se identifican las amenazas, incluso nunca antes vistas.

Además, también ha ayudado a la Constructora Los Álamos a dar un paso impor-



tante en su digitalización con la implantación de IB Building 365, la solución de Ibermática específica para este sector y el inmobiliario, que le permitirá integrar en una única plataforma sus procesos de gestión de negocio, ganando agilidad y eficiencia. Además de disponer de una extensa funcionalidad, IB Building 365 permite realizar una personalización total del sistema, adaptándose a las necesidades concretas de su cliente. Ubicada en Oviedo y fundada en 1961, Constructora Los Álamos contaba con un sistema de gestión corporativo basado en una AS/400 pero cada departamento de la compañía trabajaba con diversas herramientas (hojas de cálculo, sistemas de seguimiento de presupuestos y control, desarrollos propios...), con lo que la información podía quedar dispersa entre las distintas áreas o departamentos y el anterior sistema ERP sólo cubría parcialmente sus necesidades. Para solventar esta situación y hacer más ágiles y eficientes sus procesos de gestión, Ibermática implantó IB Building 365, basada en el ERP Microsoft Dynamics Business Central.

TRESCORE, consultora de referencia de LEET SECURITY para facilitar la calificación de servicios

Leet Security y Trescore Proyectos, especializada en consultoría del Modelo EFQM, han firmado un acuerdo de colaboración para facilitar que las empresas interesadas en obtener la calificación de ciberseguridad de sus servicios, puedan realizar una adecuación más sencilla y eficaz previa a la calificación. Esto es posible gracias a la experiencia y al amplio conocimiento que tiene la consultora en la metodología desarrollada por Leet Security.



“La experiencia de Trescore en el Modelo EFQM ha permitido la rápida interiorización del significado de la calificación de ciberseguridad, puesto que al igual que ISO 9001 certifica que el Sistema de Gestión de Calidad empleado por la organización es conforme a la normativa, EFQM es un Modelo de Excelencia, un marco de refe-



TRESCORE PROYECTOS
DE INNOVACIÓN TECNOLÓGICA Y EXCELENCIA

rencia, no normativo, cuyo concepto fundamental es realizar diagnósticos del nivel de excelencia de la gestión de las organizaciones”, ha destacado la compañía.

Calificación de BC Digital

Como se sabe, Leet ha sido uno de los principales impulsores en la creación y puesta en marcha de Pinakes, que permite cumplir con los requerimientos normativos de la European Banking Association (EBA) y que, entre otros aspectos, exige a las entidades de crédito una gestión de la ciberseguridad de los servicios externalizados. Así pues, con este acuerdo, Trescore Proyectos suma a su experiencia en auditoría la específica en adecuación de servicios para la obtención de la calificación Pinakes. Precisamente, la empresa BC Digital Services ha sido una de las más recientes organizaciones en conseguirla, con una calificación de ciberseguridad AAA en Pinakes, certificando su buen hacer en este ámbito.

NOMBRAMIENTOS



● Check Point ha reforzado su equipo con la llegada de **Oscar Macazaga** como Senior Channel Account Manager. Con más de 25 años de experiencia, ha desempeñado roles de responsabilidad en mayoristas como Arrow ECS España, Itway y Diode, y compañías como Acronis, entre otras. Estudió agrónomos por la Politécnica de Madrid y cuenta con un MBA por dicha universidad.



● Trend Micro ha contratado como Channel Manager, para focalizarse en el desarrollo de negocios de Cloud Solution Provider, a **Leandro Piovi**. Cuenta con más de 18 años de experiencia, sobre todo, en el ámbito comercial, con foco en el cliente y el desarrollo de socios de negocio. Ha trabajado para Telefónica Cybersecurity & Cloud Tech, entre otras.



● Proofpoint ha fichado a **Rafael González Maza** en calidad de Named Account Manager. Ha trabajado para Logicalis España, NTT, Axians y TecnoCom, entre otras organizaciones, y cuenta con diversas certificaciones tecnológicas.



● Tarlogic ha incorporado a **Miguel Ángel Villafáfila** como Senior Operations Manager dentro de su Área de Operaciones Corporativas y Finanzas. Cuenta con casi 20 años de experiencia en distintas compañías como S21sec, Serem, Ecija Solutions y Telefónica Soluciones, entre otras.



● Kaspersky Iberia ha fichado como Enterprise Partner Account Manager a **Almudena Álvarez**. Diplomada en Ciencias Empresariales cuenta con un Máster en Transformación Digital por el Esic. Con anterioridad, trabajó para Arrow ECS España, Citrix y Diasa Informática.



● Bidaidea ha incorporado como Key Account Manager a **David García**. Fundador de Sec2Crime, ha trabajado para Logista, la Universidad Internacional de Valencia y la Fundación de Estudios Estratégicos e Internacionales, entre otras.



● Palo Alto ha fichado a **Mario Garrido** como Regional Sales Manager. Ha desarrollado su trayectoria profesional en compañías como Fortinet, Telefónica, Innotec System y Satec, entre otras.

THREAT HUNTING

¿Sabes anticiparte a las campañas que amenazan un entorno corporativo?



16%

Crecimiento de reportes de ciberataques en empresas de 2018 a 2019.

140K€

Aumento de pérdidas por ciberataques (sin contar el daño a la marca).

87%

De los ciberataques se realizan en cuestión de minutos.



Aunque se introduzcan nuevas defensas, solo funcionan hasta que se encuentra y explota la próxima debilidad.

¿CÓMO PODEMOS AYUDARTE?

Contamos con un equipo de expertos en Threat Hunting y DFIR, con un extenso historial de detección de incidentes.

Mediante una metodología propia alineada con marcos de referencia (TAHITI y ATT&CK), nuestros expertos realizan campañas de Threat Hunting para obtener visibilidad de las amenazas.

El servicio de Threat Hunting emplea todas las herramientas disponibles en el cliente sin importar el fabricante para ejecutar campañas de Threat Hunting.

El Servicio de Threat Hunting se apoya en las fortalezas de nuestros departamentos DFIR, Threat Intelligence y Counter Threat Intelligence, proporcionando indicadores únicos en las investigaciones.

¡Solicita ya una llamada con un experto en Threat Hunting!



(+34) 916 616 679



www.s21sec.com/es/-threat-hunting-es/

S21 SEC

www.s21sec.com

La UNIVERSIDAD ROVIRA I VIRGILI mejora la gestión y la protección de su infraestructura en la nube

El cambio hacia un modelo de aprendizaje híbrido supone muchas ventajas, pero también hace que las entidades educativas tengan que hacer frente a retos, como el de administrar y gobernar entornos cada vez más complejos. Es el caso de la **Universidad Rovira i Virgili (URV)**, con



más de 2.000 profesionales y 700 departamentos en Tarragona, Reus, Vilaseca, Tortosa y Vendrell, que ha puesto en marcha un ambicioso proyecto para mejorar la gestión y la seguridad de su infraestructura de TI.

El punto de partida era buscar una mejor gestión y seguridad unificada de sus entornos de TI híbridos, que cumpliera sus requisitos funcionales, operativos y de protección. El proyecto, realizado a través de

Tokiota, partner de Microsoft, ha apostado por la plataforma SaaS de gestión híbrida de Azure Arc de la tecnológica, como la solución que cubría sus necesidades de forma más extensa y con un menor coste de implantación e integración con los sistemas de los que ya disponía la Universidad. Así, gracias a ello, ha "unificado en la nube la gestión de sus recursos y cuenta con un entorno más seguro y automatizado, al sustituir trabajo manual por acciones automatizadas, simplificando las operaciones y facilitando la gestión", destacan desde Microsoft, que también recuerda que "este proyecto ha permitido simplificar el gobierno y la administración al ofrecer una plataforma de administración local y multinube coherente, y usando Azure Sentinel, también la gestión de su infraestructura *on premise* y en nube".

ARCO ATLÁNTICO y CYBASQUE suscriben convenios con WOMEN4CYBER SPAIN

Las asociaciones **Women4Cyber Spain** y **Arco Atlántico** firmaron en marzo un acuerdo de colaboración para desarrollar diferentes actuaciones encaminadas a promover y fomentar las disciplinas de Seguridad Digital y Privacidad.

El acuerdo, rubricado por la Presidenta de Women4Cyber Spain, **Eduvigis Ortiz**, y la Presidenta de Arco Atlántico y Directora de Forensic en **Grant Thornton**, **Cristina Muñoz-Aycuens**, se configura como un marco de cooperación mutua y desarrollo de actuaciones conjuntas tendentes a lograr un mejor conocimiento y difusión de diferentes aspectos relativos a la seguridad digital y la privacidad.

Así, esta iniciativa conllevará el desarrollo de diversas actuaciones como la organización de eventos; acciones de información, promoción y divulgación de buenas prácticas,

modelos o marcos de referencia, normas técnicas, etc.; además del fomento de la capacitación en las referidas disciplinas, como palanca para la igualdad, la inclusión y la empleabilidad.

Por otro lado, ambas organizaciones se han comprometido a fomentar y divulgar estudios, informes e investigaciones que ayuden a conocer mejor la seguridad digital y la privacidad, y a desarrollar actuaciones de I+D+i en dichas materias a través de programas conjuntos.

En paralelo, el Presidente de **Cybasque (Asociación de Empresas Vascas de Ciberseguridad)**, **Xabier Mitxelena** y la Presidenta de W4CS también han suscrito un acuerdo para trabajar de manera conjunta y potenciar la incorporación de mujeres en el sector, en la comunidad vasca.



BREVES

■ El **Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco** puso en marcha en febrero su Programa de Ciberseguridad Industrial 2022. En total, destinará 3,5 millones de euros con subvenciones a fondo perdido de hasta 18.000 euros anuales por empresa. Esta ayuda ofrece la oportunidad de contar con los servicios especializados en ciberseguridad de **Talio**, que forma parte de **Cybasque** (Asociación de Empresas Vascas de Ciberseguridad) y cuenta con la certificación ENS (Esquema Nacional de Seguridad) del CCN. Las ayudas se pueden solicitar hasta noviembre de 2022.

■ Los rescates por *ransomware* alcanzaron un nuevo récord en 2021, mientras que las filtraciones de datos también aumentaron, según un informe de **Palo Alto Networks** a través de su negocio de consultoría de seguridad **Unit 42**. En él, se alerta de que el pago medio por este tipo de ataques se incrementó un 78% hasta alcanzar los 490.000 euros, mientras que las demandas de los cibercriminales crecieron un 144% hasta más de dos millones de euros, de media. El grupo de delincuentes más activo fue Conti, según el estudio, con una quinta parte de los ataques registrados, seguido por REvil, Hello Kitty y Phobos. Como curiosidad, según una investigación de **Splunk**, las empresas tienen solo 43 minutos para mitigar los ataques de *ransomware* una vez que ha comenzado el cifrado. De hecho, sus investigadores llegaron a detectar variantes capaces de cifrar 100.000 archivos, de 53 Gb, en solo cuatro minutos.

■ La **Asociación Española de Normalización (UNE)** ha publicado su primer informe del Observatorio de Vigilancia de Mercado en el que analiza su situación, en relación con el cumplimiento normativo y legislativo que busca evitar la comercialización de productos y servicios inseguros que provoquen un perjuicio a la economía y a los consumidores. Entre sus datos más llamativos destaca que las principales inconformidades se producen en juguetes (10,9%), seguidos de equipos de protección individual (8%), pequeño material eléctrico (7,2%), muebles (5,8%), textiles (4%) y calzado (3,7%).

El tipo de infracción más frecuente en la fabricación y comercialización de productos está vinculado a incumplimientos de las normas técnicas y las condiciones de venta, representando el 53,9%, seguido de las transacciones comerciales (7,6%), los precios (7,3%), y el fraude en peso (0,01%).

■ La Fundación **i2CAT** se incorporó, en marzo, a la **Red Española de Excelencia en Investigación en Ciberseguridad (RENIC)**. Se trata de un centro CERCA de investigación e innovación en tecnologías digitales avanzadas ubicado en Barcelona. Desde 2003, ha impulsado la sociedad digital del futuro a través del conocimiento generado en el desarrollo de proyectos y actividades de I+D+i en campos como la ciberseguridad, 5G, IoT, VR y tecnologías inmersivas, *blockchain*, inteligencia artificial y *New Space*, entre otras.

■ La empresa asturiana **Grupo CIES** se ha incorporado a **CSIRT.es**. Esta última es una organización pública, sin ánimo de lucro, en la que ya hay integradas más de 30 entidades, públicas y privadas para "proteger el ciberespacio español, intercambiando información y actuar de forma rápida y coordinada ante cualquier incidente que pueda afectar simultáneamente a distintas entidades en nuestro país". En www.revistasic.es se ofrece información actualizada de los integrantes tanto de CSIRT.es, como de los principales foros de este tipo de equipos como **FIRST**, **Trusted-Introducer** o el registro que ofrece **Enisa**.



Exclusive
Training Centre

ETC

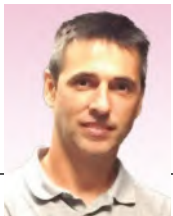
Nuevo centro de formación de Exclusive Networks.

Toda la formación, en remoto o presencial,
acreditada por los fabricantes.

Visítanos en:
www.training.exclusive-networks.com/es-ES

EMASA protege su información crítica unificando el control y la monitorización de logs y alertas

EMASA, la Empresa Municipal de Aguas de Málaga, de la mano del proveedor de servicios tecnológicos Nunsys, se ha embarcado en implantar el primer piloto del proyecto de protección de la información utilizando tecnología Microsoft y la plataforma SafeCloud. Esta plataforma, del fabricante Singlar Innovación, unifica el control y la monitorización de logs y alertas que proporcionan las herramientas IRM, DLP y MDM en un único panel centralizado fácilmente accesible para el CIO o DPO de la organización.



Jesús Doña / Pablo Borches

El Ayuntamiento de Málaga creó **EMASA** en 1986 con el objetivo de acercar la gestión del agua a la población del municipio, pasando ser de una mera empresa suministradora de agua en sus inicios a consolidarse como compañía de gestión del ciclo integral del agua que cuenta actualmente con 430 empleados.

Este proyecto piloto consiste en proteger la información que se distribuye y almacena dentro de la organización y también fuera de ella, así como asegurar el cumplimiento normativo y mantener en todo momento la trazabilidad de los documentos críticos. Esto implica controlar los permisos de accesos sobre los mismos, así como conocer en todo momento quién, cuándo y cómo accede a ellos. Además, se permite limitar el acceso a la documentación a personas que hayan dejado de trabajar en la empresa o a colaboradores externos que ya no lo sean.

Para llevar a cabo el objetivo, EMASA y **Nunsys** han apostado por SafeCloud, la plataforma de gobierno de la información del fabricante Singlar Innovación, la cual unifica el control y la monitorización de logs y alertas que proporcionan las herramientas IRM (*Information Rights Management*), DLP (*Data Leak Prevention*) y MDM (*Mobile Device Management*) en un único panel centralizado fácilmente accesible para el CIO o DPO de la organización.

Con SafeCloud, EMASA puede gobernar desde un único lugar toda la información por ella generada y gestionada, y proporciona informes muy valiosos para los concernidos los ámbitos de TI y privacidad a la hora de gestionar la evolución correcta del proyecto, el buen uso de la información por parte de los usuarios, cualquier fuga de información o mal uso de datos sujetos a RGPD, en definitiva, el portal que siempre ha faltado al DPO y al CIO

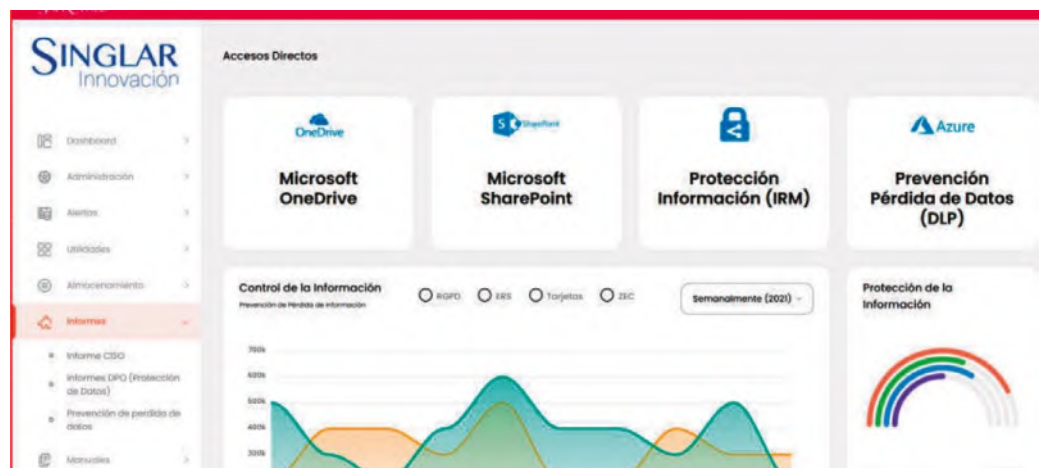


para demostrar una gestión proactiva del gobierno de la información.

En esta fase del proyecto se seleccionó como herramienta IRM el Azure Information Protection,

Microsoft y de Singlar Innovación, y actualmente está certificada con ENS de nivel alto, contando asimismo con las certificaciones de las normas ISO 27001 e ISO 20000.

Finalmente, cabe destacar que también fueron valoradas las certificaciones MS-500 y AZ-900 de su equipo de técnicos e ingenieros. ■



dada la fuerte integración que tiene esta herramienta con el ecosistema de soluciones ofimáticas de Microsoft, con lo que el impacto en la productividad del trabajador cuando la herramienta se pone en funcionamiento es prácticamente nula.

Es de resaltar que Nunsys, en tanto integrador de referencia, cuenta con un acuerdo de distribución de las mencionadas soluciones de

JESÚS DOÑA

Responsable de Infraestructura, Soporte y Ciberseguridad
EMASA

PABLO BORCHES

Senior Business Development Manager
NUNSYS

Netskope Security Service Edge

Seguridad de la nube,
los datos y la red



Netskope.com/es

MUSEO NACIONAL DEL PRADO: gestión avanzada continua y proactiva de las ciberamenazas

Si al aumento de ciberataques que hemos sufrido estos últimos años con el impulso de la digitalización que ha provocado la pandemia, le sumamos la presión extra que supone la inestabilidad geopolítica derivada del conflicto ucraniano, la situación en materia de ciberseguridad está más tensa que nunca. Y tanto pequeñas instituciones públicas como grandes ministerios han sufrido los devastadores efectos de los ciberataques causados por correos maliciosos, suplantaciones de identidad o ataques de *ransomware*, entre otros. Para gestionar las ciberamenazas, el Museo Nacional del Prado (MNP) ha optado por los servicios especializados de ICA Sistemas y Seguridad combinados con la plataforma MÓNICA NGSIM de esta compañía española.



Alberto Cañadas

Los equipos de ciberseguridad deben hacer frente al creciente volumen y sofisticación de las amenazas, pero la falta de visibilidad de la red, los análisis manuales que consumen mucho tiempo y la falta de contexto, afectan negativamente a la eficiencia de los equipos. En el caso del **Museo Nacional del Prado (MNP)**, su necesidad principal era potenciar la recogida de *logs* y la seguridad TIC de sus principales sistemas informáticos, comunicaciones y de seguridad perimetral. Esta institución tenía como objetivo mejorar los sistemas y procesos de información para corregir carencias y, para ello, buscaba un SIEM para correlacionar eventos potencialmente peligrosos para la seguridad de los sistemas de información del Museo.

Además, el MNP necesitaba una herramienta que le permitiera evidenciar digitalmente cualquier incidente de seguridad que se pudiera producir en sus instalaciones y responder a cualquier requerimiento de evidencia o respuesta a un incidente de seguridad TIC que pudiera tener lugar. Por otro lado, contaba con diferentes tecnologías tradicionales de seguridad que no estaban conectadas entre sí, por lo que el equipo de seguridad no podía tener una visión completa, ya que recibía muchos datos independientes que son difíciles de interpretar de forma individual. De esta manera, también surge la necesidad de contar con una herramienta que centralice toda la información y que pueda brindar visibilidad para detectar y proteger de ataques avanzados a este organismo.

Para abordar todos estos retos tecnológicos, el MNP determinó que la herramienta que mejor se adaptaba a sus necesidades era el NGSIM que ofrece el CCN-CERT en su catálogo de soluciones, Mónica NGSIM, ya que cumplía todas las características de interés buscadas. Desarrollado por el equipo de **ICA Sistemas y Seguridad**, se trata del único NGSIM nacional y europeo certificado *Common Criteria* y producto cualificado y aprobado por el Centro Criptológico Nacional.

Mónica NGSIM es un sistema automatizado de gestión de información y eventos de seguridad que recoge en una única plataforma toda la información existente sobre amenazas potenciales, permitiendo no solo reaccionar ante los ataques, sino prevenirlos. El NGSIM del CCN-CERT triplica la productividad de un equipo tipo de ciberseguridad y permite alcanzar un retorno de la inversión completo en solo cuatro meses.

Una visión completa y real del ciberestado de la infraestructura tecnológica

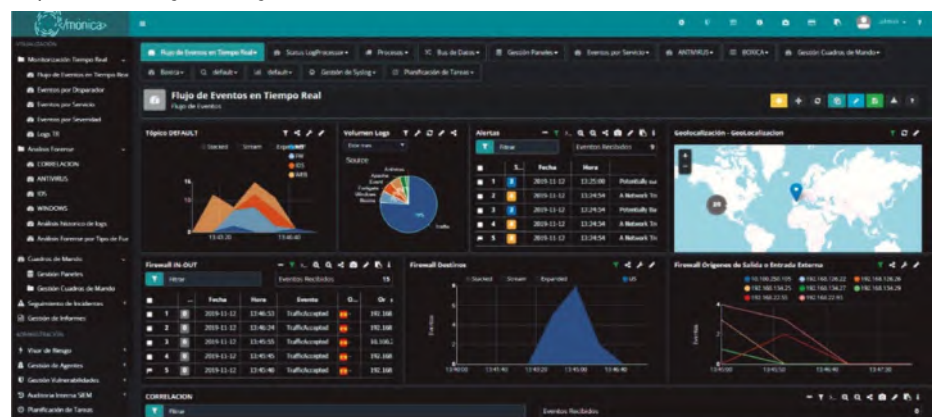
Mónica NGSIM consume cantidades masivas de datos que proceden de fuentes técnicas, investigaciones, fuentes abiertas, fuentes ocultas, redes sociales, fuentes internas y de terceros. Una vez recogida toda esta información, la agrega, analiza y contextualiza en un único lugar. Ayudado por el aprendizaje automático y la automatización, Mónica NGSIM consigue analizar más de 100.000 eventos por segundo, frente a los 4.800 eventos que una persona es capaz de procesar en un día. Sus capacidades SOAR facilitan la orquestación entre múltiples fuentes, reducen los falsos positivos, permiten establecer un triaje y una priorización de incidentes y facilitan la respuesta automática ante amenazas conocidas.

La gestión de la seguridad de Mónica NGSIM tiene en cuenta tres estadios temporales -el histórico de eventos, la acción en tiempo real y la acción preventiva- y permite la monitorización de eventos de cualquier dispositivo, sistema o aplicación. Entre los agentes intranet, se pueden encontrar dispositivos de seguridad lógica, de electrónica de

red, servidores web, sistemas gestores de bases de datos, sistemas operativos y de seguridad de Host o aplicaciones propietarias. Por otro lado, los portales web de clientes y proveedores, aplicaciones *cloud-store* y aplicaciones no corporativas, se encuentran entre los agentes extranet, mientras que los agentes ambiente incluyen redes sociales, páginas web y blogs, sistemas de información no TIC y dispositivos de seguridad física.

La recopilación, análisis y entrega automatizada de datos proporcionan inteligencia en tiempo real a escala. Mónica NGSIM emplea las técnicas más avanzadas de recopilación y análisis de datos, como el aprendizaje automático, la ciberinteligencia de amenazas y el análisis del comportamiento del usuario (UEBA).

De esta manera, el Museo del Prado pretende reducir el tiempo de trabajo que los equipos TIC internos dedican a la resolución de incidentes de seguridad y promover una gestión más eficaz de las alertas sobre ciberamenazas que afecten potencialmente a sus sistemas de información, además de dar una respuesta rápida a aquellas que lleguen a materializarse, permitiendo que sus esfuerzos se concentren en otras tareas.



Uno de los objetivos del MNP es reducir el tiempo de trabajo que los equipos TIC internos dedican a la resolución de incidentes y promover una gestión más eficaz de las alertas sobre ciberamenazas que afecten potencialmente a sus sistemas de información, además de dar una respuesta rápida a aquellas que lleguen a materializarse, permitiendo que sus esfuerzos se concentren en otras tareas.



HORNETSECURITY

No te preocupes por



PHISHING, RANSOMWARE O BACKUP PARA MICROSOFT 365

¡Ese es **NUESTRO** trabajo!

Funcionalidades de 365 Total Protection



Hornetsecurity es el principal proveedor de seguridad en la nube de correo electrónico y backup para Microsoft 365. Benefíciate del filtrado de spam y virus, del archivado conforme a la ley, de la protección avanzada contra amenazas, de la continuidad del correo electrónico, de las firmas y disclaimers. Nuestra suite de seguridad "todo en uno" incluye incluso backup y recuperación de datos para Microsoft 365 y los puestos de usuario.

¡PROTÉGETE!

www.hornetsecurity.com

En virtud del uso de esta plataforma, el equipo de seguridad del MNP puede centrarse en lo que realmente importa y sus analistas pueden identificar amenazas a una velocidad 10 veces mayor, ayudando a resolver incidentes un 63% más rápido. Con Mónica NGSIM, la eficiencia de los equipos de seguridad aumenta en un 32% y son capaces de identificar un 22% más de amenazas antes de lleguen a causar graves consecuencias.

MÓNICA, el NGSIM de referencia de la Administración Pública

El Museo Nacional del Prado se une así a las diferentes instituciones públicas locales, autonómicas y estatales que ya confían en Mónica NGSIM, como los ministerios de la Presidencia y Asuntos Económicos y Transformación Digital, las Diputaciones de Castellón y Barcelona o HAZI. En total, más de 50 organismos públicos ya disfrutan de esta plataforma y de los servicios de ciberseguridad de ICA Sistemas y Seguridad.

Mónica NGSIM es un producto certificado en sus funcionalidades de seguridad, clasificado en el Esquema Nacional de Seguridad (ENS) con categoría Alta que lo habilita para ser empleado en sistemas afectados por el ENS en cualquiera de sus niveles: Alto, Medio y Básico. Además, está incluido en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) y permite la integración con otras soluciones del CCN-CERT como Carmen, Lucía, Pilar, Claudia, SAT-INET, Reyes e Inés.

Servicios de ciberseguridad avanzados con el CiberSOC de ICA SyS

Pero si disponer de una herramienta NGSIM es casi imprescindible hoy en día, contar con personal experto lo es aún más para poder hacer un uso eficaz de ella. Además de confiar en la herramienta del CCN desarrollada por ICA, el Museo Nacional del Prado ha apostado por sus servicios del CiberSOC para la gestión de incidentes y ciberamenazas.

Los expertos del CiberSOC de ICA ofrecen al MNP el servicio de detección y respuesta en modalidad 24x7. A través de este servicio, monitorizan eventos de seguridad gracias a la plataforma Mónica NGSIM, realizan correlación y análisis de eventos, se encargan de la operación y notificación de alertas de seguridad e incluso de la coordinación de respuestas e incidentes. En este sentido,

el CiberSOC también gestiona los eventos e incidentes de seguridad del Museo. El equipo de ICA SyS ofrece respuesta ante incidentes que engloba la notificación de los detectados, así como su gestión completa, trabajando de forma alineada junto a los responsables de seguridad TIC, sistemas y redes del MNP y coordinando las actuaciones necesarias sobre los sistemas o redes que lo requieran.

Un CiberSOC altamente cualificado

Al margen de las certificaciones ISO 9000/27000/20000 y ENS categoría Alta con las que cuenta ICA, su CiberSOC es miembro de los foros y organizaciones más relevantes en el campo de la ciberseguridad a nivel nacional e internacional, FIRST, CSIRT, CERT y TF-CSIRT. Además, el equipo de ICA SyS trabaja activamente de la mano de los principales organismos gubernamentales encargados de la ciberseguridad nacional, como el INCIBE y CCN-CERT, para que las empresas nacionales y las organizaciones gubernamentales puedan operar de forma segura, minimizando el riesgo de ciberataques.

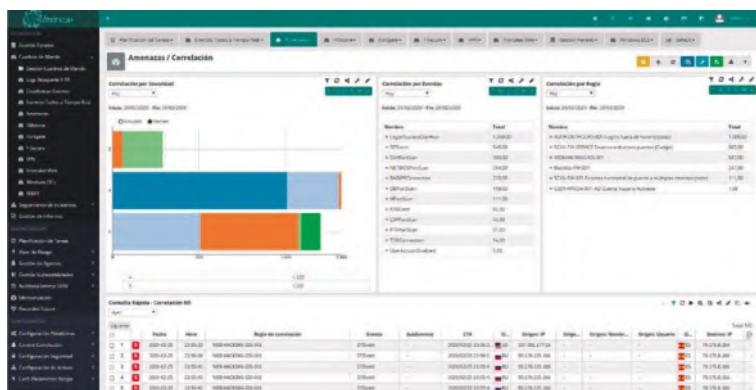
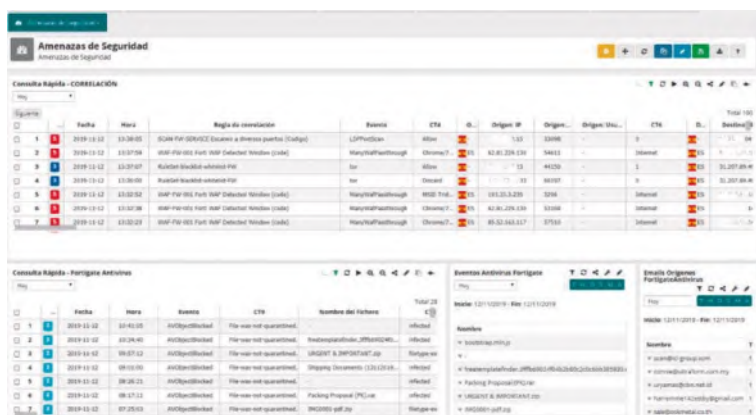
Así, Mónica NGSIM y el CiberSOC de ICA Sistemas y Seguridad forman una robusta defensa para la lucha contra la ciberdelincuencia. Mónica NGSIM es el ojo de halcón que permite ver el ecosistema completo de aplicaciones conectadas a la red en tiempo real de forma centralizada. Recopila y analiza eventos y datos contextuales y detecta más de 100.000 eventos por segundo. Además, proporciona al equipo de seguridad el contexto necesario para tomar decisiones eficientes ante amenazas desconocidas. Las ventajas de esta plataforma, junto al equipo de expertos que forman

el CiberSOC, proporcionan al Museo del Prado una gestión avanzada continua y proactiva de su ciberseguridad. ■

ALBERTO CAÑADAS

Gerente de Ciberseguridad – Preventa y Desarrollo de Negocio
BU-Ciberseguridad

GRUPO ICA SISTEMAS Y CIBERSEGURIDAD



Los expertos del CiberSOC de ICA Sistemas y Seguridad ofrecen al MNP el servicio de detección y respuesta en modalidad 24x7, a través del cual monitorizan eventos de seguridad mediante el uso de la plataforma MÓNICA NGSIM, realizan correlación y análisis de eventos, se encargan de la operación y notificación de alertas de seguridad y participan en la coordinación de respuestas a incidentes.



NO ES LA VULNERABILIDAD. ES EL VECTOR COMPLETO.



Validación Automatizada de Seguridad™

Pentera identifica la verdadera exposición al riesgo para que puedas centrarte en ese 5% de puntos débiles que constituyen el 95% del riesgo real.

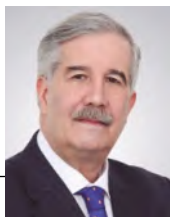
Pon Pentera a Prueba

www.Pentera.io



PENTERA

El mundo ha cambiado. El estándar internacional ISO/IEC 27002, también



El mundo ha cambiado. Las distintas crisis que estamos viviendo junto a los escenarios tecnológicos hacen que la ciberseguridad y la privacidad de las organizaciones se refuercen constantemente. Consecuencia de esto, ISO acaba de publicar la actualización de su estándar de controles de seguridad – ISO/IEC 27002. Desde AENOR, damos las principales claves para entender y aplicar este nuevo estándar.

Boris Delgado Riss / Carlos Manuel Fernández

Estamos inmersos en tiempos muy convulsos donde convivimos con una multitud creciente de riesgos y amenazas. Es el caso de la reciente invasión de Rusia a Ucrania, con un modelo de guerra híbrida (física y virtual) que está teniendo graves consecuencias, algunas de ellas aún imprevisibles; la crisis energética y la de la cadena de suministro, con un impacto negativo directo a las organizaciones y ciudadanos. Y, sin duda, la crisis sanitaria global provocada por el Covid-19 con una huella permanente en la sociedad, los gobiernos y las empresas desde hace ya dos años, y que ha cambiado la forma trabajar y relacionarse entre las organizaciones y personas.

A pesar de estos escenarios, el avance y evolución de las TIC no ha cesado en los últimos años y la transformación digital está suponiendo

IEC 27002 - Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de Seguridad de la Información. En las siguientes líneas desglosamos las principales novedades y cambios de esta nueva versión del estándar.

ASPECTOS CLAVE DE LA NUEVA ISO 27002: ANTESALA DE LA NUEVA ISO 27001

Como es por todos conocido, y con más de 15 años de historia, la ISO/IEC 27002 es una norma no certificable que ha sido una guía de implantación de controles de seguridad de la información. De hecho, está incluida en el Anexo de la ISO/IEC 27001 Sistema de Gestión de Segu-

- Cambio de nombre del comité técnico de ISO que lo desarrolla y el nombre del estándar.
- Nueva estructura, considerando “temas” de seguridad de la información.
- Nueva estructura, considerando “atributos” de los controles.
- Nuevos controles e integración de otros, desde la anterior versión de ISO/IEC27002:2013.

Veámoslos con más detalle:

1. Cambio de nombre. Esta norma/estándar se ha actualizado en el comité técnico SC27 - Seguridad de la Información, Ciberseguridad y Protección de la Privacidad-, con un nuevo nombre: “*Controles de Seguridad de la Información*” en vez de “*Código de Prácticas para Controles de Seguridad de la Información*”.

2. Nueva estructura: Temas/ Temáticas en Seguridad de la Información. Como recordaremos, la anterior versión de ISO/IEC 27002:2013 se estructuraba en 14 dominios, 35 objetivos de control y 114 controles. La nueva versión se estructura en 4 temas/temáticas, eliminando el concepto de Objetivo de Control, y reduciéndose a 93 controles. (Ver Figura 1).

3. Nueva estructura: Atributos de los controles. Los atributos son una novedad en esta versión

ISO/IEC 27002:2013 (114 controles)		ISO/IEC 27002:2022 (93 controles)	
DOMINIO	6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	TEMA	5. CONTROLES ORGANIZACIONALES (37 controles)
OBJETIVO DE CONTROL	6.1 ORGANIZACIÓN INTERNA	TEMA	6. CONTROLES DE PERSONAS (8 controles)
CONTROL	6.1.1 Roles y Responsabilidades en Seguridad de la Información	TEMA	7. CONTROLES FÍSICOS (14 controles)
...	...	TEMA	8. CONTROLES TECNOLÓGICOS (34 controles)
CONTROL	6.1.5 Seguridad de la Información en la Gestión de Proyectos	ANEXO A. ATRIBUTOS	
OBJETIVO DE CONTROL	6.2. DISPOSITIVOS MÓVILES Y TELETRABAJO	ANEXO B. RELACION ISO 27002:2013 – ISO 27002:2022	
CONTROL	6.2.1 Política de Dispositivos Móviles		
CONTROL	6.2.2 Teletrabajo.		
...	...		

Figura 1.- Comparativa de la anterior y actual versión de ISO/IEC 27002

do también un profundo cambio en las organizaciones, en las industrias y en la sociedad. El despliegue de nuevos escenarios tecnológicos como SMAC (*Social-Mobility-Analytics-Cloud*), el desarrollo de la Industria 4.0 (OT-Tecnologías de la Operación + IoT-Internet de las Cosas) y la consideración en la mejora de los sistemas de comunicación como 5G, así como el avance en inteligencia artificial y *machine learning*, requieran de herramientas e instrumentos que combatan las nuevas ciberamenazas y ciberriesgos.

Así, se pone de relevancia que las TIC, su ciberseguridad y privacidad, son los retos que en este momento y a futuro, hay que priorizar. De hecho, la digitalización está muy presente en los fondos Next Generation EU, el instrumento con el que se apoya la recuperación económica tras la crisis provocada por el Covid-19.

Ante todo esto, ISO a través de su comité técnico internacional ISO/IEC JTC 1/SC 27, tomó cartas en el asunto y en febrero de 2022 publicó la actualización de uno de sus estándares técnicos más reconocidos y utilizados: la ISO/

riedad de la Información (SGSI), que sí es certificable, como referencia de controles de seguridad que hay que aplicar, según el análisis de riesgos y conforme a la mejora continua. De hecho, a la luz de la nueva publicación de la ISO/IEC 27002 se actualizará también durante el primer semestre de 2022.

La ISO/IEC 27002 proporciona un conjunto de controles generales de seguridad de la información, contemplando para cada uno de ellos una guía de implementación. Se ha diseñado para ser utilizada por las organizaciones públicas y privadas de tres posibles formas: en el contexto de un SGSI basado en la norma ISO/IEC 27001 (en su Anexo A de controles para actualizar los 114 a 93 controles); para implementar controles de seguridad de la información basados en las mejores prácticas reconocidas internacionalmente; para desarrollar sus propias directrices de gestión de la seguridad de la información;

Esta nueva versión de ISO/IEC 27002 trae interesantes cambios, principalmente en la estructura de la norma/estándar, y son:

de la norma. Como se indica en su Anexo A, los atributos son una forma de crear diferentes vistas/agrupaciones de los controles para permitir mayor legibilidad al usuario. Es decir, a cada control se le caracteriza con cinco atributos, lo que permite clasificar/agrupar/filtrar los mismos.

Los cinco atributos de cada control son:

- **Tipo de Control.** Permite clasificar los controles en función de su relación con los riesgos, amenazas e incidentes de seguridad. Así define tres posibles valores para el atributo: *Preventivo* (control que actúa antes de un incidente), *Detectivo* (control que actúa durante el incidente) y *Correctivo* (control que actúa después del incidente).

- **Propiedades de Seguridad de la Información.** Permite clasificar los controles en función de cómo contribuye a la protección de las tres propiedades de la seguridad de la información (y que como sabemos, son utilizadas en el análisis de riesgos de la ISO/IEC 27001). Define tres posibles valores para el atributo: Confidencialidad, Integridad y Disponibilidad.



Business focused cybersecurity

Ingenia es la división de ciberseguridad de Babel.

Nace con casi 30 años de presencia en el mercado y cerca de 600 proyectos de ciberseguridad en más de 200 clientes por todo el mundo.

Con nuestros servicios y profesionales certificados, seremos tu socio estratégico en cumplimiento normativo y gestión de riesgos, despliegue de tecnologías de seguridad, seguridad gestionada, ciberinteligencia, entornos OT y desarrollo seguro.



Ingenia

Babel Cybersecurity

www.babelgroup.com/ingenia

esSOC
Centro de Operaciones
de Seguridad

esSOC
INDUSTRIAL



CSIRT.es



• **Conceptos de Ciberseguridad.** Permite clasificar los controles para determinar su relación con los cinco conceptos del marco de ciberseguridad descritos en ISO/IEC TS 27110:2021, y que a su vez son los propuestos por el *framework* de ciberseguridad del NIST – (NIST SP 800-53/171). Define cinco posibles valores para el atributo: Identificar, Proteger, Detectar, Responder y Recuperar.

• **Capacidades Operacionales.** Permite clasificar los controles desde el punto de vista de los responsables de su implantación y/o mantenimiento. Define 15 posibles valores para el atributo: Gobernanza, Gestión de Activos, Protección de la Información, Seguridad en los Recursos Humanos, Seguridad Física, Seguridad en sistemas y Redes, Seguridad en Aplicaciones, Seguridad en la Configuración, Gestión de Accesos e Identidades, Gestión de Amenazas y Vulnerabilidades, Continuidad, Seguridad en Relaciones con Proveedores, Legal y Cumplimiento, Gestión de Eventos de Seguridad de la Información, Aseguramiento de la Seguridad. Este atributo recuerda a cómo se agrupaban los controles y objetivos de control en dominios en la anterior versión de ISO/IEC 27002:2013,

• **Dominios de Seguridad.** Permite clasificar los controles considerando el campo de aplicación de la seguridad de la información y ciberseguridad, su conocimiento, servicios y productos relacionados. Define cuatro posibles valores para el atributo: Gobernanza y Ecosistema, Protección, Defensa y Resiliencia.

Conforme al Anexo A.1 de la norma, podemos ver un ejemplo no exhaustivo de los primeros controles y sus atributos: (Ver Figura 2).

En definitiva, los temas y atributos se proporcionan para permitir organizar y estructurar los controles a través de vistas/agrupaciones que le interese al usuario.

Adicionalmente, en el desarrollo de cada control se complementan con la siguiente información, haciéndolo más útil y robusto a la hora de implementarlo:

- **Título del control:** Nombre corto del control.
- **Tabla de atributos:** Una tabla muestra los valores de cada atributo para cada control.
- **Control:** Descripción del control.
- **Finalidad:** Texto descriptivo de la finalidad del control.
- **Orientación:** Guía de implementación del control.
- **Otras informaciones:** Texto explicativo o referencias a otros documentos relacionados.

4. **Nuevos controles e integración de otros, desde la anterior versión de ISO/IEC 27002:2013.** La nueva versión contempla en su Anexo B dos tablas de doble entrada, muy útiles para trazar los controles de la versión anterior a la nueva, y viceversa. Concretamente, los cambios son:

• **Nuevos controles (11).** Se destacan, entre otros, los controles de “Inteligencia de Amenazas”, “Filtrado Web” e incluso un control que se eliminó en la versión del 2013, y se recupera en esta nueva versión: “Prevención de fuga de datos”.

Id. Control ISO/IEC 27002	Nombre del Control	Tipo de Control	Propiedades de Seg. Info.	Conceptos de Ciberseguridad	Capacidades Operacionales	Dominios de Seguridad
5.1	Políticas de seguridad de la información	#Preventivo	#Confidencialidad, #Integridad, #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza y Ecosistema #Resiliencia
5.2	Funciones y responsabilidades de seguridad de la información	#Preventivo	#Confidencialidad, #Integridad, #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza y Ecosistema #Protección #Resiliencia
5.3	Segregación de funciones	#Preventivo	#Confidencialidad, #Integridad, #Disponibilidad	#Proteger	#Gobernanza	#Gobernanza y Ecosistema
5.4	Responsabilidades de gestión	#Preventivo	#Confidencialidad, #Integridad, #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza y Ecosistema
5.5	Contacto con autoridades	#Preventivo #Correctivo	#Confidencialidad, #Integridad, #Disponibilidad	#Proteger #Responder #Recuperar	#Gobernanza	#Defensa #Resiliencia
5.6	Contacto con grupos de interés	#Preventivo #Correctivo	#Confidencialidad, #Integridad, #Disponibilidad	#Proteger #Responder #Recuperar	#Gobernanza	#Defensa
5.7	Inteligencia de amenazas	#Preventivo #Detectivo	#Confidencialidad, #Integridad, #Disponibilidad	#Identificar #Detectar	#Gestión de Amenazas y Vulnerabilidades	#Defensa #Resiliencia
5.8	Seguridad de la información en la gestión de proyectos	#Preventivo	#Confidencialidad, #Integridad, #Disponibilidad	#Identificar #Detectar	#Gobernanza	#Gobernanza y Ecosistema #Protección

Figura 2.- Estructura de Atributos para Controles en ISO/IEC 27002

• **Integración y reagrupación de controles (30).** Se ha realizado un esfuerzo en agrupar e integrar controles, dando un carácter más homogéneo. Así, por ejemplo, los controles de “Política de control de acceso” y “Acceso a las redes y a los servicios de red” se fusionan en: “Control de Accesos”. O por ejemplo, los controles “Política

estado del arte de las actuales (y futuras) ISO, leyes y reglamentaciones españolas y europeas en materia de Ciberseguridad (como son el nuevo Esquema Nacional de Seguridad, el actual Reglamento General de Protección de Datos Personales, y la futura Directiva NIS2, la regulación DORA, o Cybersecurity Act, etc.).

Es decir, esta plataforma de confianza ofrece un modelo eficaz y eficiente basado en las mejores prácticas, los estándares ISO que han sido consensuados por expertos de 155 países, y dotan de una mayor visión y capacidad de reacción a la ciberseguridad. (Ver Figura 3).

Desde AENOR consideramos que esta nueva ISO/IEC 27002. y la inminente modificación en el Anexo A de la ISO/IEC 27001-SGSI, permitirá seguir disponiendo de una herramienta muy potente y actualizada de ciberseguridad que contribuye a la mejora de seguridad digital en las organizaciones.

Recordemos que el hito conseguido por todas las organizaciones que han confiado desde hace años en las certificaciones ISO/IEC 27001; y es que, en su último informe de ISO, España se sitúa en el *top ten* de países del mundo por número de certificaciones: AENOR, con más del 50% de estas.

Por último, no debemos olvidar que los estándares de ciberseguridad deben aportar soluciones a las organizaciones que las implantan (y certifican), y considerar los retos que ya están sobre la mesa: *blockchain*, *BigData*, *Edge-computing*, etc. y su relación con la Inteligencia Artificial, modelos matemáticos, datos y algoritmos que decidirán sobre cómo actuar ante una crisis como la actual y las que puedan venir. ■

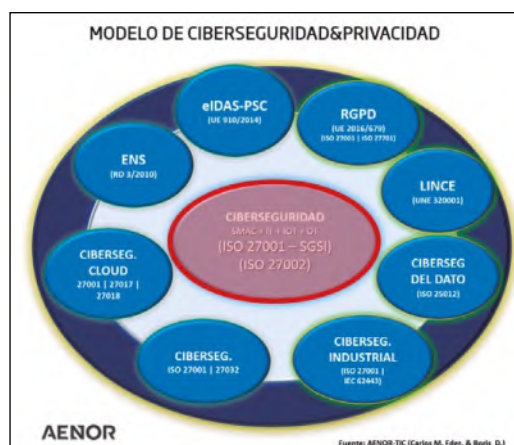


Figura 3.- Modelo de Ciberseguridad y Privacidad de AENOR.

de dispositivos móviles” y “Equipo de usuario desatendido”, se fusionan en el control: “Dispositivos de punto final del usuario”.

CONFIANZA EN LA CIBERSEGURIDAD A TRAVÉS DE LAS NORMAS Y ESTÁNDARES ISO

AENOR, fiel a su propósito de aportar soluciones que generen confianza entre organizaciones y personas, y ante los escenarios tecnológicos anteriormente presentados, diseñó la plataforma de confianza: “Proteger la Seguridad y Privacidad de los datos”. Esta se apoya en el modelo de ciberseguridad y privacidad de AENOR basado en estándares internacionales ISO, tomando como pilares fundamentales la ISO/IEC 27001 e ISO/IEC 27002; así como en el

BORIS DELGADO RISS

CISA, CISM

Director de Soluciones de Digitalización y Tecnología
bdelgado@aenor.com

CARLOS MANUEL FERNÁNDEZ

MBA, CISA, CISM

Asesor Estratégico de TI
cmfernandez@fidesol.org

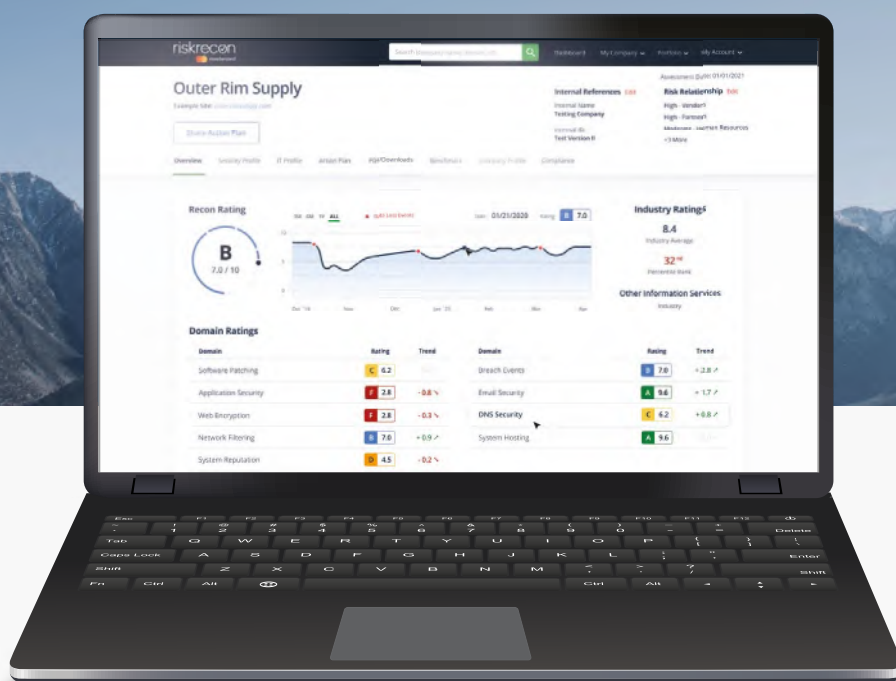
AENOR

Proteja su cadena de suministro digital

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

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

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



riskrecon  mastercard

CIC4Cyber en Cataluña: conocimiento, innovación y ecosistema, la apuesta consciente

La Agencia de Ciberseguridad de Cataluña, alineada con el marco estratégico de la Unión Europea, está impulsando la transformación fundamentada en el conocimiento colaborativo, en la coordinación del ecosistema de ciberseguridad y en el apetito por la innovación. Y esto requiere de acciones precisas y concretas: Estrategias, Estructuras y Recursos. Tomás Roy, director de una de las estructuras creadas, el Centre d'Innovació i Competència en Ciberseguretat – CIC4Cyber, expone en este artículo las iniciativas en curso en Cataluña.



Tomás Roy Catalá

Podemos considerar 1995 como el año de inicio de la era actual de la ciberseguridad. Ese año se publicó la primera versión del BS 7799, *Applied Cryptography* de Bruce Schneier que se vendía con gran éxito y la revista SIC, visionaria, ya tenía tres añitos.

Antes, la ciberseguridad eran *hackers* de centrales telefónicas, *malware* y antivirus, la ingeniería social (Kevin Mitnick). Verdaderos genios de lo oscuro... y la oscuridad dejó de ser seguridad.

La ciberseguridad pasó a ser un proceso, no un producto, y como tal... un ámbito de gestión. Y en eso estamos desde hace ya casi 30 años. No es de extrañar pues que, en el sector, algunos grandísimos profesionales se sientan envejecidos. Y ya les avanzo que no es el sentir de la *Agència de Ciberseguretat de Catalunya*.

La ciberseguridad goza de un vigor, una efervescencia y desafíos más pertinentes a la etapa de la adolescencia y que, inevitablemente, desencadenarán en una transformación que tiene que beneficiarse de estos 30 años de conocimiento para su éxito.

El sector, el ecosistema, compite por los recursos y por el talento, pero no es receptivo a aprovechar y competir por la innovación.

La importante demanda de productos y servicios de ciberseguridad, desde un punto de vista económico y social, constituye un área de oportunidad para la evolución del país digital. El número de empresas dedicadas a la ciberseguridad con presencia en Catalunya ha crecido un 20% durante el 2021 y, en

total, alcanzan las 432. El sector también ha visto aumentada la facturación en un 11%, hasta los 912,9 millones de euros; y el empleo en un 19% hasta los 8.188 puestos de trabajo respecto 2020. En Catalunya, las empresas dedicadas a la ciberseguridad son pymes en su gran

mayoría (85%). Asimismo, casi un 30% de las empresas del sector son exportadoras y hasta un 22% facturan más de 10 millones de euros.

La amenaza cibernética ha puesto de manifiesto problemas de escasez de perfiles profesionales, de enemigos dignos de alianzas locales, nacionales



Figura 1.- El ecosistema que desarrolla el conocimiento, la cooperación y la innovación.



Figura 2.- Ejes y líneas de servicio de CIC4Cyber.

e internacionales, de pandemias y guerras híbridas, riesgos que impactan en vidas humanas o la economía, y una ciencia ficción que, con la computación cuántica, cada día es menos ficción.

En este DAFO es fácil identificar la enorme oportunidad que significa Europa y su foco en la soberanía, la resiliencia y la protección de los derechos de sus ciudadanos.

Los puntos fuertes y débiles del sector son evidentes: un tejido empresarial y de investigación con capacidades excelentes, pero poco conectados unos con otros; un conocimiento científico que participa y aporta a una red Global, pero que no se traslada en innovaciones al mercado; y unos productos, servicios, procesos..., que han permitido una excelencia hasta el día de hoy, pero que tienen enormes limitaciones de escalabilidad. Una escalabilidad que a menudo los informes detectan erróneamente como "falta de recursos y talento" y pocas veces como su causa raíz: la falta de innovación. El sector, el ecosistema, compite por los recursos y por el talento, pero no es receptivo a aprovechar y competir por la innovación.

Para que Catalunya pueda dar respuesta a los retos actuales en ciberseguridad, la excelencia que le supone la *Agència de Ciberseguretat de Catalunya*, el sector ciber catalán y las capacidades R+D+I son condiciones necesarias, pero no suficientes.

Estos nuevos tiempos, solo pueden ser gobernados con la transformación fundamentada en el conocimiento colaborativo, en la coordinación del ecosistema de ciberseguridad y en el apetito por la innovación. Y esto requiere de acciones precisas y concretas. Estrategias, Estructuras y Recursos.

ESTRATEGIAS, ESTRUCTURAS Y RECURSOS

La *Agència de Ciberseguretat de Catalunya* lidera tal transformación, en línea con el marco estratégico europeo, impulsando el desarrollo de nuevas estructuras en Catalunya. Estas son: el *Centre d'Innovació i Competència en Ciberseguretat* (CIC4Cyber), la comunidad de ciberseguridad de la *Digital Catalonia Alliance* (DCA) y el *Digital Innovation Hub de Catalunya Nodo de Innovación Digital* (DIH4CAT NID) de ciberseguridad.

CIC4Cyber, un Centro de Competencia, un Centro de Innovación, con la Comunidad Cyber

El Centro Europeo de Competencia en Ciberseguridad (ECCC), junto con la Red de Centros Nacionales de Coordinación (NCC), forman el nuevo marco

Agència de Ciberseguretat de Catalunya, dentro de su ámbito competencial y territorial, crea el CIC4Cyber.

La iniciativa CIC4Cyber se organiza en 4 ejes principales y sus correspondientes líneas de servicio.

- **Desarrollo del ecosistema.** El CIC4Cyber es una *hub* para ofrecer colaboración pública en ciberseguridad al tejido empresarial ciber de Catalunya, así como al sector público, tales como la financiación de iniciativas local e internacional y la transferencia de conocimiento. Para ello trabaja en red identificando sinergias y generando alianzas con socios estratégicos a todos los niveles, y localizando y movilizándolo el talento para atraer financiación y definir una agenda de inversión en innovación en ciberseguridad.

El CIC4Cyber participa en el ecosistema, con su conocimiento en ciberseguridad, de diferentes formas (Proyectos, Laboratorios, CyberAcademy, Ciber Range, DataLabs) en ámbitos como Opera-

El CIC4Cyber se apoya en el conocimiento y la innovación como palanca de transformación y crecimiento del sector, y en el trabajo en red como vía para maximizar el impacto de sus programas y proyectos, fomentando la captación de fondos y la internacionalización.

de Europa para apoyar la innovación y la política industrial en ciberseguridad. Son la estructura de coordinación de la inversión pública europea en ciberprotección que, apoyándose en lo que se ha denominado Comunidad tecnológica de ciberseguridad, establecerá una agenda común para el desarrollo tecnológico y para su amplio despliegue, que movilizará a través de la inversión en proyectos estratégicos de ciberseguridad.

Es en este marco, y para hacer de esta visión una realidad, en el que la

ción de la Ciberseguridad, *eHealth/Administración Pública*, *5G/Smart Mobility*, y *Big data* e IA para la ciberseguridad.

La actividad del CIC4Cyber estará estrechamente vinculada y pone toda su capacidad a disposición del nodo de innovación en ciberseguridad del DIH4CAT. Asimismo, participa activamente con ACCIÓ, la Oficina de Competitividad Empresarial de la Generalitat de Catalunya, en el objetivo de coordinar y fortalecer el nivel de ciberseguridad del conjunto del ecosistema empresarial

y su transformación digital, así como participa en las entidades de colaboración público-privada, como la DCA en Catalunya o la ECSO en Europa, o redes de profesionales Cyber, entre otras entidades colaboradoras.

- **Innovación.** El CIC4Cyber debe ser un elemento de coordinación de las iniciativas de aceleración y adopción de la innovación en ciberseguridad en el ámbito autonómico. Debe coordinar, cohesionar y estimular el ecosistema autonómico de innovación en ciberseguridad para ser capaz de revertir en el propio ecosistema el conocimiento y demás activos generados mediante la innovación, para su fortalecimiento.

Para ello el CIC4Cyber trasladará necesidades y retos de las áreas operativas de la Agència y participará en actividades de *brokerage* con su rol de usuario final en proyectos de innovación colaborando con el ecosistema de I+D. Dichas capacidades deben permitir desarrollar proyectos de innovación ambiciosos, con impacto en el territorio y visibilizando la fortaleza del ecosistema autonómico catalán de ciberseguridad en el conjunto de la Unión Europea.

- **La cultura.** El CIC4Cyber despliega el *Acord GOV/143/2018* por el cual se impulsa el Programa interdepartamental Internet Segura para la sensibilización y concienciación de la ciudadanía.

La ciberacademia del CIC4Cyber, con visión estratégica sobre capacidades y formación en ciberseguridad, permitirá promover formaciones en actividades laborales específicas y avanzadas, en coordinación con las universidades, centros de formación profesional o incluso de certificadores profesionales privados. Se acerca un gran reto en proporcionar diversidad de perfiles de la ciberseguridad: de operación, de gestión, planificación de las organizaciones, y se requiere atraer talento usando técnicas de *reeskilling*, *upskilling*... El CIC4Cyber iniciará programas en Catalunya que posibiliten incrementar la presencia de mujeres en posiciones de ciberseguridad y programas de ayuda a orientadores de los centros educativos que promuevan las STEM con visión de las oportunidades que tiene a futuro el sector.

- **Ciencia y Analítica de datos.** La importancia de los datos es enorme y puede suponer una ventaja estratégica y competitiva esencial para dar soporte y elevar a otro nivel la actividad del CIC4Cyber y del sector de ciberseguridad. A la hora de tomar decisiones, diseñar

estrategias sobre el tejido empresarial o formativas, e implementar la innovación, es fundamental basarse en modelos de datos de calidad.

El desarrollo de las capacidades de recolección, estructurado y analítica serán básicas para diseñar una estrategia *data-driven* y apoyar el relato de las políticas públicas desplegadas. A su vez, permitirá garantizar su consecución supervisando que el modelo de madurez del CIC4Cyber está alineado con las iniciativas y políticas catalanas, estatales y europeas. Además, a partir de los datos, las capacidades analíticas e inteligencia deben resultar fundamentales en la generación de análisis de tendencias, prospectivas -tanto globales como sectoriales-; pero en todo caso con una perspectiva ajustada al contexto y la realidad de Catalunya.

RESTO DE MIEMBROS DEL ECOSISTEMA DE CIBERSEGURIDAD CATALÁN

- **Cybersecurity Digital Catalan Alliance.** La Cybersecurity DCA es el instrumento que tienen las empresas ciber con la voluntad de cohesión y coordinación entre ellas.

El CIC4Cyber impulsa la creación de la comunidad de ciberseguridad de la Digital Catalan Alliance-DCA. A semejanza de la PPP en ciberseguridad eu-

La Agència de Ciberseguretat de Catalunya lidera el NID ciberseguridad del DIH4CAT, coordinado por la UPC, cuya principal misión es facilitar una digitalización segura del tejido empresarial. A tal efecto, el nodo orienta su actividad al acompañamiento de las pymes desde la sensibilización y diagnóstico, guía de actuaciones y consultoría tecnológica,

LA APUESTA CONSCIENTE

En estos tiempos excitantes hay que apostar fuerte. Deseamos compartir en un ecosistema receptivo la necesidad de la innovación, aprovechando la investigación que se hace aquí y por qué no, la de fuera.

Estamos frente a problemas que hoy no tienen, ni de lejos, solución aparente: la lucha contra el cibercrimen, la identidad digital, la protección de entornos de baja conectividad o baja capacidad de computación, la automatización, la desinformación, la caída de internet, la desconfianza, la falta de talento y la pérdida de oportunidad que ello conlleva, la protección descentralizada, el respeto de los derechos digitales... Todos estos problemas no son teóricos, y no se resuelven consolidando productos y copiándose entre ellos, ni aplicando una regla de tres. Sí o sí, el CIC4Cyber, la innovación sistémica y ecosistémica es la única apuesta consciente.

En estos tiempos excitantes hay que apostar fuerte. Deseamos compartir en un ecosistema receptivo la necesidad de la innovación, aprovechando la investigación que se hace aquí y por qué no, la de fuera.

ropea ECSO, la Cybersecurity DCA promueve la colaboración público-privada para cohesionar el ecosistema de ciberseguridad, fomentar la innovación para dar respuesta a los retos del ámbito e impulsar iniciativas conjuntas, así como el mercado especializado.

- **DIH4CAT NID ciberseguridad.** El DIH4CAT ofrece una ventanilla única a pymes y administraciones públicas para el fomento de la digitalización y la innovación digital. El DIH4CAT se construye siguiendo el modelo de los *Digital Innovation Hubs* establecidos por la Comisión Europea para impulsar la transformación digital y tecnológica actuando, al mismo tiempo, como un conector avanzado entre la oferta y la demanda existente en el conjunto de Catalunya.

En conclusión, el CIC4Cyber es una estructura organizativa pública que tiene un claro objetivo de coordinación, cohesión y capacitación del ecosistema de ciberseguridad de Catalunya, se apoya en el conocimiento y la innovación como palanca de transformación y crecimiento del sector, y en el trabajo en red como vía para maximizar el impacto de sus programas y proyectos, fomentando la captación de fondos y la internacionalización. ■

TOMÁS ROY CATALÁ
Director
Centre d'Innovació i Competència
en Ciberseguretat – CIC4Cyber
AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA



CIBERSEGURIDAD

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

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

Todas las respuestas
que buscas están en
aenorciberseguridad.com



AENOR

Confía



Estrategia de Ciberseguridad de Andalucía 2022–2025

Andalucía, en su propósito de garantizar un espacio digital ciberseguro, no es ajena al nuevo escenario al que se enfrenta la sociedad, que impacta directamente en todos los sectores estratégicos de la Comunidad Autónoma e indirectamente en la industria y economía nacional y europea, en el que el uso seguro de las TIC y la protección de la información debe ser considerado como algo imprescindible para el buen funcionamiento de los servicios y sistemas soportados en el ciberespacio, de cara a ofrecer garantías y confianza digital a la sociedad.



Raúl Jiménez / Antonio Requena

Para adaptarse a la rápida evolución de la tecnología y al entorno cambiante actual, de modo que se puedan las necesidades de la ciudadanía en torno a la ciberseguridad, la Administración de la Junta de Andalucía ha desarrollado múltiples iniciativas a lo largo de los años.

En este sentido, del 23 al 25 de marzo, se celebró la primera edición del Congreso de Ciberseguridad de Andalucía, un espacio de encuentro entre Administración Pública, profesionales y empresas del sector tecnológico para compartir conocimiento y experiencia en torno a la seguridad digital, teniendo como principal hito la presentación de la nueva Estrategia de Ciberseguridad de Andalucía 2022 – 2025 (en adelante, Estrategia).

Propósito

La Estrategia tiene el propósito de construir el vínculo entre la Administración de la Junta de Andalucía y la ciberseguridad, estableciendo las líneas maestras que deben llevarse a cabo durante los años 2022 y 2025 de cara a dar respuesta a los retos y desafíos de la sociedad andaluza. En este sentido, promueve y habilita el uso seguro de las redes y sistemas de información, prestando especial atención a los operadores críticos, servicios esenciales y



sectores estratégicos de la Comunidad Autónoma, y permitiendo el posicionamiento de Andalucía entre las economías digitales más avanzadas.

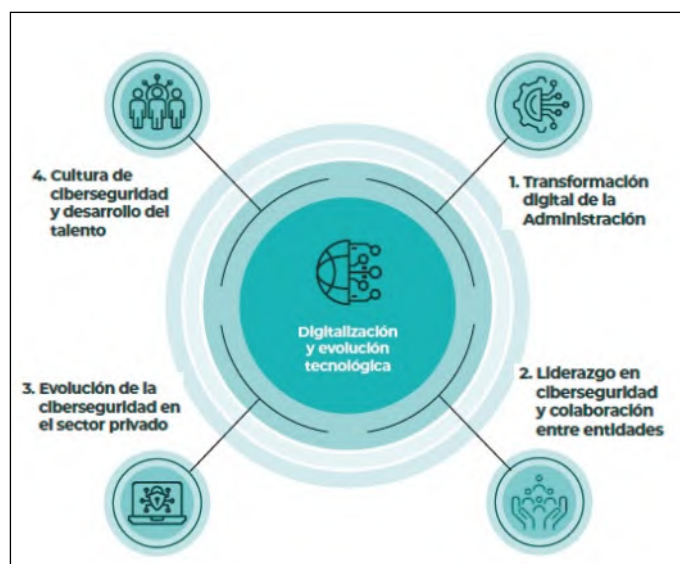
Principios

Los principios que rigen la Estrategia y son la base de su implementación exitosa giran en torno a la necesidad de colaboración y participación de todos los colectivos que forman parte del actual ecosistema digital hiperconectado:

- Ciudadanía,
- Empresas,
- Instituciones,

donde la responsabilidad en materia de ciberseguridad es compartida.

La Estrategia establece ocho objetivos clave a alcanzar durante los años 2022 y 2025, que permitirán a Andalucía posicionarse como un territorio líder en el sector de la ciberseguridad.



Retos

En la Estrategia se han definido cuatro grandes retos, derivados de la digitalización y evolución tecnológica de la sociedad, a los cuales se pretende dar respuesta a través de un escenario objetivo que permita a Andalucía convertirse en un territorio de referencia en materia de ciberseguridad.

Objetivos estratégicos

De cara a dar respuesta a los retos identificados, la Estrategia establece ocho objetivos clave a alcanzar durante los años 2022 y 2025, que permitirán a Andalucía posicionarse como un territorio líder en el sector de la ciberseguridad.

Líneas de actuación

De manera alineada a los objetivos estratégicos, en el documento estratégico se han definido ocho líneas de actuación que posibilitan la consecución de los mismos. En conjunto, todas las líneas de actuación cubren uno o más de los objetivos establecidos.

De manera alineada a los objetivos estratégicos, en el documento estratégico se han definido ocho líneas de actuación.

A continuación, se detallan las líneas de actuación a desarrollar para la consecución de los objetivos establecidos en la Estrategia. Cada línea de actuación está compuesta por una serie de actividades esenciales que pretenden dar respuesta a los retos actuales de la sociedad.



Conclusiones

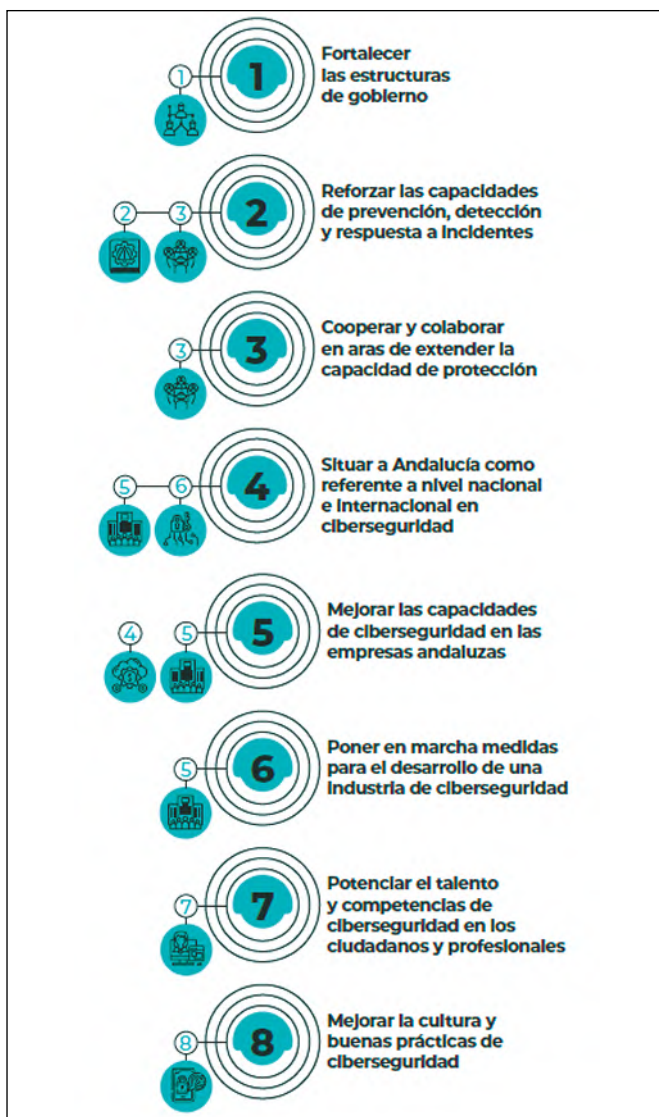
La elaboración de la Estrategia es el claro ejemplo del compromiso y de la apuesta de la Administración de la Junta de Andalucía por la ciberseguridad.

Se trata del primer paso en un largo y complejo camino, que tiene como objetivo final dar respuesta a los retos y desafíos a los que se enfrenta una sociedad cada vez más digitalizada e hiperconectada a través de las TIC.

En este sentido, la implementación de las líneas de actuación definidas en la Estrategia permitirá a Andalucía posicionarse como una sociedad digital de referencia a nivel nacional e internacional. ■

RAÚL JIMÉNEZ
Director Gerente
AGENCIA DIGITAL DE ANDALUCÍA

ANTONIO REQUENA
Socio. Business Security Solutions
PwC





wisecurity
GLOBAL

Domingo Cardona

CEO y Cofundador
de Wise Security Global

> Por Ana Adeva
> Fotografía: Jesús A. de Lucas

“Somos una de las pocas empresas tecnológicas de soluciones integrales de ciberseguridad y confianza digital que cuenta con producto propio”

Con una dilatada trayectoria, Domingo Cardona ha sido partícipe de importantes iniciativas en la construcción de equipos de detección y respuesta, tanto a nivel nacional como internacional. Su experiencia le llevó hace siete años, junto con otros profesionales, a crear una compañía donde su fuerte inversión en I+D y el desarrollo de tecnología propia le otorgan un gran elemento diferenciador. Fiel creyente de las posibilidades del *blockchain* aplicado a la ciberseguridad —particularmente a servicios de identidad—, analiza para SIC los retos del sector, el rol del CISO y la visión de Wise Security Global.

– ¿Cuándo surge Wise Security Global y cómo ha evolucionado hasta ser lo que hoy es?

– Nace en 2014 como empresa de servicios de ciberseguridad, a partir de la iniciativa de varios profesionales que habíamos trabajado juntos con anterioridad en proyectos del sector. En 2016 empezamos a colaborar con una compañía vasca de tecnología *cloud* y firma electrónica, con la que nos fusionamos en 2018. Hoy, nuestro plan estratégico inicial nos ha llevado a ser una empresa holística de servicios y productos propios de ciberseguridad, así como de identidad y certificación electrónicas en *blockchain*, cuya misión es la de proteger la actividad de nuestros clientes generando entornos ciberseguros y ciberconfiables, que les permita mantener y mejorar la confianza digital de sus *stakeholders*.

– Resulta diferenciador que en su denominación incluyera el adjetivo de ‘Sabio’...

– Sí. La verdad es que alguna vez hemos pensado que se podría interpretar de forma un poco arrogante, pero nada más lejos de la realidad. Wise (o Sabio) es un deseo para con nosotros y nuestros clientes de seguir creciendo juntos en el continuo aprendizaje y experiencia necesarias para dotar a nuestro ecosistema de la mejor protección posible.

– ¿Con cuántos profesionales cuentan y con qué grado de especialización?

– Actualmente, conformamos Wise más de 90 profesionales con un alto grado de especialización en cada una de las distintas líneas de negocio. Por ejemplo, el 80% cuenta con estudios universitarios superiores finalizados; el 5% están cursándolos; el 15% ha finalizado estudios de formación profesional; y el 40% cuenta con un máster o postgrado de especialización en los campos en los que opera la empresa. Además, contamos con una ratio de certificaciones de 1,25, que crece y fomentamos gracias a nuestro “Programa de Certificaciones”.

– ¿Cuáles son las claves para captar y conservar al talento?

– Además de ofrecer salarios acordes, nuestras claves pasan por seleccionar a gente buena y buena gente, incluirla en el eje central de nuestra estrategia, dibujar y caminar con ella su plan de carrera, orientarla a objetivos y no a actividad, capacitarla de un modo continuo, efectivo y perceptible, dotarla de una flexibilidad laboral altamente imaginativa y habilitarles un ecosistema de retos y oportunidades de desarrollo constantes, donde inauguramos realidades nuevas cada día.

– Ante la oleada de *ransomware* de los últimos 18 meses, cada vez más agresivo, ¿está la tecnología a la altura para



“Muchos CISO asumen responsabilidades que no deberían encontrarse en el ámbito de su función; y esto es algo que se tiene que definir y consensuar en etapas tempranas junto a la Dirección de la organización”

mitigar este tipo de ataques?

– Sí está a la altura, pero no así quienes tienen la responsabilidad de pilotarla y mantenerla. En los casos de *ransomware* con los que nos encontramos en Wise, tienen éxito porque alguna o algunas de las medidas que desde la compañía consideramos básicas no estaban desplegadas o se encontraban parcial e ineficazmente implementadas.

De hecho, el momento coyuntural que estamos viviendo con la guerra entre Rusia y Ucrania y la consiguiente amenaza continua de Putin hacia Occidente, tienen que ser percibidos por todos nosotros como un ‘punto de dolor’ que permita elevar los niveles de alerta en ciberseguridad y poner foco en la protección ante todo tipo de ciberataques, sobre todo de *ransomware*, que puedan tener su origen en Rusia o bien sean perpetrados por grupos ciber-criminales o estados-nación respaldados por este país.

– ¿Se está perdiendo la carrera ante la ciberdelincuencia por querer llegar a todo y por su cada vez mayor profesionalización?

– Sí, estamos perdiendo esta carrera por su cada vez mayor profesionalización, amparada en múltiples casos por estados-nación no alineados con Occidente y, también, por no apostar por un modelo de nuestra función que centre su principal actividad en el correcto tratamiento de las amenazas relevantes. Pero no me quedaría tan sólo ahí: la falta de concienciación y escasez de presupuesto todavía son deficiencias que debemos resolver en organizaciones poco

maduras. En aquellas que lo son más cabe seguir trabajando en la capacitación directiva de muchos de los profesionales de nuestro sector, que todavía necesitan para hablar en lenguaje de negocio y convencer a sus mayores.

– Si usted tuviera un ‘elixir curativo’ para mitigar el *ransomware*, ¿en qué consistiría la fórmula?

– Todo el mundo en el sector sabe que, con tiempo, dedicación y fijación suficientes, un atacante preparado podría llegar hasta tu más preciada joya de la corona. No obstante, en Wise consideramos que, además de la concienciación y capacitación de las personas que formen parte de nuestro ecosistema, existe un conjunto de medidas que ayudan o bien a parar un *ransomware* o para acabar disuadiendo al atacante de tenerlo como objetivo, o bien para mitigar el potencial impacto que pudiera darse. Para ello, debemos seguir insistiendo en una buena y focalizada organización de la privacidad, ciberseguridad, ciberresiliencia y continuidad de negocio, trabajando conjuntamente en el tratamiento de esta amenaza específica y desplegando las medidas adecuadas para su buen Gobierno, Identificación, Protección, Detección, Respuesta y Recuperación.

– Wise mantiene relación con CCN-CERT. Dentro de la cada vez más deseada colaboración público-privada, ¿cree que enraizará la compartición de información de ciberseguridad real, con un valor recíproco?

– Los más mayores de Wise tuvimos la suerte de iniciar nuestras carreras profesio-

nales en esCERT-UPC, el primer CERT que se creó en España, junto al propio de RedIRIS (Red.es). Allí, desde las iniciativas empresariales surgidas, tuvimos la oportunidad de verificar internacionalmente (participando activamente en grupos como FIRST, TF-CSIRT o APWG) la necesidad de existencia de entes especializados en la detección temprana y respuesta eficaz ante ciberamenazas: SOC/CERT/CSIRTs que, para conseguir esos objetivos de detección y respuesta, tuvieran como máxima entre sus ejes de actuación la coordinación, colaboración y compartición de información entre ellos.

Con esta máxima en mente, ayudamos en su día en el diseño, puesta en marcha e, incluso, operación de algunos de los principales centros de ciberseguridad, tanto públicos como privados, que existen en el país y la compartición de información de amenazas e incidentes entre ellos es

colabora y comparte información en su día a día con otros centros alineados y cuando el Centro publique los requisitos de membresía iniciaremos el proceso de adhesión a esta iniciativa a la que le auguramos, sin lugar a duda, el necesario éxito que nos llega requerido por la actuación de las cada vez más sofisticadas ciberamenazas.

– **En general, el portafolio de su compañía se divide en dos grandes áreas:**



“El SOC de Wise colabora y comparte información en su día a día con otros centros alineados y cuando el CCN publique los requisitos de membresía iniciaremos el proceso de adhesión a la Red Nacional de SOC”

ya una realidad; tómese como ejemplo de ello el foro CSIRT.es. Ciertamente, no obstante, que quizás esos procesos colaborativos no cuenten con la premura y eficacia deseadas por todas las partes que puedan requerir una determinada información en un momento dado, pero considero que es cuestión de tiempo que iniciativas más ágiles en este sentido, como puede ser el canal Radiomacuto en Telegram, se transformen en canales formales de compartición de información para un mejor tratamiento global de la amenaza ciber.

– **En su trayectoria tienen, además, experiencia internacional en poner en marcha SOC. ¿Qué opina de iniciativa local de creación de la Red Nacional de SOC?**

– Esta iniciativa, que cuenta desde nuestro punto de vista con el acertado impulso y liderazgo del CERT gubernamental nacional, no es más que la materialización operativa natural de esa máxima de “necesaria coordinación y colaboración” con la que el CCN-CERT fue concebido, y con la que cualquier centro de ciberseguridad que forme o vaya a formar parte de la Red Nacional de SOC debería estar dotado. El SOC de Wise, como no podía ser de otro modo,

CyberTrust, con una amplia oferta en evidencia electrónica con potentes innovaciones de identidad en blockchain, soluciones de firma y factura electrónicas, y CyberSecurity, basada en hacking ético y ciberseguridad gestionada. En un mercado donde existen fuertes competidores en estos ámbitos, ¿cómo marca la diferencia su propuesta?

– En primer lugar, porque somos una de las pocas empresas tecnológicas de soluciones integrales de ciberseguridad y confianza digital que cuenta con producto propio. Nuestra área de I+D nos facilita, por un lado, todo un ecosistema de herramientas orientadas a la industrialización efectiva de muchos de los servicios que desplegamos en nuestros clientes. Y, por otro, concibe y desarrolla nuevas soluciones que están teniendo muy buena aceptación en el mercado y a las que auguramos, sin duda, un enorme éxito en los próximos meses y años. Lo veréis.

El otro gran elemento diferenciador de la compañía es nuestro ADN Wise, una forma muy especial de compartir conjuntamente la pasión que todos los que formamos parte de Wise tenemos por la ciberseguridad y la ciberconfianza. “Once

a Wiser, always a Wiser”.

– **¿En qué están trabajando ahora dentro de su área de I+D?**

Estamos centrados en dos de los productos que ya hemos desplegado en el mercado: Definitive ID (R), como solución de identidad digital descentralizada y autosoberana; y Bastet (R), una aplicación para la automatización de todos los procesos involucrados en el descubrimiento, tratamiento y resolución de vulnerabilidades en sistemas de información.

– **Y, ¿qué opinan de la llegada de los fondos europeos en este sentido?**

– Llevamos varios años con un bombardeo continuo de información por diferentes medios pero, aún hoy, están llegando los primeros fondos a España. En febrero de 2022, nuestro Gobierno lanzó el primer programa financiado por estos fondos, el denominado Kit Digital, al que Wise se ha adherido como Agente Digitalizador y en el que actuamos como intermediario, no como beneficiario en sí. Al ser tan reciente, por el momento, solo podemos decir que estamos echando en falta información sobre el plan de ejecución y notando que los plazos se dilatan, pero confiamos en que finalmente las ayudas llegarán a las pequeñas empresas de entre 10 y 49 trabajadores a las que van destinadas. Al margen, dado que en Wise lleva-

mos años invirtiendo en I+D, contamos con la gran suerte de que las instituciones vascas están muy implicadas en apoyar e impulsar a las empresas en este sentido, sobre todo a las pymes. No obstante, no olvidemos que estas ayudas no son un regalo, requieren también un gran compromiso y sacrificio por parte de las empresas, ya que tenemos que contar con proyectos innovadores y de calidad para conseguir el apoyo necesario, poder materializarlo y asegurarnos de cumplir todos los requisitos en tiempo y forma.

– **Tras casi dos años de pandemia y el cambio masivo al trabajo en remoto, ¿cuáles son aún los aspectos más críticos y qué propone Wise para reducir sus riesgos?**

– La instauración del trabajo en remoto ha llevado a la conexión *wi-fi* de nuestras casas el punto de acceso a nuestras redes corporativas; un nuevo punto de acceso y red asociada que no cuenta, para nada, con las medidas de seguridad que teníamos en la red de nuestras organizaciones. Para corregir este nuevo espacio de vulnerabilidad, Wise ha desarrollado Haunt Keeper, un dispositivo que se conecta fácilmente al *router* de tu casa y crea automáti-

camente una nueva red aislada, totalmente bastionada, en la que puedes conectar tus dispositivos de trabajo de manera mucho más segura que a la red plana que te ofrece tu proveedor de Internet.

– **El rol del CISO es cada vez más relevante y, en determinados sectores, obligatorio. Debido a la falta de profesionales, ¿cómo valora el hecho de ofrecer servicios en remoto que cubran sus funciones?**

– Esta tipología de servicios resulta hoy en día muy necesaria dado que todavía no hay capacidad madura suficiente para cubrir la demanda actual en la capa de gobierno de la ciberseguridad. En Wise, donde el servicio es ya muy maduro, lanzamos esta solución en 2015 con el objetivo de llevar la compleja función del CISO al lugar que se merece, es decir, a las capas directivas de las organizaciones, pero hablando en lenguaje de negocio. Esto es, modulando los conceptos puros de la ciber e introduciendo la planificación estratégica alineada con negocio, y la priorización de medidas e iniciativas conforme a una relación 'Coste vs Riesgo-Beneficio'.

– **¿Qué opina de la evolución del CISO, cada vez con más peso y en conexión con la alta dirección, pero de que también muchos estudios hablan de su excesivo agotamiento?**

– Mi opinión es que muchos CISO, que lo son por la existencia de amenaza ciber, asumen responsabilidades que no deberían encontrarse en el ámbito de su función; y esto es algo que se tiene que definir y consensuar en etapas tempranas junto a la Dirección de la organización. En nuestro modelo de responsabilidad compartida, a modo de ejemplo, no responsabilizamos al CISO del tratamiento de amenazas que no sean de tipología "ciberataque"; no lideramos la adecuación al marco regulatorio específico, sino que damos soporte (sí lideramos el marco normativo interno); y tampoco nos responsabilizamos de resiliencia TI como soporte a la continuidad de negocio, sino "tan sólo" de la ciberresiliencia. Fíjese que, con tan solo estas tres acotaciones de responsabilidad, cualquier CISO podrá ver que con este modelo será invitado a ser protagonista de menos fiestas y acabará menos agotado.

– **Dentro de su oferta CyberTrust, Wise apuesta por ámbitos de la identidad digital. ¿Qué papel le otorga y qué le augura a Europa en este terreno?**

– Entendemos, en base a la lectura del borrador de la próxima versión del eIDAS y a un elaborado escrutinio del panorama internacional en colaboración con Gartner, que Europa le va a dar una total trascendencia e impulso al uso de credenciales

descentralizadas en *blockchain* como método base y principal de identificación de usuarios entre todos los países miembros, así como de otorgar al usuario la total potestad de sus datos, de ahí el concepto de autosoberanía. Para este fin, es totalmente imprescindible que los usuarios cuenten con *wallets* propios como contenedor de estas credenciales. Y nuestra apuesta es que estos *wallets* estén ubicados en los dispositivos móviles de dichos usuarios.

Creemos que el recorrido empieza en la empresa privada, quien puede lanzar sus iniciativas al respecto de manera mucho más ágil que la administración, pero sin duda el gran "empuje" al cambio de paradigma vendrá cuando la resolución de la



"La tecnología sí está a la altura para mitigar el ransomware, pero no así quienes tienen la responsabilidad de pilotarla y mantenerla"

normativa vea la luz y toda administración tenga que adoptar el sistema en los años venideros.

– **En concreto, ¿qué peso le atribuye a *blockchain* en relación con la ciberseguridad y en proveer de confianza a las actividades digitales?**

– En el nuevo sistema de credenciales que hemos desplegado en nuestras soluciones, y aunque no nos vaya a proteger de la amenaza *ransomware*, *blockchain* proporciona un avance relevante en, al menos, dos aspectos que contribuyen de gran manera en la mejora de la ciberseguridad y la confianza digital, respectivamente. En primer lugar, cualquier operación de identificación dejará en la cadena de bloques una traza inmutable y accesible por las partes en todo momento. Y, en segundo término, el usuario será soberano de sus credenciales y, por tanto, de permitir o revocar de manera activa su uso por terceros, y no como hasta ahora, donde tenemos que confiar en estos cuando solicitamos un cambio en el uso y tratamiento de nuestros datos.

– **Con cuatro sedes ya en España. ¿tie-**

ne en mente establecerse a corto plazo fuera de nuestras fronteras?

– Todavía estamos en fases tempranas del proceso pero, si las cosas van como creemos, Emiratos Árabes (UAE), donde ya contamos con un acuerdo con un socio local, Tec Evolution, podría ser el siguiente país en el que nos estableciéramos. Paso a paso.

– **En su facturación, ¿qué peso tiene el sector público y el privado, y cuáles son los principales verticales en los que están presentes y espera crecer?**

– En Wise siempre hemos priorizado el ámbito privado sobre el público por una mera cuestión de eficiencia empresarial. Así, el privado representa un 95% de nuestra facturación, donde un 35% es de ámbito internacional; y, el público, por tanto, un 5%. Estamos presentes, sobre todo, en banca, seguros e industria. No obstante, prevemos que el mayor crecimiento en los próximos años estará en ocio y *retail*.

– **¿Se basta sola la compañía para atender a las necesidades de los clientes o, en ocasiones, son necesarias las alianzas?**

– Una de las máximas de Wise es la de proveer siempre la mejor solución posible para nuestros clientes. Ello nos lleva, en ocasiones, a construir alianzas

con otros actores del sector especializados en materias muy concretas. Por ejemplo, contamos con DFIR para momentos puntuales de acumulación de emergencias o adecuación a normativas ciber de sectores económicos concretos.

– **¿Podría mencionar proyectos notables en España por su alcance o singularidad?**

– Centrándonos en soluciones con tecnología *blockchain*, estamos implantando con Definitive ID un sistema universal de identidad para los carnés de un importante organismo deportivo español, reconocido a nivel mundial. También, cabe destacar nuestros avanzados servicios de ciberseguridad ofensiva y nuestra potente solución de ciberseguridad, Bastet, en una de las entidades bancarias de mayor prestigio y reconocimiento en nuestro país.

– **¿Su gran reto para 2022?**

– Hacer realidad la identidad digital descentralizada (y cibersegura) en todos aquellos clientes que están confiando en nuestra solución. Y que la comunidad Wiser pueda verlo y disfrutarlo. ■



La Ciberguerra entre los escombros

El drama de la invasión de Ucrania por el ejército imperial ruso a finales del mes de febrero de 2022, ha golpeado irreversiblemente a la sociedad europea y marcará el futuro de Europa en las próximas generaciones. En esta ocasión, el escenario bélico convencional se da sobre un escenario de Tecnologías de la Información nunca antes vista en una guerra. Se pueden percibir los efectos reales del denominado Quinto Escenario y quizás podamos aprender algo de ello. El tiempo permitirá un análisis más detallado y sopesado de lo que aquí está ocurriendo, pero a estas alturas –finales de marzo– podemos echarle un vistazo preliminar a ver si sacamos alguna conclusión.

Es curioso ver cómo la paz suele ser inconsciente hasta que llega la guerra, en ese momento, más o menos todos los ciudadanos empiezan a sospechar que las cosas no estaban tan bien como parecían. Sin embargo, esa conciencia inmanente queda superada rápidamente por alguna idea simple, supuestamente diáfana, que termina explicando todo en pocas palabras y ubicando la culpa de todo siempre lejos de uno mismo, de nuestra sociedad o incluso de nuestro país.

Los que saben de Geopolítica siempre han dicho que el régimen de Putin, como muchos otros regímenes totalitarios a lo largo de la Historia, no duda en recurrir a la guerra y a las economías de guerra para 1) sanear y revitalizar su propia economía, 2) instaurar una unidad (aparente y efímera) entre sus ciudadanos alrededor del concepto de Nación o de Pueblo, 3) expandir su territorio económico y/o militar, y 4) establecer y/o mantener una oligarquía autoritaria de ricos frente a una multitud de siervos pobres.

No nos habíamos quitado las mascarillas y Putin coloca cientos de miles de soldados en las fronteras propias y de estados títere como Bielorrusia con Ucrania, y un 24F empieza una Guerra y una invasión que muchos no esperaban. Sin embargo, los que saben de esto, ven (ahora y entonces) movimientos económicos (controlar la producción de gas, la acumulación de reservas, la gestión internacional de la deuda nacional, el posicionamiento energético en Europa, la censura y reconfiguración de Internet para su mejor control, etc.) que auguraban algo “grande” dentro de los planes del Kremlin. A toro pasa-

do y revisando ahora aquellos datos, está más claro que esta guerra se lleva fraguando años, que era la idea central de la autocracia putiniana y su oligocrática corte de multimillonarios y que, en todo ello, los propios ucranianos nada tenían que hacer.

vencional mucho más lenta y de la que todavía no hemos visto la fase de guerra urbana y la posible fase insurgente de postguerra.

Esa guerra pone de manifiesto lo que nos gusta a los países en paz: ninguno la geopolítica y desterrar cual-



Cabría preguntarse si las iniciativas particulares no pueden terminar siendo la excusa para que imperialistas rusos decidan escalar la contienda en Ucrania y considerarlos actos de guerra por parte de las potencias de la OTAN. Tanto para atacar o defender infraestructuras TI, como para prestar ayuda y hospitalidad a los refugiados, la respuesta debería ser más profesional y controlable por parte de los que decimos ser sociedades democráticas, justas y transparentes.

La vieja Europa, atemorizada

Atemorizada, la vieja Europa toma como suya esa guerra y reconoce el flanco ucraniano como un flanco europeo y la UE y toda su población decide condenar la guerra de Putin, la invasión de Ucrania y, sobre todo, la aniquilación de cualquier infraestructura y la masacre de civiles (al estilo de la batalla de Alepo¹), que claramente representa la esencia de esta estrategia bélica.

Está claro que a los cuerpos de defensa ucranianos no les ha cogido de sorpresa esta invasión y hasta la fecha han demostrado al mundo su capacidad de combatir y de frenar al cacareado segundo (o tercero) más potente ejército de la tierra. Este valor y previsión, aderezado con las armas que pronto se han animado a mandar los demás países europeos –y Estados Unidos–, ha convertido una supuesta invasión relámpago en una guerra con-

quier *situational awareness* que pueda romper la placidez de nuestras cañas en una terraza privada invasora del espacio público. Cuando la realidad se nos impone y ya no podemos seguir negándola, empiezan los lamentos, los golpes de pecho y los espasmos de todo tipo para digerir rápidamente esta nueva realidad no deseada. Algunos se convierten espontáneamente en ONGs y llevan indiscriminadamente materiales para los refugiados; otros se transforman en Agencias de Viajes, que pretenden reubicar a los huidos del horror en vete tú a saber qué ubicaciones y en qué condiciones; otros saltan del sofá en su casa para coger el teclado de su ordenador y alistarse en supuestos ciber-movimientos *hacktivistas* para contratacar desde los suburbios burgueses de las ciudades europeas y de otras demarcaciones.

Cualquiera de esas tres situaciones son ejemplo de la falta de profesionalidad de nuestras sociedades en lo que

¹ [https://en.wikipedia.org/wiki/Battle_of_Aleppo_\(2012-2016\)](https://en.wikipedia.org/wiki/Battle_of_Aleppo_(2012-2016))

a la organización social y ciudadana se refiere. Hacer llegar materiales a un país es un problema logístico serio que hay que desarrollar profesionalmente y con mucho control; de lo contrario, pronto florecerá la corrupción y la es-ta-fa entre tantas buenas intenciones.

Mover millones de refugiados es algo que hay que tomarse mucho más en serio que dejarse llevar por el llanto de niños, mujeres u hombres que están siendo atacados y despojados de todo. Estamos hablando de seres humanos y no de mascotas por lo que las reaccio-nes viscerales no deberían es-tar permitidas. No es organi-zar unas vacaciones de unos días, sino una emigración en la que los desplazados tienen que rehacer completamente y partiendo de nada, sus vidas en otros territorios, en otros idiomas, en otras culturas. Estamos hablando posible-mente de años y no de días, y si no me creen, piensen en cuánto tiempo se tardará en reconstruir las infraestruc-turas que ahora están triturando las bombas, cohetes y misiles de crucero de la maquinaria de guerra rusa, y de la europea algo también.

Declarada la "ciberguerra" contra Rusia

Algunas cuentas de Twitter que utilizan la identidad colectiva **Anony-mous**, el mismo 25F ya habían declara-do la "ciberguerra" contra Rusia y reivindicado la autoría de varios ata-ques informáticos contra instituciones públicas rusas y medios de comunica-ción al servicio del Kremlin. El primer ataque fue al "canal de propaganda" **RT (Russia Today)**, cuyo impacto fue sólo el de paralizar la actividad de su web durante algunas horas para que luego se recuperase sin efecto perma-nente alguno.

Simultáneamente se han dado otras operaciones en el ciberespacio que han sido más interesantes. Por una parte está la banda privada de ciberdelin-cuentes conocida como **Conti Team**, los cuales no se arrugaron al ponerse al lado de Putin en la Deep Web y be-

ber de los cálices más puros de la ser-vidumbre a la autocracia rusa que les ha permitido realizar libremente y sin consecuencias sus negocios planetarios de extorsión.

Conti Team es uno de los grupos más activos de la industria del ciber-crimen. Es un operador de *ransomware* modular (EMOTET, TrickBot botnet, Co-balt Strike, Ryuk) y una de sus armas (Ryuk) es el virus que tumbó múltiples empresas e instituciones públicas espa-ñolas en 2020 y 2021, como el SEPE o el **Ministerio de Trabajo**.



Lo único novedoso en esta guerra inesperada (pero previsible) es que las bombas no han conseguido quebrar las redes de comunicación multimedia que adornan nuestro día a día, y hoy cualquiera puede mandar su opinión, sus videos, sus vivencias, sus noticias, al resto del mundo a la vez que suenan las sirenas de ataque aéreo o estallan los cohetes a decenas de metros de distancia.

Antes de la invasión de Ucrania, en el trimestre final de 2021, se rea-lizaron 722 campañas de ataque con *ransomware*, siendo LockBit 2.0 (30 %), Conti (19 %), PYSA (11 %), Hive (10 %), y Grief los virus más utilizados, lo que pone de manifiesto lo boyante que iba el cibercrimen en tiempos de paz.

Las bandas de extorsión, retratadas

La reacción al posicionamiento de Conti Team no se hizo esperar y se la conoce como **Contileaks**, que es una cuenta en Twitter² a través de la cual se ha liberado el contenido de los *chats* internos de esa organización (160.000 mensajes de enero 2021 a febrero 2022) y que son un magnífico ejemplo (digno de un estudio calmado y deta-llista) de lo bien que están organiza-das estas bandas de extorsión a muy gran escala. Del análisis de esos datos se obtiene información de gran valor, como son direcciones de Bitcoin em-pleadas por la banda, el código fuente para las funciones de cifrado y descifrado, así como un constructor de su *ransomware*, el modelo organizativo de la banda (jerarquía, salarios, depar-tamentos, etc.) e incluso guías sobre

cómo realizar ataques. Brian Krebs³ ha publicado en su sitio un análisis de la información más jugosa que se extrae de ellos.

Por otra parte, y relacionados espe-cíficamente con la invasión de Ucrania, hay varios ejemplos de *malware* dise-ñado para funcionar como ciberarmas y ese es el caso de los *wipers* disfrazados de *ransomware* (los *wipers* borran irreversiblemente el almacenamiento de los sistemas atacados). En concreto nos referimos a WhisperGate⁴, Herme-ticWiper⁵ e IssacWiper⁶. Con lo que

está claro que las facciones pro-rusas estaban dispuestas a iniciar una versión Ciber de lo que las bombas con explo-sivos químicos ya estaban haciendo sobre la población ucraniana.

Tanto el alineamiento de las bandas privadas a favor de Putin y el Kremlin, como la respuesta etérea del colec-tivo conocido como Anonymous son iniciativas particulares y no parecen ser iniciativas promovidas por ningún estado. Eso no quiere decir que "a río revuelto" no haya beneficio de pesca-dores en el este y en el oeste y que, incluso, algunos comandos de ciber-guerra rusos, ucranianos u occidenta-les puedan haberse camuflado detrás de esas iniciativas antes del inicio de las hostilidades.

Tirándose los trastos

Este escenario de organizaciones civiles, de particulares tirándose los trastos en el medio universal que es Internet, no es propiamente una ciber-guerra sino más bien una lucha de ban-das al estilo de las de Nueva York⁷ en 1920 antes de llegar la Mafia italiana. Eso no quita para que sea un enfren-tamiento polarizado por una invasión que sí se puede llamar guerra y que sí está promovida por un estado invasor, el ruso, contra un estado víctima, que es el ucraniano.

Aunque se han dado ataques con éxito por parte de Anonymous en los que ha puesto de manifiesto su pre-sencia, sólo unos pocos han aportado

² <https://twitter.com/ContiLeaks>

³ <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/>

⁴ <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>

⁵ <https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/>

⁶ <https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/>

⁷ [https://en.wikipedia.org/wiki/The_Gangs_of_New_York_\(book\)](https://en.wikipedia.org/wiki/The_Gangs_of_New_York_(book))

información que puede ser interesante. Lo más avanzado en este frente Ciber quizás sea el “hackeo” por parte de Anonymous a la agencia federal rusa **Roskomnadzor**⁸, que es el regulador de la censura de medios en Rusia, y que se ha saldado con la filtración de 800 GB de sus archivos y bases de datos⁹ de dicho organismo de control de Putin. Pero, ¿qué le importa a Putin que se sepa en el mundo cómo controla con mano dura y viril lo que sus nacionales reciben como información? Me temo que el valor de esta información es meramente historiográfico.

Por otro lado está el ataque con éxito por parte de Anonymous de la filial alemana **Rosneft Deutschland GmbH**¹⁰ de la gran petrolera rusa con el mismo nombre, y que está presidida por el ex canciller alemán Schröder (está claro, también hay puertas giratorias en Alemania). En esta acción, alguien bajo la careta de Anonymous se hace con información confidencial (20 Tera bytes) de una empresa que forma parte de las **Infraestructuras Críticas de Alemania**. Aunque aseguran que la información conseguida no afecta a las infraestructuras energéticas de Alemania, y declaran que no quieren afectar al sector petrolero, lo cierto es que no han liberado esa información (justificándose en que quieren no favorecer a sus empresas competidoras) y que no está claro quién realmente la está escudriñando.

Las iniciativas particulares, cuestionadas

Habría que preguntarse si estas iniciativas particulares no pueden terminar siendo la excusa para que imperialistas rusos decidan escalar la contienda en Ucrania y considerarlos actos de guerra por parte de las potencias de la OTAN. Mi opinión es que los invasores no necesitan de excusas para escalar hacia arriba o hacia abajo su invasión de territorio ajeno.

En cualquier caso, tanto para atacar o defender infraestructuras TI, como para prestar ayuda y hospitalidad a los refugiados, la respuesta debería ser más profesional y controlable por parte de los que decimos ser sociedades democráticas, justas y transparentes.

Lo único que es novedoso en esta guerra inesperada (pero previsible) es que las bombas no han conseguido quebrar las redes de comunicación multimedia que adornan nuestra día a día, y hoy cualquiera puede mandar su opinión, sus videos, sus vivencias, sus noticias, al resto del mundo a la vez que suenan las sirenas de ataque aéreo o estallan los cohetes a decenas de metros de distancia. La campaña ucraniana sólo representa claramente el triunfo indiscutible de ARPANET¹¹ después de 56 años.



Más allá de los defacements de páginas web, del compromiso de algunas bases de datos en la nube, y la exfiltración de alguna información jugosa de alguna compañía rusa, los ataques Ciber no se pueden comparar al efecto real e histórico de las toneladas de explosivos y proyectiles que están regando con sangre y cascotes los campos de Ucrania, los campos de Europa.

Tal es así que el Ministerio de Estadística ruso ha dado instrucciones a todos los sitios web y servicios estatales para que cambien al sistema de nombres de dominio ruso (DNS .ru), que abandonen los alojamientos en servidores extranjeros, que desactiven cualquier código JavaScript que proceda del exterior y que fortalezcan la política de contraseñas, todo ello antes del pasado 11 de marzo. Con esto, la Rusia de Putin pretende desengancharse de Internet y confinar a todos sus nacionales/residentes a una autarquía permanentemente controlada y monitorizada del Kremlin, al más puro estilo de la Internet disponible en China desde hace ya bastante tiempo.

Tecnológicamente hablando es muy fácil desconectar a un país de la Internet global; de hecho, China lo ha hecho desde hace tiempo y algunos paí-

ses también lo han conseguido, aunque sólo durante periodos transitorios. En las tecnologías de la información apagar es mucho más fácil que encender, lo que no es tan fácil es mantener una Internet local y soberana y que sus fronteras no sean penetradas por numerosos túneles que, como una hidra, se multipliquen más deprisa de lo que se van cerrando. Todo va a depender de las ganas que tenga el pueblo ruso de quedarse para siempre informativa y culturalmente confinado en su egocentrismo, o lo que es peor, en la eterna contemplación de su Zar. Lo que representa la Internet original (previa a 1995) es un genio al cual no se le puede fácilmente volver a meter en la botella.

Llegado a este punto hay que preguntarse si esto de las ciberguerras, los ciberejércitos, los ciberpatriotas o las

ciberguerrillas realmente sirven para algo. El drama ucraniano nos pone delante de la cruda realidad y nos muestra que lo Ciber sólo es importante cuando NO estallan bombas de racimo¹² en el patio de tu casa, y la “madre de todas las bombas” (MOAB¹³) es decir, las bombas termobáricas¹⁴, no te convierten en testigo de las explosiones químicas más potentes posibles.

Más allá de los defacements de páginas web, del compromiso de algunas bases de datos en la nube, y de la exfiltración de alguna información jugosa de alguna compañía rusa, los ataques Ciber no se pueden comparar al efecto real e histórico de las toneladas de explosivos y proyectiles que están regando con sangre y cascotes los campos de Ucrania, los campos de Europa. La ciberguerra sólo puede ser efectiva cuando no hay una guerra convencional que la haga palidecer. ■

⁸ Servicio Federal de Supervisión de las Telecomunicaciones, Tecnologías de la Información y Medios de Comunicación en Rusia.

⁹ Se advierte que directorios como ПОЧТА Приемная, contienen numerosos correos con adjuntos y que esos adjuntos pueden ser un vector típico de malware y enlaces de phishing, por lo que estos datos deben manipularse con herramientas de seguridad como Dangerzone y equivalentes. <https://ddosecrets.com/wiki/Roskomnadzor>

¹⁰ <https://anonleaks.net/en/2022/anonymous-germany/20-terabytes-anonymous-germany-hijacks-data-from-rosneft-germany/>

¹¹ <https://en.wikipedia.org/wiki/ARPANET>

¹² https://en.wikipedia.org/wiki/Cluster_munition

¹³ https://en.wikipedia.org/wiki/GBU-43/B_MOAB

¹⁴ https://en.wikipedia.org/wiki/Thermobaric_weapon y https://en.wikipedia.org/wiki/Dust_explosion

JORGE DÁVILA

Consultor independiente

Director

Laboratorio de Criptografía

**LSIS – Facultad
de Informática – UPM**

jdavila@fi.upm.es

En síntesis, un gemelo digital es una herramienta de tecnología inteligente, habilitada por IA utilizada para crear representaciones vivas de extremo a extremo del mundo real, desde equipos sofisticados, cadenas de suministro, ciclos de vida de productos, recursos, y demás opciones vinculadas a IT/IoT/OT subyacente. Estas representaciones digitales, susceptibles de ser compartidas, ofrecen enormes ventajas al poder aprovechar el poder de los datos en tiempo real, generalizando el acceso a conocimientos vitales y la comprensión para ayudar a mejorar la toma de decisiones estratégicas y tácticas.

Pero, por otro lado, las organizaciones que se enfrentan a ataques cibernéticos saben que tales incidentes y violaciones son muy costosas, desde la reparación de vulnerabilidades de red y la recuperación del control de datos hasta la recuperación de daños reputacionales e impactos financieros. Y la tecnología cibernética gemela coadyuva a prevenir ataques costosos a través de su capacidad para tomar decisiones más rápidas y eficientes a medida que se alimentan más datos y pruebas de penetración para la simulación doble de un sistema.

El desarrollo de una réplica virtual también significa que la empresa está en disposición de proteger sus sistemas y activos de proveedores externos y subcontratados, algo no trivial hoy día.

En este contexto, a lo largo de su trayectoria –que excede ya dos décadas– la Universidad de Málaga ha aportado al ecosistema del conocimiento en ciberseguridad no pocas investigaciones de interés. Algunas de las más importantes Revista SIC las ha canalizado en sus ediciones ofreciendo al lector succulentos anticipos de temas que *a posteriori* cobrarían una importancia crucial. Basta recordar el no repudio, la notarización electrónica, la testificación digital o la internet de los objetos/cosas. Esta vez toca el turno a un concepto, el de Gemelo Digital, destinado a ser estratégico y cuya vinculación a la ciberseguridad augura una odisea digital que empezará con fuerza en este 2022. Al tiempo.

Gemelos cibernéticos

2022, una odisea digital



Ciberseguridad en Gemelos Digitales

De entre las tecnologías emergentes de la Industria 4.0, el Gemelo Digital (GD) destaca por las enormes ventajas que aporta en el contexto de los procesos de automatización y producción. Su capacidad para simular y representar estados de elementos físicos del mundo real, experimentar configuraciones y prever situaciones anómalas, le dan un gran valor añadido que otras soluciones alternativas no pueden aportar.

No obstante, las características particulares de un GD lo predisponen especialmente a diversos tipos de amenazas de ciberseguridad. En este artículo se introduce la problemática actual al respecto de tales amenazas, a la vez que ofrece un conjunto preliminar de indicaciones que pueden abrir camino a la hora de abordar esa problemática de una manera más extensa en un futuro cercano.



JAVIER LÓPEZ / CRISTINA ALCARAZ

E.T.S. Ingeniería Informática. NICS Lab
UNIVERSIDAD DE MÁLAGA

En línea con los objetivos de la Industria 4.0, las Tecnologías de la Información (IT) de vanguardia se están incorporando progresivamente a los procesos de automatización para la continua mejora de la producción y distribución de servicios y productos. Entre estas tecnologías, el **Gemelo Digital (GD)** es una de las más prometedoras.

El concepto de GD nació en 1970 cuando la NASA necesitaba monitorizar componentes físicos para misiones aeroespaciales (por ejemplo, la nave espacial Apolo XIII), con el objetivo de diagnosticar problemas y proporcionar componentes validados^[1]. Esto difiere significativamente del concepto actual de GD, en el que puede considerarse a este como un tipo de solución mucho más compleja que los tradicionales sistemas de virtualización.

Más concretamente, en la actualidad un GD caracteriza los activos físicos (ya sean estos productos, procesos o sistemas) a través de activos digitales utilizando técnicas basadas en especificaciones, modelos matemáticos e interfaces de programación de aplicaciones. Esos activos digitales se ejecutan en servidores a través de recursos virtualizados (máquinas virtuales -VM-, contenedores y redes virtuales), con el objetivo principal de prever errores, variaciones y desviaciones relevantes que puedan cambiar el comportamiento natural de un sistema. A su vez, estos servidores se conectan al mundo físico para interactuar con componentes del mundo real y, por esa razón, un GD se asocia con tres espacios^[2]:

- **Espacio físico:** comprende todas aquellas tecnologías operativas (OT) y de información para el control de activos físicos del mundo real, como sensores, actuadores y controladores.

- **Espacio digital:** son todos aquellos activos digitales que, representando activos del

espacio físico, son capaces de simular estados, condiciones y configuraciones, además de tomar decisiones por sí mismos sobre dicho espacio.

- **Espacio de comunicaciones:** conecta los dos espacios anteriores, permitiendo al GD intervenir en las operaciones de producción a través de flujos de información y procesos de control.

Al respecto de este último espacio, es necesario destacar la importancia de las interfaces bidireccionales en el GD, de tal forma que los datos obtenidos por dispositivos operativos del espacio físico son procesados por activos digitales, mientras que estos, a su

y se envía para activar el modelo de simulación. Del mismo modo, los activos digitales establecen configuraciones y ejecutan instrucciones que pueden cambiar el estado del homólogo físico para mantener, optimizar o mejorar el rendimiento operativo de sus componentes. También se desprende de la figura que un GD integra un conjunto de algoritmos que, haciendo uso de diferentes tecnologías y sistemas de comunicación, puede representar estados y tomar decisiones para actuar automáticamente sobre los activos físicos cuando sea necesario.

De entre las distintas tecnologías que pueden servir de soporte al GD, destaca la



De entre las distintas tecnologías que pueden servir de soporte al Gemelo Digital, destaca la IoT dado que es especialmente útil para mejorar la interacción entre espacios y, además, garantiza el despliegue de otras tecnologías que van desde los Sistemas

Ciberfísicos hasta el IoT Industrial y la computación edge, haciendo uso también de técnicas de IA y Big Data para la gestión de los datos.

vez, crean nueva información valiosa y útil que puede ser devuelta al espacio físico.

El resultado es un *hilo digital* entre los espacios físico y virtual que, a la postre, diferencia al GD de los simuladores tradicionales. Es decir, mientras que un GD se conecta con el mundo físico y sigue representaciones granulares y precisas del mismo a través de modelos detallados del mundo físico, y establece interfaces bidireccionales entre los espacios, un simulador convencional no integra tales modelos especializados.

La **Figura 1** (basado en el trabajo^[3]) muestra un ejemplo de GD que caracteriza el comportamiento de un tren de alta velocidad donde la información de los activos físicos (por ejemplo, los datos de los sensores) se recoge

Internet of Things (IoT) dado que es especialmente útil para mejorar la interacción entre espacios^[3] y, además, garantiza el despliegue de otras tecnologías que van desde los Sistemas Ciberfísicos hasta el IoT Industrial y la computación *edge*, haciendo uso también de técnicas de Inteligencia Artificial y *Big Data* para la gestión de los datos. Esta heterogeneidad de tecnologías hace que el diseño de un GD sea muy variado, pudiendo estar compuesto por recursos virtuales que se ejecutan tanto dentro de un servidor como en sistemas complejos cuya lógica puede extenderse por toda la infraestructura *edge*.

Existen muchos casos de uso que han demostrado el valor práctico de los GD, ya sea para aplicaciones industriales, escenarios de

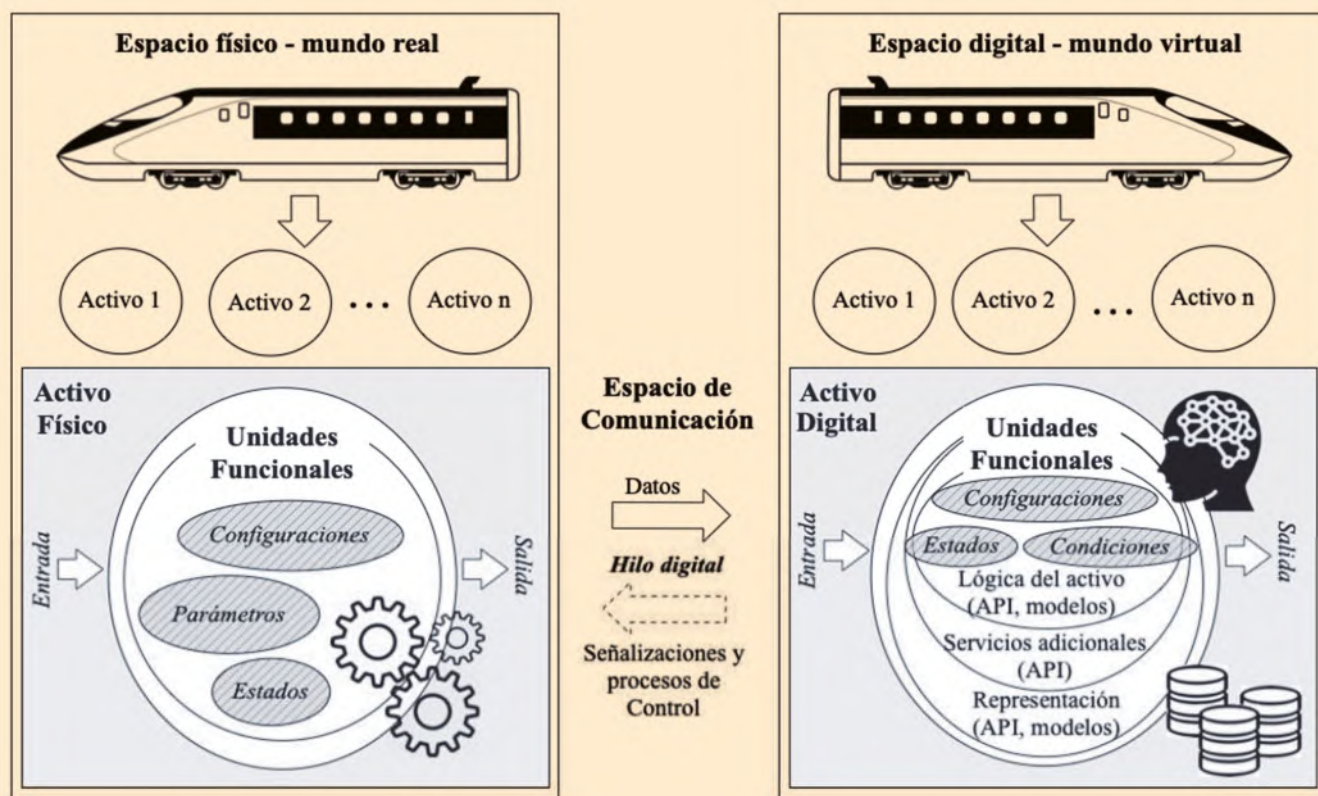


Figura 1.- Espacios de trabajo del GD.

smart cities, gestión de emergencias o entornos militares. Este aspecto práctico también lo pone de relieve **Gartner** en sus informes anuales sobre tecnologías destacadas, situando el paradigma de GD entre una de las diez principales tecnologías estratégicas^[4]: cuarta posición en 2018 y 2019, y primera en 2020. Esta novedad también se pone de manifiesto en el informe^[5], que confirma que el tamaño del mercado de GD, valorado en 2.786 millones de euros en 2020, alcanzará los 43.148 millones en 2026.

SEGMENTACIÓN EN CAPAS

El interés por parte de los diferentes sectores económicos, tanto privados como públicos, refuerza la mayor atención y esfuerzo que desde hace unos pocos años están dedicando los expertos científicos y técnicos al respecto de cómo mejorar la aplicación de la tecnología de GD en distintas áreas de la automatización y la ingeniería. Sin embargo, esos esfuerzos no están siendo ni mucho menos tan determinantes en lo que se refiere a la ciberseguridad y a la protección de la propia tecnología frente a diversos tipos de ataques, lo cual crea un problema muy considerable, principalmente por dos razones: **i)** los GD se consideran sistemas críticos por naturaleza dado que participan en los procesos de automatización; y,



Cuando se considera un escenario general, se observa que un atacante puede dañar al Gemelo Digital desde el espacio físico, pero asimismo puede dañar el espacio físico desde el espacio digital para tomar el control de la infraestructura subyacente y sus activos físicos. Esto implica que la superficie de ataque a un GD se extiende considerablemente en comparación con otras tecnologías.

ii) los GD contienen piezas de propiedad intelectual que representan la copia digital del mundo físico.

Obviamente, estos dos aspectos son de gran interés para atacantes que persigan corromper el modelo de negocio de una organización, dañar su reputación o provocar daños irreparables, especialmente en el caso de las infraestructuras críticas. Además, cuando se considera un escenario general, se observa que un atacante puede dañar al GD desde el espacio físico, pero asimismo puede dañar el espacio físico desde el espacio digital para tomar el control de la infraestructura subyacente y sus activos físicos. Esto implica que la superficie de ataque a un GD se extiende considerablemente en comparación con otras tecnologías, principalmente debido a la interconexión de los dos espacios (físico y digital) mediante el sistemas e infraestructuras de comunicación, así como de las tecnologías que intervienen.

Debido a esta complejidad, el análisis de amenazas a un GD requiere no sólo de pormenorizar los estudios e investigaciones en las diferentes tecnologías implicadas dentro del paradigma, sino también de examinar con detalle la conceptualización en capas del GD, como también se propone en ISO 23247^[6], el primer estándar de GD definido para escenarios de fabricación, y en el trabajo^[3]. La **Figura 2** ilustra dichas capas, mostrando cómo en cada una se integran un conjunto de servicios esenciales con soporte en múltiples interfaces, tecnologías y sistemas de computación. Son precisamente esas integraciones las que conllevan numerosos y serios problemas de ciberseguridad.

Para comprender mejor las diferencias entre las capas de esa figura es necesario considerar el grado de procesamiento de los datos correspondientes al espacio físico y al espacio digital, así como las tecnologías implicadas en los mismos. Por un lado, los valores de medi-



ción y de control correspondientes a los activos del mundo real suelen ser capturados y procesados por los dispositivos de la capa 1, que están desplegados cerca de los activos físicos. Tales capturas permiten al GD y sus modelos sincronizarse respecto a su homólogo físico, e iniciar los procesos de simulación para producir una comprensión más detallada y precisa del escenario correspondiente al mundo real. Por otro lado, las tecnologías que intervienen en la interpretación de los datos y su representación suelen desplegarse en las capas 2 a 4, en las que se desarrolla toda la lógica del GD y sus procesos de simulación.

Adicionalmente a lo anterior, y dado que el GD se considera un sistema crítico y, por lo tanto, de sumo interés para los adversarios, sobre todo cuando se aplican para infraestructuras críticas, un estudio exhaustivo de las amenazas de seguridad a un GD ha de tener en cuenta la necesidad de cumplir con sus requisitos operacionales del GD. Por ejemplo, la falta de integridad o la no disponibilidad de datos y de recursos esenciales de la capa 1 puede tener un efecto imprevisible en los servicios de sincronización, así como en la calidad de las simulaciones del GD en términos de precisión y granularidad.

AMENAZAS DE CIBERSEGURIDAD

En el estudio de las amenazas, se consideran dos tipos de superficies de ataque, la digital y la física. La primera comprende todos aquellos componentes software y sistemas de información que permiten ejecutar y gestionar datos críticos que están relacionados con procesos, propiedad intelectual y tareas de control. La segunda abarca el acceso a nodos e infraestructuras físicas del mundo real, ya sean dispositivos ciberfísicos y de la IoT Industrial, o infraestructuras de comunicación e instalaciones. Por lo tanto, la superficie de ataque global es realmente muy extensa, lo cual puede ser aprovechado por los atacantes para mejorar sus conocimientos y técnicas de ataque del propio GD. Por ejemplo, podrían penetrar en los sistemas de control y, una vez dentro, buscar la ubicación del GD para comprometerlo, lo que les permitiría conocer los recursos del sistema, ampliar sus capacidades técnicas y acceder al sistema crítico a través del GD para exfiltrar información o destruir sus recursos.

En la **Tabla 1** se incluye una lista no exhaustiva de los tipos de amenazas al GD, junto a una breve descripción de cada una de ellas, indicando además entre paréntesis las capas en las que se pueden producir. Las amenazas que pueden tener un mayor impacto en los requisitos operacionales son las relacionadas con el despliegue de componentes maliciosos, seguido de un MitM (*man-in-the-middle*), vulnerabilidades software y denegación de servicio (DoS, DDoS). En el caso de este último,

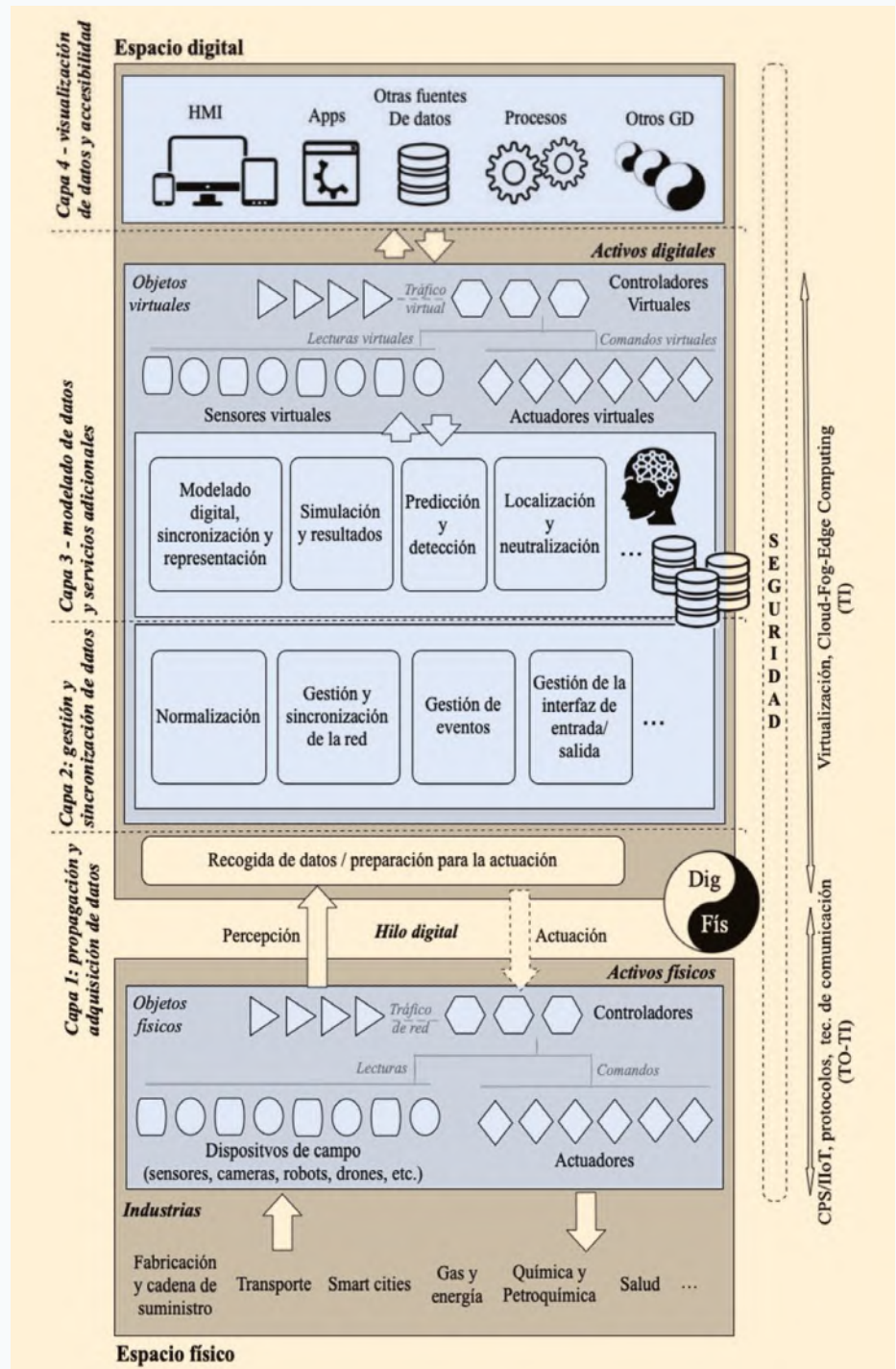


Figura 2.- Abstracción del Gemelo Digital compuesto de cuatro capas fundamentales.

el impacto será mayor o menor en función del tipo de despliegue del GD; es decir, cuanto más descentralizado, menor será el riesgo debido a colapsos intencionados o exhaustiones.

Es conveniente resaltar que casi todas las amenazas tienen alguna influencia en la consistencia final de los datos, ya sea en términos de precisión o granularidad, lo que muestra la gran debilidad de la tecnología GD en contextos críticos en los que es esencial una alta precisión en el tratamiento de los datos. Por otro lado, la protección de la propiedad inte-

lectual debe tratarse de forma prioritaria en los sistemas críticos basados en el GD, ya que las consecuencias de un ataque pueden ser devastadoras y a veces irreparables, principalmente debido a la comunicación bidireccional entre los espacios físico y digital.

EXPLORACIÓN INICIAL DE SOLUCIONES

Hasta el momento se han expuesto las diversas perspectivas de la problemática de seguridad en los GD, que como se ha podido observar es amplia y ante la que se necesitan



AMENAZAS	DESCRIPCIÓN DE LAS AMENAZAS
Vulnerabilidades SW (1,2,3,4)	Corresponden a aplicaciones y sistemas operativos, tanto en el espacio físico como en el digital, que pueden ocasionar infecciones y exposiciones que corrompan los datos de simulación además de impactar en la representación final de los mismos.
Escalado de privilegios (1,2,3)	Los atacantes pueden acceder a los tres espacios de un GD y escalar/abusar de privilegios, interrumpiendo o cambiando sustancialmente cualquier información gestionada en cada espacio y en cada capa del GD, como, por ejemplo, datos de sincronización entre espacios, especificaciones y estados de simulación, lo cual alterará posteriormente la realidad mostrada por el GD.
MitM (1, 2, 3)	Todo componente o sistema conectado al espacio de comunicación del GD (incluyendo la interconexión entre recursos virtuales) puede ser vulnerable a ataques MitM, a través del cual los atacantes interceptarán canales, realizarán manipulaciones o provocarán una DoS, corrompiendo así la sincronización entre espacios y la gestión final del GD.
Componentes maliciosos (1, 2, 3, 4)	Los atacantes con derechos de acceso a instalaciones industriales y a los tres espacios de un GD pueden desplegar dispositivos OT e IT maliciosos o tener la capacidad para manipular la configuración de los ya existentes, a fin de ejecutar con posterioridad acciones típicas de un MitM y alterar la información gestionada por el GD.
Extracción de información privada (1, 2, 3)	Cualquier acceso a los tres espacios de un GD y a sus componentes OT e IT puede implicar análisis y fugas de información privada, como los modelos digitales que representan la copia exacta de activos físicos del mundo real, así como análisis pasivos de tráfico de red o entre VM para mapear, localizar y atacar los principales componentes del GD.
Manipulaciones (1, 2, 3, 4)	La representación final de un GD puede verse seriamente afectada por manipulaciones intencionadas de datos (ya sean valores de entrada como de salida) pertenecientes a los tres espacios del GD, y que incluye desde mediciones de activos del mundo real hasta datos de virtualización, análisis, toma de decisión y visualización.
DDoS (1, 2, 3)	Las OT e IT desplegadas pueden ser objeto de ataques dirigidos a agotar recursos esenciales y deshabilitar operaciones que entorpezcan la sincronización del GD y los procesos de simulación. Dentro de esta categoría se encuentran también los ataques físicos donde los atacantes con acceso a las instalaciones pueden sustraer y destruir recursos.
Fuga de privacidad (2, 3)	Además de observar el tráfico y mapear y localizar componentes de un GD (ej. los principales servidores), los atacantes pueden derivar patrones rutinarios (ej. movimientos/acciones constantes de robots) si tienen acceso a las instalaciones y vías para escalar privilegios hacia las especificaciones de los modelos digitales y las bases de datos del GD, con el fin de, más tarde, aplicar técnicas de ingeniería inversa y de inferencia.

Tabla 1.- Lista no exhaustiva de los tipos de amenazas al GD.

soluciones de distinta índole y naturaleza. Como se ha mencionado, se requiere aún de un esfuerzo de investigación y estudio considerable en esa dirección. No obstante, a continuación se realizan algunas indicaciones iniciales que pueden abrir camino a la hora de abordar la problemática de una manera más extensa en un futuro cercano.

Dentro de este abanico inicial encontramos aproximaciones de carácter puramente técnico y otras más cercanas a la gestión y los procedimientos de seguridad. Las primeras cubren los aspectos más específicos de la protección de los GD y su despliegue, como el *hardening* de las infraestructuras de la tecnología, la detección y mitigación de intrusiones, etc., mientras que los segundos están asociados a las buenas prácticas y el buen uso del paradigma dentro de una organización, como son la gobernanza y la auditoría.

• **Seguridad hardware (HW) y software (SW).** Cualquier fallo de diseño (*seguridad por diseño*), actualización inadecuada de compo-



En el estudio de las amenazas, se consideran dos tipos de superficies de ataque, la digital y la física. La primera comprende todos aquellos componentes software y sistemas de información que permiten ejecutar y gestionar datos críticos que están relacionados con procesos, propiedad intelectual y tareas de control; la segunda abarca el acceso a nodos e infraestructuras físicas del mundo real, ya sean dispositivos ciberfísicos y de la IoT Industrial, o infraestructuras de comunicación e instalaciones.

nentes o una validación inapropiada puede conllevar a vulnerabilidades HW y SW en el GD. Por ello, resultaría recomendable establecer medidas de confianza e integridad desde el HW, implementando, por ejemplo, módulos de plataformas o entornos de ejecución de confianza, garantizando la programación segura y las buenas prácticas en base a patrones de diseño, y realizando de manera regular procesos de verificación y pruebas HW y SW.

• **Protección de redes, infraestructuras y sistemas.** Esto involucraría, por un lado, gestionar configuraciones seguras de redes y equipos IT y OT, y segmentar sistemas y fun-

ciones de acuerdo a las políticas de seguridad con el fin de proteger los procesos de simulación y el acceso a la propiedad intelectual, donde además sería necesario preestablecer los límites de acceso y de confianza, así como monitorizar todas las actividades realizadas dentro del GD. Esto podría ser especialmente útil cuando los servicios del GD estén repartidos por toda la infraestructura *edge* y/o distribuidos a lo largo de diferentes áreas de la industria y gestionados por diferentes administradores, o bien cuando fueran mantenidos de manera regular por terceras partes con derecho de acceso.



• Identidad, autenticación y autorización.

El primer servicio aborda la gestión de identidades únicas, no sólo en el espacio físico sino también en el digital. A través de esas identidades sería posible mapear los elementos de todo el ecosistema (digital y físico), identificar a los propietarios y garantizar la movilidad y la autenticación de nodos IT y OT, recursos virtuales (VM/contenedores) y datos en el espacio de comunicaciones. También, se requerirían soluciones de autorización (ej. RBAC con ABAC, XACML o SAML) para controlar el acceso de entidades (incluyendo otros GD) a datos restringidos relacionados con la propiedad intelectual, como, por ejemplo, modelos del GD.

• **Consciencia situacional.** Los sistemas de detección de intrusiones y de anomalías serían clave para prevenir riesgos importantes en el GD, especialmente cuando su lógica se puede dispersar de manera descentralizada en todo el ecosistema digital. La información generada por estos sistemas retroalimentaría mecanismos de consciencia situacional que ayuden a explicar con alto nivel de detalle lo que está ocurriendo dentro de un sistema, detallando la intensidad de una amenaza, las áreas y los recursos afectados, así como el impacto hacia otros escenarios de aplicación.

• Respuesta y recuperación.

Existe una especial necesidad por disponer de medidas reactivas y correctivas que fueran capaces de salvaguardar las operaciones de simulación bajo garantías de QoS y aportar respuestas rápidas, precisas y fiables. Esto se debe principalmente a que los activos OT y IT del mundo físico forman parte del control de una infraestructura crítica y el GD puede supervisar las funciones de estos activos. Es por ello que, en situaciones de amenaza, el GD debería tener soporte suficiente para responder y recuperar sus servicios en consecuencia, y mantener sus operaciones disponibles.

• **Gestión de eventos y compartición de datos.** Todos los eventos generados por los GD y las tecnologías implicadas habrían de ser gestionados por sistemas especializados como los SIEM a fin de tener una visión más completa y clara de los problemas de seguridad que se producen dentro de un GD, aprovechando las capacidades de estos sistemas para intensificar la consciencia situacional y la protección del GD y su entorno. Para complementar las acciones de la consciencia situacional, los SIEM podrían también considerar los mecanismos actuales de compartición de datos (vulnerabilidades y amenazas), teniendo presente, las técnicas de “cyber threat intelligence” para conectar de manera regular con los CERT/CSIRT y repositorios similares (p.ej. MITRE ATT&CK o NVD del NIST). Tam-

bién, los GD podrían tomar ventaja de sus conexiones para conectar directamente a estos servicios de protección, o crear redes inter-GD para compartir y mantener un registro de amenazas y vulnerabilidades, quizás a través de una red de tipo DLT.

• **Gestión de la confianza.** Es un requisito prioritario para crear un entorno de simulación confiable, e implicaría aplicar técnicas (distribuidas o centralizadas) específicas para gestionar las actitudes adoptadas por cada componente del GD. A través de esquemas de reputación, junto con mecanismos de recompensa y penalización, sería posible estimar la actitud de cada componente y calcular así el nivel de fiabilidad de las simulaciones, de forma que componentes con mayor reputación pudieran tener mayores oportunidades para acceder al mundo real con respecto a los

considerados a lo largo del ciclo de vida del GD y para su entorno de despliegue, donde resulta fundamental establecer controles de seguridad bajo marcos regulatorios siguiendo estándares, recomendaciones y guías oficiales, aplicados tanto para proteger el acceso al GD desde la red corporativa como para proteger el GD en la propia red de control donde generalmente se despliega. Aparte de estos controles, también existiría la necesidad de automatizar los procesos de gestión de riesgo, para dinámicamente evaluar las implicaciones que conlleva las complejidades del propio paradigma en contextos industriales.

• **Trazabilidad, auditoría y responsabilidad.** Dado que los GD se caracterizan por integrar diversas tecnologías que producen grandes volúmenes de datos, si estos se almacenaran de manera adecuada sería po-



Todos los eventos generados por los GD y las tecnologías implicadas habrían de ser gestionados por sistemas especializados como los SIEM, a fin de tener una visión más completa y clara de los problemas de seguridad que se producen dentro de un GD, aprovechando las capacidades de estos sistemas para intensificar la consciencia situacional y la protección del GD y su entorno. Para complementar las acciones de la consciencia situacional, los SIEM podrían también considerar los mecanismos actuales de compartición de datos teniendo presente las técnicas de “cyber threat intelligence” para conectar de manera regular con los CERT/CSIRT y repositorios similares.

que tengan menor reputación. La implementación de estas técnicas puede suponer un coste computacional y de almacenamiento elevado al requerir procesar evidencias del pasado para reflejarlas en las conductas del presente.

• Gobernanza y gestión de la seguridad.

Dado que el GD se aplica normalmente en sistemas críticos, las organizaciones deberían adoptar medidas de protección basadas en la metodología de “defensa en profundidad” bajo procedimientos legales, técnicos y organizativos. Estos procedimientos deberían ser

sible garantizar un registro de eventos para la auditoría, la trazabilidad y el seguimiento de acciones realizadas por el propio GD. Esto también permitiría a las organizaciones estimar cuándo activar o revisar políticas de seguridad, programas de formación y planes de mantenimiento o continuidad. Si adicionalmente los GD se combinaran con tecnologías de registro distribuido (DLT), sería posible proporcionar, además, aspectos asociados con la inmutabilidad, replicabilidad e integridad de dichos datos. ■

REFERENCIAS

- [1] B. R. Barricelli, E. Casiraghi, and D. Fogli, “A survey on digital twin: Definitions, characteristics, applications, and design implications,” *IEEE Access*, vol. 7, pp. 167 653–167 671, 2019.
- [2] M. Grieves, “Digital Twin: Manufacturing Excellence through Virtual-Factory Replication,” White paper, vol. 1, pp. 1–7, 2014.
- [3] R. Minerva, G. M. Lee, and N. Crespi, “Digital Twin in the IoT Context: A Survey on Technical Features, Scenarios, and Architectural Models,” *Proceedings of the IEEE*, vol. 108, no. 10, pp. 1785–1824, 2020.
- [4] K. Panetta, “Gartner Top 10 Strategic Technology Trends for 2018/2019/2020,” 2018/2019/2020. [URL disponible]: <https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/2019/2020>
- [5] Markets and Markets, “Digital Twin Market by Technology, Type (Product, Process, and System) – Global Forecast to 2026,” 2020. [URL disponible]: <https://www.marketsandmarkets.com/Market-Reports/digital-twin-market-225269522.html>
- [6] ISO, “Automation Systems and Integration — Digital twin Framework for Manufacturing — Part 2: Reference Architecture,” ISO 23247-2:2021, ISO/TC 184/SC 4 Industrial data, 2021. [URL disponible]: <https://www.iso.org/standard/78743.html>



235%

Akamai ha observado un aumento del 235% en los ataques de phishing.

¿Tú solución de MFA está a prueba de phishing?

Akamai MFA: Seguridad FIDO2 sin claves de seguridad físicas

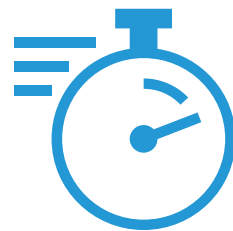
Protege tu empresa contra el robo de cuentas de empleados, y filtración de datos con la tecnología MFA de última generación. Convertimos tu smartphone en una llave de seguridad, con una autenticación sencilla, y sin carga de trabajo para tu equipo de TI.



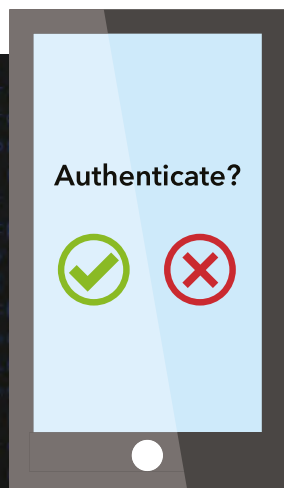
Máxima seguridad



Push mobile a prueba de phishing



Gestión de TI unificada y sencilla



Akamai MFA – Pruébalo gratis durante 60 días

Solicita una prueba gratuita en: contact-spain@akamai.com o si lo prefieres, llámanos al Tel. 91 793 32 43

Combatir la desinformación desde la ciberseguridad

Durante las últimas semanas, no pocos profesionales de la ciberseguridad han verificado cómo la manipulación de la información se consolidaba como una nueva superficie de ciberataque, surgida al amparo de la avalancha de datos utilizados en la toma de decisiones.

La Unión Europea¹ no ha sido ajena a esta situación. De facto, ENISA² ha puesto en marcha nuevas capacidades para la monitorización y seguimiento de los procesos de desinformación, apoyándose en conceptos que están íntimamente relacionados con la ciberseguridad y que se sustentan en sus cuatro grandes pilares: las cuatro "T", por sus siglas en inglés: el terreno, las tácticas, los objetivos (*targets*) y las tentaciones³⁻⁵.

Tecnología al servicio de la desinformación

Partiendo de estas premisas, el uso dual que tiene actualmente la tecnología impacta a las amenazas que genera la desinformación. Podríamos decir que hace más difícil su identificación y seguimiento. No en vano, los agentes de la desinformación han aprendido a utilizar la tecnología con contenidos reales y convertirlos en datos manipulados⁶ que llevan el sello de "verdades a medias" —o, como diría Antonio Machado, "dobles mentiras"—.

En este contexto, las técnicas de ciberseguridad tradicionales de detección y prevención parecen haberse quedado cortas y quizá ha llegado el momento de tratar la desinformación como una amenaza más —del mismo modo que, hace tiempo, ya empleamos, por ejemplo, con las inyecciones SQL o los XSS— y aplicar, por tanto, todo el conocimiento adquirido para protegerlos de su impacto.

Defensa Activa contra la desinformación

La desinformación ha abierto un nuevo debate; un debate en torno a la posibilidad de escalar en la defensa activa, en ejecutar acciones que permitan compensar el efecto multiplicador que tiene una secuencia encadenada de datos intencionadamente manipulados.

El sector la ciberseguridad lleva tiempo trabajando en cómo definir y legalizar este tipo de acciones, apoyándose fundamentalmente en técnicas como la Inteligencia Artificial. En la actualidad, ya existen soluciones **que catalogan la veracidad** de una información; el empleo de **información de contexto veraz** con la que contrastar los datos manipulados; la **lucha contra el atractivo económico** —por ejemplo, *click-baits*— que supone el consumo de este tipo de información; los **filtros tecnológicos** que impiden su propagación telemática (p.ej. la restricciones en dominios de Internet);

la identificación visual de la manipulación de la información frente las nuevas *deep fakes*; o el desarrollo de **herramientas de verificación o portales fact-checks**⁵.

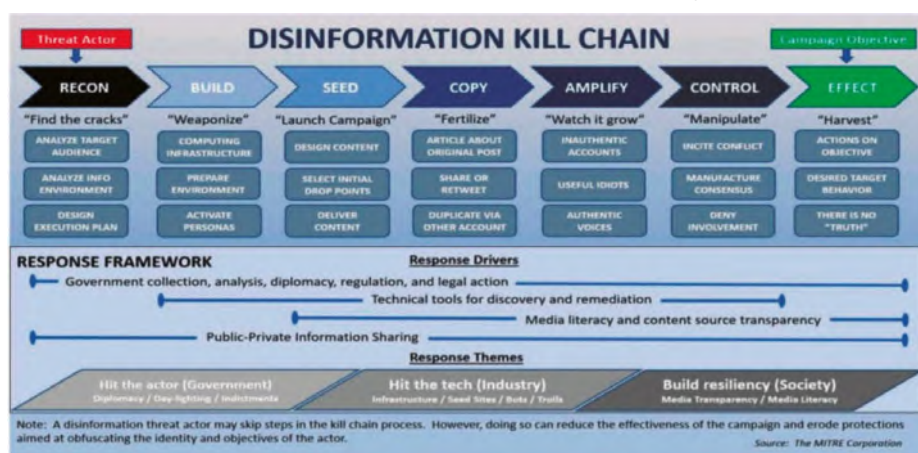
Una estrategia contra la desinformación podría desarrollarse, por ejemplo, tomando medidas que mantengan analogías con las tradicionales técnicas de ciberdefensa y que incluirían, entre otros, los siguientes pasos:

- **Un control muy riguroso de los registros de nombres en Internet.** De hecho, la Comisión Europea ha publicado una propuesta de Directiva NIS 2, que considera a los registros de dominios de primer nivel (TLD) como "entidades esenciales", junto a otros actores que

de *malware* y *spam* podría y debería ser aplicada a la identificación de campañas de desinformación.

- **La colaboración entre entidades**, y el intercambio de información de dominios divulgadores, remitentes de noticias falsas, servidores utilizados, usuarios en RRSS, etc. sería vital para poder implantar mecanismos de bloqueo eficaces y con la agilidad necesaria para que fueran realmente efectivos. Podríamos pensar en un modelo similar al que ya se realiza con LUCIA (CCN-CERT), o al intercambio de información entre la red de SOC Nacionales.

- **El uso de noticias certificadas** (como ya se planteó en su día con el código fuente certificado para el



son "críticos para la integridad de internet". Ligado al control de registros de dominios estaría el bloqueo en los sistemas de seguridad basados en el filtrado DNS de cualquier dominio no confiable.

- **La reputación o el rating de los proveedores de información o de una información concreta.** Hace más de 20 años que desde el sector se empezó a implantar la reputación de los remitentes de correo para controlar el spam y hoy en día, sigue siendo el mecanismo con el que más correo electrónico se bloquea. Sería preciso por tanto incorporar un esquema de reputación para la difusión de noticias que pudiera estar ligado al propio emisor o al contenido concreto (algo que sería más eficaz, si bien más costoso de mantener en el tiempo).

- **La supervisión y control de perfiles en las redes sociales.** Las grandes tecnológicas, Facebook⁶, Twitter⁷ o Google⁸, ya han desarrollado **herramientas para verificar la veracidad de los datos divulgados**. Por tanto, aplicar algoritmos de IA para identificar y bloquear perfiles dedicados a su difusión no debería de ser una tarea demasiado complicada.

- **Identificación de patrones.** La experiencia de tantos años en el análisis heurístico para la detección

desarrollo de aplicaciones seguras) sería sin duda alguna un gran avance en este sentido, siempre ligado, una vez más, a la integración de estos certificados, tal y como se emplea en herramientas de seguridad en el correo y la navegación por Internet. Sin embargo, esta aproximación aún presenta algunas dudas ya que podría convertirse en un arma de doble filo que tocaría de lleno el derecho a la libertad de expresión. El problema en este caso no sería técnico, sino político y habría que determinar quién *le pone el cascabel al gato*, o lo que es lo mismo, quién certifica (con una firma digital, por ejemplo) que una noticia es verdadera o no.

Como puede observarse, al final, es posible que a partir de ahora tengamos que empezar a pensar y a hablar de Sistemas de Defensa Activa contra la desinformación, clasificando las estrategias y tácticas de estos agentes de modo análogo a cómo se definen en la *Cyber Kill Chain*, pero aplicadas, esta vez, a los procesos de desinformación (p.ej. *Disinformation Kill Chain*⁹). ■



ALFONSO FRANCO
CEO & Managing Director
ALL4SEC
alfonso.franco@all4sec.es

¹ <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>

² <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>

³ <https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat/>

⁴ https://firstdraftnews.org/wp-content/uploads/2019/10/Information_Disorder_Digital_AW.pdf?x76701

⁵ <https://euvsdisinfo.eu/>

⁶ <https://about.fb.com/news/tag/misinformation/>

⁷ https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information

⁸ <https://toolbox.google.com/factcheck/explorer>

⁹ https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf

Trellix

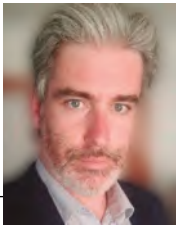
Una ciberseguridad dinámica para un mundo dinámico.

Cuando tu plataforma puede aprender y adaptarse, los ciberdelincuentes no son un problema para tu empresa. Descubre cómo Trellix te mantiene seguro.

trellix.com



Teletrabajo: reto técnico, reto humano



Este artículo aborda el nuevo escenario desde una perspectiva tanto técnica como humana, haciendo especial hincapié en el posible impacto del trabajo en remoto en la psicología de los trabajadores y diversas medidas de control para evitar la aparición de *Insider Threats* derivados del sentimiento de desapego que puede surgir en esta nueva fórmula de trabajo. A su vez, la parte técnica aborda las buenas prácticas y características de las configuraciones VPN así como las recomendaciones en materia de Políticas de Teletrabajo seguro basadas en los principales *frameworks* de referencia de NIST o CCN-CERT, entre otros.

Antonio Delgado

En una entrevista de 1964 para la BBC, el escritor y científico británico Arthur C. Clarke, autor de reconocidas novelas de ciencia ficción como "2001: Una odisea del espacio" y "El centinela", afirmaba que los ordenadores permitirían en el futuro "realizar cualquier actividad ejecutiva, administrativa o incluso física independientemente de la distancia". Casi 60 años después, con una pandemia de por medio y no pocas reticencias en los consejos de administración de medio mundo, parece que el teletrabajo ha venido para quedarse.

Es innegable que el trabajo a distancia conlleva enormes ventajas tanto para los trabajadores, (véase autonomía, flexibilidad y conciliación familiar) como para los empresarios, gracias a la mejora de la motivación de los empleados, la reducción de costes en oficinas o el acceso a mejores profesionales. Las ya conocidas soluciones de mensajería y plataformas de colaboración y la generalización de la fibra óptica y las conexiones inalámbricas (con un amplio despliegue del 5G y tecnología satelital a la vuelta de la esquina) han facilitado enormemente la transición a este nuevo modelo de trabajo. España, a pesar de tener una fuerte impronta de la cultura del "presencialismo" laboral en comparación con nuestros vecinos europeos, ha sabido adaptarse al nuevo modelo con bastante solvencia, para sorpresa de reticentes e incrédulos.

No obstante, no todo son ventajas en el teletrabajo, la dificultad para organizar proyectos complejos, la desvinculación emocional de los trabajadores con la empresa o el aislamiento social son algunos inconvenientes que deben tenerse en consideración. Entre los problemas derivados del teletrabajo, cabe destacar especialmente todos aquellos riesgos tecnológicos que pueden afectar a la seguridad de las comunicaciones y por extensión a la confidencialidad, integridad y disponibilidad de los activos de información. La utilización de redes inseguras, el robo o pérdida de dispositivos en lugares públicos o la dificultad de gestionar incidentes de seguridad con la misma eficacia que en el modelo presencial, son solo algunos de los riesgos que las organizaciones deberán seguir abordando, considerándose los aspectos operativos, técnicos y humanos.

SENTANDO LAS BASES: LA POLÍTICA DEL TELETRABAJO

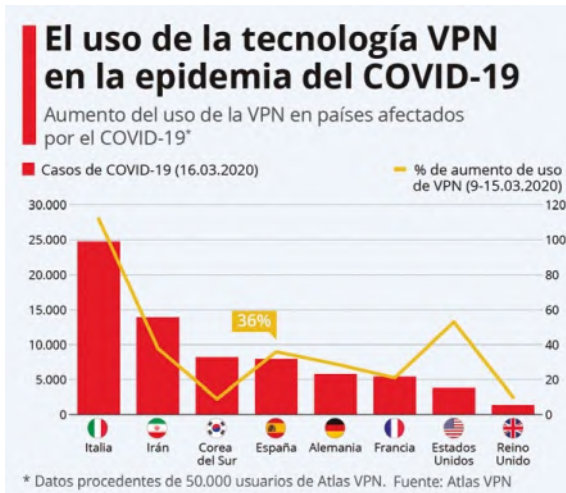
Establecer un entorno de teletrabajo seguro debe comenzar por la elaboración de una Política de teletrabajo que consolide por escrito el alcance, los procedimientos, así como los controles adecuados para que el trabajo se realice acorde a una serie de requerimientos de seguridad y objetivos de negocio previamente definidos. Documentos de referencia como CCN-CERT BP/18, NIST SP 800-46 o la guía del gobierno de Estados Unidos para el teletrabajo, entre otros, recopilan buenas prácticas y recomendaciones para definir los cimientos de una adecuada política.

El documento deberá incluir los procedimientos operacionales a cumplir por los trabajadores que accedan a los sistemas de información de la organización fuera de sus instalaciones, así como las soluciones y controles tecnológicos a considerar para una adecuada seguridad de las comunicaciones y los activos tecnológicos.

El procedimiento para la solicitud y aprobación del trabajo fuera de las instalaciones de la organización deberá definirse por escrito, siendo recomendable restringirlo a aquellos usuarios cuyo perfil contemple un mayor riesgo para la seguridad de los activos, véase administradores o

con acceso a información sensible, entre otros. Es imprescindible que la política incluya la obligatoriedad de utilizar conexiones seguras mediante VPN y la utilización de mecanismos de autenticación robustos, con especial atención al doble factor de autenticación.

La implementación de cifrado de los discos duros (especialmente en los ordenadores portátiles) es fundamental, más si se considera el aumento de posibilidades de robo o pérdida de los dispositivos fuera del entorno de la organización. Se recomienda aumentar la frecuencia de las copias de seguridad periódicas de los dispositivos utilizados, la sincronización de elementos críticos, y la verificación de su integridad de forma periódica. Entre las medidas de seguridad física a considerar se recomiendan la utilización de filtros de



Controlar de forma periódica y eficiente el sentimiento de pertenencia de los trabajadores con sus organizaciones reducirá las amenazas internas. El despliegue de soluciones DLP que monitoricen, detecten y restrinjan las fugas no autorizadas, ya sea en uso, movimiento o reposo cobran especial relevancia en este nuevo escenario.

privacidad para las pantallas de los portátiles y candados de seguridad siempre que sea posible. Es recomendable que se disponga de un listado de los usuarios que trabajen a distancia para facilitar el control y trazabilidad por parte de la organización cuando sea necesario. Y por último y no menos importante, la Política de teletrabajo debe acompañarse de acciones formativas que instruyan a los trabajadores en un correcto uso de los dispositivos informáticos fuera de las instalaciones corporativas y de los riesgos que ello supone.

VPN, LA PIEDRA ANGULAR DEL TRABAJO REMOTO SEGURO

Si algo hemos podido verificar en los últimos años es que las comunicaciones a través de Internet están cada vez más expuestas a toda clase de riesgos. A los propios tecnológicos inherentes a la utilización de telecomunicaciones, se deben añadir entre otros, el aumento cada vez mayor de ciberataques por grupos criminales y *hacktivistas*, el espionaje industrial o las intromisiones de los servicios de inteligencia. La utilización de VPN (en inglés, *Virtual Private Network*) permiten la extensión de las redes privadas a través de cualquier red pública con todas las ventajas en

CONTROL TOTAL Intercambio seguro de la INFORMACIÓN



A golpe de
click



Powered by Microsoft



Generación de
documentos



Etiquetado



Prevención Fuga
Información
(DLP)



Protección de la
Información
(IRM)



Atención
incidencias

materia de seguridad, accesibilidad y la funcionalidad que eso supone.

Y por lo general cumplen el cometido de garantizar la confidencialidad, integridad y autenticación de los clientes durante las transmisiones de información a través de redes no tan confiables como las corporativas. El funcionamiento de las VPN es sencillo: la información se cifra (habitualmente utilizando protocolos y algoritmos seguros) y solo puede ser descifrada por un sistema que disponga de la clave adecuada (previamente compartida), haciendo harto difícil el acceso no autorizado. Las arquitecturas VPN las podemos clasificar fundamentalmente en dos tipos:

– **VPN de acceso remoto:** son las más habituales en entornos empresariales y se utilizan principalmente para proteger las comunicaciones entre los dispositivos utilizados por los trabajadores y las redes privadas de sus respectivas organizaciones. Las VPN de acceso remoto permiten que los empleados puedan acceder a los recursos corporativos (intranet, aplicaciones, información, etc.) a través de Internet de forma segura. Su utilización requiere fundamentalmente dos elementos: clientes VPN instalados en los dispositivos de los trabajadores y concentradores de VPN (*Gateways*), dispositivos de hardware instalados en la red de la organización que permiten la conexión segura con los respectivos clientes.

– **VPN de sitio a sitio:** se utilizan para conectar dos redes (véase las redes de dos oficinas geográficamente distantes) a través de Internet, buscando más persistencia al establecer una conexión segura continuada entre ambas. Esta modalidad se basa en la comunicación de un *router* que actúa como servidor VPN con otro que actúa como cliente. Se pueden implementar tanto en *intranets* que pertenecen a la misma organización, como en *extranets* que pertenecen a organizaciones distintas.

Si bien la utilización de soluciones VPN aporta enormes ventajas en materia de seguridad para la organización, ha de considerarse que la velocidad de conexión y el rendimiento de las aplicaciones puede disminuir con su utilización, por lo que se recomienda una evaluación del impacto sobre la operativa de negocio antes de su despliegue, así como su escalabilidad (conexiones totales permitidas). El esfuerzo del mantenimiento de los clientes, servidores y concentradores VPN, el soporte a los usuarios (instalación, restauración de contraseñas, etc.) son costes que han de considerarse. Se deben verificar además pormenorizadamente las condiciones de servicio (rendimiento, capacidad, etc.), así como sus políticas de privacidad para evitar que los datos se compartan con terceros. Se ha de considerar por último y no menos importante, implementar las recomendaciones recogidas en las propias guías de bastionado y 'securización' de los fabricantes VPN.

LA IMPORTANCIA DEL FACTOR HUMANO

En un sector con una dependencia tecnológica tan aguzada como la ciberseguridad, el factor humano puede tender a difuminarse en la empresa y no siempre se le otorga el peso necesario que debería tener. En ocasiones se echan en falta los nuevos retos que deben abordarse no solo desde una perspectiva tecnológica y operativa, sino aquellos vinculados también al factor humano y el bienestar de los propios trabajadores. En una encuesta elaborada por la **American Psychiatric Association** a 1.000 teletrabajadores en 2021, la mayoría afirmó haber experimentado efectos negativos en su salud mental, incluyendo sensaciones como el aislamiento, la soledad o la dificultad para alejarse del trabajo al final de la jornada.

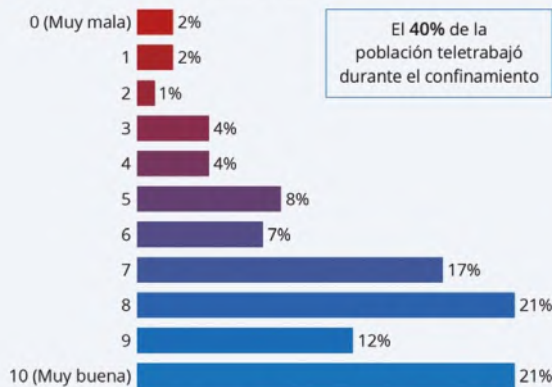
El nuevo escenario de teletrabajo supone que las organizaciones deberán definir estrategias que garanticen el bienestar de los empleados y refuercen el sentimiento de pertenencia a la empresa y a sus equipos. Dicho escenario que se presenta requerirá que los departamentos de Recursos Humanos incluyan figuras especializadas en psicología laboral y se elaboren estrategias que permitan supervisar periódicamente el estado emocional de los empleados y sus índices de satisfacción. Los modelos de teletrabajo "híbridos" que combinen el trabajo presencial y a distancia o disponer de espacios colaborativos de trabajo donde los empleados puedan acudir con carácter voluntario, son solo algunas soluciones que están siendo adoptadas por las principales empresas tecnológicas. Se debe

otorgar a los empleados la capacidad de elegir donde desarrollar sus funciones siempre que no sea incompatible con la consecución de sus responsabilidades y los objetivos de negocio. Aquellos empleados con responsabilidades familiares como tener hijos a su cargo o personas dependientes, deberán ser objetivo prioritario para incorporarse al modelo de trabajo a distancia.

Controlar de forma periódica y eficiente el sentimiento de pertenencia de los trabajadores con sus organizaciones reducirá además las amenazas internas o *insider threats*, véase aquellas que provienen de personas dentro de la organización. El despliegue de soluciones DLP (*Data Loss Prevention*) que monitoricen, detecten y restrinjan las fugas de información no autorizadas, ya sea en uso (dispositivos), movimiento (tráfico de red) o reposo (almacenamiento), cobran especial relevancia en este nuevo escenario. La implementación de DLP puede

El 71% de los españoles, contentos con el teletrabajo

Valoración de la experiencia con el teletrabajo durante el confinamiento en España*



* Encuesta realizada a 1.023 personas de 16 a 75 años entre el 6 y el 8 de abril de 2020. Fuente: El Departamento; Netquest

El 40% de la población teletrabajó durante el confinamiento

Si bien el uso de soluciones VPN aporta ventajas para la organización, ha de considerarse que la velocidad de conexión y el rendimiento de las aplicaciones puede disminuir con su utilización, por lo que se recomienda una evaluación del impacto sobre la operativa de negocio antes de su despliegue, así como su escalabilidad (conexiones totales permitidas).

combinarse además con el despliegue de controles IRM (*Information Rights Management*), que añadan una capa de seguridad extra mediante el cifrado de archivos, la restricción de los permisos (acceso, escritura, impresión, etc.) y la trazabilidad de las acciones realizadas por los usuarios.

La manida expresión "el teletrabajo ha llegado para quedarse" se ha convertido en una realidad indiscutible en nuestra sociedad. Si bien la infraestructura tecnológica y las capacidades necesarias para instaurar el trabajo a distancia hace años que estaban a nuestro alcance, la pandemia de coronavirus ha sido determinante para su rápida e inesperada implementación, demostrada efectiva. Las organizaciones deberán adecuarse a este nuevo escenario teniendo en consideración los aspectos tecnológicos, (seguridad de las telecomunicaciones y de los activos de información), organizativos, operativos y humanos. Una adecuada gestión del teletrabajo puede suponer un aumento significativo de los índices de felicidad de los empleados y el incremento de su productividad y motivación, así como la reducción de los costes empresariales en oficinas y otras instalaciones, entre otras muchas ventajas. Si intelectuales como Arthur C. Clarke ya lo anunciaban allá por los años 60, demasiado tiempo hemos tardado en adaptarnos a esta nueva realidad. Esperemos que no sea necesario otro cisne negro y brinde la proactividad necesaria. ■

ANTONIO DELGADO
Consultor de Ciberseguridad
CAPGEMINI

The background of the entire page is a photograph of the Terracotta Warriors and Horses from the Qin Dynasty. The image shows a dense array of life-sized clay soldiers standing in rows, wearing detailed armor and having distinct facial features. The lighting is somewhat dim, highlighting the texture of the terracotta.

La seguridad del emperador eterno

Los Guerreros de Xi'an

Qin Shihuang, "el primer emperador de China" (259-210 a.C.), mandó construir un ejército de más de 8.000 soldados de terracota, para mantener su seguridad y la de su imperio más allá de la eternidad.



epicbounties

The fastest-growing Bug Bounty Platform

www.epicbounties.com



Devo: la seguridad analítica en la empresa llevada a un nuevo nivel

En ciberseguridad solo podemos estar seguros de una cosa: el panorama de amenazas cibernéticas está en constante evolución, y las herramientas y soluciones que tenemos a nuestra disposición para combatir la ciberdelincuencia han de seguir creciendo si queremos adelantarnos a ellas, o al menos seguirles el ritmo. Precisamente, en este sector, el objetivo de Devo –logging corporativo y análisis de seguridad– es convertirnos en el corazón de las operaciones de seguridad de una organización.



Marc van Zadelhoff

La transformación digital, y la gran cantidad de amenazas asociadas a ella, han convertido el análisis de seguridad en la pieza central de las ciberdefensas. Pedro Castillo y nuestros fundadores crearon Devo pensando en esta transformación, y ahora las principales empresas del mundo confían en nosotros porque combinamos una escala inigualable, una potente analítica y la capacidad de obtener respuestas en tiempo real, lo que ha cambiado radicalmente la forma en que los equipos de seguridad interactúan con sus datos.

datos de una manera que no era posible anteriormente. Más allá de las funciones más potentes a nuestra disposición, tenemos una mayor confianza en la información obtenida de nuestros datos. Estamos sorprendidos por las mejoras de la plataforma y esperamos que nuestra empresa siga beneficiándose de ellas”.

Sólo en los últimos doce meses, Devo ha crecido de tal manera que corrobora la fuerza disruptiva en la que se ha convertido y envía una señal al sector: seguiremos marcando el ritmo de la innovación, aportando valor al cliente.



El pasado octubre Devo alcanzó un hito extraordinario. Anunciamos una ronda de financiación Serie E de 250 millones de dólares, lo que nos catapultó a una valoración de 1.500 millones de dólares, convirtiendo a Devo en el primer unicornio de ciberseguridad fundado en España.

Uno de nuestros clientes, Joe Wilson, director de inteligencia de amenazas informáticas de Ulta Beauty, describe muy bien el valor que Devo aporta a su equipo de seguridad:

“Ante la evolución de las necesidades y el aumento del volumen de datos, nuestro equipo necesitaba una solución con escalabilidad y visibilidad bajo demanda, eficaz y eficiente. Gracias a Devo Security Operations hemos encontrado una solución SaaS escalable y nativa en la nube que da forma y analiza nuestros

Devo alcanza el estatus de unicornio

El pasado mes de octubre, Devo alcanzó un hito extraordinario. Anunciamos una ronda de financiación Serie E de 250 millones de dólares, lo que nos catapultó a una valoración de 1.500 millones de dólares, convirtiendo a Devo en el primer unicornio de ciberseguridad fundado en España.

Me incorporé a la compañía en otoño de 2020 y, gracias a esta nueva fi-

nanciación, he podido avanzar mucho más rápido de lo estipulado en las líneas estratégicas que tracé cuando me convertí en consejero delegado. Me propuse que Devo creciera de forma significativa en nuevas regiones y sectores del mercado, aumentar nuestra inversión en la expansión del canal y lanzar al mercado nuevas innovaciones de productos que supusieran un cambio real para nuestros clientes. Desde entonces, Devo se ha expandido a la región APAC, ha lanzado el *Devo Drive Partner Program* y el *Technology Alliance Partners*, y ha estrenado nuevos productos y servicios como **Devo Content Stream**, **Devo Flow** y **Devo Exchange**.

Además, también hemos construido una increíble cultura que abraza nuestras raíces españolas y que se traslada a nuestros empleados en todo el mundo. Devo tiene ahora más de 400 profesionales en Europa, Norteamérica y la región APAC, todos ellos con estrechos vínculos con nuestra oficina fundadora en Madrid.

Devo Content Stream

En 2021, Devo presentó el nuevo Devo Content Stream, un nuevo servicio de distribución de contenidos, con el que ofrece un gran valor a los clientes de forma sencilla dentro de la plataforma de Devo. De esta manera, los equipos de seguridad disponen de acceso instantáneo y entrega continua de alertas predefinidas e información sobre amenazas que pueden utilizarse en cuestión de segundos.

Gracias a esta nueva solución, Devo Security Operations puede recibir continuamente amenazas y alertas curadas, todo ello proporcionado por Devo y sus *partners*. A medida que surjan nuevas amenazas, los clientes de Devo recibirán automáticamente nuevas detecciones e información, y podrán poner este contenido en práctica inmediatamente. Los equipos de seguridad ya no tendrán que crear sus propias alertas o curar manualmente la información sobre amenazas para estar al día sobre otras nuevas o que se encuentren en desarrollo.

Devo Flow

Los ataques no son sólo eventos puntuales, o incluso del sistema, sino que implican una cadena de actividades en múltiples frentes. El reto no consiste sim-



plemente en gestionar la acumulación de alertas, sino en convertir ese volumen de señales en información práctica.

A finales del pasado año lanzamos Devo Flow para combatir este desafío. El nuevo motor de correlación visual hace que los análisis de *streaming* sean una realidad para los equipos SOC, permitiendo a los analistas detectar ataques avanzados en tiempo real, a escala. Con un editor visual fácil de usar e intuitivo, DevoFlow agiliza el despliegue de correlaciones y análisis avanzados en datos de *streaming* en tiempo real y permite a los equipos de seguridad crear fácilmente alertas sofisticadas y enriquecer, transformar y combinar datos en Devo Platform.

Devo Exchange

Con el rápido crecimiento de los volúmenes de datos y un panorama de amenazas en constante expansión, los equipos de seguridad siguen estando muy divididos y, con demasiada frecuencia, se ven abrumados por cargas de trabajo demasiado elevadas. Los equipos de seguridad necesitan ser más ágiles a la hora de analizar los datos y actuar sobre ellos, para detectar rápidamente amenazas, visualizar riesgos e implementar nuevos casos de uso sin el esfuerzo que supone la creación de contenidos a medida. Con Devo Exchange a su disposición, nuestra comunidad de usuarios podrá alcanzar todos estos objetivos operativos y de seguridad y, de esta forma, incrementar el estado general de la seguridad de sus negocios.

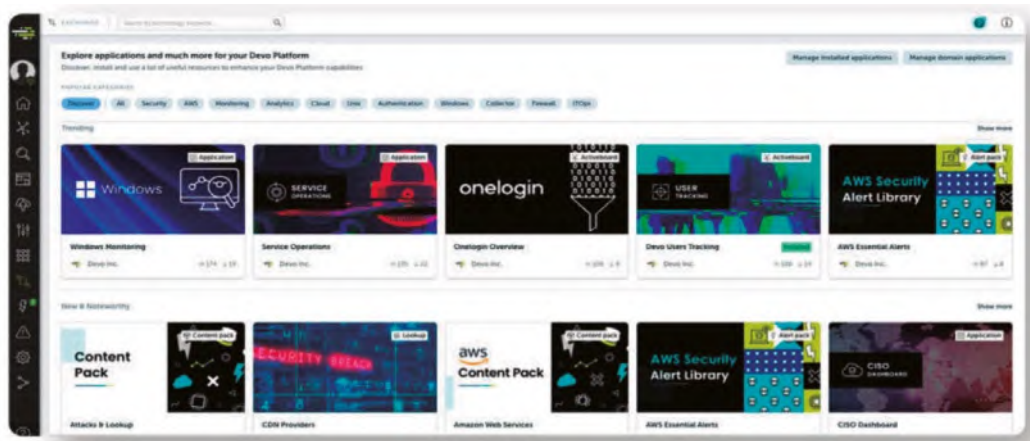
Lanzado en febrero, Devo Exchange está diseñado para agilizar y ampliar las capacidades y la experiencia de los equipos de seguridad. Además, proporciona acceso inmediato y a la demanda a un catálogo de contenido meticulosamente seleccionado por Devo, que la propia compañía, sus socios y la comunidad del mundo de la seguridad en general crea, colabora y comparte. Devo Exchange reduce notablemente el tiempo y esfuerzo necesarios para que clientes y *partners* creen y compartan contenidos que hagan las operaciones de seguridad más precisas y decisivas.

Cuando lanzamos este producto, el CISO de la Universidad de Oklahoma

(una de las principales universidades públicas de Estados Unidos) nos dijo que Exchange daría acceso a su equipo de seguridad a un valioso contenido que podrían aprovechar para optimizar sus capacidades de respuesta a incidentes y minimizar el ruido y la complejidad a la que se enfrenta el SOC.

elementos que atacar. Esta última oleada de actividad de *hacking* es la razón del éxito de empresas como Devo, ya que el sector de análisis de seguridad siempre busca a los mejores porque los hackers siempre son los mejores.

Al igual que empezamos el año con el lanzamiento de Devo Exchange, creo que



Devo se ha expandido a la región APAC, ha lanzado el Devo Drive Partner Program y el Technology Alliance Partners, y ha estrenado nuevos productos y servicios como Devo Content Stream, Devo Flow y Devo Exchange.

Mirando hacia el futuro

Como he comentado al principio de este artículo, lo único seguro en materia de ciberseguridad es que las ciberamen-



zas siempre cambian, siempre habrá un próximo ataque. De hecho, ahora mismo estamos observando un pico de actividad de *hacking* relacionado con el rápido aumento del tamaño de la superficie de ataque en los últimos años –no hay mejor ejemplo que log4j, que podría ser la mayor vulnerabilidad que hemos visto en los últimos diez años–. Todo se está trasladando a la nube, lo que significa que los *hackers* tienen un mayor número de

veremos cómo todo el sector adopta un enfoque basado en la comunidad para mejorar las operaciones de seguridad. Los entornos, las plataformas, los servicios, las regiones y los husos horarios que constituyen las operaciones de las empresas modernas e impulsan la transformación digital de los negocios siguen requiriendo una especialización y unos conocimientos cada vez mayores que van más allá de las capacidades internas actuales. Los *marketplaces* de contenidos y aplicaciones abordan directamente los problemas a los que se enfrentan los equipos de seguridad, pero el sector aún se encuentra en las primeras etapas de cualquier tipo de evolución. En este momento, las organizaciones deben analizar sus operaciones de seguridad y decidir cómo se van a reorganizar y qué van a priorizar para descubrir e incorporar las personas, las herramientas y los socios necesarios para tener éxito y seguirles el ritmo a los atacantes. ■

MARC VAN ZADELHOFF
CEO
DEVO

El 80% de las compañías consideran la ciberprotección una “prioridad estratégica” pero no invierten lo necesario

La falta de profesionales de ciberseguridad ya preocupa al 90% de los CISOs y ejecutivos de TI

La preocupación por contar con profesionales cualificados en ciberseguridad continúa siendo uno de los grandes retos de todas las empresas. Así lo ha constatado en su informe ‘Cyber Security in Focus 2022’, la firma **Stott y May** y la compañía de capital riesgo **Forgepoint** en el que ha contado con la participación de más de medio centenar de ejecutivos de ciberseguridad, un 36% CISOs de EMEA (Europa, Oriente Próximo y África) y de EE.UU.

Entre los aspectos más llamativos destaca la unanimidad existente por la falta de expertos en ciberprotección, en todo tipo de roles. De hecho, un 87% de los encuestados -frente al 76% de la edición anterior- reconocieron que están enfrentándose de forma continua al reto de conseguir contratar los profesionales que precisan y que no resulta fácil. Prueba de ello es que un 35% de las vacantes no se pudieron cubrir, según la encuesta, en tres meses. Incluso mucho más, ya que, según datos de la asociación (**ISC**)², actualmente hay sin cubrir en el mundo en torno a 2,7 millones de vacantes de ciberprotección -sólo en EE.UU. más de 375.000-. Y esta carestía se agudiza en tres especialidades según el informe: detección y respuesta, ciberseguridad de productos, y aplicación y protección en la nube.

Los participantes también destacaron como su gran preocupación la carencia de habilidades internas (43%) para cubrir estos puestos, lo que supone un importante freno a la estrategia de ciberseguridad que implementan las compañías. La falta de profesionales ya es considerada, según el estudio, como el principal problema para lograr una protección cibernética y control del

riesgo. Por delante de otros retos, muy habituales, como la falta de presupuesto (35%) y el empleo eficaz de la tecnología (13%). Un aspecto que también han destacado los preguntados por su preocupación por la proliferación de herramientas y proveedores, que aumentan la complejidad para sacarles partido. Por último, también se incluyó como factor de preocupación la falta de comprensión de la situación por parte de la alta dirección (9%).

Curiosamente, a pesar de que el 80% de los ejecutivos de ciberseguridad destacaron que sus empresas ven la protección cibernética como una “prioridad estratégica” -en el anterior estudio esta cifra era sólo de un 54%, más de la mitad (51%)-, también lamentó que esto no se plasme en una inversión acorde al ritmo que se está acometiendo para la transformación digital en la que están inmersas las compañías. Eso sí, un 5% destacó que la ciberseguridad aún se ve “como un gasto innecesario (5%)”, un problema técnico (15%) y una prioridad estratégica (80%).

Así pues, se valora mucho la ciberseguridad -incluso de cara a lo que aporta de imagen de marca a los clientes-, pero no se dedica a ello lo que se precisa. Por eso, el Director General de Forgepoint Capital, **William Lin**, considera que cada vez es más decisivo contar con CISOs preparados que sean capaces de acompañar la evolución digital de la compañía aportando experiencia, conocimiento y gestión eficaz a los desarrolladores para lograrlo de forma “rápida y segura”. O, dicho de otra forma: apuesta por el perfil del CISO centrado en la ingeniería y el ciclo de desarrollo de productos y servicios para primar la ‘seguridad por defecto’.

El documento también resalta que “la frecuencia y la magnitud de las ‘violaciones’ de datos de ‘alto perfil’”, la mayor concienciación de los clientes y el incremento de la regulación y estrategias digitales han creado la ‘tormenta perfecta’ para que los responsables de ciberseguridad aporten -y se vea- valor al negocio”. Prueba de ello, es que casi la totalidad de los participantes en la encuesta consideró que la ciberprotección se ve como un valor en la oferta que se hace a los clientes. Un incremento significativo respecto a

la edición anterior de este informe donde esta cifra se quedaba en un exiguo 31%.

Retos 2022

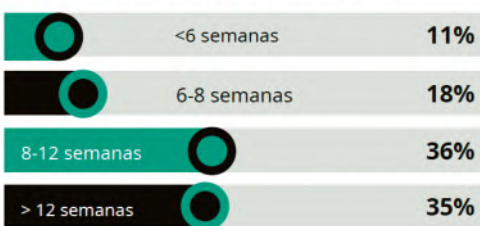
El informe termina dedicando un apartado amplio a analizar qué suponen estos resultados en el día a día y las responsabilidades de los CISOs. En él se recuerda que estos ejecutivos “se han quejado durante mucho tiempo de la falta de integración y consolidación, del uso de demasiadas herramientas, del exceso de ruido y confusión. Y que, con el tiempo, la frustración ha crecido en torno al gran volumen de proveedores y soluciones puntuales. Y esto está reduciéndose, por lo que la ‘ola de consolidación’ que estamos viendo actualmente, sin duda, será bien recibida por ese grupo de CISOs”.

De cualquier forma, recuerda que, a pesar de que se ha mejorado mucho, el gran problema para la ciberprotección de las empresas es que “no existe una ‘bala de plata’ o una herramienta estándar de facto que resuelva todos los desafíos que deben acometer los CISOs”. Así, el documento también explica que ello está motivando que los responsables de ciberseguridad están apostando por reducir la complejidad de lo que les rodea -recursos, tecnologías, procesos, etc.- sin depender de los proveedores “gestionando mejor el riesgo e identificando de forma clara qué supone un peligro y qué no”.

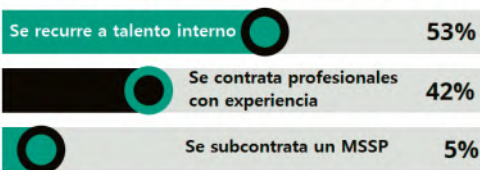
El beneficio de este conocimiento es que le permite evitar decisiones que pueden parecer arriesgadas en un determinado momento pero que, al final del día, no lo son en absoluto, según pone en valor el estudio. Por ello, vaticina que en 2022, los CISOs priorizarán los proyectos que se ajusten a una variedad de categorías de ciberprotección entre las que están desde disponer de lo último en tecnología para proteger redes y datos, hasta “volver a lo básico” en torno a la identidad, la respuesta a incidentes, la seguridad de la aplicación y del punto final. ■



TIEMPO MEDIO PARA CUBRIR VACANTES EN EL EQUIPO DE CIBERSEGURIDAD



¿CON QUÉ ENFOQUE REFUERZA SU CIBERPROTECCIÓN?



Mayores salarios

Así las cosas, este déficit está llevando a un incremento de los salarios, ya sea para atraer a nuevos profesionales o para conservar a los que se tiene. En total, un 54% de los responsables de RRHH destacaron un crecimiento medio de un 11% en el último año en el sector. “Otro 31% señaló que la inflación salarial se sitúa entre el 6% y el 11%. Este aumento en la compensación, vinculada a la demanda, ejerce una mayor presión sobre los CISOs cuando buscan asignar presupuestos”, destaca el informe.



Sería más fácil reparar este auto...
que utilizar un LMS convencional para concienciar en ciberseguridad.

www.smartfense.com
info@smartfense.com



Varios informes ponen en valor su trabajo, pero alertan del exceso de horas, estrés y falta de medios para realizarlo con éxito

El excesivo agotamiento del CISO pone en riesgo a las empresas ante la preocupación de que también les afecte la 'Gran Renuncia'

En 1995, Citigroup creó un nuevo cargo para 'mantener la seguridad de la información y las operaciones contenidas dentro de las infraestructuras tecnológicas internas de las que dependían las corporaciones'. Lo denominó 'Director de Seguridad de la Información (CISO)' y el designado fue Steve Katz, convirtiéndose en el primero en ejercer con tal denominación. Desde entonces, sus funciones han venido cambiando notablemente tanto en lo que atañe a su trayectoria, como a sus responsabilidades, capacidades y ubicación. Y con la denominada 'Gran Renuncia', la marcha voluntaria de millones de trabajadores en países como EE.UU. o en Europa, su labor se ha tornado aún más compleja y desafiante, según varios estudios recientes.

Los responsables de ciberseguridad de las empresas, posiblemente, nunca han tenido tanta tecnología, medios y recursos humanos. Pero, también, nunca han sufrido tanta presión por ofrecer a la Junta Directiva un indicador claro del menor riesgo posible y, sobre todo, de contar con los medios necesarios para hacer frente a ciberamenazas cada vez más complejas y dirigidas. A ello se suma ahora la tensión que supone la 'Gran Renuncia'. Se trata de un fenómeno que se detectó con fuerza en países como EE.UU. en 2021 con la renuncia voluntaria a sus trabajos de más de 50 millones de personas o de Italia, donde 1,3 millones presentaron su renuncia. En España, según las estadísticas de la Seguridad Social, esta cifra fue más discreta, en torno a 30.000 bajas voluntarias. Pero no hay que engañarse: muchos expertos alertan de que se trata de un fenómeno global y que puede impactar a corto y medio plazo con fuerza en sectores, como el de ciberseguridad, donde ya hay un déficit importante de profesionales.

No obstante, la situación aún no es preocupante. Así lo cree **Evanta**, una compañía de **Gartner**, que entrevistó a más de 225 profesionales de ciberseguridad en su estudio 'CISO Community Pulse', en octubre de 2021. Entre sus datos más llamativos, destaca que el 89% de los participantes explicó que el impacto de la 'Gran Renuncia' no ha sido superior en bajas a las vividas en años anteriores. Sólo un 11% destacó un incremento achacado a la búsqueda de un mejor salario, la posibilidad de teletrabajar –o hacerlo en modo híbrido–, mejor conciliación entre vida laboral y personal, y mayor empatía con la cultura de la empresa. Frente a esta situación de pérdida de talento, la encuesta reveló que las principales estrategias para captar nuevos profesionales pasan por 'ven-



der' una mejor cultura empresarial (67%), más flexibilidad laboral (65%) y mayores compensaciones económicas (49%).

foques (Zero Trust, SASE, etc.), el profesional que está al frente de la estrategia de ciberprotección de cada compañía también vive un momento complejo. Así lo constata un estudio de **Tessian**, realizado por **Forrester**, titulado 'Reclaiming Hours Lost to Cybersecurity Incidents', que ha contado con la opinión de más de 300 CISO de EE.UU. y Reino Unido.

En él, se destaca que la actual tensión y exigencia de estos profesionales es tal que, incluso, deben trabajar días festivos emblemáticos,

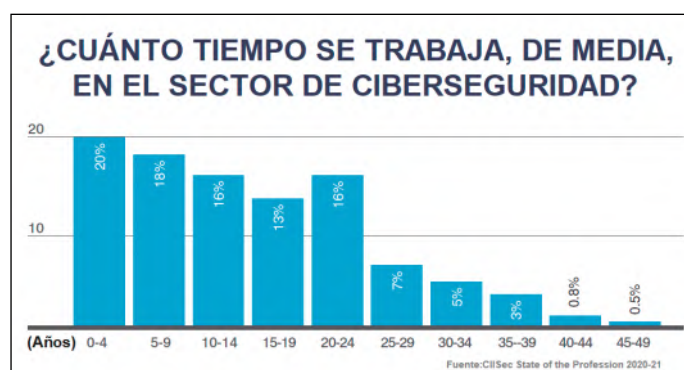
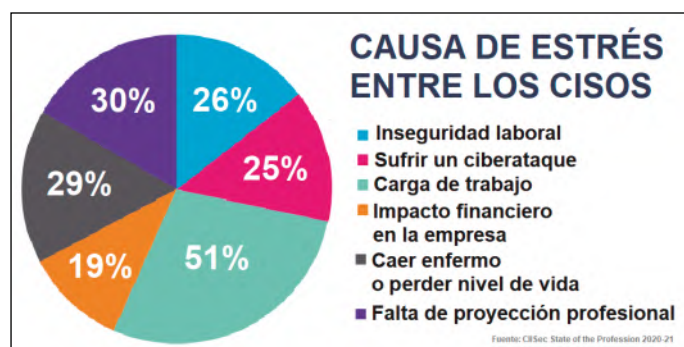
poder recuperar las horas perdidas a causa de incidentes de seguridad, en muchas ocasiones por errores humanos.

Falta de desconexión

Sirva como ejemplo que, según la encuesta, uno de cada cuatro CISO reconoció no haber cogido vacaciones en el último año, con 11 horas semanales más de las contratadas, que en un 10% de los casos llegan hasta las 24. Así, el 59% confesó que tiene serias dificultades para desconectar del trabajo al final del día. De las tareas que más tiempo les lleva son los incidentes causados por errores humanos, que el informe cuantifica en 600 por mes y que, en el caso de los CISO, suponen entre nueve y 12 horas al mes investigando este tipo de fallos. De hecho, el 34% de los preguntados lamentó que pasa demasiado tiempo clasificando e investigando incidentes. Uno de cada cuatro (38%) también destacó que pierde demasiado tiempo en reuniones o informando al Consejo, mientras que una cantidad algo inferior considera que "se siente agotado por las tareas administrativas". Como consecuencia, un 38% resaltó que dedica poco tiempo a su propio desarrollo profesional y que le gustaría tener más tiempo para contratar talento para su equipo (36%), asistir a reuniones no departamentales (38%), comunicarse con los clientes (35%) e investigar nuevas actualizaciones de la industria y tendencias (36%).

Sin tiempo para ir al médico

La exigencia de su responsabilidad es tal, que un 44% llegó a destacar que, además de faltar a eventos familiares o no poder disfrutar de días de vacaciones, incluso, han llegado a no acudir a citas médicas, con el riesgo que conlleva para su salud. Y en



Agotamiento de los CISO

Lo que está claro es que en un panorama donde el trabajo híbrido, la apuesta por la nube y el incremento de ataques de *ransomware* están dando pie a todo tipo de nuevos en-

en Norteamérica, como el de 'Acción de Gracias' o renunciar a parte de sus vacaciones para hacer bien su trabajo. Así, esta situación, según los participantes, está colocando a muchos CISO al borde del agotamiento. Precisamente, ello está incrementando su apuesta por la automatización para

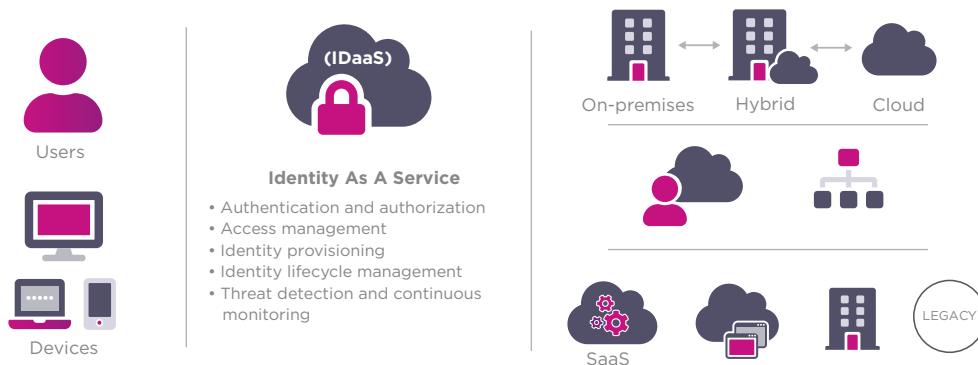
Entrust Identity as a Service

Todos los usuarios protegidos. Posibilidades ilimitadas para entornos híbridos.

Cloud-based Identity and Access Management (IAM) con cobertura para entornos híbridos

Entrust Identity as a Service (IDaaS) protege la identidad digital de su organización, garantizando un acceso seguro a los sistemas de sus clientes, trabajadores y partners.

Nuestra plataforma IAM permite aplicar un control de acceso basado en la estrategia Zero Trust, proporcionando una Autenticación, Autorización y control de acceso unificado a los recursos de la organización desde múltiples ubicaciones valorando el nivel de riesgo soportado en función del contexto de la conexión.



BENEFICIOS

Aplicación de Estrategia Zero Trust

Mantenimiento de la seguridad en identidad digital a través de la autenticación adaptativa basada en el contexto

Gestión IT Simplificada

Optimice el aprovisionamiento de usuarios, simplifique la gestión de identidades y aproveche las herramientas de autoservicios de usuarios. Opción de implementación tradicional o como servicio gestionado.

Mejore la experiencia de usuario

Proporcione una experiencia de usuario optima a través de adaptive risk-based authentication, SSO, passwordless login, Identity proofing y federación de aplicaciones cloud.

Cumpla con requerimientos normativos

Proteja la identidad de los usuarios y la privacidad de la información.

Implemente, gestione y crezca de una manera sencilla

Aproveche las múltiples APIs disponibles, integraciones OTS y SDKs

Evolucione según su organización lo requiera

A través de las características como adaptive risk-based authentication MFA, passwordless, identity orchestration y access management controls, IDaaS proporciona una protección integral para todos sus requerimientos actuales y futuros a través de una plataforma unificada.

PRINCIPALES FUNCIONALIDADES

- La mejor autenticación multifactor (MFA) de su clase
- Acceso basado en credenciales de alta seguridad
- Inicio de sesión único (SSO)
- Acceso sin contraseña
- Orquestación de identidad
- Gestión de autorizaciones y accesos
- Protección URL/API
- Autenticación y autorización embebida de aplicaciones en dispositivos
- Adaptive risk-based access and authentication
- Cifrado de correo electrónico y archivos, firma de documentos
- Identity Proofing
- Fraud detection and prevention
- Secure Portals
- Self-service password resets
- Integraciones, API y kits de herramientas para desarrolladores
- Disponible como un servicio Gestionado



ENTRUST

SECURING A WORLD IN MOTION

CONOZCA MÁS SOBRE NUESTRAS SOLUCIONES EN WWW.ENTRUST.COM/ES

© 2022 Entrust Corporation. All rights reserved.

torno al 30% achaca a su trabajo la falta de tiempo para hacer ejercicio de forma regular.

No es el único estudio que habla del agotamiento de los CISO. El informe 'The Burnout Breach', de la compañía 1Password, corroboró esta situación, confesándola el 84% de los participantes. Incluso, un 10% dejó claro que están "completamente desprotegidos" y que "hacen lo mínimo en el trabajo" debido al agotamiento. Además, un 44% afirmó estar 'muy cansados', y el 19% de los que sólo estaban 'agotados' llegaron a decir que sienten que las reglas y políticas de seguridad "no valen la pena".

Tres tipos de CISO

Asimismo, la firma de headhunter, **Heidrick & Struggles**, realizó en 2021 una encuesta a 354 CISO de todo el mundo, que publicó bajo el título '2021 Global Chief Information Security Officer (CISO) Survey'. En ella, identificó tres 'perfiles CISO': por un lado, el de ciberseguridad tradicional, por otro, el que apuesta por trabajar en reducir el riesgo y generar confianza y, por último, el que el informe denomina 'CISO Plus', que cuenta con mayores capacidades. Eso sí, sólo el 12% de los participantes en la encuesta destacó que este tipo de perfil es un puesto "ideal".

De cualquier forma, el 45% de los preguntados reveló que tienen responsabilidad en las tres áreas más frecuentes para este rol -seguridad, riesgo y confianza- y un 55% que ya están especializados en uno o dos de esos campos. Además, se comprobó que los sectores que más apuestan por este perfil laboral son los de tecnología y servicios financieros, con profesionales muy especializados.

Desafíos sin precedentes

Otro estudio, realizado por **Code42** junto con **Vanson Bourne**, destacó que el sector se enfrenta a "desafíos sin precedentes cuando se trata de proteger los datos corporativos confidenciales de la exposición, la fuga y el robo" por la adopción de



ÁREAS Y DPTOS. QUE REPORTAN AL CISO

Test de intrusión	90
Arquitectura de seguridad	90
Operaciones de seguridad	90
Gobernanza y riesgo	88
Seguridad de producto	85
Continuidad de negocio	37
Confianza	28
Gestión de crisis	28
Seguridad física	28
Privacidad	21
Fraude	18
Seguridad	18
Otros	12

Fuente: Encuesta global del director de seguridad de la información (CISO) de Heidrick & Struggles, 2021, n = 354 profesionales de seguridad de la información

la nube, el impacto de la 'Gran Renuncia', los empleados deshonestos y, también, los "malentendidos continuos y la mala comunicación entre las partes interesadas a nivel de la junta directiva, el liderazgo de seguridad y los profesionales de seguridad".

Solo el 21% de los presupuestos de seguridad cibernética de las empresas tienen un componente dedicado a mitigar el riesgo interno, y el 91% de los líderes senior en seguridad cibernética aún creen que la junta directiva de sus empresas requiere una

mejor comprensión del riesgo interno. Y no es un momento fácil por la popularización del trabajo en modo híbrido y por la mencionada "Gran Renuncia", que está poniendo en peligro miles de datos de propiedad intelectual, ya que en torno al 71% de los equipos de ciberseguridad preguntados desconocía con precisión qué datos se van cuando los empleados dejan la empresa. De hecho, el 71% de los responsables de ciberprotección también mostraron su in-

'CISO Circuit', **YL Ventures** destaca que 70% de los encuestados no creen que las soluciones TPRM (*third-party risk management*) les haya ayudado significativamente a evitar riesgos, por su falta de contexto, según destaca el 83%. En concreto, alertan de dos puntos ciegos críticos que impiden aprovechar el verdadero potencial del TPRM: cómo se interactúa con terceros y cómo se relacionan estos entre sí en sus propios entornos. Lo que supone un freno a la implementación con eficacia de estrategias como las de 'Confianza cero' y de protección del dato. No obstante, el documento recuerda que "esto no niega la utilidad actual de las soluciones TPRM, ya que todavía se encuentran entre los enfoques más completos disponibles para administrar la seguridad de la cadena de suministro".

Impacto de la pandemia

A estos datos se suman los ofrecidos por el británico **Chartered Institute of Information Security (CIISec)**, que ha publicado su sexto informe sobre el 'Estado de la profesión', con la opinión de 557 profesionales. En él, los participantes destacan, en un 61%, que las personas son el mayor desafío al que se enfrenta la ciberseguridad, aunque esta cifra ha mejorado algo, ya que en su edición precedente era de un 67%. En cuanto a las capacidades más buscadas entre perfiles de ciberseguridad el estudio destaca las de pensamiento analítico y resolución de problemas, mientras que las que menos son las 'habilidades de comunicación'. Además, alerta de que los "ambientes de trabajo tóxicos también parecen ser un problema persistente para la profesión" y que entre las razones que llevan a los profesionales de ciberseguridad a abandonar su trabajo están desde una mala gestión de los equipos de trabajo, ineficaz o desagradable, hasta el incremento de horas de trabajo por la pandemia: casi la mitad (47%) de los encuestados confesó trabajar más de 41 horas a la semana, y algunos, incluso, hasta 90.

Además, el 80% dijo que el personal de todas las organizaciones ha estado más ansioso o estresado durante la pandemia. Así las cosas, el 65% consideró que esta crisis sanitaria ha tenido un impacto algo o muy positivo en el mercado de seguridad en general y que la profesión está mejorando (82%). ■

¿Quieres detectar brechas legales y evitar multas y sanciones?



MIA es la primera solución en **Breach Hunting** que mediante Inteligencia Artificial detecta de forma automática Brechas Legales en las empresas.



Analiza la información interna en busca de vulnerabilidades legales.



Construye de forma automática un Mapa de Riesgos.



Ofrece soluciones legales para mitigar los incumplimientos detectados.



www.miaintelligence.com

Los sectores financiero y bancario, tecnológico y de consultoría los que más reclutan, aunque está creciendo mucho el *fintech*

La demanda de profesionales se dispara: seis de cada 10 confiesan estar abiertos a cambios en 2022

La compañía británica CyberShark Recruitment, especializada en contratación de perfiles de alta cualificación, publicó en febrero un completo estudio, junto a SC Media, sobre los sueldos medios en el sector de la ciberseguridad en el Reino Unido, con la participación de más de 1.200 profesionales. Quizá, el dato más significativo es el incremento del 16,55% de los sueldos en el último año, al cambiar de empresa o rol.

Eso sí, el 29% de los encuestados destacaron que en su caso esa cifra creció hasta el 26% o más. “Esto evidencia la gran demanda de la persona adecuada con las habilidades adecuadas para unirse a una organización”, recuerda el informe que, también, explica que la subida media del



bienar de trabajo en 2022 y que casi otro tanto no está trabajando en ciberseguridad pero espera hacerlo, la cifra alcanza el 62,78% por lo que organizaciones como LinkedIn hablan de esta situación como el momento de la “gran renuncia” por la cantidad de personas que cambiarán de trabajo en breve.



No todo es dinero

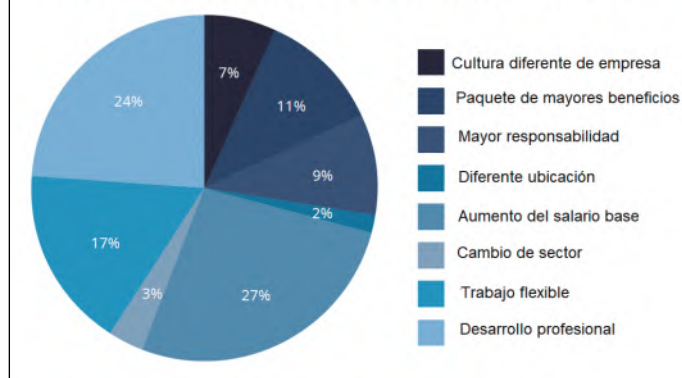
Entre los principales motivos para irse de la empresa, uno de cada tres participantes (27%) confesó que fue para conseguir un aumento de salario. “Cuando cambian de trabajo, las personas quieren ser recompensadas por el valor que aportan a una organización y existe un riesgo involucrado, por lo que necesitan un incentivo”, destaca el

estudio que también identificó cinco aspectos que animan a los candidatos a buscar otra empresa o responsabilidad: la mejora de la pensión contributiva, contar con asistencia médica privada, una bonificación por rendimiento y la posibilidad de mejorar su trayectoria profesional. Precisamente, los participantes en la encuesta lamentaron que sería deseable contar con más información y trayectorias claras para mejorar y no sufrir un desgaste excesivo en su trabajo.

De cualquier forma, sólo el 12,14% de los que cambiaron no lo hicieron “sólo por dinero”, aunque muchos destacaron la atracción que les suponen compañías que cuidan al trabajador y tienen una cultura de empresa acorde a lo que quieren.

El informe también destaca que “con más de 3,5 millones de puestos de seguridad cibernética abiertos en todo el mundo, es imposible que un candidato pueda revisar ni siquiera una fracción de las oportunidades dentro del mercado, además de trabajar en un puesto de tiempo

¿QUÉ ES LO MÁS VALORADO PARA CAMBIARSE DE EMPRESA?



salario para los profesionales que no cambiaron de empresa o responsabilidad fue de un 8,71%, lo que también es notable. Eso sí, cuatro de cada 10 profesionales que continuaron con normalidad en la empresa no tuvieron ningún aumento de salario. Incluso, un 21% vio reducida su retribución, pudiendo ser “un claro indicador de la pandemia”. De cualquier forma, el bonus medio pagado en 2021 creció un 13,71%.

Si a estas cifras se le suma que el 36,84% de los encuestados actualmente trabajando confesaron que buscarán cam-

¿CÓMO ESPERA ENCONTRAR SU PRÓXIMO TRABAJO?



¿Quién nos puede ayudar con la ciberseguridad industrial?



Catalogo.CCI-es.org



Centro de
Ciberseguridad Industrial



completo. Esta es la razón por la que el 31% de las personas optaron por contratar a un reclutador especializado". En este sentido, la empresa destaca que ello permite hacer una lista de todos sus deseos, necesidades, factores decisivos y lo que exactamente están buscando y pedir que se facilite una lista corta de roles que se ajustan a sus necesidades. De hecho, sólo un 5,78% de los profesionales se presentan a las empresas que quieren que las contraten.

Y el movimiento laboral es importante en el sector: el 66% de las personas encuestadas cambió de rol en los últimos dos años y el 43% en el último año. O sea que muy pocos profesionales permanecen en el mismo puesto o empresa al cabo de cuatro años. En cuanto a los perfiles más habituales de contratación, el 67% se encuadra dentro de los de consultor y analista, consultor y analista *senior* o gerente. Un aspecto que determina la gran demanda de los más especializados, con capacidad de gestión ejecutiva.

Procesos de contratación más rápidos

Además, el estudio evidencia que los procesos de contratación en ciberseguridad deben ser rápidos para ser eficaces. Por ejemplo, uno de cada tres profesionales cambió de rol en sólo dos semanas desde que envió el currículum hasta que la aceptaron. "Esto es extremadamente ágil y cuando observamos la demanda en el mercado y la tasa de 'deserción' en el sector en su conjunto, se hace evidente que las organizaciones, una vez que identifican a un buen candidato, se muevan rápido para protegerlo", explica el documento, que identifica el cambio de empresa en un plazo de solo cuatro semanas en el caso del 59% de los participantes. "Si su proceso de contratación consta de tres etapas, teniendo en cuenta el horario de trabajo del candidato y el del gerente de contratación, es probable que exceda esas

SALARIO MEDIO, SEGÚN PERFIL Y EXPERIENCIA, EN REINO UNIDO EN 2021

	1-4 años	4-7 años	7-10 años	10-15 años	15-20 años	20 + años
Gobernanza, riesgo y cumplimiento	47.005€	74.970€	82.110€	85.085€	110.670€	154.700€
	70.805€	92.820€	102.043€	110.075€	143.395€	190.400€
Arquitecto de Seguridad	63.070€	83.300€	98.175€	117.215€	136.255€	183.260€
	82.110€	104.125€	124.950€	160.650€	184.450€	228.480€
Ingeniero de Seguridad	60.690€	74.970€	92.225€	108.290€	133.280€	152.320€
	78.540€	94.010€	110.075€	130.900€	171.360€	182.070€
Respuesta a incidentes	47.600€	65.450€	77.350€	94.903€	113.050€	140.420€
	66.938€	86.275€	96.390€	120.488€	145.478€	181.178€
Descubrimiento electrónico y Forense	36.295€	53.550€	71.400€	80.325€	101.448€	119.000€
	51.765€	71.400€	89.250€	107.100€	130.900€	160.650€
Analista de Seguridad	47.600€	60.690€	77.945€	91.333€	107.100€	133.280€
	68.425€	79.730€	96.688€	107.398€	138.040€	167.790€
Seguridad de red	41.650€	53.550€	70.210€	85.085€	104.125€	116.620€
	54.145€	71.400€	88.060€	105.910€	120.488€	146.370€
Infraestructuras críticas	40.460€	53.550€	77.350€	101.150€	116.620€	142.800€
	57.715€	70.210€	101.150€	120.190€	139.230€	177.310€
Inteligencia de amenazas	46.708€	65.450€	89.250€	101.150€	116.025€	130.900€
	67.235€	80.920€	104.720€	130.899€	141.610€	159.460€
Test de intrusión	58.310€	78.540€	107.100€	142.800€	No disponible	No disponible
	82.110€	96.390€	135.660€	168.980€		
Riesgo Tecnológico y auditoría de TI	41.055€	57.418€	71.400€	78.838€	94.010€	116.025€
	58.310€	71.103€	88.060€	96.985€	120.190€	152.320€
Identidad y gestión de accesos	41.650€	53.550€	73.780€	89.250€	107.100€	119.000€
	53.550€	70.210€	91.035€	103.530€	130.900€	172.550€
Ciberresiliencia	35.700€	53.550€	77.350€	101.150€	116.620€	142.800€
	53.550€	70.210€	101.150€	120.190€	139.230€	177.310€
Gestión de continuidad de negocio	33.320€	53.550€	65.450€	88.060€	110.075€	130.900€
	51.170€	61.880€	89.250€	106.803€	127.330€	173.740€
Programa de recuperación de crisis	33.320€	53.550€	65.450€	88.060€	110.075€	130.900€
	51.468€	61.880€	89.250€	106.803€	127.330€	173.740€
Seguridad en la nube	41.650€	70.210€	77.350€	101.150€	142.800€	205.870€
	65.450€	91.630€	95.200€	130.900€	190.400€	257.635€

Fuente: 'Cyber Security UK salary survey 2022' de CyberShark Recruitment

cuatro semanas y no sea eficaz para conseguir el mejor talento", destacan desde CyberShark Recruitment.

Sectores tractoros

En cuanto a qué sectores son los que más profesionales atraen, encabeza el *ranking* el financiero y bancario, con un

26,78% de los casos, seguidos del tecnológico, con un 23,84% y de las empresas de consultoría, con un 15,48%. Algo que no va cambiar en el próximo año porque "estas organizaciones ofrecen variedad de trabajo, así como una sólida cultura empresarial y paquetes financieros considerables". El estudio sí destaca que el sector *fintech*

crecerá de forma significativa en contratación de profesionales de ciberprotección por cuanto "tienen nuevas tecnologías que desafían a los bancos, con un enorme respaldo financiero, lo que permite atraer a algunos de los mejores talentos del mercado con paquetes lucrativos y tecnología nueva e innovadora en la que trabajar". ■



Si te pillan...

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

Alerta Temprana

Respuesta



Monitorización Activa

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

Detección de Intrusión

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

Respuesta ante Incidentes

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

Equipo de Respuesta ante Incidentes

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

**SERVICIOS
GESTIONADOS
SOC 24x7**

OneseQ
by alhambra

OneseQ.es

Un informe del *think tank* germano SWP evidencia demasiadas carencias y pone como ejemplo a la alianza 'Five Eyes'

La atribución de ciberataques, un proceso lento y complejo en la UE que precisa de más inversión y "unidad de voz"

"Si conoces al enemigo y te conoces a ti mismo, no debes temer el resultado de cien batallas. Si te conoces a ti mismo, pero no al enemigo, por cada victoria que obtengas también sufrirás una derrota. Si no conoces al enemigo ni a ti mismo, sucumbirás en cada batalla", destacaba el general chino **Sun Tzu** en su célebre libro 'El arte de la guerra' hace más de 2.500 años. La atribución era y es un elemento fundamental ante una acción hostil y, ahora, en el ámbito cibernético es uno de los grandes 'talones de Aquiles' para países, empresas y, también, aseguradoras, ya que sin 'culpable' no existe la posibilidad de sanción o acción de defensa alguna.

Para analizar qué se está haciendo y qué se debería hacer en Europa para contar con más capacidades de atribución de ciberincidentes, el **Instituto Alemán de Asuntos Internacionales y de Seguridad (SWP)**, ha publicado un amplio informe en el que ofrece una visión en profundidad y pormenorizada de las iniciativas que tiene en marcha la UE y cómo se ha realizado la atribución hasta ahora, estudiando cinco ataques significativos: los mediáticos WanaCry, NotPetya, Cloud Hopper, Bundestag Hack y el perpetrado contra la **Organización para la Prohibición de las Armas Químicas (OPCW)**.

El documento comienza recordando que "la atribución de ciberataques es un acto soberano de los estados miembros", un proceso que no resulta nada sencillo por las grandes diferencias de capacidades entre unos y otros. La razón es que los países, en general, "son reacios a com-

partir inteligencia confidencial a nivel de la UE, ya que permite inferencias sobre las capacidades nacionales de ciberdefensa".

Así, el estudio explica que el ac-

política creíble de atribución requeriría que todos los estados miembros hablaran con una sola voz", reclaman los autores.

Estos obstáculos hacen que en la UE el "proceso de atribución colectivo y compartido" sólo se produzca de forma esporádica, ya que es cada país el que atri-

ciberataques. Una circunstancia que los responsables del informe consideran mejorable puesto que dificulta que los estados miembros actúen juntos para nombrar y 'avergonzar' a los atacantes, tal y como se busca con la estrategia de ciberdiplomacia europea.

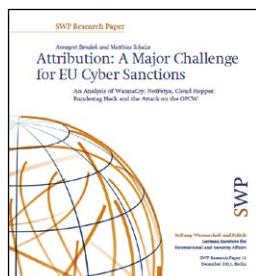
Carencias de capacidades

A ello se suma el hecho de que, según el documento, solo unos pocos países –como Suecia, Países Bajos, Estonia, Austria, Francia y Alemania–, tienen capacidades de atribución y la voluntad política de compartir información con otros países a través de la **EU INTCEN**, la Unidad de Análisis de Inteligencia del **Servicio Europeo de Acción Exterior (SEAE)**.

De hecho, lamenta que la UE esté muy lejos de las capacidades y forma de actuación de la alianza '**Five Eyes**' –integrada por Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos–. Estos países "gestionan la atribución pública mejor que sus homólogos de la UE, ya que se coordinan con rapidez y eficacia, y emiten pronunciamientos simultáneos basados en una amplia evidencia. Además, con el Brexit, la autoridad de atribución de la UE ha disminuido significativamente, ya que el Reino Unido ya no comparte inteligencia a través de la EU INTCEN, aunque intercambia información de forma bilateral con estados seleccionados de la UE".

Definir indicadores

El informe también profundiza en cómo funciona el proceso de atribución de ciberataques desde una perspectiva legal, técnica y política en la UE. En este sentido, destaca que aún hay demasiado por hacer ya que, de momento,



tual proceso de atribución es lento y depende, a la hora de la verdad, de la inteligencia de los socios de la OTAN, así como de aspectos técnicos y legales que no siempre coinciden entre países. Por ello, recuerdan que "una

buye un incidente "de forma autónoma". O, dicho de otra forma, actualmente, la UE lo único que hace para intentar tener capacidades de atribución es agrupar la información relevante y coordinar la respuesta política a los

MARCO DE RESPUESTA DE CIBERDIPLOMACIA DE LA UE (CAJA DE HERRAMIENTAS DE CIBERDIPLOMACIA)*

Medidas preventivas	Medidas cooperativas	Medidas de estabilización	Medidas restrictivas	Medidas según leyes internacionales
■ Confianza y seguridad con diálogo ■ Capacidades con terceros países ■ Concienciación	■ Procedimientos de la UE (si es necesario junto a terceros países) ■ Protesta diplomática	■ Posición común del Consejo UE ■ PESC ■ Decisión ■ Determinación del Alto Representante en nombre del Consejo ■ Declaración del Alto Representante	■ Medidas bajo Art.215 TFUE/PESC ■ Decisión Título V Capítulo 2 TUE ■ Bloqueo de cuentas ■ Restricciones de viaje	■ Cláusula de solidaridad ■ Art. 222 TFUE ■ Cláusula de asistencia ■ Art. 42 (7 TUE) de conformidad con Art. 51 ONU
Resiliencia		Defensa	Sanciones	
Ejemplos: ■ Con "la necesidad de respetar el orden basado en reglas en el ciberespacio" (Abril de 2019) ■ Con "la necesidad de respetar el orden basado en reglas en el ciberespacio" (Noviembre de 2019)		Ejemplos: ■ Conclusión del Consejo de WanaCry y NotPetya (abril de 2018) ■ Mensajes comunes (2018) ■ Declaración del Alto Representante, de los Presidentes del Consejo europeo y de la Comisión del ataque contra OPAQ (octubre de 2018) ■ Declaración del Alto Representante para respetar reglas en ciberespacio (abril de 2019)	Ejemplos: ■ Régimen de ciber sanciones horizontales (mayo de 2019) ■ Atribución coordinada a nivel de la UE (Directrices de implementación, junio de 2019. Reglamento del Consejo (julio de 2020)) ■ Régimen de ciber sanciones horizontales (mayo de 2019)	

*Fuente: Council of the European Union, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption (Brussels, 7 June 2017), and Council of the European Union, Draft Implementing Guidelines for the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Brussels, 9 October 2017).

TRANSFORMACIÓN DIGITAL

SEGURA

Ciberseguridad | Inteligencia | Tecnología



**BUSINESS-ALIGNED
SECURITY**



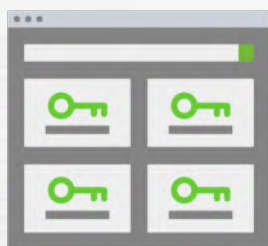
**INDUSTRY
SOLUTIONS**



**DIGITAL
PROTECTION**



**CYBER
DEFENSE**



**SOC/
CERT**



INNOVATE
a MN_EMO company

MN_EMO



www.mnemo.com



info@mnemo.com



su capacidad de atribución “depende en gran medida del intercambio de inteligencia con EE.UU. y el Reino Unido”.

Además, se precisa de mayor rapidez y coordinación entre estados y, también, es necesario perfeccionar “los criterios que debe cumplir un incidente cibernético para justificar sanciones legales”. Asimismo, recuerda que “se debe hacer una mayor distinción entre ataques exitosos e intentos de ataque. La intención delictiva y la motivación estratégica de los ataques rara vez se pueden inferir solo a partir de indicadores técnicos”. No obstante, “estos indicadores sí son clave para la valoración jurídica de un ataque y la posterior justificación de una decisión sancionadora. Por lo tanto, el lenguaje técnico y legal debe armonizarse”, indica el estudio.

De cualquier forma, se recuerda que, desde 2013, la UE “viene desarrollando políticas y medidas regulatorias para responder a operaciones cibernéticas maliciosas, dirigidas desde terceros países” y que, en 2015, la comunidad internacional acordó que una respuesta a los ciberataques debe ser proporcional. Esto es, que las contra reacciones solo están legitimadas por el derecho internacional si los ataques son de cierta escala y producen ciertos efectos. Es decir, son similares en intensidad a un ataque armado. En este aspecto subraya que “el requisito de proporcionalidad incluye, por ejemplo, abstenerse de realizar operaciones cibernéticas contra infraestructuras críticas”.

Sanciones proporcionadas

El documento también reclama que las sanciones cibernéticas sean “proporcionadas, específicas y destructivas”, ya que “ataques preventivos, como WannaCry o NotPetya, deberían conllevar un castigo más severo que los casos cotidianos de ciberespionaje, como Cloud Hopper o el hackeo

del Bundestag”. Por ello, se pide que la UE endurezca los criterios legales y que “la Unidad Cibernética Conjunta de la UE y la EU INT-CEN se fortalezcan para mejorar el intercambio de información forense y se coordine la política de atribución de manera más efectiva”. También se recuerda que las responsabilidades en materia de ciberdelincuencia, ciberespionaje y contrainteligencia, y ciberdefensa

militar recaen principalmente en los estados y deben coordinarse a nivel de la UE a través de **Europol**, en el SEAE, a través de EU INT-CEN y, en el futuro, también a través de la Unidad Cibernética Conjunta en la Comisión de la UE.

Recomendaciones

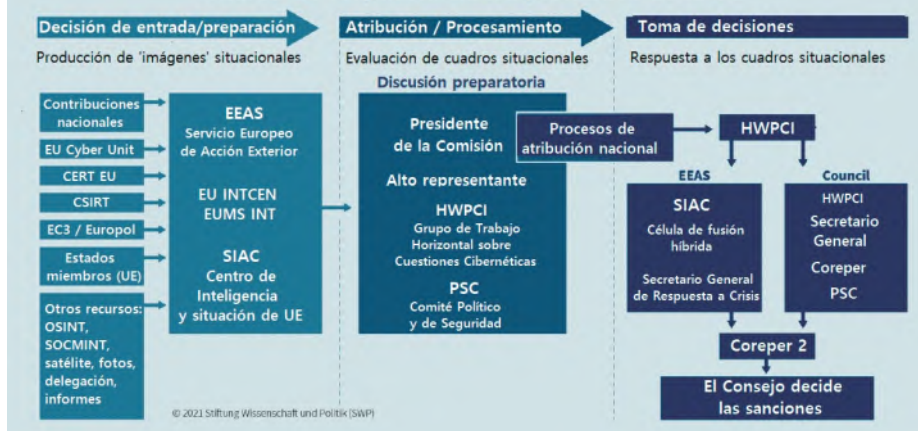
A modo de conclusión, los autores aconsejan a la UE “de-

sarrollar capacidades analíticas” e invertir en ello. Además, el informe pide más medidas de cooperación, operativas y sostenibles, de la Unión respecto a los socios de la coalición ‘Five Eyes’. Sobre todo, en lo que atañe a las que aportan prevención y detección.

Por ello, consideran importante “recopilar datos sobre campañas de ataques pasadas y actuales, presuntos perpetradores, objetivos, número de estados miembros afectados, daños sufridos y su calificación jurídica en una base de datos de ciberconflictos y poner toda esa información a disposición de los estados miembros”, para una mejor comprensión de los ciberconflictos. Y, lógicamente, una mejor atribución. ■

CAJA DE HERRAMIENTAS DE DIPLOMACIA CIBERNÉTICA

Marco de respuesta ciberdiplomática de la UE



En busca de la atribución para una respuesta militar eficaz y proporcional

Durante las pasadas ‘XV Jornadas STIC’ del CCN, en diciembre, el teniente coronel **Emilio Rico**, analista de la Fuerza de Operaciones del **Mando Conjunto del Ciberespacio (MCE)**, explicó la importancia de la atribución destacando que, “cuando te atacan, resulta vital saber quién es para dar una respuesta proporcional”. “La atribución consiste en averiguar quién está detrás de algo, no quién lo ha hecho. Y es muy complejo porque nos hemos dedicado a impulsar la ‘anonimación’”, recordó en su conferencia, en la que recomendó la guía para la atribución de ciberataques que emplea EE.UU., con indicadores para identificar al atacante –en la imagen–. También, repasó otros métodos de atribución, como ‘The Cyber Kill Chain’ –que muestra las siete fases de un ataque–; el de ‘diamante’, del CCN –y base

de la Guía STIC 425, del Ciclo de Inteligencia y el Análisis de Intrusiones–; o las matrices Mitre ATT&CK y Mitre Engage, que ofrecen la posibilidad, incluso, de desplegar señuelos para llevar la iniciativa respecto al enemigo. No faltó en su exposición la preocupación por los ataques de ‘falsa bandera’ que buscan engañar a los defensores con una falsa atribución. “La disuasión y la atribución no son asuntos binarios, ni sencillos. La atribución llega con el tiempo, ergo, el problema no es tenerla sino gestionarla. Hay que contar con capacidades ofensivas, sí, pero hay que saber usarlas y, además, en este aspecto la legislación que lo permite no se puede quedar atrás”, finalizó Rico, enfatizando la complejidad de la atribución, pero su imperiosa necesidad para responder con eficacia.



Forcepoint ONE

Welcome to the
power of **ONE**

ONE Platform
ONE Console
ONE Agent

Forcepoint

Security Simplified

En 35 compañías analizadas se encontraron fallos de seguridad en bases de datos y errores de configuración en la nube, según Reposify

Casi el 100% de las empresas de ciberseguridad tienen activos expuestos con lo que supone de riesgo para ellas... y sus clientes

Dice un refrán popular que “en casa de herrero, cuchillo de palo” y, seguramente, ese es un buen resumen del informe que ha realizado la compañía israelí, **Reposify**, bajo el título ‘¿Quién protege a los protec-

tores?: industria de ciberseguridad, estado de la superficie de ataque externa’. En él, ha analizado si las empresas que la ‘venden’ están tan bien protegidas como se espera. Para ello, durante dos semanas de enero, ‘monitorizó’ a 35 empresas y más de 350 filiales buscando desde servicios y plataformas expuestos hasta posibles problemas críticos o qué proveedores de nube con los que trabajan cuentan con activos expuestos. Y el resultado ha sido, ciertamente, desolador, ya que, con casi todos los sectores en riesgo, las organizaciones de ciberprotección son tan ciberinseguras como el resto. En solo 15 días se detectaron más de 200.000 activos expuestos, muchos de ellos de gravedad alta (30%) o crítica (12%), además de un 58% media.

Y es que, según destacan desde la compañía israelí, el crecimiento de las huellas digitales de las empresas, también en las compañías de ciberseguridad, están “creando puntos ciegos masivos para los equipos de TI y protección”. Y a los más clásicos, de aplicaciones, dispositivos y procesos, se suman ahora los generados por los proveedores de nube, a los que se está contratando para hacer la transición a los espacios de trabajo híbridos, también en el sector de ciberseguridad. Precisamente, la cada vez mayor dependencia de proveedores externos está incrementando la superficie de ataque.

De hecho, una encuesta reciente de **MIT Technology Review** halló que el 51% de las compañías de Asia-Pacífico culpan de muchos de sus incidentes a ‘activos desconocidos’ y no identificados por la propia compañía. Por eso,



aunque el 43% de los encuestados reconoció en dicho estudio su confianza en la nube, con más de la mitad de sus activos digitales en ella, también destacaron, en un 67% de los casos, que la monitorización continua de activos es un pilar de su estrategia de ciberseguridad para evitar incidentes de gravedad.

Problemas en la nube

En esta ocasión, entre los datos más relevantes del estudio de Reposify destaca que hasta el 97% de las compañías de ciberprotección mostraron tener activos expuestos en la nube. En concreto, se encontró que gran parte de las empresas de seguridad cibernética que los usan tienen servicios expuestos: en **AWS** un 97,14%, en **Microsoft** el 82% y en **Google** el 76% que permitían, en un 86%, al menos, un acceso remoto sensible e, incluso, bases de datos expuestas en un 51% de las organizaciones, dando lugar a “posibles fugas” de información. “Y la tendencia es que vaya a más a media que se populariza el teletrabajo”, destaca el estudio que recuerda que estos problemas de seguridad se deben tanto a vulnerabilidades conocidas (y no parcheadas), como a errores de configuración y a fallos humanos.

Demasiada superficie expuesta

Además, el 80% de las empresas también presentaron activos de red expuestos, reflejando el impacto que tiene

el control de los equipos de TI en entornos descentralizados. Además, en el 63% de las compañías se encontraron redes internas de *back office* y en un 51% se halló “al menos, una base de datos expuesta, sensible a los ataques de malhechores”. Asimismo, entre los problemas más críticos, se encontró que el 40% de las empresas analizadas tenía expuestas herramientas de desarrollo –por falta de actualización a la última versión–, pudiendo exponer desde el código fuente hasta análisis de negocios o puntos finales de API desprotegidos, entre otros. Además, el 37% presentaron fallos de seguridad en herramientas de almacenamiento y copias de seguridad, pudiendo perder la información que hay en ellas en caso de verse comprometidas.

Entre las plataformas sensibles expuestas –en un 88% de los casos a través de OpenSSH– también se

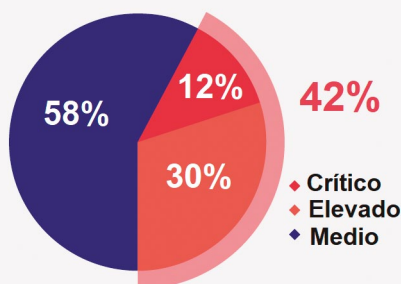
encontraron desde las que permiten el acceso remoto, hasta las que se usan para herramientas de desarrollo, almacenamiento y copias de seguridad o de comunicación (por ejemplo, usando FTP que, según se constató, no estaban conectados a una VPN y carecían de autenticación integrada), entre otras.

De cualquier forma, en este último caso, Reposify destaca que el número de fallos encontrados “es significativamente menor que en otros sectores como el financiero o el farmacéutico”. El problema, más si cabe, en la industria de ciberseguridad, “es que cada vulnerabilidad representa un posible punto de entrada para un atacante”, destaca el estudio.

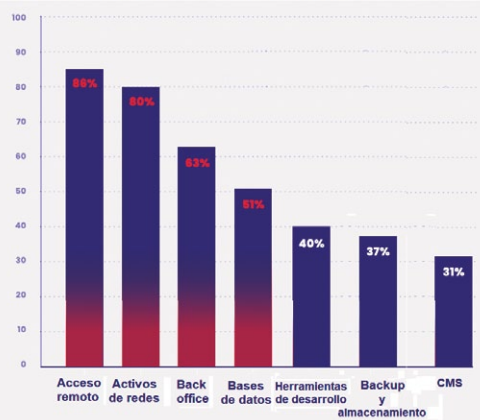
Conclusiones

A modo de conclusión, Reposify resalta que “la industria de la ciberseguridad ha hecho un trabajo increíble para proteger a sus clientes”, pero “ahora debe poner esa misma atención en sí misma”. De hecho, la compañía recuerda que, en su investigación, ha encontrado en este sector desde herramientas de desarrollo expuestas, hasta fallos de seguridad en proveedores de servicios en la nube, servidores web, bases de datos y plataformas de acceso remoto... “lo que obliga a las empresas de ciberseguridad a reforzar su protección para ponérselo más difícil a los atacantes y afianzar sus sistemas, comenzando por tener una visión clara de sus superficies de ataque externas”. En definitiva, el informe considera que, a la vista de sus resultados, la situación en la industria de ciberseguridad es lo “suficientemente preocupante” como para plantearse una mayor inversión en su seguridad para que “practique mejor lo que predica”. ■

GRADO DE SEVERIDAD DE LOS PROBLEMAS ENCONTRADOS



EMPRESAS DE CIBERSEGURIDAD CON SERVICIOS EXPUESTOS



Counter Craft

SOLICITA UNA DEMO

La nueva generación de inteligencia de amenazas

Dirigida a tu organización,
relevante y en tiempo real.

Equipos de seguridad de todo el mundo confían en CounterCraft

Gobiernos, infraestructuras críticas, empresas industriales, entidades financieras y organismos sanitarios se protegen con CounterCraft. ¡Únete a ellos!



Follow us:  @countercraftsec

 @countercraft

 @countercraftsec

www.countercraftsec.com

San Sebastián - Madrid - Londres - Nueva York

SIEMENS: Seguridad gestionada para entornos industriales

En los entornos empresariales actuales, las empresas se enfrentan a importantes amenazas para sus activos digitales en entornos de tecnología operativa de diversas maneras: desde sofisticados programas maliciosos hasta personas con acceso a información privilegiada, pasando por actividades delictivas organizadas y grupos de actores de amenazas patrocinados por estados hostiles. La multinacional Siemens dispone de servicios de seguridad gestionada que presta con tecnologías propias y acuerdos con terceros. En ellos se combinan los proporcionados por su CDC (Centro de Ciberdefensa) y el servicio de Detección de Anomalías y Monitorización de la Seguridad OT, CDC-OT. Ambos forman parte de la solución de servicio de ciberprotección IT-OT-IoT de la compañía europea.

Las organizaciones despliegan estrategias de protección específicas para proteger sus entornos IT y OT, pero deben enfrentarse a la posibilidad de que un atacante tenga éxito. El impacto para una línea de producción o para una oficina puede ser muy importante, pero puede disminuirse de gran manera con una rápida detección y respuesta.

En Siemens, el “Centro de Ciberdefensa” (CDC), junto con el servicio de Detección de Anomalías y Monitorización de la Seguridad OT (CDC-OT) son componentes clave de esta respuesta. El CDC y el CDC-OT proporcionan detección y análisis de ataques en toda la empresa y lo complementan con servicios de *threat hunting* y *threat intelligence* para entornos de IT y OT.

El servicio de detección de anomalías y monitorización de seguridad OT que Siemens ofrece a todas sus fábricas incluye los siguientes módulos:

- 1) Evaluación del grado de madurez IT/OT de la fábrica y determinación del alcance del servicio. 2) Supervisión de la seguridad de OT (24/7). 3) Análisis de seguridad OT. 4) Alojamiento y gestión de infraestructuras e ingeniería de detección.*

El Centro de Ciberdefensa (CDC) de Siemens se ofrece como un servicio de ciberseguridad global y corporativo para proteger nuestros negocios de Siemens. El CDC implementa un entorno de detección y análisis global funcionando en un modelo “follow the

sun” con analistas de seguridad repartidos en distintas regiones del mundo para detectar y mitigar amenazas a nuestra organización en un régimen de 24/7.

La base tecnológica del CDC es una plataforma de detección de amenazas global y flexible (ARGOS), que permite un fácil despliegue en entornos *on-premise* y en la nube con capacidades *multitenant*.

COMPONENTES DEL SERVICIO GESTIONADO DE SEGURIDAD CDC-OT

El servicio de detección de anomalías y monitorización de seguridad OT que Siemens ofrece a todas sus fábricas incluye los siguientes módulos:

1.- Evaluación del grado de madurez IT/OT de la fábrica y determinación del alcance del servicio. Es muy importante dada la gran

variedad de los distintos entornos industriales que existen en Siemens, que se haga un análisis inicial del grado de madurez y complejidad del entorno IT/OT de estos. Desde niveles muy bajos (factorías en las que solo se pintan locomotoras Siemens) hasta altos niveles de sofisticación (entornos de alta automatización con líneas de producción para construcción de componentes de control HVAC).

2.- Supervisión de la seguridad de OT (24/7). La supervisión de seguridad OT incluye la detección de anomalías de seguridad creando una inicialmente una línea base de inventario de dispositivos y actividad. Para ello existe una fase previa de detección e inventariado de activos en las redes de la fábrica. De manera opcional en esta fase, se puede utilizar el servicio SIESTA (desarrollado internamente en Siemens) para detección de activos y vulnerabilidades en entornos OT.

3.- Análisis de seguridad OT. En este módulo se incluyen el análisis y triaje de eventos de ciberseguridad para su descarte o elevación a categoría de incidente (en cuyo caso, se gestionarían desde el Global CERT de Siemens). Igualmente ofrece la búsqueda activa de amenazas mediante técnicas de *threat hunting*.

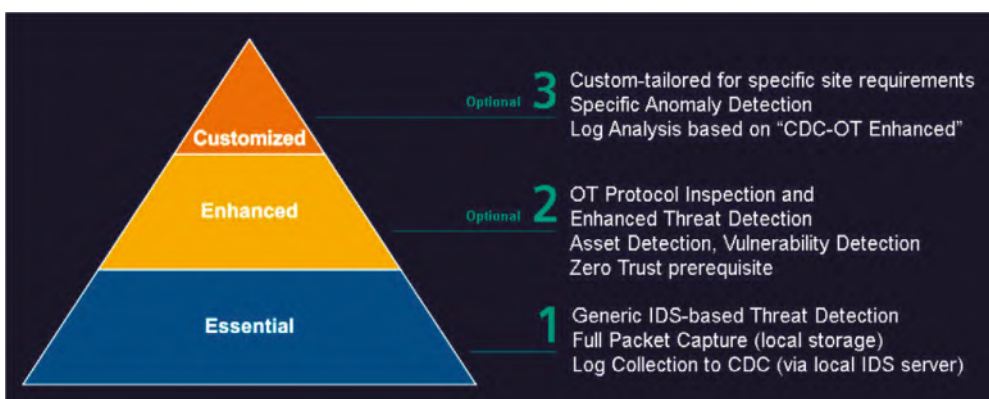


Figura 1.- CDC OT: Niveles de servicio.

El nivel Essential está pensado para entornos industriales con un nivel de complejidad y de madurez OT medio/bajo, pocos dispositivos ICS y una red sencilla; en tanto que el Enhanced lo está para entornos de mayor complejidad y madurez. El nivel Customized incluye todas las características de los anteriores, pero incorpora capacidades pensadas para entornos industriales críticos o partes críticas de fábricas más grandes.

Todo ello se beneficia a su vez de los servicios de *threat intelligence* provistos de manera centralizada por el área de Global TI de Siemens.

4.- Alojamiento y gestión de infraestructuras e ingeniería de detección. Con el servicio se incluyen tanto el despliegue de servicios de hardware y software como la operación remota de la solución. Además, se ofrece la posibilidad de desarrollo conjunto con el cliente de nuevos casos de uso de detección basados en su propio entorno para la reducción de falsos positivos.

MODALIDADES DE SERVICIO

El servicio de CDC OT se ofrece en tres modalidades distintas a las fábricas de Siemens, en función de sus distintos grados de madurez. No todas las fábricas tienen un entorno IT / OT con el mismo nivel de complejidad, por lo que las soluciones de monitorización y respuesta se deben adaptar a cada una de las circunstancias.

Es especialmente importante que los servicios gestionados de monitorización y respuesta a amenazas sean lo suficientemente flexibles como para poder adaptarse a los distintos entornos de cada fábrica. La colaboración entre los gestores IT / OT de la fábrica y el servicio depende de ello. Los servicios gestionados tienen que ser percibidos como una ayuda y una solución a posibles problemas, en vez de una imposición del *holding*.

Las tres modalidades de servicio de CDC OT son: *Essential*, *Enhanced* y *Customized*.

El nivel de cobertura *Essential* está pensado para entornos industriales con un nivel de complejidad y de madurez OT medio / bajo. Pocos dispositivos ICS y una red sencilla.

En este modelo el objetivo es cubrir los básicos de la monitorización de seguridad con el despliegue de un IDS y un recolector de *logs* sencillo. Esta información se agrega a la que ya se recibe desde los agentes EDR en los puestos IT de la fábrica para tener una imagen completa del entorno.

La gestión y la operación de las tecnologías de seguridad y la monitorización de las alertas se hace de manera centralizada por el equipo del CDC, de manera que el servicio es totalmente transparente para el usuario.

El nivel de cobertura *Enhanced* está diseñado para entornos ICS de mayor complejidad y madurez. En este caso, además de la tecnología incorporada en el nivel *Essential* se añaden soluciones de monitorización y detección de amenazas específicas de protocolos OT.

Las dos tecnologías utilizadas en este nivel de cobertura son OSA (OT Cybersecurity Appliance) desarrollada íntegramente por Siemens para la monitorización y detección de amenazas en entornos OT y Claroty.

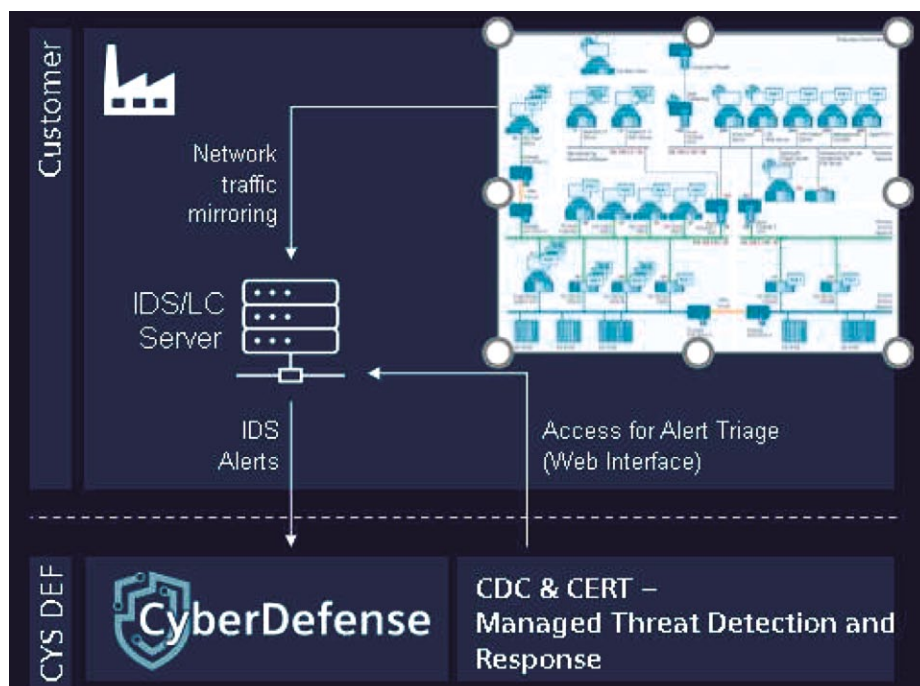


Figura 2.- Diagrama de arquitectura de CDC OT.

En el nivel de cobertura Enhanced, además de la tecnología incorporada en el Essential, se añaden soluciones de monitorización y detección de amenazas específicas de protocolos OT. Las dos tecnologías usadas en dicho nivel son OSA-OT Cybersecurity Appliance (ver interfaz en la Figura 3) desarrollada íntegramente por Siemens para la monitorización y detección de amenazas en entornos OT, y Claroty.



Figura 3.- Interfaz de la solución OSA desarrollada por Siemens.

El último nivel de cobertura *Customized* incluye todas las características de los dos servicios anteriores pero, además, está pensado para entornos industriales críticos o partes críticas de fábricas más grandes. En este nivel se hace un análisis profundo del entorno para poder construir *parsers* de *logs*, reglas de detección e informes totalmente adaptados al

mismo para poder aumentar al máximo el grado de detección y respuesta a incidentes. ■

KAREN GAINES
Global Head of Cybersecurity Defense

PEDRO MARTÍN
Cyber Defense Center Service Manager
SIEMENS

uTile, la solución de GMV para generalizar el uso de las PETs

Las tecnologías de mejora de la privacidad (Privacy-Enhancing Technologies, PET por su acrónimo en inglés) permiten dotar de un lugar de encuentro a los equipos de seguridad, los DPO y los servicios jurídicos para proteger la confidencialidad, la integridad y la accesibilidad de los datos. La solución propuesta en este frente por la multinacional española GMV se denomina uTile. En este artículo se describen sus principales características y se exponen dos ejemplos de uso: Tartaglia, Red federada de Inteligencia Artificial para acelerar la investigación sanitaria; y Maza, Preservación de la privacidad en aprendizaje federado aplicado a Observación de la Tierra.

Si bien la cantidad de datos de que disponemos hoy ha aumentado de forma exponencial, habitualmente estos se encuentran disgregados entre distintas partes (o entidades), dificultando la obtención de conclusiones generales, al contar sólo con datos parciales que describen el comportamiento o características de una reducida parte de la información existente. Este hecho puede incluso derivar en la implementación de sistemas sesgados, alejados del comportamiento general.

Con el fin de ofrecer información de calidad, la primera opción que nos planteamos es la agregación de los datos que disponemos con el objetivo de extraer conclusiones generales. Para ello, las distintas fuentes de datos deben compartirlos. Sin embargo, no siempre es posible hacerlo, ya sea por criterios de confidencialidad, de carácter estratégico o porque la normativa actual no lo permite cuando se trata de información personal o sensible. Obviamente, esta circunstancia puede dificultar el desarrollo de proyectos de tal índole, convirtiéndose en una barrera insalvable en muchos casos.

Cuando los propietarios de los datos pueden conservarlos y tener un control claro en todo momento, se hacen realidad las posibilidades de colaboración. De tal forma, cuando distintas fuentes tienen la certeza de que al compartir sus datos podrán multiplicar su valor y están dispuestas a hacerlo, faltaría disponer de tecnología solvente capaz de dar respuesta a esta voluntad de intercambio, garantizando la protección y privacidad de los datos.

Las PET protegen de forma única los datos

durante su procesamiento. Hace tiempo que existen soluciones orientadas a proteger los datos en reposo en el sistema de archivos o los datos en tránsito mientras se mueven por la red, pero las organizaciones suelen pasar por alto la necesidad de protegerlos mientras se utilizan,

desconfiamos de cada elemento. Sin excepciones. Y lo hicimos porque nos pusimos en los zapatos de quien tuviera que aprobar la utilización de una herramienta con tecnología disruptiva como las PETs: Primero debo verificar, sigo verificando periódicamente y después confío.

La arquitectura de uTile es descentralizada, por diseño. Todos los cálculos se realizan en cada uno de los nodos de computación segura. La copia de los datos originales nunca sale de la memoria del nodo de computación segura.

uTile minimiza especialmente dos riesgos a los que todo dato está expuesto: exfiltración y corrupción, a lo largo de los tres estados estándar por los que un dato pasa: reposo, tránsito y uso. Para ello, utiliza tecnologías menos habituales en este ámbito, como *Secure Multi Party Computation* (SMPC) o Entrenamiento Federado (FL), combinadas con otras bien conocidas como control de acceso, computación segura, o comunicaciones seguras, ya sea *on premise* como en nube. Y este despliegue tecnológico está regido por el principio fundamental de soberanía del dato, teniendo especial cuidado con evitar operaciones innecesarias.

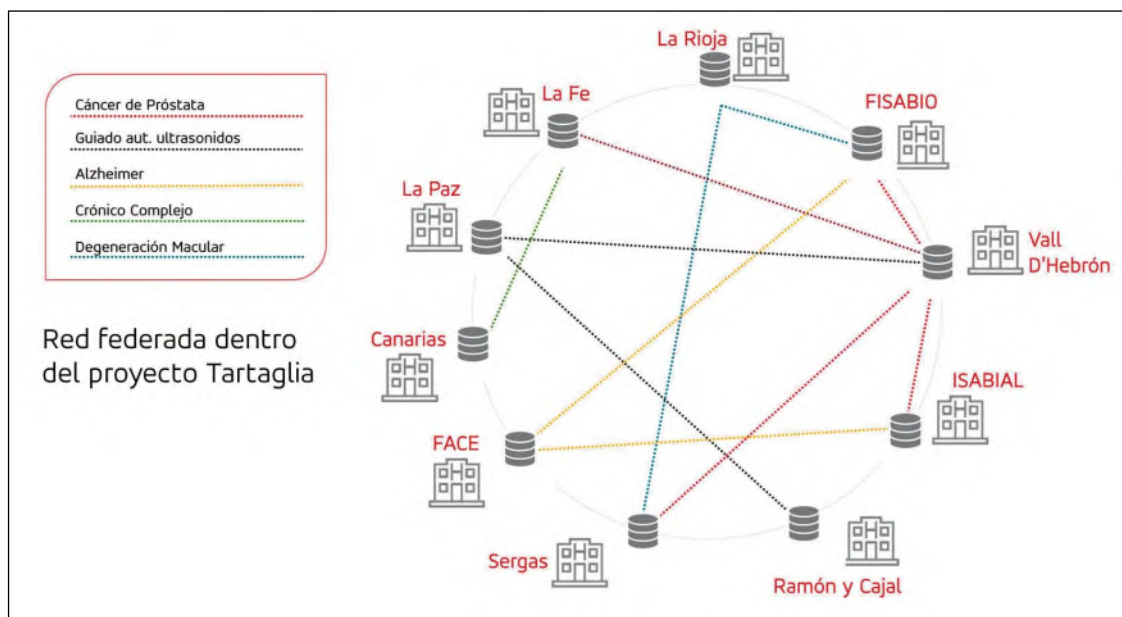


Figura 1.- Red federada dentro del proyecto Tartaglia.

porque es un problema difícil de resolver y que propicia no compartir para evitar el riesgo. Por eso las PET ofrecen un cambio de paradigma: nos permiten aprovechar los datos de forma segura y privada.

Detalles de seguridad y también privacidad

La privacidad y la seguridad por diseño han estado presentes desde el principio. Para dar respuestas a los retos anteriores, nuestra propuesta es uTile. La estrategia se basó en que

Referencias

Todo este trabajo no tiene otro objetivo que permitir resolver con ingeniería sofisticada problemas aparentemente no resolubles hasta la fecha. Presentamos dos casos de uso, en dos proyectos distintos, en los que uTile es la pieza clave, ya que giran en torno a las PET: Tartaglia: Red federada de Inteligencia Artificial para acelerar la investigación sanitaria y Maza: Preservación de la privacidad en aprendizaje federado aplicado a la Observación de la Tierra.

¹ El proyecto TARTAGLIA ha recibido financiación del Ministerio de Asuntos Económicos y Transformación Digital (Nº expediente MIA.2021.M02.0005), correspondiente a los fondos del Plan de Recuperación, Resiliencia y Transformación.

Tartaglia

El objetivo del proyecto Tartaglia¹ es demostrar que gracias a las tecnologías PET es posible realizar investigaciones en el campo de la Inteligencia Artificial que no serían posibles sin compartir los datos de los pacientes.

La red federada propuesta en Tartaglia cuenta con algunos de los referentes sanitarios más importantes de España, con un total de 18 participantes. En este tipo de consorcio es habitual que haya distintos roles, como pueden ser: los expertos sanitarios encargados de definir y validar los resultados; los proveedores de datos con la responsabilidad de custodiar la privacidad de estos; y los científicos de datos, que son los que modelan la Inteligencia Artificial con todos los datos agregados virtualmente.

Dentro de los casos de uso de Tartaglia, cabe resaltar el de diagnóstico precoz de cáncer de próstata (CaP). El diagnóstico de CaP es un proceso complejo, pudiendo requerir la realización de diversas pruebas médicas, cada una de las cuales introduce una demora en la identificación del cáncer. Por ello, el principal objetivo de este caso de uso es acelerar su diagnóstico mediante modelos de Inteligencia Artificial (IA) basados en datos biomédicos, como pueden ser imágenes o notas clínicas.

Aunque la IA tiene un enorme potencial disruptivo en el sector de la salud, la naturaleza altamente sensible de los datos complica el acceso a éstos, lo que a su vez limita el aprendizaje y la aplicación de los modelos. Tareas como la anonimización o la aprobación de comités éticos de los hospitales (similar a los que podría ser un NDA en un ámbito empresarial) para acceder a los datos conllevan una alta carga de trabajo, lo que suele dar lugar a modelos poco robustos por la limitación que en la práctica supone superar estos obstáculos de forma eficiente. El uso de la red federada de Tartaglia supone la posibilidad de que los modelos de IA aprendan patrones más generales detrás del CaP, gracias al uso de un mayor volumen de datos sin necesidad de que tengan que ser compartidos, preservando en todo momento su privacidad.

Antes de **uTile**, la construcción de esta red federada resultaría extremadamente compleja, ya que no hay un mecanismo seguro de compartición, lo que daría lugar a la no colaboración debido a la confidencialidad de los datos. Adicionalmente, las soluciones IA que se construyen alrededor de los datos de una única institución pueden estar sesgados, debido por ejemplo a la demografía de la zona.

Maza

Por otro lado, el ámbito del proyecto MAZA, es totalmente diferente, ya que aquí la idea es



Figura 2.- Imagen tomada por la misión Copernicus Sentinel-2 donde se ve el río de lava provocado por la erupción del volcán de Cumbre Vieja (Credit: ESA/Copernicus/Sentinel 2021 – CC BY-SA IGO 3.0)

aplicar las técnicas PET a Observación de la Tierra (EO).

La Observación de la Tierra es clave para describir los distintos fenómenos que ocurren en nuestro planeta. Un ejemplo cercano lo hemos visto recientemente con la erupción del volcán de Cumbre Vieja situado en la isla de La Palma. Aquí las imágenes aportadas por DRAGO², una cámara infrarroja desarrollada por el Instituto de Astrofísica de Canarias lanzada al espacio a principios del 2021, ha ayudado a la monitorización de este fenómeno terrestre.

MAZA es un proyecto realizado en colaboración de la Agencia Espacial Europea (ESA) y tiene un doble objetivo: uno técnico y otro estratégico. El objetivo técnico es la identificación y clasificación del suelo para saber si es rural, residencial o una zona industrial. El Catastro sí diferencia estas zonas, pero su actualización no es sencilla, por lo que tiene sentido desarrollar un modelo de IA que ayude a estas tareas de clasificación y verificación.

Por otra parte, el objetivo estratégico consiste en definir la estructura de una plataforma de aprendizaje federado que permita a distintas partes tener establecido un marco de trabajo con datos al mismo tiempo protegidos en su privacidad como disponibles para entrenar un algoritmo. El desarrollo de una plataforma colaborativa desde cero no es viable por coste y plazo, pero **uTile** permite tenerla disponible sin estos inconvenientes.

Por otro lado, la Observación de la Tierra se realiza a través del programa Sentinel 2, una

flota de satélites diseñada específicamente para proporcionar los abundantes datos e imágenes de que se nutre el programa Copernicus, de la Comisión Europea³. Las imágenes aportadas por Sentinel 2 son públicas, y están a disposición de cualquier usuario, pero entonces, ¿qué aportan las técnicas PET? Es aquí donde entra **uTile**. A la hora de entrenar un algoritmo de IA, tan importante son los datos (en este caso las imágenes), como los metadatos asociados (a qué tipología de suelo corresponde cada imagen). Estos metadatos, que en el campo de la IA se conocen como etiquetas, son realmente costosos de generar y los dueños no siempre están dispuestos a compartirlos, es decir, las imágenes son públicas pero sus metadatos no.

Antes de **uTile**, los dueños de los metadatos no podían sacar partido de los conocimientos de sus homólogos ya que para ello tenían que cedérselos (y este es justamente el núcleo de su negocio), pero con **uTile** es posible usar estos datos sin compartirlos obteniendo modelos de IA más robustos preservando la privacidad.

Los dos casos de uso anteriores demuestran la idoneidad de **uTile** como herramienta de Privacidad, Big Data y Analítica Avanzada que democratiza el uso de las PETs, haciendo transparente su utilización en los entornos en los que los científicos de datos trabajan habitualmente. ■

LUIS GRAÑANA
Business Partner

JUAN MIGUEL AUÑÓN
Senior Product Manager
GMV

² <https://www.iac.es/es/divulgacion/noticias/el-volcan-de-cumbre-vieja-traves-de-la-camara-drago>

³ https://www.esa.int/Space_in_Member_States/Spain/SENTINEL_2

Forcepoint ONE, la plataforma SASE 'all-in-one' de Forcepoint

En los tiempos que corren los límites del perímetro de la gran parte de las organizaciones se ha difuminado, como contrapartida la ciberseguridad ha surgido con más fuerza. Los usuarios se conectan de muchas formas, desde muchos dispositivos, procedentes de diversas localizaciones a plataformas, aplicaciones y datos ubicados fuera y dentro de nuestro perímetro. Con las herramientas actuales abarcar toda esta casuística resulta complejo y costoso. Forcepoint ONE es la solución SASE 'todo en uno' que permite cubrir todos estos casos de uso con un enfoque principal: la simplicidad.

En seguridad el término simplicidad significa menos tiempo de puesta en marcha y operación, pero, sobre todo, menos propensión a errores de configuración y visibilidad, lo que se traduce directamente en la reducción del riesgo.

La propuesta **Forcepoint ONE** integra capacidades *Cloud Access Security Broker* (CASB) multi-modo, *SmartEdge Secure Web Gateway* (SWG), *Zero Trust Network Access* (ZTNA), se gestionan con políticas unificadas desde una sola consola y un solo cuadro de mandos, todo ello integrado en nuestra arquitectura global nativa en la nube. La arquitectura de Poliescala de Forcepoint ONE se adapta automáticamente a las necesidades de carga en cualquiera de los más de 300 puntos de presencia, garantizando una disponibilidad del 99,99%.

La plataforma Forcepoint ONE se ha diseñado atendiendo a los principios *Zero Trust*, la granularidad basada en la autorización por aplicación, la prevención frente al *malware* basada en tecnología CDR (*Content, Dissarm and Reconstruction*) son ejemplos de la orientación de la solución a la filosofía *Zero Trust*.

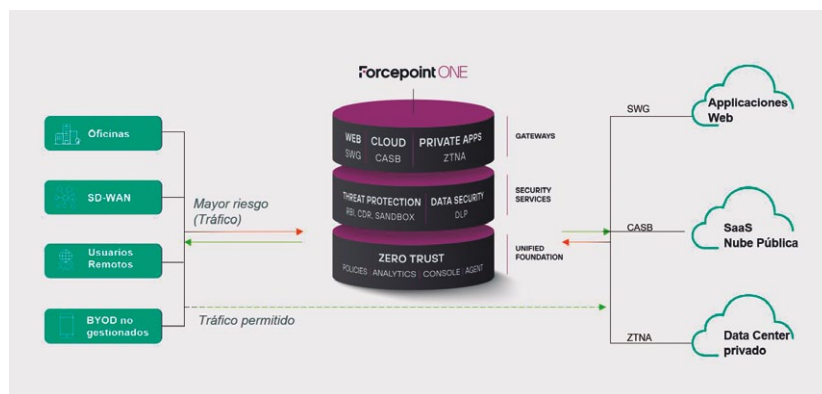
El control del acceso desde dispositivos BYOD a datos y aplicaciones corporativas, la protección de la navegación frente a amenazas externas, el acceso transparente a aplicaciones corporativas en nube privada, la defensa contra el *malware* y la prevención frente a la exfiltración de datos sensibles son casos de uso que Forcepoint ONE resuelve de forma sencilla aplicando políticas unificadas y con una visibilidad global.

COMPONENTES DE LA SOLUCIÓN

Cloud Access Security Broker multimodo

El CASB multi-modo de Forcepoint ONE asegura una protección integral para los datos de todas las aplicaciones corporativas *cloud*,

incluidas las aplicaciones privadas, las plataformas *IaaS* como AWS, GCP y Azure, así como *SaaS* gestionados como Office 365 y Salesforce. La solución permite trabajar con o sin agente y establecer políticas orientadas al control de dispositivos no corporativos.



El modo sin agente basado en la tecnología patentada AJAX-VM ofrece controles en tiempo real en el acceso desde cualquier dispositivo, incluidos los terminales personales y a distancia y lo que es realmente diferencial, el acceso a cualquier aplicación por compleja que sea. Permite por tanto la protección granular de los datos, la protección contra las amenazas de tipo *Zero Day*, la gestión de accesos e identidades así como tener una visibilidad completa de los datos en reposo y en movimiento (modo API e *inline*).

SmartEdge Secure Web Gateway

SmartEdge SWG de Forcepoint ONE es la única solución que permite descifrar e inspeccionar el tráfico localmente en los dispositivos de los usuarios, evitando así el encaminamiento al *proxy Cloud*. De este modo, se elimina la latencia en la red, la escalabilidad es ilimitada y la confidencialidad está asegurada, ya que, no requiere descifrado HTTPS en la nube. La solución aplica de manera automática la políticas DLP y ATP (*Advanced Threat Protection*), controla las aplicaciones no corporativas y bloquea los sitios web que albergan *malware* o categorizadas como

prohibidas en la organización.. La gestión automatizada de certificados se realiza directamente en el *endpoint* con el agente SmartEdge asegurando la responsabilidad de certificación.

Forcepoint ONE permite controlar el Shadow IT tanto a nivel de descubrimiento a partir de la ingesta de *logs* desde dispositivos de terceros, o bien control *inline* de dichas aplicaciones estableciendo controles granulares sobre las mismas. Dispone de una base de datos de más de 650.000 aplicaciones categorizadas por riesgo usando mecanismos avanzados de ML.

Zero Trust Network Access (ZTNA)

El acceso a la red *Zero Trust* (ZTNA) es otra pieza fundamental de las plataformas SASE. ZTNA ofrece un acceso seguro de confianza cero a los recursos locales. Idealmente, estas soluciones evitan el uso de terminadores de túneles en centros de datos propios, así como clientes VPN y se despliegan en la nube pública para ofrecer una escalabilidad y un rendimiento óptimos. Al contar con una solución ZTNA basada en la nube,

los usuarios simplemente se autentican a través de SSO para poder tener un acceso seguro a las aplicaciones locales de forma explícita (en vez de acceder a toda la red). La solución aplica políticas de protección de amenazas y datos en tiempo real para proteger la información sensible o regulada, impedir la descarga de *malware* y ofrecer un acceso contextual a los archivos y las carpetas clave...

Es de resaltar que la solución ZTNA de Forcepoint permite trabajar con dispositivos sin agente o bien con agente por lo que es indicado para el acceso de dispositivos no gestionados.

Advanced Threat Protection

La solución Forcepoint ONE dispone de mecanismos de prevención frente amenazas como son la solución *antimalware* integrada y la posibilidad de usar motores de otros fabricantes líderes en el mercado EDR o bien activar la funcionalidad AMD (*Advanced Malware Detection*).

Por otra parte, ofrece la posibilidad de activar de forma opcional *Browser Isolation* (RBI) lo que permite proteger el puesto de trabajo frente a contenido web malicioso, así como usar la tecnología CDR cuyo objeto es prevenir contra el *malware*. Se trata de reconstruir un archivo partiendo de una copia del original pero eliminando cualquier contenido impropio (dinámico, macros, javascript embebido...). ■

JAVIER LARREA JASPE
Senior Sales Engineer
FORCEPOINT

#SellaTuSeguridad



CyberSecurity
Rating Agency

LOS RETOS DE LA CIBERSEGURIDAD

¿Cuáles son los suyos?

El primero de todos debería ser saber si con
su inversión obtiene un nivel de protección
adecuado para sus sistemas de información

Conozca su nivel real de ciberseguridad y
optimice el resultado de sus inversiones con la
calificación de LEET Security

Contáctenos: info@leetsecurity.com

Qualys Cloud View IaC Security: Detección de errores de configuración en recursos en nube antes de la implementación

Las nuevas capacidades de protección de Qualys CloudView permiten detectar implementaciones no estándar en plantillas IaC (Infrastructure as Code). La evaluación de seguridad de IaC analiza las plantillas de Terraform, AWS CloudFormation, Azure Resource Manager e identifica las configuraciones incorrectas antes de que los recursos se implementen en la nube, incorporando la seguridad en la nube directamente en las herramientas y flujos de trabajo de desarrollo.

Según el informe DBIR 2021 de Verizon, el 54% de las brechas de seguridad en entornos *cloud* se produjeron debido a configuraciones inseguras.

En los últimos años, se ha vuelto cada vez más común que los equipos de DevOps opten por el uso de IaC mediante archivos de configuración para la implementación de aplicaciones nativas en la nube y aprovisionar de forma automatizada su infraestructura, permitiendo a la organización desplegar y escalar aplicaciones en la nube con mayor velocidad y a menor coste. No obstante, este tipo de implementaciones conllevan una serie de riesgos que no siempre se ven a simple vista.

Por ejemplo, la implementación de un *bucket* S3 privado se puede definir con tan sólo un par de líneas de código Terraform:

```
resource "aws_s3_bucket" "bucket" {
  bucket = "my-tf-test-bucket"
  acl    = "private"
}
```

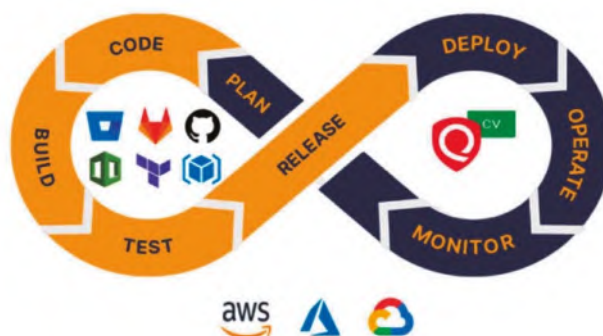
¿Qué puede estar mal? No hay cifrado habilitado en el *bucket*, no hay registro de acceso habilitado... Desde el punto de vista de seguridad, faltan varias cosas...

Hasta ahora, las herramientas CSPM (Cloud Security Posture Management) como Qualys, han permitido evaluar los recursos en la nube de forma reactiva, informando de las configuraciones no recomendadas que puedan tener los recursos *cloud* y permitiendo evaluar el cumplimiento de las mejores prácticas establecidas por la industria.

A medida que IaC se ha vuelto más común, se demanda una respuesta más rápida a los problemas de seguridad que puedan presentarse, como el despliegue de recursos en entornos

productivos que no cumplan con la postura de seguridad desde el mismo instante en que son puestos en producción.

Las detecciones a través de herramientas CSPM son efectivas, pero al ser un tipo de he-



rramientas reactivas, únicamente informarán de las malas configuraciones una vez que el recurso ha sido desplegado, no impidiendo que en los entornos de producción se desplieguen recursos con configuraciones inseguras que pueden tardar días o semanas en ser corregidas. Mientras tanto, estos recursos pueden estar siendo el objetivo de un atacante.

Para corregir estas situaciones, Qualys ha

ampliado las capacidades de CloudView, añadiendo la posibilidad de detectar configuraciones incorrectas, e implementaciones no estándar en el origen de estas: las plantillas IaC.

Entre las nuevas capacidades de Qualys CloudView IaC destacan:

- **Escanero de plantillas IaC:** Terraform, AWS CloudFormation, Azure ARM.
- **Compatibilidad con diferentes entornos cloud:** AWS, Azure, y GCP.
- **Evaluación de controles CIS:** Admite los controles existentes de CloudView CSA para las evaluaciones de las plantillas IaC.
- **Gestión de excepciones** en las evaluaciones IaC.
- **Gestión unificada de evidencias:** Las evaluaciones de IaC se muestran en la interfaz de usuario de CloudView con los detalles y evidencias.

• Capacidad de reporting:

Los resultados del escaneo están disponibles en formatos JSON y SARIF. Además, es posible generar reportes en formatos .pdf y .csv.

• **Integración con herramientas CI/CD:** Esto permite al desarrollador obtener los resultados de la evaluación sin necesidad de acceder a la UI de la consola central de Qualys CloudView.

• **Integración con repositorios Git:** Esto permite activar flujos de trabajo para asegurar las plantillas alojadas sobre los repositorios Git (GitHub, GitLab, Bitbucket).

• **Integraciones avanzadas:** Posibilidad de realizar integraciones avanzadas a través del API.

Gracias a estas nuevas funcionalidades, las organizaciones podrán evaluar la postura de seguridad de los recursos y servicios *cloud* en entornos AWS, Azure y GCP durante el ciclo de desarrollo y antes de la implementación, desde el mismo Qualys CloudView.

A través de una interfaz unificada, los equipos de ciberseguridad dispondrán de la información tanto de IaC como de CSPM, pudiendo dar así una respuesta más ágil tanto de manera proactiva como reactiva a las posibles brechas de seguridad y reduciendo el riesgo de las organizaciones de manera drástica. ■

PABLO VELÁZQUEZ
Security Solutions Architect
QUALYS
pvelazquez@qualys.com



Entrena a tu equipo
frente a ataques de
Ingeniería Social



¡Elige tu estrategia de defensa!



Anti-Phishing



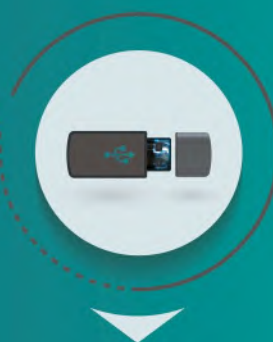
Anti-Vishing



Anti-Smishing



Anti-Fraude QR



Anti-MediaDropping

**Diseño de Campañas ES-CIBER
contra ataques de Ingeniería Social:**

detección de riesgos
concienciación
microlearning
gamificación
simulación controlada



NOVEDADES

FORTINET INCORPORA EL FORTIGATE 3000F A SU GAMA DE CORTAFUEGOS, OFRECIENDO CONVERGENCIA DE ALTO RENDIMIENTO DE RED Y SEGURIDAD

FortiGate 3000F es el nuevo miembro de la familia de cortafuegos de nueva generación (NGFW) de **Fortinet**, que destaca por estar equipado con los procesadores de seguridad propios de la compañía, los NP7 y CP9, y con el que quiere facilitar la creación de arquitecturas de TI híbridas que aceleren la digitalización de las empresas.

Para conseguirlo, dichos procesadores han sido diseñados "para aumentar de forma notable la velocidad, la escala, el rendimiento y la eficiencia, al tiempo que mejoran en gran medida la experiencia del usuario, reducen la huella y disminuyen los requisitos de energía", explica la compañía.

Los FortiGate NGFWs cuentan también con un *proxy* de Acceso a la Red de Confianza Cero (ZTNA) integrado de forma nativa, para permitir a los usuarios acceder a las aplicaciones y recursos desde cualquier lugar y en cualquier momento, con una autenticación



constante mientras se realiza este proceso, además de mantener controles efectivos de cumplimiento y seguridad.

Junto a ello, el Centro de Gestión de Fortinet Fabric proporciona una gestión, automatización y orquestación de toda la arquitectura Security Fabric.

Cabe recordar que las soluciones de Fortinet entrelazan la red, la seguridad y los servicios esenciales de FortiGuard impulsados por la inteligencia artificial y aprendizaje de máquina (IA/ML) en una sola plataforma, permitiendo a los equipos de TI gestionar las amenazas internas y externas, prevenir la propagación lateral y ataques, como el *ransomware*, así como evitar las interrupciones del negocio y el consecuente daño reputacional.

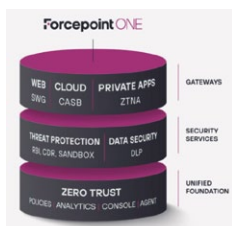
FORTINET

www.fortinet.com

SIMPLIFICAR LA SEGURIDAD EN UNA PLATAFORMA CLOUD 'TODO-EN-UNO', OBJETIVO DE LA NUEVA FORCEPOINT ONE

Forcepoint ha presentado **Forcepoint ONE**, una plataforma nativa de la nube 'todo en uno' con la que la compañía simplifica la seguridad para los equipos de trabajo tradicionales y remotos, permitiendo a los usuarios obtener un acceso protegido y controlado a la información en la web, en la nube y en aplicaciones privadas, gracias a su enfoque de Confianza Cero y un conjunto de políticas administradas desde un único lugar.

La solución facilita para ello la adopción de Security



Service Edge (SSE) al unificar servicios de seguridad, como Secure Web Gateway (SWG), aislamiento remoto del navegador (RBI), desarme y reconstrucción de contenido (CDR), agente de seguridad de acceso a la nube (CASB) y acceso a la red de confianza cero (ZTNA). A ello, se le une, además, tecnologías de protección avanzada de amenazas (ATP) y de prevención de pérdida de datos (DLP) integradas, que evitan el *malware* y protegen los datos confidenciales en las aplicaciones de negocio y los dispositivos BYOD, eliminando también la necesidad de contar con productos fragmentados.

FORCEPOINT

www.forcepoint.com/es

ZSCALER INTRODUCE CAPACIDADES ZTNA PARA FACILITAR LA SUSTITUCIÓN DE FIREWALLS Y VPN HEREDADOS

Zscaler ha dado a conocer su **Marco Security Service Edge (SSE)** con tres importantes novedades de Zero Trust Network Access (ZTNA), para que los equipos de TI y de seguridad puedan sustituir, de forma segura, los cortafuegos y VPN heredados. Estas innovaciones, que se incluyen como parte de Zscaler Zero Trust Exchange, "crean un nuevo estándar para reducir la superficie de ataque y evitar el movimiento lateral, al tiempo que consigue bloquear a los usuarios comprometidos y las amenazas internas con la protección de aplicaciones privadas, el engaño integrado y las opciones de acceso remoto privilegiado para los distintos servicios de la empresa y los sistemas OT", explican desde la compañía.

Las tres novedades incluidas son, por un lado, la protección de aplicaciones privadas, introduciendo inspección del tráfico de aplicaciones privadas en línea para detener los ataques más comunes, incluidos los 10 principales de OWASP, con unas defensas



que se actualizan constantemente, gracias a la labor de su equipo de investigación ThreatLabz y el respaldo de firmas externas.

Por otro lado, ha sumado a su propuesta capacidades de engaño integradas, con las que busca reducir la saturación de las alertas por aquellas que sean de alta confianza generadas por señuelos que identifican y frenan instantáneamente a los usuarios infectados y las amenazas internas, a través de la integración con Zero Trust Exchange y las plataformas de operaciones de seguridad.

Asimismo, Zscaler ha reforzado su plataforma con el Protocolo de Escritorio Remoto (RDP) y el Protocolo Shell Secure (SSH), que soportan los dispositivos no gestionados, tanto para IoT y OT, como para aplicaciones privadas.

ZSCALER

www.zscaler.com

TREND MICRO ACTUALIZA SU OFERTA DE SERVICIOS DE EVALUACIÓN CON VISION ONE

Trend Micro ha actualizado su oferta de servicios de evaluación de seguridad, **Security Assessment Service**, para incluir Log4j y Samba. Esta evaluación de vulnerabilidades ofrece herramientas personalizadas para abordar las más recientes y exposiciones comunes (CVE) específicas. Ahora, los clientes de la compañía pueden analizar los puntos finales y las aplicaciones de servidor en busca de las recientes CVE de Samba o Log4j (Log4Shell) para recibir un informe completo, acciones recomendadas y una mayor visibilidad de su superficie de ataque.



Utilizando su plataforma **Trend Micro Vision One**, la compañía también dispone de un servicio de evaluación de riesgos, que proporciona información detallada sobre el índice de riesgo de la empresa, las entidades incluidas en el análisis, los usuarios y dispositivos que pueden estar bajo ataque y el uso de aplicaciones en la nube en su red.

A ello, se le une el servicio de evaluación de buzones de correo en la nube en riesgo, para descubrir intentos de compromiso de correo-e empresarial (BEC), ataques de *phishing*, *ransomware*, archivos maliciosos o URL en mensajes enviados y recibidos en los últimos 15 a 30 días.

TREND MICRO

www.trendmicro.es

¿Cuánto podría ahorrar su organización con las llaves de seguridad YubiKey?

Número de Empleados	Ahorro Anual
100	41.300 €
1.000	413.000 €
5.000	2.065.000 €
10.000	4.130.000 €



© 2022 Dot Force S.L.

Calcule usted mismo cuánto podría ahorrar su empresa con la calculadora ROI de Yubico en:

dotforce.es/calculadoraROIyubikey.

¡Lo sabrá en segundos!

Olvídese de los problemas de seguridad y la baja productividad que conlleva el uso de contraseñas estáticas y las de un solo uso (OTP) con las llaves de seguridad de Yubico.

¡Tome decisiones informadas basadas en datos reales y sorpréndase con el resultado!

Para un cálculo personalizado y para conseguir dos llaves de Yubico gratis rellene ahora el formulario en dotforce.es/calculadoraROIyubikey, o llame al 914 230 991.

yubico



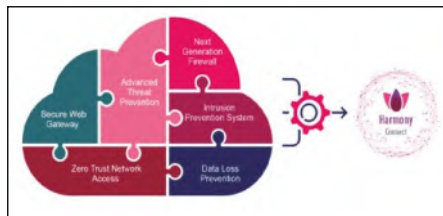
NOVEDADES

CHECK POINT REFUERZA HARMONY CONNECT SASE QUE INCLUYE UNA VPN COMO SERVICIO Y POLÍTICAS DE CONFIANZA CERO PARA OFRECER UNA CIBERSEGURIDAD DE RED EFICAZ

Check Point ha mejorado su servicio **Harmony Connect Secure Access Service Edge (SASE)**, añadiéndole funciones de confianza cero con una 'VPN como servicio' integrada. Harmony Connect es una solución en la que la compañía unifica servicios de ciberseguridad de red esenciales, como Secure Web Gateway, Acceso de Red de Confianza Cero (ZTNA), cortafuegos como servicio, Sistema de Prevención de Intrusiones (IPS) y Prevención de Pérdida de Datos (DLP).

Con esta mejora, ahora ofrece una VPN como servicio, "que permite acceso a nivel de red basado en el cliente y proporciona la potencia de conectividad de red de 'capa 3', asegurada

por las políticas de acceso de confianza cero", destacan desde la compañía. El servicio incluye también DLP en la nube e IPS para proteger las aplicaciones de vulnerabilidades, como Log4J.



Check Point, además, ha incorporado puntos de presencia en la nube (PoPs) en nuevas ubicaciones (Suiza, Noruega, Países Bajos,

centro y sur de los EE.UU., Emiratos Árabes Unidos y China), para aumentar la velocidad y mejorar la seguridad de los entornos corporativos, gracias a una nueva validación de la configuración de los dispositivos gestionados que se conectan de forma remota.

Con todo ello, la compañía facilita la protección de los equipos de trabajo híbridos, en remoto y en las oficinas, ofreciendo un modelo SASE que elimina las limitaciones de las arquitecturas de red tradicionales, convergiendo la red y la seguridad en la nube.

CHECK POINT

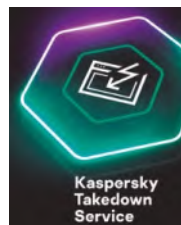
www.checkpoint.com

KASPERSKY APUESTA POR ELIMINAR LOS DOMINIOS MALICIOSOS CON TAKEDOWN SERVICE

Cada día, **Kaspersky** bloquea más de 15.000 URLs de *phishing* y estafa, y **Google**, por ejemplo, detecta alrededor de 46.000 nuevos sitios web maliciosos. Se trata de procesos fundamentales, ya que "si una empresa no es capaz de identificar dominios maliciosos, sus clientes pueden acabar siendo víctimas de sitios web falsos que permitan que los atacantes accedan a su información personal y financiera o ser objeto de graves filtraciones de datos causadas por *botnets*", señalan desde la firma rusa.

Para evitarlo, Kaspersky ha creado **Takedown Service**, un servicio con el que busca eliminar rápidamente cualquier dominio de *phishing* malicioso sin importar dónde se encuentre. Para ello, la compañía prepara todas las pruebas necesarias, incluida una copia del sitio web, capturas de pantalla y volcado de tráfico, tanto de forma manual como a través de herramientas auto-

matizadas. Después, envía la solicitud de eliminación a la autoridad local o regional pertinente que tiene los derechos legales para cerrar el recurso. Y, finalmente, el cliente recibe notificaciones de cada paso del proceso hasta que el dominio es eliminado con éxito. El servicio se puede adquirir de forma independiente o como parte de la suscripción de Digital Footprint Intelligence (DFI). En el primer caso, los clientes pueden enviar solicitudes para eliminar ciertos dominios no deseados que descubran a través de la cuenta de empresa de Kaspersky. Y, en el segundo, el servicio DFI se encargará de identificar los recursos maliciosos o de *phishing* que atacan al cliente. "Cada vez que se identifique contenido dañino el cliente recibirá una notificación y, a continuación, podrá iniciar el proceso de eliminación",



explican desde Kaspersky. El paquete estándar incluye diez eliminaciones al mes y puede personalizarse según las necesidades del cliente.

Formación a través de videojuegos

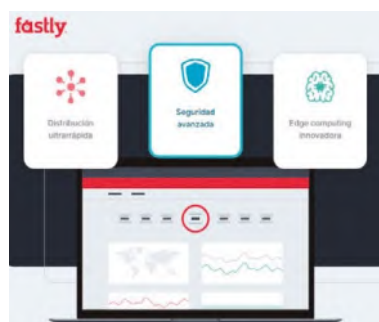
La compañía también ha lanzado un juego para dispositivos móviles sobre ciberseguridad con el nombre de **[Dis]connected**. Con él, quiere mostrar a los usuarios los beneficios de contar con hábitos seguros en Internet. Su objetivo es servir como refuerzo en los programas de formación sobre ciberseguridad para empleados, o incluirse en campañas públicas de formación dirigidas a la ciudadanía.

KASPERSKY

www.kaspersky.es

FASTLY BUSCA PROTEGER LAS APLICACIONES Y APIS EN CUALQUIER UBICACIÓN, INCLUIDO EL EDGE, CON SU WAF UNIFICADO PARA OFRECER LA MÁXIMA VISIBILIDAD

Fruto de su estrategia encaminada a proporcionar seguridad en cualquier ubicación, **Fastly** ha anunciado la opción de despliegue en el *edge* para su cortafuegos de aplicaciones web **Fastly Next-Gen WAF**, desarrollado por **Signal Sciences**.



Su propuesta busca proteger las aplicaciones y las APIs en cualquier lugar en el que se encuentren, y puede desplegarse en una amplia gama de arquitecturas: desde contenedores, infraestructura propia del cliente (*on-premise*), en la nube y ahora en el conocido como 'borde' o *edge*. Todos estos despliegues pueden ser gestionados dentro de una única plataforma con una visión consolidada de los datos de seguridad, desbloqueando la visibilidad a través de toda la huella de aplicaciones y APIs de las organizaciones.

Con esta solución, Fastly se desmarca de otras ofertas del mercado, "con las que las empresas se ven obligadas a gestionar diferentes productos WAF, dependiendo de sus variadas necesidades de despliegue", explica

la compañía. "Esto puede consumir muchos recursos y aumentar la complejidad y la proliferación de herramientas". El hecho de que el WAF de próxima generación de Fastly pueda "desplegarse tanto en el borde, como en otras múltiples ubicaciones, y pueda ser gestionado dentro de una única plataforma, ofrece una visión consolidada de los datos de seguridad, mejorando la visibilidad y protegiendo las aplicaciones de los clientes, tanto las que están en las instalaciones propias y en la nube, como las que se construyan en el borde en el futuro", añaden desde la empresa.

FASTLY

www.fastly.com/es

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa
estés donde estés.



Digital Security
Progress. Protected.



CAPACIDADES XDR CONTEXTUAL Y REMEDIACIÓN AVANZADA, LO ÚLTIMO DEL PORTAFOLIO DE QUALYS



Apostando por una continua mejora de su plataforma en la nube, **Qualys** ha incorporado su

primer XDR contextual y ha añadido nuevas capacidades de remediación avanzadas.

En el primer caso, y bajo el nombre **Context XDR**, la compañía combina “un rico inventario de activos y contexto de vulnerabilidades, telemetría de red y del punto final a través de sensores propios, junto con una inteligencia de amenazas de alta calidad y datos de registros de terceros”, destacan sus impulsores. La compañía prioriza así la detección de amenazas con un contexto integral, buscando reducir el desgaste producido por las alertas de seguridad.

Su objetivo es ofrecer una alternativa a las soluciones SIEM y XDR actuales “que recopilan de forma pasiva y reactiva registros dispares y no relacionados, depositando todo el peso y la responsabilidad de correlación y priorización en los analistas”, afirma.

Frente a ello, la solución Qualys Cloud Platform en la que se basa Context XDR es capaz de procesar más de nueve billones de *data points*, recopilando telemetría de TI, seguridad y cumplimiento, utilizando sus múltiples sensores nativos, así como registros de terceros. “Todo esto permite que la plataforma pueda brindar una visión más amplia de las redes globales de las organizaciones”. Context XDR, por su parte, aprovecha esta inteligencia y las capacidades de respuesta del agente en la nube de la plataforma (como la aplicación de parches, la corrección de errores de configuración, la eliminación de procesos y conexiones de red o la cuarentena de hosts), para remediar las amenazas identificadas y aumentar la productividad de los analistas de seguridad.

Remediación avanzada

La compañía, también ha incorporado en su plataforma en la nube la nueva funcionalidad **Qualys Advanced Remediation**, con el objetivo de que sus clientes dispongan de un enfoque más integral en el proceso de remediación, corrigiendo errores de configuración de activos, además de aplicar los parches correspondientes.

Entre otras acciones, permite corregir vulnerabilidades relacionadas con cambios de configuración para remediar aquellas basadas en Windows desde una única consola y un flujo de trabajo. También, implementa y parchea software basado en Windows para cualquier dispositivo, sin importar si está en las instalaciones, en la nube o en una ubicación remota. A ello, se le une la implementación de parches y cambios de configuración en entornos complejos con dependencias y flujos de trabajo muy detallados.

QUALYS

www.qualys.com

DEVO PRESENTA EXCHANGE, UN MARKETPLACE PARA MEJORAR LAS CAPACIDADES Y LA EXPERIENCIA DE LOS SOC

Devo ha dado a conocer **Devo Exchange**, un *marketplace* basado en su comunidad de usuarios que ya está disponible para clientes y *partners*. Diseñado para agilizar y ampliar las capacidades y la experiencia de los equipos de seguridad, la propuesta de la compañía proporciona “acceso inmediato, y a demanda, a un catálogo de contenido especialmente seleccionado por Devo, que la propia compañía, sus socios y la comunidad del mundo de la seguridad en general crea, colabora y comparte”, explican.

Con ello, la firma asegura reducir notablemente el tiempo y el esfuerzo necesarios para que clientes y socios creen y compartan contenidos que hagan las operaciones de seguridad más precisas y decisivas.

Los contenidos de Devo Exchange, aportados por la comunidad y validados por Devo, incluyen *packs* de alertas, con colecciones (analíticas de datos de seguridad creadas por expertos) relacionadas, que permiten a los clientes detectar, en tiempo real, indicadores relevantes en sus datos. Ofrece aplicaciones interactivas de propósito específico para una mayor capacidad de interacción con los datos, permitiendo



a los clientes acceder a niveles de detalle más profundos y desbloquear nuevos casos de uso con facilidad. Cuenta también, con los denominados Devo Activeboards, es decir, cuadros de mando que permiten a los clientes visualizar, interactuar y explorar con mayor facilidad sus datos.

Todo ello, se complementa con *Lookups*, conjuntos de datos que permiten el enriquecimiento y la contextualización de los datos procesados, y que permiten acelerar las investigaciones y la comprensión de las amenazas; y con una colección preconfigurada de contenidos relacionados (aplicaciones, paquetes de alertas, *lookups* y/o cuadros de mando), empaquetados de forma conjunta para un uso rápido y fácil.

DEVO

www.devo.com

WISE SECURITY GLOBAL TRASLADA AL MÓVIL EL CONTROL DE LA IDENTIDAD A TRAVÉS DE BLOCKCHAIN CON DEFINITIVE ID

Que el usuario controle su identidad digital desde su dispositivo móvil, a través de *blockchain*. Ese el propósito de la solución **Definitive ID** de la compañía **Wise Security Global**. Se trata de un nuevo sistema de identificación digital para entidades, basado en la tecnología de cadena de bloques, con el que los usuarios pueden identificarse en una o varias plataformas con su único ID, de manera más segura, más fácil y teniendo en cuenta el control soberano de sus datos. La compañía, además, ha adelantado que “el uso de



esta solución podrá ser generalizado y con un amplio catálogo de casos”.

Definitive ID se basa así en la auto soberanía y descentralización de la identidad digital a través de *blockchain*. A ello se suma que, además de tener el control de su privacidad, los usuarios podrán

identificarse mediante las credenciales almacenadas en su móvil y cifradas en *blockchain*, sin necesidad de contraseñas (*passwordless*) y con seguridad.

De acuerdo con la compañía, “la solución ya se utiliza en sectores como clubes de fútbol de alto nivel (gestión de socios), el sector *retail* (tarjetas de fidelización) y la administración pública (control de accesos), entre otros”.

Junto a este desarrollo innovador, Wise Security Global también ha presentado **Bastet**, una herramienta para la gestión de vulnerabilidades, basada en la automatización y centralización de todos los procesos que intervienen en el ciclo de vida de dicha vulnerabilidad.

WISE SECURITY GLOBAL

www.wsg127.com/es

Es el momento de ciber proteger su empresa

DETECCIÓN Y RESPUESTA

SOC 24x7
Detección de amenazas
Respuesta a incidentes
Análisis forense
Inteligencia de amenazas
Vigilancia digital

Gestión vulnerabilidades

PREVENCIÓN Y PROTECCIÓN

Test de intrusión
Ejercicios de red team
Protección puesto de trabajo
Seguridad del cloud
Seguridad de las aplicaciones

GOBIERNO Y ESTRATEGIA

Plan director de seguridad
CISO as a service
DPO as a service
Oficina de seguridad de la información
Plan de concienciación

RIESGO Y CUMPLIMIENTO TI

ISO 27001, ENS, NIST, LEY PIC
Riesgos de proveedores
Plan de continuidad TIC
Protección de datos (RGPD)
Auditoría de buenas prácticas





F5 SIMPLIFICA LA GESTIÓN Y PROTECCIÓN DE LAS APLICACIONES CON DISTRIBUTED CLOUD SERVICES



Para poder dar respuesta a las actuales demandas de los usuarios,

las organizaciones se basan, cada vez más, en portafolios complejos de aplicaciones y en despliegues multinube. Una problemática que la compañía F5 quiere resolver con **F5 Distributed Cloud Services**. Se trata de una importante ampliación de su cartera de soluciones de entrega y seguridad de aplicaciones, que proporciona seguridad, *networking* multi-nube y soluciones de computación basadas en el *Edge*, sobre una plataforma unificada de software como servicio (SaaS).

La compañía, además, ha presentado su primera solución sobre esta plataforma, **F5 Distributed Cloud WAAP** (Protección de API y aplicaciones web), que añade múltiples capacidades de seguridad a las tecnologías de F5, también, sobre un modelo SaaS.

La plataforma de servicios distribuidos de F5 se basa en una combinación de esta y los servicios adquiridos con la compra de **Volterra** y los servicios de seguridad de F5 y **Shape**. Ofrecen servicios nativos de nube de entrega y seguridad de aplicaciones que se administran de forma centralizada, pero se pueden implementar en entornos multinube, centros de datos y en el *edge*. También, proporcionan visibilidad de extremo a extremo y control de políticas a través de todas las aplicaciones y desde un único cuadro de mando, además de disponer de “una red privada global integrada en más de 20 áreas metropolitanas”, según explican sus responsables.

La compañía ya cuenta con varios servicios de nube distribuidos disponibles, como **F5 Distributed Cloud Multi-Cloud Transit**, que ofrece *networking* multi-*cloud* (MCN) con conectividad segura y de alto rendimiento entre las nubes y un cortafuegos de red. Y **F5 Distributed Cloud Load Balancer and Kubernetes Gateway**, con el que

proporciona un balanceador de carga integrado con Kubernetes y *gateways* API para implementar fácilmente cargas de trabajo modernas y microservicios a través de diferentes clústeres distribuidos, ubicaciones y proveedores de nube.

F5 Distributed Cloud WAAP

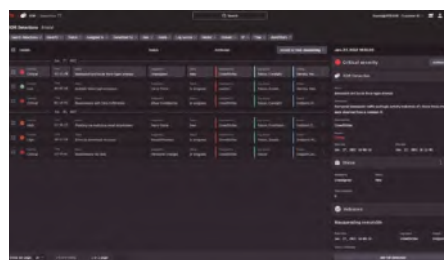
Asimismo, como primer nuevo servicio en F5 Cloud Services se ha comenzado a ofrecer F5 Distributed Cloud WAAP, que simplifica la seguridad y automatiza los procesos, permitiendo que los equipos de aplicaciones puedan centrarse en ofrecer más capacidades y funcionalidad. Esta propuesta aúna el cortafuegos de aplicaciones web de F5, la mitigación de ataques DDoS y de *bots* y las capacidades de protección de API en una única solución, fácil de implementar.

F5
www.f5.com

FALCON XDR, LA PROPUESTA DE CROWDSTRIKE PARA MEJORAR LAS CAPACIDADES DE DETECCIÓN DE AMENAZAS

Bajo el nombre **Falcon XDR**, CrowdStrike ha presentado un módulo que amplía las capacidades de detección y respuesta en el punto final y que, a su vez, facilita la visibilidad de las amenazas a lo largo de las infraestructuras corporativas. El objetivo es que, a través de esta solución, las empresas puedan simplificar sus operaciones de seguridad y reducir los tiempos de respuesta, contención y remediación frente a los ataques más sofisticados.

Para ello, una de las principales características de Falcon XDR es que sus usuarios pueden unificar los datos de detección y respuesta. Para ello, este módulo incorpora datos de terceros (entre los que se incluye información sobre la red, el correo electrónico, la web, la nube o el CASB) y los relaciona con los datos recogidos por la CrowdStrike Security Cloud para optimizar la detección de amenazas y la respuesta ante incidentes.



Además, Falcon XDR utiliza una consola única y centralizada en la que se prioriza cualquier incidente, ofrece programación de búsquedas flexibles y la personalización de cualquier detección, así como la visualización interactiva de gráficos y contextualización de los ataques.

Asimismo, con el objetivo de equilibrar y automatizar las respuestas en todos los flujos de seguridad, se ha incorporado de forma nativa Falcon

Fusion, el marco de trabajo SOAR de la compañía. Así, los equipos de seguridad pueden ser más eficientes en su trabajo, desarrollando capacidades de notificación y respuesta en tiempo real, así como desencadenantes personalizados basados en categorizaciones de detección e incidentes.

Falcon XDR también relaciona de forma automatizada los datos de detección a lo largo de toda la infraestructura. Y reduce los tiempos de investigación y detección gracias a la interfaz CrowdStrike Security Cloud. Incluso, “permite analizar la información procedente de las soluciones de seguridad existentes en la organización, aunque se trate de productos desconectados e independientes”, destaca.

CROWDSTRIKE
www.crowdstrike.com/sites/es

ESET CREA NETPROTECT, UNA SOLUCIÓN DE PROTECCIÓN Y FILTRADO DE DNS ESPECÍFICA PARA EMPRESAS DE TELECOMUNICACIONES Y PROVEEDORES DE SERVICIO DE INTERNET (ISP)

Enfocada específicamente a empresas de telecomunicaciones y proveedores de servicio de internet (ISP), Eset ha presentado su solución **NetProtect**, de filtrado de DNS para proporcionar “un nivel adicional de seguridad para los usuarios al filtrar e informar sobre el acceso a los dominios”. Para adaptarse al perfil de cada cliente, se ofrece dividida en dos productos: por un lado uno ‘Esencial’ y, por otro, el ‘Avanzado’. Así, mientras el primero busca proteger un dispositivo móvil, el segundo incorpora también la solución para el hogar, sin límite de dispositivos, y pensado de forma especial para los entornos de trabajo híbridos.

Entre sus principales funcionalidades destaca una protección en red que ‘blinda’ todos los



dispositivos conectados a redes Telco/ISP (fijas o móviles) contra dominios web maliciosos y categorías de dominios como *malware*, *phishing* y PUAs (aplicaciones potencialmente no deseadas). Ofrece, a su vez, portales en los que los usuarios autorizados pueden gestionar las reglas de NetProtect y ver los registros y las estadísticas de uso de los dispositivos conectados.

La solución, además, cuenta con filtros DNS que proporcionan una protección proactiva contra los dominios que contienen archivos clasificados como software malicioso. Estos filtros, también protegen contra dominios sospechosos o sitios web que albergan contenidos no deseados, bloqueándolos.

En lo que respecta a la gestión, Eset NetProtect permite a los usuarios administrar y monitorizar la configuración de sus dispositivos conectados y gestionar las listas blancas y negras, proporcionando informes de seguridad.

ESET
www.eset.com/es



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



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





Los días 27 y 28 de este mes de abril, en Madrid

Las dimensiones del impacto del *ransomware*, a escena en Espacio TiSEC

Bajo el clarificador título de “Ransomware: ¿quién paga la fiesta”, SIC organiza los días 27 y 28 de este mes en Madrid una nueva edición de Espacio TiSEC. Es pretensión del evento, que en esta ocasión será en modo híbrido

–presencial y retransmitido– arrojar la máxima luz posible sobre un tema crucial por su desbocado impacto en la sociedad digital, exacerbado si cabe aún más en estos tiempos ante la efervescencia geopolítica. Para ello ha convocado a un plantel de ponentes especialistas de primer nivel en todas las dimensiones en las que el *ransomware* irradia consecuencias.

El “negocio” de la (ciber)delincuencia –principalmente económica– crece a medida que profundizamos en el modelo vigente de “digitalización”, afectando a personas físicas, hogares, pequeñas organizaciones, grandes corporaciones y administraciones públicas, y a sus interrelaciones en todo frente.

Se ha creado un escenario ciberfísico en el que la (ciber)criminalidad, que ha avanzado de modo fulgurante en automatización de procesos, industrialización de servicios y maximización de beneficios, le saca partido tanto al miedo de la víctima al conocimiento público del hecho (reputación, caídas en ratings...), como a tener que exponerse a multas por haber incurrido, quizá, en algún incumplimiento legal (privacidad), cuando no a generar un conflicto

con segundos y terceros, o en la cadena de suministro y en las relaciones asociadas a la interdependencia del mercado.

El perfeccionamiento del gobierno de la ciberseguridad, más allá de la requisitoria legal, es responsabilidad de los consejos y la alta dirección; y disponer de un buen análisis continuo global de negocio y actividad –en el que se incorpore el específico de ciberseguridad– se entiende como una condición indispensable para transferir riesgos al sector asegurador y mitigar, en medida razonable, las pérdidas causadas por ciberataques.

En esta edición de Espacio TiSEC se ha confeccionado un programa en el que está representada la cadena de valor asociada a este tipo de riesgos: una multinacional con notable experiencia en ciberseguridad (**Mapfre**), una empresa aseguradora (**Tokio Marine HCC**), una empresa mediadora (**Aon**), una firma global de servicios profesionales (**Alvarez & Marsal**), una tecnológica experta en investigación de incidentes y en análisis forense (**One eSecurity**), un proveedor de servicios de ciberseguridad (**S2 Grupo**), el Departamento

de Delitos Telemáticos de la **Guardia Civil**, el **Centro Criptológico Nacional** y las compañías proveedoras de soluciones tecnológicas de ciberseguridad **Check Point**, **CrowdStrike**, **Kaspersky** y **Stormshield**.



PROGRAMA

DÍA 27 DE ABRIL, MIÉRCOLES

CCN-CENTRO CRIPTOLÓGICO NACIONAL

Ransomware: una bomba de relojería para estados, empresas y administrados

Javier Candau, Director de Ciberseguridad

GUARDIA CIVIL

¿Qué estamos aprendiendo en la lucha policial contra la ciberdelincuencia económica para anticiparnos y romper la industrialización de su “negocio”?

Juan Sotomayor, Jefe del Dpto. de Delitos Telemáticos.
UCO-Unidad Central Operativa Policía Judicial

TOKIO MARINE HCC

La encrucijada del riesgo cibernético, el negocio asegurador y la ciberseguridad

José Carlos Jiménez, Senior Underwriter – Cyber.

AON

Entre dos aguas: El valor del mediador en la instauración de la compartición de riesgos asegurado-aseguradora

Claudia Gómez, Executive Director Financial & Professional Solutions
Verónica Jiménez, Director Specialty Cyber Insurance España

ALVAREZ & MARSAL

Reporte de datos de riesgo de ciberseguridad para el recálculo de la prima en tiempo real

Julio San José, Managing Director. Transformación Digital y Ciberseguridad

PROTECCIÓN TECNOLÓGICA ANTE EL RANSOMWARE. ESTADO DEL ARTE I

CHECK POINT

Eusebio Nieva, Director SE para Iberia

CROWDSTRIKE

Luca Nilo Livrieri, Manager Sales Engineering Southern Europe

DÍA 28 DE ABRIL, JUEVES

RAZONA LEGALTECH

Daños causados por ciberataques: cobertura aseguradora y límites legales en España

Paloma Llana, CEO

MAPFRE

Gestión de crisis y ciberataques: ámbitos de mejora

Andrés Peral, Director de Seguridad en Sistemas de Información

Daniel Largacha, Director de Security Operation Center-SOC

ONE eSECURITY

Servicios de respuesta: experiencia para la mejora del riesgo de las pólizas ciber

Alfredo Zorzo, Director de Ciberseguros

Aitor Azpiroz, Director Global de Respuesta a Incidentes

S2 GRUPO

El impacto de las soluciones y servicios gestionados de ciberseguridad en el abaratamiento de las primas

Antonio Sanz, Head of DFIR

PROTECCIÓN TECNOLÓGICA ANTE EL RANSOMWARE. ESTADO DEL ARTE II

KASPERSKY

Dani Creus, Lead Security Researcher

STORMSHIELD

Antonio Martínez, Director Técnico para Iberia



 **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

GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

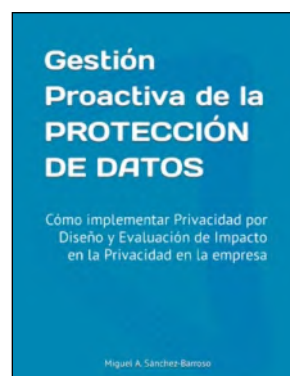


Autora: Maite Moreno García
Editorial: Editorial Ra-Ma
Año: 2022 – 202 páginas
ISBN: 978-8418971730
www.ra-ma.es

También, ofrece información detallada de la utilidad de las plataformas de inteligencia de amenazas y cómo se monitorizan los incidentes. Por supuesto, no faltan abundantes ejemplos prácticos y un capítulo dedicado a las métricas e indicadores, así como la importancia de las 'lecciones aprendidas'.

Se trata pues de un libro de gran utilidad, tanto para los profesionales que trabajan en estos ámbitos, como para los que quieren acercarse a ellos. De hecho, los contenidos han sido adaptados para lo requerido en el módulo profesional de 'Incidentes de ciberseguridad', que se engloba dentro del 'Curso de Especialización de Ciberseguridad en Entornos de las Tecnologías de la Información' (del Título LOE).

GESTIÓN PROACTIVA DE LA PROTECCIÓN DE DATOS



Autor: Miguel A. Sánchez Barroso
Editorial: Publicación independiente
Año: 2022 – 236 páginas
ISBN: 978-1549513619
www.iberlibro.com

El autor, un reconocido profesional con más de una década de experiencia en privacidad y seguridad de la información con foco en escenarios financieros, aporta de forma precisa y muy 'al grano', a modo de manual, información completa y fácil de aplicar sobre cómo cumplir el enfoque de riesgos que ahora se exige en la normativa europea.

En definitiva, Sánchez Barroso permite acceder a abundante información sobre procesos esenciales que deben tenerse en cuenta, como el inventariado de tratamientos de datos o cómo realizar una evaluación de impacto en la privacidad. Sin duda una obra de referencia dada la escasa bibliografía, en castellano, existente sobre este tema.

Con un lenguaje claro y didáctico, **Maite Moreno** –experta de **S2 Grupo** y ponente en **Securmática**– ofrece una guía muy práctica para adquirir rápido los conocimientos necesarios para establecer y definir las líneas de actuación ante incidentes de ciberseguridad. Para ello, a lo largo de sus 10 capítulos, va desglosando los diferentes aspectos esenciales para gestionar crisis cibernéticas, partiendo de la taxonomía de los incidentes y analizando el papel que juegan los equipos de respuesta, qué capacidades deben tener, así como las herramientas, procesos y estándares más habituales.

Tras el éxito de su primera edición, en 2017, **Sánchez Barroso** ofrece una revisión actualizada y ampliada para ayudar a "implementar la Privacidad por Diseño y la Evaluación de Impacto en la Privacidad en la empresa", según se destaca en su portada. En ella, el lector encontrará un listado exhaustivo de los mejores métodos y herramientas que permiten llevar a cabo un programa de Gestión de la Privacidad basado en los requisitos de responsabilidad proactiva del Reglamento Europeo de Protección de Datos.

MALWARE MODERNO: TÉCNICAS AVANZADAS Y SU INFLUENCIA EN LA INDUSTRIA



Autor: Sergio de los Santos
Editorial: Oxword
Año: 2022 – 366 páginas
ISBN: 978-8409366231
Oxword.com

de las muestras de *malware* más relevantes detectadas en las últimas dos décadas, acompañándolas de abundantes explicaciones, ejemplos y cómo se han analizado. Por ello, este libro, fruto de muchos meses de trabajo de uno de los grandes especialistas españoles en la materia, se convertirá posiblemente en obra de referencia para los que quieran comenzar y entender el mundo del *malware*, cómo funciona, cómo se analiza, y, también, para cualquier profesional de ciberseguridad que ya trabaje en este campo. No obstante, es, hasta la fecha, el libro más voluminoso de la editorial que no ha querido escatimar en páginas ante lo que considera una valiosa fuente de información.

CONFESIONES DE UN BOT RUSO



Autor: Bot Ruso
Editorial: Debate
Año: 2022 – 224 páginas
ISBN: 978-8418619151
www.penguinlibros.com

insultándote en redes sociales porque alguien me pagaba. Ahora que ya no estoy en nómina, quiero contarte cómo lo hacía", destaca su autor que confiesa que ha escrito el libro "desde el arrepentimiento ante el daño realizado".

Por eso, y en estos tensos tiempos que corren, se convierte en una obra de especial interés en el ámbito de la desinformación que, también, incluye numerosas indicaciones para anticiparse a este tipo de campañas, cada vez más sofisticadas y que "amenazan con dejar en manos de las grandes corporaciones el control de la información y la opinión pública". Con una prosa irónica y muy entretenida es una buena forma de conocer la 'trastienda' y consecuencias de lo que ha sido la popularización de la web 2.0 provocando que las redes sociales se hayan erigido como el mayor termómetro social.

Con una redacción técnica, pero al alcance del público profesional, **Sergio de los Santos**, veterano de lides malagueñas del sector y experto en Telefónica, ofrece una excelente perspectiva –salvo el garrafal error de utilizar 'troiano' en lugar del apropiado 'Caballo de Troya'– sobre cómo ha evolucionado el software malicioso desde el año 2000 hasta hoy y qué pasos ha dado la industria de la ciberseguridad para hacerle frente, a través de normativas, tecnologías o regulaciones nacionales.

Así, la obra ofrece una rigurosa recopilación de las características

Bajo el pseudónimo de 'Bot ruso', el autor desvela que es un profesional que "ha pasado años manipulando conversaciones en Internet en una empresa de *astroturfing*", término referido a campañas de influencia. Precisamente, el valor de esta obra es la ilustrativa realidad que plantea, vivida en primera línea y en primera persona, mostrada de forma espeluznante a través del 'modus operandi' oscuro que utilizan empresas, partidos políticos y clubes deportivos, entre otros, para influenciar en la opinión pública. "He pasado bastantes años

Venga conmigo si quiere sobrevivir



Servicio de Ciber**inteligencia**

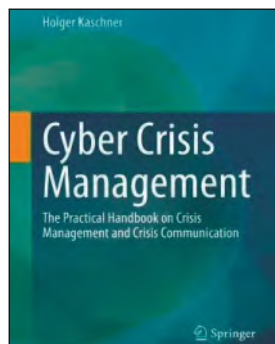
La Inteligencia de Amenazas más Avanzada

www.grupoica.com

grupo
ICA
Sistemas y Seguridad

Tlf. 913 110 487
seguridad@grupoica.com

CYBER CRISIS MANAGEMENT: THE PRACTICAL HANDBOOK ON CRISIS MANAGEMENT AND CRISIS COMMUNICATION



Autor: Holger Kaschner
Editorial: Springer
Año: 2022 – 236 páginas
ISBN: 978-3658354886
link.springer.com

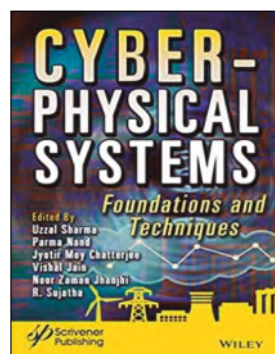
blicado en alemán– y estructurado de forma muy intuitiva, está pensado para facilitar la labor de los profesionales que trabajan con equipos de respuesta a incidentes, en cualquiera de sus ámbitos, tanto el técnico como el más ejecutivo o el de comunicación. Por eso, incluye numerosas ilustraciones y listas de verificación e, incluso, un capítulo dedicado a los “siete pecados capitales de la gestión de crisis cibernética”.

La obra resultará así de utilidad para una variedad de perfiles profesionales, que abarcan desde los miembros de los equipos de gestión de crisis, hasta los CIO y gerentes de TI, los delegados de protección de datos, los CSO y CISO y, por supuesto, los directores generales que quieran contar con una visión más precisa y exhaustiva de qué hacer en este tipo de situaciones.

Los ataques cibernéticos y los fallos de seguridad en TI amenazan a todas las organizaciones. Los incidentes se acumulan y, a menudo, forman el preludio de crisis complejas que amenazan a miles de empresas cada día. Por ello, el autor ha querido plasmar su experiencia –está especializado en crisis cibernética y la ISO 27032– en este volumen a modo de guía de consejos y buenas prácticas para ayudar a gestionarlas, así como a prepararse y prevenirlas.

En inglés –inicialmente fue pu-

CYBER-PHYSICAL SYSTEMS: FOUNDATIONS AND TECHNIQUES



Autores: Uzzal Sharma, Parma Nand, Jyotir Moy Chatterjee, Vishal Jain, Noor Zaman Jhanjhi, R. Sujatha
Editorial: Wiley-Scrivener
Año: 2022 – 336 páginas
ISBN: 978-1119836193
www.amazon.com

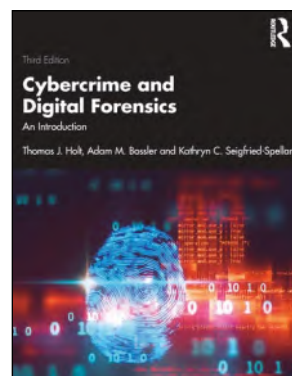
Learning (ML) o Deep Learning (DL) que mejoran sus capacidades, pero, también, lo hacen más vulnerables”, destacan sus autores.

Precisamente, para conocer en profundidad este tipo de sistemas el sexteto de autores de este innovador y bien actualizado volumen cubren los diferentes aspectos asociados con los CPS dando información abundante, desde del tipo de algoritmos que se usa como la aplicación de la tecnología en esta clase de sistemas.

Quizá, no es la primera obra dedicada a ellos, pero sí la más actual, con abundante bibliografía y la experiencia de un amplio elenco de profesionales muy experimentados en la materia.

Interesante aproximación a los denominados ‘sistemas ciberfísicos’ (CPS, por sus siglas en inglés) que representan la interconexión de los virtuales o cibernéticos con los físicos y que cada vez están más presentes en todo tipo de entornos corporativos e industriales. “En los CPS, el proceso físico y el procesamiento de la información están tan estrechamente conectados que es difícil distinguir la contribución individual de cada proceso de la salida” y, cada vez, surgen más tecnologías nuevas como la Inteligencia Artificial (IA), el Internet de las Cosas (IoT), Machine

CYBERCRIME AND DIGITAL FORENSICS: AN INTRODUCTION



Autores: Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar
Editorial: Routledge
Año: 2022 – 794 páginas
ISBN: 978-0367360078
www.penguinlibros.com

de productos, tanto en Open Web como en Dark Web. Además, incluye abundantes estudios de casos que permitirán tener un conocimiento exhaustivo de las últimas tendencias en pericia forense y cibercriminalidad.

Por supuesto, repasa los diferentes ciberdelitos contemplados en legislaciones internacionales y nacionales, cómo los encaran los cuerpos de seguridad de forma transnacional y qué aporta la investigación forense digital. En definitiva, a través de la gran experiencia de sus autores, reconocidos criminalistas, y con abundantes ejemplos, algunos de especial actualidad, se ofrece una perspectiva global sobre el delito cibernético difícil de encontrar en el ámbito académico.

La tercera edición de ‘Cybercrime and Digital Forensics’ ofrece una información actualizada y de gran utilidad para los profesionales que trabajan en la lucha o la investigación del cibercrimen. El libro es un recurso fundamental tanto para los especialistas en la materia como para los que quieren acercarse a ella, destacando dos nuevos capítulos: uno dedicado a la guerra cibernética y las operaciones de información en línea; y, el otro, a las operaciones en mercados ilícitos para todo tipo

SPIES, LIES, AND ALGORITHMS: THE HISTORY AND FUTURE OF AMERICAN INTELLIGENCE



Autora: Amy B. Zegart
Editorial: Princeton University Press
Año: 2022 – 424 páginas
ISBN: 978-0691147130
press.princeton.edu

cadras de investigación y decenas de entrevistas, ofrece una apasionante historia del espionaje estadounidense desde la Guerra de Independencia, en tiempos de George Washington, hasta nuestros días, a través de las capacidades que da el ciberespacio, “analizando cómo los ‘espías ficticios’ influyen en los funcionarios reales”.

También, incluye una excelente relación de los conceptos básicos de inteligencia y cómo es la vida de verdad dentro de las agencias de EE.UU., prestando atención a temas controvertidos, como las acciones encubiertas, quién ‘vigila al vigilante’ o los posibles traidores. Pero, quizá, el aspecto más interesante es su capacidad para mostrar cómo la tecnología está empoderando a nuevos enemigos.

En ‘Espías, mentiras y algoritmos’, esta reconocida especialista en inteligencia, muestra con precisión –separando la realidad de la ficción–, el pasado, presente y futuro de la comunidad de inteligencia estadounidense, ahora impulsada por la revolución cibernética. Ello supone que “necesitamos reimaginar lo que la Inteligencia puede y debe hacer en la era digital, y eso comienza por darnos cuenta de que los secretos ya no juegan el papel que solían jugar”, destacó la autora.

El libro, basado en sus tres dé-



Una plataforma. Un agente. Una vista.

Consolidación de:
Asset Management
Vulnerability Management
Policy Compliance
Patch Management
Indication of Compromise
File Integrity Monitoring
Cloud & Container Security
Web App Security

¡Y ahora EDR multivectorial!

Solicite una demostración

www.qualys.com/apps/endpoint-detection-response



Llega WatchGuard for SOC: anticipación, capacitación y unificación de la seguridad avanzada

Seguridad de calidad, modular y adaptable
para MSSPs/MDRs y clientes corporativos

Protección unificada, inteligencia de amenazas
proactiva y confianza cero para los equipos
de respuesta y proveedores de servicio

La identidad y la automatización
de la detección y la respuesta, cruciales

ENTREVISTA

Miguel Carrero

Vicepresidente de
Proveedores de Servicios
de Seguridad Gestionada y
Cuentas Estratégicas



El valor añadido de la protección unificada y la inteligencia proactiva

WatchGuard-Cytomic: seguridad de calidad, modular y adaptable, con alcance generalizado para MSSPs/MDRs y clientes corporativos

Decía Henry Ford que “llegar juntos es el principio; mantenerse juntos es el progreso y trabajar juntos es el éxito”. Una máxima que cumple a la perfección WatchGuard-Cytomic, especializada en acompañar a grandes corporaciones y proveedores de servicios en su protección digital. Desde que fuera creada por un equipo multidisciplinar la compañía no ha dejado de crecer en su apuesta por simplificar y generalizar la ciberprotección, adaptándola a las necesidades de cada organización, a través de soluciones innovadoras y el conocimiento experto. Una oferta que se ha plasmado en su evolución hacia lo que es ahora: WatchGuard for SOC, su propuesta de seguridad avanzada.

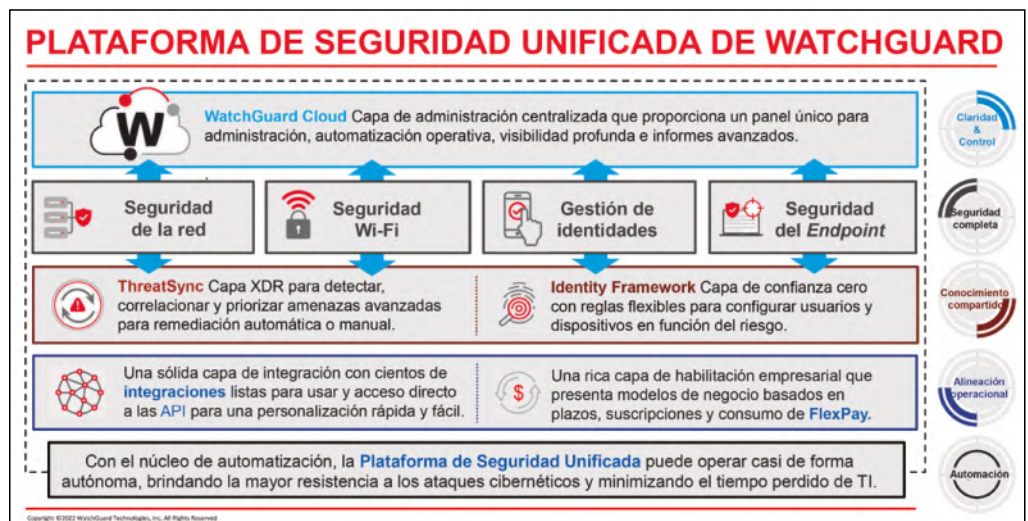
En un mundo cada vez más complejo, descentralizado y donde las cibermenazas ganan día a día en sofisticación, las grandes corporaciones y los proveedores de servicios de seguridad gestionada (MSSP) buscan los mejores aliados para disponer de la resiliencia necesaria para garantizar que su negocio continuará, incluso, ante el cibertaque más inesperado. Porque el cibercrimen aprieta, y sus ataques se han incrementado más de un 27% en un solo año, con incidentes cada 39 segundos y llegando a impactar a más de 2.244 empresas de todo tipo cada día.

Minimizar este peligro es un reto al que contribuye de forma decisiva uno de los referentes del mercado, **WatchGuard-Cytomic**, que ha actualizado su propuesta bajo la denominación **WatchGuard for SOC**, en la que prima el valor de conocer “qué necesitan las empresas” para “poder ofrecer la perfecta combinación de soluciones y servicios para cada una”, destacan en la compañía. Y es que un mismo incidente, según el grado de madurez y preparación de cada organización, puede resultar inocuo o de un impacto devastador para el negocio y actividad.

La organización de WatchGuard para grandes compañías y MSSP/MDR fue creada en 2019, poco antes de que su matriz, Panda Security, fuera adquirida por la multinacional estadounidense. Desde entonces, viene desarrollando un paquete de soluciones de última generación y servicios de caza de amenazas (*threat hunting*) pensados para los entornos corporativos más críticos. Integrada en el equipo multinacional de WatchGuard, la compañía está conformada por más de 1.300 especialistas en todo el mundo, cuenta

actualmente con más de 80.000 clientes, incluyendo a siete de los mayores bancos internacionales, más de dos decenas de operadores de telecomunicaciones, 26 proveedores de sanidad y 115 gobiernos, además de más de 230 industrias e Infraestructuras Críticas, disponiendo igualmente de acuerdos suscritos con 18.000 *partners*.

Los riesgos que se plantean son críticos, según el último informe del **Foro Económico Mundial**. Y en WatchGuard-Cytomic consideran que solo hay dos opciones de comportamiento: “esperar y ser víctima... o responder al atacante”. De hecho, la compañía se define como “un arma de caza contra el cibercrimen”, un desafío para el que cuenta con



Enfoque proactivo para un reto no trivial

En este contexto cabe reseñar que el reto no es sencillo en un entorno digital descentralizado y en expansión, donde se ha popularizado el trabajo híbrido y las compañías están llevando todo tipo de activos a la nube; en muchos casos, los más sensibles.

más de 25 años de innovaciones continuas, siendo tanto su matriz, WatchGuard, como la veterana Panda, pioneras en conceptos y tecnologías como antivirus para entornos de nube o la seguridad como servicio (SaaS). Y es que ambas pueden exhibir dos décadas de innovaciones a sus espaldas y un I+D+i que continúa siendo una de sus ‘señas de identidad’.

Proporciona la ciberseguridad que realmente se precisa, aportando tecnología de vanguardia y, al tiempo y sobre todo, valor, derivado de opiniones expertas, que saben escuchar y recomendar lo adecuado a cada caso.

Así, este 'savoir faire' se plasma desde en sus productos EPP y EDR hasta en sus servicios de ciberinteligencia y caza de amenazas; si bien se ejemplifica a la perfección en su Plataforma de Seguridad Unificada (USP), una plataforma focalizada en los proveedores de seguridad gestionada con un enfoque modular, adaptado al cliente, y dos propuestas, una más preventiva y otra más proactiva, en las que se incluye desde soluciones de protección de red, hasta la autenticación multifactor y la inteligencia de amenazas, aplicando técnicas de Inteligencia Artificial, Aprendizaje Automático y *Big Data*, todo ello en un enfoque orientado a la 'Confianza Cero' en aplicaciones. Su éxito es permitir, de forma sencilla, neutralizar con anticipación ciberataques que instrumentalizan cualquier tipo de *malware*, *exploits*, o exhiban comportamientos anómalos en el entorno corporativo.

El valor de los analistas

Por supuesto, no todo es tecnología, ya que una parte importante se basa en el alto grado de cualificación de un equipo de especialistas y analistas de un ecosistema de *partners* capaces de hacer frente a todo tipo de técnicas de ataque, incluso las más sofisticadas, como los denominados 'living off the land' (LotL), que hacen uso de lo que ya está en los dispositivos y servidores de una organización, para atacarla sin necesidad de descargar o instalar ninguna otra aplicación. En definitiva, la compañía basa su oferta en generalizar la seguridad de calidad poniéndola al alcance de todo tipo de empresas y tamaños, de forma modular y adaptada a las necesidades específicas. "No queremos vender ciberseguridad en general, sino la que realmente se precisa. Tenemos lo último en tecnología pero, sobre todo, el valor de nuestra aportación se centra en la opinión experta que aportamos con nuestros socios y colaboradores: sabemos escuchar y recomendar lo mejor según las necesidades de cada cliente", destaca el Vicepresidente de Cuentas Estratégicas y MSSPs/MDRs, **Miguel Carrero**, que ha redirigido el enfoque de la compañía apostando por convertirla "no solo en un proveedor de seguridad, sino además en un *partner* de negocio para el segmento MSSP/MDR, proporcionando un portafolio de soluciones, capacitación, iniciativas *go to market* y apoyo a las relaciones con los clientes finales, entre otras muchas cosas". Y, por ello, uno de sus grandes valores diferenciales se basa en las capas de servicio, que brindan a los clientes el valor añadido en la dualidad tecnología-servicio.

Pensando en el cliente

El último hito de la compañía ha sido su solución 'WatchGuard for SOC', una sofisticada propuesta pensada para facilitar el trabajo de los analistas de los Centros de Operaciones de Ciberseguridad

y capaz de detectar lo indetectable por otras organizaciones y tecnologías. Y es que, actualmente, el proveedor de servicios de seguridad exige un enfoque diferente de capacitación –desde la funcionalidad y la agrupación de producto, hasta el soporte de ventas y marketing–.

Se trata de una propuesta que combina soluciones de seguridad y servicios gestionados para una efi-



ciente caza de amenazas y respuesta a incidentes en la protección de puestos de trabajo, servidores, entornos virtuales y dispositivos móviles.

Y todo ello, apoyando a las empresas en su proceso de maduración hacia un programa de ciberprotección avanzada, con su propio equipo de seguridad y respuesta a incidentes o delegándolo en su proveedor de servicios de seguridad (MSSP/MDR y/o CSIRT).

"A diferencia de otras compañías, nosotros a través de nuestros colaboradores, queremos dar una solución real y adaptada a las necesidades del cliente. Ese es nuestro gran valor, ya que podemos acompañar a proveedores especializados dotándolos de plataformas y herramientas, únicas en el mercado, que les permita expandir su catálogo de servicios de *hunting*, detección y respuesta a incidentes en tiempo reducido", resalta Carrero.

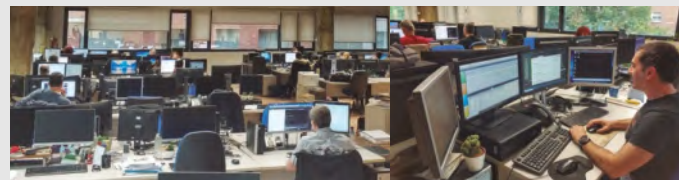
La propuesta cuenta con las certificaciones más exigentes: Common Criteria (EAL2) o la Categoría Alta del Esquema Nacional de Seguridad (ENS), además de ser productos certificados por el Centro Criptológico Nacional (CCN). El buen hacer

de la compañía se plasma en su amplia presencia en los foros internacionales de referencia, como la **Cyber Threat Alliance (CTA)** –con la que comparte indicadores de amenazas–, la **Cybersecurity Tech Accord** o la **AMTSO (Anti-Malware Testing Standards Organization)**, de la que es miembro fundador, además de tener acuerdos con tecnológicas de referencia, como **Microsoft**, entre otras. ●

WatchGuard-Cytomic Lab: la referencia mundial en I+D+i del área endpoint está en Bilbao

Dentro de un gran edificio acristalado, en Bilbao, se ubica uno de los centros de I+D+i centrados en ciberseguridad más importantes de la UE. Se trata de las instalaciones que albergan los equipos de soporte, de Research y de Inteligencia de Amenazas de WatchGuard-Cytomic, con más de 250 integrantes.

Sus capacidades tecnológicas son tales que, tras la compra de Panda, esta ha convertido a Bilbao en su centro de investigación de referencia en Europa y, a nivel mundial, de protección del *endpoint* y de caza de amenazas (*Threat hunting*).



Su equipo e instalaciones han ido ganando peso en la compañía y, actualmente, son su gran motor en innovación y desarrollo, además de ofrecer soporte, de segundo y tercer nivel, para sus soluciones de punto final.

Entre sus grandes hitos destaca la protección de aplicaciones a través de un enfoque de confianza cero, una estrategia que se plasma en hacer un seguimiento de lo que hacen,

basado en su contexto y comportamiento, y que ha permitido a sus clientes reducir de forma drástica el riesgo de sufrir ciberataques exitosos a través de ellas.

Además, desde WatchGuard-Cytomic Lab, también se centralizan todos los datos de amenaza con los que trabaja, tanto de la base de soluciones instaladas, como de organizaciones internacionales en las que está presente y con las que se comparten indicadores de compromiso. "Se trata de parar de forma preventiva cualquier mínimo indicio de amenaza", destaca el Strategy & Technology Advisor de Watch-

Guard Technologies, **Josu Franco**, que recuerda que el éxito de su trabajo es tal que las infecciones en clientes han

caído drásticamente en el último lustro. Por supuesto, Bilbao, a través del departamento de Investigación, también es innovador a la hora de desarrollar nuevas tecnologías aplicadas a casos de uso, para dificultar los objetivos del cibercrimen.

De él salen muchos de los productos y soluciones que están permitiendo ganar mercado a la compañía.

Miguel Carrero, Vicepresidente de Proveedores de Servicios de Seguridad Gestionada y Cuentas Estratégicas

Con una experiencia de 15 años en grandes multinacionales y exitosas *startups* en el mercado estadounidense, Miguel Carrero tomó las riendas de WatchGuard-Cytomic en 2021 para ayudar a los MSSP/MDR y a las grandes corporaciones a mejorar su protección digital a través de una oferta innovadora pero, también, generalizando la ciberseguridad y haciéndola sencilla para sacar de ella el máximo partido. “Se trata ofrecer una propuesta modular, adaptada a las necesidades de cada cliente”, destaca.

“Cytomic es la organización que cristaliza la aproximación de WatchGuard a proveedores de servicios y cuentas estratégicas”

– Han pasado tres años desde la creación de Cytomic. ¿Qué es ahora y qué retos tiene por delante?

– Cytomic es la organización que cristaliza la aproximación de WatchGuard a proveedores de servicios y cuentas estratégicas. Nació dentro de Panda y con un foco exclusivo en la protección del *endpoint*. Pero, ahora, Cytomic es WatchGuard y, por tanto, representa la aproximación del portafolio completo de productos y servicios a lo largo de nuestras cuatro familias de soluciones (protección avanzada de *endpoint*, seguridad de red, identidad y Wi-Fi seguro) y nuestra aproximación a la *Unified Security Platform*.

– ¿Qué ha supuesto integrarse en una compañía internacional como WatchGuard y qué peso tiene Cytomic actualmente en su negocio?

– La integración en una multinacional como WatchGuard afecta a muchos aspectos de procesos, operacionales, legales, etc. Pero en lo que más nos hemos focalizado es en que la propuesta de valor de WatchGuard sea significativamente mejor y diferencial para clientes y colaboradores.

La integración y coordinación de un conjunto de soluciones y su ‘*go to market*’ no es trivial, pero el resultado da una mayor y más eficiente solución de seguridad, que ofrece grandes posibilidades a nuestros colaboradores para aportar valor añadido. Es importante resaltar nuestro foco en los proveedores de servicios de seguridad como un vehículo crítico para convertir nuestra propuesta en soluciones prácticas para clientes finales de distintos segmentos.

– Siempre han tenido un ADN innovador con una clara apuesta por el I+D+i, plasmada en un laboratorio puntero en Bilbao. ¿Qué líneas de investigación siguen?

– Este ADN no solo continúa, sino que se ha fortalecido con la innovación de WatchGuard. El equipo de Bilbao sigue siendo el centro mundial de desarrollo con foco en el *endpoint* y, además,

evoluciona en áreas muy interesantes de *threat hunting* y XDR. Para ello, es muy importante la innovación en otras áreas (como la protección de red, la identidad...) y ahí hay una gran sinergia con la compañía. WatchGuard tiene un modelo muy bien implementado de I+D+i distribuido y basado en capacidades y experiencia y no en puros elementos de centralización logística y geografías de optimización de coste.

– Apuestan por lo que denominan ‘Unified Security Platform’ (USP), que combina varios productos (*endpoint*, seguridad de red, gestión de identidades, protección wi-fi, etc), integrados en la solución WatchGuard Cloud, para la gran empresa. ¿Cuál es su valor diferencial?

– El gran valor diferencial son las soluciones que trabajan conjuntamente para dar un resultado de seguridad mayor y más eficiencia, a la vez que minimizar la complejidad para cliente y colaborador; tanto en la solución, como en su gestión. En cualquier caso, es crítico resaltar el componente de modularidad, pues entendemos que Unified Security Platform cubre un espectro de funcionalidad muy amplio y que ciertos clientes pueden tener otras soluciones en alguna de estas áreas. La ventaja es que pueden seguir disfrutando de las ventajas del diseño integrado, pero modular, de USP.

– La Confianza Cero ha sido siempre uno de sus grandes pilares. ¿Cuál es el enfoque específico de la compañía en lo que toca a protección y gestión y su crucial vinculación con la identidad digital?

– Llevamos años aplicando la filosofía *Zero Trust* al mundo de la seguridad del *endpoint*. Y fruto de esta experiencia sabemos que las implicaciones para hacer esto bien no son triviales (tipo de tecnología que se usa, impacto en rendimiento, necesidad de elementos *cloud*...). Una aproximación *Zero Trust* requiere de una serie de capas y elementos que enlazan fuertemente con la gestión de identidad, pues al final hay ‘confianza cero’, incluso, en que la identidad que se presenta es la que dice ser. Asuntos como el doble factor de autenticación (MFA) son críticos, así como el uso de la identidad para la implementación de políticas de seguridad adecuadas a las necesidades de cada perfil.

– Una de las principales propuestas de



Cyatomic es su plataforma Orion de *threat hunting*, y detección y respuesta avanzada. ¿Cómo ha evolucionado?

– Es una herramienta fundamental, pues tiene capacidades avanzadas que permiten contar con una seguridad proactiva, mediante la búsqueda exhaustiva de IoC o, incluso, indicadores totalmente desconocidos (*threat hunting* en sentido estricto).

Además, a través de ella se pueden realizar investigaciones profundas para entender el inicio de los problemas (*zero patient*) y la evolución de una infección en la empresa para poder, no ya solo corregir lo ocurrido sino, además, inocular el entorno para que no pueda ocurrir en el futuro. Por último, dispone de *playbooks*, tanto en la investigación como en las actividades de remediación, para contener, automatizar (donde sea posible y apropiada) y mitigar el problema de falta de personal o experiencia de seguridad en la industria.

– La unidad de Cuentas Estratégicas de WatchGuard actúa no solo como un proveedor de seguridad sino, además, como un *partner* de negocio para el decisivo segmento MSSP/MDR. ¿Qué es lo que más se está demandando?

– Los MSSP/MDR tienen tres áreas de demanda bien identificadas: por un lado, precisan las tecnologías con las funcionalidades de seguridad que habilitan un servicio efectivo para proteger a sus clientes con la modularidad necesaria; por otro, requieren los elementos de gestión que permiten ser eficientes dentro de un entorno complejo de multi clientes, *multi-tiers*... Y, por último, necesitan la adecuación a su modelo de negocio (recurrente, de suscripción, con flexibilidad ante el cambio y evolución de servicios, etc). Así que, alineados con estas necesidades, aportamos un gran valor a nuestros MSSP/MDR con la efectividad de soluciones de seguridad que trabajan de forma conjunta (“la complejidad es el mayor enemigo de la ciberseguridad”), con la gestión eficiente de estas tecnologías, ofreciendo plataformas que estén diseñadas para que un tercero de valor sobre ellas y, también, con la adecuación al modelo de negocio.

– Acaban de presentar ‘WatchGuard for SOC’. ¿Qué papel juega en su portafolio?

– Es una evolución lógica de WatchGuard, una vez que ha integrado Cyatomic ofreciendo una propuesta apropiada para entidades que tienen cierto nivel de madurez en sus programas de seguridad (como, por ejemplo, los proveedores de servicios de seguridad y las cuentas estratégicas). El término SOC entra y sale de moda cada ‘x’ años, pero lo que es indiscutible es que el resultado de la seguridad está en la intersección de personas, tecnologías y procesos, y desde WatchGuard estamos poniendo mucho foco en esa realidad y en la colaboración con nuestros *partners* para que la seguridad, de verdad, no sea un privilegio de unos pocos.

– ¿Cómo valora la creación de la Red Nacional de SOC’s, coordinada por el CCN?

– En general, nos parece una iniciativa muy buena y necesaria. Siempre hemos sido unos grandes defensores de esta aproximación para tener “masa crítica” en esos SOC’s y la compartición de experiencias necesaria. También vemos que, sobre todo, en el sector público hay un componente de Seguridad Nacional en el que es crítico buscar un cierto nivel de autosuficiencia digital dentro del país. Eso sí, tener recursos nacionales que ‘viven’ y son ‘ciudadanos’ de este país es un tema muy relevante, que nos parece que no se valora en su justa medida. Yo, personalmente, he vivido en otros países donde este tipo de factores se tiene muy en cuenta y por razones relevantes.

– ¿Cuál es la madurez actual de los MSSP/MDR y qué espacio de mejora se espera de ellos?

– El panorama actual de seguridad está detrás del crecimiento de los MSSP/MDR, que se dan cuenta de las necesidades del mercado y de las oportunidades que hay. Algunos elementos críticos que hay que tener en cuenta son pasar de un *outsourcing off premise* a un modelo de servicios gestionados donde hay repetitividad (modelo ‘one to many’) y dirigirse hacia una pro-



“Nuestra propuesta WatchGuard for SOC es apropiada para entidades que tienen cierto nivel de madurez en sus programas de ciberprotección como, por ejemplo, los proveedores de servicios de seguridad y las cuentas estratégicas”

puesta donde el MSSP/MDR pueda, de verdad, extrapolar conocimiento y eficiencia de un cliente a otro. Para ello, es necesario avanzar en la madurez de evaluar y seleccionar un *stack* tecnológico determinado que se utiliza consistentemente vs ‘adaptarse’ a todos los ‘sabores’ de tecnologías y preferencias de cada cliente individual. Tenemos mucho talento, pero hemos de ser capaces de industrializar el servicio para ganar la masa crítica que facilita la mejora del servicio y la habilitación de un modelo de negocio con márgenes adecuados al valor que se entrega.

– ¿Qué le gusta destacar de Cyatomic a profesionales tan especializados como los CISO, a los que el mercado apabulla con propuestas tecnológicas y de servicios?

– Ese “apabullamiento” es el problema al que nos referimos cuando decimos que la complejidad es el mayor enemigo de la ciberseguridad, y en lo que nos afanamos en solucionar (orgánicamente y vía adquisiciones). De ahí la propuesta con varias familias de tecnologías que se unifican con modularidad en el entorno de *Unified Security Platform*. Yo les diría que hablásemos. Lo cierto es que cuando les contamos nuestra propuesta, no solo la filosofía sino la implementación y caso de uso, estamos teniendo muy buena respuesta.

– ¿Qué clientes de referencia tienen?

– Contamos con referencias muy importantes dentro de la Administración Pública y del sector privado: Banca y Seguros, Infraestructuras Críticas y servicios esenciales, así como en Educación y Retail.

– Con 15 años de experiencia en el mercado estadounidense, ¿qué podríamos aprender de allí y viceversa?

– He tenido la suerte de estar expuesto a entornos de producto y cliente muy sofisticados y dicha experiencia –y alguna cicatriz que otra– ha sido enriquecedora. No creo, ni mucho menos, estar en posesión de la verdad, pero sí puedo aportar una vivencia que se completa con la local para dar mejores soluciones. Pienso que el valor de la experiencia es saber qué cosas han funcionado y cuáles no. Algo especialmente crítico en ciberseguridad donde, a nivel global, hay retos críticos (falta de personal, gran profusión de *vendors*, entorno de TI que se complica con la nube, movilidad, trabajo remoto...), y un adversario bien financiado y que se sigue especializando y profesionalizando. ●

Protección unificada, inteligencia de amenazas proactiva y confianza cero para los equipos de respuesta y proveedores de servicios

Con un portafolio integrado de soluciones, disponible de forma modular, WatchGuard-Cytomic ofrece a grandes corporaciones y proveedores de servicios protección avanzada con capacidades preventivas y anticipativas, una propuesta de valor abanderada por sus capacidades de analítica, inteligencia avanzada, automatización, control de la identidad, así como por un equipo de expertos especializados en análisis y caza de amenazas.

Para ser lo que hoy son, la innovación lleva más de dos décadas marcando el camino tanto de WatchGuard, como de la adquirida Panda Security. Mientras que la compañía española fue pionera, en 2004, en análisis de comportamiento, en ofrecer un producto basado en el escaneo en la nube tres años después y, en 2016, erigirse como único proveedor europeo de la Guía del Mercado EDR de Gartner, la estadounidense, que hoy es su matriz, por su parte ofreció en 1996 su primera aplicación de ciberseguridad; en 2014, aportó al mercado un novedoso sistema de protección frente a APTs; y, en 2018, tras comprar Auth-Point, se convirtió en un referente en autenticación multifactor (MFA).

Todos ellos son hitos que hereda el actual portafolio de WatchGuard-Cytomic con tecnologías y servicios gestionados que cubren desde la protección avanzada de red, endpoints, wi-fi seguro y autenticación multifactor, hasta la provisión de servicios de inteligencia de amenazas y capacidades preventivas y anticipativas.

Con él da respuesta a una realidad donde las oficinas híbridas, así como el continuo uso de la nube y, en especial, de las aplicaciones SaaS, está generando peligrosos vectores de ataque a través del compromiso de credenciales, la suplantación de identidad y la ingeniería social, y los generados por las vulnerabilidades en el software de terceros y la pérdida o robo de dispositivos.

WatchGuard for SOC: fruto de la evolución

Entre las novedades de la compañía destaca, sin duda, su evolución a lo que ha denominado 'WatchGuard for SOC'. Se trata de una propuesta unificada y modular, pensada para facilitar la labor de los analistas de los centros de operaciones de seguridad, sobre todo, en los incidentes que precisan de una investigación posterior con herramientas y telemetría. En definitiva, se trata de una apuesta clara para incrementar la velocidad de acción de los equipos de los SOC con decisiones documentadas y razonadas frente a cualquier posible amenaza.

Por eso, su diseño permite cubrir las diferentes fases del SOC, a través de tecnologías innovadoras e integrando Jupyter Notebooks, embebida en la solución Orion, pero adaptada a cada caso de uso. Esta propuesta también incluye el reconocido Advanced Endpoint Security para SOC, que se basa en capacidades de procesamiento escalables y en su arquitectura nativa de la nube, pudiéndose ampliar a través de su API.

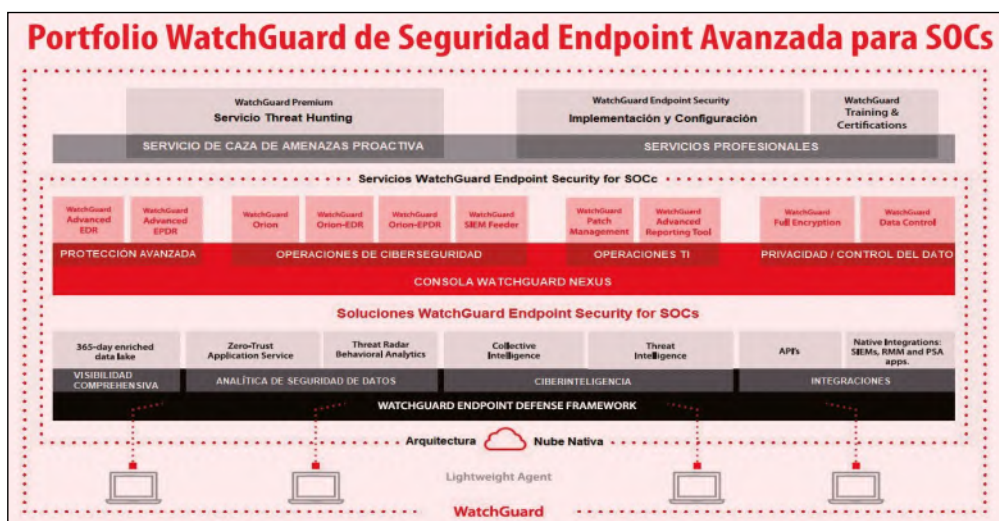
A través WatchGuard for SOC, la compañía busca reforzar, por un lado, a los equipos de seguridad (SOC) y de respuesta a incidentes (CERT/CSIRT), que adolecen de falta de expertos, problemas para administrar de forma eficaz múltiples soluciones de ciberprotección, así como tiempos de detección y respuesta insuficientes. Y, por otro, a los proveedo-

ra a servicios de búsqueda, detección y respuesta de incidentes, y apoyándoles en su relación con el cliente final.

Unified Security Platform

La compañía ha construido así un portafolio integrado, unificado y modular, capaz de adaptarse a las soluciones de ciberseguridad con las que ya cuenten sus clientes e integrar sus tecnologías y herramientas en el stack tecnológico de cualquier organización, sin fisuras.

El fiel reflejo de esta aproximación también reside en otra de las grandes propuestas de valor de WatchGuard-Cytomic: su Unified Security Platform (USP), construida desde cero para habilitar servi-



res de servicios gestionados, especialmente a los MSSP/MDR, un canal cada vez más estratégico. Dentro de este último aspecto, el valor añadido de la propuesta de WatchGuard-Cytomic es acompañar a los proveedores especializados, dotándoles de una plataforma y herramientas de búsqueda y EDR completas, permitiéndoles ampliar su carte-

cios de protección potentes, eficientes y escalables. Con ella, la compañía busca reemplazar el antiguo enfoque de seguridad de 'mosaico', que ha incrementado la carga de gestión de las empresas y les ha mermado la capacidad de protección contra amenazas actuales y aquellas en evolución. A través de esta plataforma de seguridad unificada, se pue-

'WatchGuard for SOC' es la novedad estelar de la compañía, una propuesta modular pensada para facilitar la labor de los analistas de los SOC, sobre todo, en incidentes que precisan de una investigación posterior con herramientas y telemetría.

de disponer de tecnologías avanzadas, que por lo general suelen estar desconectadas, para contar con una seguridad integrada de múltiples capas en la red, los usuarios, los *hosts* y las aplicaciones. Para ello, se compone de cinco elementos clave que se combinan para elevar y armonizar la entrega de seguridad:

1) El primero reside en una cartera integrada de productos y servicios de protección de red, autenticación multifactor y *endpoint* para proteger entornos, usuarios y dispositivos.

2) Bajo el nombre de WatchGuard Cloud, ofrece, además, una interfaz de visibilidad y generación de informes para toda la plataforma de seguridad unificada, que permite a los equipos contar con un único panel para la administración de extremo a extremo de todo el *stack* de seguridad de WatchGuard.

3) El tercer elemento clave hace referencia a su capacidad de automatización, a través de Automation Core, que brinda simplificación y escala a todos los aspectos del consumo, la entrega y la gestión de la seguridad.

4) A ello se le suma el hecho de ser una plataforma preparada para adoptar una postura de seguridad de confianza cero, a través del Identity Framework de WatchGuard, e implementar un enfoque basado en XDR real para la detección y reparación de amenazas, a través de ThreatSync.

5) Por último, ofrece acceso directo a la API, un rico ecosistema de integraciones listas para usar y herramientas para una rápida implementación. Cabe destacar que, como parte de su cartera de soluciones, los usuarios de USP pueden disponer desde de un servicio de inteligencia, a través de la solución Orion, hasta de EDR (*Endpoint Detection and Response*), EPDR (*Endpoint Protection, Detection and Response*), a través de los que se puede contar con parcheo automático, cifrado, visibilidad de los datos y, por supuesto, gracias a la

automatización, la clasificación automatizada de posibles amenazas, Indicadores de Compromiso (IoCs) y control nativo EPP, EDR y Servicios de Ciberseguridad Gestionados. Todo desde una sola consola de fácil uso y rapidez de acción, que permite acceder a capacidades avanzadas.

Confianza cero y caza de amenazas

En su propuesta tampoco falta un enfoque de Confianza Cero, que constituye el pilar de las soluciones de WatchGuard-Cytomic, entre las que destaca la protección avanzada del *endpoint* que proporciona WatchGuard a través del servicio Zero Trust Application, que permite la supervisión continua de los *endpoints*, la detección y la clasificación de toda la actividad para revelar y bloquear comportamientos anómalos de los usuarios, las máquinas y los procesos.

Al tiempo, destacan también los servicios de *Threat Hunting* y telemetría para una detección proactiva y una efectiva caza de amenazas. Y sobre ello, un *framework* de soluciones y servicios focalizados en descubrir a los atacantes con técnicas *living off the land* y *malwareless* (en su intento de evadir los controles existentes y comprometer a la organización), con tecnologías y procesos que aceleran

la investigación, mitigación y respuesta de forma sencilla y unificada, a través de diversos algoritmos y técnicas de IA. Esta tecnología hace posible el registro de más de 70 millones de eventos cada semana, así como contar con un *'data lake'* para sus sistemas de *machine learning* (ML) e IA de más tres billones de eventos.

El factor humano

Junto con las tecnologías, el elemento humano de los *hunters* y los analistas expertos de WatchGuard-Cytomic es crítico para poder adaptarse a la evolución de los adversarios y las nuevas técnicas. La

compañía cuenta así con una unidad de Seguridad Data Science, especialistas en amenazas, además de un equipo de operaciones y *hunters*.

La primera es responsable del servicio Zero-Trust Application, donde el sistema de ML a escala en la nube, "asegura la clasificación del cien por cien de los binarios descubiertos", destacan desde la compañía. Además, "maximizan los resultados del proceso de *threat hunting*, aplicando técnicas de aprendizaje automatizado y profundo a los más de 10.000 millones de eventos diarios que procesa la plataforma, automatizando el análisis a partir de las anomalías identificadas", añaden.

Por su parte, los especialistas de amenazas apoyan al resto de unidades con su profundo conocimiento en *reverse engineering*, análisis avanzados sobre artefactos y TTPs, análisis de fuentes de *threat intelligence* y explotación de vulnerabilidades.

De forma paralela, los *threat hunters* son analistas expertos en detectar nuevos ataques o principios de ataque en los clientes, operando con Orion, lo que les permite investigar en lagos de datos de eventos con un gran nivel de profundidad y detalle, en tanto que el equipo de operaciones de seguridad gestiona las anomalías de comportamiento (TTPs) e Indicadores de Ataque (IoA). ●



La importancia de la identidad para anticiparse a las amenazas

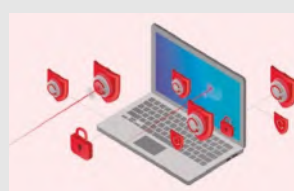
WatchGuard-Cytomic da la máxima importancia a la gestión y protección de la identidad. De hecho, en su catálogo destaca su propuesta de factor de doble autenticación (MFA). Para ello cuenta con productos innovadores, como **Authpoint**

WatchGuard Identity Framework, ciberseguridad centrada en el usuario



MFA, un servicio basado en la nube con un bajo coste total de propiedad (TCO), protección robusta a través del inicio de sesión único (SSO), autenticación basada en riesgos (a través de las ubicaciones de red, programación de tiempo, ADN móvil, ubicación geográfica, etc.) y Confianza Cero, tanto para empresas que trabajen en local como en entornos híbridos y, sobre todo, a través de la nube.

Orion, la automatización de la detección y la respuesta



Sin duda uno de los principales logros de WatchGuard-Cytomic se concreta en su solución estrella: **Orion**, que permite acelerar la respuesta a incidentes y búsqueda de amenazas sin *malware*, basándose en analítica de comportamiento a escala, desde la nube. "La clave es anticiparse a los adversarios" gracias a la "cantidad y calidad de eventos monitorizados en los *endpoints* y a la capacidad para enriquecerlos con inteligencia y analizarlos a escala", destacan desde la compañía. El objetivo es mejorar las capacidades del SOC gracias a una mayor anticipación ante cualquier ataque, un proceso ágil y continuo de caza, investigación y respuesta, así como una mayor facilidad para la atribución y el mapeo con cientos de TTPs del *framework* ATT&CK de Mitre, además de contar con indicadores de compromiso (IoCs) en tiempo real y retrospectivo y de inteligencia de amenazas.

Seguridad Avanzada WatchGuard for SOC

En busca de lo desconocido con Threat Hunting



Servicios de
Threat Hunting



Detección, investigación
y respuesta



Ciber
Resiliencia

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



SEGURIDAD
ENDPOINT AVANZADA



AUTENTIFICACIÓN
MULTIFACTOR



NUBE SEGURA
WI-FI



SEGURIDAD
DE RED

Smart Security, Simply Done.

Contacto: 900 840 407

Email: strategic.accounts@watchguard.com

www.watchguard.com

ViCON

Congreso de Ciberseguridad de Vigo

Fechas: 8/9-4-2022
Lugar: Círculo de Empresarios de Galicia. Vigo
Correo-e: vicon@galicia.com
Sitio: vicon.gal

Formación en Ciberseguridad especializada

- CEH (Ethical Hacking and Countermeasures v11)
 - CND (Certified Network Defender)
 - CCISO (Certified Chief Information Security Officer)
 - CHFI (Computer Hacking Forensic Investigator)
 - CSCU (Certified Secure Computer User)
 - CPENT (Certified Penetration Testing Professional)
- Organiza: M2i Formación
Tel.: 91 578 23 57
Correo-e: info@m2iformacion.com
Sitio: m2iformacion.com

Webminario. Nuevos controles de ciberseguridad en la actualización ISO/IEC 27002:2022

Organiza: Sothis
Fecha: 21-4-2022
Tel.: 900 923 533
Correo-e: info@sothis.tech
Sitio: sothis.tech/webinars

La voz de la Industria de Andalucía

- Málaga, 26-4-2022
 - Sevilla, 28-4-2022
- Organiza: Centro de Ciberseguridad Industrial-CCI
Tel.: 910 910 751
Correo-e: info@cci-es.org
Sitio: cci-es.org

Espacio TISEC

Ransomware ¿Quién paga la fiesta?

Organiza: Revista SIC
Fechas: 27/28-4-2022
Acto presencial y retransmitido
Lugar: Hotel Novotel
Campo de las Naciones. Madrid
Sitio: revistasic.com/tisec

Cursos SANS INSTITUTE

- Security Essentials: Network, endpoint and Cloud 25-4/6-5-2022.
 - Hacker tools, techniques, exploits and incident handling 4/15-7-2022.
 - Reverse-Engineering Malware: malware analysis tools and techniques 14/15-11-2022
- Organiza: One eSecurity
Lugar: Madrid
Tel.: 911 011 000
Correo-e: sans@one-esecurity.com
Sitio: one-esecurity.com/events_training.html

C1b3rWall

Congreso de seguridad digital y ciberinteligencia

Organiza: Escuela Nacional de Policía
Fechas: 21/23-5-2022
Lugar: Escuela Nacional de Policía en Ávila
Sitio: congresociberwall@policia.es

Barcelona Cybersecurity Congress

Fechas: 10/12-5-2022
Lugar: Fira Gran Via
Hospitalet de Llobregat
Organizan: Fira Barcelona y Agència

de Ciberseguretat de Catalunya
Sitio: barcelonacybersecuritycongress.com

XXIX Congreso @ASLAN 2022

Fechas: 18/19-5-2022
Lugar: IFEMA Palacio Municipal de Congresos. Madrid
Organiza: Asociación @ASLAN
Tel.: 91 831 50 70
Correo-e: info2022@aslan.es
Sitio: aslan.es

RSA Conference

Fechas: 6/9-6-2022
Lugar: San Francisco. EE.UU.
Correo-e: information@rsaconference.com
Sitio: rsaconference.com

Congreso Euskalhack

Organiza: Asociación Euskalhack
Fechas: 24/25-6-2022
Lugar: Colegio Mayor Olarain. San Sebastián
Sitio: securitycongress.euskalhack.org

JNIC 2022

VII Jornadas Nacionales de Investigación en Ciberseguridad

Organizan: Secretaría de Estado de Digitalización e Inteligencia Artificial, INCIBE y Tecnalia
Fechas: 27/29-6-2022
Lugar: Palacio Euskalduna. Bilbao
Correo-e: jnic2022@tecnalia.com
Sitio: 2022.jnic.es

UAD360. II Edición

Organiza: Hispasec
Fechas: 10/11-6-2022
Lugar: Escuela de Informática y

Telecomunicaciones. Málaga
Tel.: 952 020 494
Sitio: uad360.es

SECURMATICA 2022

Pensar la ciberseguridad. Y repensarla.

Organiza: Revista SIC
Fechas: 4/6-10-2022
Lugar: Hotel Novotel
Campo de las Naciones. Madrid
Tel.: 91 575 83 24
Fax: 91 577 70 47
Correo-e: info@securmatica.com
Sitio: securmatica.com

AENOR Formación

Organiza: AENOR
Tel.: 91 432 61 25
Sitio: aenorciberseguridad.com

Cursos Ciberseguridad

Westcon-Comstor

Organiza: Westcon-Comstor
Lugar: Madrid
Tel.: 91 419 61 00
Correo-e: academy.es@westcon.com
Sitio: https://academy.westconcomstor.com/es/

Cursos ES-CIBER

Organiza: Escuela Superior de Ciberseguridad, ES-CIBER
Correo-e: info@es-ciber.com
Sitio: es-ciber.com

Centro de Formación Exclusive

Organiza: Exclusive Networks
Tel.: 91 197 66 01
Sitio: training.exclusive-networks.com/es-ES

INDICE DE ANUNCIANTES

EMPRESA	PAG.	EMPRESA	PAG.	EMPRESA	PAG.
AENOR	115	F5	13	QUALYS	177
AIUKEN	19	FACTUM	27	RISKRECON	111
AKAMAI	131	FASTLY	173	S2 GRUPO	49
ALL4SEC	171	FORCEPOINT	153	S21SEC	99
ARROW	75	FORTINET	21	SECURMÁTICA	7
BARRACUDA	59	GMV	43	SEIDOR	31
BLUELIV	73	HORNETSECURITY	105	SENTINELONE	85
BROADCOM	41	ICA	175	SIEMENS	45
CAPGEMINI	39	IMMERSIVE LABS	33	SMARTFENSE	141
CCI	147	INGENIA	109	SOPHOS	63
CEFIROS	89	INVICTI	37	SOTHIS	169
CHECK POINT	4	ITS	77	STORMSHIELD	93
CIPHER	91	JTSEC	69	TARLOGIC	23
CISCO	9	LEET SECURITY	161	TECH DATA	79
COUNTERCRAFT	155	LOGICALIS	81	THALES	83
CROWDSTRIKE	25	MDTEL	87	TISEC	Contraportada
CYBERRES	65	MNEMO	151	TRELLIX	133
CYMLATE	57	NETSKOPE	103	TREND MICRO	97
DELINEA	29	NUNSYS	135	VMWARE	17
DOTFORCE	165	OKTA	95	V-VALLEY	2-3
ELIX-MIA	145	ONE ESECURITY/SANS INSTITUTE	179	WALLIX	51
ENTELGY INNOTECH	35	ONE IDENTITY	61	WATCHGUARD-CYTOMIC	55
ENTRUST	143	ONESEQ	149	WESTCON	53
EPIC BOUNTIES	137	ONTINET-ESET	167	ZEROLYNX	47
ES-CIBER	163	PENTERA	107	ZSCALER	67
EXCLUSIVE NETWORKS	101	PROOFPOINT	71		
EY	15	PWC	11		



SANS INSTITUTE EN ESPAÑA
LA EXCELENCIA EN LA FORMACIÓN
EN CIBERSEGURIDAD



One eSecurity, empresa líder en servicios DFIR y ciberseguridad, te brinda la posibilidad de **formarte y certificarte en España** en los prestigiosos cursos de **SANS Institute**.

Aprende y comparte con nuestros instructores de talla mundial como **Jess García, SANS Senior Instructor**, con más de 14 años compartiendo y difundiendo conocimiento.

Formato Live Online



Sesiones interactivas con los instructores de SANS



Laboratorios prácticos



Acceso a las grabaciones durante 4 meses tras el curso



Programa y materiales en formato electrónico



Flexibilidad de tiempo (2 semanas)

CALENDARIO 2022



SEC401 | GSEC |

Security Essentials: Network, Endpoint, and Cloud

25 ABR - 6 MAY de 2022

15h - 21h CEST

De Lunes a Viernes



SEC504 | GCIH |

Hacker Tools, Techniques, Exploits, and Incident Handling

4 - 15 JUL de 2022

15h - 20h CET

De Lunes a Viernes



FOR610 | GREM |

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

14 - 25 NOV de 2022

15h - 20h CET

De Lunes a Viernes



Carlos Frago



Jess García

Otoño 2022 :

FOR500: Windows Forensic Analysis - **FOR508**: Advanced Incident Response, Threat Hunting, and Digital Forensics

El precio de los cursos es de 6.995 € + IVA. Todos los cursos deben abonarse un mes antes de su inicio. La certificación GIAC tiene un precio adicional de 725 € + IVA (válido solo si se reserva en conjunto con el curso).

Información de contacto

www.one-esecurity.com | sans@one-esecurity.com | [in](https://www.linkedin.com/company/one-esecurity) one-esecurity | Teléfono: +34 911 011 000

espacio

tiSec

RANSOMWARE

¿Quién paga la fiesta?

FORMATO MIXTO:

presencial y retransmitido

Madrid

27 y 28 de abril _2022

Organiza:

Copatrocinan:

Revista **Sic**

www.revistasic.com/tisec



AON



kaspersky

