



Revista

Ciberseguridad, seguridad de la información y privacidad

CISOS

**Ser o no ser
...de primera
o de segunda**

PROYECTOS

• **Ministerio
de la Presidencia**
• **Seat**

CIBERSEGURIDAD 5G

**A primer plano
por derecho propio**

SOLDADO VIRTUAL

**Convergencia:
Ciberseguridad/Ciberarmas**

ENTREVISTA



Rosa Kariger
CISO Global
IBERDROLA

ENTREVISTA



Josep Albors
Director
de Investigación
y Concienciación
ESET España

CIBERSEGURIDAD EUROPEA

Marcada a fuego



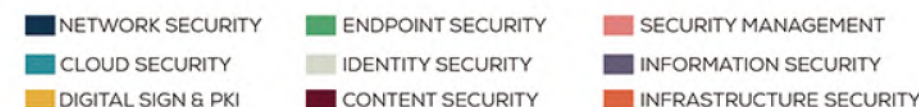


Ciberseguridad: el mejor socio de valor a ambos lados del mercado.

- Equipo experto
- Tecnologías punteras
- Soluciones adaptativas
- Capacidad financiera



Ciberseguridad Corporativa





Check Point®
SOFTWARE TECHNOLOGIES LTD



Infinity-Vision

Seguridad absoluta Zero Trust con Check Point Infinity-Vision

Con las ciberamenazas existentes dentro y fuera del perímetro de seguridad, se ha vuelto esencial adoptar un enfoque de seguridad Zero Trust para mantener los datos protegidos, en cualquier lugar. Nuestro enfoque práctico y holístico para la implementación de Zero Trust le permite evitar complejidades y riesgos con una única arquitectura de seguridad Zero Trust consolidada.

Más información: www.checkpoint.com/es

SECURE YOUR EVERYTHING™



>> Sumario

DOCUMENTOS



I-VIII



86 ROSA KARIGER,
CISO de IBERDROLA



160 JOSEP ALBORS, Director
de Investigación
y Concienciación
de ESET

6 EDITORIAL	132 INFORMES Y TENDENCIAS
8 DOBLE FONDO	164 PROPUESTAS
10 SIN COMENTARIOS	170 NOVEDADES
12 NOTICIAS	178 BIBLIOGRAFÍA
79 PROYECTOS	182 ACTOS Y CONVOCATORIAS

>> en este número

- 91** Especial CISOs: Ser o no ser... de primera o de segunda
 - Crónicas desde el monte Nebo, por MANUEL CARPIO
 - Implicaciones para el Operador y su CISO de la Declaración de Aplicabilidad. FAQ, por MARIANO JOSÉ BENITO y JAVIER ZUBIETA
- 97** Especial Ciberseguridad europea... marcada a fuego
 - La apuesta por la evaluación y certificación de productos en la UE: panorama
 - Algunas fuentes de información: ENISA, ECSO y la OC-CCN
 - La carrera de la certificación más allá de la UE
 - La certificación de ciberseguridad en Europa: dos años del Cybersecurity Act, por JOSÉ RUIZ y JAVIER TALLÓN
 - LINCE, una herramienta que aporta más confianza a la ciberseguridad, por BORIS DELGADO y CARLOS M. FERNÁNDEZ
 - ¿Quién evalúa al evaluador?, por PABLO LÓPEZ
 - Modelo de las tres sonrisas en un esquema de certificación en ciberseguridad industrial, por JOSÉ VALIENTE
 - La seguridad y la evaluación de conformidad y certificación de PSC eIDAS y servicios, un enfoque global, por PALOMA LLANEZA
 - Sobre la Certificación de la Seguridad en una Industria Digitalizada, por JORGE DÁVILA
- 150** Redes 5G, la ciberseguridad pasa a un primer plano por derecho propio, por IGNACIO PÉREZ y ÓSCAR DÍAZ
- 154** La convergencia de la CiberSeguridad con las CiberArmas y el nacimiento del 'soldado' virtual, por JUAN MIGUEL VELASCO
- 156** ESTRATEGIA: Sophos: ciberseguridad potente e intuitiva para una protección efectiva, por RICARDO MATÉ

• **Evaluación y certificación de productos, procesos y servicios.** Hasta la fecha, esta es una de las dos grandes líneas abiertas por la UE tras la publicación de su Ley de Ciberseguridad. No es un asunto fácil de entender para todo el mundo (y sí muy polémico para algunos), porque a la complejidad previa en la materia a escala global y de cada estado, se viene a sumar el complicado modelo por el que hemos optado los europeos y el vibrante y multidimensional escenario digital, que quizá no aguante una sistemática anclada a efectos prácticos en el sector industrial del siglo pasado, si no fuera con el apoyo digital de una hipotética IA en la que se pueda confiar.

En esta edición SIC dedica unas páginas especiales a exponer el estado del arte de la evaluación y certificación de la ciberseguridad del conjunto de productos TIC, del que por ahora los que tienen propósitos exclusivos de ciberseguridad son una pequeña parte.

La idea es ir creando un marco de esquemas europeos en distintos frentes (productos TIC (EUCC), nube, 5G, IoT, componentes industriales, desarrollo seguro, IA, criptografía...), y establecer distintos niveles, además de contemplar la sectorización. También se quieren armonizar (en lo que fuera necesario) las metodologías de certificación ligeras. Y por añadidura, que el constructo vaya siendo compatible con lo que se guise en los espacios extracomunitarios.

La idea es promover el cumplimiento legal a la europea en los productos que se fabriquen y que se vendan y/o consuman en el mercado interior y, al tiempo, potenciar la industria propia, algo a lo que sin duda debe contribuir decisivamente la otra gran apuesta de la UE: el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación.

Estas loables pretensiones tienen un notable impacto en el mercado (oferta y demanda), en las regulaciones, la capacitación de las personas, la competitividad, la I+D+i + P (de Producción)... Y, por supuesto, requieren de un plan B, no vaya a ser que la globalización funcione de verdad y se nos caigan a todos las barreras.

• **RSIs/CISOs.** El Real Decreto 43/2021 ha provocado una explosión de webeventos para explicar, supuestamente a los interesados, las consecuencias que tiene su contenido para los RSIs/CISOs.

Con el ánimo de aportar, tres excelentes profesionales (un CISO y dos que lo han sido) brindan en esta edición sus opiniones, que no tienen desperdicio. Un ex habla directamente de CISOs de primera y de segunda (según estén o no regulados); y un CISO en activo y un ex, le entran a la Declaración de Aplicabilidad. Para no perderselo.

• **Países en los que mirarnos.** Algunos están peor; pero otros nos llevan ventaja en darle valor a su ciberseguridad. Mencionaremos dos, uno de la UE y otro que se acaba de marchar. El primero, Francia, preocupado por los ciberataques a hospitales, va a reforzar su estrategia con un presupuesto extra de 1.039 millones de euros (720 los pondrá el Estado y 319 el sector privado).

El segundo, Reino Unido, que cuenta con una estrategia de seguridad cibernética dotada con 2.200 millones de euros, ha creado un Consejo de Seguridad Cibernética y tiene avanzada una propuesta para desarrollar el mercado de la identidad digital. (Los británicos son así).

En España tenemos más leyes, normas, organismos, los mejores expertos, los mejores proveedores, *hubs*, *clusters*, observatorios... Pero no tenemos euros.

• **Telefónica.** No es de extrañar que gran parte del sector esté todavía recuperándose de la sorpresa causada por la noticia del despido de Pedro Pablo Pérez, hasta ese momento CEO de la Unidad de Negocio de Ciberseguridad. Y no solo de él, sino de otras personas de su Equipo. En los mentideros del gremio se oye de todo. Veremos si la cosa da más que hablar.

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:** Horatiu Bandoiu, Mariano J. Benito, Alberto Cañadas, Manuel Carpio, Jorge Dávila, Boris Delgado, Óscar Díaz, Carlos M. Fernández, Eutimio Fernández, Manuel García, Raúl Gordillo, Julián Hernández, Paloma Llana, Ricardo Maté, Francisco Quintero, Pablo López, Alberto Partida, Ignacio Pérez, José Ruiz, Javier Tallón, José Valiente, Juan Miguel Velasco, Javier Zubieta **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.

Entelgy Innotec

SECURITY

Live confident,
be (cyber) secure

Para ti,
¿cuánto cuesta la
tranquilidad?

 Entelgy Innotec Security

 Entelgy Innotec Security

 @InnotecSecurity

 @innotec.security

innotec.security

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





JOSÉ DE LA PEÑA MUÑOZ
Director
jpm@codasic.com

La ciberseguridad bien merece una sonrisa

Los que gustamos de guardar una cierta corrección en el uso del castellano ya perdimos la batalla del cifrado, al considerar los académicos de la lengua el horripilante anglicismo encriptar como sinónimo de cifrar. Hace poco hemos perdido otra, al aceptar también la Academia el vocablo troyano, al que entienden como caballo de Troya; quiere decirse, por tanto, que para los guardianes del idioma, y según el significado que atribuyen en el diccionario a esta palabra en su tercera acepción, un troyano es un caballo de Troya.

Al dar carta de naturaleza general a esta aberración conceptual de uso muy común en los ambientes TIC poco cuidadosos, la RAE ha escrito una nueva página del manual que justifica el significado exclusivamente por el uso (con ser este importante). Así, en un futuro quizá no lejano, si se pusiera de moda llamar a los ladrones policías y a las pérdidas ganancias, los académicos lo podrían admitir. Por nuestro bien.

Algunos promotores de entes dedicados a la ciberseguridad, no encontraron el nombre redondo a la hora de bautizarlos, porque los facilones ya los usaban otros y porque los que se les ocurrían eran deplorables. Y como tenían poco cacumen y mucha prisa, ¡zas, se quedaron con la ciber y han desechado la seguridad!

Y por lo que se observa, se están cociendo otras subversiones, una de ellas gloriosa. Me explico: Resulta que en algunos ambientes universitarios para ahorrar saliva al hablar y redundancia al escribir, profesores y alumnos llaman a la ciberseguridad “la ciber” (o “la cyber”), fiando el significado al contexto –lo haya o no– y apoyándose inconscientemente en semejante reducción para criar sensación de identidad de grupo. O para que entre en un tuit. ¡Qué triste final le espera a la cibernética, apiolada por los intelectuales de “la ciber” (o “la cyber”)!

Ciberlincas

En otros escenarios sucede lo mismo con esta palabra. Pongamos por ejemplo el del mundillo de las asociaciones y centros. Algunos promotores y socios fundadores de entes dedicados a la ciberseguridad, al tener que ponerles nombre usando el maldito término compuesto, no dieron con la fórmula, sea porque las buenas opciones ya la usaban otros o porque quedaban fatal las que se les ocurrían. Y como hay

poco cacumen y prisa (sobre todo, prisa), izas, se quedaron con la ciber/cyber y desecharon la seguridad! Y listos para confundir en *webentos* copatrocinados, amenaza y riesgo, evaluación y certificación, esfera y toroide...

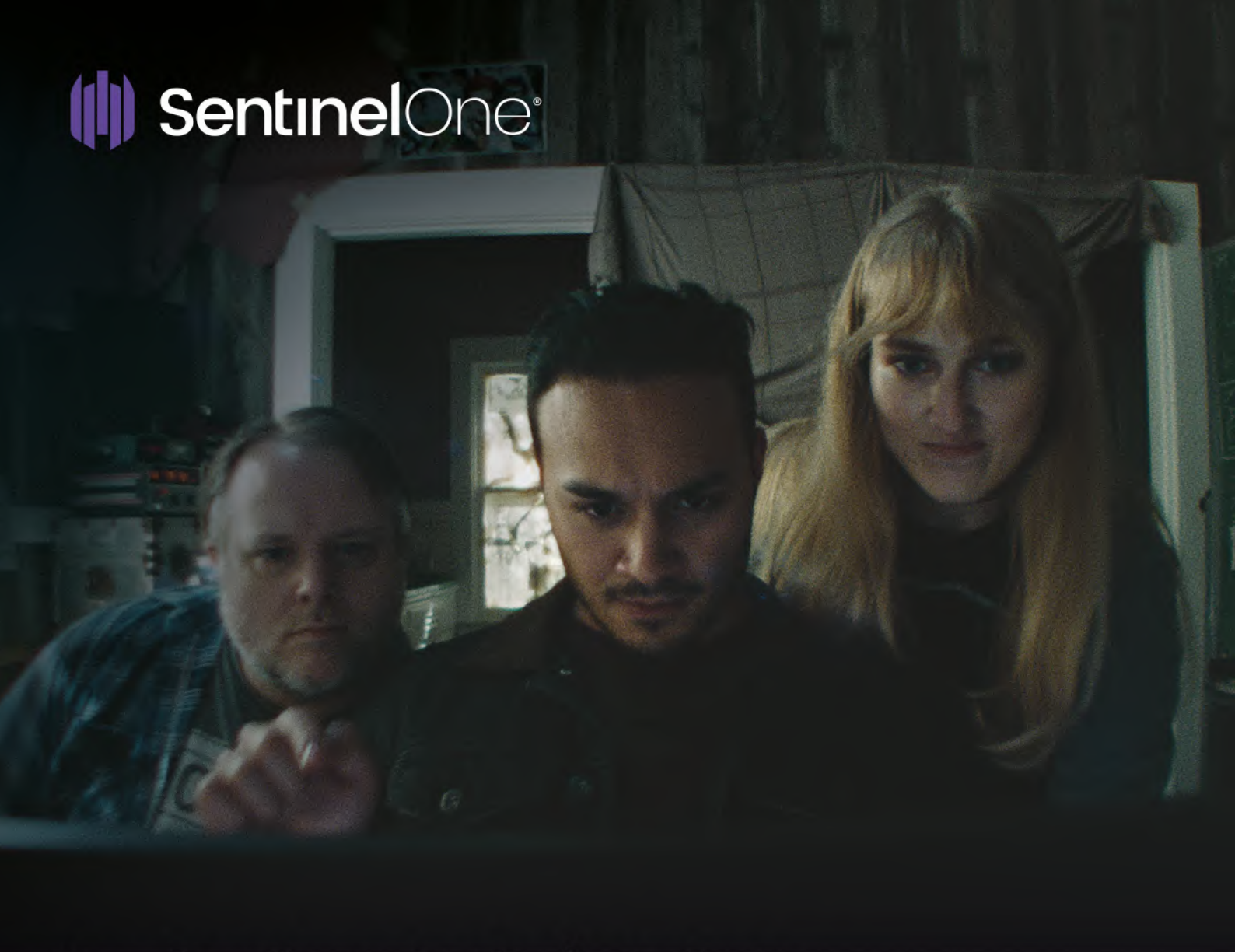
También se tiene noticia de una persona –a la que no identificaremos– que con la buena intención de buscarle al *ransomware* un término en español, descubrió la palabra *ranzón* (que significa dinero para rescate). Y sin más, nuestro intrépido alquimista del lenguaje, se lanzó a proponer por las redes sociales que al *ransomware* le deberíamos llamar *ranzón*, o, a lo sumo, “*ranzonware*”. Pero la cosa no ha prendido, como le paso en su momento al *jeriñac*, palabro con el que se quería castellanizar al *cognac*, hoy coñac.

Desde luego, en este gremio no lo pasamos tan mal. Y como voy teniendo una edad, no me resisto a contar a los lectores más jóvenes y a los recién llegados (que son muchos) un par de anécdotas. Una vincula a esta publicación y a un grupo de colegas del sector, que hace muchos años creamos un exitoso grupo de rock al que pusimos de nombre ¡SpamTo! El grupo ya no existe; pero el *spam* está que se sale de los buzones.

Ya se nos veía entonces la ironía. Y va la segunda: cuando se planteó en INTECO el cambio de nombre, hubo una persona del Instituto que propuso denominarlo CECINA (Centro de Ciberseguridad Nacional). Ganó INCIBE.

Esto demuestra que el buen humor y la sorna acompañan a la ciberseguridad, y que no todo en el ambiente sectorial se centra en la regulación de los CISOs regulados, de los CISOs no regulados todavía, de la responsabilidad civil de todos, de los riesgos en la cadena de provisión, de estrategias, planes, cuadros de mando, despidos, cierres de Q, cambios de trabajo, compras de empresa, proyectos, ataques, amenazas, orquestación, servicios gestionados, ciberseguridad OT, IT, IoT...

A veces tenemos tiempo para bromear y sonreír, para conocer los pasatiempos de nuestros colegas, para colaborar en pro de un bien común fuera y dentro de la profesión, y para reivindicar el buen hacer de privados y públicos. Y llegados a este punto, no quiero despedirme sin volver a recordar que desde este verano la página web del CNPIC sigue a fecha de cierre de esta edición (finales de marzo de 2021) con el certificado caducado, el cartel de obras puesto y el nombre antiguo. Supongo que, tras la reciente aprobación del plan estratégico del Ministerio del Interior para luchar contra el cibercrimen –dotado con la abultada cifra de un millón de euros– habrá medios para actualizarlo. ●



Los hackers trabajan duro. Nosotros trabajamos inteligentemente.

Descubra la ciberseguridad autónoma para el punto final, la IoT y la nube.

Solicite una demostración.

Más información en [**https://es.sentinelone.com/**](https://es.sentinelone.com/)



LUIS FERNÁNDEZ DELGADO
Editor
lfernandez@codasic.com

La Ciber Nostra



está haciendo la ciberseguridad acreedora de la debida consideración en estos días? Con la que está cayendo cabe temer que se socave su imagen de compañera indispensable y fraternal en esta desbocada odisea protagonizada por la sociedad digital que nos ocupa.

¿Razones? Aquí va la primera. Con enorme estupor el sector español de la ciberseguridad tuvo conocimiento en marzo pasado de una noticia inquietante: Telefónica, una de las mayores empresas en España con foco intenso en ciberseguridad –448 millones de facturación en 2020 bajo la marca ElevenPaths– había despedido en febrero a su máximo responsable del área de ciberprotección, Pedro Pablo Pérez, por presunto fraude en varias operaciones corporativas. Junto a él también trascendía que otros empleados fueron

origen británico especializada en tecnología de orquestación de antifraudes.

Como es sabido, la reestructuración de Telefónica –anunciada en noviembre de 2019– propició una remodelación de su división Tech –de la que SIC ya dio cuenta en su edición anterior– por la que se agrupaban las áreas de ciberseguridad y nube, de un lado, y de IoT y Big Data, de otro, dentro del paraguas genérico de Telefonía Tech. De esta guisa, y en coincidencia con la visibilidad mediática del ‘affaire’, la matriz anunciaba el inmediato nombramiento al frente de la misma de María Jesús Almazor, anteriormente Consejera Delegada de Telefónica España.

Y ahora la segunda: el calvario **SEPE (Servicio Público de Empleo Estatal)**. Si no teníamos bastante ya con las oleadas de extorsiones causadas por *ransomware* cada vez más

agresivos en sus estragos e insaciables en sus pingües chantajes (la reciente a Acer andaba por los 50 millones), el golpeo con esta ‘técnica’ al SEPE y sus derivadas sociales de indefensión para con el desvalido afectado, visibiliza la acusada fragilidad y vetustez cibernética de una mayoría de entidades y organismos de carácter público cuya precariedad ciberdefensiva roza lo sonrojante, dejando en su sitio a los bocazas proclamadores de supuestos posicionamientos españoles favorables en rankings de ciberseguridad de cuestionable solvencia y/o representatividad. La verdad es que estarían

mejor calladitos (y dando más el callo con discreción para paliar las carencias). Entretanto, desde Interior se anuncia con gran boato un plan estratégico de ‘1 millón de euros’ para reforzar la lucha contra la cibercriminalidad. ¡Cielos, con semejante dotación ya podemos respirar tranquilos!

Y toca concluir con la tercera. Es bochornoso constatar cómo el triunvirato de grandes potencias mundiales –China, Rusia y EE.UU.– con sus respectivos prebostes al frente, buscan cualquier ocasión, cumbres incluidas, para arrojar los cibertrastos a la cabeza con la ciberseguridad por montera. Antes ni se la mentaba y ahora es una glamurosa arma arrojadiza. Resulta cansino oírles reprobarse mutuamente sus respectivas *razzias* digitales y, por supuesto, su bravuconería verbal nunca acompañada de pruebas fehacientes de la atribución. Eso sí, no resultaría extraño colegir que los daños derivados de su fraticida lucha en pos de la soberanía tecnológica mundial –*state-nation gangs* mediante–, sigan propiciando *vendettas* colaterales en países que como el nuestro, irremediabilmente han de alinearse con alguna de esas sensibilidades para disgusto de las restantes en este *wild west* digital global.

Proclama final: ¡Políticos planetarios, gestores y *celebrities* embelesados por la ciberprotección: no queremos que la ciberseguridad sea mentada en vano y mucho menos manoseada de modo utilitarista, no vaya a ser que la Ciber Nostra se nos venga arriba de verdad! ●

Con la que está cayendo, el zarandeo al que la ciberseguridad está siendo sometida bien pudiera socavar su imagen de compañera indispensable en esta odisea protagonizada por la sociedad digital.

igualmente desvinculados de la pujante unidad de negocio, tras un proceso investigador iniciado meses atrás y cuyas depuraciones tal vez no hayan concluido aún.

Ante las presuntas irregularidades –supuestamente cercanas al conflicto de intereses, contrataciones inapropiadas con proveedores, enriquecimiento ilícito...–, no sería extraño que la compañía presidida por Jose María Álvarez-Pallete considerara oportuno propiciar una taxativa y pronta *damnatio memoriae* y emprendiera acciones en los tribunales para esclarecer estos comportamientos reprobables, máxime con la celebración en el horizonte (23 de abril) de la Junta General de Accionistas, con el deseo a medio plazo de vender una más que suculenta unidad y con Europa muy atenta a toda señal de posible corrupción en los instantes previos al chorreo de euros para la recuperación (5G incluida).

Es de público conocimiento que la multinacional española venía acometiendo en los últimos años una activa política de inversiones y adquisiciones en nuestro segmento, entre otras vías merced a Telefonía Tech Ventures –vehículo de inversión de Telefónica en *startups* en el campo de la ciberseguridad– y al *hub* de innovación abierta Wayra. Al respecto cabe recordar en los últimos tiempos las operaciones en España vinculadas con **Govertis**, **Pridetect**, **Nozomi**, **Smart Protection**, **iHacklabs**, **Alias Robotics** y hace escasas dos semanas **fcase**, *startup* de

Identi::sic



Organiza:

Revista **Sic**

www.revistasic.com/identisic

FORMATO MIXTO:
presencial y retransmitido

Madrid_
16 y 17 de noviembre_2021
Hotel Novotel Campo de las Naciones

Se están poniendo en marcha diferentes iniciativas, como crear una red de SOC y grupos de trabajo de seguridad en 6G y ciberinteligencia, entre otras acciones que servirán como base para la transformación europea

EL CONSEJO DE LA UNIÓN EUROPEA marca un plan de trabajo para reforzar la ciberprotección continental, mejorar la diplomacia cibernética y alcanzar una 'hegemonía digital'

Tras la presentación en diciembre de la nueva Estrategia de Ciberseguridad para la UE, el **Consejo** dio a conocer en marzo sus conclusiones, para esta década, sobre cuáles deben ser las prioridades para que Europa disponga de un "autonomía estratégica preservando una economía abierta".

Para ello, es fundamental "reforzar la capacidad de tomar decisiones autónomas en el ámbito de la ciberseguridad, con el objetivo de fortalecer el liderazgo digital". En definitiva, según destaca el documento aprobado, se trata de poner los pilares para construir una Europa "resiliente, verde y digital".



Ámbitos de actuación

Así, el Consejo ha identificado varios ámbitos de actuación fundamentales en los que hay que trabajar para incrementar la ciberprotección del Viejo Continente. Ello pasa por "crear una red de centros de operaciones de seguridad en toda la UE para monitorizar y anticipar señales de ataques a las redes", poner en marcha "una unidad cibernética conjunta que proporcione un enfoque claro al marco de gestión de crisis de ciberseguridad de la UE", aplicar y completar rápidamente la implementación de las medidas de la 'caja de herramientas 5G', garantizar la seguridad de estas redes, incrementar los esfuerzos conjuntos para acelerar la adopción de estándares clave de protección de Internet y, también, "apoyar el desarrollo de un cifrado sólido como medio de proteger los derechos fundamentales y la seguridad digital, garantizando al mismo tiempo la capacidad de las autoridades policiales y judiciales para ejercer sus poderes tanto en línea como fuera de línea".

Prevenir ataques

El Consejo también considera importante "mejorar la eficacia y la eficiencia de la caja de herramientas de la diplomacia cibernética, prestando especial atención a prevenir y contrarrestar los ciberataques con 'efectos sistémicos' que podrían afectar las cadenas de suministro, la infraestructura crítica y los servicios esenciales, las instituciones y los

Crear una red europea de SOC's

No ha sido la única novedad estos meses en la UE, ya que la **Comisión** también ha propuesto invertir más de 300 millones de euros en desarrollar una red de SOC que genere conocimiento colectivo y comparta las mejores prácticas en la lucha contra las ciberamenazas. Asimismo, dio a conocer su intención de impulsar una asociación

europea que trabaje en la protección de redes y servicios inteligentes para 6G que, inicialmente, contará con una inversión pública en I+D+i de 900 millones de euros durante el nuevo período presupuestario 2021-2027. La asociación europea, según explica la Comisión, coordinará las actividades de investigación sobre la tecnología 6G dentro de Horizonte Europa, así como las iniciativas de implementación de 5G en el marco del Mecanismo Digital Conectando



procesos democráticos y socavar la seguridad económica".

Además, propone estudiar la creación de un nuevo grupo de trabajo de ciberinteligencia para fortalecer la capacidad específica de la UE en este ámbito, así como reforzar la cooperación con las organizaciones internacionales y los países socios que permitan defenderse mejor de las ciberamenazas.

Para garantizar que estas propuestas se desarrollan y se llevan a cabo, el Consejo animó a la Comisión y al Alto Representante de la UE a acometer un plan detallado en el que se fijen los hitos que se deben conseguir. Además, el Consejo ha mostrado su intención de seguir de cerca este plan de acción para que se revise y se actualice periódicamente, según las nuevas necesidades europeas en este ámbito.

Europa y otros programas.

A ello, se suma la apuesta de la Comisión por construir una infraestructura de comunicación cuántica segura ("**QCI**"), que garantice la protección de las comunicaciones de las autoridades públicas y que estará compuesta tanto por redes de comunicaciones por fibra, como por satélites enlazados que cubran la UE y los territorios de ultramar de la Unión. El organismo también ha avanzado que pondrá en marcha un plan de contingencia para escenarios extremos que afecten a la integridad y disponibilidad del sistema raíz del DNS global. Por último, ha destacado la necesidad por parte de los estados de **revisar el Marco de políticas de ciberdefensa ("CDPF")** y desarrollar "capacidades de vanguardia", a través de diferentes políticas e instrumentos de la UE.



Ante un ciberataque...
¿Cree que sus medidas de protección son
suficientes?

Proteja lo más importante



EN BREVE

ENISA incrementa sus acuerdos y publica documentos sobre el eIDAS, notificación de incidentes y 5G

Acuerdo Enisa Cert-EU

La Agencia de Ciberseguridad de la UE (Enisa) y el CERT-UE han firmado un Memorando de Entendimiento (MoU) con motivo de la 13ª reunión de la red CSIRT.

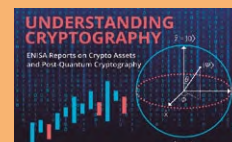


Este MoU establece el marco para apoyar el trabajo de los demás y lograr un mayor grado de eficiencia. El acuerdo surge como un esfuerzo por crear sinergias significativas y mutuamente beneficiosas entre ambas organizaciones y evitar posibles superposiciones o duplicaciones de actividades.

Por tanto, el acuerdo se incorporará directamente a los esfuerzos en curso a nivel de la Unión para mejorar la eficiencia y la eficacia del marco de ciberseguridad de la UE y sus actores.

Criptografía post-cuántica: estado actual y mitigación cuántica

Enisa también dio a conocer un nuevo estudio con la situación actual sobre el proceso de estandarización de la criptografía post-cuántica (PQC). En él identifica cinco familias principales de algoritmos: la basada en código, en isogenia, en *hash*, en celosía y en multivariante.



Además, analiza los finalistas de la tercera ronda del NIST para dar con uno que sea la referencia, algo que tardará aún unos años. Por ello, el documento propone dos candidatos que los propietarios de sistemas pueden implementar ahora para proteger la confidencialidad de sus datos contra un atacante con capacidad cuántica; a saber, implementaciones híbridas que utilizan una combinación de esquemas pre-cuánticos y post-cuánticos, y la mezcla de claves precompartidas en todas las claves establecidas mediante criptografía de clave pública.

Cuándo y cómo informar de los incidentes de seguridad

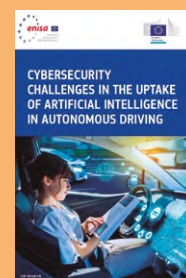
Enisa publicó en marzo nuevas directrices en un documento titulado 'EECC (Código europeo de comunicaciones electrónicas EECC)' para facilitar la notificación de incidentes de seguridad por parte de las autoridades nacionales de seguridad de las telecomunicaciones. Con ellas, se pretende "ayudar a las autoridades nacionales de seguridad de las telecomunicaciones a informar de incidentes importantes a Enisa y a la Comisión Europea en virtud del EECC".



Estas nuevas directrices sustituyen a las anteriores emitidas por la Agencia sobre notificación de incidentes. Según destaca el organismo hay tres tipos de notificación de incidentes previstos en el artículo 40 de la EECC: notificación de incidentes nacionales de los proveedores a las autoridades de seguridad nacional; de incidentes *ad hoc* entre las autoridades de seguridad nacional y Enisa; e informe resumido anual de las autoridades de seguridad nacional a la Comisión Europea y a Enisa.

Conducción autónoma e IA

La Agencia realizó un informe en profundidad, elaborado junto con el Centro Común de Investigación (JRC), analizando los ciberriesgos relacionados con la Inteligencia Artificial (IA) en vehículos autónomos y ofrece recomendaciones para mitigarlos. "Al eliminar la causa más común de accidentes de tráfico, el conductor humano, se espera que los vehículos autónomos reduzcan los accidentes y las muertes. Sin embargo, destaca que "los vehículos autónomos utilizan sistemas de IA, que emplean técnicas de aprendizaje automático", estos sistemas, "como todos los sistemas de TI, son vulnerables a ataques que podrían comprometer el correcto funcionamiento del vehículo". Entre sus recomendaciones está acometer evaluaciones de seguridad de los componentes de la IA, realizar procesos continuos de evaluación de riesgos, respaldados por inteligencia de amenazas, e impulsar por que el sector de automoción aumente su nivel de preparación y refuerce sus capacidades de respuesta a incidentes", resalta el documento.



Cinco informes para la regulación eIDAS

Enisa ha presentado su 'paquete' de cinco informes para impulsar la implementación de la regulación eIDAS y promover la adopción de servicios de identificación electrónica y de confianza. Enisa recordó que la iniciativa 'Sistema de identificación digital de la UE para transacciones en línea en toda Europa' impulsará la revisión del eIDAS y promoverá las identidades digitales para todos los europeos.

Cuatro de los informes sobre servicios de confianza constituyen una actualización de las directrices de Enisa para proveedores de servicios de confianza calificados y representan un conjunto de herramientas voluntarias diseñadas para ayudar a los proveedores de servicios de confianza a cumplir con eIDAS.

Certificación en ciberseguridad para 5G

Tras una solicitud de la Comisión Europea, Enisa procederá con la preparación del nuevo esquema de certificación de ciberseguridad candidato en 5G. Este paso es una continuación de la caja de herramientas de la UE para la seguridad 5G y se espera que mejore aún más la ciberprotección de estas redes, ya que contribuye a abordar ciertos riesgos, como parte de una estrategia más amplia de mitigación de riesgos. A tal efecto, un esquema de certificación de ciberseguridad en 5G se basará en las disposiciones ya disponibles mediante esquemas de certificación de ciberseguridad existentes, así como en la experiencia adquirida desde que la Agencia comenzó a participar en estos asuntos.

El SOC del futuro a tu alcance

Detección, prevención y automatización basada en IA

CORTEX® XDR™

Detección y respuesta extendida

- > x50 de reducción en el volumen de alertas

CORTEX XSOAR

Automatiza tus SecOps

- > 95% de tareas automatizadas

EXPANSE®

Reducción de superficie de ataque

- > Descubre, evalúa y mitiga exposiciones

paloaltonetworks.com/cortex

El FBI alertó de que el cibercrimen supuso en 2020 pérdidas en el país de más de 3.600 millones de euros

BIDEN podría implementar nuevos estándares de ciberseguridad para el software, además de apostar por una política ofensiva frente a sus adversarios

El nuevo mandatario de la **Casa Blanca**, **Joe Biden**, ha comenzado la legislatura con una fuerte apuesta por la ciberseguridad ante incidentes de extrema gravedad, como han sido las crisis desatadas por el ciberataques contra **SolarWinds**, a finales de 2020, con cerca de 15.000 organizaciones afectadas y las vulnerabilidades en Microsoft Exchange Server, que podrían haber impactado en 60.000 compañías facilitando la labor de ciberespionaje, según **Eset**, a una decena de grupos de ataques persistentes avanzados (APT).

Esta situación ha dado pie a que especialistas de la Administración, como **Jake Sullivan**, Asesor de Seguridad Nacional, hayan planteado la necesidad de incrementar las acciones ofensivas en el ciberespacio ante posibles atacantes, como Rusia. Su táctica, según publicó **The New York Times**, forma parte de una estrategia que permita marcar unas 'líneas rojas' y disuadir a otros países con intenciones 'ciberhostiles' ante el temor a represalias.

Medidas proactivas

Además, la Casa Blanca ha anunciado su intención de aprobar una orden ejecutiva que aliente a las compañías de software a mejorar la seguridad de sus productos y que trabajen con una cadena de suministro que tenga una higiene cibernética mínima. Algo que podría exigirse con esta nueva directiva que podría obligar a cumplir unos estándares de protección para el software, sobre todo en sus áreas más críticas. "Debemos asegurarnos de que las cadenas de suministro sean seguras y confiables", destacó Biden en febrero, tras firmar una

primera orden ejecutiva para mejorar su protección cibernética. Esta iniciativa, de hecho, fue bien acogida por el **Consejo de Industria y Tecnología de la Información**, del que forman parte muchas multi-

Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) en su respuesta a incidentes en todos los sectores de la industria, ampliando sus competencias a la monitorización de posibles vulnerabi-

lidades de los sistemas de control industrial. "Estos sistemas operan muchos componentes vitales de la infraestructura crítica de nuestra nación y permanecen bajo el ataque constante de los ciberdelincuentes y los actores del estado nacional. Un ejemplo lo tuvimos recientemente, cuando una instalación de tratamiento de agua de Florida fue atacada, así pues, estos ataques pueden tener consecuencias devastadoras en el

mundo real", destacó el impulsor de esta iniciativa que podría plasmarse en la Ley de Mejora de los Sistemas de Control Industrial del **Departamento de Seguridad Nacional**.

Ciberdefensa

El gobierno estadounidense también está trabajando en desarrollar nuevos requisitos de ciberseguridad que sean aplicables a los contratos de sistemas de armas. El organismo de auditoría del Pentágono (**GAO**), ha recomendado que el **Ejército**, la **Armada** y la **Infantería de Marina** "desarrollen una guía para los programas de adquisición sobre cómo incorporar requisitos de ciberseguridad, criterios de aceptación y procesos de verificación de sistemas de armas personalizados en los contratos". De cualquier forma, funcionarios del GAO reconocieron que la contratación "efectiva" de ciberseguridad es un desafío para los programas de adquisiciones y abogaron por "estandarizar los requisitos de



Foto: Adam Schultz

nacionales estadounidenses como **Apple** y **Zoom**, aunque también recordaron que esta apuesta debe combinarse con una financiación significativa en subvenciones a través del Departamento de Comercio.

La Casa Blanca también estaría contemplando implementar clasificaciones y estándares de ciberseguridad para el software de EE.UU., de forma similar al etiquetado que llevan los dispositivos de bajo consumo de la **Agencia de Protección Ambiental** y el **Departamento de Energía**, según explicó un alto funcionario en una conversación *off the record*. De hecho, en 2020, la Comisión Solarium ya recomendó al Congreso que se creara una **Autoridad Nacional de Certificación y Etiquetado de Ciberseguridad**, eso sí, siendo voluntario someterse a él.

Mayor peso de CISA

Entre otras iniciativas parlamentarias, se ha presentado una legislación bipartidista que busca centralizar el papel de la



jtsec

BEYOND IT SECURITY

LABORATORIO LÍDER en Evaluaciones LINCE



- Mejora la **CIBERSEGURIDAD** de tu **PRODUCTO TIC**



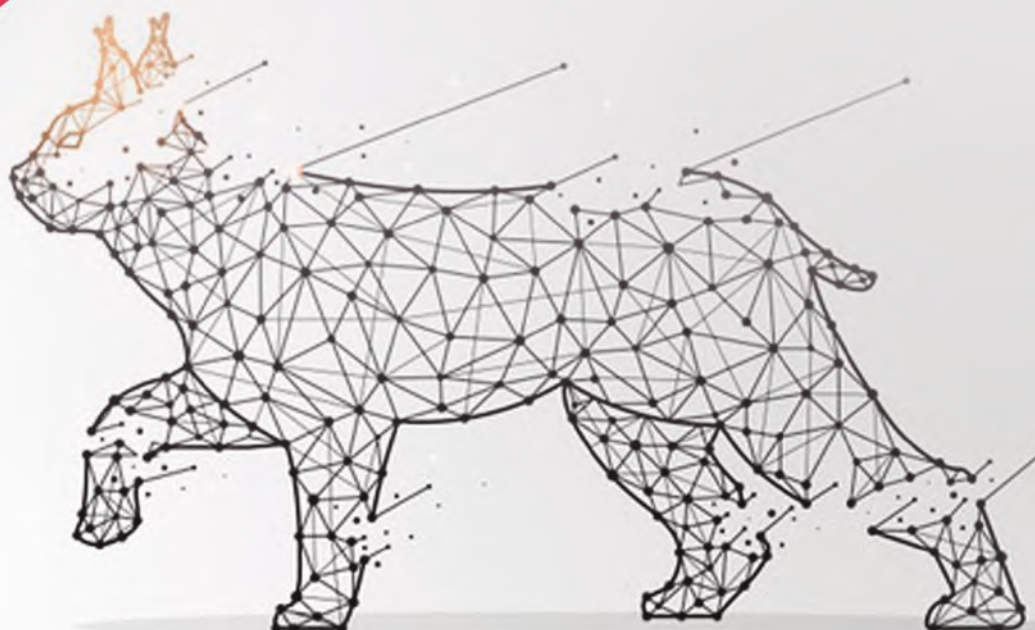
- **POSICIONA** tu producto **TIC** en la **ADMINISTRACIÓN PÚBLICA**



- Obtén un **CERTIFICADO** de ciberseguridad emitido por **CCN**



- Incluye tu producto en el **CATÁLOGO DE REFERENCIA NACIONAL** en ciberseguridad CPSTIC



Escanea este código y obtén un **10% DTO.** en tu **EVALUACIÓN LINCE**



ciberseguridad". No obstante, destacaron ser conscientes de que "es difícil y el departamento necesita comunicar mejor los requisitos de ciberprotección" para que los usuarios decidan si un riesgo de ciberseguridad es aceptable o no.

Por otro lado, el **FBI** también publicó en marzo su informe sobre el cibercrimen en 2020, en el

que se calcula que causó en el país unas pérdidas que rondaron los 3.600 millones de euros, un 20% más que el año anterior.

Pérdidas millonarias

El **Centro de Quejas de Delitos en Internet** del **FBI** recibió, de hecho, una media de más de 2.000 notificaciones de usuarios

por día hasta 2020 (frente a las 1.200 de 2019), relacionadas sobre todo con incidentes como el compromiso del correo-e empresarial (BEC), con unas pérdidas estimadas al año de 1.500 millones de euros, los ataques de *ransomware* (con 2.727 quejas y pérdidas de 24 millones de euros) y las estafas de soporte tecnológico. El caso más fla-

grante de los ataques BEC supuso el pago, tras ser estafada, de más de 50 millones de euros por parte de una empresa a una cuenta de Hong Kong.

El más grave de *ransomware* fue sufrido por **Universal Health Services**, un proveedor de dispositivos sanitarios, con unas pérdidas estimadas de 56 millones de euros.

EN BREVE

El CONGRESO de EE.UU. quiere sacar adelante más proyectos de ciberseguridad intentando superar los 316 de los últimos dos años

El **Congreso** está convencido de la necesidad de aprobar más y mejores normativas de ciberprotección y prueba de ello es el incremento de medidas presentadas para su aprobación. En total, se presentaron para votación 316 proyectos de legislaciones relacionadas con la ciberseguridad, entre 2019 y 2020, frente a los 22 de hace dos legislaturas. De ellos, 14 se convirtieron en ley, con nueve relacionados con la legislación sobre asignaciones o autorizaciones de agencias, en comparación con los 11 de la sesión anterior. Entre las normas aprobadas están desde recomendaciones de la **Comisión Solarium** para el ciberespacio, hasta la primera normativa para establecer unos estándares de ciberprotección en dispositivos IoT. El mayor grado de conciencia sobre los posibles peligros de las acciones en el ciberespacio de China, Irán, Corea del Norte y Rusia hizo que se aprobaran, por ambos partidos, hasta 48 normativas de política exterior en las que también estaban presentes temas de ciberseguridad.



El PENTÁGONO pondrá su programa de divulgación de vulnerabilidades a prueba —y a disposición— de sus contratistas

El **Pentágono** y, en general, la Administración estadounidense ha puesto en marcha en los últimos años diferentes programas para implementar programas de 'pago por vulnerabilidades' (*bug bounty*) entre organismos y compañías públicas.

La más reciente conocida ha sido promovida por el **Centro de Delitos Cibernéticos de Defensa** que, en colaboración con la Agencia de Seguridad de Contrainteligencia de Defensa, puso en abril a disposición de más de 20 contratistas del sector industrial las posibilidades de probar su seguridad.

El **Cyber Crime Center** del **DOD** ya alberga un programa voluntario de ciberseguridad con un entorno colaborativo para compartir información que incluye a más de 720 empresas, según el **Instituto de Ingeniería de Software** de **Carnegie Mellon**, que realizó un estudio de viabilidad sobre la expansión del programa a otros departamentos. Para comprobar su eficacia el Instituto ofrecerá su 'Vulnerability Reporting Management Network', a través del que espera obtener "información valiosa sobre la seguridad del sector".



INTEL se asocia con DARPA para desarrollar cifrado totalmente homomórfico

El fabricante de chips, **Intel**, ha firmado un acuerdo con la **Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA)** para desarrollar el programa de Protección de Datos en Entornos Virtuales (DPRIVE). Tiene como objetivo desarrollar "un acelerador para cifrado totalmente homomórfico (FHE)" que permita aplicarlo a la nube que **Microsoft** está desarrollando para el Pentágono en el 'programa JEDI'. "El cifrado totalmente homomórfico sigue siendo el santo grial en la búsqueda de mantener la seguridad de los datos mientras están en uso. A pesar de los fuertes avances en entornos de ejecución confiables y otras tecnologías informáticas confidenciales para proteger los datos en reposo y en tránsito, los datos no se cifran durante el cálculo, lo que abre las posibilidades de la Darpa".

Esta modalidad de cifrado permite a los usuarios realizar cálculos sobre datos siempre cifrados o criptogramas, lo que reduce el potencial de ciberamenazas. Fruto de esta colaboración Intel y Microsoft trabajarán para desarrollar estándares internacionales para FHE.



La NSA publica una guía sobre la adopción de la seguridad Zero Trust

La **Agencia de Seguridad Nacional** de EE UU. (**NSA**) ha publicado una guía sobre cómo los profesionales pueden aplicar el modelo de seguridad Zero Trust para proteger las redes empresariales y los datos confidenciales. Titulada 'Adopción de un modelo de seguridad de confianza cero', en ella se destacan los beneficios y desafíos de este modelo de seguridad y se ofrecen recomendaciones sobre la implementación de confianza cero en las redes existentes.

"Los sistemas que se diseñan utilizando principios de Confianza Cero deben estar mejor posicionados para abordar las amenazas existentes, pero la transición a un sistema de este tipo requiere una planificación cuidadosa para evitar debilitar la postura de seguridad en el camino. La NSA continúa monitorizando las tecnologías que pueden contribuir a una solución de Confianza Cero y proporcionará orientación adicional según se justifique", destacan desde el organismo. Eso sí, la NSA también recuerda que implementar Zero Trust requiere tiempo y esfuerzo.





Soluciones de Seguridad de Negocio

La ciberseguridad ya no es una opción. La superficie de exposición es cada vez más grande, y las amenazas mayores y más sofisticadas. Por ello, en PwC disponemos de servicios profesionales adaptados a nuestros clientes y su negocio, para acompañarles en la gestión del riesgo tecnológico y de la ciberseguridad, en un mundo lleno de desafíos digitales.

www.pwc.es/bss



© 2020 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.

MACRON anuncia una nueva estrategia de ciberseguridad dedicando 1.039 millones de euros más para proteger FRANCIA e impulsar su ciberindustria

Francia redobla sus esfuerzos para luchar contra el cibercrimen fruto de su preocupación por ciberataques contra hospitales como los de Dax-Côte d'Argent y Villefranche-sur-Saône. Su presidente, **Emmanuel Macron** anunció en febrero un refuerzo a su estrategia de ciberseguridad con un presupuesto extra de 1.039 millones de euros (el Estado aportará 720 y los 319 restantes procederán del sector privado). Las aportaciones irán dirigidas al desarrollo de la oferta tecnológica (515 millones), el refuerzo de las sinergias (148 millones), el apoyo a la demanda de "soluciones de ciberseguridad" (176 millones) o a través de fondos propios estatales (200 millones). Su objetivo es contar con "sistemas mucho más robustos y mejorar sistemas de defensa al mismo tiempo". Es más, el presidente también propuso que cada programa digital que se acometa en el sector salud cuente, de forma sistemática, con una parte dedicada de entre el 5% y el 10% del total destinado a la seguridad digital.

Destacó, asimismo, la labor realizada por el ejecutivo hasta ahora y que, entre otros ejemplos, se plasman en la contratación, desde 2017, de más de 200 especialistas en este ámbito para luchar contra el cibercrimen a través de la **Agencia Nacional de Ciberseguridad (ANSSI)**, que cuenta con más de 550 agentes focalizados en dicho objetivo. El organismo, entre otras iniciativas, ya ha acompañado con auditorías de ciberseguridad a 110 hospitales franceses y con 11 de ellos se trabaja "en el día a día". También, recordó la importancia de la cooperación policial y judicial y destacó que es clave "ir más lejos y más rápido, para estar a la vanguardia".

Además, el plan tendrá como finalidad incrementar la facturación del sector de ciberseguridad francés a 25.000 millones de euros en 2025 (frente a los 7.300 de 2019) y duplicar la participación de las exportaciones en esta facturación del 20% en 2019 al 40% de la facturación en cuatro años. Un reto que también supondrá dupli-



car los profesionales de ciberprotección del país, que podrían alcanzar los 75.000 para entonces respecto a los 37.000 actuales. El presidente también avanzó la necesidad de impulsar la cultura de ciberseguridad entre empresas de todos los tamaños pero "especialmente, entre las más pequeñas para permitirles optimizar la seguridad de sus redes".



Cybercampus

Asimismo resaltó, como ya informó **Revista SIC** en 2020, la importancia del 'Cyber Campus' que se está creando en el barrio de La Défense, en París, que será inaugurado en el segundo semestre de este año con más de 25.000 m² y capacidad para 1.000 expertos. Estas instalaciones forman parte de la apuesta del país por crear un ecosistema de ciberseguridad más fuerte, impulsando los vínculos entre la administración y la industria con el fin de reducir la participación de actores extranjeros que representan del 30% al 40% del mercado francés.

RESUMEN DE LOS MONITOS DE LA ESTRATEGIA CIBERNETICA NACIONAL (NUEVOS CREDITOS EXCLUYENDO MILITARES Y ENTRENAMIENTO)

en M€	Developper des solutions souveraines	Renforcer les synergies	Soutenir l'adoption de solutions cyber	Soutien en fonds propres	Total
Part publique	290	74	156	200*	720
Part privée	225	74	20	n.a.	>319
Financement	515	148	176	200	>1 039

* Montants prévisionnels

REINO UNIDO presenta su CONSEJO DE SEGURIDAD CIBERNÉTICA para supervisar los estándares del sector y facilitar el acceso profesional a él

El sector cibernético británico mueve unos 9.600 millones de euros anuales con un crecimiento continuo hace años.

Para garantizar su buena salud y calidad, el gobierno ha puesto en marcha, en marzo, el **Consejo de Seguridad Cibernética** que tiene como objetivo "alinear la industria con otras profesiones como el derecho, la medicina y la ingeniería". La idea, según explicaron desde el Departamento de asuntos digitales, es que establezca los conocimientos, las habilidades y la experiencia necesarios para diferentes trabajos de ciberseguridad y brinde la orientación necesaria a las personas que quieran trabajar en el sector.

También, defenderá la diversidad y la inclusión, impulsando los estándares y ayudando a la nación a reconstruirse mejor y de manera más segura". Además, está previsto que preste apoyo a la Estrategia



de Seguridad Cibernética nacional que cuenta con un presupuesto de 2.200 millones de euros.

Nuevo marco de identidad digital

El gobierno también presentó en febrero un borrador como punto de partida de una propuesta para desarrollar el llamado 'mercado de la identidad digital', con el objetivo hacer más fácil la identificación y autenticación en servicios digitales que permita usar, también pasaportes o identificaciones bancarias. Elaborado por el **Ministerio de Asuntos Digitales**, en colaboración con el sector privado, el marco ofrece recomendaciones que las empresas deben seguir, incluidos los principios, políticas, procedimientos y estándares que rigen el uso de la identidad digital.



La ISA GLOBAL CYBERSECURITY ALLIANCE aumenta sus esfuerzos para implementar la ISA/IEC 62443

La **ISA Global Cybersecurity Alliance (ISAGCA)**, creada por la Sociedad Internacional de Automatización (ISA), está trabajando para promover la inclusión de la serie ISA/IEC 62443

rencias cruzadas auditable completamente detallada que mapee los estándares ISA/IEC 62443 a otros estándares de ciberseguridad en múltiples industrias. En concreto, la Alianza quiere

comenzar a facilitar análisis comparativos que identifiquen las implicaciones de seleccionar y aplicar la serie de estándares ISA/IEC

ISA 99 / IEC 62443 Standards



de estándares de ciberseguridad en las políticas globales que pretenden mejorar la ciberprotección de las infraestructuras críticas y publicar una guía de refe-

62443 y ayudar a reducir el esfuerzo que precisa cumplir con los estándares y políticas de ciberseguridad, según destacó la asociación en un comunicado.

Proteja su organización con inteligencia de seguridad de manera gratuita.

Acelere la clasificación de alertas, priorice las vulnerabilidades e investigue las amenazas emergentes con inteligencia de seguridad en tiempo real.

Recorded Future Express es una extensión de navegador que ofrece inteligencia en tiempo real a través de calificaciones de riesgo y contexto en direcciones IP, dominios, hashes, URLs, y CVEs.

Con Recorded Future Express, puede priorizar instantáneamente las alertas del SIEM, detectar, y prevenir el phishing y enriquecer los IOCs en cualquier lugar.

Descarge Express gratuitamente en:
recordedfuture.com/express

España ya cuenta en él con más de medio centenar de organizaciones e instituciones públicas registradas

La COMISIÓN EUROPEA crea el 'Atlas de la Ciberseguridad' para identificar e impulsar la colaboración entre empresas, instituciones y expertos

La **Comisión Europea** ha puesto en marcha una gran plataforma de gestión del conocimiento —en cybersecurity-atlas.ec.europa.eu— con el fin de 'mapear', clasificar, visualizar y fomentar la colaboración entre las empresas, las instituciones públicas y los profesionales y expertos europeos del sector. Bajo el nombre de **European Cybersecurity Atlas**, la iniciativa tiene entre sus objetivos facilitar el establecimiento de una comunidad en la que sea posible identificar, por ejemplo, con quién colaborar en proyectos futuros en cualquier país de la UE, así como las áreas de especialización de las organizaciones registradas, a través de un mapa interactivo.

Así, todos aquellos que se adhieran, tendrán la oportunidad de ampliar su red y mejorar su visibilidad e, incluso, podrán beneficiarse de información específica sobre próximas licitaciones y oportunidades de financiación a nivel nacional y de la UE, además de acceder a cursos y prácticas.

La plataforma ya cuenta con más de medio centenar de insti-



tuciones públicas y organizaciones presentes en España, como **ElevenPaths, Atos, GMV, Indra, Tecnalia, S21sec, S2 Grupo, Policía Nacional, Guardia Civil, el Mando Conjunto del ciberespacio (MCCE), el Incibe, la Agencia de Ciberseguridad de Cataluña,** y buen número de universidades como la **Autónoma de Madrid, Rey**

Juan Carlos, Castilla la Mancha, Cantabria, Málaga, etc.

La plataforma, que además servirá como herramienta de gestión del conocimiento para el **Centro Europeo de Competencia en Ciberseguridad**, con sede en Bucarest, también creará una taxonomía común que alinee las definiciones y terminologías de ciberseguridad

para permitir la categorización de las instituciones y la experiencia existentes en toda Europa. “Un paso crucial para facilitar la colaboración y fomentar el establecimiento del Centro y su Red de Competencia”, destaca la Comisión.

Con la plataforma, también se pretende “mejorar la coordinación de los esfuerzos europeos en I+D en este campo, contribuir a dar forma a las orientaciones estratégicas de los programas de la UE, la tecnología y las capacidades en ciberseguridad, así como proporcionar información relevante para la formulación de políticas de ciberseguridad en Europa”. Además, quiere servir como referencia a la Comisión para la gestión de programas de trabajo y asignación de fondos, así como en el fomento de la diversidad y la inclusión. De hecho, cabe destacar en este último aspecto la integración en esta plataforma del registro de mujeres europeas expertas en ciberseguridad de la iniciativa **Women4Cyber** (del que SIC ya se hizo eco en su número 141).

La nueva normativa de la UE sobre pruebas electrónicas (e-Evidence) para investigar delitos transfronterizos, aún en fase de negociación pero más cerca de ser aprobada

Más de la mitad de todas las investigaciones criminales incluyen una solicitud transfronteriza para acceder a pruebas electrónicas, como mensajes de texto, correos electrónicos o aplicaciones de mensajería. Por ello, la **Comisión Europea** lleva trabajando desde hace años en aprobar una normativa, conocida como e-Evidence, que facilite y agilice el acceso de las autoridades policiales y judiciales a las pruebas electrónicas para detener y condenar a delincuentes y terroristas. Un proceso que se ha dilatado por la falta de acuerdo entre el Parlamento y el Consejo de los límites y procesos que deberían aprobarse y en cuyo debate han participado los Estados miembros y la industria.

El último paso hacia su aprobación se ha producido a finales del 2020, cuando la **Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE)** del **Parlamento Europeo** publicó su esperado Informe sobre la propuesta de reglamento sobre las Órdenes europeas de producción y conservación de pruebas electrónicas en materia penal. Un documento que permitirá acometer la aprobación

de esta nueva normativa, tan esperada por las Fuerzas y Cuerpos de Seguridad, y en el que se da respuesta a preocupaciones planteadas por los participantes en ella respecto a cómo garantizar el estado de derecho, la protección de los derechos fundamentales y las cargas sobre los proveedores de servicios frente a innumerables órdenes de acceso a datos por parte de una miríada de autoridades policiales y judiciales en todos los Estados miembros de la UE.

Por ejemplo, el informe recomienda una forma de trabajar para que las autoridades del ‘estado de ejecución’ se involucren cuando una autoridad judicial o policial extranjera emita una solicitud de acceso a datos al proveedor de servicios. El documento también pide a la Comisión establecer “un sistema de intercambio europeo común con canales seguros para el manejo de la comunicación, autenticación y transmisión transfronterizas



autorizadas” de las órdenes de acceso a datos y los datos solicitados entre las autoridades competentes y los proveedores de servicios.

Además, se estipula que, en caso de que la orden de acceso a los datos esté

incompleta o no contenga información suficiente, el proveedor de servicios podrá solicitar una aclaración a la autoridad de emisión, así como a la autoridad de ejecución. El plazo para cumplir con las órdenes de acceso a datos extranjeros, en principio, debería ser de 10 días y en casos de emergencia de 16 horas, según la recomendación de la Comisión de Justicia.

Eso sí, los participantes de las conversaciones a puerta cerrada entre el Parlamento y la Comisión consideran que la postura de ambas instituciones están alejadas, ya que los eurodiputados quieren “soluciones jurídicamente sólidas para obtener pruebas electrónicas en casos transfronterizos”.



SU SOCIO DE CONFIANZA EN CIBERSEGURIDAD

spain@advantio.com

+34 91 418 58 17

[ADVANTIO.COM/ES](https://advantio.com/es)

Aborde su Estrategia en Seguridad Informática con un Socio de Confianza

Servicio global con profesionalidad y coherencia. Respalados por una década de experiencia, ayudamos a bancos, proveedores de servicios de pago y comerciantes con sus desafíos en materia de ciberseguridad.

Experiencia QPA real en certificaciones PCI PIN y P2PE así como en certificaciones PCI 3DS



PCI 3DS



PCI PIN



PCI P2PE



PEN TESTING

“Advantio nos ha proporcionado unos servicios ejemplares de consultoría en ciberseguridad durante más de 8 años, especialmente en el ámbito de PCI DSS. Ha superado nuestras expectativas y nos ha impresionado con un enfoque proactivo y minucioso para nuestros desafíos de ciberseguridad. Esperamos que nuestro negocio siga creciendo con el apoyo de Advantio.”

ESTEN HOEL, SVP Quality & Security  **basefarm**

Otros Servicios

RGPD	ISO 27001 / 22301	Análisis de Malware
CMMI	Pruebas de Penetración	Seguridad en la Nube
SOC2	Oficina de Seguridad	Servicios Administrados

Acreditaciones PCI

PCI QSA	PCI QPA	PCI ASV	P2PE QSA
PCI 3DS	PA-QSA	PCI TSP	P2PE PA-QSA



10 AÑOS DE EXPERIENCIA



SIEMPRE A TIEMPO Y DENTRO DE PRESUPUESTO



13 UBICACIONES
14 IDIOMAS

Se interesó de forma especial por los equipos específicos de la unidad y por cómo se anticipan a los posibles ciberincidentes

El REY visita el MANDO CONJUNTO DEL CIBERESPACIO comprobando el alto nivel de preparación del que es considerado el CERT de Defensa por el RD 43/2021

El Rey Felipe VI visitó en febrero el Mando Conjunto del Ciberespacio (MCCE), acompañado del jefe del Estado Mayor de la Defensa, almirante general Teodoro Esteban López Calderón y el comandante del MCCE, general de división del Ejército del Aire, Rafael García Hernández. Se trata de su primera visita a las nuevas instalaciones del mando cibernético. En ella presenciaron un ejercicio a nivel nacional de verificación, validación y confirmación FMN (Federated Mission Network, Redes de Misión Federadas) con el doble objetivo de adiestrar y actualizar a las Fuerzas Armadas en ellas y de comprobar su alistamiento ante eventuales contribuciones a la estructura de la OTAN.

En uno de los edificios anexos, el Rey también tuvo la oportunidad de visitar una exposición estática de un dron y de un kit Desplegable de



Fuente: Casa Real

Ciberdefensa (CDK), que tiene la capacidad de monitorización de sistemas, gestión de incidentes, análisis forense digital y comunicaciones seguras. Este sistema está probado y validado

en operaciones reales y actualmente está desplegado en el Hospital Central de la Defensa Gómez Ulla, participando en la Operación Misión Baluarte.

El recorrido por el MCCE finalizó con

la visita al Centro de Operaciones de Seguridad que tiene como misión la monitorización de sistemas, la gestión de incidentes y la coordinación de los Centros de Operaciones de

Seguridad del Ministerio de Defensa, todo ello operado las 24 horas al día. Y, posteriormente, con un encuentro en el Centro de Multiconferencias con el personal del MCCE. "Su Majestad mostró mucho interés por cómo funciona el Centro realizando preguntas que tenía sobre él

y su funcionamiento" destacaron a Revista SIC fuentes del Mando que explicaron que, durante toda la visita, el Monarca mostró su interés por el que es uno de los departamentos más tecnológicos del Ministerio de Defensa y que ha sido reconocido como su CERT en el RD 43/2021.

El CONGRESO DE LOS DIPUTADOS destinará casi 700.000 euros anuales para contar con servicios de SOC que protejan sus sistemas y dispositivos

El Congreso destinará cerca de 700.000 euros al año para contar con un servicio de Centro de Operaciones de Ciberseguridad 24x7 para proteger sus redes y dispositivos. Para ello, la Cámara Baja publicó en febrero un concurso público cuya adjudicación se dará a conocer en primavera, en la que se contempla una protección no sólo de la información sino también, de forma proactiva, de cualquier posible amenaza para la institución que se pueda detectar a través de redes sociales, foros e internet profunda.

"Dada la naturaleza evolutiva de las amenazas a la seguridad de la información y del propio Sistema Informático del Congreso de los Diputados, el adjudicatario se compromete a colaborar, durante la duración del contrato, en todas las integraciones y reconfiguraciones necesarias del sistema ofertado para incorporar todos aquellos elementos y tecnologías en relación con la seguridad de la información que el Congreso de los Diputados estime necesario agregar a sus sistemas a lo largo del tiempo", destaca el pliego del concurso.

El contrato quedó listo para adjudicación el 29 de marzo, cuando se cerró la presentación de ofertas, con un presupuesto máximo de 2,7 millones de euros (689.438 euros al año, impuestos incluidos), teniendo el contrato una duración de

agosto de 2021 a julio de 2025, pudiendo prorrogarse por otro año más.

El concurso busca una empresa que ofrezca una solución 'llave en mano', por lo que los proveedores de servicios de ciberprotección que se presenten deberán "proveer, instalar y configurar previamente la infraestructura informática necesaria". Además, deberá tener capacidad para "operar, configurar, administrar y dar soporte a todos los dispositivos y al software asociado, así como gestionar y dar solución a los incidentes de seguridad que se puedan presentar".

Por ello, se pide que el licitador cuente con un SOC, con todas las capacidades necesarias para la prestación del servicio, así como elaborar informes tanto sobre los incidentes registrados, clasificados por tipologías y nivel de gravedad, como de las "vulnerabilidades encontradas" y de las propuestas para corregir éstas.

Así pues, se busca que la empresa adjudicataria sea capaz de ofrecer una protección perimetral de red, los sistemas controladores de



entrega de aplicaciones, la monitorización y gestión de eventos, además de contar con capacidad de respuesta ante incidentes, entre otros aspectos. También, deberá ayudar a poder implementar un sistema de gestión de la seguridad

de la información para el cumplimiento normativo relativo al Esquema Nacional de Seguridad (ENS), la adecuación de los sistemas de la Cámara al Reglamento General de Protección de Datos y a cualquier otra norma que deba cumplir en el ámbito digital.

Penalizaciones

Como curiosidad, el contrato prevé penalizaciones por incumplimiento del nivel de servicio. En función de la severidad de la incidencia (en una escala de tres), el carácter del incumplimiento (leve o grave) y el tiempo de respuesta (entre dos horas y media y ocho horas y media) que ofrezca el proveedor, éste verá descontada su facturación mensual entre un 1% y un 4%.

¿Puede hacer esto tu SIEM?

Detecta de forma instantánea el
alcance completo de un ataque

Con NetWitness® Platform



Learn more at rsa.com/netwitness

Su objetivo es mejorar las capacidades de los órganos del Ministerio para detectar, prevenir y perseguirlo

INTERIOR aprueba un plan estratégico, dotado con un millón de euros, para luchar contra el cibercrimen

Como avanzó SIC en la portada de su anterior edición, el cibercrimen está experimentando un auge inusitado aprovechando la desbocada apuesta de las empresas por la transformación digital y por la fragilidad derivada del trabajo en remoto por la pandemia. Sin embargo, los medios disponibles para luchar contra él por parte de la Administración no parecen ser suficientes para afrontar este reto nada trivial. Prueba de ello es que ante estos acontecimientos países como Francia han decidido aprobar un presupuesto adicional de 1.000 millones de euros extras para ciberprotección, en tanto que la cifra de España para tal menester palidece por su modestia: un millón de euros, anunciados en marzo pasado por el titular del **Ministerio del Interior, Fernando Grande-Marlaska**,

con la denominación "Plan Estratégico para reforzar la lucha contra la ciberriminalidad".

El objetivo es potenciar las capacidades para detectar, prevenir y perseguir esta modalidad delictiva y generar un nuevo impulso operativo que garantice la protección de los derechos y libertades y la seguridad ciudadana.



Cuatro meses de plazo

Diseñado por la Secretaría de Estado de Seguridad, la iniciativa ha puesto el foco en la prevención; en la

cooperación entre las diferentes Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y los operadores jurídicos; en la dotación de capacidades suficientes y adecuadas para articular respuestas adaptadas a las diferentes modalidades delictivas; en la cola-

boración con la industria y los operadores relevantes en materia de ciberseguridad en el sector público y privado; y en el respeto escrupuloso a la libertad, a la privacidad y demás derechos fundamentales.

Para la consecución de estos objetivos, el plan contempla cuarenta y nueve líneas de acción concretas que se articulan en torno a seis ejes estratégicos: cultura de prevención de la cibercriminalidad, potenciación de capacidades, generación de ciberinteligencia, coordinación nacional y cooperación internacional, generación de un marco normativo adecuado y colaboración público-privada.

Tras su puesta en marcha, todos los centros directivos y organismos del Ministerio del Interior con competencias en materia de ciberdelincuencia disponen de cuatro meses de plazo para presentar sus correspondientes planes de acción operativos.

Las medidas y actuaciones contempladas en el Plan contarán con una dotación económica de un millón de euros para 2021.

El INCIBE gestionó un 21% más de incidentes en 2020, y canalizará propuestas para fortalecer el sector dentro del Plan de Recuperación del Gobierno

El **Instituto Nacional de Ciberseguridad (Incibe)**, a través de su Centro de Respuesta a Incidentes de Seguridad, gestionó el año pasado un total de 133.155 incidentes de ciberseguridad, un 21% más que el anterior. Asimismo, será el encargado de recoger las solicitudes de la consulta lanzada por el Gobierno, para identificar propuestas de fortalecimiento de las capacidades de ciberseguridad de las pymes y el impulso a la industria del sector, en el marco del Plan de Recuperación.

Según datos del Instituto, de los más de 130.000 ciberincidentes gestionados, 106.466 hacen referencia a ciudadanos y empresas, 1.190 a operadores estratégicos y 25.499 a la Red Académica y de Investigación española (**RedIRIS**). De ellos, el 35,22% correspondió a *malware* y el 32,02% a cualquier tipo de fraude, seguido de

sistemas vulnerables, con un 17,39%.

Se trata de una cifra con un incremento notable respecto al año anterior, cuando el Instituto reportó la detección de 107.397 incidentes, lo que supone que han crecido un 21%, ya sea por mejorar las capacidades del Incibe o, también, por una mayor actividad delictiva. Además, a través de la Línea de Ayuda en Ciberseguridad (017), la institución atendió 47.503 consultas, 8.297 a través de correo electrónico, en 2020.

Plan de Recuperación

El **Ministerio de Asuntos Económicos y Transformación Digital** ha puesto en marcha una consulta en el marco del Plan de Recuperación, Transformación y Resiliencia y en la agenda España Digital 2025, que tiene a la ciberseguridad como uno de sus diez ejes estratégicos.



Convocatoria para presentación de Manifestaciones de Interés

¿Tienes una **idea** para fortalecer las capacidades de **ciberseguridad** de las **pymes**?

¿Quieres **impulsar** a la **industria** del sector?

Haznos llegar tus propuestas y forma parte del cambio

Fecha límite: 21/04/2021 - 19:00h.

Más info en: <https://forma.administracionelectronica.gob.es/forma/oper/corp/5450uW9y>

incibe

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Las solicitudes se realizan a través del Incibe y en ellas se valorarán las propuestas que apuesten por "la dinamización y el impulso de las empresas españolas de ciberseguridad mediante el emprendimiento, la internacionalización, la mejora de las capacidades de I+D+i, la identificación y generación del talento o el desarrollo de servicios y soluciones competitivas que respondan a las crecientes necesidades de prevención, protección y respuesta a incidentes de ciberseguridad".

Las solicitudes están abiertas hasta el 21 de abril y pueden consultarse en la página web ministerial.

Código de Derecho de la ciberprotección

Por otro lado, a finales de febrero, el Incibe publicó en el BOE una nueva edición del compendio denominado 'Código de Derecho de Ciberseguridad', con casi 1.150 páginas y la inclusión de normativas aprobadas en el último semestre, entre ellas, el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, entre otras.

SPAM PARA PICAR



#CIBERCUIDADO

Ciberseguridad, Ciberinteligencia, Red Team

www.tarlogic.com

GOOGLE opta por Málaga para establecer en Europa un Centro de Excelencia para la Ciberseguridad

Con el objetivo de apoyar la transformación digital en España, Google anunció recientemente la inversión de más 540 millones de euros en cinco años con un conjunto de acciones que incluyen el establecimiento de la primera Región Cloud de Google en nuestro país, anunciando la colaboración con Telefónica y el primer cable submarino privado de Google para conectar nuestro país con Estados Unidos y Reino Unido.



conferencias, talleres y mentorías, además de investigación y desarrollo de producto, uno de los grandes retos asociados a la transformación digital.

Igualmente, incluirá la creación de un centro de excelencia para la ciberseguridad en Málaga capital, en un espacio de 2.500 metros cuadrados en el que se ofrecerá formación,

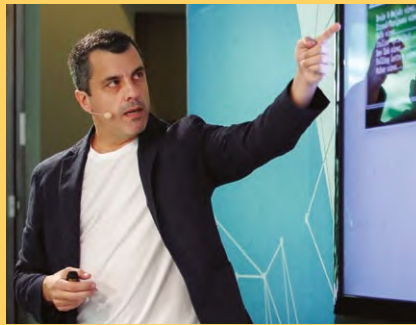
Bernardo Quintero, Security Engineer Manager en Google

“Este nuevo centro nace con el objetivo de abordar la ciberseguridad de una forma amplia y transversal, así que va a tocar las diferentes aristas y con diferentes niveles de profundidad”

– Desde que en 2012 Google se hiciera con los activos de la empresa española VirusTotal, la ciberseguridad ha venido adquiriendo una gran relevancia en su contribución al afianzamiento de la sociedad digital. ¿Por qué Google ha decidido que su ubicación física, en Málaga, sea el lugar elegido para la instalación de un centro de ciberseguridad en el ámbito español?

– La elección de Málaga es un paso natural si observamos la trayectoria seguida durante estos años. Como consecuencia de la adquisición, ya configuramos una primera y pequeña oficina de Google en Málaga para hospedar al equipo de VirusTotal, por aquel entonces con tan sólo seis ingenieros. Tras cuatro años en Google, donde conseguimos doblar las métricas año tras año, nos convertimos en el primer equipo de ciberseguridad que se trasladaba a X, los laboratorios de Google donde se llevan a cabo los proyectos más disruptivos de la compañía. El objetivo era estudiar el estado del arte de la ciberseguridad y proponer soluciones que supusieran un cambio de paradigma, lo que se viene a llamar un “moonshot”. Durante el periodo en X el equipo de Málaga siguió creciendo junto a otro en Mountain View, lo que finalmente daría lugar a Chronicle, la primera empresa de ciberseguridad de Alphabet. Ya durante ese periodo en X, y nuestra posterior graduación como Chronicle, vimos la necesidad de formar talento especializado en ciberseguridad para escalar el equipo local, comenzando una serie de colaboraciones con la Universidad de Málaga para la impartición de cursos de experto. En 2019 se anunció que Chronicle se incorporaba a Google Cloud para potenciar la seguridad en la nube, para entonces ya contábamos con más de 35 ingenieros especializados trabajando en el equipo de Málaga y todo un plan en marcha para seguir aumentando la cantera de talento y escalando el proyecto.

Si a todo lo anterior le sumamos las propias características de Málaga, una ciudad con buenas conexiones nacionales e internacionales, un ecosistema de startups vibrante e incubadoras y aceleradoras de empresas que llevan cultivando el tejido tecnológico mucho tiempo, el Parque Tecnológico de Andalucía, numerosos proyectos para convertir a la ciudad en una smart city, etc., pues la verdad es que se presen-



taba como un lugar idóneo para hospedar este Centro de Excelencia para la Ciberseguridad.

– El recinto del centro que será habilitado se encuentra en Málaga ciudad. ¿Cabe pensar que la cuarentena de trabajadores que, grosso modo, integran la plantilla de VirusTotal seguirán en la nueva sede y que incorporarán a más talento y personal especialistas?

– Sí, el plan pasa por continuar nuestro crecimiento paulatinamente. Este año, pese a las circunstancias especiales ocasionadas por la pandemia, seguiremos aumentando la plantilla en Málaga. La apertura del nuevo centro está prevista para principios de 2023, momento en el que iniciaremos una serie de programas que también aumentará las oportunidades de incorporar más talento al equipo. Nuestra estrategia pasa por seguir formando una cantera muy especializada en ciberseguridad, gracias a la colaboración con la Universidad de Málaga, y también captar talento experto foráneo. En el apartado de formación especializada cabe destacar el Curso de Experto Universitario en Ingeniería Inversa e Inteligencia Malware en estrecha colaboración con la Universidad de Málaga, del que impartimos la tercera edición este año. Además, este curso cuenta con una serie de becas para mujeres otorgadas por Google, lo que también nos permite fomentar la diversidad en el sector.

– Según lo previsto, además de las actividades –mayormente analítica–, que ya viene llevando a cabo VirusTotal, ¿qué nuevos ámbitos de especialización y orientaciones en investigación y

desarrollo de soluciones y productos cabe esperar que tendrá el citado centro?

– Este nuevo centro nace con el objetivo de abordar la ciberseguridad de una forma amplia y transversal, así que va a tocar las diferentes aristas y con diferentes niveles de profundidad. Desde el punto de vista de soluciones, como parte de Google Cloud, tenemos un portafolio que no deja de aumentar. Además de la mencionada VirusTotal –la mayor base de datos de ciberseguridad–, podemos encontrar soluciones como Security Command Center para la gestión integral de la seguridad en GCP, Chronicle como plataforma analítica cloud nativa, reCAPTCHA y Web Risk para la prevención de fraude online, o BeyondCorp para implantar modelos Zero Trust, entre otras.

Además, contaremos con la colaboración del resto de equipos de seguridad interna de Google y X. Así, por ejemplo, tendremos la oportunidad de disfrutar de charlas técnicas y talleres impartidos por parte del equipo Project Zero para analizar las últimas vulnerabilidades, conocer de la mano del Threat Analysis Group cuáles son los ataques más avanzados y cómo se encuentra el mapa de actores a nivel mundial, o abordar los últimos avances en criptografía cuántica de la mano de X. Por último, es importante también destacar la vertiente de educación y concienciación, con programas para llevar la ciberseguridad a usuarios y pymes, y el área de mentorización a nuevas startups de ciberseguridad.

– Dado que la inciberseguridad no entiende de fronteras, ¿vislumbran colaboraciones con las entidades y actores regionales, territoriales y continentales con foco en la ciberprotección?

– Este nuevo Centro de Excelencia para la Ciberseguridad nace para sumar a nivel global, en ese sentido vamos a buscar de forma activa colaboraciones tanto públicas como privadas que puedan potenciar los diferentes programas. Si bien esperamos que tenga un impacto muy directo a nivel local y regional, por una simple razón de cercanía física, esperamos mantener una colaboración muy estrecha con los diferentes actores en España y convertirnos en referencia para toda Europa.

Luis Fernández Delgado

La nueva dimensión de gestión de vulnerabilidades

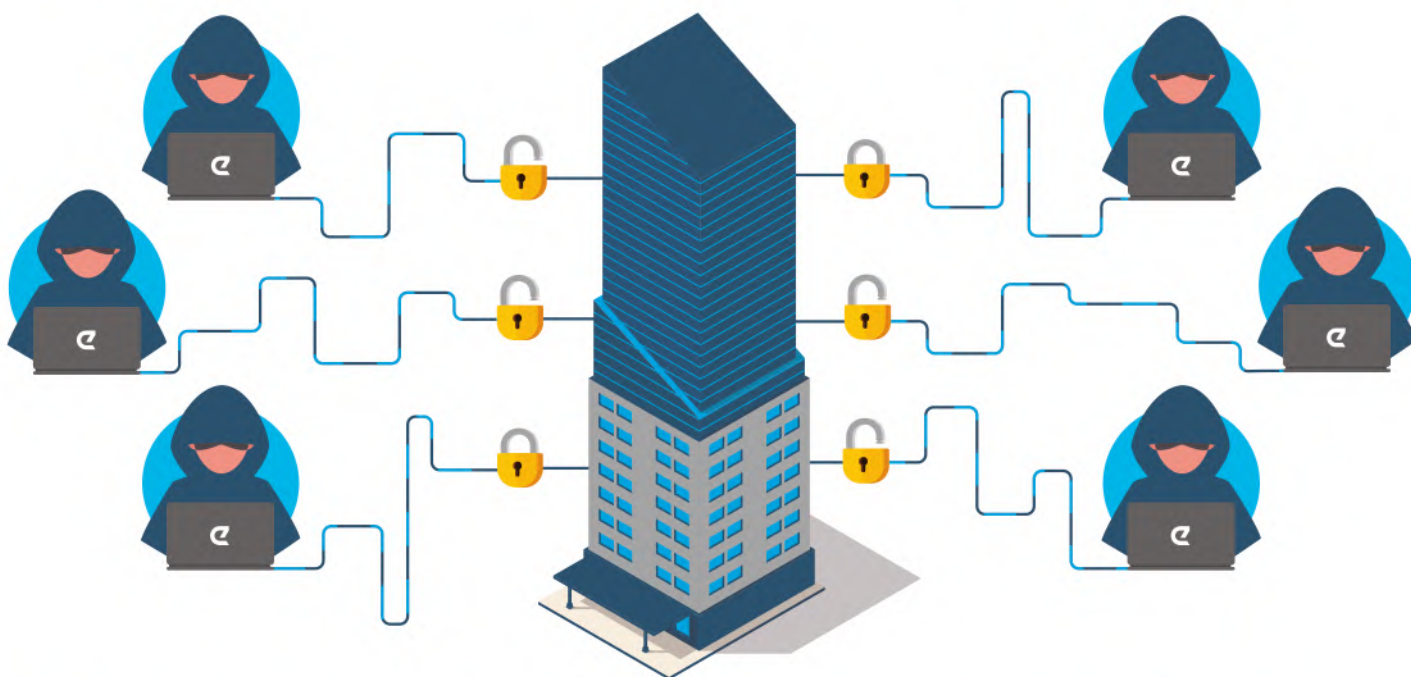
Optimice la seguridad de los activos en el tiempo.

Mejora la optimización de búsqueda de vulnerabilidades. Trabajo realizado desde una comunidad de hunters de confianza que solo cobra cuando encuentra una vulnerabilidad.

1 Validada frente a los CISOS y los responsables de la ciberseguridad.

2 Diseñada para ser utilizada por servicios gestionados.

3 Metodología utilizada desde hace 10 años en Estados Unidos.



Es la mejor herramienta para la detección de nuevas vulnerabilidades tras una auditoría de ciberseguridad inicial porque:



Optimiza el presupuesto. Solo consumirá presupuesto al sumar nuevas vulnerabilidades identificadas. Ideal para entornos con un nivel de seguridad alto con un coste de localización de vulnerabilidades de larga duración.



Permite ajustar y controlar totalmente los tiempos. Al regular el propio MSSP el número de investigadores participantes, se puede acelerar al máximo la búsqueda de nuevas vulnerabilidades.



Selecciona las vulnerabilidades reales de forma totalmente personalizada y súmalas a la capa de seguridad. Los programas son totalmente regulables para sólo obtener un tipo concreto de vulnerabilidad con el grado de criticidad que se quiera sumar a la capa de seguridad.



Los resultados son aplicables en tiempo real. En el momento en que una vulnerabilidad es encontrada, es reportada de inmediato.

Su vicepresidenta, Montserrat Martínez, destaca la necesidad de no asumir riesgos innecesarios con nuevas tecnologías

La COMISIÓN NACIONAL DEL MERCADO DE VALORES considera que invertir en ciberseguridad "es cuestión de supervivencia"

La **Comisión Nacional del Mercado de Valores (CNMV)** ha vuelto a recordar, de forma especial a las empresas, de la necesidad de contar con una ciberprotección adecuada para garantizar la continuidad del negocio. Aprovechando las jornadas sobre *fintech* y ciberseguridad organizadas por el organismo en marzo, tanto su Presidente, **Rodrigo Buenaventura**, en el acto inaugural, como su Vicepresidenta, **Montserrat Martínez**, en el de clausura, recordaron la importancia de dedicar

recursos a la ciberseguridad, ya que se considera que limitar y gestionar el riesgo tecnológico mediante la inversión es "una cuestión de supervivencia". Al respecto, Martínez recordó que "el 23% de las grandes empresas sufrió algún incidente de seguridad durante 2020 y la tendencia es creciente". De hecho, lamentó que "nos estamos acostumbrando



a noticias de ataques para acceder a datos o realizar algún tipo de fraude".

Además, reconoció que el reglamento de ciberseguridad de la UE **DORA**, (del que **SIC** ya informó en profundidad en su nº 134) requerirá de un importante esfuerzo por parte de las empresas, asegurando no obstante que traerá importantes beneficios.

Durante las jornadas los participantes también mostraron su preocupación por la digitalización en el ámbito financiero que, junto a notables beneficios en eficiencia y competitividad, supone nuevos riesgos que los supervisores deben monitorizar y comprender bien. "Se debe encontrar un buen equilibrio entre el fomento de la innovación y el uso de las nuevas tecnologías, con la necesidad de mantener la integridad del mercado de valores y la adecuada protección al inversor", añadió Martínez.

Por ello, se evidenció la importancia de colaborar entre los supervisores nacionales e internacionales y los distintos participantes del mercado, siendo muy cautos a la hora de apostar por tecnologías no reguladas. "Mientras no dispongamos de un marco claro, debemos preguntarnos siempre si tenemos la información suficiente, si entendemos el producto y los riesgos que se asumen con la

operación", subrayó recordando tecnologías en crecimiento como el uso masivo de datos, la nube o la IA.

Alertas continuas

La CNMV lleva varios años alertando de los diferentes ciberriesgos a los que se enfrentan las empresas reguladas a través de ataques como el de suplantación (*phishing*). Precisamente este marzo, la **Policía Nacional** investigó nuevos posibles casos de suplantación del organismo, haciéndose pasar por él por teléfono para recabar datos de inversores a los que defraudar. O, pocas semanas antes, de empresas consideradas 'chiringuitos financieros' que se hacen pasar por entidades autorizadas por la CNMV para confundir a los posibles inversores dando una sensación de legalidad. En 2018, también se detectó una campaña por correo-e, haciéndose pasar por la institución para captar datos personales.

El BANCO DE ESPAÑA alerta de las ciberamenazas en el sector financiero y pone en marcha el marco TIBER-ES para analizar su resiliencia

El **Banco de España (BdE)** publicó en marzo su 'Memoria de Supervisión 2020' en la que la institución, dirigida por **Pablo Hernández de Cos**, resume las funciones y la organización de la supervisión y de la vigilancia que realiza y, también, resalta el cibercrimen como uno de los principales riesgos del sector bancario en 2021. "La actividad supervisora de 2020 se ha visto muy condicionada por la crisis de la Covid-19. A las tareas de supervisión continuada habituales se han añadido otras, como el seguimiento de las medidas establecidas por el Gobierno, como las moratorias y los avales públicos, y del impacto de la pandemia sobre la calidad de los activos, los planes de contingencia con especial atención a la ciberseguridad y la continuidad de negocio, la liquidez y los efectos de la crisis sobre la actividad, la cuenta de resultados y la solvencia de las entidades".



Asimismo, el documento recuerda los importantes esfuerzos europeos hechos en este campo, ya que "en los últimos cinco años, la UE ha realizado un importante esfuerzo regulador encaminado a mejorar la resiliencia tecnológica y digital del sector financiero y destacan por su relevancia dos iniciativas regulatorias: las directrices de la **Autoridad Bancaria Europea** (EBA, por sus siglas en inglés), sobre gestión de los riesgos de las TIC y de seguridad, y la propuesta de reglamento de la UE **Digital Operational Resilience Act (DORA)**".

Arranca TIBER-ES

Además, la Comisión Ejecutiva del BdE ha aprobado "el diseño del marco local de las pruebas **TIBER-EU** del **Banco Central Europeo** (BCE)", con lo que las entidades financieras que

así lo soliciten podrán comprobar su nivel de ciberprotección a través de un análisis avanzado frente a él.

La 'autoridad propietaria' de TIBER-ES será el Banco de España, con la cooperación de la Comisión Nacional del Mercado de Valores (CNMV) y la **Dirección General de Seguros y Fondos de Pensiones (DGSyFP)**. Su objetivo es fortalecer la ciberresiliencia de las instituciones financieras españolas y, a pesar de que la versión europea permite utilizarlo en cualquier sector, el regulador español ha avanzado que en nuestro caso se limitará al entorno financiero. Así, próximamente se publicarán las guías para acceder a este tipo de pruebas a las que podrá acceder cualquier entidad y proveedor de ciberseguridad interesado para lo que se ha habilitado un correo-e de contacto: tiberes@bde.es.

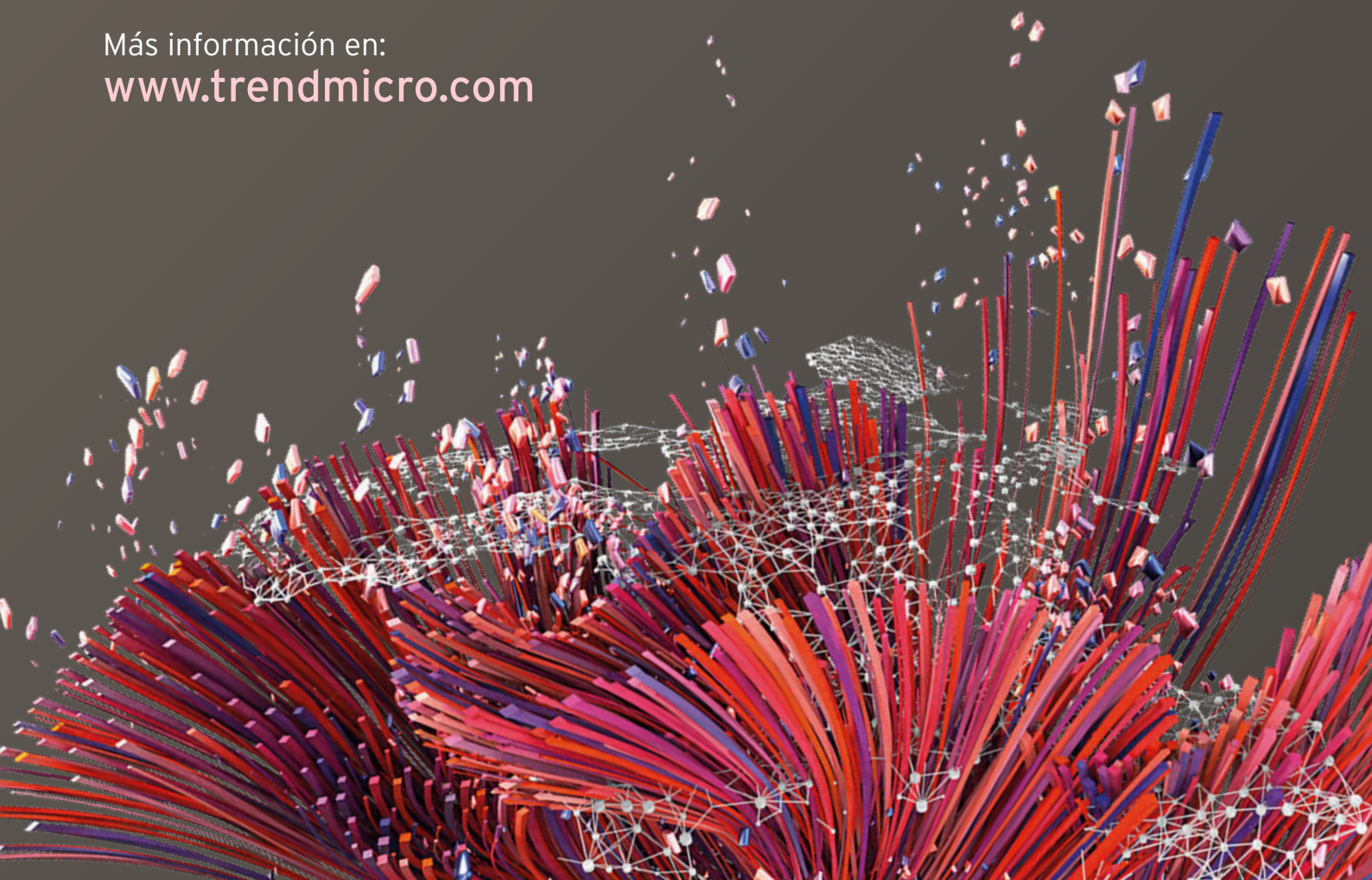


Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

Una plataforma especialmente diseñada para la
defensa contra amenazas que va más allá que
otras soluciones XDR

Más información en:
www.trendmicro.com





CAVILACIONES SEGURAS

Una breve introducción al proceso legislativo europeo de la mano de NIS2 y DORA

Los ejecutivos de multinacionales europeas y jefes de gobierno de distintos países nos recuerdan que, en estos tiempos de crisis, necesitamos “más Europa”: una receta para poder competir en un mundo multipolar con potencias cuyas poblaciones son más jóvenes que las nuestras y cuyas economías crecen más rápido. La estrategia de digitalización de la Unión Europea trae consigo potenciales mejoras legislativas relacionadas con la ciberseguridad. Por delante hay, sin embargo, un complejo camino que recorrer hasta que, finalmente, se conviertan en realidad. Hablemos de dos leyes en proceso de aprobación para mejorar la ciberseguridad en Europa: **NIS2** y **DORA**.

Para explicar el desafío desgranado, paso a paso, el proceso legislativo en la Unión Europea (UE): Las piezas más importantes del entramado legal europeo



“DORA es calificada como ‘lex specialis’, es decir, está alineada con la directiva NIS2 y tiene prioridad sobre ella. En otras palabras, DORA instrumenta la adopción de NIS2 en el sector financiero”

son los tratados, también llamada legislación primaria. Los tratados han de ser aprobados por todos los países de la UE y ratificados por sus respectivos parlamentos. El cuerpo legislativo que se crea a partir de los tratados se conoce como legislación secundaria e incluye regulaciones, directivas, decisiones, recomendaciones y opiniones legales.

Las regulaciones se aplican en todos los países de la Unión tan pronto como son aprobadas, sin necesidad de ser transpuestas a legislación nacional como suceden con las directivas.

El proceso legislativo ordinario en la UE comienza en la Comisión Europea, que elabora una propuesta legislativa. En esa propuesta, los ciudadanos, las empresas y las organizaciones presentes en la UE pueden participar en consultas públicas para hacer valer su opinión. Ese borrador es revisado por dos instituciones con igual peso: el **Parlamento Europeo**, elegido en las elecciones europeas por los ciudadanos de la Unión, y el **Consejo de Europa**, formado por representantes de los 27 gobiernos de la UE. Ambas instituciones tienen que estar de acuerdo con el texto legislativo a aprobar, bien en su primera o en su segunda lectura.

NIS2

En el campo de la ciberseguridad, el 6 de julio de 2016 el Parlamento Europeo aprobó la Directiva 2016/1148 sobre la **Seguridad en Redes y Sistemas de Información**, más conocida como la Directiva NIS. La primera ley europea sobre ciberseguridad. Todos los estados de la Unión estaban obligados a transponer esta directiva antes del 9 de mayo de 2018. En julio de 2020 se abrió un proceso de consulta para una directiva revisada (NIS2), en línea con la prioridad de la Comisión de preparar a Europa para la era digital.

En diciembre de 2020, la Comisión Europea presentó el borrador de NIS2, casualmente con elementos que, sólo unos meses más tarde, se han revelado esenciales para atravesar tiempos de pandemia. NIS2 añade más sectores críticos para la economía, como son los servicios logísticos, la gestión de residuos, la alimentación y los productos farmacéuticos. También otorga a los estados miembros la posibilidad de identificar como críticas a pequeñas entidades con riesgo alto de seguridad. Asimismo, elimina la distinción entre operadores de servicios esenciales y proveedores de servicios digitales, asumiendo así la imparable digitalización de toda nuestra sociedad.

NIS2 también refuerza la necesidad de las empresas de gestionar su riesgo tecnológico y es más precisa en el reporte de incidentes. Asimismo, propone la gestión del riesgo de la cadena de valor y de proveedores. La mejora en la gestión de vulnerabilidades y de incidentes de seguridad es también objetivo de NIS2.

DORA

En el mundo de las instituciones financieras, el 24 de septiembre de 2020 la Comisión Europea publicó el borrador de la **Regulación sobre Resiliencia Operacional para el sector de servicios financieros de la UE** (DORA). La primera buena noticia es que se trata de una regulación de aplicación directa y no de una directiva que requiere transposición en cada país de la Unión. La segunda buena noticia es que DORA es calificada como “lex specialis”, es decir, está alineada con la directiva NIS2 y tiene prioridad sobre ella. En otras palabras, DORA instrumenta la adopción de NIS2 en el sector financiero.

DORA profundiza en la necesidad de mejorar la gestión y el reporte de incidentes de seguridad, así como la gestión del riesgo tecnológico y su gobernanza. Un elemento esencial es la gestión de los proveedores críticos de servicios de información, como son los servicios de nube pública. DORA propone la supervisión de dichos proveedores por parte de las instituciones de supervisión europeas del sector financiero. Con estas medidas, el potencial de mejora de la resiliencia del sector financiero es patente.

Es evidente que NIS2 y DORA son, potencialmente, un gran paso hacia adelante. No obstante, el proceso de elaboración y, sobre todo, de aprobación de legislación europea, requiere de tantos acuerdos y compromisos que, en campos tan estratégicos como la ciberseguridad, sólo podremos evaluar el éxito de esta campaña cuando podamos leer el texto final de ambas leyes. Invito a todos los lectores a seguir en el sitio web de la Comisión Europea eur-lex.europa.eu el procedimiento 2020/0359/COD para NIS2 y el 2020/0266/COD para DORA. Actualmente ambos están en las discusiones de su primera lectura en Parlamento Europeo y el Consejo de Europa. Crucemos fuertemente los dedos.

Alberto Partida

Experto en Ciberseguridad

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



GMV amplía su presencia internacional abriendo sede en Bruselas

La multinacional tecnológica española **GMV** continua con su crecimiento internacional abriendo una sede en Bruselas para reforzar su negocio en la **UE** y ampliar

su presencia en siete Estados miembro, con lo que se convierte en el sexto grupo industrial que más empleo genera en el sector espacial en Europa.

Con esta nueva oficina, desde la que también se ofrecerán sus servicios de ciberseguridad, la com-



pañía reforzará “el diálogo con la UE y promoverá una comunicación continua y constructiva con las diversas instituciones y partes interesadas”. Además, abordará

“los importantes retos y oportunidades de las principales áreas de actividad de la compañía: espacio, defensa, TIC y transporte”.

La oficina de GMV trabajará en especial con la **Comisión Europea**, el **Consejo de la Unión Euro-**

pea, el **Parlamento Europeo** y las **Agencias de la UE**. También servirá de enlace con las Representaciones Permanentes nacionales ante la UE.

Cabe recordar que GMV contribuye de manera clave en programas emblemáticos de la UE, como Galileo, Copernicus, SST, Gvsatcom y Horizonte Europe, desempeñando una función primordial en la ejecución de las agendas de Seguridad y Defensa, particularmente respecto a los Fondos de Defensa Europeos.

Our value, our difference

One shared success

Cómo añadimos valor

Descubra nuestro valor añadido único y cómo puede ayudarle a acelerar su negocio

Nuestros servicios

Nuestra experiencia técnica, conocimiento de la industria y experiencia en el canal ayuda a nuestros socios a ganar y suministrar proyectos

Carrera en Westcon

Si está buscando un lugar dinámico para desarrollar su carrera, vea lo que tenemos para ofrecer.

Partners. Nosotros estamos a su lado.

addon

at&t
Your world. Delivered.

audiocodes

AVAYA

CERTES
NETWORKS

Check Point
SOFTWARE TECHNOLOGIES LTD.

cisco

cisco Meraki

ciena

CROWDSTRIKE

Extreme
networks

ff5

FIREM Q N

infovista

Jabra GN

JUNIPER
NETWORKS

Menlo
Security

Microsoft

Mitel

NETSCOUT

ORACLE

paloalto
NETWORKS

Ping
Identity

poly

ribbon
communications

RUCKUS
an ARUBA company

silver peak

SKYBOX
SECURITY

sumo logic

spectralink

Symantec
A Division of Broadcom

TITUS

Westcon-Comstor Spain



www.westconcomstor.com



+34 91 419 61 00



marketing.es@westcon.com



Westcon-Comstor Spain



@WestconEspana

La e-PRIVACY presenta un nuevo borrador con notables mejoras para aprobarse en 2021 en la EU

Tras más de cuatro años de negociaciones y nueve presidencias europeas, el reglamento sobre la vida privada y protección de los datos personales en las comunicaciones electrónicas, conocido como 'e-Privacy' (que reemplazará a la actual legislación, en vigor desde 2002), parece estar más cerca. En febrero, tras varias revisiones, el Consejo y el Parlamento de la UE presentaron una propuesta que se discutirá para su aprobación, que según sus impulsores supone un gran paso adelante.

El reglamento detalla las condiciones en las que los proveedores de servicios pueden tratar los datos de las comunicaciones electrónicas, incluyendo los transmitidos en el uso de servicios en línea, como los mensajes enviados en WhatsApp, Telegram y apps similares, así como las videollamadas en plataformas como Zoom y Skype.

Su objetivo es que las comuni-



caciones en línea tengan la misma protección de la privacidad que se otorga a las comunicaciones de telecomunicaciones tradicionales. Ahora, los 27 países de la UE iniciarán conversaciones con

los representantes del Parlamento Europeo aunque, según fuentes de Bruselas, no será un proceso sencillo por las fuertes discrepancias que ha habido hasta ahora: por ejemplo, países como Alemania o Austria se abstuvieron en la votación del texto propuesto por considerar que va contra algunos aspectos de la protección de datos.

Los operadores a favor

De cualquier forma, de momento, los operadores europeos sí han defendido el nuevo borrador a través de ETNO y GSMA que publicaron una declaración conjunta indicando que el sector se compromete plenamente con el principio de las co-

municaciones confidenciales y que apoya la ambición del continente de liderar la economía de los datos. De igual forma, organizaciones como la Junta Europea de Protección de Datos (EDPB) han acogido con satisfacción el texto, aunque también pidió aclarar algunos de sus puntos.

Importantes cambios

Entre las razones que han pospuesto su aprobación destaca que algunos países muestran su reticencia ante la posibilidad de que contradiga el RGPD, algo que se ha tenido muy en cuenta en esta propuesta en la que se subraya que, en caso de conflicto, se aplicará el segundo. Además, el documento introduce aspectos sustanciales como la aclaración de qué se considera metadatos cubiertos, incluyendo como tales los números de teléfono llamados y los sitios web visitados, así como la hora, la fecha y la duración cuando una persona hizo una llamada o visitó un sitio web.

También, permitirá a los países nombrar diferentes autoridades para hacer cumplir el RGPD y el Reglamento de privacidad electrónica, sin tener en cuenta los llamamientos anteriores de la EDPB de no dividir la supervisión de ambos instrumentos. De cualquier forma, la versión actual no incluye un mecanismo de ventanilla única similar al RGPD para las

nuevas reglas de ePrivacy. A nivel de la UE, el EDPB sería el organismo supervisor designado, aunque sus poderes serían más limitados que en el marco del RGPD.



Sanciones acordes al RGPD

Por el contrario, las sanciones y la responsabilidad siguen estando más alineadas con el RGPD, incluida la facultad de imponer multas administrativas de hasta 10 o 20 millones de euros, o si son más altas, del 2% o el 4% de la facturación anual mundial total del año financiero anterior, dependiendo de la disposición infringida.

Más respeto a los derechos humanos y a las normativas de privacidad, líneas rojas de las directrices del CONSEJO DE EUROPA para usar biometría facial

La Dirección General de Derechos Humanos y Estado de Derecho del Consejo de Europa ha emitido unas directrices sobre el reconocimiento facial en relación "con el tratamiento automático de datos personales", dentro del llamado 'Convenio 108'. En ellas, se destaca que imágenes "solo estarán cubiertas por la definición de datos biométricos cuando se procesen a través de un medio técnico específico que permita la identificación o autenticación única de una persona". A su vez, recuerdan que estas recomendaciones "cubren los usos de las tecnologías de reconocimiento facial, incluidas las tecnologías de reconocimiento facial en vivo", pero también destaca que "la legislación que autoriza una vigilancia amplia de las personas puede resultar contraria al derecho al respeto de la vida privada".

De hecho, plantea, entre otras cuestiones, que "la integración de tecnologías de reconocimiento facial a los sistemas de vigilancia



existentes plantea un grave riesgo para los derechos a la privacidad y la protección de los datos personales, así como a otros derechos fundamentales, ya que los usos de estas tecnologías no siempre requieren el conocimiento o la cooperación de las personas cuyos datos biométricos son procesados, como ocurre con las imágenes de Internet".

En definitiva, el documento destaca que "la legalidad del uso de tecnologías de reconocimiento facial se basará en los propósitos del procesamiento biométrico previstos por la ley y las salvaguardas necesarias que complementan la Convención 108". Además, recomienda invertir en certificar que los datos usados son los correctos, que son representativos y que los algoritmos empleados son eficientes para lo que se busca, así como usar herramientas con una alta fiabilidad y ser conscientes de que tiene que primar la transparencia y el respeto por la privacidad.

Nuevo marco ético de privacidad para reconocimiento automatizado del rostro

El departamento de videovigilancia de la British Security Industry Association (BSIA) presentó en febrero una guía de uso ético y legal para el reconocimiento facial automatizado (AFR), recomendada por la Organización para la Cooperación y el Desarrollo Económicos. En ella se describen unas pautas que las empresas deberían seguir para aplicar de forma responsable esta tecnología.

Entre otras recomendaciones, el marco destaca que para un uso ético de esta tecnología "no debe causar daño a ningún individuo, ya sea en su privacidad, dignidad o derechos humanos, además de contar con una evaluación de riesgos y datos previa para tener claro el impacto de su uso". Además, exige una información fiable, transparente y precisa al usuario, así como a los profesionales que trabajan con ella y determinar en qué "instancias" podría tener un impacto negativo para la persona.





Actualización completada



ZEROLYNX

Security and Intelligence



El segmento de la identidad protagoniza operaciones de calado y la histórica McAfee vende su negocio corporativo

En estos tiempos excepcionales que corren se calcula que el gasto en seguridad será más que notable en la mayoría de los presupuestos de TI de 2021 y que en un 37% de las organizaciones las mejoras en este aspecto será su principal prioridad de inversión en TI, según una encuesta de Syntax entre 500 ejecutivos del sector. Así las cosas, se estima que el sector de la ciberseguridad crezca este año en España entre un 9% y un 11%, según previsiones de SIC, con un volumen de negocio que superaría los 1.720 millones de euros. Estos halagüeños guarismos son consecuencia de la fuerte apuesta por la digitalización que gran parte de las compañías hicieron en 2020 para adaptarse a las nuevas circunstancias de la pandemia así como por apuntalar el trabajo en remoto.

El año ha comenzado, como vaticinaban los analistas, con un fuerte movimiento en el mercado de compra y venta de compañías de ciberseguridad, así como de alianzas, con operaciones millonarias como la adquisición de la compañía de protección de la identidad **Auth0** por casi 5.400 millones de euros por parte de **Okta**. Se trata de la tercera compra más importante de la historia de la ciberseguridad,

do. **James Legg**, Director Ejecutivo de **Thycotic**, ejercerá de Presidente. También, ha sido llamativa la compra de la *start up* **HubStor**, por parte de **Veritas**, con la intención de integrar su tecnología y capacidades de respaldo como servicio en su plataforma de servicios de datos empresariales. **Varonis** se hizo con **Polyrize**, que cuenta con un software para 'mapear' y analizar las relaciones entre los usua-

Sumo Logic adquirió **DF Labs** para ampliar las capacidades de su solución SIEM nativa de la nube y "ayudar a reducir o eliminar las tareas manuales tediosas y propensas a errores y capacitar a los equipos de SOC para acelerar la detección de amenazas, el análisis, la respuesta a incidentes y las investigaciones forenses". Una operación que se prevé que se cierre en 2022.

works con **Bridgecrew**, por más de 128 millones de euros, para ofrecer a través de su plataforma protección a lo largo de todo el ciclo de vida de la aplicación.

CrowdStrike anunció la compra, por algo más de 330 millones de euros, de **Humio** para mejorar la detección y respuesta. Así sumará capacidades de provisión de datos para ofrecer análisis contextuales y mejorar la toma de decisiones corporativas.

OneTrust adquirió **Convercent**, especializada en ética y cumplimiento. Se trata de un paso más para "crear un tejido tecnológico de confianza dentro de una organización, uniendo privacidad, seguridad, gobierno de datos, ética y cumplimiento, GRC, riesgo de terceros y ESG (software medioambiental, social y de gobernanza) en un solo flujo de trabajo operativo", explicaron desde OneTrust.

Además, **PayPal** compró la empresa de custodia de criptomonedas, **Curv**, con sede en Israel como parte de su estrategia para "invertir en el talento" y su apuesta por "un sistema financiero más inclusivo", destacaron desde la compañía.

Fondos de inversión

Las rondas de financiación también han sido bastante numerosas. **Telefónica Tech Ventures** ha invertido en **fcase**, una *startup* especializada en tecnología de orquestación para la detección y prevención del fraude y la *startup* tecnológica **Plume**, dedicada a servicios para el hogar inteligente, con operaciones en España desde hace tres años y que ha recaudado 227 millones de euros. Asimismo, la compañía **Autocrypt**, de ciberseguridad en las conexiones de los vehículos, recaudó 12 millones de euros.



La apuesta por empresas de protección en la nube, identidades y servicios de ciberprotección centran gran parte de las operaciones de fusiones y adquisiciones

por cantidad pagada, sólo por detrás de lo abonado por **Broadcom**, en 2019, para hacerse con **Symantec** (8.800 millones) y de **Intel** cuando compró **McAfee** (6.300 millones). Eso sí, **Auth0** continuará funcionando como "unidad de negocios independiente" dentro de **Okta**, con ambas plataformas integradas juntas a lo largo del tiempo. También, ha sido importante la venta por parte de **McAfee**, de su negocio para empresas a **Symphony Technology Group** (STG) por más de 3.300 millones de euros, dedicándose a partir del cierre de la operación en exclusiva al mercado de Consumo. En principio, el negocio corporativo cambiará de marca, lo que se espera que ocurra en los próximos meses. Se espera que la transacción se cierre a finales de 2021.

Además, **Thycotic** y **Centrify** se fusionarán en un acuerdo de 1.160 millones de euros que ha liderado **TPG Capital**, que combinará a ambos proveedores de administración de acceso privilegiado (PAM). El Director Ejecutivo de **Centrify**, **Art Gilliland**, será el Director General del negocio recientemente amplia-

rios y los datos en almacenes de datos en la nube como **Salesforce**, **G-suite** y **Amazon S3**, y correlacionar las cuentas dispares que se utilizan para acceder a estas tiendas.

Por su parte, **Deloitte** adquirió la estadounidense **Root9B**, centrada en la capacitación en ciberseguridad con la visión de brindar tecnología de grado militar al sector privado.

Ivanti, que cuenta con **Neurons**, una plataforma de automatización que hace que cada conexión de TI sea más inteligente y segura, compró **Cherwell** para habilitar el servicio de extremo a extremo y la gestión de activos, "proporcionando un servicio integral y gestión de activos desde TI hasta líneas de negocio y desde todos los puntos finales hasta el borde de IoT". **Rapid7** se hizo con el proveedor de seguridad de la israelí **Kubernetes Alcide** por poco más de 41 millones de euros, una compra que se produce tras la adquisición de **DivvyCloud** en abril de 2020. **HelpSystems**, por su parte, se hizo con **Digital Defense** para impulsar aún más sus ofertas de productos de seguridad.

SentinelOne adquirió **Scalyr**, una plataforma de análisis de datos a escala y nativa de la nube. Con esta adquisición, **SentinelOne** podrá ingerir, correlacionar y buscar datos de cualquier fuente, disponiendo de una plataforma XDR integrada, de referencia, para la mitigación de amenazas en tiempo real en la empresa y la nube.

La multinacional francesa **Atos** se hizo con **Motiv ICT Security**, un proveedor independiente de servicios de seguridad gestionados (MSS) de los Países Bajos, y con **In Fidem**, una consultora canadiense de ciberprotección con experiencia en identidad digital, seguridad en la nube, análisis forense digital, gestión de riesgos, respuesta a ciberseguridad y operaciones de seguridad.

Por su parte, **Tenable** anunció su intención de comprar, por más de 90 millones de euros, a **Alsids**, especializada en protección del Directorio Activo. Asimismo, **Proofpoint** adquirió **IntelliSecure** por 52,7 millones de euros, con la que ofrecerá mejor protección a sus clientes en datos críticos en diversos entornos; y **Palo Alto Net-**



STORMSHIELD

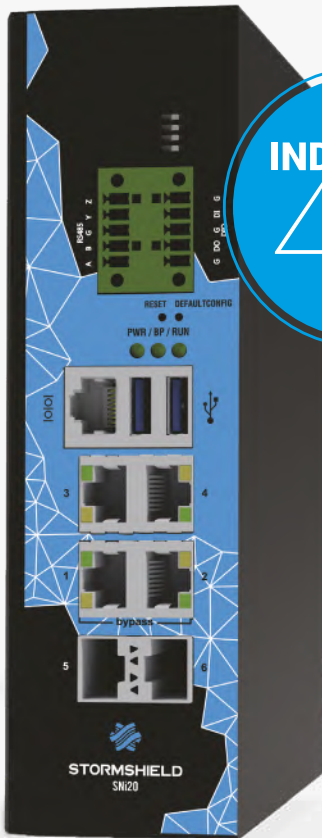
INDUSTRY
4.0

PROTECCIÓN DE INSTALACIONES INDUSTRIALES

De amenazas dirigidas a estaciones de trabajo o provenientes de la red



SNi20



SNi40



Stormshield ofrece innovadoras soluciones de seguridad integrales para proteger las redes (Stormshield Network Security), los puestos de trabajo (Stormshield Endpoint Security) y los datos (Stormshield Data Security).

www.stormshield.com

El mercado corporativo de ciberseguridad en España podría superar en 2021 los 1.700 millones de euros con un crecimiento del 9%

Según estimaciones de Revista SIC, que lleva realizándolas desde el año 2000, referidas a la actividad del mercado corporativo de ciberseguridad en España y algunas áreas de influencia, el sector facturó en 2020 la cifra 1.569 millones de euros, experimentando un crecimiento promediado del 11% respecto del año anterior, en tanto que su proyección estimada para este 2021 experimentaría un incremento del 9% promediado, situando la facturación en los 1.710 millones de euros previsto para este año.

El normal devenir del sector, en continua pujanza y crecimiento desde hace dos décadas, se vio afectado el año pasado 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 crecimientos 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 pro-

piciando 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.

Estas estimaciones de SIC ha-

cen referencia exclusivamente a las actividades mercantiles del sector con clientes corporativos (privados y públicos) que aglutinaría las actividades de consultoría/asesoría, prescripción, implantación de herramientas y soluciones, licencias/mantenimiento/actualización, externalización de servicios (mayormente

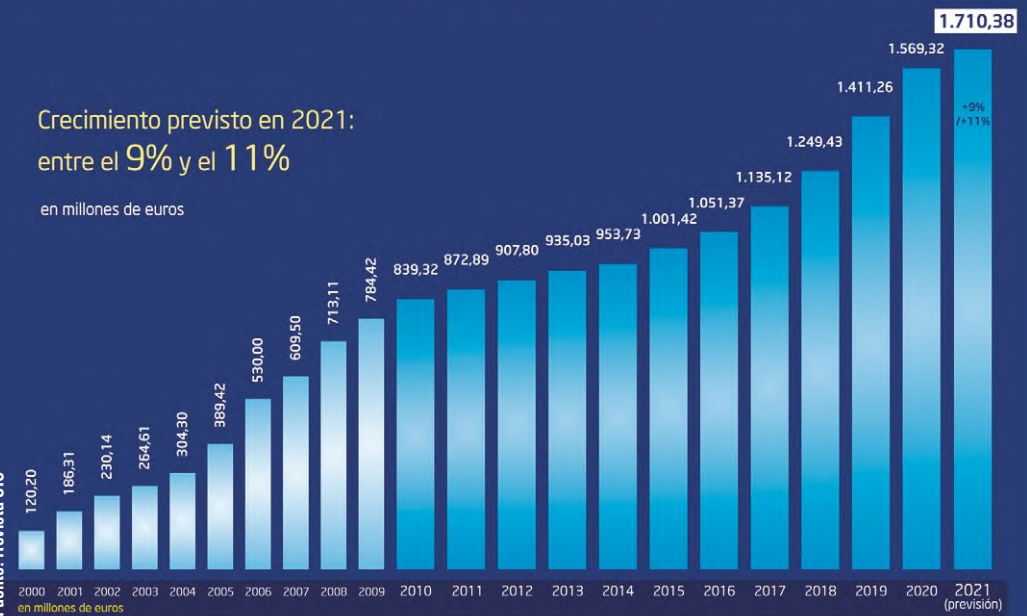
te MSSPs) y en la nube, auditoría, personal externo, formación y seguros. De este conjunto de actividades quedan excluidas las referidas a la estrictamente jurídicas de protección de datos personales (que no las TIC) y a la I+D+i de laboratorios, centros de investigación y universidades.

Mercado corporativo de Ciberseguridad en España

Crecimiento previsto en 2021:
entre el 9% y el 11%

en millones de euros

Fuente: Revista SIC



CYBASQUE, primera entidad de Iberia que podrá emitir el sello 'Cybersecurity Made in Europe'

La Asociación de Industrias de Ciberseguridad de Euskadi (Cybasque) se ha convertido en la primera entidad de la Península capacitada para emitir el sello 'Cybersecurity Made in Europe', tras el visto bueno por parte de la Organización Europea de Ciberseguridad (ECISO) y con el apoyo del Basque CyberSecurity Centre (BCSC), como miembro y socio estratégico.

Esta nueva certificación se dirige a las empresas del sector y su obtención aporta un notable valor añadido a las organizaciones ya



De izq. a drch: Xabier Mitxelena (Cybasque), Arantxa Tapia (Gobierno Vasco) y Javier Diéguez (BCSC)



que avala que la ciberseguridad, tanto de sus tecnologías como de las propias empresas tiene su origen en Europa, según

explican desde la asociación.

Así pues, el objetivo principal del sello lanzado por la ECISO es servir como un diferenciador en el mercado, poniendo en valor la ubicación geográfica de la empresa. Además, con su lanzamiento se pretende concienciar a los usuarios, organizaciones e inversores sobre

de confianza; así como incrementar su visibilidad ante posibles socios comerciales, usuarios finales o inversores.

Las empresas que estén interesadas deberán cumplir con varios requisitos como: ser una entidad legal radicada en Europa, que su actividad se lleve a cabo principalmente en el continente y que sus soluciones cuenten con los requisitos mínimos marcados por la Agencia Europea de Ciberseguridad (Enisa).

"Que Cybasque sea la primera entidad de España y Portugal capacitadora para la emisión de este 'sello' pone en valor el trabajo que estamos desarrollando", ha subrayado el presidente de la iniciativa, Xabier Mitxelena.

¿Se identifica?

BAJO MI RESPONSABILIDAD

T

ENGO UNA RED OT

CUENTO CON UNAS

R

EDES PLANAS

EL ACCESO SE REALIZA CON

U

NA AUTENTICACIÓN DÉBIL

LOS PROTOCOLOS DE LOS

S

CI SON INSEGUROS

LOS DEPARTAMENTOS DE IT Y O

T

NO COLABORAN ENTRE SÍ

HAY UNA VISIBILIDAD

I

NSUFICIENTE DE LAS REDES SCI

LAS VULNERABILIDADES

N

O SE ESTÁN MONITORIZANDO

NECESITO EL CONTROL DE ACCES

O

REMOTO BIEN ADMINISTRADO

MI EQUIPO Y

Y

O NO TENEMOS LOS RECURSOS

LA ALTA DIRECCIÓN DEMANDA

L

A ESTRATEGIA A LARGO PLAZO

¿CÓMO INCORPOR

O

LA RED IoT A ESTE ECOSISTEMA?

EL CLÚSTER DE CIBERSEGURIDAD DE MADRID conforma cuatro grupos de trabajo y ya dispone de imagen corporativa

El Clúster de Ciberseguridad de Madrid, creado a finales de 2020 por el sector privado con el apoyo del Ayuntamiento de la capital, ha marcado su programa de objetivos para 2021. Una ambiciosa 'hoja de ruta' para la que ha creado cuatro grupos de trabajo que estarán coordinados por reconocidos profesionales del sector:

Jorge Hurtado, de **Cipher**, a cargo del 'Desarrollo y Fortalecimiento Empresarial', **Alberto de las Heras**, de **Entelgy Innotec**, quien liderará el de 'Formación y Empleabilidad', mientras que el de 'Investigación, Desarrollo e Innovación' estará a cargo de **Miguel Rego**, de **Funditec**, y el de 'Comunicación y Concienciación' de **Daniel García**, del **ISMS Fórum**.

A través de ellos, la asociación pretende desarrollar lo que considera sus ejes estratégicos: formación y empleabilidad; I+D+i; desarrollo y fortalecimiento empresarial; comunicación y concienciación; y



colaboración entre agentes.

Así, el Clúster, que está presidido por **Damián Ruiz**, CISO de **Singular Bank**, espera contar a mediados de año con casi dos decenas de integrantes, realizará acciones formativas para el mundo ejecutivo y pymes e, incluso, para impulsar la formación en ciberprotección a través de la FP. También, espera presentar una herramienta de autodiagnóstico,

así como estudiar la viabilidad de crear una aceleradora para *startups* madrileñas de este entorno.

Objetivos

En cuanto a los objetivos de cada grupo de trabajo, el de Desarrollo se ha marcado como meta para este año realizar un estudio de Madrid, como polo europeo de la ciberseguridad, realizar una guía de ciberprotección para pymes y acometer un plan de fomento de la



concienciación entre el mundo directivo. Además, se quiere ofrecer desde el Clúster una herramienta de autodiagnóstico para empresas de medio y pequeño tamaño.

El de Formación, por su parte, realizará una nueva versión, junto con **Hays**, del ya presentado informe sobre Competencias y Demanda de Ciberseguridad en la región, además de elaborar itinerarios formativos para el desarrollo de profesionales en la Comunidad, entre otras acciones que incluyen desde forma-

ción para profesorado, hasta impulsar la ciberseguridad en FP, con especializaciones concretas, o participar en la Escuela Municipal de Talento del Ayuntamiento. En tercer lugar, el de Investigación se centrará en detectar qué necesidades emergentes hay en materia de ciberseguridad y estudiar la viabilidad de crear una aceleradora específica en Madrid, así como convocar un concurso de ideas entre universitarios y participar en misiones comerciales. El Clúster no olvida la importancia de la Comunicación y prevé realizar una presentación pública próximamente, además de generar información a través de su web y redes sociales.

Además, en la primera reunión de su Junta, a principios de año, se aprobó su logo oficial bajo la denominación **CyberMADRID**, cuyo diseño tal vez sea desafortunado al no incluir el necesario término ciberseguridad en él y por ello inducir a la errónea percepción de que abarca otros segmentos de actividad ciber, e, igualmente, por guardar no pocas similitudes gráficas con el del CCI-Centro de Ciberseguridad Industrial.

FUNDITEC estrena Director y centrará sus actividades de investigación en ámbitos de la ciberseguridad con foco en la Industria 4.0

La Fundación para el Desarrollo y la Innovación Tecnológica (**Funditec**), creada en 2003 y cuyo director general actual –desde este mes de abril– es **Miguel Rego**, profesional de dilatada trayectoria en el ámbito de la ciberprotección en ámbitos públicos y privados, es una organización privada sin ánimo de lucro ubicada en Madrid, centrada actualmente en el desarrollo de proyectos de investigación en dos áreas estratégicas: materiales avanzados y ciberseguridad.

Las actividades de Funditec relacionadas con la ciberseguridad están especialmente focalizadas en las líneas de investigación relacionadas con el desarrollo de la Industria 4.0, como la robótica, los *smart systems* y la impresión aditiva. Estos proyectos buscan responder a los retos y

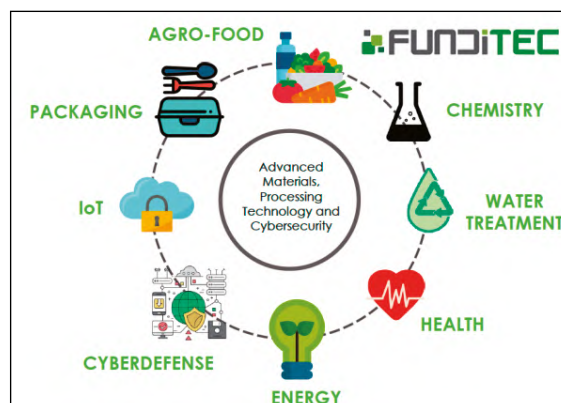


Miguel Rego

amenazas derivados de la aplicación del *Internet of Things* a ámbitos como la industria, los entornos médicos y la salud, y las Fuerzas Armadas. Actualmente, Funditec trabaja en el desarrollo de modelos de "adversarial machine learning" para prevenir ataques contra siste-

mas de inteligencia artificial, aportar integridad y autenticidad a través del *blockchain*, aplicar arquitecturas de inteligencia artificial distribuida a la generación de la respuesta ante ciberamenazas o la detección de anomalías en despliegues de *edge computing*.

Todos estos proyectos se financian con fondos



públicos nacionales o europeos o con financiación privada de compañías que confían en Funditec para el desarrollo de sus iniciativas innovadoras. Los servicios de investigación abarcan desde el diseño de la solución, a la creación de prototipos y pilotos con distintos TRLs.

Identity Security for the Cloud Enterprise.

En el mundo digital de hoy, no se puede hacer negocios sin tecnología y no se puede utilizar la tecnología de manera segura sin protección de la identidad.

Solo SailPoint Identity Security puede ayudarle a habilitar su negocio y gestionar el riesgo cibernético asociado con la explosión del acceso a la tecnología de su empresa en la nube, lo que garantiza que cada trabajador tenga el acceso correcto para hacer su trabajo, ni más ni menos.

Obtenga una visibilidad e inteligencia inigualables mientras automatiza y acelera la gestión de las identidades, derechos, sistemas, datos y servicios en la nube de todos los usuarios.

Habilite el acceso y proteja su negocio, en cualquier lugar.

Para más información, visite sailpoint.com/es



El BCSC presenta el plan estratégico de ciberseguridad 'EUSKADI 2025' de la mano de CYBASQUE

El pasado 2 de marzo, desde el **Centro Vasco de Ciberseguridad (BCSC)** y de la mano de su socio estratégico **Cybasque**, se organizó un evento virtual exclusivo para los clústeres de Euskadi. El evento fue seguido por cerca de 50 asistentes representando a los sectores estratégicos de Euskadi: **HEGAN** (aeronáutico), **Basque Food Cluster** (alimentación), **Basque Energy Cluster** (energía), **AFM** (fabricación avanzada), **MAFEX** (ferroviario), **FEAF** (fundición), **FMV** (industrias marítimas), **Basque Health Cluster** (salud), **SIDEREX** (siderurgia) y diferentes agrupaciones empresariales como **Cebek**.

En este evento, **Javier Diéguez**, director del BCSC, presentó las líneas maestras del plan estratégico de ciberseguridad **Euskadi 2025**, elaborado con la participación del sector proveedor, pero también con la contribución esencial de algunos clústeres y empresas industriales.

Por su parte, **Xabier Mitxelena**, presidente de **Cybasque**, centró su intervención en el valor que tiene la ciberseguridad para los sectores industriales, como herramienta para aumentar su competitividad y el impacto de la misma en sus cadenas de valor. En su presentación, Mitxelena habló de un mercado mundial potencial en ciberseguridad para 2022 de 130 billones de euros, con incrementos anuales de entre el 12% y el 15% y una tasa de paro en el sector de un 0% (con un aumento previsto del 36,5% hasta 2022). Esto implica más de 3,5 millones de profesionales en ciberseguridad para este año.

Objetivos del Plan

El Plan estratégico de ciberseguridad se concibe a finales de 2019, cuando el Gobierno vasco solicita al Centro Vasco de Ciberseguridad que impulse la creación de un *hub* tecnológico de excelencia en el ámbito de la ciberseguridad industrial que posicione a Euskadi como referencia internacional. La especialización en la protección de la Industria 4.0 fue identificado como un nicho con gran potencial de crecimiento, baja madurez en los posibles competidores y un mercado local tractor que presenta tres fortalezas esenciales para el éxito del nodo: fuerte digitalización, vocación innovadora y amplio despliegue internacional.

El plan, sustentado en la colaboración público-privada, iniciativas existentes y tejido ya construido, permite integrar esfuerzos y capacidades para crear una imagen de marca como nodo especializado de ciberseguridad industrial. Por ello, deberá dinamizar el tejido empresarial vasco vinculado a la ciberseguridad, fomentando el emprendimiento y la creación de *startups*, impulsando las empre-



Inversión y Relaciones), **30 líneas estratégicas** y **65 acciones** que contemplan la ciberseguridad alineada con otras actividades económicas (ver **Tabla 1**).

Siendo esencial dotar al BCSC de un rol clave en la dinamización del ecosistema como motor de las relaciones, como embajador del *hub* a nivel global y como impulsor tanto del sector como de la transferencia a la industria. Dentro de las administraciones públicas de Euskadi, el BCSC es actualmente el único CERT homologado en FIRST, lo que abre un espacio adicional de

colaboraciones para intercambio de experiencias e información.

Avances más relevantes en tiempos de pandemia

En la parte final de su intervención, Diéguez comentó que la actual coyuntura de pandemia ha obligado a adaptar las priorizaciones establecidas

sas ya constituidas, desarrollando y atrayendo talento, y atrayendo inversión.

La misión es constituir el ecosistema idóneo y sostenible que permita atraer talento, ideas e inversión (estatal e internacional) y a la vez, fomentar las relaciones necesarias entre estos componentes en busca de disparar la innovación y el emprendimiento en el ámbito de ciberseguridad industrial, para con ello situar a Euskadi como marca de referencia

	IDEAS	TALENTO	INVERSIÓN	RELACIONES
Líneas estratégicas (30)	7 líneas estratégicas	9 líneas estratégicas	6 líneas estratégicas	8 líneas estratégicas
#Acciones (65)	11 acciones	25 acciones	13 acciones	16 acciones

Tabla 1.

internacional de ciberseguridad industrial a efectos de relevancia económica, avances tecnológicos, seguridad ciudadana y empresarial, cultura emprendedora y dinamización académica y laboral.

Plan de trabajo

Tomando la ambición estratégica y el tejido actual como punto de partida, se han analizado **12 hubs** de referencia internacional (Bretaña, Helsinki, Tel Aviv, París, Irlanda del Norte, Lombardía, Lisboa, Barcelona, Tosca, Gales, Valencia y Madrid) y se ha entrevistado a 85 agentes del ecosistema (redes sociales y empresariales, Universidades y centros tecnológicos, clústeres, empresas tractoras e inversores, Gobierno y entidades públicas).

Esta sesión de co-creación ha permitido definir **cuatro ámbitos de actuación** (Ideas, Talento,

antes de febrero de 2020. Haciendo un rápido resumen a las acciones realizadas en 2020, destaca la creación de **Cybasque**, la creación del **Venture Club en Bind 4.0** para apoyar a *startups* buscando ronda de inversión o la colaboración permanente con **Basque Research and Technology Alliance**, entre otros.

Por último, las acciones que se van a priorizar a corto plazo atendiendo al escenario creado por la pandemia, pasan por la **compra pública de innovación** y el refuerzo de **cultura emprendedora** en ámbito educativo (*Ideas*); explorar **modelos de reskilling y upskilling** junto con el Servicio Vasco de Empleo (*Talento*); acompañar a las empresas industriales en el **cumplimiento regulatorio o de estándares de ciberseguridad** reconocidos (*Inversión*); impulso de **Bootcamps y role-plays** de simulación de crisis y simulación de ciberataques en el Basque Digital Innovation Hub (*Relaciones*).

Cytomic Orion

Analítica que acelera la — detección y la — respuesta

La solución cloud que acelera el Threat Hunting, la detección y la respuesta en tu organización.

Automatiza búsquedas de amenazas malwareless, triajes de alertas y la investigación de casos gracias a la aplicación de análisis de eventos e inteligencia de amenazas.

Cytomic Orion guía a tus analistas de seguridad en el proceso de triaje, investigación y reacción inmediata.

Para más información visita:

<https://www.cytomic.ai/es/soluciones/orion/>

LIBERBANK, primera entidad bancaria en obtener la doble certificación de Seguridad y de Privacidad de la Información de AENOR en su Banca Digital

Liberbank ha logrado dos certificaciones de la mano de Aenor que certifican su buen hacer en la protección y gestión de la información. La primera, 'Sistema de Gestión de Seguridad de la Información' (ISO 27001), establece los requisitos para implantar, documentar y evaluar un sistema de gestión de la seguridad de la información, que garantiza la aplicación de un sistema de ciberseguridad orientada a los procesos y objetivos del negocio considerando el análisis de riesgos de TIC. La segunda, 'Gestión de Información de Privacidad' (ISO 27701), supone el refrendo de su forma de trabajar para la gestión de la privacidad, complementando los requisitos necesarios en la ISO/



En la imagen, de izq. a dcha., Juan Carlos Valle, director de seguridad de la Información y riesgo Tecnológico de Liberbank; Severino Méndez, director general de Personas y Medios de Liberbank; Juan L. García, director de AENOR en Asturias; y Alberto García, director de Protección de Datos (DPO) y Liberbank

IEC 27001 e ISO/IEC 27002 con relación a la privacidad y la protección de los datos de carácter personal. Con ellas, Liberbank se erige en la primera entidad financiera en recibir esta doble certificación en su Banca Digital.

Además, según explican desde la entidad, supone un importante paso en "su modelo de banca abierta, reforzando la seguridad y la privacidad de los clientes y, en consecuencia, la experiencia de uso".

La auditoría a la que se sometió la entidad destacó, entre otros aspectos, su apuesta por la formación y concienciación en materia de seguridad de la información y la privacidad, la experiencia y conocimientos de la seguridad y privacidad de la información que han demostrado los responsables de estos ámbitos, la implicación de la Alta Dirección y la gestión de la seguridad de la información que se ha realizado durante la crisis sanitaria originada por la Covid-19.

También, se destacó de ella su transparencia y eficacia frente a los clientes y accionistas a la hora de gestionar la privacidad de la información y el tratamiento de datos personales.

Los incidentes de 'derrame de credenciales' se duplican a medida que aumenta la sofisticación de los ciberdelincuentes

Los llamados 'derrames de credenciales', un tipo de incidente de seguridad que implica la filtración de una combinación de datos compuesta por nombre de usuario y correo-e y contraseña, se han duplicado desde 2016, según la última edición del informe 'Credential Stuffing Report' de F5.

A pesar de ello, el volumen total de credenciales 'derramadas' de 2016 a 2020 cayó un 46%, debido a que si entonces se veían comprometidos una media de 63 millones de registros en cada incidente, en 2020 esa cifra se redujo a 17 millones. Según el informe de F5, lo que está creciendo considerablemente son los incidentes de tamaño mediano, ya que en 2020 se vieron afectados dos millones de registros en cada uno de ellos, lo que supone un 234% más, con respecto a 2019. No obstante, aún no se han superado los 2,75 millones de registros afectados en cada incidente de tamaño mediano de 2016.

Lo preocupante es que la explotación de los datos filtrados, que se materializa en la práctica conocida como relleno de credenciales (cre-



dential stuffing), ya se ha convertido en un problema global, según F5 que recuerda que el mismísimo FBI ha alertado recientemente de que este tipo de incidente fue la principal amenaza de seguridad para el sector financiero estadounidense desde 2017, al representar el 41% del total de los ataques.



Deficiente almacenamiento de contraseñas

El gran problema, según el estudio, es que el deficiente almacenamiento de contraseñas sigue siendo uno de los problemas más recurrentes. Así, en el 42,6% de los derrames de credenciales de los últimos tres años se ha comprobado que se carecía de protección para unas contraseñas almacenadas en texto sin formato.

El incremento de ciberamenazas y la mayor presión regulatoria podría incrementar el precio de los seguros cibernéticos hasta un 50% este año

Los titulares de pólizas cibernéticas pueden esperar aumentos en las tasas del 20% al 50% de la cobertura lo largo de 2021, ya que las tendencias que comenzaron el año pasado continúan a un ritmo acelerado, dijo la compañía británica de seguros Aon en el informe publicado en febrero: 'Instantánea del seguro cibernético: Una visión enfocada al riesgo en 2021'.

Estas tendencias incluyen una mayor frecuencia y gravedad de las reclamaciones, en gran parte impulsadas por eventos de ransomware, según el informe. Una situación que ha golpeado con dureza a todo tipo de sectores desde que comenzara 2021, siendo el último caso conocido, la multinacional Acer a la que, al parecer, se le podría haber pedido un rescate de 50 millones de dólares por recuperar su información. De hecho, el documento destaca que los incidentes de ransomware aumentaron un 486% entre el primer trimestre de 2018 y el cuarto trimestre de 2020, mientras que las violaciones de datos y los eventos de privacidad disminuyeron el año pasado. Por ello, "para mantener un compromiso con la capacidad

cibernética estable a largo plazo, las aseguradoras están revisando áreas de su cartera donde se necesita una acción de suscripción y reevaluando el despliegue de la capacidad, específicamente en lo que se refiere a las pérdidas de ransomware", destaca el informe de Aon.

El estudio resaltó que las tendencias es que estas pólizas suban de precio teniendo en cuenta el cada vez mayor número de incidentes que se producen por errores de



configuración u omisiones, derivadas de las iniciativas de transformación digital acelerada de muchas organizaciones.

También, alerta del incremento de riesgo que supone para las compañías las, cada vez, mayores y más variadas regulaciones lo que incrementa la complejidad para cumplirlas o del riesgo que supone depender de la seguridad de proveedores, entre otros aspectos.

Los activos digitales de su empresa, más seguros que nunca

La enorme acumulación de datos corporativos y su gran relevancia para los negocios exige contar con una arquitectura de protección que mantenga a salvo las aplicaciones, sistemas y bases de datos de su organización de posibles amenazas internas y externas. En definitiva, de todos sus recursos digitales.

IBM Security Guardium es la respuesta de seguridad integral, escalable y dinámica que ofrece una visión global de los sistemas de información corporativos, descubre, clasifica y evalúa cualquier vulnerabilidad, evita los accesos no autorizados y automatiza el cumplimiento normativo en materia de protección de datos.

Confíe en la tecnología de seguridad más avanzada y en la visión de un especialista para llevarla a su terreno. **IBM Security Guardium y Logicalis**, la combinación más segura para sus activos digitales.

Si quiere saber más sobre el papel de la tecnología en protección de datos descárguese el siguiente QR



¿Qué podemos hacer por su organización?

Contacte con Logicalis y conozca cómo podemos ayudarle.

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

Email
marketing-es@es.logicalis.com

EY obtiene, de AENOR, una certificación en ciberseguridad doble: la del ENS y de Seguridad de la Información (ISO 27001) refrendando sus objetivos estratégicos

EY ha renovado la certificación de la norma ISO 27001 relativa a Seguridad de la Información y ha obtenido la certificación de conformidad con los requisitos del Real Decreto 3/2010 del Esquema Nacional de Seguridad (ENS) para los sistemas de información que dan soporte a los servicios de consultoría de ciberseguridad.

Con estas certificaciones, la firma ha acreditado que gestiona la información de sus clientes, en todas sus líneas de servicio, conforme a las mejores prácticas internacionales en ciberseguridad y que los sistemas de información que prestan estos servicios de seguridad cumplen con las directrices establecidas por el **Centro Criptológico Nacional**.

Ambas certificaciones fueron obtenidas como consecuencia de un amplio y exhaustivo proceso. Durante el acto de entrega, el Director de Aenor para la Región Centro y EMEA, **Gonzalo Piédrola**, destacó “el enorme esfuerzo que EY ha hecho para prote-



Gonzalo Piédrola, director de AENOR para la Región Centro y EMEA, junto a Elena Maestre, Socia responsable de Ciberseguridad de EY

ger un bien preciado, la información y los datos, cuya seguridad le permite mejorar la calidad del servicio que ofrece y optimizar la confianza de sus clientes”. Además, enfatizó que “este proceso de certificación es particularmente complejo, por lo que quiero dar la enhorabuena al equipo implicado por haberlo impulsado de forma muy activa, ya que, además, la ciberseguridad forma parte de la propia estrategia de la compañía”. Por

su parte, **Elena Maestre**, Socia responsable de Ciberseguridad de EY, explicó que estas “certificaciones vienen a confirmar que tenemos implantados una serie de controles y medidas que minimizan los riesgos de ciberseguridad, a la vez que constatan las mejores prácticas por parte de la firma a la hora de ofrecer a nuestros clientes los máximos estándares de seguridad”. También destacó que la compañía ha apostado, de forma estratégica por “cumplir los mismos estándares que promovemos y ayudamos a cumplir a nuestros clientes, sobre todo en estos tiempos que por la irrupción de la pandemia ha cambiado el foco de exposición de las organizaciones debido, entre otros aspectos, al teletrabajo e implantación de soluciones en la nube. Por eso es necesario que los CISO revisen su estrategia, prioricen y garanticen las actividades clave de su compañía y acompañen a la organización en los nuevos desafíos a los que se enfrentan”.

plir a nuestros clientes, sobre todo en estos tiempos que por la irrupción de la pandemia ha cambiado el foco de exposición de las organizaciones debido, entre otros aspectos, al teletrabajo e implantación de soluciones en la nube. Por eso es necesario que los CISO revisen su estrategia, prioricen y garanticen las actividades clave de su compañía y acompañen a la organización en los nuevos desafíos a los que se enfrentan”.

El ‘Programa Nacional de Seguridad para Aviación Civil’, con más exigencias en ciberseguridad

La **Secretaría General de Transportes y Movilidad** aprobó la actualización de la parte pública



del ‘Programa Nacional de Seguridad para la Aviación Civil’. El documento, publicado en el BOE, destaca en su capítulo primero la necesidad de establecer una “definición de los sistemas críticos de tecnología de la información y las comunicaciones y de los datos críticos empleados para los fines de la aviación civil y protección de estos frente a las ciberamenazas”, precisando que este aspecto entrará en vigor el 31 de diciembre de 2021. Asimismo, el texto recuerda que “la Autoridad competente velará por que los gestores aeroportuarios, las compañías aéreas y las entidades definidas en el Plan Nacional de Seguridad (PNS) definan y protejan sus sistemas críticos de

tecnología de la información y las comunicaciones y los datos críticos frente a ciberataques que pudieran afectar a la seguridad de la aviación civil”. También, obliga a los gestores aeroportuarios, las compañías aéreas y las entidades a marcar las pautas en su programa de seguridad, o en cualquier documento pertinente a que este haga referencia, los sistemas críticos de tecnología de la información y las comunicaciones y los datos críticos. Precisamente, tanto en su plan de seguridad o cualquier documento que haga referencia a ella deberá ofrecerse información detallada de las medidas que garanticen la protección frente a ciberataques para “garantizar que estos son detectados, que se responde a ellos y que se subsanan sus efectos”.

El teletrabajo dispara los riesgos de incumplir el RGPD por la posibilidad de imprimir información sensible fuera del entorno corporativo

Dos tercios de los trabajadores remotos corren el riesgo de infringir las pautas del RGPD al imprimir documentos relacionados con



el trabajo en casa, según un nuevo estudio de la compañía británica **Go Shred**. La empresa constató en su investigación que el 66% de los trabajadores en remoto han impreso documentos relacionados con el trabajo desde que comenzaron a trabajar desde casa, con un promedio de cinco documentos por semana. Dichos documentos incluyen notas y agendas de reuniones (42%), documentos internos que incluyen manuales de procedimientos (32%), contratos y documentos comerciales (30%), así como formularios de recibos y gastos (27%).

Además, el 20% de los trabajadores a domicilio admitió haber imprimido información confidencial de

los empleados, incluida la nómina, las direcciones y la información médica, y el 13% tenía currículums impresos o formularios de solicitud.

“El problema de esta situación es que, para cumplir con el RGPD, todas las empresas que almacenan o procesan información personal sobre ciudadanos de la UE dentro de los Estados miembro deben tener un proceso efectivo, documentado y auditable para la recopilación, almacenamiento y destrucción de información personal”, destaca el estudio. Sin embargo, cuando se les preguntó a los participantes si habían desechado algún documento impreso desde que trabajaba desde casa, el 24% de los encuestados dijo que aún no lo había desechado, ya que planeaba llevarlo a la oficina y otro 24% dijo que los usaba en casa.

Los ciberataques avanzados están ocupando los titulares. Imposibilita la misión de los atacantes con:



Bitdefender GravityZone™ XDR

la herramienta idónea para los analistas
de seguridad de tu SOC



Bitdefender Managed Detection and Response

si no tienes analistas de seguridad
te ofrecemos nuestro SOC

¡No te quedes atrás por la falta de información,
herramientas y recursos!

Bitdefender®

También ha dado a conocer un informe para impulsar la Ciberseguridad y Movilidad Inteligente

La ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN publica el primer estándar mundial sobre intercambio de Inteligencia de Ciberamenazas

El impacto del cibercrimen no ha parado de crecer en los últimos años, con ataques cada vez más sofisticados y más colaborativos



entre distintos actores y con una cadena de producción cada vez más especializada. En este contexto, la necesidad de adquirir conocimiento o inteligencia global por parte de las empresas y organizaciones para poder minimizar los riesgos se ha vuelto una obligación. Para facilitar esta labor la **Asociación Española de Normalización (UNE)** publicó en febrero la 'Norma UNE 320002 Arquitecturas de confianza para el intercambio de Inteligencia de Ciberamenazas', convirtiéndose así en el primer estándar mundial sobre modelos de gestión y compartición de Inteligencia de Ciberamenazas, todo un hito.

En la norma se define el marco

de referencia genérico para el diseño, gobierno y monitorización del rendimiento y confianza de las redes de intercambio de Inteligencia de

Ciberamenazas. Los modelos normalizados aportan a las empresas mayores garantías y confianza en este ámbito.

La falta de confianza de las empresas en los diferentes ecosistemas de intercambio de Inteligencia de Ciberamenazas es precisamente uno de los principales obstáculos para cubrir esa necesidad. En este sentido, la Norma española UNE 320002 contempla una serie de conceptos y procesos de diseño, gobierno y monitorización de arquitecturas de compartición que permiten crear un ecosistema de garantías y confianza para las entidades que componen la red. Esta norma se ha desarrollado en el

Comité Técnico de Normalización CTN320 de la UNE, dentro del SC4, con la participación y consenso de todas las partes implicadas.

Con la publicación del estándar, culmina un intenso trabajo iniciado en julio de 2019 con la creación del **Grupo de Trabajo ACIIC** 'Arquitecturas de Confianza para el Intercambio de Inteligencias de Ciberamenazas' del CTN 320/SC 4, que ha estado a cargo de la elaboración de la norma. De hecho, para su desarrollo, se han celebrado más de 20 reuniones. Además, servirá de base para el futuro desarrollo de otras referencias normativas en ciberinteligencia. En este sentido, ha sido propuesta para norma internacional ISO.

su entorno', elaborado con la colaboración de las organizaciones participantes del Grupo Específico CTN320/GT CAV Ciberseguridad en Ámbito del Vehículo, del CTN 320 de la UNE.

Este documento tiene como objetivo anticiparse al desarrollo previsto en los sistemas cooperativos inteligentes de transporte y en los avances en la conectividad del vehículo con el entorno. En él se analizan los avances en el campo de las normas y reglamentos que se están desarrollando tanto a nivel gubernamental, como privado. También, se identifican los órganos técnicos de normalización, estándares e iniciativas más relevantes

Ciberseguridad en vehículos

La UNE también ha publicado el 'Informe Normalización en Ciberseguridad para la Movilidad Conectada y Automatizada de vehículos y



relativos a la ciberseguridad y privacidad en el ámbito general de la industria de la Movilidad Conectada. El documento pone de manifiesto la necesidad de contar con nuevas normas técnicas en este contexto.

La ciberprotección con sistemas SASE aún tiene mucho por recorrer: sólo una de cada diez empresas lo ha implementado

Ante la popularización del teletrabajo, el concepto SASE (*Secure Access Service Edge*) ha experimentado un gran crecimiento pero el proveedor de soluciones de protección, **NetMotion**, ha realizado un estudio en el que se desprende que, a pesar de que es muy conocida y demuestra gran interés su adopción real, aún está lejos de lo que se espera: solo el 12% de las empresas han adoptado plenamente SASE.

La encuesta, realizada a 750 expertos en TI de todo tipo de sectores



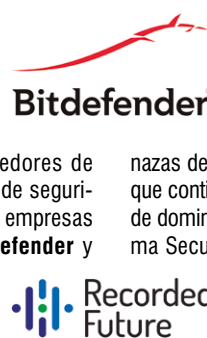
de Europa, Australia y EE.UU., encontró que dos tercios (67%) de los participantes comprenden este enfoque, aunque un 25% no mostró interés por él. En cuanto a qué tecnologías de SASE son más utilizadas, VPN lidera el ranking (54%), seguida de optimización WAN (49%), pasarelas web seguras en la nube (46%), cortafuegos como servicio (39%) y SD-WAN (29%). El informe resalta que el 56% de las organizaciones han comenzado a adoptar una postura de confianza cero.

BITDEFENDER y RECORDED FUTURE suman fuerzas para mejorar las capacidades de detección a través de inteligencia compartida

La inteligencia de seguridad impulsa la toma de decisiones de ciberprotección y la eficiencia operativa

de empresas y proveedores de servicios gestionados de seguridad. Para ayudar a las empresas en este aspecto, **Bitdefender** y **Recorded Future** han firmado un acuerdo para compartir inteligencia de amenazas.

Con él "mejora la amplitud y profundidad de ambas compañías en esta área, para proporcionar a los clientes una mayor visibilidad en el dominio de nivel superior y conocimientos prácticos para eliminar las ciberamenazas contra



los entornos", han destacado.

Así pues, Recorded Future incorporará inteligencia sobre amenazas de los feeds de Bitdefender que contienen datos de reputación de dominios y URL en su Plataforma Security Intelligence. De esta forma, los clientes del Proveedor de Servicios Gestionados de Seguridad y del Centro de

Operaciones de Seguridad se beneficiarán de una mayor visibilidad de la evolución del panorama de amenazas. Esto les permitirá validar las amenazas para tomar decisiones de gestión de riesgos de seguridad más rápidas e informadas.

¿Cómo redefinir tu estrategia de ciberseguridad en la era del COVID-19?

La pandemia ha acelerado los procesos de transformación digital en las compañías, por lo que un planteamiento estratégico en materia de ciberseguridad que garantice la confianza de los clientes es más importante que nunca. Descubre cómo nuestro enfoque EY Resilient Enterprise puede ayudarte a afrontar los desafíos de la nueva realidad.

ey.com/es_es



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

The EY logo, consisting of the letters 'EY' in a bold, white, sans-serif font, with a yellow diagonal line above the 'Y'.

Building a better
working world

BBVA apuesta por Chronicle de GOOGLE CLOUD para contar con una plataforma avanzada de detección y prevención basada en IA

BBVA y Google Cloud han llegado a un acuerdo de colaboración para incorporar a la estrategia de seguridad de la entidad una plataforma para el desarrollo de nuevos modelos de inteligencia artificial (IA) y aprendizaje automático o *machine learning* (ML) para predecir y prevenir ciberataques contra su infraestructura bancaria.

BBVA se convierte así en el primer banco de Europa en utilizar Chronicle, un sistema de análisis de seguridad de Google Cloud que permite almacenar y analizar sus datos de seguridad en un solo lugar para detectar e investigar amenazas a gran escala.

Además, el banco creará lo que ha denominado como el 'Centro Operativo de Seguridad' del futuro. Se trata de un centro en el que Google Cloud y BBVA trabajarán para desarrollar de forma conjunta una nueva plataforma que permitirá al banco adoptar una tecnología más avanzada, optimizar costes y disponer de mayor

escalabilidad. Y es que, el uso de Chronicle, combinado con la experiencia de los departamentos de operaciones de seguridad de BBVA, entidad altamente digitalizada desde hace años, permitirá al banco aprovechar capacidades avanzadas de IA contando con una seguridad más automatizada para el análisis y prevención de ciberataques.

Para **Álvaro Garrido**, Chief Security Officer de BBVA, "esta alianza representa un



salto adelante para el banco y nos permite estar a la vanguardia en la prevención de amenazas a la seguridad de nuestra infraestructura financiera y de nuestros clientes". "La plataforma nos ha sorprendido por su capacidad para mitigar de manera rápida y precisa posibles amenazas. Chroni-



Álvaro Garrido, CSO

cle de Google Cloud cumple con nuestras expectativas y será un magnífico aliado en la transformación de nuestra seguridad general, al igual que Google Cloud lo ha sido en otras áreas del banco", añade.

BBVA colabora con Google Cloud desde 2011 cuando empezó a utilizar, entre otros, las aplicaciones de Workspace de Google para promover una forma de trabajar más ágil y segura y permitir la colaboración global entre

sus trabajadores, minimizando el riesgo en los datos y los documentos generados. En esta línea, cabe recordar, además, que el pasado año, a través del Campus BBVA, la entidad formó a cerca de 2.000 empleados de varios países ante nuevas ciberamenazas, así como en el uso más seguro de sus herramientas corporativas o cómo proceder ante un ciberataque.

EUROPA pone en marcha el proyecto ENSURESEC para proteger al comercio electrónico

Fruto de su apuesta por la digitalización, **Europa** quiere fortalecer también la seguridad del comercio electrónico frente a ciberataques. Para ello, entre otras iniciativas, ha puesto en marcha el proyecto europeo

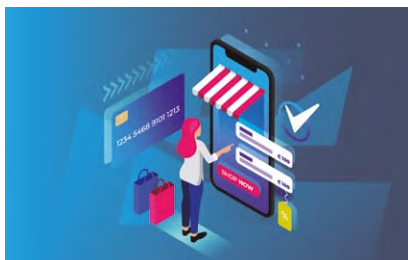


Ensuresec, para proteger el ecosistema de esta actividad del mercado único digital frente a los crecientes riesgos cibernéticos durante todo el ciclo de venta.

problemas del proceso de entrega, el fraude interno, etc. Según **AtoS**, uno de sus participantes, se trata de aplicar un enfoque "holístico y eficaz, centrándose no solo en el desarrollo de soluciones técnicas, sino también en generar conciencia sobre el impacto potencial de estos ataques para la sociedad".

En definitiva, se trata de ofrecer una "plataforma enfocada en la prevención, evaluación y certificación de operaciones de comercio electrónico capaz de detectar nuevos ataques o vulnerabilidades". Algo que se espera tener en tres años de trabajo involucrando a 22 organizaciones de 14 países entre las que están también organizaciones españolas como

CaixaBank. Además, cuenta con el respaldo de reconocidas empresas de comercio electrónico en el mundo como **Mastercard** y la **European Small Business Alliance**, **ESBA**.



El proyecto abordará las amenazas digitales que pueden surgir de la presentación de productos y servicios en las plataformas electrónicas, las transacciones de pago digitales, los

El BCSC releva a RENFE y S21SEC como comité coordinador de CSIRT.es

El **Centro Vasco de Ciberseguridad (BCSC)** ha sido elegido como comité coordinador de **Csirt.es**, la red estatal de equipos de respuesta a incidentes de ciberseguridad. En concreto, será **Asier Martínez**, responsable del CERT del BCSC, quien asuma las labores de coordinación. La organización está integrada por más de 45 equipos tanto públicos

de **Ciberseguridad (INCIBE)** y el **Mando Conjunto de Ciberespacio (ES-DEF-CERT)**; además de los autonómicos y de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), así como de proveedores de ciberseguridad.

Dentro del alcance de Csirt.es se promueven iniciativas que contribuyen a la mejora de la seguridad de las redes locales y estatales,

se comparten experiencias, lecciones aprendidas, e información operativa relevante sobre incidentes de ciberseguridad.

Además, se colabora activamente en iniciativas con

intereses comunes. Dentro de esta actividad, la organización también participa en el Foro Nacional de Ciberseguridad.



como privados, entre los que están desde los tres CERT de referencia: el del **Centro Criptológico Nacional (CCN-CERT)**, el **Instituto Nacional**

¿Sigue luchando contra los problemas
que generan las contraseñas?

La solución es fácil:
Deje de usar contraseñas

Con las YubiKeys de Yubico puede dejar de usar
contraseñas hoy mismo para usuarios de Microsoft AD
y Azure AD para acceder a Windows y Microsoft 365

Yubico + Microsoft: Going Passwordless



Solicite una demostración hoy mismo en dotforce.es

También puede ver una demostración en nuestro canal
de YouTube: dotforce.es/youtube/yubico

Para más información, visite: dotforce.es/yubico/,
llámenos al +34 914 230 991 o escribanos a info@dotforce.es

DotForce – Mayorista de soluciones
de ciberseguridad y optimización de operaciones TIC

También ha abierto un centro en Valencia para IoT y GRC y firmado un acuerdo con Navantia sobre ciberdefensa

TELEFÓNICA estrena la marca NextDefense para sus servicios avanzados de ciberseguridad

Ante las cifras record de vulnerabilidades alcanzadas en 2020 por cuarto año consecutivo, la operadora, actualmente en fase de reestructuración, ha presentado su marca 'NextDefense', dependiente de **Telefónica Tech**, bajo la que ofrecerá sus servicios avanzados de ciberseguridad para grandes empresas.

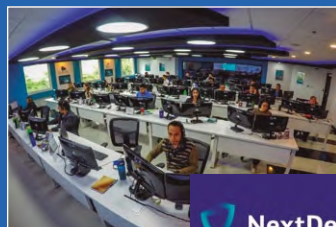
"NextDefense unifica y amplía las soluciones de seguridad ofrecidas hasta ahora para hacer frente a los sofisticados ciberataques de la nueva era postCovid-19. Integra en una única solución la Gestión de Vulnerabilidades basada en Riesgo (Vulnerability Risk Management), la Inteligencia de Amenazas (Cyber Threat Intelligence) y la Detección y Respuesta Gestionada (Managed Detection and Response)", explican desde la compañía, que también destaca que estos servicios se verán reforzados con el respaldo del centro de operaciones de ciberseguridad global de la compañía.

Este cuenta ya con 11 ubicaciones en el mundo y se ha incorporado en los últimos meses un nuevo equipo de análisis de *malware*, inteligencia de amenazas, *threat hunting*, respuesta a incidentes,

análisis forense y análisis de vulnerabilidades.

Apuesta por Valencia

Telefónica Tech también inauguró en febrero su centro de ciberseguridad en la Marina de Valencia, con más de 300 m². En él trabajarán "más de un centenar de personas con perfiles de alta cualificación que se encargan del desarrollo de tecnología, productos y servicios de ciberseguridad relacionados con IoT y GRC, campos en los que Valencia es pionera en España", destacaron desde la empresa, añadiendo que junto a las instalaciones también estará un espacio de *crowdworking*, con el objetivo de impulsar *startups* relacionadas con ese sector y convertirse en centro de conocimiento e innovación participativa y colaborativa. El centro también cuenta con el apoyo de la **Generalitat Valenciana** y el **Ayuntamiento**.



Alianza con Navantia y servicio de drones

Asimismo, Telefónica y **Navantia** firmaron un acuerdo para comercializar y desarrollar proyectos de ciberseguridad integral para la Defensa y el sector naval en el ámbito nacional e internacional.

La colaboración se extenderá al ámbito de las plataformas militares aéreas, terrestres o marítimas durante su ciclo de vida. En el ámbito nacional, ambas compañías trabajarán conjuntamente en la ciberseguridad del submarino S80 y de las fragatas F110.

La multinacional española también dio a conocer en febrero su plataforma de gestión de drones que facilitará el uso y las distintas aplicaciones que estos pueden aportar en el ámbito de la seguridad de las compañías. La herramienta funcional que facilita Telefónica junto con su filial **Ingeniería de Seguridad (TIS)** de la división Telefónica Tech, permite, mediante la plataforma de gestión, que una flota de drones pueda volar de forma autónoma desde cualquier punto geográfico del planeta.

El CCI presenta varias guías sobre protección industrial y, también, sobre ciberprotección en Iberoamérica

Los *gateways* IoT actuales son una mezcla de conectividad, procesamiento y funciones de usuario que todavía no incorporan capacidades de ciberseguridad a un alto nivel. Con el objetivo de analizar en profundidad estos dispositivos el **Centro de Ciberseguridad Industrial (CCI)**, junto a **Deloitte**, ha presentado un nuevo número —el cuarto— de la serie cuadernos del CCI, llamado 'Gateways IoT, Evaluación de seguridad en entornos industriales', escrito por **Abraham Martínez**, Socio y Manager, respectivamente, de Risk Advisor y de la consultora.

El documento está dividido en cuatro capítulos en los que se explica desde las posibilidades y beneficios de la tecnología IoT hasta qué metodologías de evaluación pueden aplicarse

a ella para gestionar la ciberseguridad. El CCI también ha publicado la primera guía de su serie Infraestructuras Críticas Industriales. En ella, se presenta la situación actual de la cadena de suministro en la digitalización industrial y cómo establecer los roles y responsabilidades que reduzcan riesgos tecnológicos.

Además, ha dado a conocer un completo documento con el estado de la ciberprotección en siete grandes países de Iberoamérica —Argentina, Brasil, Colombia, Costa Rica, Chile, México y Paraguay—.



ZEROLYNX estrena imagen corporativa y patrocina la liga ESL de eSports acercando la ciberseguridad al mundo gamer

Tras tres años en el sector y un crecimiento exponencial desde su creación, **Zerolynx** ha renovado su imagen corporativa apostando por transmitir de forma más directa y sencilla "los pilares de una empresa tecnológica, innovadora y cercana". "Elegimos el lince porque es un ágil cazador que, gracias a su agudeza visual y su oído, reconoce a sus presas y en un salto certero y por sorpresa, puede capturarlas en segundos de un solo zarpazo. De la misma manera, Zerolynx hace uso de sus capacidades de análisis y adaptabilidad para localizar vulnerabilidades y corregirlas con una calidad y eficacia singular", recuerdan desde la empresa, que también ha presentado una renovada imagen de su **Open Mobility Security Project**, un *framework* abierto para la evaluación



ZEROLYNX



OPEN MOBILITY SECURITY PROJECT

de la ciberseguridad de todo tipo de vehículos.

La compañía, además, se ha aliado con la **Electronic Sports League (ESL)** para patrocinar la novena temporada del ESL Masters España de CSGO. ESL, la mayor empresa de eSports del mundo, es el principal operador de competiciones nacionales e internacionales abarcando todos los niveles, desde las

competiciones *amateur*, hasta la élite profesional. "Este patrocinio refleja la importante apuesta de Zerolynx por el mundo de los eSports. Estar en el ESL Masters es sin duda clave para la estrategia de internacionalización de nuestra firma", ha destacado su CEO, **Juan Antonio Calles**. Además, "esta colaboración nos permitirá acercar la ciberseguridad al mundo *gaming* y afianzar la cultura de ciberprotección al público joven", dijo su COO, **Daniel González**.

Ingénia

Adaptarse al cambio es
aprovechar el impulso de la
transformación. Conoce nuestro
menú de productos y servicios en
materia de ciberseguridad.

SCAN



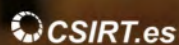
MENU
CIBERSEGURIDAD

eSOC

Centro de Operaciones
de Seguridad

eSOC

INDUSTRIAL
Powered by Ingénia



Según un estudio de Kaspersky, que también ha acometido un plan de capacitación de su Canal en España

Más del 50% de las empresas europeas prohíben a sus analistas compartir Inteligencia sobre amenazas

El 59% de los analistas de inteligencia de amenazas europeos participan en comunidades profesionales; sin embargo, el 58% de los que trabajan en funciones de TI y ciberseguridad no están autorizados por sus empresas a compartir los artefactos de inteligencia de amenazas descubiertos con dichas comunidades, según el informe de **Kaspersky**, 'Managing your IT security team'. En él, la firma rusa ha encuestado a más de 5.200 profesionales de TI y ciberseguridad en todo el mundo para comprobar si otras empresas estaban dispuestas a colaborar y compartir inteligencia de amenazas.

Entre otros aspectos de interés, la investigación reveló que en Europa los encuestados con responsabilidades de análisis de inteligencia de amenazas, en particular, son propensos a participar en foros de la Web Oscura (39%), foros y blogs especializados (24%) o grupos de redes sociales (16%). Sin embargo, cuando se trata de compartir sus

propios hallazgos, sólo el 36% los hace públicos.

Por otro lado, fruto del cambio hacia el trabajo a distancia y el crecimiento de las ciberamenazas por la pandemia, la empresa elaboró el informe 'Cerrar las brechas: predicciones sobre la seguridad informática de las empresas en 2021'. En él, se detallan consejos para cada rol relacionado con



la ciberseguridad, incluyendo a los CEO o propietarios de empresas, CISOs, líderes de equipos SOC y directivos de TI, a los que recomienda acometer programas en gestión de la identidad, apostar por la nube y su protección con SASE.

Programa para el Canal

Kaspersky Iberia dispone de un canal formado por más de 7.000 *partners*, entre los que se

encuentran *resellers* con un nivel muy distinto de conocimiento y formación sobre sus soluciones. Por ello, la compañía ha diseñado un nuevo Programa

de Capacitación para el Canal, con una completa oferta para facilitar formación personalizada a cada tipo de *partner*, y mostrarles cómo ir aumentando su nivel de conocimiento paso a paso. La iniciativa presentada por **José Antonio Morcillo**, Head of Channel Iberia, hará que "nuestros *partners* se posicionen como expertos y que los clientes reciban las mejores soluciones de seguridad y los mejores servicios por su parte". El objetivo para Kaspersky, además, "es crear un alto nivel de lealtad y que puedan aprovechar a largo plazo los conocimientos que les estamos proporcionando."

Por otro lado, Kaspersky ha reforzado su apuesta por el talento joven de los deportes de motor como patrocinador oficial del equipo **Aprilia Racing**, y potenciado su presencia internacional copresidiendo el Grupo de Trabajo 6 del **Paris Call**, junto a **Cigref**, la asociación digital de las principales empresas y administraciones públicas francesas.

¿Comparten los analistas de seguridad TI europeos sus descubrimientos sobre Inteligencia de Amenazas?



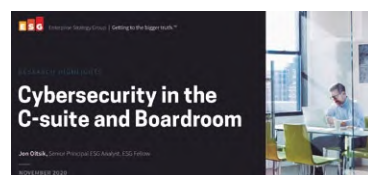
TREND MICRO alerta de los retos en la integración de la seguridad y el negocio

Trend Micro ha publicado una investigación en la que alerta de desafíos sistémicos de la integración de la seguridad en los procesos de negocio. El informe, titulado 'Enterprise Strategy Group', incluye las principales formas de impulsar el compromiso y el acuerdo en torno a las estrategias de ciberseguridad dentro de una orga-

mación Empresarial para mejorar la alineación de la seguridad corporativa, desarrollar un programa en dirección descendente y cuantificable para ayudar a los CISO a comunicarse mejor con sus consejos de dirección o cambiar las estructuras de *reporting* para que los CISO informen a su CEO.

Además, pone de manifiesto que cuando los miembros de los consejos de administración están más formados con la función de ciberseguridad son más propensos a dar el salto de las cuestiones técnicas a las de negocio.

La empresa también dio a conocer su Informe anual de ciberseguridad de detección de amenazas en 2020, en el que identificó más de 62.600 millones, un 20% más que el año anterior.



nización. Entre otros aspectos, destaca que solo el 23% de las organizaciones priorizan la alineación de la seguridad con las iniciativas de negocio clave. Para remediar este desafío, aconseja incorporar un Responsable de Seguridad de la Infor-

NETSKOPE propone desarrollar una estrategia de seguridad avanzada para mejorar en ciberprotección

A la vista de los últimos incidentes y brechas que están impactando contra empresas de todo el mundo, **Netskope** ha destacado la necesidad de avanzar y desplegar una estrategia de seguridad sustentada en tres pilares clave: cooperación, visibilidad y control, y gestión permanente de los riesgos.

"Ataques como el de **SolarWinds** o los dirigidos contra otras empresas del sector han puesto de manifiesto una obviedad: nadie está salvo de sufrir un ciberataque, pero también, algo más preocupante, las estrategias de seguridad no están funcionando adecuadamente", manifiesta la compañía.

Además, desde la firma destacan que a medida que las organizaciones siguen adoptando la nube, las viejas formas de pensar en la protección de datos ya no son efectivas. Así, por ejemplo, la concepción o idea que se mantiene sobre la Prevención de Pérdida de Datos (DLP) pertenece a

una era de seguridad anterior a la nube. Dicha concepción, construida sobre la base de que los "objetos" están en un centro de datos, protegidos por un perímetro que evita que los datos se filtren "hacia fuera" y que otros entren "hacia dentro", ya no es válida.

Mayor integración con Microsoft

Por otro lado, Netskope ha anunciado su adhesión al Programa de *Partners* de Redes de **Microsoft 365** (Microsoft 365 Networking Partner Program). Esta certificación NPP se suma a la creciente lista de integraciones entre ambas compañías, que se extienden a la gestión de accesos e identidades, la inteligencia de amenazas, las operaciones de seguridad, la seguridad en la nube, la protección de datos, la gestión

de aplicaciones, la arquitectura Zero Trust y la preparación para SASE.





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

AIUKEN CYBERSECURITY se convierte en la única compañía española de servicios Managed Detection & Response (MDRS) con una triple calificación AAA

La multinacional española **Aiuken Cybersecurity** ha obtenido una de las más altas calificaciones que ofrece el sello **Leet**, la triple AAA. Este sello es una etiqueta que materializa y muestra el nivel de ciberseguridad que tiene un proveedor en el servicio calificado.

Tras el proceso de evaluación, se otorga la certificación para sus servicios desde el Centro de Operaciones de Seguridad (SOC), los de seguridad basada en nube, así como los de protección gestionada (MSSP / MDRS).

“Esta calificación cumple de acuerdo con los criterios de calificación correspondientes a la versión 2.3 del estándar para evaluar los niveles de seguridad implementados en el servicio calificado en las dimensiones de Confidencialidad, Integridad y Disponibilidad de la información”, destacan desde la compañía.

“Obtener esta triple certificación es un hito nuevamente para Aiuken. Nuestro objetivo es ofrecer a nuestros clientes un portafolio de servicios con una alta cualificación en materia de ciberseguridad y dar una respuesta de acuerdo a sus necesidades”, ha resaltado su CEO, **Juan Miguel Velasco**.

Cabe recordar que, a esta calificación de nivel AAA, Aiuken

suma la certificación obtenida ISO 27001 para su red de SOC's internacional. También cuenta con el certificado de conformidad con el Esquema Nacional de Seguridad (ENS). Así mismo, **Gartner** incluyó a la compañía dentro de su 'Market Guide para Managed Detection & Response' (MDR), como única empresa española.



SEIDOR refuerza su apuesta por la IA con un nuevo centro de competencia en Israel

La consultora multinacional **Seidor**, especializada en servicios y soluciones tecnológicas para gran empresa y pymes, inauguró en Israel su primer centro de competencia en Inteligencia Artificial (IA). Con esta operación, la consultora incorpora el conocimiento, las buenas prácticas y los últimos avances en tecnología que se generan en este país, uno de los ecosistemas de innovación más dinámicos del mundo, y los pone a disposición de su red global de clientes.

Así pues, la creación de este nuevo centro de competencia se asienta sobre dos ejes estratégicos de Seidor en innovación tecnológica: la Inteligencia Artificial (IA) y el IoT (Internet de las Cosas). De esta forma, con el nuevo centro, cobra una nueva dimensión la *joint venture* que Seidor impulsó hace casi dos años con **MalamTeam**, un reconocido grupo de servicios informáticos en TI de Israel. A partir de aquel acuerdo estratégico, inicialmente centrado en soluciones SAP Cloud, surgió Seidor Malam, proyecto empresarial que ha hecho posible que el nuevo centro de competencia incorpore el *know how* israelí.

Conexión Tel Aviv-Barcelona, de la IA al IoT

El refuerzo de la conexión entre Tel Aviv y Barcelona, mediante la actividad conjunta entre el IoT Center de Barcelona y el centro de competencia de Israel, permitirá a Seidor ofrecer soluciones innovadoras a nivel internacional. Con esta operación, Seidor prevé doblar en el presente año su equipo actual de más de medio centenar de profesionales especializados en IoT e IA. Así, desde sus instalaciones en la capital catalana, Seidor coordinará de forma integrada el refuerzo de esta relación entre España e Israel y se orientará al desarrollo de soluciones innovadoras que respondan a retos de negocio de empresas de diferentes sectores. “Desde Seidor apostamos por una visión única en términos de innovación basada en diferentes palancas, de presente y futuro, como son el IoT y la IA y, por extensión, sobre una estrategia de internacionalización de sinergias a través del vínculo entre dos ciudades tan punteras en términos de innovación tecnológica como son Barcelona y Tel Aviv”, destaca el CEO de Seidor, **Josep Benito**.



Josep Benito, CEO

El volumen de negocio del sector superará los 37.000 millones en 2021, con un incremento del 20% en sólo dos años

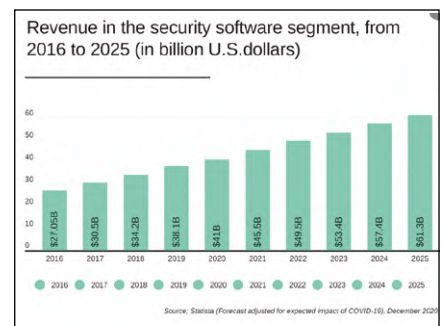
El incremento de inversión en transformación digital por parte de las empresas, fruto de las exigencias por la pandemia y los mayores requisitos regulatorios en protección de datos está impulsando, en todo el mundo, el mercado de la ciberseguridad. Se calcula que este año su volumen de negocio superará los 37.000 millones de euros, con un incremento de un 20% desde hace dos años, según datos de **StokApps**.

Un crecimiento importante por cuanto en 2016 se considera que rondaba, según Statista, los 22.000 millones.

Y es que, según un estudio como el de **TrustRadius** se calcula que en el último año la inversión de las empresas en ciberprotección ha crecido un 41% de media para hacer frente a las nuevas amenazas generadas por el teletrabajo y los riesgos

digitales que están surgiendo. Por ello se calcula que, para 2025, el mercado llegará al umbral de los 50.000 millones de facturación.

Eso sí, con importantes desigualdades geográficas, ya que se calcula que actualmente EE.UU. representa el 50% de la inversión mundial en la industria de ciberseguridad. Según los datos de StockApp le seguirían, con 10 veces menos presupuesto, Alemania y a continuación Reino Unido, Japón y China, aunque también es cierto que estos rankings carecen de información de inversiones reales en países como China, Rusia o Corea, entre otras.





El 95% de los ciberataques que sufren las empresas tiene su foco en el usuario

Concienciar es la única forma de prevenir y reducir el riesgo.



¿Cuál es su estrategia?

Solución Gestionada ES-CIBER

según el nivel de madurez de la cultura de ciberseguridad

	 PLAN ESTRATÉGICO Empresas con un nivel ALTO de madurez de cultura de ciberseguridad	 CAMPAÑAS Empresas con un nivel MEDIO de madurez de cultura en ciberseguridad	 CIBERPACKS Empresas con un nivel BAJO de madurez de cultura de ciberseguridad.
Servicio gestionado	★	★	★
Personalización	★	★	★
Usuario tutor	★	★	★
Detección necesidades	★	★	★
Análisis riesgos	★	★	★
Avance secuencial	★	★	★
Simulacros	★	★	★
Reuniones seguimiento	★	★	★
Informes	★	★	★
Dashboard, KPIs	★	★	★

La iniciativa, en tanto recurso ágil de incorporación de talento al sector, prosigue su línea expansiva y continua contando con la decidida colaboración de SIC

FUNDACIÓN GOODJOB hace balance anual satisfactorio de #INCLUDE tras formar en ciberseguridad a 174 alumnos con discapacidad y sumar más empresas del sector al programa

A falta de un mes para cumplirse el primer año de la puesta en marcha, a instancias de la **Fundación Goodjob**, del **Programa #include** de empleabilidad en Ciberseguridad y dirigido a personas con discapacidad, cabe deducir un más que positivo balance de sus actuaciones, ya que en el 'haber' de esta iniciativa se acredita la formación de 174 participantes de Barcelona, Castilla y León, Madrid y Valencia

El impulso y arranque de esta ejemplarizante acción, en la que la aportación de **Revista SIC** y **RootedCon** fueron decisivas, dibuja un horizonte muy positivo en lo que a su consolidación y expansión se refiere

Como ya informara esta revista en números anteriores, este programa de formación intensiva viene contando en sus diferentes ediciones con la coordinación académica de **Román Ramírez**, de RootedCon así como del equipo especializado de Goodjob, al que

se unen profesionales expertos voluntarios –incluida SIC– procedentes de instituciones públicas de referencia (DSN,

Programa #include
Empresas #includeR y Colaboradoras



talana de Ciberseguridad, Fuerzas y Cuerpos de Seguridad...) y de empresas del sector.

Respecto a estas últimas, dicha formación es impartida por profesionales voluntarios de las propias compañías de tecnología comprometidas con el proyecto –prestadores, integradores, mayoristas y fabricantes– en las que muchas de las cuales, a futuro, podrían desarrollar posteriormente su actividad profesional. El plantel de impartidores



Luis Fernández (SIC) impartiendo formación #include

cuenta asimismo con la participación, en calidad de invitados, de reputados profesionales del mundo de la ciberseguridad quienes se prestan a aportar a los alumnos su visión y experiencias.

Entre las acciones recientes para dar mayor visibilidad a la iniciativa, el direc-

tor de Goodjob, **César López** ha tenido la oportunidad de dar cuenta de los avances del Programa #include participando en la **I Jornada STIC capítulo de Colombia**, de notable alcance iberoamericano, exponiendo la evolución del contenido de la fase formativa y de capacitación, en la que se ha reforzado el contenido en las áreas de Ciberseguridad Industrial, OT, IOT, así como con Cibervigilancia, así como la adición de nuevas empresas, como **Grupo Seidor**, **Evolutio**, **UST Global** e **Innocv**.

IBEROAMÉRICA mira al blockchain como la tecnología que podría dar una identidad digital autosoberana a los países que carecen de ella

El **Banco Interamericano de Desarrollo**, junto con la iniciativa **Inclusión cívica social y económica de habitantes de barrios vulnerables en Buenos Aires mediante modelos de Blockchain (DIDI)** y la **Asociación Civil para el Desarrollo de Ecosistemas Descentralizados (DECODES)** han acometido un estudio en profundidad sobre cómo ofrecer una identidad digital, segura y autosoberana en Iberoamérica aprovechando las capacidades de la cadena de bloques. En él se estudia qué tipo de normativas hay en 20 países de la región (desde Argentina hasta México, Brasil u Honduras...) que permitiría acometer este reto y se dan

unas recomendaciones para lograr esa identidad digital autosoberana.

Entre ellas, destaca que los responsables del estudio consideran que "todo sistema de identidad digital basado en tecnología blockchain o de registros distribuidos debería anteponer los intereses del titular de los datos personales sobre los intereses que terceros pudieran tener sobre ellos". Además, consideran que la participación en sistemas de identidad digital no debiera ser obligatoria sino

voluntaria: en todo momento, el usuario debería ser capaz de eliminar su perfil de forma plena.

"De lo contrario, se vulneraría la

base misma sobre la cual se construye la idea de identidad digital autosoberana".

También, se pone en valor que la base legal para todo tratamiento de datos que se haga a partir de información que forme parte del

perfil del usuario debería contar con su consentimiento expreso e informado, conforme sea establecido en la normativa aplicable

de protección de datos personales. Además, se considera fundamental que "el uso de los datos de la persona por parte de terceros debería estar precedido por la provisión clara y sencilla sobre qué datos pretenden usarse, cómo serán empleados y qué terceros podrán tener acceso a ellos".

Por último, entre otros consejos, se considera de gran interés que los desarrolladores del software estructuren los sistemas de identidad de forma que la privacidad de los usuarios se encuentre resguardada siempre por defecto y que cualquier marco regulatorio en torno a estos desarrollos sea tecnológicamente neutro.



Seguridad Evolutiva

Defensa adaptativa y conectada

DEFENSA
ADAPTATIVA



CSIRT
FINANCIERO



INTELIGENCIA
DE AMENAZAS



MONITORIZACIÓN
Y GESTIÓN
DE INCIDENTES



RED
TEAM



PROTECCIÓN
INTELIGENTE
DEL DATO



MNEMO
LABS



GESTIÓN
ESTRATÉGICA DE
VULNERABILIDADES



España | México | Colombia



www.mnemo.com



info@mnemo.com

MNEMO

EXCLUSIVE NETWORKS afronta 2021 con 17 nuevas marcas, un aumento en 450 personas de su plantilla y la mirada puesta en DevSecOps

Tan solo seis meses después de su nombramiento como CEO, **Jesper Trolle** ha hecho balance del negocio de **Exclusive Networks** en un encuentro virtual el 17 de marzo, tras un año marcado por la Covid-19. A pesar de las dificultades, el mayorista francés ha conseguido dar continuidad a su estrategia y crecer (orgánicamente) un 8% en el número de ventas. Además, ha ampliado su presencia mundial gracias a tres adquisiciones estratégicas: la de **Veracom**, con la que amplía su negocio en



Jesper Trolle

10 países de Europa; la de **Jjnet**, con la que tendrá mayor presencia en Hong Kong y en el noreste de Asia; y la de **Nuaware**, con la que entra con fuerza en el mundo DevSecOps y de contenedores, reforzando también los servicios nativos en la nube. Estas operaciones han ayudado, además, a que durante 2020 su cartera se ampliara con tecnologías de 17 nuevos fabricantes, como **Proofpoint**, **CrowdStrike**, **Okta**, **Netskope**, **F5**, **Vectra** e **Infoblox**, así como a un crecimiento de su

plantilla en 450 profesionales. En 2020 también tuvo como hito el lanzamiento de la plataforma de entrega bajo demanda, **X-OD**, con la que abanderará el 'todo como servicio' y que está disponible en España desde noviembre, expandiéndose los últimos seis meses a nueve países de EMEA. Para 2021, Trolle avanzó que incrementará el alcance de X-OD a América del Norte durante el segundo trimestre. Además, desveló su intención de convertirse en uno de los referentes en DevSecOps y en servicios nativos de la nube.

Premio al Liderazgo en la Comunidad de Madrid

En marzo, **Carmen Muñoz**, Directora General de Exclusive Networks Iberia, recogió el Premio al Liderazgo en Ciberseguridad que fue otorgado a su compañía, en los Premios Pymes de la Comunidad de Madrid. Estos galardones



Carmen Muñoz

reconocen el talento, la innovación y el esfuerzo de las pequeñas y medianas empresas que desarrollan su actividad en la Comunidad. "Este reconocimiento nos honra y nos motiva para seguir trabajando con esta filosofía", dijo Muñoz.

WOMEN4CYBER SPAIN presenta su hoja de ruta para los tres próximos años impulsada por la asesoría, formación y colaboración

El capítulo español de la fundación europea sin ánimo de lucro **W4C**, **Women4Cyber Spain**, cuya creación se anunció de forma oficial en octubre, celebró en febrero un evento en línea para presentar los objetivos, iniciativas y actividades de la asociación, además de dar a conocer su nueva web, www.women4cyberspain.es.

El encuentro, que contó con un centenar de asistentes, tuvo como invitada de honor a la Presidenta y Directora General Adjunta de Women4Cyber, **Anett Mádi-Nátor**. También participaron la Presidenta y Vicepresidenta, **Eduvigis Ortiz** y **Rosa Díaz**, respectivamente, así como las integrantes de la junta directiva, entre las que están **Mar López**, **Idoia Mateo**, **Daniela Kominsky**, **Concepción Córdón**, **Begoña García**, **Elena García** y **Beatriz Soto**, entre otras.

Durante el evento, se dio a conocer la hoja de ruta de la asociación para los tres próximos años que persigue "identificar y visibilizar la presencia femenina, realizar proyectos e investigaciones conjuntas, programas de formación, concienciación y de desarrollo profesional. Además de impulsar el cambio en el sector nacional con el apoyo europeo y la coope-



ración internacional".

Y es que, a pesar de que el 47% de las profesionales españolas del sector TIC ha visto mejorar los niveles de igualdad de género en su organización en los dos últimos años, según un estudio

de **Kaspersky**, éste también pone de manifiesto la brecha aún existente. Además, un 24% lamenta la falta de referentes femeninos en el sector.

Para contribuir a la resolución de este problema, el capítulo español ya está empezando a ofrecer distintas iniciativas de *mentoring*, formación y *networking*. Además, impulsará su colaboración con entidades públicas y privadas, así como con instituciones académicas, como los ya firmados con **Fundación ASTI**, **Isms Forum** o **Inspiring Girls**, entre otras.

La asociación, también presentó los grupos de trabajo a través de los cuales impulsará sus objetivos como los de Emprendimiento, Investigación, Talento Juvenil, RR.HH., etc. Y se explicaron las opciones para asociarse y acceder a los beneficios que conlleva, como el acceso a la bolsa de trabajo, becas y talleres, así como la participación en eventos, entre otros.

La Ley de Ciberseguridad 5G llegará antes de verano

Tras su debate y fase de audiencia pública, la conocida como Ley de Ciberseguridad 5G, que busca garantizar la seguridad nacional y protección en la explotación y despliegue de este tipo de red, ha entrado ya en su última etapa y fuentes cercanas a ella dan por hecho que se aprobará próximamente, a más tardar antes de verano. De momento, el anteproyecto establece importantes requisitos para operadores y suministradores, así como para la Administración Pública. En definitiva, pretende ofrecer un marco regulatorio adecuado para desplegar las nuevas redes 5G, cuya frecuencia



de 700 MHz se ha vuelto a retrasar, ya que estaba prevista para marzo y muchos auguran que no será antes de mayo.

Entre las obligaciones que previsiblemente incluirá la normativa para los operadores estarán desde efectuar análisis de riesgos 5G cada dos años, hasta realizar prácticas de seguridad de sus suministradores. También tendrán que implementar medidas técnicas y de organización para la gestión de riesgos y garantizar que adoptan procedimientos de supervisión seguros y tienen requisitos exigentes de acceso a los elementos y funciones de la red 5G. Por supuesto, la normativa obligará a los operadores a "analizar su dependencia en la cadena de suministros y elaborar e informar de la ejecución de una estrategia de diversificación de suministradores".

Esquema de Seguridad en 5G

Asimismo, se impondrá la obligación de enviar al **Mº de Asuntos Económicos y Transformación Digital** los resultados del análisis de riesgo que realicen y que cumplan con las obligaciones de la normativa.

Tras aprobarse la Ley, el **Gobierno** deberá poner en marcha el llamado **Esquema de Seguridad 5G**, con los informes de riesgos facilitados por los operadores y las medidas que se implementen para reducirlos. Por supuesto los operadores, además de estar obligados al mantenimiento seguro de las credenciales de usuario para el acceso a la red, entre otros aspectos, estarán sujetos a los esquemas europeos de certificación de productos y controles que se impongan para garantizar la ciberseguridad de las redes 5G en el Viejo Continente.



¿Está su organización preparada para un ataque?

SERVICIOS DE RED TEAM

Los servicios avanzados de Red Team (RTS) de Cipher utilizan docenas de herramientas y sistemas propios para emular las mismas Técnicas, Tácticas y Procedimientos (TTPs) que utilizan los adversarios en ataques reales. Comprobando no sólo las debilidades, sino realizando una evaluación en profundidad del ciclo dinámico de protección, detección y respuesta de la organización ante un ataque sofisticado.

OTROS SERVICIOS AVANZADOS

Pentesting de Entornos Cloud

Análisis de Directorio Activo

Portal de Vulnerabilidades

Respuesta Ante Incidentes



ENTELGY INNOTECH SECURITY, *partner* de la solución Carla del CCN-CERT para compartir datos de forma segura

Entelgy Innotech Security ha sido una de las tres primeras entidades en superar el procedimiento establecido por el Centro Criptológico Nacional (CCN) para obtener la certificación de su herramienta Carla, convirtiéndose



así en *partner* certificado. Carla es una solución de protección centrada en los datos, que permite que

Entelgy Innotech

la información corporativa viaje protegida y bajo control en todo momento, minimiza la posibilidad de fugas de datos aumentando el control de la organización sobre los mismos más allá de las defensas de protección perimetrales. Esta herramienta permite consultar, gracias

a su completa auditoría de acceso a la información, quién ha accedido a un documento, con qué permisos, así como monitorizar intentos de acceso bloqueados.

Por otro lado, el equipo de *hacking* de Entelgy Innotech ha descubierto una vulnerabilidad en ProjectSend, un software gratuito para compartir archivos con los clientes desde un propio servidor. La CVE-2020-28874, identificativo con la que ha sido registrada, se sitúa en el componente de establecimiento de contraseñas de este software de compartición de archivos.

El descubrimiento ha sido realizado por el auditor de la compañía, Ricardo Pelaz. La vulnerabilidad podría provocar que un atacante pueda cambiar la contraseña de cualquier usuario conocido por su nombre de usuario, como admin, sin un *token* válido.

BREVES

■ La compañía **Tecnobit-Grupo Oesía** protegerá el servicio restringido (PRS) del sistema de navegación por satélite europeo Galileo en el marco del proyecto **Geode**, que busca potenciar el uso del servicio PRS del mencionado sistema satelital en diferentes escenarios operativos, tanto en defensa como en otros entornos gubernamentales. Esta iniciativa forma parte de la primera convocatoria del 'Programa Europeo de Desarrollo Industrial de la Defensa' (Edidp) para desarrollar las capacidades del receptor de navegación de Galileo PRS europeo estandarizado.

■ **Fujitsu y Logality** han firmado un acuerdo de colaboración con el objetivo de liderar el mercado en materia de Servicios de Interposición que habiliten la evolución digital de las empresas. Este acuerdo tiene como objetivo el desarrollo y comercialización conjunto de soluciones personalizadas según las necesidades de los clientes, con servicios de Contratación Electrónica, Comunicación Electrónica e Identificación Digital.

■ Un año más, la gallega **Tarlogic** forma parte del *ránking* con las mil empresas europeas de mayor crecimiento que elabora el **Financial Times** cada año. En esta nueva edición ha ocupado el puesto 829. De hecho, es la única compañía española del sector de ciberseguridad que figura este año en el 'Top 1000'. Entre los clientes de Tarlogic, con más de 70 empleados, están la mayoría de las empresas del Ibex 35, entre otros clientes de referencia.

■ **Autek Ingeniería y Tecnobit-Grupo Oesía** han firmado un acuerdo de colaboración en comunicaciones seguras para plataformas embarcadas de ámbito militar. Con él, suman capacidades y experiencia para desarrollar soluciones *cross-domain* para el sector de Defensa. En la actualidad, España carece de los equipos militares de condiciones especiales de entorno con soluciones *cross-domain*, que permitan el intercambio seguro de información con el grado de seguridad NATO SECRET en misiones OTAN o bien el equivalente de RESERVADO en operaciones nacionales. Gracias a esta alianza ambas organizaciones trabajarán, de forma conjunta, en el diseño, desarrollo y producción de este tipo de soluciones militares.

■ El **Ministerio de Igualdad** ha encargado a la sociedad pública **Ineco** (Ingeniería y Economía del Transporte) las labores de apoyo a la división TIC del departamento, entre las que también figura su ciberseguridad. En concreto, el contrato, cuyo valor ronda los 700.000 euros (para 2021 y 2022), incluye servicios relacionados con la seguridad de la información, así como el desarrollo de la sede electrónica y otros servicios de administración digital, entre ellos el alojamiento en la nube.

■ **Syneto**, fabricante europeo de soluciones de hiperconvergencia y seguridad avanzada del dato, ha desembarcado en España abriendo su primera oficina. Así, la compañía acelera su presencia en el mercado ibérico, donde estaba presente de la mano de su mayorista **Esprinet**. La compañía ha apostado por la creación de un equipo local de gran experiencia en el sector TIC, liderado por **Matteo Restelli** como Country Manager, **Eduardo García Sancho** como Sales & Channel Manager y **Andrés Cabarcos**, Technical & Presales Manager.

VERSIA apuesta por los servicios de ciberseguridad creando su nueva marca CYBER SHIELD

Versia Cyber Shield es la apuesta de la compañía vasca **Versia**, con más de 30 años de trayectoria en el sector TIC, la digitalización y la innovación, para ampliar su negocio en el entorno de la ciberprotección y cubrir las necesidades de las empresas que están en procesos de transformación digital.

Versia Cyber Shield nace así con un Equipo de Respuesta a Incidentes de Seguridad (CSIRT) que opera en las oficinas de Baracaldo (Vizcaya), donde tiene su sede. Cuenta, además, con un DSOC (*Defense and Security Operation Center*) donde trabaja su equipo de respuesta, siendo miembro de pleno derecho de FIRST y aspira a obtener el sello de TF-CSIRT y Csirt.es.

Al frente de la nueva empresa estará **Eder San Millán** como Director, junto a **Andoni Alcalde**, como Managed Security Services Manager, y **Miguel Tubía** como Cybercrime & Threat Intelligence Manager.

Su portafolio inicial se divide en cinco grandes líneas: Security Assessments, Managed Security Services, Defense SOC, Threat Intelligence y Cybercrime investigation. "Tenemos un plan ambicioso y queremos posicionarnos como referentes en áreas muy concretas, como la seguridad en entornos en la nube o la analítica forense digital", comenta San Millán a SIC. "Es fundamental ofrecer servicios basados en la calidad, objetividad e integridad a través de la cercanía hacia nuestros clientes". Así pues, la propuesta de valor será "multisectorial dentro del ámbito nacional sin descartar, a medio plazo, poder llegar a otro tipo de mercados fuera de España. Nacemos con una orientación pura de servicios y muy apalancada en grandes alianzas con *partners* estratégicos", añade.

Para ello, "hemos comenzado la actividad con un equipo de cinco analistas más el que opera el SOC, con intención de duplicar esta plantilla para



De izq a dcha: Miguel Tubía, Eder San Millán y Andoni Alcalde

finales de 2021 e, incluso, volver a duplicarla a lo largo del ejercicio próximo", concluye el directivo.

La compañía busca "consolidar en una empresa lo que hasta ahora veníamos haciendo dentro de una división. Es una apuesta por un negocio creciente que necesita una estructura autónoma, con un plan estratégico para abordar los servicios, soluciones y productos que está requiriendo y va a requerir el mercado, y aprovechando las sinergias con el resto de áreas de conocimiento de Versia", explica su presidente **Manuel Mosteiro**.



Your security, our expertise.

BOTECH amplía los servicios de su tecnología ISOPH.

Nuestras soluciones ayudan a prevenir el ransomware.



ISOPH
COMMUNITY

ISOPH COMMUNITY

Cierra los agujeros de seguridad de mayor impacto y vacúnate contra el ransomware.



ISOPH
PRO

ISOPH PRO

Pentesting, Gestión de Vulnerabilidades y Auditoría orientada a MITRE ATT&CK.



ISOPH
DNS

ISOPH DNS

Navega de forma segura gracias a la Inteligencia avanzada de BOTECH.



ISOPH
VULNERABILITY

ISOPH VULNERABILITY

Monitorización continua de vulnerabilidades y recepción periódica de informes.



ISOPH
FIM

ISOPH FIM

Tecnología que vigila y atestigua qué modificaciones se han realizado en tus ficheros y quién las ha realizado.



ISOPH
MOBILE

ISOPH MOBILE

Aplicación que analiza los dispositivos en busca de evidencias que ayudan a conocer si están o han estado comprometidos.

Prueba ISOPH Community

Accede a nuestra web y descárgate gratis el software.



SCAN ME

TREND MICRO refuerza sus alianzas con MNEMO y GRUPO CMC para potenciar sus servicios

Trend Micro y Mnemo han firmado una nueva alianza, ampliando su colaboración de los últimos años para ayudar a sus clientes en la protección de sus entornos de *cloud* híbrida. Como parte de la estrategia de Mnemo de posicionarse como referente en seguridad *cloud* en España y Latinoamérica, y con el objetivo de dar respuesta a los nuevos retos de ciberseguridad en el mundo digital incorporando la innovación "orientada a resultados" como principal eje, la compañía española también ha puesto en marcha recientemente Mnemo Innovate. Esta nueva división de negocio permite a la firma ampliar su portafolio de servicios a clientes en las áreas de estrategia, *cloud* y *data security*. La firma, que cuenta con un equipo de arquitectos de seguridad de nube, ha seleccionado la plataforma Cloud One de Trend Micro para la protección de entornos complejos y heterogéneos (híbridos y multi-nube).

Alianza con Grupo CMC

Por otro lado, el desarrollador de origen nipón también ha ampliado su acuerdo de colaboración techno-

lógica con la española **Grupo CMC** para ofrecer a sus clientes nuevos servicios de seguridad para la nube híbrida y soluciones de protección de entornos industriales (OT) e Internet de las Cosas (IoT). Con este acuerdo, formalizado a través de la Unidad de Ciberseguridad y Protección del Dato del Grupo CMC, responden a la creciente necesidad de protección en estos entornos. Cabe recordar que, durante el pasado año 2020, el 57% de las empresas españolas sufrieron un incidente de seguridad en la nube pública y este porcentaje se eleva hasta el 70% a nivel global. Además, a través de la nueva colaboración, Grupo CMC utilizará las soluciones Trend Micro Cloud One y TXOne Networks, que se suman a Apex One, Deep Security y Apex Central, de las que ya ha venido haciendo uso.

Finalmente, Trend Micro también anunció un acuerdo con **Nuffield Health**, una organización benéfica de referencia en el sector de la salud con una amplia infraestructura de TI distribuida alrededor de 300 centros y a la que dará protección a través de la nueva plataforma Trend Micro Vision One.



MNEMO



INETUM consigue la categoría Platinum como socio de FORCEPOINT

Inetum ha logrado obtener el máximo nivel de *partenariado* que otorga la compañía estadounidense, **Forcepoint**. Un reconocimiento que "demuestra la capacidad que Inetum tiene para afrontar proyectos de la mano de las soluciones de Forcepoint. Es, además, un indicador clave para los clientes sobre el conocimiento y experiencia de Inetum y sobre su capacidad de reacción ante incidencias", destacó el Head of Cybersecurity Alliance de Inetum en España, **Ricardo Gaspar**. Para Inetum, haber alcanzado el nivel *platinum* con Forcepoint es un logro que "nos distingue del resto de nuestros competidores, al demostrar solvencia en proyectos de



seguridad. Solo hay dos empresas españolas con este alto nivel de capacidad en soluciones Forcepoint", añadió.

Forcepoint tiene un portafolio de ciberseguridad muy especializado y enfocado en áreas en las que Inetum es fuerte y mantiene una posición consolidada. Para ello, busca ofrecer las mejores soluciones fomentando entornos seguros y de confianza. Unos objetivos que comparten con Inetum, que proporciona servicios y soluciones digitales y un grupo global para ayudar a las compañías e instituciones a aprovechar al máximo el *flow digital*. El Grupo está en más de 26 países con más 27.000 empleados.

NOMBRAMIENTOS



● **Daniel Puente** se ha incorporado a **CIRSA** como CISO, tras haber trabajado previamente como tal en Wolters Kluwer España. Cuenta con certificaciones como OSCP, BSI Lead Auditor 22301 CRISC, y ha desempeñado diferentes roles de responsabilidad en la Universidad Autónoma de Barcelona, ASPY Prevención o Cima, entre otras entidades.



● **CriteriaCaixa** ha contratado a **Daniel Moll** como CISO. Este profesional cuenta con varias titulaciones en Informática y un Máster en Administración de Empresas por el EADA. Ha trabajado para compañías como Evolium, Innevis y CIRSA, de la que venía siendo CISO desde 2014.



● **Javier Pinillos** ha sido nombrado Global CISO del **Grupo Parques Reunidos**, que gestiona más de 60 parques a nivel mundial. Entre sus propósitos, tiene la labor de definir e implementar la estrategia del grupo, así como armonizar la Seguridad de la Información de los diferentes países. Cuenta con más de 20 años de experiencia en el área de Seguridad de la Información, tanto en empresas de consultoría como en cliente final. Es Ingeniero en Informática y cuenta con un MBA.



● Actual vicepresidente de **Isaca Chapter Madrid** y Presidente de Aesyc, **Pablo Blanco** ha comenzado en **Grupo Caminos** como Gerente de Seguridad de la Información. Hasta ahora, ocupaba el cargo de Gerente IT GRC en Sareb, además de haber trabajado para Eulen Seguridad, KPMG y Esa Security, entre otras. Cuenta con sendos Máster en Auditoría de Sistemas por la Politécnica de Madrid, y de Dirección y Gestión de la Seguridad de la Información por la Pontificia de Salamanca. Además, posee el título de Director de Seguridad por la UNED, entre otras titulaciones.



● **Grupo Enel** ha promocionado a **David Villalba** a Responsable de Seguridad de las Infraestructuras. Con casi una década de experiencia en el sector, es licenciado en Matemáticas y Computación por la Complutense de Madrid y lleva más de 10 años en la compañía, aunque ha trabajado también en Endesa y la Universidad Europea.



● **Juan Santonja** ha sido reconocido y promocionado en **Sabis** a Responsable de Gestión de Riesgos TI, Vulnerabilidades y Auditoría, donde hasta ahora era Audit and Security Operations Control Manager. Santonja ha trabajado para entidades como Banco Sabadell, Caja Mediterráneo y la Universidad de Alicante, además de participar como instructor para Isaca Barcelona. Es ingeniero de Informática y cuenta con un Máster en Ciberseguridad por la Universidad de Alicante.



● La **Fundación para el Desarrollo y la Innovación Tecnológica (Funditec)** ha asignado la Dirección General desde este mes de abril a **Miguel Rego**. Con una amplia experiencia en el sector, ha sido Vicepresidente de Defensa y Seguridad Nacional en ElevenPaths, CEO de iHack-Labs, miembro del Consejo de Ciberseguridad y Director de INCIBE. Es oficial de Intendencia de la Armada y cuenta con un Master en Auditoría de Sistemas por la Politécnica de Madrid, entre otras titulaciones.



ARROW

Potencie y proteja el trabajo desde cualquier lugar con Fortinet y Microsoft

FORTINET

 Microsoft

Contáctenos: arrow.com/ecs/es • fortinet.ecs.es@arrow.com • cloudteam.ecs.es@arrow.com

NETSKOPE y MIMECAST colaboran para ofrecer DLP omnicanal y seguridad en la nube

Netskope y **Mimecast** han sumado fuerzas a través de varias integraciones estratégicas diseñadas para ofrecer a los clientes una solución de prevención de pérdida de datos (DLP) omnicanal corporativa, “combinada con inteligencia robusta para proteger los recursos y el uso de la nube y la web, ya sea SaaS directo a Internet, web o correo electrónico”, destacan ambas compañías.



nazas (ATP), Cloud Access Security Broker (CASB), Prevención de Pérdida de Datos (DLP) y Gateway de Correo Electrónico Seguro (SEG), perfectamente implementadas y que se coordinen entre sí en un entorno de nube nativo”.

A través de este acuerdo esperan que los clientes pueden aprovechar su solución DLP omnicanal para gestionar y proteger

completamente el correo-e entrante y saliente, utilizando la inspección de Netskope y el análisis de Mimecast, bloqueando el correo electrónico sospechoso y el contenido sensible basado en etiquetas DLP hasta apostar por Netskope Cloud Threat Exchange, creado para descubrir y mejorar las posturas de prevención y riesgo, entre otras capacidades.

DOTFORCE trae a España la plataforma de CORELIGHT de detección y anticipación a ciberataques

El mayorista **DotForce** ha firmado un acuerdo con **Corelight**, proveedor de una plataforma de código abierto de detección y respuesta en la red



(NDR), para desarrollar, implementar y dar soporte a sus soluciones a través de los canales de distribución de la compañía en Italia, España y



Portugal. Para ello, DotForce seleccionará *partners* centrados en ciberseguridad y con amplio conocimiento en servicios de protección en la red y en el SOC, además de llevar a cabo campañas de ventas y marketing para crear nuevas oportuni-

des para sus socios, capacitándoles y facilitándoles las herramientas que necesitan para llevar a cabo demostraciones, Pruebas de Concepto (POC) e implementaciones de producción de las soluciones de Corelight.

“Nuestra experiencia ha demostrado que los MSSP y los integradores de sistemas buscan soluciones NDR potentes pero asequibles que se integren fácil y rápidamente con sus ofertas de servicios. Corelight se basa en **Zeek** y **Suricata**, con los que la mayoría de los MSSP ya están familiarizados. La plataforma *multi-tenant* de Corelight brinda a los proveedores de servicios la capacidad de implementar servicios NDR rápidamente, con resultados inmediatos y excelentes retornos de inversión”, ha destacado el CEO de DotForce España, **Zane Ryan**.

NOMBRAMIENTOS



● **Ángel Luis Sánchez Aristi** ha sido designado Director General de la nueva **Dirección de Digitalización e Inteligencia Artificial**, del **Ministerio de Asuntos Económicos y Transformación Digital**. Licenciado en Ciencias Económicas y Empresariales por la Universidad Autónoma de Madrid (UAM) y con un MBA por la Universidad de Chicago, comenzó su trayectoria profesional en el ámbito financiero en 1985. Hasta enero de 2017, ocupó diversos cargos con diferente responsabilidad en Dresdner Bank, Banco Exterior de España, Argentaria y BBVA. Actualmente, también imparte clases en la UNED sobre Transformación Digital y Big Data.



● **María Jesús Almazor** ha sido nombrada Consejera Delegada del negocio de Ciberseguridad y Cloud de **Telefónica Tech**. **Rames Sarwat** ha sido ascendido a Offnet Markets Sales Director en dicha división y **Gonzalo Fernández** ocupará el puesto CTO de la división de Ciberseguridad de la compañía. Además, **David Prieto**,



responsable de Riesgo y Cumplimiento, Identidad y Servicios Antifraude de ElevenPaths, se ocupará de dirigir el Centro de Ciberseguridad abierto por la empresa en Valencia. Ingeniera por la Politécnica de Cataluña, Almazor ha pasado toda su trayectoria profesional en Telefónica donde comenzó en 1996. Sarwat ha trabajado en Microsoft, NCR, Smart Acces y fue Vicepresidente de Aslan, entre otras entidades. Fernández es Ingeniero Informático por la Universidad de Valladolid y ha trabajado para Ceas, Software Factory Deusto y Telefónica, en la que lleva dos décadas. Finalmente, Prieto, ingeniero de Telecomunicaciones, cuenta con más de 15 años de experiencia y ha sido Responsable Global MSSP de productos de marketing de la operadora.



● **Iván del Amo** ha sido promocionado por **Prosegur** a Director del SOC en España. Del Amo cuenta con el Grado de Ingeniería en Sistemas de Información, así como varios Máster en Auditoría, y ha trabajado, entre otras, para Cipher, Sothis, Prosegur y Eulen.



● **Microsoft** ha promocionado a **Pablo Vera** como Sr. Sales Manager Cybersecurity Solutions. Ingeniero de Telecomunicaciones por la Politécnica de Madrid, con amplia experiencia en el sector, ha trabajado para Symantec, FireEye, McAfee y Network General, entre otras. Cuenta con formación específica en gestión empresarial por el IESE de Navarra y de gestión de riesgos por la Universidad de Harvard.

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

STORMSHIELD y LOGPOINT trabajan juntos para mejorar la visibilidad de los eventos de red

Stormshield y **LogPoint**, centrada en soluciones de gestión de eventos e información de seguridad, han firmado un acuerdo tecnológico que permitirá a la primera "ofrecer soluciones mejoradas para garantizar la visibilidad

y la seguridad de las infraestructuras operativas y de TI, con el lanzamiento de Stormshield Log Supervisor (SLS), una nueva solución de gestión de registros para los cortafuegos de su Network Security".

Con esta nueva tecnología los clientes podrán aprovechar las capacidades de recopilación, organización y almacenamiento de registros de la solución LogPoint, optimizada para los productos Stormshield Network Security (SNS). Esto les proporcionará una mejor visibilidad de sus redes e infraestructuras de seguridad a través de cuadros de mando generales y de-

tallados que proporcionan una visión rápida del estado y de los eventos del cortafuegos, búsquedas multicriterio a través de los registros de SNS.

Universidad Castilla-La Mancha

En paralelo, la **Escuela Superior de Ingeniería Informática (ESII)** de la **Universidad de Castilla-La Mancha (UCLM)** ha cerrado un acuerdo con Stormshield para organizar, de manera independiente, cursos de certificación para la formación de profesores, alumnos y profesionales de la industria.

La alianza abarca también la utilización por parte de los usuarios de la universidad de *appliances* virtuales Elastic Virtual Appliance (EVA), que Stormshield cede con fines educativos.



NOMBRAMIENTOS



● **Vicente Gonzalez Pedrós** se ha incorporado a la **Agencia Europea de Ciberseguridad (ENISA)** como Experto en Ciberprotección. Con casi dos décadas de trayectoria en Isdefe (los tres últimos años dedicados a ciberdefensa), también ha trabajado en entidades como Ibermática y Alten, entre otras. Es licenciado en Informática por la Pontificia de Salamanca, entre otras titulaciones.

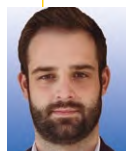


● **Capital Group** ha fichado a **Marta Zárraga** como Directora Global de Información para supervisar la tecnología y la ciberseguridad de la firma. Zárraga acumula 25 años de experiencia en el sector.

Previamente, ocupó el cargo de Directora General de Información de Aviva. Además, fue directora de Información en Vodafone y British Telecom. Respecto a su formación, tiene un máster en ingeniería informática por la Universidad de Deusto (España).



● **Zerolynx** ha designado a **David Jiménez**, socio de la compañía, la dirección de los Servicios de Seguridad en Cloud, extendiendo su dirección del área de Ciberdefensa. **Diego León**, también socio, tomará la responsabilidad de cumplir con el



plan estratégico de internacionalización, manteniendo la dirección del área de Seguridad Ofensiva. Otro de sus socios, **Jesús Alcalde**, ha sumado a su cartera de Innovación la nueva línea de Gaming & eSports, con la que se busca traer al mercado servicios disruptivos. Junto a esta labor, continuará liderando el área de Seguridad en Desarrollo. Y **Sergio Gutiérrez** ha sido promocionado al equipo de Management de Zerolynx, como Gerente de Proyectos



● **Roberto Fañanás** ha sido nombrado Information Assurance Officer en la **Agencia Europea del GNSS**, encargada de garantizar la correcta defensa y representación de los intereses públicos esenciales en los programas de navegación GPS de la UE. Ingeniero por la Politécnica de Madrid, Fañanás ha desempeñado diferentes roles de responsabilidad en Entelgy Innotec, VeriForce, Spire Payments, la Armada y la OTAN.

SOTHIS impulsa junto a TELEFÓNICA, SAP e HIBERUS la transformación digital, de forma segura, de GRUPO JORGE

Grupo Jorge cerró un acuerdo con **Sothis**, **Telefónica**, **SAP España** e **Hiberus** para abordar su plan de transformación digital con la solución SAP S/4HANA Meat&Fish Management. La compañía, presente en el sector cárnico, cuenta con una larga trayectoria y en los últimos años ha experimentado un gran crecimiento, especialmente en los mercados internacionales.

Para acompañarlo, el grupo va a implementar el software SAP S/4HANA como sistema de gestión empresarial que ordenará y unificará la forma de trabajo de su plantilla, con más de 5.000 empleados. Sus exportaciones suponen ya



el 75% de sus ingresos que, en 2020, superaron los 1.400 millones de euros. La transformación digital se realizará a lo largo de este año y el que viene ya que se enmarca dentro de una estrategia a medio y largo plazo. El objetivo es conseguir mayor flexibilidad en el uso de las aplicaciones y en el funcionamiento de las soluciones que sean vitales para el negocio, además de mejorar la seguridad del sistema de cara a su transformación hacia un sistema orientado a la nube y a un entorno hiperconectado.

Por otro lado, Sothis también ha anunciado que ha implementado la tecnología de **Nutanix** para optimizar su infraestructura tecnológica.

CIBERSEGURIDAD, UNA CUESTIÓN DE TIEMPO



EL INCIBE, MANDO CONJUNTO DEL CIBERESPACIO y CANTABRIA LABS eligen al GRUPO ICA para mejorar su ciberinteligencia y protección

Grupo ICA Sistemas y Seguridad ha continuado con su crecimiento en los últimos meses tras firmar con el **Instituto Nacional de Ciberseguridad de España (Incibe)**, en lo

que ha denominado como “el mayor contrato de Inteligencia de Amenazas de España”. En concreto, la unidad especializada en Ciberseguridad del Grupo se hará cargo del servicio de información de ciberamenazas relacionadas con el compromiso de usuarios, el de información de URLs maliciosas y el servicio especializado de análisis e información de inteligencia de ciberseguridad y cibercrimen del Instituto. Además, el Incibe contará con la plataforma de *Threat Intelligence* de **Recorded Future**, que es socio de la compañía en España. También proporcionará, a través de dicha plataforma, Inteligencia de Ciberamenazas al **Mando Conjunto del Ciberespacio**. Un aspecto que la unidad militar considera vital por cuanto le permite “contar con *insights* y conocimiento para prevenir y proteger las redes y sistemas CIS del **Ministerio de Defensa** de ciberataques”. ICA suma así a nuevos clientes en esta área de negocio en la



que cuenta, entre otros, con el **Ministerio de la Presidencia**.

Cantabria Labs

Además, **Cantabria Labs** ha elegido a ICA

Sistemas y Seguridad para proteger su infraestructura TI mediante el servicio avanzando de Ciberseguridad 360: desde la monitorización de incidentes de seguridad a la contención de las amenazas. Además, Cantabria Labs contará con la plataforma SIEM Next Generation, de la que ICA Sistemas y Seguridad es fabricante, y que cuenta con estándares de calidad y seguridad por parte de *Common Criteria* y del **Centro Criptológico Nacional**.

Los servicios se prestarán desde el CiberSOC de la compañía, certificado en ISO 27000, ISO 20000, Esquema Nacional de Seguridad en la Categoría Alta, así como el reconocimiento CERT, acreditado por la Universidad de **Carnegie Mellon**, siendo también miembro de los Foros de Respuesta ante Incidentes CSIRT.es, TF CSIRT y FIRST.



GOOGLE se alía con ALLIANZ y MUNICH RE para poner en marcha una póliza de ciberriesgos para la nube

Google Cloud, Allianz y Munich Re han decidido unirse para crear el denominado “Programa de protección contra riesgos” para los usuarios de Google Cloud y reducir el riesgo y los costes para los clientes. La iniciativa desarrollará una nueva herramienta de seguridad llamada Risk Manager para que las empresas tengan la capacidad



de medir y administrar su riesgo a través de Google Cloud y recibir informes sobre su madurez en ciberprotección, según han explicado los participantes en el acuerdo.

Disponer de estos informes permi-

tirá a las compañías acudir a Allianz y Munich Re facilitando la contratación de una ciberpóliza para trabajar en la nube de Google. En definitiva, “el objetivo del programa es ayudar a las empresas no solo a reducir el riesgo, sino a crear potencialmente un programa de gestión de riesgos más completo”, destacan los participantes en esta iniciativa. De momento, Risk Manager a está disponible en versión preliminar privada para clientes en los Estados Unidos, pero se irá ofreciendo a otras regiones del mundo para ayudar a las empresas que usan estos servicios a “construir un programa de gestión de riesgos más completo y facilitarles su camino en transformación digital”.

NOMBRAMIENTOS



● **Jose Antonio Lancharro** se ha incorporado al equipo de **Tarlogic** en calidad de Director Ejecutivo de **BlackArrow**, donde aportará la experiencia adquirida en materia de seguridad ofensiva, durante los últimos 15 años. Durante su carrera profesional, se ha especializado tanto en el desarrollo equipos de alto rendimiento como en la internacionalización de servicios de *pentesting*, *red teaming*, *threat hunting*, *blue teaming* y respuesta a incidentes. Durante su trayectoria profesional destaca tanto su participación como Director Técnico en Blueliv y como Senior Manager de Seguridad Ofensiva en EY.



● **SailPoint** ha elegido a **Heather Gantt-Evans** como su nueva CISO. Con amplia experiencia en ciberseguridad, Gantt-Evans ha trabajado para compañías como The Home Depot, EY y Booz Allen Hamilton, entre otras, tras haber ejercido como analista de inteligencia de amenazas en el Ejército de EE.UU.



● **Carlos Garcia** se ha incorporado a **IT Asseco Spain** como Director de Ciberseguridad y **Sergio Garcia Carranza** como BDM de Ciberseguridad. García, cuenta con una dilatada experiencia en el mundo del gobierno de la seguridad, el riesgo, el cumplimiento y la continuidad de negocio y ha pasado por diversas empresas como Bidaidea, Grupo INV, Everis y SIA, entre otras. García ha desempeñado diferentes roles en compañías como Wise Security, S21sec y Alhambra IT.



● **Albert Castellanos** ha entrado en **DPLL** como Socio en Privacidad y Ciberseguridad. Doctor en Derecho por la Autónoma de Barcelona, este profesional con amplia trayectoria profesional ha pasado por EY, Ecix, Crowe Spain e Icab, además de ser docente de la Oberta de Cataluña y la Universidad de Barcelona.



● **Ingenia** ha promocionado a **Carlos Cortés** a Director Adjunto de Ciberseguridad y Servicios Gestionados. Ingeniero de Telecomunicación por la Universidad de Málaga, cuenta con más de 15 años de experiencia en el sector TIC, desempeñando roles técnicos y de gestión en distintos países (España, UK, Chile, Perú) y ha trabajado para organizaciones como cxLoyalty, en su sede de Londres, y Libera Networks, donde fue Director de I+D.



● **Miguel García Menéndez** ha sido nombrado CEO de **Grupo Castroalonso**, al que “aportará su experiencia y pondrá en marcha ideas centradas en hacer crecer la cartera de clientes, consolidar y expandir la marca **BloomverTech** e internacionalizar la compañía”, destacan desde la empresa. Actual Vicepresidente de la iniciativa Arco Atlántico de Ciberseguridad y Entorno digital y de ETSI ISG E4P, es ingeniero en Informática por la Universidad de Oviedo y ha desempeñado diferentes roles de responsabilidad en organizaciones como CCI, Alastria Blockchain, iTi y ATI, entre otras.



● **Cipher**, compañía de Prosegur, ha fichado a **Rafael Cuenca** como Sales Manager. Licenciado en Sociología, cuenta con una gran experiencia en el sector en el que ha trabajado para compañías como Pulse Secure, Rohde & Schwarz, Palo Alto, RealSec y McAfee, entre otras.



www.novared.net

Innovación en CiberSeguridad

EXPERTOS EN CIBERSEGURIDAD

Para mitigar los riesgos de su negocio

**Soluciones
Cloud y
On Premises**

CSOC 7x24

Consultoría

Concienciación

www.comunixgroup.com
Escuela de Hacking Ético de Novared



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



BOTECH aterrizó en Norteamérica a través de BOTECH USA, donde operará con el nombre PHISHINGHUNTERS

Botech ha aterrizado en Estados Unidos con la creación de **Botech USA** y la apertura de su oficina en Miami, desde donde operará bajo el nombre comercial de **PhishingHunters**. A pesar de la crisis sanitaria, la compañía apuesta por la expansión internacional y da un paso importante para el desarrollo de su negocio, ofreciendo sus últimas soluciones de protección, ciberinteligencia y el fraude en el mercado americano. Este paso "responde al interés que tenemos por crecer en el país norteamericano y ofrecer nuestras soluciones de ciberseguridad a un mercado al cual es muy difícil acceder sino es con instalaciones *in situ*", explica su CEO, **Miguel Ángel Rojo**. Para esta iniciativa, la compañía



PhishingHunters



BOTECH

contará con su buque insignia, *PhishingHunters*, una solución que va más allá de la seguridad ante el *phishing*, ayudando a sus clientes a protegerse también de incidentes de *malware*, apps maliciosas, cuentas mulla, *cybersquatting* y fraude en tarjetas. Destaca por contener una de las bases de datos de *phishing* más grandes del mundo, con un almacenamiento de 2.500.000 de *phishing*. Utiliza *machine learning*, inteligencia artificial, análisis de *malware* y Big Data/Smart Data para identificar, "casi sin margen de error (99%)", según la compañía, los dominios causantes de las estafas cibernéticas. Se trata de un tipo de servicio orientado a la banca, que ahora puede aplicarse en cualquier sector.

Nace WALLIX INSIDE para impulsar la protección de identidades y accesos bajo el concepto de 'seguridad por diseño'

Wallix, especializada en software de seguridad de acceso e identidad, tiene nueva marca, **Wallix Inside**. Basada en el concepto de 'seguridad por diseño', ofrece a los fabricantes la posibilidad de integrar en sus propias soluciones y productos toda la tecnología de seguridad de acceso e identidad de la compañía. De esta forma, los fabricantes y proveedores tecnológicos podrán mejorar el valor sus propuestas y ofrecer a sus clien-

Nuevas alianzas y sectores

Wallix Inside se basa en un modelo de venta OEM (*Original Equipment Manufacturer*), lo que supone una importante novedad para la compañía, ya que les permite llegar a un mercado más amplio. "Recientemente, hemos entrado así en el sector industrial con nuestro *partner Fives*, pero nuestro objetivo es llegar a otros entornos como el sanitario sanitaria, el *smartbuilding* o a las cadenas de suministro", añade Marcos.

De esta forma, el reciente anuncio de la colaboración con el proveedor francés ayudará a los fabricantes, industrias y maquinaria industrial, a reforzar y tener acceso a sistemas de ciberseguridad y protección de datos en su digitalización. A su vez, Fives ha reconocido a Wallix como "el único fabricante actualmente en el mercado capaz de ofrecer soluciones que se integran directamente con su herramienta Fives CortX Gateway, algo que ha sido clave para la alianza", destaca la compañía.

WALLIX
INSIDE

tes herramientas digitales más seguras y alineadas con la protección de datos, al incorporar la ciberseguridad desde la etapa de diseño.

"El trabajo conjunto de los equipos de I+D y marketing de Wallix ha permitido crear un portafolio de soluciones que es muy sencillo de integrar en todos los clientes y con costes de desarrollo controlados", afirma **Jorge Marcos**, PEDM Unit Manager de Wallix.

NOMBRAMIENTOS



● **Alexandre Tovar** ha sido designado Channel Account Manager de **Trend Micro**. Su rol principal será potenciar la estrategia de canal ayudando a los *partners* a desarrollar negocio con una aproximación a la seguridad por diseño. Con más de 15 años de experiencia en compañías como Abast, Everis e IPM, conoce y ha cubierto todo el ciclo de vida de servicios y productos, incluyendo la venta. Los últimos tres años, en IPM, los dedicó a la creación de una unidad de Ciberseguridad. Es Sociólogo por la Universidad de Barcelona.



● **Dynatrace** ha fichado a **Gabriel Agatiello** como Senior Security Sales Executive, tras casi una década en Cisco como especialista de ciberseguridad. Entre otras, ha trabajado para Trend Micro, Tecnom, Softnet Logicalis. Agatiello está titulado en Electrónica y Comunicaciones y también tiene la certificación CISSP.



● **Carlos Fernández** ha sido nombrado Global Head International Sales & Business Development en el **Grupo SIA**. Con amplia experiencia en el sector de la protección, Fernández ha trabajado para compañías como Minsait, BT, Symantec, IBM y Codere, entre otras.



● **WatchGuard** ha nombrado a **Miguel Carrero** Vicepresidente de Cuentas Estratégicas. Se responsabilizará del crecimiento y la expansión global de la compañía para dirigirse, incorporar y gestionar alianzas con compañías estratégicas, incluyendo proveedores de servicios de seguridad gestionada (MSSP). Cuenta con más de 20 años de experiencia ejecutiva en compañías como Mobileum, Siemplify y Hewlett Packard, entre otras.



● **B2BRouter** contará con **Sergio Ruiz Mahillo** como Country Manager para el desarrollo del mercado en España. Con amplia experiencia en el sector de desarrollos tecnológicos y, especialmente, la implantación de la facturación electrónica, ha desarrollado proyectos para la digitalización en España como CERES, además de liderar otras iniciativas como la Plataforma @firma y CODICE. También, colabora en grupos de trabajo de la red Peppol, entidad europea para la contratación pública electrónica.



● **Ovanes Mikhaylov** ha sido fichado por **VMRay** como Business Development Manager para el Sur de Europa. Con anterioridad, fue Managing Director en SMARTII Internacional Business Development Agency, además de trabajar para Kaspersky Lab, VDEL y Deutsche Telekom AG, entre otras, en cargos de responsabilidad. Es titulado en Economía y Marketing Internacional.



● **Carlos Muñoz Garrido** ha sido elegido Vicepresidente de Producto (CPO) de **Smart Protection**. Cuenta con una amplia experiencia en el sector, en el que ha trabajado para McAfee, Intel y Anyware Seguridad Informática, entre otras compañías. Cuenta con numerosas certificaciones como CISA, CRISC y CISSP.

A close-up of a hand clicking a keyboard key. From the point of contact, a bright, glowing burst of light and digital data (represented by binary code and colorful streaks) emanates, suggesting a cyber event or data transmission. The background is blurred, focusing on the hand and the digital effect.

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

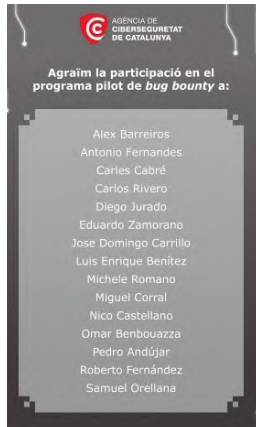
Confía



La AGENCIA DE CIBERSEGURIDAD DE CATALUÑA realiza una prueba piloto de un programa de 'pago por vulnerabilidades'

En coordinación con los **Departamentos de la Vicepresidencia y de Economía y Hacienda**, la **Agencia de Ciberseguridad de Cataluña** puso en marcha en febrero una prueba piloto pionera de un programa de 'pago por vulnerabilidades' (*bug bounty*) en la Administración, para el que contaron con el asesoramiento del especialista en este campo, **Antonio Fernandes**, entre otros participantes.

El objetivo de esta primera experiencia fue ver su eficacia en la administración pública catalana de cara a identificar vulnerabilidades en los sistemas de información y para prevenir posibles ataques. En concreto, los investigadores participantes, que lo hicieron de forma altruista, informaron de cinco vulnerabilidades: dos presentes en webs de la Generalitat y tres en aplica-



ciones corporativas, lo que ha permitido proceder a su verificación y resolución. El equipo de respuesta a incidentes **Catalonia-CERT** de la Agencia supervisó todo el desarrollo de la prueba piloto con la validación de las vulnerabilidades identificadas y la gestión de la solución para evitar posibles ataques.

Este tipo de iniciativas cada vez son más impulsadas en el sector público por países como EE.UU. que convocó su primer programa de *bug bounty* en 2016. En la **UE**, los Países Bajos fueron pioneros en 2013 y desde entonces Europa ha puesto en marcha varias iniciativas para detectar errores en el software abierto utilizado en sus instituciones. Según la lista CVE (*Common vulnerability and Exposure*), en 2019, los investigadores reportaron más 12.174 fallos.

ZIUR lanza una guía para la definición de la función de seguridad para las empresas industriales

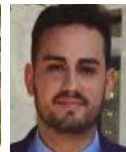
La fundación vasca **ZIUR**, en colaboración con **PwC**, presentó la 'Guía/Framework para la definición de la función de seguridad', para ayudar a las **empresas industriales** a definir su función de **ciberprotección** y alinearla con sus procesos productivos. El objetivo del documento es facilitar a las empresas aplicar criterios y políticas de ciberprotección adecuadas "en el nuevo escenario generado por los avances tecnológicos y las nuevas obligaciones y necesidades surgidas en el ámbito de la ciberseguridad". Y es que, desde Ziur recuerdan que la apuesta por todo tipo de nuevas tecnologías en estos entornos también ha supuesto un incremento del riesgo cibernético. A ello se suman, según la fundación, "las obligaciones impuestas



por el RD43/2021 a empresas de servicios esenciales y proveedores de servicios digitales", a la hora de proteger sus redes y sistemas de información, ya que, entre otras cuestiones, contempla la creación, en el plazo de **tres meses**, de la figura del CISO, cuya principal función es gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información.

En definitiva, propone unas pautas para que las empresas puedan identificar "los objetivos y expectativas en materia de ciberseguridad, así como las demandas que sus clientes o el mercado les pueda requerir al respecto y facilitarles una herramienta para poder definir la función de ciberseguridad en sus empresas", destacó el Director de la entidad, **Koldo Peciña**.

NOMBRAMIENTOS



● **Cipher** ha incorporado a **Ismael Moyano** y **Ángel Yegros**, como Service Manager y a Consultor GRC, respectivamente. Moyano, ingeniero técnico por la Politécnica de Madrid, ha tra-

bajado con antelación para Everis, FCC, Alma, Capgemini y Orange, entre otras. Por su parte, Yegros, también Ingeniero de Telecomunicaciones por la UPM, cuenta con el grado en Derecho y un Master en Derecho de las Telecomunicaciones y Protección de Datos y ha trabajado para Sidertia, Grupo Oesía y Cyberdata, entre otras.



● **S2 Grupo** ha potenciado su área de ventas en Madrid con la incorporación de **Gonzalo Quintero** como Senior Business Development Manager. Es ingeniero técnico en Informática con especialización y formación en ventas, desarrollo de negocio y liderazgo, cuenta con una dilatada trayectoria en el sector tecnológico y ha formado parte de empresas como Indra, Bull y Atos, entre otras.



● **RSA** ha promocionado a **David Pastor Pascual** nombrándole Enterprise Sales Executive. Con más de 10 años de trayectoria profesional, Pastor ha trabajado para compañías como Telefónica, Entelgy Innotec y Grupo Antea, entre otras. Es Ingeniero Técnico de Telecomunicaciones por la Politécnica de Madrid, donde también ha ejercido como profesor.



● **Palo Alto** ha apostado por **Tomás de Lara Aguilar** como District Sales Manager. De Lara, físico por la Complutense de Madrid, acredita una solvente trayectoria en la que ha sido General Manager de Trend Micro para Iberia, y con antelación ha trabajado para compañías como Secuware e Iecisa, entre otras.



● **Pcysys** ha designado a **Rodrigo Irala** como Sales Engineer para Iberia. Es Ingeniero en Sistemas de la Información por la Universidad de Alcalá de Henares. Llegó procedente de mayoristas como Exclusive Networks e Ireo, centrado en ciberseguridad. En su nuevo puesto será el encargado de la parte técnica para España y Portugal.



● **Jaime Maña** se ha incorporado a la israelí **ThinkCyber** como Senior Advisor. Con más de 25 años de experiencia en el mundo empresarial, tanto en España como en Latinoamérica y EE.UU., Maña ha trabajado para organizaciones como Grupo Atrium, Ntechcon y Zeb Consulting, entre otras.



● **Micro Focus** ha incorporado a **Jorge López Ranz** como Cybersecurity Sales. Ha desempeñado diferentes roles en BeyondTrust, Bitdefender, Core Networks, Thales España y Panda Security, entre otras. Es licenciado en Administración y Dirección de Empresas por la Carlos III de Madrid.

tu negocio siempre protegido

SERVICIOS GESTIONADOS **SOC/NOC 24x7** ADAPTADOS A TU NEGOCIO



Alerta Temprana



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.



Gestión de Vulnerabilidades

Identificación, evaluación y corrección de vulnerabilidades en tus sistemas de información y aplicaciones.



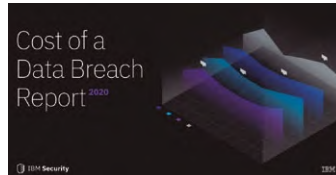
Control Continuous Endpoint

Servicio de detección y respuesta en el endpoint, clasificando tus aplicaciones para ejecutar únicamente lo que es lícito.

El sector sanitario registró en 2020 el mayor coste medio por brechas de datos, valorado en más de 5,9 millones de euros

En 2020, la Covid-19 fue una temática recurrente utilizada por los ciberdelincuentes para la obtención de información sensible de las empresas, a través de técnicas de *phishing*, *ransomware* o suplantación de identidad. Precisamente, en medio de este clima de ciberamenazas, llamó especialmente la atención los ataques contra el sector sanitario, uno de los más afectados, registrando el coste medio por brecha de datos más alto en comparación con otros sectores, valorado en más de 5,9 millones de euros. Lo que supone un incremento del 10% respecto a 2019, según el estudio de **IBM 'Data Breach Report'**.

El ataque más extendido consistía en el chantaje, pidiendo rescates económicos a cambio de volver a hacer accesibles los datos clínicos. El estudio destaca que la mitad de las causas de las brechas producidas en este sector corresponden a ataques malintencionados, frente a un 23% de fallos técnicos y un 27% de errores humanos.



Asimismo, el sector sanitario tardó, de media, 329 días en identificar y contener una brecha de datos, el mayor tiempo promedio en comparación con otras industrias. Además, se detectaron ataques contra la cadena de frío de las vacunas del coronavirus en todo el mundo, lo que destaca la importancia de mantener unos niveles altos de seguridad para la información más confidencial de las organizaciones e instituciones. El estudio de IBM también resalta que las credenciales comprometidas y los entornos en nube mal configurados fueron la causa de un 19% de las brechas de seguridad intencionadas, por lo que mejorar la seguridad en estos entornos es crucial en el escenario tecnológico actual.

Empresas españolas desarrollarán un controlador SDN nativo de la nube seguro para redes más allá de 5G en el proyecto europeo TERAFLow

El proyecto TeraFlow, financiado por la **Comisión Europea** dentro del Programa Horizonte 2020, comenzó el 1 de enero como parte de los proyectos de la Fase 3 de 5GPPP que trabajan en la 'Conectividad inteligente más allá del 5G'. Las tecnologías desarrolladas durante el proyecto, de 30 meses de duración, podrán ser usadas por operadores de telecomunicaciones, proveedores de nube de borde e hiperescala. Su objetivo será construir un nuevo tipo de controlador SDN nativo seguro en la nube que transformará drásticamente las redes Beyond 5G (B5G) al integrar los marcos actuales de **NFV** y **Mec**, y permitirá mejorar la gestión del flujo en la capa de servicio, además de la integración de equipos de redes ópticas o de microondas en de infraestructura. Además, prevé mejorar la seguridad de su controlador mediante el uso de aprendizaje automático (ML).

En un contexto en el que las redes

están aumentando exponencialmente debido a la implementación de 5G, y las próximas redes B5G, existe una necesidad latente de gestión de flujo masivo combinada con capacidades de automatización avanzadas, ya que la gestión humana y la operación de las redes se volverán más compleja. Para ayudar a ello, TeraFlow propone una arquitectura con altos niveles de confiabilidad, redundancia y seguridad construida sobre tres pilares principales: redes autónomas e integración de computación, *multi-tenancy* confiable, y ciberseguridad basada en ML.

El proyecto está coordinado por el **Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)** y reúne a otros 13 socios de ocho países con diferentes áreas de especialización, entre ellos, cuatro participantes españoles. **Telefónica I+D**, la **Politécnica de Madrid**, **Volta Networks** y **Atos**.



"EU-funded project TeraFlow to develop a novel and secure cloud-native SDN controller for beyond 5G networks"

NOMBRAMIENTOS



● **Bitdefender** ha incorporado a **Sergio Bravo** como Director de Ventas para la zona Oeste y a **Alfonso Gimeno** para la zona Este. Bravo cuenta con más de 20 años de experiencia en el sector

TI, donde ha sido Director de Canal para Iberia en Kaspersky, además de haber desempeñado cargos de responsabilidad en Hewlett Packard Enterprise, MicroStrategy o McAfee, entre otras. Por su parte, Gimeno ha sido Director de Ventas y Director General de la compañía OneSpan (antes Vasco Data Security) para Iberia. También ocupó distintos roles en Oracle, IBM y Lenovo. Ambos reportarán al Director Comercial de la compañía para el sur de Europa, Denis Valter Cassinerio.



● **Raquel Hernández** desempeñará el cargo de Regional Sales Manager en **Zscaler**. Ha trabajado para compañías como Gartner, Repsol y Hewlett Packard, entre otras. Es graduada en Administración de Empresas por la UNED e ingeniera industrial por la Universidad de Las Palmas.



● **CyberArk** ha fichado a **Karina Rojas** como Channel Sales Manager en España y Portugal. Será responsable del diseño y ejecución de la estrategia de Canal y la coordinación con los socios y mayoristas en Iberia, reportando a Carsten Wenzel, Channel Manager para el Oeste y Sur de Europa de la compañía. Con más de 15 años de experiencia en el ámbito de la ciberseguridad, Rojas es ingeniera de sistemas y ha trabajado para organizaciones como Cytomic/Panda, Tech Data, Westcon y Afina.



● **Siemens** contará con **Alejandro García Nieto** como Head of Business Excellence en Ciberseguridad. Licenciado en Administración de Empresas y Sistemas de Información, ha trabajado en los ámbitos de la ciberprotección para compañías como Sage, IBM, IT Deusto y PwC.



● **Karl Buffin** ha sido nombrado Vicepresidente de Ventas para las regiones de SEUR, CEUR y África por **XM Cyber**. Con más de 20 años de experiencia, Buffin ha desempeñado cargos de responsabilidad en diversas empresas de ciberprotección como Skybox Security, Logtrust, Symantec y Verisign. Cuenta con la titulación en Matemáticas y Ciencias, y un Master en Económicas.



● **Versia** ha designado a **Miguel Tubia** como Cybercrime & Threat Intelligence Manager, **Andoni**

Alcalde como Managed Security Services Manager y **Eder San Millán** como Director de Versia Cyber Shield. Tubia cuenta con 20 años de experiencia en el sector y ha trabajado en Symantec, EY e ITS Security. Participa, a través del Colegio de Ingenieros, como miembro del Comité de Privacidad CTN 320 de la UNE y del comité de ciberseguridad de AMETIC. Alcalde ha trabajado para Movistar, Panda Security, GFI y Versia, entre otras. Por su parte, San Millán lleva más de siete años vinculado a la ciberseguridad en empresas de sectores como el de distribución, banca, seguros y administración pública.



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



S2 GRUPO crece un 12%, ingresa en CYBASQUE y GAIA, y prevé un 2021 con más ciberataques por el teletrabajo y más ciberespionaje

La pandemia hizo que todas las predicciones de ciberseguridad de 2020 quedaran alejadas de la realidad debido a todos los cambios que surgieron, principalmente en entornos laborales, a raíz de este hecho. Por ello, desde **S2 Grupo** consideran que este año estará marcado por la decidida apuesta por el teletrabajo, "que se mantendrá", obligando a "reforzar la ciberseguridad tanto de las empresas, de los dispositivos personales y de los propios hogares, porque ahora aprovechar las brechas en este cam-

videoconferencias, Dropbox, mensajería, etc. Expertos de S2 Grupo han asegurado que al tratarse de herramientas básicas, se incrementa su exposición en todos los sentidos y puede, incluso, encontrarse venta de credenciales de Zoom en los mercados negros. No olvidan sus investigadores destacar que los criminales están usando el término 'covid' como un cebo para que los usuarios se descarguen código dañino, robar datos personales, etc.

De hecho, explican que se han detectado al día más de 1.500 dominios 'covid' maliciosos. En abril de 2020, Google bloqueó al día 18 millones de correos maliciosos relacionados con el término 'covid'. No olvidan la vigencia que tendrá el ciberespionaje, sobre todo, relacionado con las

vacunas e investigaciones sanitarias. Asimismo, S2 Grupo se ha unido a **Cybasque** (Asociación de Industrias de Ciberseguridad del País Vasco), y **GAIA** (Asociación de Industrias de Conocimiento y Tecnologías Aplicadas de Euskadi).

La compañía cerró 2020 incrementando su volumen de negocio en un 12%, con una facturación de 19,5 millones de euros e incrementando su plantilla en un 19%.



po es uno de los grandes objetivos de la ciberdelincuencia para ciberatacar a las organizaciones". En este sentido, la empresa valencia destaca que las infraestructuras críticas son todavía más críticas en situaciones de crisis debido, entre otros factores, a que se degrada la capacidad de respuesta al no estar físicamente, etc.

Además, ha recordado que otro de los objetivos directos de los ciberdelincuentes serán los sistemas de

NOMBRAMIENTOS



● **Entelgy Innotech Security** ha incorporado como Cybersecurity Director & OT Advisory Board a **Alejandro Villar**. Villar, que ha trabajado en compañías como Repsol, donde venía siendo CISO, cuenta con más de 20 años de experiencia en soluciones tecnológicas de ciberseguridad, incluida la de los sistemas de automatización industrial y la entrega operativa de servicios de TI/OT, así como en gestión de riesgos y gobernanza.



● **Raúl Benito** y **Carlos Payés** se han sumado a **SentinelOne** como Regional Sales Manager para Iberia y Sales Engineer, respectivamente. Benito está licenciado en Económicas por la Universidad de Alcalá de

Henares, y ha trabajado en Qualys, Trend Micro y Check Point en diferentes puestos de responsabilidad dentro del área comercial y del canal. Por su parte, Payés cuenta con una amplia experiencia en compañías como Mmemo y Qualys, entre otras.



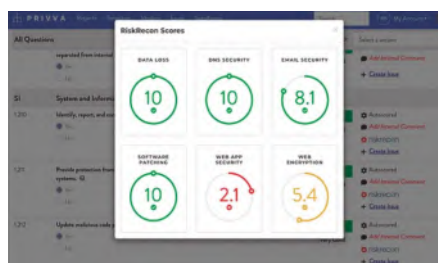
● **Nunsys** ha incorporado a **Maria José Montes**, **Carlos José Hernández** y **Fernando Moreno**, como Coordinadora de su

CyberSOC, Técnico especialista en Ciberseguridad y Analista Funcional, respectivamente. Montes es conferenciante y formadora en congresos técnicos españoles y ha trabajado para Eset, SVT Cloud, Quantika14 y Securizame, entre otras. Hernández cuenta con más de dos décadas de experiencia como Administrador de Sistemas en el Ministerio de Defensa. Moreno, licenciado por la Politécnica de Madrid, ha trabajado entre otras en Microsoft y Vignette y se incorpora al área de software dando apoyo al departamento de ciberseguridad y gobierno TIC.

RISKRECON monitoriza ya a cuatro millones de empresas y recomienda las 'calificaciones de riesgo' como medida para reducir posibles brechas de datos

La compañía de calificaciones de ciberseguridad, **RiskRecon**, de **Mastercard**, que cuenta con más de 3.400 clientes, ha superado ya la monitorización de cuatro millones de compañías en todo el mundo. Además, ha sumado a su programa de socios nuevos integrantes como **RSA Archer**, **Interos** e **Whitsic**. Además, **Privva** y **RiskRecon** ofrecen un sistema integral de riesgos para proveedores.

A este crecimiento también está contribuyendo las mejoras continuas que ha acometido en su plataforma para facilitar su uso y acceso a datos. En el primer trimestre, entre otros aspectos, ha implementado varias funcionalidades que permiten añadir empresas de forma simple a la cartera de clientes y socios, o consultar de forma más completa el perfil de TI —a través de más detalles sobre *hosts*, geolocalización, proveedores de *hosting* y dominios, etc—. A ello se suma que también ha añadido un nuevo criterio de seguridad: el de código malicioso, en el que hay incluidos todos los encontrados por la compañía en páginas webs de acceso público.



Calificación vs brechas de seguridad

RiskRecon también ha destacado la necesidad de que las compañías acometan un modelo de calificación de seguridad como el que ofrece para predecir, entre otros aspectos, la frecuencia de eventos de incumplimiento que se espera de las empresas, según su nivel de ciberprotección identificado. Así lo resalta en uno de sus últimos informes en el que consta que, por ejemplo, el sector financiero tiene más precisión para identi-

ficar y anticiparse a eventos que el educativo, tras analizar más de 45.000 empresas. Además, la compañía ha actualizado su plataforma para gestionar de forma más sencilla las suscripciones a RiskRecon, agregando un resumen de estas a la página de administración.

Por otro lado, la compañía ha publicado un estudio del impacto de ataques como el ocurrido contra la empresa **SolarWinds**, a finales de 2020, a través de su plataforma Orion, lo que puso en evidencia los riesgos que asumen las empresas al depender de terceros.

"Esta brecha brinda una oportunidad única para comprender cómo las organizaciones responden a una amenaza de alto perfil", resaltó a la vez que alertó de que, conforme a sus datos, "una gran mayoría de empresas no han tomado ninguna medida para abordar su exposición a SolarWinds", un aspecto preocupante dado que se estima que afectó a más de 15.000 organizaciones de todo el mundo.

M^o DE LA PRESIDENCIA: la apuesta por la Inteligencia Avanzada de Amenazas y los Servicios Gestionados

Mientras algunas organizaciones realizaban una gestión de la ciberseguridad tradicional, el Ministerio de la Presidencia (MPR) ha dado un paso al frente y ha innovado en su gestión de la ciberprotección. Junto a ICA Sistemas y Seguridad (ICA SyS), esta organización ha apostado por un cambio de paradigma en su seguridad informática con el objetivo de garantizar la disponibilidad de los servicios críticos que presta en la actualidad de cara a Internet, incluyendo páginas web, servicio de correo electrónico y accesos remotos.



Julián Hernández Vigliano / Alberto Cañadas Álvarez

ICA SyS, la unidad especializada en Ciberseguridad de Grupo ICA, ha analizado y diseñado a medida del MPR una solución, con el Servicio de Inteligencia Avanzada de Amenazas como base, que revoluciona el enfoque que su ciberseguridad había tenido hasta entonces, pasando de una estrategia reactiva a una proactiva y preventiva. Para una protección máxima del entorno del **Ministerio de la Presidencia**, el CiberSOC de ICA SyS combina servicios y plataformas de última generación para adaptarse a los constantes cambios que tienen lugar en el ámbito de la seguridad tecnológica, especialmente tras los nuevos escenarios generados por la Covid-19 y los cambios generados en la sociedad.

Por todo ello, se consideró estratégico el disponer de:

- Soporte en la toma de decisión estratégica, táctica y operativa del modelo de Ciberseguridad TIC.
- Diseño de la organización de Ciberseguridad dentro de Tecnologías TIC para afrontar nuevos retos.
- Priorización de actividades de ciberseguridad.
- Conocimiento de *scoring* de ciberseguridad de proveedores de servicios al Ministerio.
- Acceso a los analistas especializados en la gestión de la Ciberseguridad y CiberInteligencia.
- Acceso a toda la información de CiberInteligencia de **Recorded Future** (información recopilada y procesada desde 2009): vulnerabilidades, actores, TTPs, amenazas.

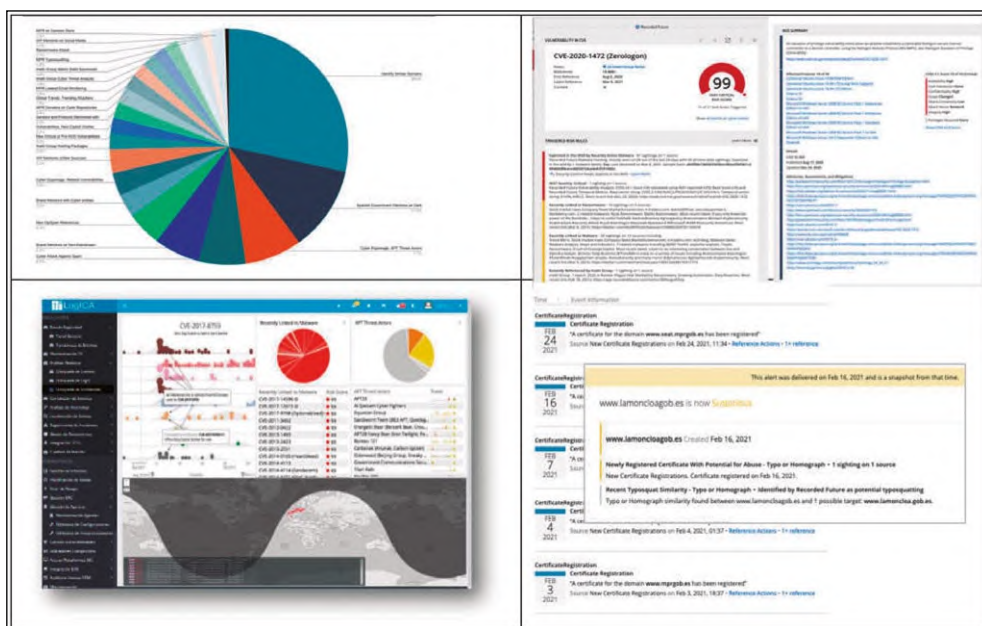
Detección proactiva de ciberamenazas

La solución de ICA SyS parte de una monitorización de la infraestructura tecnológica completa, que suministra logs y otros flujos de información a la plataforma LogICA NGSIEM, la primera plataforma SIEM 100% nacional. Dando un paso más adelante, el MPR cuenta con la Inteligencia Avanzada de Amenazas de ICA SyS, lo que le permite recibir todos los *insights* rela-

cionados con la protección de marca, aspectos geopolíticos relacionados, el ciclo completo de vulnerabilidades y el seguimiento de actores y amenazas. Además, el servicio también incluye el seguimiento de exfiltración de datos en entornos *deep web*, *dark web*, redes sociales e internet. Gracias a ello, se logra una protección mucho más completa de la ciberseguridad del Ministerio, cubriendo ámbitos sobre los que no se tenía visión anteriormente.

Entrando más en detalle, el Ministerio dispone de un modelo de análisis de amenazas en tiempo real, capaz de detectar, mediante la correlación

de información procedente de sus sistemas internos, de la información extraída de la analítica de información de internet, de la *deep web* o de la *dark web*, intentos de ataques por parte de grupos organizados, exfiltración de información, manejo de datos sensibles, análisis de información corporativa, analítica de vulnerabilidades y *exploits* asociados y seguimiento de actores, así como mitigación de ataques en países extranjeros (bloqueo de IPs, dominios concretos, etc.). Con toda esta información recogida sobre amenazas potenciales y gracias a la inteligencia de amenazas, los analistas de seguridad pueden reaccionar



El Ministerio disfruta de un modelo de análisis de amenazas en tiempo real, capaz de detectar, mediante la correlación de información procedente de sus sistemas internos, de la información extraída de la analítica de información de internet, de la deep web o de la dark web, intentos de ataques por parte de grupos organizados, exfiltración de información, manejo de datos sensibles, análisis de información corporativa, analítica de vulnerabilidades y exploits asociados y seguimiento de actores, así como mitigación de ataques en otros países.

ante los ataques con el mayor conocimiento posible, incluso llegando a adelantarse a ellos antes de que sucedan.

Visión 360° de la ciberseguridad

Con inteligencia proactiva y predictiva, ICA SyS cuenta con información procesable, rica en contexto y en tiempo real, lista para la integración en todo el ecosistema de seguridad del MPR. Para un control mayor, el Ministerio cuenta con un servicio de auditoría periódica externa e interna, bajo los servicios del CiberSOC de ICA SyS, que combina las capacidades que brindan las plataformas más innovadoras desarrolladas por ICA SyS con los conocimientos y la experiencia del equipo de expertos analistas.

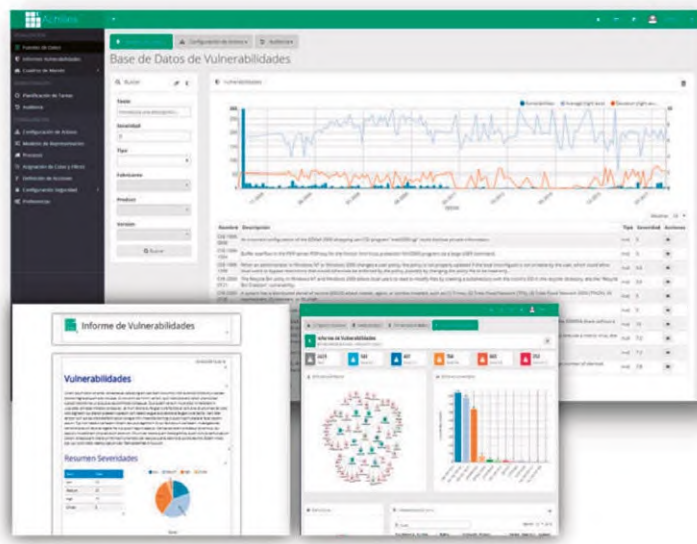
Estas auditorías están orientadas a la detección temprana de vulnerabilidades, errores de configuración o situaciones que puedan derivar en una degradación del servicio. Por ello, se incluyen análisis de vulnerabilidades y test de intrusión, con el objetivo de identificar y subsanar posibles debilidades en la arquitectura de seguridad, evitando su explotación malintencionada y procediendo a su reconfiguración y subsanación.

De esta manera, el Ministerio de la Presidencia e ICA Sistemas y Seguridad han construido un servicio de gestión de la ciberseguridad para una protección 360° con las tecnologías de ciberseguridad más avanzadas y que cuenta con personal técnico capaz de desarrollar las actividades con los máximos requisitos de seguridad y calidad. Además, dada la criticidad de los activos y servicios que proteger, se ha desarrollado un sistema de trabajo en modalidad mixta, con soporte in situ mediante especialistas en seguridad TI perteneciente al CiberSOC



CiberSOC de ICA Sistemas y Seguridad

El MPR e ICA SyS han construido un servicio de gestión de la ciberseguridad para una protección 360° con las tecnologías de ciberprotección más avanzadas y que cuenta con personal técnico capaz de desarrollar las actividades con elevados requisitos de seguridad y calidad.



de ICA SyS en modalidad 8x5 y el soporte remoto del personal completo del CiberSOC en modalidad 24x7.

Hoy en día, los ciberataques son cada vez más numerosos, complejos y creativos, lo que hace más necesarias que nunca la automatización, orquestación, visibilidad de la red y control del punto final, además de brindar un protagonismo especial a los analistas de seguridad. En este sentido, ICA Sistemas y Seguridad es puntera en España en la prestación de servicios avanzados MDR y Threat Intelligence y cuenta con el respaldo y la colaboración de su *partner* Recorded Future.

En definitiva, y al margen de un servicio que cubre ámbitos sobre los que no se tenía visión anteriormente, la estrecha colaboración entre el Ministerio de la Presidencia e ICA Sistemas y Seguridad se muestra como clave del éxito en el diseño de un servicio completo y con las últimas tecnologías para hacer frente a diferentes ciberescenarios de manera proactiva. ■

OBJETIVOS A CUBRIR EN EL SERVICIO	¿CÓMO AYUDA EL SERVICIO DE CIBERINTELIGENCIA?
Protección de marca	• Typoquatting y dominios similares • Menciones de marca en fuentes no convencionales • Menciones de interrupciones del servicio • Menciones de marca con Cyber Events • Supervisión de VIP en las fuentes
Protección frente a las amenazas internas y la fuga de propiedad intelectual	• Dominios en repositorios de código • Monitoreo de amenazas internas • Monitorización de credenciales / correos electrónicos filtrados • Correo electrónico de la empresa en el repositorio de códigos
Gestión de Vulnerabilidades	• Tarjetas de inteligencia • Puntuación previa a NVD • Notas técnicas sobre vulnerabilidades
Inteligencia de amenazas	• Tarjetas de inteligencia. • Notas insikt relacionadas con España y Gobierno • Tarjetas de inteligencia de actores de amenazas • Seguimiento de movimientos hacktivistas, hacktivistas ocasionales y de falsa bandera (p.e OPSpain)

JULIÁN HERNÁNDEZ VIGLIANO
Subdirector General
Subdirección General de Tecnologías
y Servicios de Información
**Mº DE LA PRESIDENCIA, RELACIONES
CON LAS CORTES Y MEMORIA DEMOCRÁTICA**

ALBERTO CAÑADAS ÁLVAREZ
Gerente Preventa y Desarrollo de Negocio
de Ciberseguridad
ICA SISTEMAS Y SEGURIDAD



CONFIANZA CERO

ACCESO
PRIVILEGIADO
AL MOMENTO

#Zero trust #JiT #Pam

Producto recomendado por el CCN



www.oneidentity.com/solutions/zerotrust/

SEAT: La Ciberinteligencia aplicada al mundo de la seguridad física

Cipher comenzó su colaboración con Seat en 2019 a partir de necesidades básicas de cibervigilancia y ciberinteligencia, desplegando un servicio de continuidad basado en alertas e informes periódicos donde se anticipaban las amenazas, su impacto y la posible evolución a partir de la información procedente de cualquier tipo de fuente abierta, analizada y categorizada, para la dirección de las diferentes áreas de negocio. La necesidad era palpable. En la actualidad reciente de nuestro país, la situación de inestabilidad se ha trasladado a las calles de nuestras grandes ciudades en numerosas ocasiones, suponiendo riesgos de diversa naturaleza para las grandes compañías, desde las campañas de ciberataques hasta los posibles daños en activos físicos. Posverdad y desinformación se han convertido, por otra parte, en riesgos reales contra la reputación de las empresas y la continuidad de negocio. En este contexto, el equipo de seguridad de Seat trabajó con el equipo de ciberinteligencia de Cipher para buscar soluciones innovadoras y rentables para la circunscripción de un marco de protección que permitiera detectar vulnerabilidades, mejorar la normativa de seguridad y anticipar riesgos en eventos que no podrían haber sido detectados con métodos tradicionales.



Manuel García Muñoz / Francisco de Asís Quintero Lopez

En el ámbito de la ciberseguridad no sólo hay cabida para la protección de activos digitales, que se enfoca al *cyber-dependant crime* -aquellas amenazas en las que los sistemas digitales son el medio y el objetivo del ataque al mismo tiempo-. Es necesario valorar la protección de la continuidad de negocio en otros ámbitos y con una visión más transversal, ya que ésta puede verse afectada por cuestiones vinculadas a entornos tangibles y sociales, creando modelos de amenazas que, a través del ciberespacio, toman forma física. Entre ellos, el fraude y la estafa, la ingeniería social, los movimientos de activismo radical, boicots, el uso fraudulento de información confidencial parte de un empleado *insider*, o condicionantes de movilidad -climáticos, o motivados por alarma social- que puedan afectar o impedir que el negocio corporativo se desarrolle con normalidad.

Desde que la tecnología es rutina, el ojo humano ya no es la fuente de información predominante. La superficie de riesgos en el mundo actual incorpora nuevas variables a diario, y requiere una constante atención de las áreas de dirección en los distintos ámbitos de la seguridad. Los servicios de ciberinteligencia, en cualquiera de sus vertientes, ha pasado **de ser valor añadido a esencial**; por encima, en ocasiones, de las medidas tradicionales de vigilancia física o la escolta. Recopilar, clasificar y analizar la información expuesta en la red es crucial para la previsión de riesgos. ¿A qué te enfrentas si has organizado un viaje de tu presidente y se queda atrapado en la ruta planificada por una movilización que no se tuvo en cuenta? ¿Podría haberse previsto este escenario de vulnerabilidad? Y si las vías y accesos de los empleados a tus instalaciones están cortadas por protestas o condiciones climáticas ¿qué pérdidas podría suponer para la compañía? ¿se podrían haber tomado medidas? La respuesta es

sí, a través del análisis de inteligencia, como solución avanzada para cubrir un espectro de riesgos para el que la seguridad física tradicional no está preparada. Y es primordial para los directores de seguridad la elección de este sendero.

La importancia de un servicio externalizado

Muchas compañías necesitan incorporar servicios de inteligencia que anticipen amenazas reales y que evalúen posibles escenarios a partir de la información expuesta en fuente abierta; tanto en medios de prensa digital, foros,

pueden permitirse la conformación de equipos multidisciplinares y holísticos de analistas, capaces de implementar análisis técnicos de ciberamenazas, identificar y desgranar vulnerabilidades de activos digitales, o de realizar un análisis de escenarios de una crisis sanitaria al mismo tiempo. Ese nicho queda, por tanto, para los equipos de inteligencia en proveedores de servicios de ciberseguridad como Cipher, que cuenta en su equipo con analistas con una amplia diversidad de perfiles, tales como criminólogos, economistas, abogados, periodistas, expertos en relaciones internacionales, en filosofía, comunicación audiovisual, o ingenieros informáticos. Todos

Los servicios de ciberinteligencia no tienen una orientación exclusiva a áreas IT. La seguridad física también es ciberseguridad. Por tanto, los servicios deben ir dirigidos a prevenir cualquier amenaza que pueda incidir en la continuidad de negocio.

blogs o redes sociales, portales de *e-commerce* y compraventa, como en cualquier otra fuente que permita recopilar información para realizar análisis de amenazas. De esta manera pueden tomar medidas a tiempo para mitigar o eliminar las amenazas que empañen su horizonte de éxito comercial.

Para el despliegue de este tipo de servicios, más allá del soporte de herramientas de recopilación y filtrado de información, se requieren perfiles de analistas tanto técnicos como estratégicos. El papel del analista tiene una doble vertiente: aplicar su *expertise* en la afinación de las herramientas y, sobre todo, aportar el valor humano del análisis, una vez el dato está filtrado y recabado, para la construcción de entregables en diferentes formatos. Muchas compañías no

ellos con el enriquecimiento en formaciones posgrado orientadas a la ciberseguridad.

SEAT y Cipher

Cipher comenzó su colaboración con Seat en 2019 a partir de necesidades básicas de cibervigilancia y ciberinteligencia, donde Cipher desplegó un servicio de continuidad basado en alertas e informes periódicos donde se anticipaban las amenazas, su impacto y la posible evolución a partir de la información procedente de cualquier tipo de fuente abierta, analizada y categorizada, para la dirección de las diferentes áreas de negocio. La necesidad era palpable. En la actualidad reciente de nuestro país, la situación de inestabilidad se ha trasladado a las calles de nuestras

De ser la víctima a estar protegido.

Conciencie a sus empleados. Elimine las amenazas. Haga que sus usuarios participen y prepárelos para enfrentarse a los ciberataques del mundo real.

En lugar de perder tiempo con contenidos generales para todos los usuarios, le ayudamos a **proporcionar el curso de ciberseguridad adecuada a cada persona, en el momento preciso.**

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

proofpoint®

La protección empieza por las personas



grandes ciudades en numerosas ocasiones, suponiendo riesgos de diversa naturaleza para las grandes compañías, desde las campañas de ciberataque hasta los posibles daños en activos físicos. Posverdad y desinformación se han convertido, por otra parte, en riesgos reales contra la reputación de las empresas y la continuidad de negocio.

En este contexto, el equipo de seguridad de Seat trabajó con el equipo de ciberinteligencia de Cipher para buscar soluciones innovadoras y rentables para la circunscripción de un marco de protección que permitiera detectar vulnerabilidades, mejorar la normativa de seguridad y anticipar riesgos en eventos que no podrían haber sido detectados con métodos tradicionales. De esta manera, pudieron detectar y eliminar riesgos de movilidad y continuidad de negocio -a través del sistema de alerta temprana-, prevenir posibles acuerdos con partners de dudosa reputación o intentos de fraude a directivos -a través de investigaciones online-, o detectar rápidamente imágenes de prototipos de la marca difundidos por canales alternativos antes de ser publicados oficialmente. El objetivo final era tener respuestas para preguntas como ¿He evaluado de manera superficial a un potencial distribuidor en otro país por no conocer las actividades de sus managers? ¿Quiénes están detrás de los ataques de ingeniería social sobre nuestros directivos para suplantarlos? ¿Qué técnicas utilizan? ¿Puede una tarjeta de visita entregada en un avión a un miembro de nuestro consejo de dirección suponer una amenaza que requiera una investigación? ¿Es posible que un *insider* dentro de mi compañía esté facilitando información confidencial a la competencia?

La situación convulsa y cambiante de la realidad social en todos sus ámbitos requería de una capacidad de previsión en diferentes ámbitos como la protección de directivos, la protección de la cadena de producción y del flujo con proveedores esenciales. Del mismo modo había que abordar el control de fugas de información, el análisis y prospectiva de temas que preocupan a la compañía en el ámbito internacional -de alcance propio o del sector competitivo-, o las amenazas que pueden derivarse de las nuevas tendencias en el mercado de la automoción. Entre estos últimos se pueden encontrar los riesgos de reciente aparición sobre movilidad eléctrica, o nuevas formas de negocio en vertiginoso ascenso como *carsharing*, *motosharing* o *kicksharing*. En poco tiempo el servicio evolucionó. Se incorporaron nuevas herramientas y los formatos de entrega se fueron adaptando al requerimiento de SEAT como una llave a su cerradura, incluyendo en el *delivery* huellas digitales y huellas virtuales de infraestructuras críticas, para evaluar de manera categorizada por tipología de riesgo la exposición digital de personas y activos físicos que proteger.

Seguimiento de acontecimientos de crisis

A partir de las necesidades impuestas por una realidad sociopolítica en la que la continua

alteración de factores se ha ido normalizando, aparecieron en el escenario nuevas necesidades. Entre estos factores se encuentran la crisis sanitaria provocada por la pandemia del Covid-19, o la inestabilidad política y social reciente. Las crisis de otras firmas del sector se convirtieron en foco de atención, tanto a nivel nacional como internacional. A lo largo de 2020, en el sector de automoción se anunciaban planes de recortes y cierres de plantas. Cipher, implantando su servicio de monitorización intensiva, desplegó para Seat un observatorio que incluía la monitorización continua de la crisis y su posible repercusión en la continuidad de negocio. El ámbito cubriría los riesgos tanto a corto plazo, en cuanto a la

peso cayó, en posteriores reuniones, su aplicación a nuevas temáticas vinculadas a la seguridad. Cipher comenzó a preparar diferentes *dashboards* para directivos y los temas de interés de sus unidades de negocio, de una manera totalmente personalizada según los intereses que les fueron transmitidos por SEAT. De esta manera, cada directivo tenía información, amenazas, previsión, tendencia y análisis competitivo en tiempo real. El producto final es un buscador avanzado, inteligente, personalizado y preconfigurado que permita tener en tiempo real una respuesta a todas las preocupaciones de las diferentes áreas de dirección de la compañía en un solo reporte orientado a la previsión de amenazas y conocimiento de tendencias a corto plazo.

Y mañana, ¿qué?

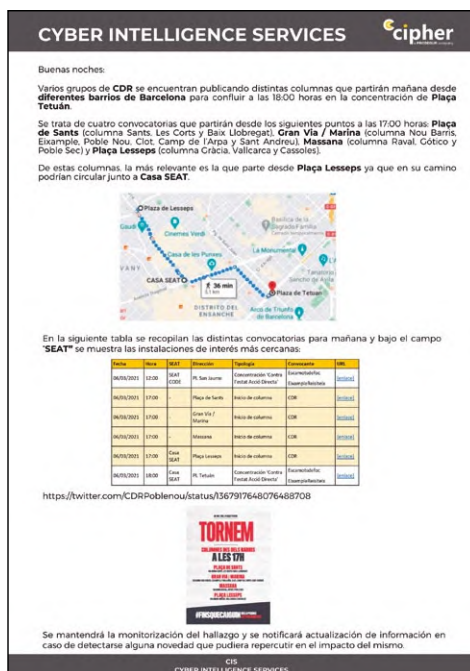
En un año pandémico como 2020 de continuo cambio de escenarios y previsiones, el servicio ha ido mutando y adaptándose a la par según las nuevas amenazas y oportunidades que se han ido presentando, de manera que el año 2020 ha terminado con una excelente relación de equipo operacional entre las unidades de seguridad y de negocio de Seat y la unidad de ciberinteligencia de Cipher. En este contexto disruptivo, donde la naturaleza de los riesgos exige una rápida reacción, los servicios de ciberinteligencia evolucionan hacia modelos más flexibles y abiertos, basados en contratos marco, con un amplio portafolio de soluciones a diferentes tipologías de riesgos, de manera que sea tan sencillo de contratar como lo es para un comensal seleccionar la cena en la carta del menú de un restaurante.

Las posibilidades de evolución de la ciberinteligencia van alineadas con la evolución de las amenazas, y nuevas formas de servicio irán aflorando en los próximos años para hacerles frente. El resultado de esta colaboración de vanguardia entre Seat y Cipher lleva a una conclusión clara: los servicios de ciberinteligencia no tienen una orientación exclusiva a áreas IT.

La seguridad física también es ciberseguridad. Por tanto, los servicios deben ir dirigidos a prevenir cualquier amenaza que pueda incidir en la continuidad de negocio. La seguridad tiene un plano específico de actuación en cada *business unit* de las compañías y, sobre todo, para los responsables de la seguridad. Es por esta última razón por la que el CSO debe considerar la ciberinteligencia como una herramienta vital, y no accesorio, para hacer frente a las amenazas que se ciernen sobre el entorno actual del negocio a nivel mundial y a todas las escalas. ■

MANUEL GARCÍA MUÑOZ
Country Manager - Seguridad/Security
VW GROUP IN SPAIN

FRANCISCO DE ASÍS QUINTERO LOPEZ
Cyberintelligence Services Manager
CIPHER



afectación de la movilidad en la zona sobre su propia cadena de producción, como a nivel de prospectiva y escenarios a medio y largo plazo. Esto permitió a Seat ser los primeros en disponer en tiempo real de información útil, filtrada, categorizada y analizada con la que evaluar las amenazas y encontrar indicadores clave para la toma de decisiones.

Adicionalmente, Cipher puso a disposición de Seat un panel de análisis de impacto en tiempo real y personalizado hacia la crisis, construido a partir de herramientas de recolección de información, y configurado con su equipo de analistas expertos que, a través de *queries* complejas que combinan términos de riesgo, depuraban y clasificaban la información eliminando la presentación de resultados erróneos. De esta manera, Seat tuvo la posibilidad evaluar las temáticas que iban tomando relevancia para poner el foco, las tendencias en redes sociales y medios en fuentes abiertas, anticipar *topics* susceptibles de ser viralizados, y disponer de un análisis de impacto competitivo en las principales marcas del sector.

La presentación de los paneles de impacto supuso un antes y un después. Por su propio



**No te enfrentes a un rey
con las armas de un peón**

PenTera

Leaders in continuous security validation

“Tenemos que ser capaces de gestionar los riesgos asociados a nuestra cadena de suministro”

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

–¿Cómo está organizada en Iberdrola la gestión de riesgos de ciberseguridad?

– Se basa en una estrategia de descentralización coordinada. Me explico: no nos parece factible que exista un grupo con todos los conocimientos necesarios para dominar los aspectos técnicos de la gestión de la ciberseguridad en todos los escenarios de actividad y de negocio en los que estamos presentes como Grupo multinacional. Además de conocimientos, tendrían que tener acceso a las tecnologías y a los proyectos de estas actividades y líneas de negocio.

En la segunda línea estamos nosotros, es decir, la Dirección corporativa de ciberseguridad, en global y en los países. Nuestra misión consiste en establecer la normativa, los mecanismos de control, el marco de coordinación, la supervisión, la asesoría y la revisión. En esta segunda línea se encuentra también el Comité de Riesgos, al que nosotros reportamos trimestralmente. También reporto a la Comisión de Auditoría y Supervisión de Riesgos del Consejo de Administración, que tiene competencias específicas en materia de ciberseguridad.

En la tercera línea se encuentra la Audi-

Rosa Kariger CISO Global de IBERDROLA

Rosa Kariger es, sin lugar a duda, una de las mejores ejecutivas de ciberseguridad que tiene España. Ingeniera Industrial con 23 años de experiencia en Iberdrola, desde 2016 ocupa la posición de CISO Global. Y es, en su representación, copresidenta del Grupo de Sistemas de Ciberresiliencia en Electricidad del Foro Económico Mundial (WEF, por sus siglas en inglés). Conversar con ella es aprender de una persona con criterio, sin pelos en la lengua y que reivindica con orgullo el estilo femenino de ejercer el liderazgo.

Por esta razón, hemos apostado por una integración de la ciberseguridad en los procesos de toma de decisiones en los propios negocios. Y, en consecuencia, hemos nombrado a responsables de ciberseguridad con sus correspondientes equipos técnicos dentro de cada uno de los negocios. Y, sobre ellos, una capa de supervisión.

Básicamente, adoptamos el clásico modelo de las tres líneas de defensa: la primera línea está formada por estos expertos en ciberseguridad en los negocios: Sistemas TIC –que, como no puede ser de otra manera, tiene un Equipo importantísimo de ciberseguridad–, la operación OT (generación, distribución, renovables ...). Y también en las áreas de apoyo como Recursos Humanos, Administración General o SSJJ.

toría Interna, que revisa que la primera línea cumple con lo que está establecido y, al tiempo, nos audita a nosotros el modelo de control.

Desde el punto de vista del Gobierno, esto se coordina a través de un Comité Global de Ciberseguridad, en el que están representados todos los negocios y las áreas del Grupo.

– ¿Cuántas personas trabajan hoy en ciberseguridad en Iberdrola?

– Aproximadamente, unas 270. Todas especializadas. Pero insisto: a ellas se suman los 34.000 empleados del Grupo, que son nuestra primera línea de defensa.

– ¿Cómo contempla los riesgos de ciberseguridad, nacidos de lo más profundo de las ingenierías de Informática y de Telecomunicaciones?

– Como Ingeniera Industrial, y desde la óptica de los procesos y de la tecnología que los soporta, creo que la aproximación que se ha hecho desde el mundo IT tiene que cambiar.

Debemos entender que el de ciberseguridad no es sino un riesgo operativo más de entre todos los que ya tenemos en los entornos que se gestionan. Hay que dar este salto. Existe una concentración de riesgos de ciberseguridad en IT, y se deben gestionar allí, en IT; pero existe toda una tecnología específica del entorno industrial, que se concibió aislado, y que hoy está dejando de estarlo a pasos agigantados. Y no se puede gestionar igual que en IT o desde IT.

Llevo tiempo escuchando que la ciberseguridad IT está más madura que la OT. Puede que sea cierto; pero le aseguro que no tanto como lo está la cultura de seguridad en los entornos industriales, mucho más acostumbrados a hablar en clave de riesgos. Ya me gustaría que hubiese dicha cultura en los entornos IT.

– ¿Qué opina del rumbo que ha tomado la UE en lo que toca a la evaluación y certificación de ciberseguridad de productos, procesos y servicios?

– La certificación es positiva porque ayuda a incrementar de base la seguridad de nuestros productos y servicios. En general, las regulaciones –no solo las de la UE– se orientan solo a los operadores, y no a los proveedores, ya lo sean de productos o servicios, hecho que nos obliga a nosotros a establecer requisitos y vigilar que se cumplen. A ver si esto se equilibra.

Pero no es la panacea. El abrumador nivel de dispersión tecnológica existente, su evolución acelerada y la sofisticación de los ataques, va a hacer que todo esfuerzo de certificación, si no es de suficiente alto nivel, se quede obsoleto, y si es de demasiado alto nivel resulte inútil. Pero tiene que existir una base, especialmente para la IoT y las tecnologías emergentes, como el 5G, que deberían salir al mercado con funcionalidades de ciberseguridad por diseño.

También es cierto que cada tecnología y cada servicio que se incorporan en una compañía llevan asociados nuevos riesgos, que no dependen de la certificación. Ya sabe: podemos usar productos certificados, pero configurarlos o integrarlos de forma insegura en nuestra infraestructura.

Por otra parte, las multinacionales tenemos cadenas de suministros globales cuya gestión resulta de por sí complicada, por lo que lo deseable sería disponer de

un marco de certificación homogéneo y global. Si no, tanto operadores como proveedores vamos a tener problemas.

– **¿Cuáles son sus principales preocupaciones como CISO Corporativa?**

– Dos principales. La primera es, internamente, llegar a todas partes y a lo nuevo. Tenemos todavía una forma de operar muy reactiva. Somos cada vez mejores en identificar, detectar y proteger lo conocido, pero no en anticiparnos. Estrictamente hablando, no se trata

¿Cómo podemos asegurar que, al menos, detectamos, o somos capaces de detectar problemas de ciberseguridad de nuestra cadena de suministro, de todos nuestros proveedores en cualquier frente? Nuestra dependencia es enorme.

– **¿Qué aspectos de gestión le ocupa más tiempo en su actividad? ¿Cumplimiento, reporting...?**

– He de decirle que no me centro en el cumplimiento; aunque lo aprovecho. La cultura de cumplimiento es un rasgo

mos ahora mismo desarrollando una nueva línea de aseguramiento interno basado en riesgos, un proyecto interesantísimo que iniciamos el año pasado. No podemos tener al regulador dictándonos los planes de ciberseguridad, ni podemos estar esperando a ver si nos dicen si una infraestructura es crítica o esencial para protegerla o no, máxime teniendo en cuenta que también trabajamos en países y mercados que no tienen estas regulaciones.

Con el proyecto mencionado, queremos cambiar esa mentalidad. Así pues, estamos yendo a cada área de negocio para que nos indiquen qué procesos consideran críticos. Una vez identificadas las joyas de la corona, las vamos a perfeccionar en materia de ciberseguridad: las que no estén ya sujetas a cumplimiento las someteremos a un exhaustivo modelo de aseguramiento interno.

Este proyecto también persigue lograr eficiencias para que las diferentes iniciativas de cumplimiento no se hagan por silos, y para involucrar a todos y cada uno de los responsables de las áreas concernidos, que son los propietarios del riesgo. Lo ejecutaremos en forma de autoserivicio.

– **¿Decía antes que no se centraba en el cumplimiento?**

– Estamos involucrados en el cumplimiento, obviamente. Sin embargo, el fuerte de nuestra actividad regular es la gestión en clave de riesgos, la supervisión de los planes de actuación en los negocios y la preparación del *reporting*.

– **Siempre he pensado que el *reporting* debería incluirse en el catálogo de las bellas artes.**

– No le digo que no. Creo en el poder del *reporting*, porque es, a su vez, el producto de otros dos poderes, el de la pregunta y el del dato. A los integrantes de la Alta Dirección y a los miembros del Consejo de Administración, hay que explicarles qué riesgos hay para la compañía y qué preguntas tienen que hacer y a quiénes.

Yo tengo tres tipos de reporte según el objetivo perseguido. El primero es estratégico y está orientado a mover a la acción. Es de abajo-arriba y hace posible que la cifra de gasto e inversión anual de Iberdrola en ciberseguridad ronde los 50 millones de euros.

El segundo nos permite identificar riesgos. Basado en lo que vemos en nuestro cuadro de mando de ciberseguridad, está al servicio de los miembros del Comité de Ciberseguridad, responsables de desplegar las acciones. Con este mode-



“El Consejo de Administración de Iberdrola y la Alta Dirección están muy sensibilizados con la gestión de riesgos de ciberseguridad; buena prueba de ello es que nuestro presupuesto anual de inversión y gasto en la materia ronda los cincuenta millones de euros”

de una cuestión exclusiva de tecnología, sino de que la ciberseguridad esté completamente embebida en todos los procesos de toma de decisiones y proyectos. Hemos avanzado mucho, pero no hemos llegado a ese punto.

Mi segunda preocupación, en este caso hacia el exterior, es la de la ciberseguridad en nuestra cadena de suministro, especialmente después de lo que estamos sabiendo tras el asunto de SolarWinds, entre otros.

que distingue a sectores muy regulados como el nuestro. Pero en ocasiones, y aplicado a lo nuestro, puede llevarnos a una falsa sensación de seguridad; además, retrae recursos que deberían dedicarse a gestionar y operar la ciberseguridad.

Las dos actividades que más tiempo me ocupan hoy son el *reporting* y el desarrollo de nuevas líneas estratégicas.

– **¿A qué se refiere con esto último?**

– Le pongo un ejemplo: nos encontra-

lo trabajamos más orientados al plano táctico.

El tercer tipo es un informe más operativo, que nos guía en la gestión de la ciberseguridad: alertas, incidentes, vulnerabilidades, ...

– **¿Se siente apoyada por su Presidente, José Ignacio Sánchez Galán?**

– Absolutamente. El presidente y el Consejo en su conjunto son muy sensibles a este tipo de riesgos. Contamos con su apoyo, y para dejarlo más patente no tengo nada más que remitirme al modelo que le he descrito antes: no jerárquico, multidisciplinar, integrador... Sin su apoyo decidido, no funcionaría. Tiene también gran interés en promover nuestra colaboración a escala europea e internacional, a fin de contribuir a la resiliencia del ecosistema.

– **¿Aboga usted por el tratamiento sectorial de la ciberseguridad?**

– Sí. Tenemos unas características muy diferenciales, precisamente por el gran peso y la complejidad de las tecnologías, procesos y servicios OT. Por otra parte, nuestras infraestructuras físicas son objeto de ataques especialmente diseñados. La colaboración sectorial, por tanto, es indispensable.

– **Iberdrola ha sido pionera en la contratación de pólizas de seguros específicas para cubrir daños causados por ciberataques. ¿Cómo se está desarrollando esta parcela de la gestión de riesgo?**

– Para nosotros el seguro es un elemento complementario para darnos cierta tranquilidad sobre el riesgo de nuestra cuenta de resultados. He de decirle que el factor económico en sí no nos preocupa tanto como el elemento reputacional o la afección de servicios esenciales.

Estamos observando un endurecimiento del mercado y una cierta tendencia a la exclusión de ciertos tipos de ciberataques, como por ejemplo los de *ransomware*.

En materia de seguros, como en muchas otras cosas, somos presa de la historia, de la forma en la que ha evolucionado la ciberseguridad. No entiendo por qué



“Como Ingeniera Industrial, y desde la óptica de los procesos y de la tecnología que los soporta, creo que la aproximación que se ha hecho desde el mundo IT a la protección digital tiene que cambiar. Debemos entender que el de ciberseguridad no es sino un riesgo operativo más de entre todos los asociados a los entornos que gestionamos”

no hay ya en el mercado pólizas únicas, que incluyan todo tipo de eventos, ciber y no ciber. Seguramente la probabilidad de ocurrencia se calcularía de una forma distinta. Vale; pero el impacto es el mismo. El mercado de los seguros debería evolucionar.

– **No son pocos los ingenieros industriales que participan en el diseño de pólizas de seguros.**

– Y no me parece mal. Profesionalmente llevamos muchas décadas trabajando en la resiliencia de nuestros sistemas, redes, instalaciones, servicios: redundancia por diseño, planes de respuesta ante contingencias de todo tipo para que no se caiga, pongamos por caso, un suministro

de electricidad. Y no tiene sentido que si la interrupción, en vez de ser causada por una tormenta lo es por un ciberataque, la cosa cambie.

Créame: ya sea por la gestión de riesgos, con complemento asegurador o no, la cultura de seguridad industrial es alta, y tenemos que poner en valor los mecanismos de resiliencia existentes ante eventos del mundo físico, y unificar riesgos desde la perspectiva de su impacto. Por ahí va el futuro.

– **¿Cómo están encarando los grandes proveedores de OT la ciberseguridad?**

– Están acostumbrados a tenerlo todo muy procedimentado y a cumplir estándares. Como no tenemos todavía estándares en ciberseguridad industrial, solo algunos operadores pedimos requisitos y los fabricantes, digamos, los cobran aparte. Básicamente, los proveedores venden por un lado el producto inseguro y por otro el servicio de ciberseguridad, pero la seguridad no se debe negociar en las mesas de contratación. Unos y otros estamos intentando cambiar este modo de funcionar.

– **Por el modelo de gestión que han**

“La función de CISO y la de DPO requieren de coordinación, pero son radicalmente diferentes. Aunque nuestra DPO global está en mi Equipo, tenemos una completa separación de modelos y ella informa directamente al Consejo de Administración”

adoptado en Iberdrola, no parece usted muy a favor de la NIS1, del RD-L de su incorporación a la legislación española y del reciente RD 43/2021 en el que se reconoce la figura y función de los Responsables de Seguridad de la Información.

– Y además este último sale cuando está ya avanzada la NIS2. No, no estoy de acuerdo con la orientación que está tomando a efectos regulatorios la figura del CISO. Lo que se busca es una *superwoman* o un *superman* que entienda de ciberseguridad en todo frente y nivel

– ¿Cómo está implantada en Iberdrola la figura del DPO?

– Tenemos una DPO global y DPOs en cada país en donde es obligatorio. Y en los que no, un Privacy Officer. Además, los negocios, y particularmente Comercial y Recursos Humanos, cuentan con responsables de protección de datos en su seno.

La función de CISO y la de DPO requieren de coordinación, pero son radicalmente diferentes. Aunque nuestra DPO global, Teresa Rodríguez de Tembleque, está en mi Equipo, tenemos una completa sepa-

suministro. Estamos intentado ver el problema *out of the box* para llegar a un consenso sobre cuál debería ser el papel de los reguladores para ayudar de verdad a todos a paliar este problemón e incrementar la resiliencia sistémica. La idea es llegar a conclusiones y emitir recomendaciones de valor para gobiernos, especialmente aquellos que están redefiniendo su marco de ciberseguridad.

Este es el papel del WEF: brindar una visión integradora y neutral en el contexto de la colaboración público-privada con la filosofía de aportar a las empre-

sas y reguladores y contribuir, al tiempo, a la defensa colectiva, en un entorno de confianza, aumentando la ciberresiliencia del ecosistema global.

– ¿Tiene Iberdrola intereses en el mercado radioeléctrico?

– Tenemos una enorme dependencia de las telecomunicaciones en general, aunque dispongamos de nuestra red propia de fibra óptica. Cuando despegue de verdad 5G, no nos gustaría depender de, por ejemplo, los picos de Netflix para ver si operamos o nos comunicamos. Tenemos que disponer de un espacio reservado. Creemos, en buena lid, que se deberían tomar al respecto algunas medidas de seguridad y reserva de ancho de banda para evitar problemas ante picos de consumo, o ante la evidente dependencia en tiempo real de las señales en caso de uso típicos que puedan darse en 5G. La regulación lo recoge, pero de forma excesivamente sucinta.

– Una última pregunta: ¿qué aportan las especialistas en ciberseguridad al ámbito profesional de la ciberseguridad?

– Las mujeres aportamos a la diversidad, necesaria para poder afrontar soluciones a problemas complejos que no las tienen predefinidas. Las mujeres enriquecemos la capacidad de pensamiento en grupos en los que han preponderado los hombres, al igual que los hombres también lo hacen en grupos en los que hayamos predominado las mujeres.

Por otra parte, nuestro estilo de liderazgo es, en general, más colaborativo, y, como le comento, creo que es fundamental para abordar este reto. Y quiero ser muy precisa aquí: este “estilo femenino” ni es exclusivo de las mujeres, ni aplica a todas. Las hay que por su carácter o por presiones ambientales tienen un “estilo masculino” de actuar. ■



“Las mujeres aportamos diversidad para afrontar problemas complejos que no tienen soluciones predefinidas y un estilo propio de liderazgo diferente al de los hombres”

de abstracción: IT, OT, IoT, 5G, *Cloud*, IA, *Machine Learning*...

Creo en los equipos multidisciplinares. He de decirle que en Iberdrola la gestión de OT la lleva OT, y la de IT, Sistemas. Pero sobre todo, es una responsabilidad de los negocios, que son los que mejor conocen los impactos y que con sus decisiones pueden reforzar o anular cualquier medida técnica de seguridad desplegada.

Creo que el modelo al que vamos con esta legislación fomentará la cultura de cumplimiento y no la seguridad efectiva de una organización, y no creo que los estados les deban decir a las compañías cómo tienen que organizar y gestionar la ciberseguridad.

ración de modelos y ella informa directamente al Consejo de Administración.

– Usted es, en representación de Iberdrola, Copresidenta del Grupo de Sistemas de Ciberresiliencia en Electricidad del Foro Económico Mundial. ¿Qué asuntos tratan allí?

– Lo copresidimos Iberdrola y ABB. En el Grupo están representados no solo los CISOs de las mayores Eléctricas a nivel mundial, sino también los principales fabricantes y reguladores, laboratorios e instituciones procedentes de prácticamente todas las geografías, aunque todavía exista preponderancia de Europa y EE.UU.

Nuestra principal preocupación hoy es la ciberseguridad de nuestra cadena de



ágorasIC Centro de Conocimiento en Ciberseguridad

CISOs



**Ser o
no ser**

**...de
primera
o de
segunda**

La publicación del RD 43/2021 ha desencadenado una ‘pandemia’ de eventos en remoto sobre su contenido e interpretaciones que, en ocasiones, se ubican en el territorio de lo parapsicológico, especialmente si tenemos en cuenta que está en proceso de tramitación la NIS2.

En esta sección especial, y sin la pretensión de analizar el contenido de esta pieza legal –que todo se andará–, pero sí con el ánimo de bucear en algunas de las repercusiones que afectan a los CISOs-RSIs regulados, se enjuician dos circunstancias que cambian el panorama profesional, empresarial y mercantil: los interrogantes que se presentan a la luz de lo desarrollado en lo que concierne a la Declaración de Aplicabilidad; y dos, la aparición, de facto, de CISOs-RSIs no regulados.

SUMARIO

- Crónicas desde el monte Nebo, por MANUEL CARPIO
- Implicaciones para el Operador y su CISO de la Declaración de Aplicabilidad. FAQ, por Mariano JOSÉ BENITO y JAVIER ZUBIETA



Crónicas desde el monte Nebo

La publicación y entrada en vigor del Real Decreto 43/2021 por el que se ha desarrollado reglamentariamente el Real Decreto-ley mediante el que se transpuso a la legislación española la directiva NIS, ha puesto en primera línea de actualidad a los CISO al reconocer la figura del Responsable de Seguridad de la Información en los operadores regulados. Uno de los mejores expertos españoles –fuera y dentro de España– en esta disciplina, curtido en mil batallas, brinda su documentada opinión sobre el alcance de esta pieza legal española en su relación con el actual contenido de la futura NIS 2.0.



Manuel Carpio

Han pasado casi cuatro años desde que se publicó en esta revista el artículo “el CISO no tiene quien le escriba”. Se hacía allí un símil entre el CISO español y el Coronel de la célebre obra de Gabriel García Márquez, que esperaba la llegada, aunque fuera tardía, de un reconocimiento del gobierno a los servicios prestados. Por fin, y a diferencia de lo que ocurre al final de la novela, parece que los CISOS españoles recibirán buenas noticias de su gobierno, que serán felices y comerán perdices, y no lo que auguraba el coronel en su última frase.

Muertos de envidia por la jugada maestra del “lobby” abogacil en Bruselas con el RGPD, coetáneo de la Directiva NIS, nos quejábamos los CISOS allá por 2016 de que ésta tenía que haber sido en realidad un Reglamento, y no una Directiva.

Efectivamente, su trasposición en España, una mera traducción “cuasi literal” del texto bruselese, nos hizo presagiar un duro y largo “invierno regulatorio” sin apoyos a la figura organizativa del Responsable de Seguridad de la Información o CISO.

Pero hete aquí que, en una maniobra intrépida y audaz, el regula-

dor español se descuelga, el pasado 26 de enero, con un tardío regalo de Reyes en forma de Real Decreto en el BOE: el reconocimiento “de iure” del Responsable de Seguridad de la Información. Y creemos que ha sido valiente porque la publicación de este RD supone ir más allá de lo exigido en la Directiva, y liderar en solitario esta postura en la UE.

Por primera vez (si descontamos lo que ya se establecía en el ENS para

sas. Así, el RD 43/2021 en general, y su Art. 7 en particular, han venido a restañar ese agravio comparativo.

Con gran atino, el legislador no solo se limita a decirle al CISO lo que tiene que hacer, sino que se atreve a dar indicaciones sobre el diseño organizativo de dicha figura: perfil profesional y posición idónea en el organigrama para ejercerla. Algo parecido a lo que ya habíamos visto cuando en su día se crearon las men-

Algunos CISOS poco avisados quizá vean este RD como una odiosa regulación más, que tendrán que cumplir como si de un castigo divino se tratara. Y no les faltaría razón, pues tenemos regulaciones en ciberseguridad “como para alicatar un cuarto de baño”. Sin embargo, exceptuando el providencial Art. 7 y adláteres, el resto de prescripciones de este RD no suponen novedad en su quehacer diario.

los responsables de seguridad en las AA.PP.) y, parafraseando al presidente Adolfo Suárez, se ha “elevado a la categoría política de normal, lo que a nivel de calle es plenamente normal”. Y es que, a pesar de ser una realidad en España desde mediados de los ‘90, los CISOS han visto cómo otras figuras organizativas (el Responsable de Seguridad y Enlace, y el DPD) les han pegado una pasada por izquierda y por derecha, en la carrera (no declarada) por obtener credenciales oficiales que respaldaran su actividad en el seno de sus empre-

cionadas figuras del Responsable de Seguridad y Enlace y del DPD.

A favor o en contra

Algunos CISOS poco avisados quizá vean este RD como una odiosa regulación más, que tendrán que cumplir como si de un castigo divino se tratara. Y no les faltaría razón, pues (si el lector me permite la licencia, en honor a nuestro añorado Chiquito de la Calzada) tenemos regulaciones en ciberseguridad “como para alicatar un cuarto de baño”. Sin embargo, exceptuando el providencial Art. 7 y adláteres, el resto de prescripciones de este RD no

Creemos que el regulador ha sido valiente porque la publicación de este Real Decreto supone ir más allá de lo exigido en la Directiva, y liderar en solitario esta postura en la UE.



suponen una novedad en el quehacer diario del esforzado CISO: Ya las estaba cumpliendo al amparo de las regulaciones sectoriales, o de las certificaciones varias por las que tienen que rendir cuentas a las partes interesadas: "Business as usual".

Otros CISOS, por el contrario, quizá vean el vaso medio vacío, y se lamenten al considerar insuficiente la cobertura legal que este RD les ofrece, sobre todo si la comparamos con el blindaje que la LOPDGGD confiere al DPD. En nuestra opinión, debemos darnos por satisfechos ya que, al menos en esta ocasión, el legislador no ha enfocado al CISO como chivo expiatorio, y éste puede estar tranquilo si cumple con sus obligaciones con la diligencia debida.

NIS 2.0

Mientras tanto, en Bruselas, la heterogeneidad de los resultados obtenidos transcurridos más de dos años desde la trasposición de la Directiva, han decepcionado y hecho recapacitar al legislador europeo que ya prepara una segunda dosis de la vacuna NIS, más contundente que la primera. No será un Reglamento, sino una actualización de la Directiva, mucho más enfocada en esta versión hacia los requerimientos para los operadores de servicios esenciales.

Entre la batería de nuevas obligaciones para los EEMM y los OSEs, y por no salirnos del ámbito de este artículo, nos detendremos únicamente en el Art. 29.

En sus apartados 4, 5 y 6 se requiere a los Estados Miembro para que identifiquen a la persona jurídica y a las personas físicas "...director ejecutivo o representante legal en esa entidad esencial, y de cualquier otra persona física..." que serán consideradas obligadas a garantizar el cumplimiento o, por el contrario, conllevarán las responsabilidades por el incumplimiento, de lo dispuesto en la Directiva.

Entre las admoniciones reservadas para la dirección ejecutiva y el representante legal de la empresa (en el caso de que resultaran ineficaces las medidas adoptadas para remediar las deficiencias), está la inhabilitación para seguir ejerciendo funciones gerenciales. Del CISO, nada se dice.

Quizá era necesario que la dirección ejecutiva viera llegar el agua

previstas en el Plan Director de Seguridad.

Pero, un momento... ¿no nos estaremos dejando nada atrás?

Puede que el alcance de este RD, y de la futura NIS 2.0, hayan creado una falla, algo parecido a una liga con dos divisiones: por un lado tendremos la "champions league" donde juegan los CISOS de los operadores designados servicios esenciales,



hasta sus pies, causando un revuelo parecido al que removió al sector en el año 2010 con la modificación del Código Penal (en virtud de la cual se hacía penalmente responsable a la persona jurídica por los delitos co-

avalados y protegidos por la Ley, y por otro lado la de aquellos otros responsables de seguridad que todavía no han alcanzado ese Nirvana, como por ejemplo los de los denominados en la Directiva "servicios

El alcance del RD 43/2021 y de la futura Directiva NIS 2.0 llevan en volandas al CISO de operadores de servicios esenciales hacia días de vino y rosas, mientras dejan en la estacada a los pre-CISOS de "servicios importantes", los nuevos parias de la Seguridad de la Información.

metidos en nombre o por cuenta de las mismas, por sus representantes legales y administradores de hecho o de derecho).

No hay nada que ablande más el corazón de un departamento de compras que una página del BOE con obligaciones para la Alta Dirección, como portada del "Power Point" presentado por el CISO, y con las inver-

importantes", y a los que podrían comenzar a llamárseles los "pre-CISOS", por jugar en una categoría inferior. ■

MANUEL CARPIO

Asesor de Seguridad de la Información
Grupo ABAI
Miembro del FORO NACIONAL
DE CIBERSEGURIDAD

Implicaciones para el Operador y su CISO de la Declaración de Aplicabilidad. FAQ

Desde la publicación el pasado 28 de enero del Real Decreto 43/2021, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (abreviado RD NIS1), se han publicado numerosos artículos y celebradas no menos sesiones y webinars para desgranar los puntos principales del mismo, normalmente focalizados en las implicaciones para los operadores afectados. Este artículo se centra en uno de sus aspectos cruciales: la Declaración de Aplicabilidad y sus implicaciones tanto para el operador como para sus proveedores y para los respectivos CISOs (Responsable de Seguridad de la Información en el RD43), y se desarrolla en modo de autorreflexión por los autores, que se formulan a sí mismos preguntas de interés e intentan responder algunas de ellas.



Mariano J. Benito / Javier Zubieta

¿Qué es la declaración de aplicabilidad? ¿Qué finalidades satisface?

En el Artículo 6.4 se establece que: *“La relación de medidas adoptadas se formalizará en un documento denominado Declaración de Aplicabilidad de medidas de seguridad, que será suscrito por el responsable de seguridad de la información designado”*. La Declaración de Aplicabilidad (DA o SoA) es una herramienta ya conocida por las organizaciones con experiencia en certificación de su seguridad. Por ejemplo, ISO 27001 la cita como requisito en su cláusula 6.1.3; o el Esquema Nacional de Seguridad, que la exige en su artículo 27.4. Por lo tanto, el RD43 propone un saludable reuso de un concepto ya conocido y asentado.

En estos esquemas, la Declaración de Aplicabilidad busca ser el resumen ejecutivo del estado de seguridad, describiendo los controles de seguridad que están efectivamente aplicados. Y este debería ser en este caso, más aún cuando es un documento que debe ser firmado por una persona física (salvo que NIS2 cambie este requisito al “RSI designado”) y entregado a la Autoridad de Control. Así, la Declaración de Aplicabilidad pasa a ser un documento legalmente vinculante y las inexactitudes en el mismo pueden acarrear consecuencias para la persona física que firma.

Por ello, la DA debería ser un documento intuitivamente sencillo para que pueda ser asequible para una PYME. Porque, aunque el operador típico y los servicios digitales no son una PYME, gran parte de

sus proveedores sí lo son, y van a estar impactados por este RD.

Preguntas que le pueden surgir a cualquier RSI

– ¿Cuál deberá ser la Declaración de Aplicabilidad de un operador que opera varios servicios esenciales?

El Reglamento dice que la Declaración debe contener las medidas adoptadas por la organización, pero podría ocurrir que

zación. Además, se podrían generar ambigüedades no deseables, ya que por un lado podría entenderse que hay controles aplicados cuando en realidad no lo están y, al contrario, dar una falsa impresión de inseguridad igualmente incorrecta.

– ¿Cuál deberá ser la Declaración de Aplicabilidad de los proveedores de los operadores?

En el RD no se establece la obligación de que los proveedores de los operadores dispongan de una Declaración de Aplicabilidad, pero es esperable que los operadores así lo exijan como parte de sus requisitos a sus proveedores.

La situación se complica cuando un mismo proveedor presta un mismo servicio a varios operadores, pero los distintos operadores exigen Declaraciones de Aplicabilidad de

distintos formatos, contenidos y nivel de detalle. Derivadas por supuesto de sus distintos requisitos de seguridad. Ello generará que los proveedores, que ya habrán aplicado sus marcos de controles adecuados y suficientes para estos requisitos, deban dedicar un esfuerzo adicional a completar variopintos documentos de declaraciones de aplicabilidad: una sobrecarga de trabajo administrativo que detrae recursos del esfuerzo realmente importante: la seguridad de sus servicios Y que para los proveedores que sean PYMES puede llegar a ser insostenible.

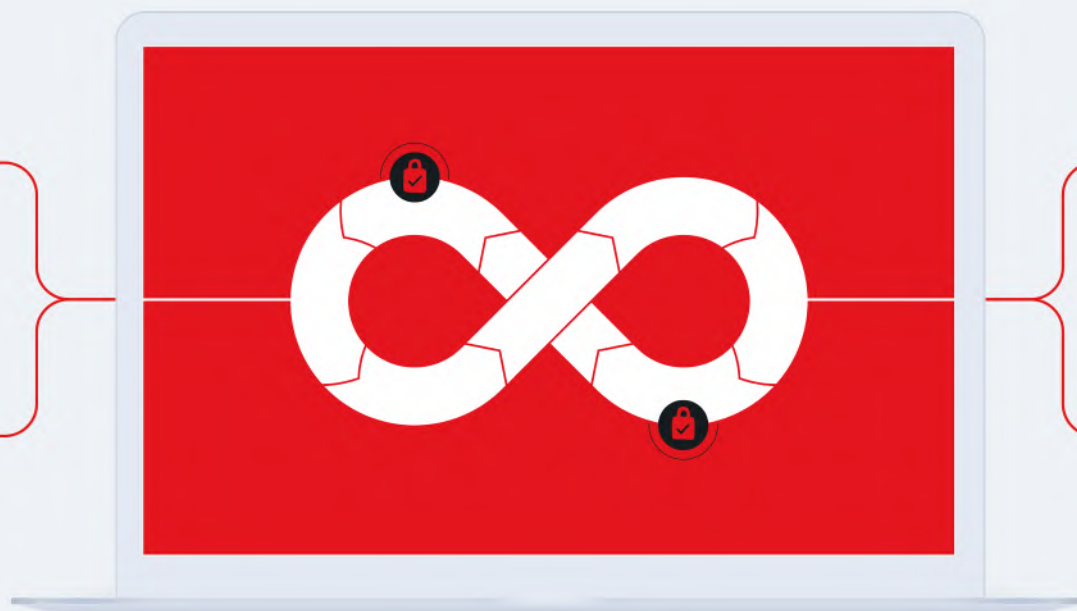
Por último, no debemos olvidar el carácter legalmente vinculante de la Declaración de Aplicabilidad. Si se deben proporcionar varias declaraciones de aplicabilidad distintas, cada una de ellas supone un riesgo. Sin duda, deberían darse pasos

¿Una o varias?	¿DA del proveedor?	¿Solo cada tres años?
¿Serán comparadas?	¿Eficaz o existente?	¿Qué se sancionará?

Figura 1. Interrogantes sobre la DA de un operador de varios servicios esenciales.

la organización adoptase diferentes medidas de seguridad en distintos servicios, o que los distintos servicios fueran valorados en categorías distintas, de acuerdo a ENS. ¿Debería el RSI preparar una Declaración por cada servicio? ¿Debería preparar una Declaración global para toda la organización? Si fuera este el caso, ¿Cómo deberían reflejarse los controles que están implantados solo en parte de la organización?

La respuesta a esas preguntas tiene serias consecuencias. Si se genera una única declaración de aplicabilidad para todos los servicios, podría resultar en un documento extenso, prolijo y farragoso de entender: Si, para evitar esos problemas, se realiza una Declaración sencilla, podría ser un documento que no aporte el detalle suficiente sobre qué controles concretos están presentes en “islas” de la organi-



Fastly y Signal Sciences han unido sus fuerzas para transformar el panorama de la seguridad.

Juntos creamos una plataforma de seguridad unificada, creada para DevOps de hoy en día. Signal Sciences, reconocida como visionaria en el informe Gartner Magic Quadrant 2020 para Web Application Firewalls, aporta a la familia Fastly soluciones de seguridad líderes en el sector.

Más información en:

[**fastly.com/es/signalsciences**](https://fastly.com/es/signalsciences)



desde el regulador para asegurar que se minimizan los riesgos legales que se originan en problemas burocráticos o formales.

– **¿Deben las Declaraciones de Aplicabilidad ofrecer información de eficacia de los controles declarados?**

La Declaración de Aplicabilidad exige enumerar los controles de seguridad que están implantados, pero no exige informar del grado efectivo de seguridad que proporcionan esos controles. En realidad, el RD no plantea en ningún momento que sea preciso implantar controles eficaces ni medir la eficacia de los controles implantados. Es obvio que el RSI es el primer interesado en evitar incidentes implantando controles eficaces; pero ¿qué ocurrirá ante incidentes que se produzcan por controles ineficaces?

Más aún, la definición de controles en varios marcos de referencia es muy superficial, cuando su implantación es muy compleja, por lo que es difícil evaluar esta eficacia. Por ejemplo, el control op.exp.1 de ENS describe en tres líneas la necesidad de un inventario de activos. Pero aplicarlo requiere abundante personal y herramientas dedicadas ex profeso a esta tarea.

– **La Declaración de Aplicabilidad se revisa cada tres años, mucho es eso ¿verdad?**

Este plazo es más amplio que el que establece el ENS (2 años) o en el resto de esquemas de seguridad habituales (1 año). De hecho, es el plazo de vigencia más amplio. Ante la más que probable dinámica

falta de adopción de medidas para subsanar las deficiencias detectadas en respuesta a un requerimiento dictado [...]. Pero no parece razonable que la Autoridad Competente establezca sanciones según una Declaración que puede tener hasta 3 años de antigüedad, generando indefensión en los operadores o trayendo como consecuencia un exceso de reclamaciones.

– **¿Será posible usar la Declaración de Aplicabilidad para hacer comparaciones?**

El RD no establece un formato uniforme para la Declaración de Aplicabilidad. Dado que cada organización ya tenía

su contenido. De esta forma se articularía un mínimo mecanismo de uniformidad de criterio tanto a nivel sectorial como al nivel de línea base.

Conclusiones

La selección por el RD de la Declaración de Aplicabilidad como elemento de comunicación a las autoridades competentes de las medidas de seguridad aplicadas es un paso en la dirección correcta. Nuestra experiencia en gestión de seguridad también apoya su uso como fundamento tangible de la estrategia de

En el RD no se establece la obligación de que los proveedores de los operadores dispongan de una Declaración de Aplicabilidad, pero es esperable que los segundos así lo exijan como parte de sus requisitos para proveedores.

adoptados sus propios marcos de control, con controles específicos y particulares que necesita para sus propias finalidades. Así, cada organización utilizará su propio modelo de Declaración de Aplicabilidad. Por lo tanto y salvo que se estandarice, la Declaración de Aplicabilidad no va a servir para comparar el grado de seguridad.

Dicho esto, la tentación es grande y habrá comparaciones. ¡Ay de aquellos que hayan sido demasiado exigentes consigo mismos!

seguridad de la organización. Que será más efectiva si se aplica con dos mejoras que nos permitimos la licencia de sugerir:

Admitir que haya Declaraciones de Aplicabilidad también por servicio, complementarias a las Declaraciones de Aplicabilidad del Operador. Para servicios bien definidos permitirá tener documentos más precisos, más maduros y, en definitiva, más confiables.

Interoperabilidad de las Declaraciones de Aplicabilidad. No es previsible ni deseable que haya un único formato de Declaración de Aplicabilidad. Hay controles de seguridad claramente sectoriales, y hay marcos de control y estándares de referencia ya aceptados. Pero sí debería exigirse a las Autoridades Competentes que trabajen en ser interoperables entre sí: Formatos comunes o convertibles entre sí, un mecanismo de control y seguimiento lo más parecido posible. Y evitar así el riesgo de que las Autoridades de Control se constituyan en Islas de Cumplimiento.

Y sin perder nunca el objetivo de la Directiva: “lograr un elevado nivel común de seguridad para mejorar el funcionamiento del mercado interior”. Este Reglamento y su DA deben contribuir a ello, o fracasará.

Y no se nos olvide, la persona física que firma una Declaración de Aplicabilidad adquiere responsabilidades legales. Cuidado con lo que firman. ■

MARIANO J. BENITO
CISO

JAVIER ZUBIETA
Director de Marketing y Comunicación
Secure e-Solutions de GMV

Si el CSIRT de referencia conociera la DA podría asesorar también sobre su contenido. De esta forma se articularía un mínimo mecanismo de uniformidad de criterio tanto a nivel sectorial como al nivel de línea base.

de cambios en esta Declaración durante su plazo de vigencia, ¿qué riesgos comporta que el supervisor disponga sólo de una versión anticuada de la Declaración de Aplicabilidad? ¿Estará la autoridad competente para procesar declaraciones actualizadas cada varios meses?

– **¿Se puede aplicar sanciones basadas en Declaraciones obsoletas?**

Aunque el reglamento no hace referencia a las sanciones, RDL 12/2018 establece entre otras como infracción muy grave (Art 36, 2.a) la “falta de adopción de medidas para subsanar las deficiencias detectadas [...] cuando éstas le hayan hecho vulnerable a un incidente [...] y no hubiera atendido los requerimientos dictados por la autoridad competente con anterioridad a la producción del incidente.” Y establece como infracción grave (art 36.3.b) “b) La

– **¿Darán las Autoridades Competentes feedback sobre las Declaraciones de Aplicabilidad entregadas?**

No parece, aunque podría ser muy interesante. El Artículo 15.4 señala capacidades de inspección de cumplimiento por parte de la Autoridad Competente apoyada en el CSIRT de referencia. Pero el Reglamento limita esta inspección a comprobar cumplimiento, pero no se exige que se sugieran mejoras en su contenido.

Pero en el Artículo 15.5, al hilo de la función supervisora, señala que “Los CSIRT de referencia colaborarán con las autoridades competentes [...] En particular, facilitarán asesoramiento técnico sobre la idoneidad de las medidas de seguridad adoptadas”. Y si el CSIRT de referencia conociera la Declaración de Aplicabilidad podría asesorar también sobre



ágora**SIC**

Centro de Conocimiento en Ciberseguridad

CIBERSEGURIDAD EUROPEA

Marcada a fuego



Una de las grandes apuestas de la UE –y no exenta de polémica– se está concentrando en crear un marco común de esquemas de evaluación y certificación de la ciberseguridad de productos TIC, procesos y servicios (incluidos los especializados en ciberseguridad). No es tarea fácil, porque hay que tocar muchos palos: fabricantes y desarrolladores de TIC y con TIC, grandes proveedores de servicios y usuarios esenciales, críticos y estratégicos...; y todo ello en un contexto en el que las perspectivas del despliegue de 5G, la migración a la nube, la IA, la OT conectada y el crecimiento hipermasivo de la IoT no dan respiro.

Sin embargo, la ocasión se presenta también como una oportunidad para fomentar la tecnología europea, dejando algún terreno a cada Estado miembro (en la medida en que se lo gane) y, también –por qué no decirlo– para intentar proteger los mercados de la UE y a la ciudadanía de proveedores con requisitos en ciberseguridad no aceptables, vengan de fuera o de dentro.

SIC realiza en este especial una puesta al día de la construcción de la evaluación y certificación en Europa, un edificio con cimientos, pero cuya obra no ha terminado.

SUMARIO

- La apuesta por la evaluación y certificación de productos en la UE: panorama
- La certificación de ciberseguridad en Europa: dos años del Cybersecurity Act, por JOSÉ RUIZ y JAVIER TALLÓN
- LINCE, una herramienta que aporta más confianza a la ciberseguridad, por BORIS DELGADO y CARLOS M. FERNÁNDEZ
- Modelo de las tres sonrisas en un esquema de certificación en ciberseguridad industrial, por JOSÉ VALIENTE
- La seguridad y la evaluación de conformidad y certificación de PSC eIDAS y servicios, un enfoque global, por PALOMA LLANEZA
- ¿Quién evalúa al evaluador?, por Pablo López
- Sobre la Certificación de la Seguridad en una Industria Digitalizada, por JORGE DÁVILA



El primer esquema aprobado en 2021 podría ser EUCC-Common Criteria based European Candidate Cybersecurity Certification Scheme

La apuesta por la evaluación y certificación de ciberseguridad de productos TIC en la UE: panorama

La Unión Europea quiere que los productos que se comercializan en ella y, también, los que se fabrican en su seno tengan un nivel de ciberprotección adecuado. Para ello, desde 2019, con la aprobación de la Ley de Ciberseguridad se puso en marcha una carrera a contrarreloj para aprobar un esquema de evaluación y certificación de productos TIC (también de servicios y procesos). Este año se espera que ENISA deje fijada definitivamente su propuesta tras un trabajo de casi tres años, en el que participan el sector público y el privado. De hecho, hay varias entidades españolas colaborando en los grupos de trabajo establecidos: no en vano somos uno de los referentes de la UE en algunos segmentos de la evaluación y la certificación.

| ANA ADEVA y JOSÉ MANUEL VERA (Equipo SIC) |

Decía el físico y matemático británico **William Thomson Kelvin** (1824–1907) que “lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre”, una máxima con la que manifestaba la importancia de evaluar y certificar productos, servicios, personas... Y en esas estamos: intentado desarrollar formas de proceder y revisar (en este caso, evaluar y certificar) que garanticen que lo que se ofrece ‘cumple con lo que promete’. Quizá el ejemplo genérico más cercano sea el **marcado CE (Conformidad Europea)**, fruto de la Directiva 93/68/CEE, y que llevan gran parte de los productos que consumimos (ver **Figura 1**).

Curiosamente, no implica mejor o peor calidad, sino únicamente que el producto ha sido evaluado (puede ser por su fabricante), y que reúne unos requisitos mínimos de seguridad, salud y respeto medioambiental, etc., propios de la UE. Pero se limita a productos físicos y marca, únicamente, el mínimo exigido. Por eso, sectores en los que la seguridad es una prioridad, como el de automoción, además tienen en marcha iniciativas privadas, como **EuroNcap**, que certifica y valora el nivel de protección de cada modelo frente a pruebas de seguridad concretas.

El problema es que en el mundo digital no existen apenas certificaciones reconocidas y generalizadas en todo el mundo y que, a efectos generales, garanticen un mínimo grado de protección de los dispositivos conectados a consumidores y empresas, algo preocupante teniendo en cuenta que el año pasado, un estudio del **Ponemon Institute** encontró que el 80% de las aplicaciones

de dispositivos conectados (IoT) tenían vulnerabilidades de seguridad. Por ello, evaluar y certificar la ciberseguridad de productos, sis-

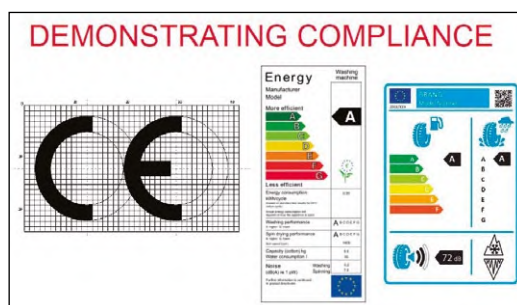


Fig. 1.- Certificaciones de consumo.

temas y servicios se ha convertido en una de las grandes prioridades de la UE. Su objetivo en lo que toca a los productos: que cualquiera, vendido en el Viejo Continente, tenga un sello que indique que es ‘ciberseguro’ frente a lo conocido.



Fig. 2.- El NCSC publicó la ‘Serie Rainbow’ pionera de la actual evaluación.

Un proyecto de Defensa: la serie ‘Rainbow’

No es una idea nueva. La historia de las certificaciones de ciberseguridad de productos comenzó en EE.UU. hace casi cuatro décadas y, como pasó con Internet, el origen de las evaluaciones y certificaciones en ciberseguridad también tiene un origen militar, fruto de su preocupación por contar con sistemas de confianza en entornos críticos. Para ello, el **Centro Nacional de Seguridad Informática (NCSC)** estadounidense, publicó la denominada ‘Serie Arcoiris’ (*Rainbow Books*), en la que se ofrecían unas pautas para realizar un proceso de evaluación para sistemas confiables. Quizá el documento más conocido, por su importancia para la ciberseguridad de aquel momento, fue el denominado ‘Criterios de evaluación de sistemas informáticos de confianza’ (*Trusted Computer System Evaluation Criteria, TCSEC*) o Libro naranja –por el color de su portada–, que fue implementado en 1983 –y actualizado en 1985– como estándar por el Departamento de Defensa (DoD) estadounidense (ver **Figura 2**).

El TCSEC se utilizó para evaluar, clasificar y seleccionar los sistemas informáticos que se estaban considerando para el procesamiento, almacenamiento y recuperación de información confidencial o clasificada. Sin embargo, conllevaba un proceso que era lento y costoso para las empresas TIC proveedoras por lo que no tuvo el éxito esperado.

Europa también se fijó en ese modelo y en 1990, Francia, Alemania, Países Bajos y Reino Unido publicaron un documento conjunto bautizado como ‘Criterios de Evaluación



ción de la Seguridad de la Tecnología de la Información-ITSEC', que un año después la **Comisión de las Comunidades Europeas** aprobó como esquema de evaluación y certificación de seguridad informática (con niveles de E0 a E6) y que fue adoptado por otros muchos países. A diferencia de TCSEC, ITSEC (e ITSEM, que exponía el método) no requería que los objetivos evaluados contuvieran características técnicas específicas para lograr un nivel de garantía particular. Cada evaluación se basada en verificar las características de seguridad identificadas en el objetivo de protección.

Sin embargo, tanto TCSEC como ITSEC-CITSEM no disfrutaron de la aceptación esperada ni supieron evolucionar al ritmo de la llegada de adelantos y nuevas TIC. Así que, para impulsar una certificación global, en 2005, ambos sistemas fueron reemplazados, tras un acuerdo global, por los llamados Criterios Comunes (*Common Criteria*, CC), actualmente en vigor (que califican los productos según su nivel de confianza de EAL1 al EAL7).

Su objetivo era ofrecer unos niveles de evaluación definidos para evaluar la seguridad de un producto de forma similar en todo el mundo, a través de centros acreditados. Su implantación es tal que, incluso, existe una metodología con esos criterios: la Norma ISO/IEC 18045. Además, también se estableció un estándar de validación criptográfica relacionado, el FIPS 140-2.

Se trata de generar confianza en productos que hayan sido evaluados conforme a estas metodologías de forma que, para su uso, no se precise una evaluación adicional. Y se trata de una certificación que aún tiene mucho recorrido. Prueba de ello es que 2020 fue el segundo año desde su creación con mayor número de productos certificados (388), sólo superado, en 2016, con 395.

Cabe destacar también que, en 1997, se firmó un acuerdo en Europa, conocido como **SOG-IS** ('Seguridad de los Sistemas de Información del Grupo de Altos Funcionarios'), para poner en marcha un grupo de trabajo fruto de la Decisión del Consejo de la UE del 31 de marzo de 1992 (92/242/CEE) para "coordinar la estandarización de los perfiles de protección Common Criteria (CC) y las políticas de certificación entre los organismos de certificación europeos para tener una posición común frente al resto del mundo". Actualizado en 2010, sus participantes son organizaciones gubernamentales o agencias nacionales de países de la UE o la **EFTA (Asociación Europea de Libre Comercio)**, entre las que están una decena de entidades, como el **CCN**, por parte de España, el **BSI** alemán, la **ANSSI** de Francia, el **OCSI** de Italia, el **NLNCSA** de los Países

Bajos y el **CESSG** de Reino Unido. El conjunto de hechos significó la firma de un acuerdo de reconocimiento mutuo de certificados CC.

Buscando una certificación aceptada

Sin embargo, dado que certificar productos bajo la metodología de Criterios Comunes es un proceso complejo y costoso, varios países europeos también han puesto en marcha otro tipo de certificación denominada 'ligera', mucho más sencilla y básica, pero al alcance de gran parte de las compañías. Así, actualmente en Europa, en distintos niveles de desarrollo y aplicación, conviven **Lince** (España), **BSZ** (Certificación Acelerada de Ciberseguridad, Alemania), **CSPN** (Francia) y **BSPA** (Holanda). Además, los países también cuentan con certificaciones específicas, por ejemplo, para productos criptográficos usados en Defensa o para manejo de información clasificada.

Otros estados de la UE han puesto en marcha otro tipo de certificación y evaluación de ciberseguridad de productos con distintos criterios. Por ejemplo, a finales de 2019, el **Centro Nacional de Seguridad**

Cibernética de Finlandia (NCSC-FI), lanzó un programa de certificación de seguridad de información de dispositivos inteligentes, basado en los estándares para el IoT del **Instituto Europeo de Normas de Telecomunicaciones (ETSI)**. Su cumplimiento permite recibir una etiqueta oficial que los designará como aprobados por NCSC-FI.

Además, destaca la iniciativa de Reino Unido (hoy fuera de la UE), a través del **Departamento para lo Digital**, a mediados de 2020, para certificar la seguridad de productos. Precisamente, a ello dedicó más de 500.000 euros, para incentivar la creación de esquemas de diseño que prueben la seguridad de los productos de Internet de las cosas (IoT). Y el gobierno de ese país tiene en marcha su 'Código de prácticas para la seguridad de IoT del consumidor' al que se pueden adherir de forma voluntaria las marcas para evidenciar que tienen unos requisitos mínimos de ciberseguridad.

Cifrado seguro

También es destacable la apuesta por certificar la calidad criptográfica de productos TIC (sean o no de seguridad) que incorporen criptografía, algo cada vez más común. El Reglamento (UE) nº 910/2014 sobre identifica-

ción electrónica (eID) y servicios de confianza para transacciones electrónicas en el mercado interior, más conocido como **eIDAS**, supuso desde hace más de un lustro un cambio importante en la UE al facilitar las interacciones electrónicas confiables entre los ciudadanos, las empresas y las autoridades públicas, a través de las fronteras estatales europeas. Su objetivo es establecer unos mecanismos, de obligatorio cumplimiento, que garanticen la confianza en estos servicios. Para ello, esta normativa requiere que los sistemas y proveedores de servicios estén cualificados con respecto a unos requisitos específicos. El estado cualificado se aplica a certificados, marcas de tiempo, hardware criptográfico, firmas electrónicas y sellos. En este último sentido, la UE estableció una serie de normas técnicas para evaluar la seguridad de los dispositivos cualificados de creación de firmas y sellos electrónicos, que se recogen en la Decisión de Ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016.

Asimismo, destaca en EE.UU. el **FIPS 140-3**, el nuevo estándar para módulos criptográficos que sustituirá al FIPS 140-2. Así, hasta septiembre de 2021, los fabricantes pueden testar su tecnología contra FIPS 140-2 o FIPS 140-3. Esto supone una ventana temporal en la que los productos que actualmente se encuentran certificándose bajo FIPS 140-2, pueden terminar siéndolo en dicho estándar, aunque "es recomendable hacerlo contra FIPS 140-3", dicen los especialistas, ya que será el nuevo estándar que se imponga en el mercado.

En todo caso, y a futuro, la Comisión Europea tiene en mente promover la creación de un esquema de certificación de criptografía, un asunto complejo, como también lo es hacer lo propio con la IA o con el desarrollo seguro.

Sello de certificación de privacidad

En el entorno de la privacidad también existen iniciativas como el 'Sello Europeo de Privacidad' (*European Privacy Seal*), un prototipo de Certificación impulsado por la UE que se basa en la confidencialidad, calidad y seguridad en la gestión de los datos de carácter personal. El Sello establece un estándar europeo de privacidad. Fue creado como un proyecto en el 2007 pero actualmente ya se encuentra en funcionamiento, de forma voluntaria, dirigido por la autoridad de Protección de Datos establecida en Alemania y con la colaboración de la Agencia Española de Protección de Datos. De momento, ya cuentan con el Sello Europeo de Privacidad entidades significativas como **Quentry**, **Microsoft**, **Telemed** e, incluso, en su momento, españolas como el **Banco Guipuzcoano** (hoy Banco Sabadell).



Fig. 3.- Ciberetiqueta del NCSC de Finlandia.



European Privacy Seal
EP-S-XZ57BD / Valid till 2022-07
- Criteria Catalogue v201701 -

Fig. 4.- Sello europeo de privacidad.



No obstante, conviene no olvidar que una cosa es certificar la gestión de los datos personales (confidencialidad, calidad y seguridad), y otra diferente (aunque relacionada) certificar a efectos técnicos la seguridad de los productos TIC y los procesos.

Cybersecurity Act

El antes y el después de este camino hacia la certificación y evaluación de la ciberseguridad de productos (entre los que se encuentra el subconjunto de productos específicos de ciberseguridad) llegó –como antes se apuntaba– con la **Ley de Ciberseguridad europea** (Cybersecurity Act), aprobada en 2019, y cuyo artículo octavo otorga a **ENISA** el mandato de supervisar los avances en el ámbito de la normalización y la certificación, acorde a lo ya hecho por entidades europeas como **CEN**, **CENELEC**, **ETSI**, así como el **Grupo de Coordinación de Ciberseguridad (CSCG)**. “La certificación desempeña un papel fundamental para aumentar la confianza y la seguridad en productos y servicios que son cruciales para el mercado único digital. En este momento, existen en la UE varios esquemas de certificación de seguridad diferentes para productos de TIC. Pero, sin un marco común, existe un riesgo creciente de fragmentación y barreras en el mercado único europeo”, se decía en la Ley de Ciberseguridad.

Así, el objetivo es crear un marco que permita desarrollar esquemas de certificación personalizados y basados en riesgos que hagan posible atestiguar que tanto los dispositivos informáticos tradicionales, como los dispositivos conectados que componen el Internet de las cosas (IoT) y servicios, cumplen con los requisitos especificados.

Según se destaca en la Ley, cada esquema europeo especificará: las categorías de productos y servicios cubiertos, los requisitos de ciberseguridad, por ejemplo, por referencia a estándares o especificaciones técnicas, el tipo de evaluación (como autoevaluación o evaluación de terceros), y el nivel de seguri-

dad deseado (básico, sustancial y alto), que son proporcionales al nivel de riesgo asociado con el uso previsto del producto, servicio o proceso, según la probabilidad e impacto de un incidente. En definitiva, se trata de generar una mayor confianza en los productos IoT y usar, también esta etiqueta, similar, en su espíritu, a la que llevan ya electrodomésticos, ruedas, etc. como argumento comercial en el mercado internacional.

Grupos de trabajo

En línea con lo dicho, a través de ENISA se pusieron en marcha en 2019 los trabajos

SOG-IS, MRA (Acuerdo de Reconocimiento Mutuo), que cuenta con 20 años de experiencia. Por supuesto, también estará inspirado en los Criterios Comunes de Evaluación de la Seguridad de la Tecnología de la Información.

Meses para el primer gran esquema

Europa no cuenta todavía con el primer esquema. Hay dos adelantados, el de servicios Cloud, que se espera aprobar en 2021 y el EUCC (Common Criteria based European candidate cybersecurity certification scheme, por sus siglas en inglés). Basado en los Criterios Comunes (ISO/IEC 15408 y 18045), servirá para productos tan variados como circuitos integrados, tarjetas inteligentes para firma electrónica, identificación (pasaportes), banca, tacógrafos para camiones y, por supuesto, software (para cifrar discos, clientes VPN, etc.).

La idea es que sea el heredero de los esquemas que ha habido hasta hoy y se convierta en Ley europea con un periodo de transición que podría rondar los dos años, un tiempo considerado aceptable tanto para ‘migrar’ los antiguos certificados al nuevo estándar como para poner en marcha medidas que precisarán cumplirse como, por ejemplo, un sistema de gestión de parches de seguridad y actualizaciones para garantizar la protección de los dispositivos durante su vida útil. De cualquier forma, el “nuevo esquema necesitará una cooperación más estrecha entre los proveedores y los laboratorios para funcionar adecuadamente”, destaca un notable experto español, que también recuerda el papel fundamental que jugarán los laboratorios para la certificación y para vigilar y garantizar que se cumpla lo

certificado durante el tiempo que se comercialice un producto.

Eso sí, de momento, el marco será “voluntario” aunque la Ley de Ciberseguridad ‘abra la puerta’ a que la certificación sea obligatoria para ciertos productos si la Comisión cree que son productos en riesgo. De cualquier forma, muchos consideran que será uno de sus grandes problemas: la falta de cumplimiento ante la falta de infracciones por no exigirse ‘por

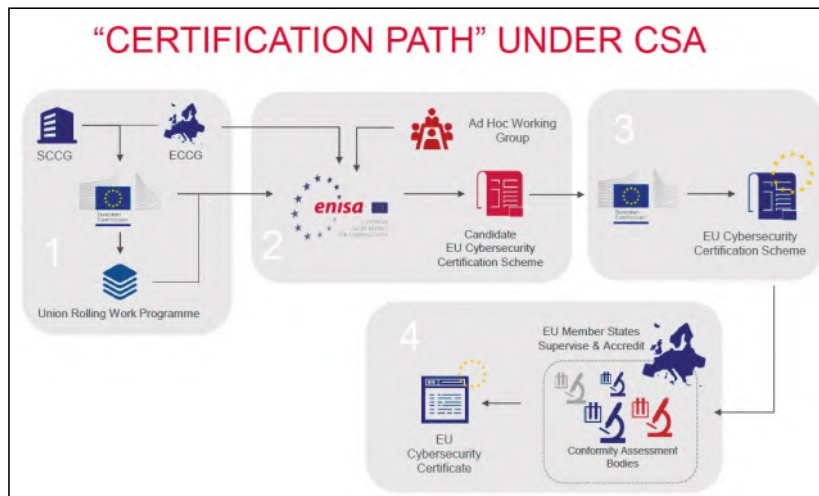


Fig. 5.- El camino hacia la certificación en la UE.

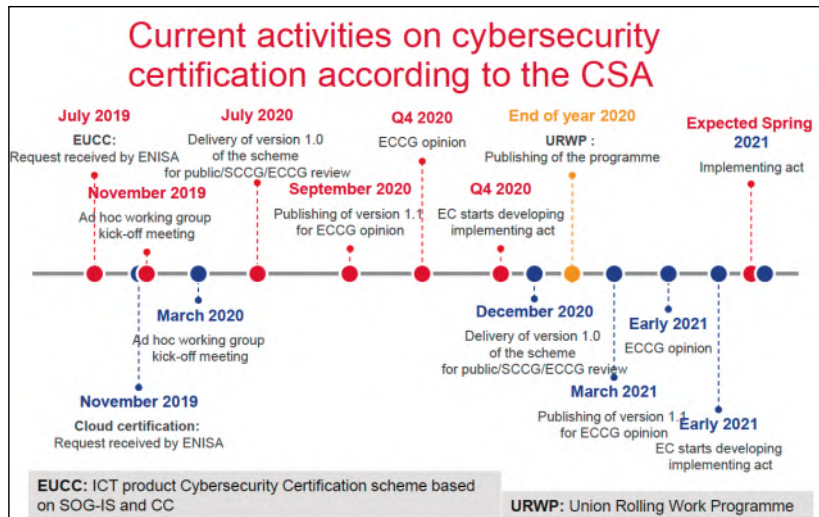


Fig. 6.- Calendario de aprobación del esquema de certificación de productos.

para aprobar el esquema de certificación con la participación del **Grupo Europeo de Certificación de Ciberseguridad (ECGG)** y del **de Certificación de Ciberseguridad de Partes Interesadas (SCCG)**, que es el responsable de asesorar a la Comisión y a la propia Agencia sobre cuestiones estratégicas acerca de este tema. El objetivo: presentar un borrador de esquema de certificación de ciberseguridad candidato que sirva como sucesor del actual



Ley'. De hecho, algunos también consideran negativo que, para facilitar este tipo de certificados, aquellos que aspiran al nivel 'básico' puedan "realizar ellos mismos pruebas de conformidad" para productos y servicios que "presentan un bajo riesgo para el interés público", algo que ocurre en la mayoría de los productos de consumo, cuyos distribuidores o fabricantes 'garantizan' su seguridad.

Iniciativas privadas

Desde hace años, el sector privado también está impulsando en paralelo certificaciones de productos IoT. En 2015, la **Alianza Fast Identity Online (FIDO)**, creada en 2013 para proporcionar estándares abiertos para una autenticación más simple y sólida, hizo el suyo, que adoptaron los primeros productos iOS de Egis, Nok Nok Labs y Samsung SDS, junto con una línea de teléfonos inteligentes, entre otros. En 2016, **ICSA Labs**, de **Verizon**, dio a conocer un programa de certificación y pruebas específicamente para dispositivos y sensores de IoT, en un intento por mejorar los estándares generales de seguridad en los dispositivos informáticos integrados. El estándar estaba basado en iniciativas como el OWASP Internet of Things Top 10, Industrial Internet Consortium Reference Architecture y IoT Trust Framework de la **Online Trust Alliance**.

El año pasado, el **Comité Técnico de Ciberseguridad de ETSI** presentó un nuevo estándar para la ciberseguridad en IoT. En él, se establecieron unas 'líneas rojas' que no se deberían pasar para ofrecer una ciberprotección aceptable en los productos de consumo conectados a Internet y que deberían incluir futuros esquemas de certificación de IoT. La norma ETSI **EN 303 645**, 'Ciberseguridad para la Internet de las cosas de los consumidores', también pretende inspirar otras iniciativas similares para evitar ataques a gran escala usando dispositivos inteligentes. Así, ETSI EN 303 645 describe 13 disposiciones para la seguridad de una amplia gama de dispositivos de consumo de IoT y sus servicios asociados. En la norma también se establecen cinco disposiciones específicas de protección de datos para la IoT del consumidor. Este estándar también es la base del esquema de certificación de seguridad cibernética IoT de empresas privadas como **Nemko**.

El futuro

Para analizar la situación y el futuro de las certificaciones en ciberseguridad tanto en producto, como en servicios y procesos, Enisa ya ha llevado a cabo reuniones con los principales referentes del sector público y privado a fin de conectar los requisitos regulatorios europeos con 'fórmulas' para alinear la estandarización y los objetivos políticos de la UE.

COMPARACIÓN DE METODOLOGÍAS DE CERTIFICACIÓN LIGERA EN EU

LINCE ST	CSPN ST	BSPA ST	BSZ ST
Identificación del TOE	Identificación del TOE	Identificación del TOE	Identificación del TOE
Uso de TOE	Uso de TOE	Uso de TOE	Uso de TOE
Descripción del TOE	Descripción del TOE	Descripción del TOE	Descripción del TOE
Entorno operativo	Entorno operativo	Entorno operativo	Entorno operativo
Supuestos	Supuestos	Supuestos	Supuestos
Activos	Activos	Activos	Activos
			Atacantes
Amenazas	Amenazas	Amenazas	Amenazas
Funciones de seguridad	Funciones de seguridad	Funciones de seguridad	Funciones de seguridad
	Límites de evaluación (CR)	Límites de evaluación (DA)	Límites de evaluación (ST)

Fig. 7.- Comparación de metodologías ligeras.

Además, la Comisión ha solicitado a ENISA preparar un plan de certificación candidato de seguridad cibernética en las redes 5G lo antes posible. También, está preparando 'actos delegados' y solicitará la normalización de las certificaciones que se aprueben a CEN-CENELEC y ETSI.

Así, el sector trabaja ya en los pasos posteriores a la certificación y cómo afectará el comportamiento del usuario final o cómo impulsar los productos certificados. Sin embargo, aún hay muchas preguntas por responder como, por ejemplo, la forma de fabricar productos cumpliendo por defecto el esquema, cómo aplicarlo por sectores o, en caso de que el dispositivo sufra un problema de seguridad, quién será el responsable si ha sido certificado.

Críticas contra la certificación

De hecho, hay especialistas que consideran que la Ley de Ciberseguridad en este aspecto podría terminar siendo una legislación fantasma, aprobada pero sin apenas em-

presas que apuesten por no seguirla en este frente si no es obligatorio o se nombran organismos encargados de hacerla cumplir, bajo sanción. De cualquier forma, la Ley sí prevé que las Autoridades Nacionales de Certificación de Ciberseguridad tramiten las reclamaciones, acorde a la gravedad de la denuncia e informando del progreso y el resultado de la investigación en un tiempo razonable.

Asimismo, podría generar 'sentimientos encontrados', especialmente entre las empresas de fuera de la UE. Ya en 2017, la **Coalición de Ciberseguridad de IoT**, entre otras entidades, manifestó que este tipo de iniciativas deberían "aprovechar las mejores prácticas existentes y estándares mundiales dirigidos por la industria". Incluso hay quien sostiene que "las regulaciones inhiben la innovación". También, ha sido criticado el hecho de que las certificaciones pudieran crear una 'falsa sensación de seguridad' alertando de la complejidad de garantizar la misma seguridad durante la vida de un producto que cuando se certificó antes de venderse. ■

Certificación de automóviles conectados

Pocos productos conectados son tan complejos de certificar como los coches conectados, sobre todo cuando puedan hacerlo a redes 5G y tengan capacidades autónomas o semiautónomas. Por eso, tanto las marcas de coches, como fabricantes y proveedores están poniendo en marcha diferentes iniciativas, alineadas con las leyes europeas, que les permitan certificar la ciberseguridad de sus coches. En España, por ejemplo, la compañía **Eurocybcar** es una de las pioneras europeas en ofrecer un sello de ciberseguridad para todo tipo de vehículos, con tres tipos de pruebas y niveles de seguridad de uno a cinco. En Reino Unido, también se trabaja en esa dirección, para automóviles, en el consorcio '**Cinco estrellas**'. En definitiva, se trata de emular el trabajo de organizaciones como '**EuroNCAP**' pero en ciberseguridad.

También, es destacable el caso de la empresa española **Zerolynx**, que ofrece su 'Open Mobility Security Project', un proyecto de código abierto dedicado a estandarizar un marco de controles técnicos para evaluar la seguridad en todo tipo de vehículos, desde un tren hasta un coche. Precisamente, en 2020, la ONU aprobó un Reglamento, elaborado por ONU / **UNECE WP.29**, que se aplicará en la UE a partir del 1 de julio de 2022 a los vehículos de nueva homologación y a partir del 1 de julio de 2024 a todos los vehículos nuevos que se vendan en sus países miembros. Se espera que más de 50 países se sumen a él, certificando la ciberseguridad de sus coches.



Algunas fuentes de información: ENISA, ECSO y la OC-CCN

Existe una gran variedad de informes y documentos que recogen el estado y las diferentes actividades relacionadas con la evaluación y certificación de la ciberseguridad de productos (además, de los sistemas y procesos) publicados por organismos públicos y asociaciones vinculados con la materia. Aunque en menor medida, también hay disponibles otros realizados por empresas privadas dedicadas a esta labor, como *jtsec* o *Leet Security*, entre otras, que ofrecen abundantes análisis sobre las novedades en este ámbito.

Las propuestas de ENISA

En Europa, los documentos de **ENISA** son de obligada lectura, dado su papel en la elaboración de los esquemas candidatos que compondrán el futuro Marco de Certificación de Ciberseguridad europeo y que, como bien es sabido, abarcarán productos, servicios y procesos TIC (véase SIC 139).

Los más recientes, publicados en 2020, son dos amplios informes que recogen la situación actual y los próximos pasos en la materia. El primero de ellos, es el borrador del Esquema de Certificación de Ciberseguridad europeo basado en Criterios Comunes (EUCC), el primer esquema candidato de la UE que sustituirá los existentes que operan bajo el SOG-IS MRA para productos TIC. Éste se detalla ampliamente en el documento titulado **'Cybersecurity Certification. EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS'**. En él, la Agencia explica que "el EUCC cubrirá la evaluación de las vulnerabilidades de las implementaciones criptográficas en las funcionalidades de seguridad de un producto de TIC de acuerdo con los requisitos de los criterios de evaluación y la metodología definidos en las normas de evaluación descritas en el documento".

En paralelo, ENISA está preparando un segundo esquema para la certificación de la ciberseguridad de los servicios en la nube y en diciembre publicó el informe **'EUCS - Cloud Services Scheme'**. Aunque es muy diferente del esquema EUCC, centrado en productos TIC, la Agencia explica que comparten puntos en común. Por ejemplo, "en torno a la organización de la supervisión del cumplimiento y las evaluaciones entre pares", y "aprovecha algunos principios que se definen por primera vez en el esquema EUCC".

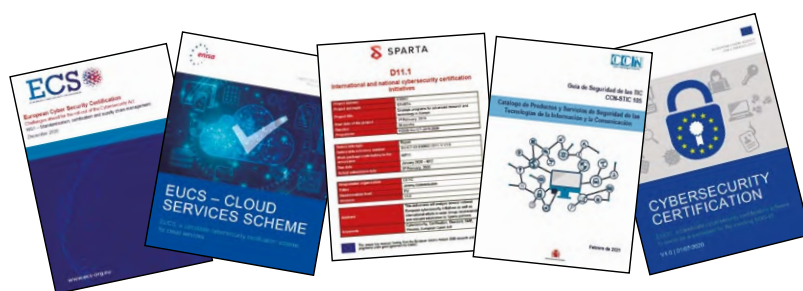
Estado del arte de la certificación

Otros de los documentos de referencia sobre certificación es el publicado el año pasado por el proyecto **SPARTA** de la UE, la red de colaboración para el desarrollo de la investigación, innovación y la formación en el ámbito

de la ciberseguridad europea, financiado por el programa Horizonte 2020.

Bajo el título **'Iniciativas de certificación de ciberseguridad nacional e internacionales'**, ofrece un buen resumen tanto de lo que supone, por primera vez, la aprobación de un marco de certificación en ciberseguridad en la UE, como de los estándares y marcos de certificación más importantes en el resto del mundo. Entre otras recomendaciones, la iniciativa recuerda que "las certificaciones de ciberse-

Precisamente, en su informe 'Certificación europea de ciberseguridad. Desafíos futuros para la implementación de la Ley de Ciberseguridad', de diciembre de 2020, la ECSO explica que "el Marco europeo de Certificación de ciberseguridad incluirá varios esquemas de certificación para productos, servicios y procesos de TIC horizontales, como el de Criterios Comunes (EUCC) o cubriendo verticales específicos, como servicios en la nube, IoT o 5G. Pero estos verticales podrían usarse como es-



guridad deben ser, siempre que sea posible, un valor agregado a los productos, procesos o servicios y no algo que cree una barrera de entrada o distorsione la competencia". Además, resalta la importancia de no dejar de lado "a los actores más pequeños, como las pymes" evitando "el diseño de esquemas 'monstruosos' que requieran una gran inversión de tiempo y dinero".

Certificación de componentes

El documento también resalta que "los sistemas basados en la nube, las implementaciones de IoT en fábricas o en ciudades, o incluso automóviles, son ahora tan complejos que una certificación global solo se puede lograr mediante el ensamblaje de certificación de componentes. 'Composición' es el nombre genérico de este proceso de ensamblaje. Éste será un campo en crecimiento ya que certificaremos cada vez más partes involucradas en productos complejos. Algunos actores, como la **Organización Europea de Ciberseguridad (ECSO)** y sus socios, ya están analizando esto y deberíamos seguir de cerca cualquier nuevo desarrollo", concluye.

quemas horizontales que luego se especializan para un sector específico, como dispositivos médicos, medidores inteligentes o movilidad conectada. Por lo tanto, la capacidad de certificar un producto 'por composición' desempeñará un papel clave para la rentabilidad y la usabilidad de la certificación de la UE. Aunque también es consciente de que "la combinación de "productos 'seguros' certificados" no da como resultado un "sistema seguro" o un "producto conectado seguro".

Ley de Ciberseguridad y RGPD

La **Universidad de Tilburg** (Holanda) también dispone de un interesante y exhaustivo análisis, realizado como tesis doctoral por **M.H. Veldhoen**, sobre la relación entre el próximo marco de certificación de Ciberseguridad europeo frente a los mecanismos del RGPD (regulados en los artículos 42 y 43), en relación con los dispositivos de IoT. Recordando que en el caso del RGPD son mecanismos en materia de protección de datos, destaca, por ejemplo, el carácter voluntario de ambos, no siendo la certificación obligatoria. Sin embargo, "la Ley de Ciberseguridad tiene una excepción en la

Ingecom

www.ingecom.net

okta

www.okta.com



Ante una nueva normalidad, un nuevo modelo de identidad

Okta se distribuye en Iberia a través de Ingecom, Value Added Distributor (VAD) especializado en soluciones de ciberseguridad y ciberinteligencia. Si quieres más información sobre las soluciones de identidad de Okta, llama al +34 915 715 196 o contacta con nosotros en comercial_ingecom@ingecom.net



que esa cláusula puede ser anulada, creando un marco en el que ciertos certificados podrían ser obligatorios para ciertos productos si la Comisión cree que son productos en riesgo". Asimismo, indica el hecho de que "en ambos casos deben emitirse por un período de tiempo específico y luego pueden renovarse". Sin embargo, mientras que el RGPD permite un período máximo de certificación de tres años, la Ley de Ciberseguridad deja la duración exacta del período de certificación para que se determine en un esquema específico. Para los dispositivos de IoT que tienen diferentes duraciones es algo bueno, dado que la importancia que puede tener la certificación de ciberseguridad para estos dispositivos difiere enormemente en función de cuán (no) complicados y (no) importantes son y con qué frecuencia el estado del arte para una categoría en particular o tipo de cambio de dispositivo, lo que requiere que la certificación se actualice con más o menos frecuencia".

España, ENS y certificación de productos de TIC y de seguridad TIC

Nuestro país es uno de los más adelantados de Europa en estos terrenos por requisitoria legal (información clasificada y ENS y guías derivadas), sino por disponer de un esquema. Además de trabajar con CC, dispone de la metodología de certificación ligera LINCE. Uno de los documentos de referencia sobre la certificación de ciberseguridad es, sin duda, el **Catálogo de Productos de Seguridad TIC (CPSTIC)**, que publica y actualiza asiduamente el Organismo de Certificación (OC) del **Centro Criptológico Nacional (CCN)**. En él, se ofrece un listado de los productos de seguridad TIC que disponen de unas garantías de protección contrastadas en dos categorías: 'Productos Aprobados', aquellos cuyo uso está aprobado en sistemas que manejen información clasificada y 'Productos Cualifica-

dos', los que son aptos para ser utilizados en sistemas contemplados por el Esquema Nacional de Seguridad (ENS).

A fecha de cierre de esta edición, la más reciente actualización publicada del CPSTIC (febrero de 2021) incluye cerca de 330 productos cualificados y aprobados. Dentro de los primeros se incluyen ocho categorías en las que hay productos 'cualificados' de 45 fabricantes, según la web del **OC-CCN**. De ellos, una decena son españoles: **Autek Ingeniería, authUSB, Epicom, Grupo ICA, Indra, Istria, Panda Security, S2 Grupo, CCN y SIA**.

Dentro de los productos 'aprobados' existen también ocho con un total de 24 fabricantes que tienen productos 'aprobados', según el OC-CCN. De ellos, una decena son de origen español: **Arpa, Auttek, authUSB, Consuegra S. Coop., Epicom, Grupo ICA, Indra, Safelayer Secure Communications -hoy Entrust-, Novatronik Sistemas y Tecnobit. ■**

Quién evalúa y con qué metodología en España

EMPRESA	EVALUACIÓN	INFORMACIÓN
APPLUS LABORATORIES Barcelona / Madrid	Common Criteria. EAL6+ (ASE_TSS.2, ALC_FLR.3) Dominio técnico de TI SOG-IS. Calificado para los dominios técnicos "Tarjetas inteligentes y dispositivos similares" y "Dispositivos de hardware con cajas de seguridad". LINCE	 www.appluslaboratories.com
BRIGHTSIGHT Barcelona	Common Criteria EAL2 + ADV_FSP.3, ADV_TDS.2, ALC_FLR.2, ATE_COV.2, ATE_DPT.1 LINCE	 www.brightsight.com
CLOVER TECHNOLOGIES Leganés (Madrid)	Common Criteria. EAL1 LINCE	 www.cloverttechnologies.es
DEKRA TESTING AND CERTIFICATION San Sebastián de los Reyes (Madrid)	Common Criteria. EAL4+ (AVA_VAN.5, ALC_FLR.3 y ALC_DVS.2) ISO/IEC 19790 y 24759. Requisitos de Seguridad y Pruebas para Módulos Criptográficos. Hasta SL4. Dominio técnico de TI SOG-IS. Calificado para los dominios técnicos "Dispositivos de hardware con cajas de seguridad". LINCE	 www.dekra-product-safety.com/en/programs/cyber-security
INSTITUTO NACIONAL DE TÉCNICA AEROSPAZIAL (INTA). Centro de Evaluación de la Seguridad de las Tecnologías de la Información (CESTI) Torrejón de Ardoz (Madrid)	Common Criteria. EAL4+ (AVA_VAN.5 y ALC_FLR.2) ITSEC/ITSEM. Hasta E4	 www.inta.es
JTSEC BEYOND IT SECURITY Granada	Common Criteria (en proceso) LINCE	 www.jtsec.es
LAYAKK SEGURIDAD INFORMÁTICA Paterna (Valencia)	Common Criteria. EAL2 LINCE	 www.layakk.com
SGS CYBER LAB Madrid	Common Criteria (en proceso) LINCE	 www.sgs.es

* A fecha de 31 de marzo de 2021

S21^{SEC}

ACELERE SU TRANSFORMACIÓN DIGITAL

CON SERVICIOS DE CLOUD
BASADOS EN ZERO-TRUST

S21sec tiene el personal certificado en distintos entornos de Cloud para ayudarle a conseguir el máximo nivel de seguridad

IDENTIDAD



PROTECCIÓN DEL
DATO EN TRÁNSITO Y
EN REPOSO



MONITORIZACIÓN
CONTINUA



ACCESO
MÍNIMO



AUTOMATIZACIÓN
DE LA RESPUESTA



¡Contacte con nosotros para más información!



www.s21sec.com | 902 020 222 | marketing@s21sec.com



Laboratorios que certifican productos con el estándar Common Criteria

(*) En proceso

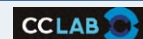
ALEMANIA	
Atsec information security GmbH Prüfstelle für IT-Sicherheit (München)	 www.atsec.com
Deutsche Telekom Security GmbH Prüfstelle für IT Sicherheit (Bonn)	 geschaeftskunden. telekom.de/security
Deutsches Forschungszentrum für künstliche Intelligenz GmbH Prüfstelle IT-Sicherheit (Saarbrücken)	 www.dfki.de
Media transfer AG Prüfstelle für IT-Sicherheit (Darmstadt)	 www.mtg.de
Secuvera GmbH (Gäufelden)	 www.secuvera.de
SRC Security Research & Consulting GmbH IT Security Evaluation Facility (Bonn)	 www.src-gmbh.de
TÜV Informationstechnik GmbH Unternehmensgruppe TÜV-Nord Prüfstelle IT-Sicherheit (Essen)	 www.tuvit.de

ESPAÑA	
Applus Laboratories (Bellaterra, Barcelona)	 www.appluslaboratories.com
BrightSight Barcelona (Sant Cugat del Vallès, Barcelona)	 www.brightsight.com
Instituto Nacional de Técnica Aeroespacial (INTA). (Torrejón de Ardoz, Madrid)	 www.inta.es
Clover Technologies Leganés, Madrid	 www.clovertechnologies.es
Dekra Testing and Certification (S. Sebastián de los Reyes, Madrid)	 www.dekra-product-safety.com
Layakk Seguridad Informatica (Paterna, Valencia)	 www.layakk.com
SGS Cyber Lab (*) Madrid	 www.sgs.es
jtsec Beyond IT Security (*) Granada	 www.jtsec.es

SUECIA	
Atsec information security (Danderyd)	 www.atsec.com
Combitech (Växjö)	 www.combitech.com

AUSTRIA	
SGS Digital Trust Services GmbH (Graz)	 www.sgs.com/ cybersecurity-services

FRANCIA	
Amossys (Rennes)	 www.amossys.fr
Cea - Leti (Grenoble)	 www.leti.fr/en
Oppida (Montigny le Bretonneux)	 www.oppida.fr
Serma Safety & Security (Pessac)	 www.serma-safety-security.com/ en/laboratories/jitself
Thales/CNES (Labège)	 www.thalesgroup.com
Trusted Labs (Meudon)	 www.trusted-labs.com

HUNGRÍA	
CCLab Software Laboratory (Budapest)	 www.cclab.hu

ITALIA	
Tsec Information Security (Roma)	 www.atsec.com
IMQ/LPS (Milán)	 www.imq.it
LVS - Selta (Roma)	 www.selta.com
LVS Leonardo (ex Consorzio RES) (Roma)	 www.leonardocompany.com
Technis Blu (Roma)	 www.technisblu.it

PAÍSES BAJOS	
BrightSight (Delft)	 www.brightsight.com
Riscure (Delft)	 www.riscure.com
Secura (Amsterdam)	 www.secura.com

* A fecha de 31 de marzo de 2021

La economía de suscripción llega a

Exclusive Networks



exclusive networks.
on demand.

la nueva plataforma
on demand

www.x-od.com



Transición hacia
el modelo
as-a-service



Personalización de
servicios: inclusión del
hardware y software



Elección del tipo de
suscripción (mensual,
trimestral, anual)



La carrera de la certificación más allá de la UE

EE.UU.: Marcos, estándares y CMMC



Estados Unidos ha adoptado, históricamente, un enfoque de la ciberseguridad diferente del de la UE, sobre todo en tres áreas: estándares y certificación, privacidad y protección de datos, e intercambio de información público-privada. El documento 'Actions for eu-us cyber dialogue', del

Proyecto AEGIS, (una iniciativa de Horizonte 2020 que tiene como objetivo fomentar la cooperación entre la UE y EE.UU. en investigación e innovación (I+D) en ciberseguridad y privacidad), señala que el de los estándares y la certificación es uno de los ámbitos que tiene mayor actividad, aunque el problema se aborda de forma diferente en ambas jurisdicciones. De hecho, apunta que "todavía queda mucho por hacer para crear normas y certificaciones de ciberprotección transatlántica armonizadas". El informe destaca que, a diferencia de Europa, EE.UU. no cuenta con un esquema federal de certificación de productos (ni servicios) propiamente dicho para toda la industria, aunque es muy activo publicando marcos y estándares en este campo. Su mayor exponente es el **Instituto de Estándares y Tecnologías (NIST)**, responsable de desarrollar sus reconocidas guías con los requisitos mínimos para los sistemas federales. Aunque tanto estas como su Marco de Ciberseguridad carecen de valor reglamentario, tienen una gran influencia en la industria debido a que las empresas que hacen negocios con las agencias gubernamen-

tales necesitan interactuar con la tecnología que el gobierno considere aceptable. De cualquier forma, EE.UU. sí considera prioritario contar con certificaciones de ciberseguridad para sus organizaciones más críticas. Por ello, desde 2020, tiene en marcha el programa de Certificación del Modelo de Madurez de Ciberseguridad (CMMC) del **DoD-Departamento de Defensa** (SIC 140). El CMMC establece que todos los contratistas y subcontratistas que suministran productos o servicios al DoD deberán demostrar, si quieren trabajar con él, que cumplen con rigurosos requisitos de ciberseguridad en el manejo de la información protegida y sensible aunque no esté clasificada.

Para obtener la certificación CMMC, que cuenta con cinco niveles, las organizaciones deben completar una evaluación formal de un asesor externo. Para ser uno de ellos es necesario contar con la aprobación del **Organismo de Acreditación de la CMMC** (CMMC Accreditation Body, AB), una organización sin ánimo de lucro, que acredita tanto a los evaluadores individuales, como a las Organizaciones de Evaluación de Terceros (C3PAO).

Eso sí, esta iniciativa lleva ya un año de retraso, ya que a principios de este 2021 no había aún empresas acreditadas para realizar evaluaciones. Se espera que sea a principios de este verano cuando se empiece a realizar las evaluaciones formales. Para 2025, se prevé que todos los proveedores del DoD, más de 300.000, cuenten ya con la certificación CMMC.

REINO UNIDO: Cyber Essentials



El gobierno británico ha apostado por llegar a acuerdos para garantizar la protección de datos como cuando formaba parte de los 27. En el caso de las certificaciones de ciberseguridad de productos, al igual que otros países comunitarios, busca ofrecer una alternativa a *Common Criteria*. Entre sus iniciativas más destacadas, ya en junio de 2014 y fruto de su trabajo con el consorcio para la **Seguridad de la Información para Pequeñas y Medianas Empresas (IASME)**, el **Foro de Seguridad de la Información (ISF)**, la **British Standards Institution (BSI)** y la industria, puso en marcha su 'Cyber Essentials'. Se trata de un esquema de certificación, operado por el **Centro Nacional de Seguridad Cibernética (NCSC)**, que establece cinco controles de seguridad básicos (cortafuegos, gestión de parches, protección frente al *malware*, control de accesos y configuraciones seguras). Según el propio Gobierno, con él "se protegerán a las organizaciones del 80% de las brechas de seguridad más comunes".

El proceso de certificación lo realiza el IASME, que otorga las licencias a los organismos que certifican productos (EC). El sistema incluye dos niveles: Cyber Essentials y Cyber Essentials Plus. El primero, más básico, con un coste que ronda los 350 euros, se basa especialmente en una autoevaluación a través de un cuestionario (SAQ, por sus siglas en inglés). El segundo, el Cyber Essentials Plus, supone una auditoría más exhaustiva de los controles implementados, realizada por una entidad certificada. Su precio alcanza algo más de 1.600 euros.

CANADÁ: "CyberSecure" para pymes



Otro país muy activo en este sentido es Canadá, que en 2019 lanzó un programa de certificación de ciberseguridad para que las pymes contasen con un nivel básico de protección. CyberSecure Canada se presenta como un programa voluntario compuesto por un conjunto básico de controles desarrollados por el **Centro Canadiense de Seguridad Cibernética**. Estos controles incluyen, entre otros, contar con un plan de respuesta a incidentes, el parcheo regular de sistemas operativos y aplicaciones, el uso de software de seguridad y la configuración segura de dispositivos.

El gobierno canadiense utiliza seis organismos de certificación para verificar estos controles: **Cyber Security Canada, Bell Canada, Bulletproof Solutions, Siemens, SourcetekIT y WatSec**. La certificación tiene una duración de dos años, momento en el que se debe volver a pasar por el proceso de certificación.

CHINA: Revisiones para salvaguardar la ciberseguridad nacional



Sin duda, uno de los países que ha desarrollado regulaciones a lo largo de su historia con una línea política muy específica es China. Aunque no se trata sobre certificación propiamente dicha, una de las acciones más recientes en materia de evaluación de la ciberseguridad de productos es la que entró en vigor en junio del pasado año y que ya se venía mencionando en su controvertida Ley de Ciberseguridad, adoptada en 2017.

Se trata de una serie de reglas que instan a los operadores de infraestructura de información crítica del país a que realicen revisiones de una lista de servicios y productos tecnológicos (p.e. equipos de red central, computadoras y servidores de alto rendimiento, sistemas de almacenamiento a gran escala, etc.), de sus proveedores para garantizar la seguridad de la cadena de suministro y defender la seguridad nacional. Muchos expresaron su preocupación aludiendo que las nuevas reglas restringirían el uso de soluciones extranjeras, pero el gobierno chino negó las acusaciones, alegando que el objetivo era simplemente salvaguardar la ciberseguridad nacional.

Lanza la plataforma Pinakes

La banca española une fuerzas y crea un 'marketplace' para evitar los ciberataques

Permitirá calificar el nivel de seguridad de más de un millar de proveedores

Las principales auditoras planean participar en el proyecto

Cinco Días, 3 de marzo de 2021

Ahorro y eficiencia
en el **sector financiero**
gracias a nuestra metodología



CyberSecurity
Rating Agency

#TransmiteConfianza

www.leetsecurity.com/pinakes



La certificación de ciberseguridad en Europa: dos años del Cybersecurity Act

Una de las grandes apuestas de la UE en el activo frente de la ciberseguridad en el espacio europeo se centra en la evaluación y la certificación de productos, de procesos y de servicios TIC, siendo las iniciativas referidas a los primeros, los productos, las más avanzadas por el momento. Ya en el estado actual de las iniciativas en curso y en preparación –que afectarán de lleno al mercado interior y a las posibles exportaciones de tecnología segura–, tanto los fabricantes como el resto de proveedores (incluidos los evaluadores) y, por supuesto, los compradores (máxime si están regulados), deberían empezar a tomar medidas, unos para ofrecer productos certificados y los otros para comprarlos o adquirir derechos de uso.

Legislación Europea de Ciberseguridad

Hace ya muchos años que Europa lidera el panorama legislativo sobre ciberseguridad, siendo ejemplo y fuente de inspiración en esta materia para el resto de países de fuera de la Unión.

Comenzando con la GDPR, publicada en 2016, centrada en la privacidad de datos tanto de personas físicas como jurídicas. Este mismo año también salió a la luz eIDAS, estableciendo pautas para la identificación y transacciones electrónicas.

En 2017 se hizo pública la Directiva NIS, que proponía medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión Europea. Actualmente la Comisión está trabajando en una Directiva NIS 2, que ampliará los sectores de aplicación y forzará que todas las empresas medianas y grandes de cada sector tengan que cumplirla.

En enero de 2020 se publicó el 5G Toolbox; los objetivos de este *toolbox* son identificar un posible conjunto común de medidas capaces de mitigar los principales riesgos de ciberseguridad de las redes 5G.

A finales de ese mismo año, se publicó la nueva estrategia de ciberseguridad europea, que incluía entre

sus prioridades la certificación en ciberseguridad.

¿En qué consiste el Cybersecurity Act?

Durante 2019 se sentaron las bases de lo que sería el nuevo reglamento europeo Cybersecurity Act, que plantea la creación de un marco común europeo para la cer-

dores de ciberseguridad a exportadores de ciberseguridad.

Para ello, es clave la capacidad de emitir certificados de ciberseguridad reconocidos en toda Europa para sistemas, procesos y productos minimizando el coste de los mismos.

El Cybersecurity Act pretende lograr este objetivo mediante la creación de un

El Cybersecurity Act pretende crear un marco común europeo para el desarrollo de esquemas comunes para la certificación de la ciberseguridad en los que habría tres niveles de garantía (básico, sustancial y alto) que permitirán la evaluación de sistemas, procesos y productos.

tificación de productos y servicios TIC “ciberseguros”. Esta iniciativa fue posiblemente la más arriesgada hasta la fecha por su carácter novedoso.

Uno de los principales objetivos del Cybersecurity Act es incrementar la competitividad y el crecimiento de las empresas europeas, para pasar de ser importa-

marco común europeo para el desarrollo de esquemas comunes para la certificación de la ciberseguridad.

El Cybersecurity Act o CSA marca tres niveles de garantía (básico, sustancial y alto) que permitirán la evaluación de sistemas, procesos y productos según se muestra en la **Tabla 1**.

NIVEL	¿QUÉ SE PRUEBA?	OBJETIVO	TIPO DE EVALUACIÓN MÍNIMA
Alto	Cumplimiento y robustez	Preservar la soberanía, proteger al ciudadano y a la industria de organizaciones criminales	• Pruebas de penetración • Ataques <i>State-of-the-Art</i>
Sustancial	Cumplimiento y robustez	Prevenir ataques escalables en dispositivos de coste medio/alto	• Ausencia de vulnerabilidades públicas • Pruebas de conformidad
Básico	Cumplimiento	Prevenir ataques masivos en dispositivos de bajo coste	• Revisión de documentación técnica • Auto-evaluación

Tabla 1



ESQUEMA	FASE EN LA QUE SE ENCUENTRA	FASE PRÓXIMA	SECTORES A LOS QUE AFECTA
EUCC	Pendiente de Aprobación	Convertir el esquema en Ley Europea	Productos de Tecnologías de la Información y la Comunicación (TIC)
Servicios Cloud	Modificaciones en el borrador tras consulta pública	Aprobación del esquema candidato por parte de la Comisión Europea	Proveedores de servicios en la nube
5G	Solicitud por parte de la Comisión Europea de la realización del esquema candidato Incluido en el URWP	Creación del <i>ad-hoc Working Group</i> para la elaboración del borrador	Dispositivos que formen parte de la infraestructura 5G
IoT	Incluido en el URWP	Solicitud por parte de la Comisión Europea de la creación del esquema candidato	Aún por definir, potencialmente cualquier dispositivo considerado IoT
IACS	Incluido en el URWP	Solicitud por parte de la Comisión Europea de la creación del esquema candidato	Industria y fabricantes de componentes industriales

Tabla 2

Actores principales en el proceso de creación de los nuevos esquemas de certificación europeos

Existen varios actores que entran en escena una vez se aprueba el Cybersecurity Act. El primero de ellos ENISA, que asume el rol de la nueva Agencia Europea para la Ciberseguridad, y cuyo cometido es coordinar y armonizar las políticas que conciernen a ciberseguridad a escala europeo, dando soporte a los Estados Miembros en la implementación de planes y estrategias.

Uno de los primeros pasos que da ENISA en 2019 es crear el **SCCG** (*Stakeholder Cybersecurity Certification Group*), un selecto grupo de partes interesadas del que forman parte **Tecnalia**, **Iberdrola**, **Leet Security** y **jtsec** como representantes españoles y cuya función es ofrecer asesoramiento sobre cuestiones estratégicas relativas a la certificación de ciberseguridad y asistir a la Comisión Europea en la preparación del URWP (*Union's Rolling Work Programme*), un documento anual que describe las prioridades en la creación de nuevos esquemas de certificación de ciberseguridad.

El **CCN** (**Centro Criptológico Nacional**), por su parte, como autoridad de certificación de ciberseguridad a nivel nacional (*National Cybersecurity Certification Authority* o **NCCA**), representa a España dentro del **ECGG** (*European Cybersecurity Certification Group*). Este grupo asiste a la Comisión Europea en la implementación del marco europeo de certificación.

Además, para cada esquema candidato, ENISA crea un grupo de trabajo *ad-hoc* con expertos de la industria que se encarga de dar soporte a ENISA en la preparación del esquema.

URWP, un cuaderno de Bitácora imprescindible

La necesidad de que las diferentes certificaciones e iniciativas lleguen a buen puerto, ha llevado a la Comisión Europea a marcar una hoja de ruta a seguir, el denominado **URWP**.

Este documento creado por la Comisión Europea define las prioridades a nivel europeo en materia de certificación de ciberseguridad. Es, por tanto, un documento a tener muy en cuenta por fabricantes, organismos públicos y empresas relacionadas con el sector de la certificación en ciberseguridad.

EL URWP contiene una serie de ejes estratégicos, concretamente cinco, que ponen el foco en la mejora de la ciberseguridad en el conjunto de la Unión Europea, abarcando tanto el sector público como el privado:

1. Estandarización: Proveer de fondos para el desarrollo y puesta en marcha de estándares y normas aplicables que permitan un aumento de la ciberseguridad a nivel europeo.

2. La seguridad por diseño y la seguridad por defecto: Promocionar la seguridad en el ciclo de vida de los productos desde su diseño, así como el uso de con-

figuraciones seguras por defecto.

3. Gestión de riesgos: Aplicar diferentes niveles de garantía basada en riesgos. Permitir la autoevaluación para el nivel más bajo.

4. Coherencia entre esquemas: Evitar duplicidad de esfuerzos y pruebas entre las diferentes metodologías de evaluación.

5. Cooperación internacional: La búsqueda de la cooperación internacional teniendo en cuenta no sólo lo que se está desarrollando en Europa, sino también lo que se está creando en el resto del mundo.

La propuesta marcada por la Comisión Europea y plasmada en el URWP es ambiciosa, adoptando Europa una postura de liderazgo en lo que toca a la certificación de ciberseguridad cuyos esquemas sirvan de base a nivel internacional.

Fases a completar para la aprobación de un esquema de certificación en Europa

El proceso para la aceptación de un esquema según el Cybersecurity Act es complejo y cuenta con diferentes fases; por ello es importante el consenso dentro de la comunidad.

Existen cuatro fases clave:

1. Creación del URWP (*Union's Rolling Working Programme*), donde se reflejan los potenciales esquemas en cuanto a certificación en ciberseguridad que tiene la Comisión Europea y se plasman en dicho documento.



2. Para cada potencial nuevo esquema de certificación, la Comisión Europea solicita a ENISA la creación del mismo. ENISA, junto al SCCG y los grupos de trabajo *ad-hoc*, preparan un esquema candidato.

3. Se hace una consulta pública del esquema candidato y se envía a la Comisión Europea.

4. Tras la aprobación de la Comisión Europea, ese esquema candidato se convierte en ley.

Esquemas de ciberseguridad europeos en desarrollo, EUCC y Servicios Cloud

Actualmente existen dos esquemas sobre la mesa que serán aprobados por la Comisión Europea en los próximos meses. El más avanzado y del que se espera su aprobación para el segundo cuatrimestre de este mismo año es el EUCC, o *Common Criteria based European Candidate Cybersecurity Certification Scheme* por sus siglas en inglés, desarrollado para la certificación de ciberseguridad de productos TIC y cuya esencia se encuentra en el estándar internacional *Common Criteria* y el acuerdo de reconocimiento europeo SOG-IS. Sobre esta base, ya por todos conocida, se han realizado mejoras sustanciales tales como la gestión de parches o una mayor agilidad a la hora de actualizar la versión de un producto actualizado.

Se espera un período de transición para la aplicación del EUCC, necesario para la adaptación de fabricantes, laboratorio y Organismos de Certificación, teniendo en cuenta que no existirá emisión paralela de los nuevos certificados EUCC y los *Common Criteria* tradicionales.

El otro esquema de certificación que se encuentra actualmente en desarrollo, pero en una fase algo menos avanzada que EUCC, es el de Servicios Cloud. El esquema candidato finalizó la consulta pública el 7 de febrero, por lo que está en fase de realizar modificaciones si fueran necesarias. Se prevé que, para finales del presente año, si el proceso no sufre ninguna interrupción grave, pase a ser aprobado por la Comisión Europea.

Futuros esquemas de ciberseguridad europeos contemplados en el URWP

La comisión europea ha encomendado a ENISA la elaboración de un Esquema relativo a **5G**, debido a la importancia y a la cantidad de servicios críticos que dependerán de esta tecnología. Este mandato respalda los objetivos del **5G Toolbox** desarrollado por la Comisión. ENISA ya está creando el grupo de trabajo *ad-hoc* que iniciará la preparación del esquema y que potencialmente reutilizará parte del trabajo desarrollado por GSMA en los últimos años.

El URWP identifica otros dos esquemas como prioritarios:

1. Componentes industriales (IACS). El término IACS se refiere a todos los componentes (controlador lógico programable, sistema de control de supervisión y adquisición de datos, etc.) que se integran en infraestructuras críticas y establecimientos de producción industrial.

Este esquema se basará potencialmente en el trabajo previo ya desarrollado ERNCIP (*European Reference Network for Critical Infrastructure Protection*) y podría formar parte de la actualización de la Directiva NIS 2.

2. Internet de las cosas (IoT). La comisión propone definir un esquema con diferentes niveles de evaluación que tenga en cuenta los distintos entornos de criticidad (Ej. salud, coche conectado, juguete, etc.). ETSI y JTC13 han trabajado en el desarrollo de estándares para evaluar productos IoT que pueden ser la base del futuro esquema.

Mirando al futuro, la Comisión contempla la creación de esquemas de certificación para Inteligencia Artificial, Criptografía o ciclos de vida de Desarrollo Seguro.

La Comisión también se plantea la uni-

ficación de las diferentes metodologías ágiles creadas en Europa (ej.- LINCE en España) en un solo esquema utilizando la metodología de evaluación FITCEM (*Fixed Time Common Evaluation Methodology*).

Momento de pasar a la acción

La Cybersecurity Act pone en marcha una serie de obligaciones; pero también aporta una serie de beneficios. El principal es una mayor confianza por parte del ciudadano en el mercado y las soluciones digitales, lo que repercutirá en una mayor demanda de dichas soluciones. Además, para los fabricantes y proveedores es un momento de oportunidad, mejorando la competitividad respecto a las empresas de fuera de Europa.

Tras dos años, podemos afirmar que ahora es el momento de dar respuesta a

Existen dos esquemas que serán aprobados por la Comisión Europea en los próximos meses. El más avanzado es el EUCC, desarrollado para la certificación de ciberseguridad de productos TIC y cuya esencia se encuentra en el estándar internacional Common Criteria y el acuerdo de reconocimiento europeo SOG-IS; el otro esquema de certificación, en desarrollo, es el de Servicios Cloud.

los distintos desafíos a los que el Cybersecurity Act nos enfrenta, tanto para el sector público como para el privado.

Los fabricantes y proveedores deben **“ponerse las pilas”** para adaptarse y estar preparados para certificar sus productos.

Las Administraciones Públicas deben **dotar de suficientes medios** a todos los actores implicados de forma inminente, si no, existe la amenaza de no tener capacidad de respuesta ante la creciente demanda del mercado. ■



JOSÉ RUIZ
CTO



JAVIER TALLÓN
COO

JTSEC

Tome medidas contra las ciberamenazas.



Sophos Managed Threat Response

Nuestro equipo de expertos ofrece un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas las 24 horas.

Más allá de la simple notificación de ataques o comportamientos sospechosos, Sophos adopta medidas específicas en su nombre para neutralizar incluso las amenazas más sofisticadas y complejas.

www.sophos.com/es

SOPHOS
Cybersecurity evolved.



LINCE, una herramienta que aporta más confianza a la ciberseguridad

Europa tiene un mandato claro, y es dotar de ciberseguridad a todos los estados miembro. España ha hecho sus deberes, presentando como norma UNE a LINCE: metodología de evaluación y certificación práctica y ligera, que permita obtener un producto de seguridad certificado, considerando las vulnerabilidades y amenazas que acechan sobre ellos. Desde AENOR consideramos esta nueva norma como una potente herramienta que contribuye a la mejora de la ciberseguridad de los productos TIC. El disponer de una norma UNE impulsará el reconocimiento de la metodología LINCE en el ámbito europeo y permitirá a los fabricantes nacionales prepararse para las futuras regulaciones europeas.

El avance y evolución de las TIC no ha cesado en los últimos años y la transformación digital está teniendo un profundo impacto 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 de los modelos de inteligencia artificial y *machine learning*, requieren de herramientas e instrumentos que combatan también las nuevas ciberamenazas y ciberriesgos.

Si además le sumamos el grave impacto de la pandemia global por Covid-19 en la que nos encontramos desde hace un año, son las TIC, su ciberseguridad y privacidad los retos más prioritarios actualmente y para los próximos años; donde los esfuerzos de todas las administraciones de cada país, como son los fondos de recuperación europeos y nacionales, consideran la digitalización y la ciberseguridad prioritarias en sus estrategias de ayuda.

En este complejo escenario, es precisamente la **Metodología de Evaluación de Seguridad de productos TI - LINCE** del **Centro Criptológico Nacional (CCN)**, dependiente del Centro Nacional de Inteligencia español, la que se ha adoptado como **norma/estándar nacional, UNE 320001**, siendo un potente instrumento que permitirá combatir de raíz y eficazmente muchas de las ciberamenazas y ciberriesgos en la nueva realidad digital.

Así, desde España se lanza una propuesta pionera para alinearse con las estrategias y exigencias que las diferentes regulaciones europeas están preparando en materia de ciberseguridad y privacidad de los productos de TI, donde exigirán su evaluación y certificación.

Anteriormente a LINCE, las certificaciones de ciberseguridad bajo las que se podían evaluar los productos TIC eran las desarrolladas en el ámbito internacional, por ejemplo, *Common Criteria*. Este tipo de estándares orientados a niveles de seguridad altos requieren de un esfuerzo, tiempo y coste que pueden ser inasumibles por muchas empresas, especialmente las pymes. Por este motivo nace LINCE, una metodología de las denominadas "ligeras" que permite la expansión del concepto de certificación de ciberseguridad en el ámbito nacional.

Ahora bien, y considerando el acertado artículo de Jorge Davila (septiembre 2018 / SIC nº 131): **¿Para cuándo la certificación gene-**

ralizada de productos?, como bien indica el autor, *"La certificación de productos es obligatoria en sectores industriales sensibles en los que un fallo puede tener serias consecuencias y afectar negativamente a la salud y calidad de vida de la persona o personas que utilicen ese producto"*.

A lo largo de este artículo intentaremos dar una respuesta a esta importante cuestión.

ASPECTOS CLAVES DE LA UNE 320001 Y SU ADOPCIÓN EN LOS PRODUCTOS TI

LINCE es una metodología de **evaluación y certificación para productos de seguridad TIC** desarrollada por el CCN, que permite valorar y acreditar la capacidad de un producto TIC para manejar información de forma segura. Surge en base a otro tipo de certificaciones ligeras implementadas en otros países europeos. Este es el caso de BSZ (Alemania), CSPN (Francia), BSPA (Países Bajos) y LINCE (España). Todas ellas son certificaciones ágiles y ligeras, centradas en el análisis de la vulnerabilidad y las pruebas de penetración, acotada en esfuerzo y tiempo sobre las características de seguridad declaradas en un producto TIC que requieran un nivel medio o bajo de seguridad.

Así, se crea LINCE como respuesta a la necesidad de evaluación de productos cuyo despliegue está previsto en entornos en los cuales el nivel de amenaza es de tipo básico o substancial de

Para evitar fragmentaciones y certificaciones por cada país, en Europa se está creando un nuevo estándar que intenta paliar la fragmentación del mercado: FITCEM (Fixed-Time Cybersecurity Evaluation Methodology for ICT products) desarrollado por CEN/CENELEC JTC13 WG3, cuya aprobación se espera en los próximos meses.

acuerdo con el *Cybersecurity Act* (Reglamento (EU) 2019/881), sobre ENISA y sobre el marco europeo de certificación. Para los casos en los que el nivel de amenaza sea más elevado, sigue siendo recomendable que se empleen metodologías de evaluación como *Common Criteria*.

La metodología de evaluación LINCE sirve para verificar que un producto ha superado exitosamente una evaluación de seguridad (a través de una tercera parte independiente debidamente acreditada); tiene las siguientes características principales:



1. Debe de ser llevada a cabo en un tiempo y con una carga de trabajo acotada y predefinida.
2. Debe analizar la conformidad del producto con las funciones de seguridad implementadas por el TOE (*Target of Evaluation*).
3. Debe medir la resistencia de las funciones de seguridad del producto.
4. Debe de estar orientada al análisis de vulnerabilidades y test de penetración.

Esta metodología está formada por un paquete base y dos módulos opcionales (*MEC-Módulo de Evaluación funcional Criptográfica*; *MCF – Módulo de Revisión de Código Fuente*). La inclusión en la evaluación de estos dos módulos permite incrementar las garantías de seguridad sobre el producto.

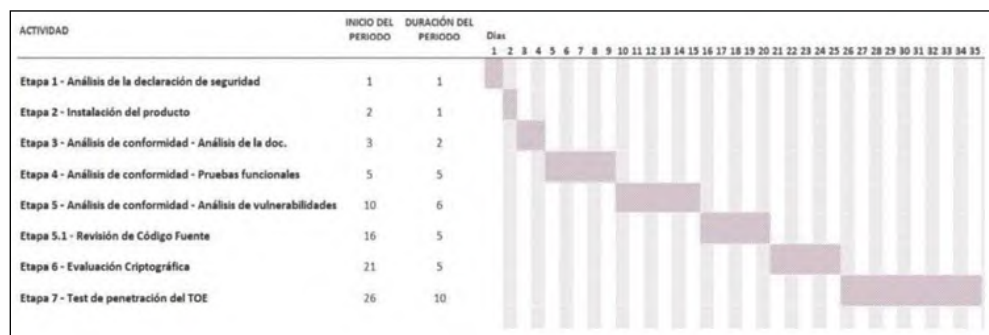


Figura 1.- Ejemplo orientativo diagrama de Gantt – tareas/tiempo/esfuerzo evaluación producto con LINCCE (evaluación que incluya los dos módulos - MCF y MEC) Fuente: UNE 320001

La nueva norma/estándar español, UNE 320001 especifica los pasos necesarios para realizar una evaluación de seguridad básica de productos TIC. Es decir, describe la metodología LINCCE.

El objetivo de la evaluación es el de permitir a un equipo evaluador verificar si el producto es conforme a su especificación, determinando la efectividad de las funciones de seguridad implementadas e incluyendo los resultados en un Informe Técnico de Evaluación (ETR, *Evaluation Technical Report*).

La evaluación se basa en:

- **Declaración de Seguridad** (ST, *Security Target*) que define el alcance de la evaluación, guías de uso y configuración segura del producto; así como información pública del producto.
- **El propio producto** (TOE, *Target of Evaluation*).

Los pasos de la metodología de evaluación se recogen en la norma a través de 10 capítulos y dos anexos de apoyo. Los capítulos, además de explicar el objeto de aplicación y terminología utilizada, describen:

- **Quiénes son los actores implicados**, así como evidencias mínimas para dar comienzo una evaluación.
- **Cuáles son los procedimientos** para realizar la evaluación de un producto.
- **Posibles veredictos emitidos al final del proceso de evaluación**, así como posibles restricciones temporales y de esfuerzo.
- **Resultados y conclusiones** emitidos por una entidad evaluadora.
- **Anexos, con la plantilla de la declaración de seguridad** y la plantilla a utilizar por el evaluador para emitir el **informe técnico de evaluación**.

Así, por ejemplo, para una evaluación que incluya los dos módulos (MCF y MEC), una evaluación LINCCE debe llevarse a cabo con un esfuerzo de 35 jornadas laborales/evaluador y una duración máxima de 12 semanas de esfuerzo. Ver **Figura 1** (diagrama de Gantt orientativo).

Finalmente, con la publicación de esta norma se persiguen tres objetivos:

- **Concienciación** y el **apoyo** a la hora de utilizar certificados de ciberseguridad en los productos TIC a nivel nacional, considerando la seguridad desde el diseño de los productos de TI.
- **Ampliar el alcance** de la metodología LINCCE.
- **Dar visibilidad** e impulso al reconocimiento de la metodología LINCCE en el ámbito europeo, permitiendo a los fabricantes nacionales prepararse para las **futuras regulaciones europeas**.

Para la obtención de una certificación bajo la metodología LINCCE es necesaria una evaluación de un laboratorio acreditado para tal efecto, lo que posibilita el acceso al catálogo de Productos de Seguridad CPSTIC, utilizado como referente de ciberseguridad en España para productos TIC, recomendado por el CCN.

Además de la norma UNE, en relación con la metodología LINCCE, el **Centro Criptológico Nacional (CCN)** ha elaborado una serie de **Guías CCN-STIC (serie 2000)**, cuyo objetivo es recoger todas aquellas guías, procedimientos y formularios, para **facilitar los procesos de evaluación y certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información**.

Los documentos que ya se pueden consultar y descargar, en la parte pública de CCN-CERT son:

1. Guía CCN-STIC-2001 - Definición de la Certificación Nacional Esencial de Seguridad (LINCCE).
2. Guía CCN-STIC-2002 - Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCCE)
3. Guía CCN-STIC-2003 - Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCCE)
4. Guía CCN-STIC-2004 - Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCCE)

CONFIANZA A TRAVÉS DE LAS NORMAS Y ESTÁNDARES UNE ISO. RELACIÓN DE LINCCE CON OTRAS NORMAS Y ESTÁNDARES DE CIBERSEGURIDAD

AENOR, fiel a su propósito de aportar soluciones que relacionen las organizaciones y las personas, y ante los escenarios tecnológicos anteriormente presentados, diseñó la plataforma de confianza: **"Proteger la Seguridad y Privacidad de los datos"**, apoyado en el modelo de ciberseguridad y privacidad de AENOR basado en estándares/normas internacionales ISO (desde la veterana ISO 27001 de seguridad de la información hasta la reciente ISO 27701 de privacidad de la información); así como en el estado del arte de las actuales (y futuras) leyes y reglamentaciones españolas y europeas en materia de ciberseguridad (como son el ENS, RGPD, NIS o el Cybersecurity Act).

Es decir, ofrecer un modelo eficaz y eficiente basado en las *best-practices* (estándares ISO), consensuadas por 155 países don-



de por supuesto se incorpora esta norma nacional, la UNE 320001 LINCE, dotando de una mayor visión y capacidad de reacción a la ciberseguridad (ver **Figura 2**).

Como es sabido, la interrelación entre los procesos de seguridad y los productos de seguridad es muy sólida. Un claro ejemplo de ello se evidencia en las auditorías de ISO 27001-Sistema de Gestión de Seguridad de la Información y/o del Esquema Nacional de Seguridad-ENS, pues se pueden considerar como evidencia válida aquellos productos certificados en **LINCE incorporados en el catálogo CPSTIC, para el cumplimiento del Art. 18 – Adquisición de productos de seguridad” y el control/medidas “Componentes certificados [op.pl.5]”**. Como decíamos anteriormente, el hecho de disponer desde 2018 de la metodología LINCE y haberse publicado en 2021 como Norma Española – UNE, certificable por un laboratorio acreditado, sin duda se sumará en el futuro, al actual hito conseguido por todas las organizaciones españolas que han confiado desde hace años en las certificaciones ISO 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 certificaciones, y basado en nuestra experiencia, estimamos que LINCE será la herramienta que posicione adecuadamente la ciberseguridad de las organizaciones de una forma más eficaz.

CONCLUSIONES

Europa tiene un mandato claro, y es dotar de ciberseguridad a todos los estados miembro. España ha hecho sus deberes, presentando como norma UNE a LINCE: metodología de evaluación y certificación práctica y ligera, que permita obtener un producto de seguridad certificado, considerando las vulnerabilidades y amenazas que acechan sobre ellos. Desde AENOR consideramos esta nueva norma como una potente herramienta que contribuye a la mejora de la ciberseguridad de los productos TIC.

El disponer de una norma UNE impulsará el reconocimiento de la metodología LINCE en el ámbito europeo y permitirá a los fabricantes nacionales prepararse para las futuras regulaciones europeas. Supondrá ventajas competitivas en Europa sin tener que llevar a cabo la certificación a nivel nacional en cada país, posibilitando posiblemente el acceso a los paquetes y fondos de ayuda de la UE (NextGeneration UE).

No obstante, y como se indicó al principio del artículo, hay diferentes países que han realizado su propia metodología de evalua-

ción de producto TIC. Para evitar fragmentaciones y certificaciones por cada país, en Europa se está creando un nuevo estándar que intenta paliar la fragmentación del mercado: *FITCEM (Fixed-Time Cybersecurity Evaluation Methodology for ICT products)* desarrollado por CEN/CENELEC JTC13 WG3, cuya aprobación se espera en los próximos meses.

Pero hay que continuar alerta para que las nuevas amenazas y riesgos no impidan mantener la actividad laboral y empresarial. Y

desde AENOR, dentro de nuestro propósito, seguiremos muy atentos para aportar procesos que generen y devuelvan confianza a las organizaciones de hoy y a las del futuro.

Como respuesta a la cuestión planteada al principio del artículo, es necesario concienciar a la sociedad en su conjunto. En este caso, son los fabricantes de productos TI los que deben considerar desde ya, la incorporación de la seguridad en los productos TI que evalúa LINCE. Para que no se queden atrás, para que sean competitivos, y para que al igual que sucedió hace 15 años, con la ISO 27001, sea LINCE en los próximos años un

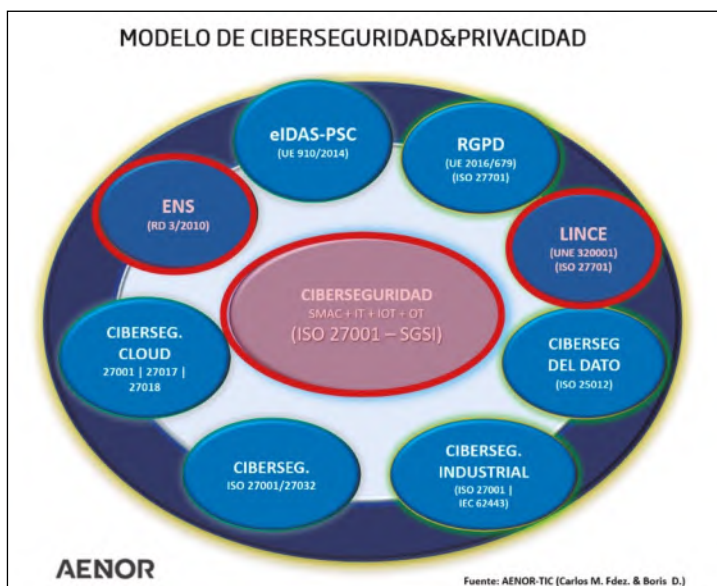


Figura 2.- Modelo de Ciberseguridad & Privacidad de AENOR.

Es necesario concienciar a la sociedad en su conjunto y en este caso, son los fabricantes de productos TI los que deben considerar desde ya, la incorporación de la seguridad en los productos TI que evalúa LINCE. Para que no se queden atrás, para que sean competitivos, y para que al igual que sucedió hace 15 años, con la ISO 27001, sea LINCE en los próximos años un “commodity”.

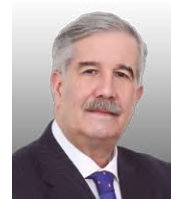
“commodity”. En base a nuestra experiencia, se podrá conseguir que LINCE sea una de las herramientas básicas de la seguridad en productos TI, con la voluntad de todos los que formamos este mundo de la ciberseguridad.

Sin olvidar los retos que ya están sobre la mesa: *blockchain*, Big Data, 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. ■



BORIS DELGADO

Gerente de TIC
Evaluación de la Conformidad
bdelgado@aenor.com



CARLOS MANUEL FERNÁNDEZ

Asesor Estratégico de TI
cmfernandez@fidesol.org

AENOR



Asegure su transformación al Cloud

Zscaler asegura miles de empresas en su migración hacia la nube, proporcionando:

Experiencia de usuario óptima

Protección idéntica para cada usuario, en cualquier lugar

Una pila de seguridad completa, sin renuncias

Conexión Directa a Internet, liberando la WAN MPLS

Máximas capacidades de seguridad, sin dispositivos físicos

zscaler.com

© 2020 Zscaler, Inc. All rights reserved. Zscaler is a trademark or registered trademark of Zscaler, Inc. in the United States and/or other countries. All other trademarks are the properties of their owners.



¿Quién evalúa al evaluador?

La adquisición de un producto de seguridad TIC que va a manejar información sensible debe estar precedida de un proceso de comprobación de que los mecanismos de seguridad implementados en él son adecuados para proteger dicha información. Pero, ¿cómo saber si las personas que han realizado dicha comprobación están lo suficientemente preparadas para hacerlo? ¿Cómo averiguar si conocen los requisitos y poseen los conocimientos necesarios en relación con las especializaciones que procedan? El Centro Criptológico Nacional, responsable de evaluar y certificar los productos de seguridad TIC y, entre tales responsabilidades, acreditar a los laboratorios que efectúan esta actividad de certificación, ha venido fundamentando su actuación en lo recogido en la normativa internacional, apostando en la actualidad por alcanzar una certificación para los profesionales en función de cinco dimensiones: conocimientos, capacidades, experiencia, educación y efectividad.

De todos es sabido que la evaluación y posterior certificación de un producto de seguridad TIC es el único medio objetivo que permite valorar y acreditar su capacidad para manejar información de forma segura. Una **evaluación** con criterios rigurosos y contrastados, homologables con los países de nuestro entorno y que dé paso al proceso de **certificación**; es decir, a la confirmación por parte de un tercero independiente de que el producto o sistema tiene la capacidad de proteger la información hasta el nivel de seguridad otorgado.

En España, el **Organismo de Certificación (OC)**, en adelante, adscrito al **Centro Criptológico Nacional (CCN)**, tiene la responsabilidad¹ de certificar la seguridad de productos y sistemas de Tecnologías de la Información, tras considerar, entre otras pruebas, los informes de evaluación emitidos por los **laboratorios acreditados** (por el propio OC) y realizados conforme a los criterios, métodos y normas de evaluación de la seguridad mencionados.

Antes de comenzar esta evaluación, el laboratorio debe enviar al OC un plan detallado que contemple las fases, tareas y unidades de trabajo correspondientes, la asignación e identificación del personal afecto y su responsabilidad en la misma.

Capacitación del personal del laboratorio

Dentro de este Plan de Evaluación se consideran los requisitos de capacidad, formativos o de experiencia previa de los evaluadores. Incluso, en el artículo 22 de

la citada Orden se establece la obligatoriedad para los laboratorios del Esquema de demostrar su competencia técnica conforme a la norma ISO/IEC 17025, cuyo alcance incluya los criterios, métodos y normas de evaluación admitidos por el esquema (**Common Criteria** y **LINCE**, a día de hoy).

Tomando en consideración todo ello, el OC podría denegar el comienzo de la evaluación si el personal asignado al proyecto no contase con los conocimientos y experiencia adecuados que permitan garantizar la calidad de los resultados.

do se trata de evaluaciones dentro de los dominios técnicos establecidos por el acuerdo de reconocimiento mutuo SOGIS.²

Certificación del personal evaluador

Para obtener la acreditación de un laboratorio, el OC requiere, entre otros aspectos, la competencia técnica conforme a la norma **ISO/IEC 17025**, que establece los requisitos que deben cumplir los laboratorios de ensayo y calibración de cualquier ámbito, incluyendo la ciberseguridad. Esta norma contempla una serie de

Como parte del nuevo esquema europeo de certificación de la ciberseguridad EUCC, uno de los puntos que se está desarrollando es precisamente el de los requisitos de cualificación exigidos al personal de los laboratorios.

Entre sus funciones, además, el OC realiza tareas de seguimiento sobre cada proyecto en curso. Este seguimiento depende, por supuesto, del nivel de garantía con que se evalúa el producto: a mayor nivel de garantía, mayor es el seguimiento realizado por el OC, especialmente cuan-

exigencias para garantizar que el personal evaluador del laboratorio tiene la competencia necesaria para realizar las actividades bajo el alcance de las evaluaciones, así como realizar un adecuado seguimiento mediante procesos de formación continua. Se garantiza, además, mediante

¹ Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información y Comunicaciones.

² El acuerdo SOGIS se elaboró en respuesta a la Decisión del Consejo de la UE de 31 de marzo de 1992 (92/242/CEE) en el ámbito de la seguridad de los sistemas de información, y a la posterior Recomendación del Consejo de 7 de abril (1995/144/CE) sobre criterios comunes de evaluación de la seguridad de las tecnologías de la información; y sus objetivos son: a) Garantizar que las evaluaciones de los productos IT y los perfiles de protección se realicen con arreglo a normas estrictas y coherentes, y se considere que contribuyen significativamente a la confianza en la seguridad de dichos productos y perfiles; b) mejorar la disponibilidad de productos IT y perfiles de protección evaluados y mejorados en cuanto a su seguridad; c) eliminar la carga que supone la duplicación de las evaluaciones de los productos IT y los perfiles de protección y d) mejorar de forma continuada la eficiencia y la rentabilidad del proceso de evaluación y certificación de los productos IT y los perfiles de protección.



las auditorías que se realizan en los países firmantes de los acuerdos de reciprocidad.³

Pese a los requisitos señalados, tanto las normas de evaluación (**Common Criteria** y **LINCE**) como la propia ISO/IEC 17025, son independientes de la tecnología y, por lo tanto, queda en manos del propio laboratorio y del organismo de certificación velar por que el conjunto del personal asignado a una evaluación sea capaz de desarrollarla adecuadamente.

Como parte del nuevo esquema europeo de certificación de la ciberseguridad EUCC⁴, uno de los puntos que se está desarrollando es precisamente el de los requisitos de cualificación exigidos al personal de los laboratorios.

Con toda probabilidad, Europa sabrá sacar ventaja de normas ISO ampliamente reconocidas y utilizadas, como la **ISO/IEC 23532**, que proporciona una interpretación de la **ISO/IEC 17025** para laboratorios de evaluación de la ciberseguridad. En ella se exige que los laboratorios utilicen un sistema de gestión de las competencias de acuerdo a la norma ISO/IEC 19896-3:2018, que determina los requisitos de competencia, conocimiento, habilidades y eficacia orientados a los evaluadores de la seguridad de IT (basados a su vez en ISO/IEC 15408). Estos criterios se organizan en base a cinco (5) dimensiones: conocimientos, capacidades, experiencia, educación y efectividad. Para cada una de ellas, se establecen cuatro (4) niveles de capacitación.

Aun cuando ISO/IEC 23532 considera -aunque de forma meramente informativa- requisitos específicos de conocimiento para diferentes tecnologías, será responsa-

bilidad de cada laboratorio ajustar estos requisitos a sus capacidades técnicas. En esta misma línea se expresa ENISA (Eu-

y habilidades específicos de la tecnología, como son los necesarios para realizar la evaluación de determinado tipo de produc-



Figura 1.- Laboratorios acreditados o en proceso en las metodologías Common Criteria y LINCE.

Buscando una estandarización o, en su defecto, un modelo competencial para el personal evaluador, quizá no estaría de más determinar un catálogo de dominios técnicos en función de la tipología de productos IT a certificar, estableciendo las competencias específicas requeridas para los evaluadores de los laboratorios que participen en el proceso de certificación de cada uno de ellos.

ropean Agency for Cybersecurity) en el precitado documento “Cybersecurity Certification – EUCC”. En él se señala que la ISO/IEC 19896-3:2018 únicamente aborda las competencias metodológicas básicas y no la forma de evaluar los conocimientos

to y el conocimiento específico del sector.

De esta manera, si bien en los procesos de evaluación asociados a las certificaciones de productos no existen específicamente requisitos directos que exijan que los evaluadores cuenten con algún tipo de certificación –como las ya conocidas CISSP, OSCP o CISA–, sí que se requiere, como requisitos indirectos, que el personal que participa en las actividades de evaluación posea un conocimiento técnico solvente para el desarrollo de éstas.

Para mayor abundamiento respecto a estos requisitos indirectos, cabe citar que

³ En la actualidad, otros esquemas europeos como, por ejemplo, el holandés requiere la realización de exámenes acerca del uso de la metodología al personal de los laboratorios que participa en las actividades de evaluación.

⁴ A raíz de la solicitud de la Comisión Europea, de conformidad con el artículo 48.2 de la Cybersecurity Act, ENISA ha creado un grupo de trabajo ad hoc para apoyar la preparación de un esquema de certificación de ciberseguridad de la UE candidato, como sucesor de los esquemas existentes que operan bajo el SOGIS MRA. Este esquema se ha denominado EUCC (Common Criteria based European candidate cybersecurity certification scheme) y estudia la certificación de la ciberseguridad de los productos TIC, basándose en los Common Criteria, la Common Methodology for IT Security Evaluation y su normativa correspondiente, respectivamente, ISO/IEC 15408 e ISO/IEC 18045.



la norma ISO/IEC 17065:2012 sobre requisitos para organismos que certifican productos, procesos y servicios, también referenciada en el capítulo 3 del ya mencionado documento de ENISA, junto a la ISO/IEC 17025, señala en su apartado 6.1.2 relativo a la competencia para el personal involucrado en el proceso de certificación, que el organismo de certificación debe establecer, implementar y mantener un procedimiento que determine los criterios de competencia del personal para cada función, identifique sus necesidades de formación e impulse programas formativos cuando sea necesario.

El Organismo debe demostrar que el personal tiene las competencias requeridas y le autoriza para las funciones del proceso de certificación; en consecuencia, debe realizarse un seguimiento permanente del desempeño profesional del personal evaluador de los laboratorios de certificación.

En este sentido, buscando una estandarización o, en su defecto, un modelo competencial para el personal evaluador, quizá no estaría de más determinar un catálogo de dominios técnicos en función de la tipología de productos IT a certificar, estableciendo las competencias específicas requeridas para los evaluadores de los laboratorios que participen en el proceso de certificación de cada uno de ellos. Evidentemente, dicho catálogo debería evolucionar en la medida de los avances que experimente la tecnología subyacente.

Una base de partida para lograrlo podría utilizar la categorización de los productos de seguridad que, si bien se trata de un subconjunto de los productos IT, sí son los que precisan de mayor confianza por quienes han de emplearlos o integrarlos en su arquitectura. Para esta catalogación, podría ayudar la taxonomía empleada en la guía "CCN-STIC 140 Taxonomía de referencia para productos de Seguridad TIC"⁵. A partir de ella, deberían establecerse las competencias requeridas para el posible personal evaluador de cada una de las agrupaciones o familias de productos.

En definitiva, es preciso que los laboratorios que certifican la seguridad de los

productos y sistemas de seguridad mantengan un sistema de gestión de las competencias de sus profesionales de acuerdo a sus conocimientos, habilidades y eficacia en función de cinco (5) dimensiones: conocimientos, capacidades, experiencia, educación y efectividad. En este sentido, será el Organismo de Certificación quien establezca, implemente y mantenga el procedimiento a seguir, identifique sus necesidades de formación e impulse programas formativos orientados a cubrirlas.

De esta manera, se trata de identificar personal con conocimientos, experiencia

persona para desempeñar esta labor, entre las que cabe destacar:

Competencia para estar al corriente, conocer e interpretar adecuadamente la normativa jurídica y de cumplimiento que se vaya promulgando o modificando, relacionada con la ciberseguridad, asesorando asimismo en su aplicación a la organización.

- Conocimiento de las buenas prácticas y estándares internacionales y capacidad para supervisar el cumplimiento de los mismos.

- Capacidad para elaborar o supervisar



Figura 2.- Cinco dimensiones que deberían abordarse en las competencias de los profesionales.

profesional y con capacidad para desempeñar su labor sin que se puedan comprometer los principios de independencia e imparcialidad que rigen las tareas de evaluación y de certificación, al que se le valorarán méritos como: titulación universitaria superior a la de grado, estar en posesión de certificaciones vigentes relacionadas con la ciberseguridad, publicación de libros, artículos o ponencias relacionados con la ciberseguridad, etc.

En resumen, nos encontramos con profesionales con conocimientos especializados de ciberseguridad, así como experiencia práctica en materia de seguridad de la información y, en su caso, protección de datos.

Además de ello, no podemos olvidar aquellos conocimientos, habilidades y destrezas necesarias que debe poseer la

las diferentes métricas e indicadores relacionados con la seguridad.

- Capacidad para estar al corriente y gestionar los informes procedentes de controles y amenazas, verificando la idoneidad de la protección y su ajuste, en caso de ser necesario.

- Capacidad para interpretar informes forenses, reflexionar sobre las lecciones aprendidas, definir planes de acción y hacer seguimiento de su aplicación. ■



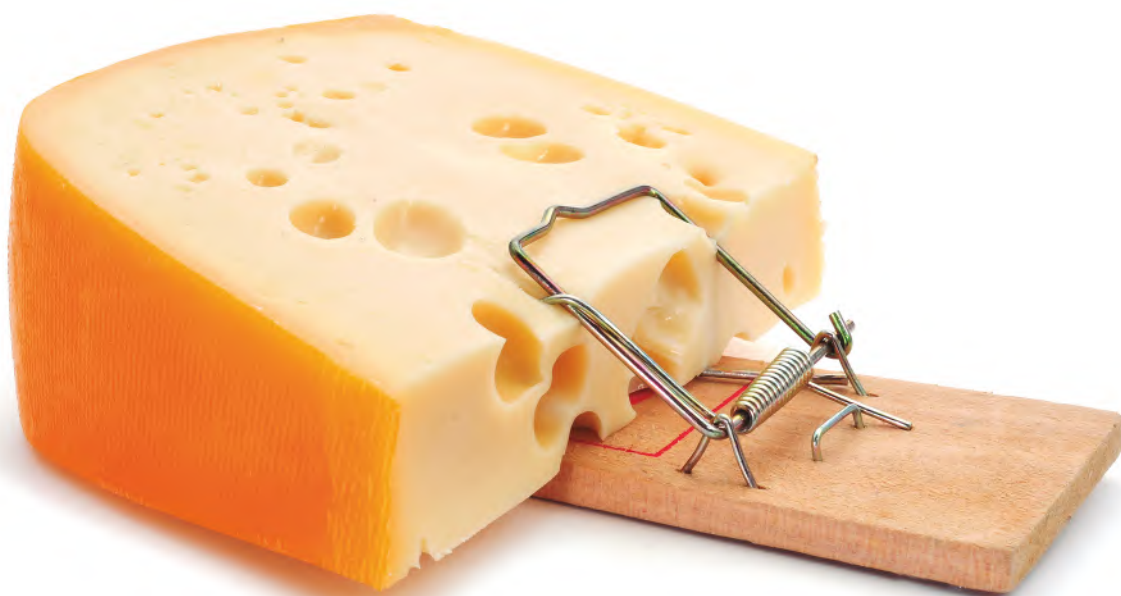
PABLO LÓPEZ

Jefe del Área de Normativa y Servicios de Ciberseguridad

CENTRO CRIPTOLÓGICO NACIONAL – CCN

⁵ <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2518-ccn-stic-140-taxonomia-de-referencia-para-productos-de-seguridad-tic/file.html>

WWW.FACTUM.ES
comercial@factum.es
t_ 902 53 37 73



**ESPECIALISTAS EN
DÁRSELA CON QUESO**

factum

CYBERDECEPTION – COUNTERINTELLIGENCE



Modelo de las tres sonrisas en un esquema de certificación en ciberseguridad industrial

Si estuviera obligado a proteger su casa ¿sería más seguro poner todas las puertas y ventanas blindadas con la certificación exigida, o aplicar las medidas necesarias según un estudio de riesgos realizado por una empresa especializada en seguridad? Probablemente la primera opción será muy conveniente para los fabricantes de puertas y ventanas blindadas, así como para las empresas de certificación, pero para el bolsillo del dueño de la casa, e incluso para su seguridad no lo será tanto. Este es un ejemplo donde no obtenemos la sonrisa de las tres partes. Algo parecido sucede con el esquema de certificación de ciberseguridad de los Sistemas de Control y Automatización Industrial (IACS) en Europa.

El entorno industrial es complejo y cada sector tiene sus características. Automatizar la operación de sus procesos físicos requiere gestionar multitud de señales y actuar sobre motores, turbinas, tanques, reactores o robots. La tecnología IACS para automatizar estos procesos es diversa, PLCs, RTUs, HMIs, DCS, MES, Gateways... y en muchos casos sus limitaciones de procesamiento, memoria y almacenamiento no permiten incorporar capacidades de ciberseguridad.

Para este complejo escenario, **ERNCIP** (*European Reference Network for Critical Infrastructure*) viene trabajando desde 2016 en un esquema de certificación de ciberseguridad de las tecnologías de automatización industrial a través de un marco donde se comparten conocimientos y experiencia para mejorar la protección de infraestructuras críticas y armonizar los protocolos de prueba en toda Europa. Inicialmente los participantes en ERNCIP eran **ENISA**, las agencias

ras. Un proceso de certificación es lento, a ello se suma que el cumplimiento de las normativas internacionales y las normas nacionales es un reto para los fabricantes, cada una de estas regulaciones requiere su propia certificación. Esto aumenta mucho el coste de certificación para un producto, en términos económicos, de tiempo y esfuerzo. La

reuniones programadas para la elaboración del *framework* del esquema de certificación ICCF, cuyo alcance se limita a la certificación de componentes IACS.

Durante 2017 y 2018 se avanza en el desarrollo del borrador, pero desde CCI observamos la pugna entre la agencia francesa (ANSSI) y alemana (BSI) por imponer su metodología de certifica-

Estamos lejos de alcanzar, en los próximos meses o años, un esquema completo de certificación de ciberseguridad europea para entornos industriales.

metodología de evaluación técnica y los procedimientos administrativos necesarios pueden variar sustancialmente entre los distintos esquemas de certificación, y lógicamente su elevado coste termina trasladándose al resto de la cadena de suministro, y por supuesto al comprador del producto.

En octubre de 2016 ERNCIP presenta uno de los primeros borradores de IACS

ción; esto favorecerá a los fabricantes industriales de su país, y es lógico. También observamos que la participación se reduce cada vez más a los actores más interesados, las agencias, empresas certificadoras y fabricantes de tecnología IACS europeos que se pueden ver sometidos a su cumplimiento. A finales de 2017 se planifican varios pilotos para probar el esquema de certificación.

Desde CCI se coordinó inicialmente uno de los pilotos con miembros de nuestro ecosistema español, un usuario, un fabricante y una certificadora, entre otros, pero finalmente estas pruebas se dilataron, y a mitad de 2018, en CCI decidimos centrar los esfuerzos en construir una

plataforma con la participación de todas las partes y que no solo contemple componentes, sino que también permita crear arquitecturas seguras de sistemas IACS e incorporar requisitos de ciberse-

Desde ERNCIP se han hecho grandes esfuerzos para alinearse con la Ley de Ciberseguridad de la UE –Cybersecurity ACT (CSA)–, teniendo que adaptar lo desarrollado hasta el momento para lograr que su esquema ICCS sea desarrollado por ENISA como candidato a Esquema Europeo de Certificación de Ciberseguridad en el área respectiva.

ANSSI (Francia), **BSI** (Alemania), **INCIBE**, el **Centro de Ciberseguridad Industrial (CCI)**, algunos representantes individuales de usuarios industriales, fabricantes e integradores industriales y certificado-

Compliance & Certification Framework (ICCF) en el congreso internacional de ciberseguridad industrial organizado por CCI. También dentro del marco del congreso se celebra una de las primeras



ACTIVOS DE INSTALACIÓN INDUSTRIAL



Fuente: Centro de Ciberseguridad Industrial

guridad en los sistemas según el estándar IEC 62443-3-3.

En paralelo se ha construido una plantilla para proveedores que mapea automáticamente estos requisitos IEC 62443 con las capacidades de ciberseguridad, que facilitará a proveedores y certificadoras identificar el grado de cumplimiento, proporcionando un modelo de las tres sonrisas del usuario final, el proveedor y la certificadora.

La norma IEC 62443 y sus diferentes partes cubren todo el ciclo de vida de un IACS desde el diseño del producto del fabricante, hasta el diseño del sistema y su instalación y aspectos operativos relacionados desde el lado del usuario final. El esquema de certificación internacional IEC 62443 aborda cada etapa, especialmente con respecto a la certificación de IACS. Por otro lado, los esquemas de certificación nacionales e internacionales existentes, como **CSPN** (por **ANSSI** en Francia), **BSZ** (por **BSI** en Alemania), **LINCE** (por **CCN** en España) o **Common Criteria**, se centran en productos de seguridad de TI como principal elemento de evaluación (por ejemplo, chip de hardware de seguridad, firewall, etc.).

¿Qué ha ocurrido con ERNCIP en este tiempo? Finalmente, ERNCIP publica en diciembre de 2020 *Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS)*, iniciando un camino hacia

un esquema de certificación con la publicación de recomendaciones basadas solo en la certificación de componentes IACS, sin contemplar los sistemas IACS, ni su diseño, lo cual reduce significativamente su alcance. Desde ERNCIP se han hecho grandes esfuerzos para alinearse con la Ley de Ciberseguridad de la Unión Europea –Cybersecurity ACT (CSA)– pu-

Podemos concluir que estamos lejos de alcanzar, en los próximos meses o años, un esquema completo de certificación de ciberseguridad europea para entornos industriales, y tendremos que convivir con esquemas de certificación parciales o peor aún excesivamente exigentes para cumplir con la normativa de certificación europea.

Tendremos que convivir con esquemas de certificación parciales o peor aún excesivamente exigentes para cumplir con la normativa de certificación europea.

blicada el 17 de abril de 2019, teniendo que adaptar lo desarrollado hasta el momento para lograr que su esquema ICCS sea desarrollado por ENISA como candidato a Esquema Europeo de Certificación de Ciberseguridad en el área respectiva.

Como señalaba al principio, el entorno industrial es complejo y desarrollar un esquema de certificación en ciberseguridad para este entorno también lo es. Hay que valorar el gran esfuerzo que desde ERNCIP se ha hecho, pero ha faltado la representación de usuarios para un esquema de certificación y que se cumpla el modelo de las tres sonrisas. Se debería haber solicitado la participación del usuario a través de asociaciones sectoriales, como ocurre con otras certificaciones industriales.

La plataforma y el catálogo de cobertura de IEC 62443-3-3 que hemos construido con el ecosistema de CCI permitirá avanzar a usuarios finales, proveedores y certificadoras reduciendo su tiempo y esfuerzo en el camino hacia la certificación europea. ■



JOSÉ VALIENTE

Director

CCI – CENTRO DE CIBERSEGURIDAD INDUSTRIAL



La seguridad y la evaluación de conformidad y certificación de PSC eIDAS y servicios, un enfoque global

La autora, una reputada jurista, muy comprometida desde hace años con la estandarización en los terrenos de la confianza digital y la ciberseguridad, Editora del esquema de certificación eIDAS (EN 319 403), y las normas EN 319 401 y EN 319 521, y Directora técnica del esquema acreditado eIDAS de CERTICAR, explica de forma resumida el enfoque de la evaluación y certificación de la seguridad los Proveedores de Servicios de Confianza (PSC) cualificados, que no solo se fundamentan en la evaluación y certificación cripto y de seguridad CC (preferentemente), sino además en el cumplimiento de una “panoplia de controles de seguridad alineados con los controles de la IE/ISO 27002”, lo que permite la implantación integrada y alineada con el SGSI del PSC.

Cuando hace ya unos cuantos años nos reunimos en Bruselas para ver cuál sería el esquema bajo el que se acreditarían a las entidades de evaluación de la conformidad que certicasen el cumplimiento del Reglamento eIDAS, esta norma legal aún no se había publicado pero el caso DigiNotar ya estaba en la picota.

Una de las exigencias del Reglamento eIDAS se centra en garantizar la seguridad de los servicios de confianza frente a actos deliberados o fortuitos que afecten a sus redes o sistemas de información. En este sentido, todos los prestadores de servicios de confianza, cualificados y no cualificados, están sometidos a la obligación de adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan, así como de notificar al órgano de supervisión cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado.

Y estos requerimientos no vienen de la nada, fueron incluidos en el Reglamento eIDAS a partir del caso de la CA holandesa DigiNotar. El grave incidente de seguridad que sufrió esta entidad no solo tuvo un impacto en la redacción del Reglamento sino también en la estructura de los estándares y su redacción, apareciendo como norma cúspide el documento de políticas y seguridad para cada uno de los servicios de confianza.

Caso DigiNotar

Hagamos un poco de historia. DigiNotar era una autoridad de certificación holandesa propiedad de Vasco Data Security International, Inc. creada originalmente en 1998 por el notario Dick Batenburg de Beverwijk y la Koninklijke

Notariële Beroepsorganisatie (KNB), el organismo nacional de los notarios holandeses. El KNB ofrecía, al estilo de los colegios notariales españoles, todo tipo de servicios centralizados, entre los que incluyó la emisión de certificados de firma.

El 3 de septiembre de 2011, después de que se evidenciara que una violación de seguridad había dado lugar a la emisión fraudu-

gestión operativa de los sistemas de DigiNotar declarándose poco después y dentro de ese mismo mes la quiebra de la compañía.

El gobierno holandés encargó una investigación a la consultora Fox-IT, entidad que identificó a 300.000 usuarios iraníes de Gmail como el objetivo principal del ataque, sospechando del gobierno de este país como autor del mismo. Sin embargo, **Bruce Schneier**¹ era

La seguridad en el ámbito de aplicación del eIDAS compete a todos los sistemas involucrados en la prestación del servicio de confianza, no solo al módulo criptográfico y sus aledaños, y la supervisión no depende de inspecciones aleatorias o de su total ausencia, sino de una evaluación bienal realizada al prestador por una tercera parte independiente y con capacidad técnica para extraer consecuencias.

lenta de numerosos certificados –y decimos evidenciara, porque aún no se sabe con certeza desde cuándo DigiNotar estaba comprometida–, el gobierno holandés se hizo cargo de la

de la opinión de que el ataque pudo haber sido un trabajo de la NSA o las vulnerabilidades detectadas podrían también haber sido explotadas por la NSA.

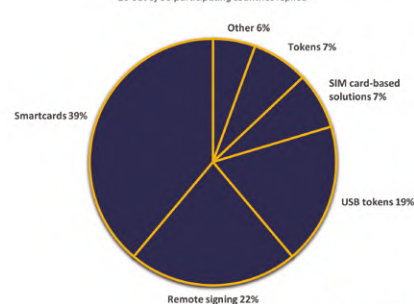
State of play of e-signatures and e-seals in the EU

National information on electronic signatures and seals

*For the purpose of this survey the group of participating countries was conformed by all EU Member States, Iceland, Liechtenstein and Norway

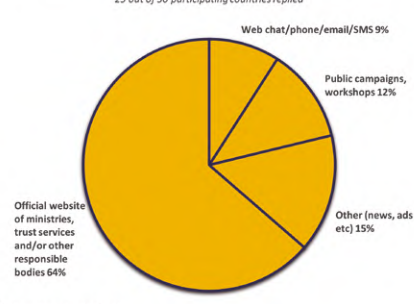
Which signature creation technologies are used in the participating countries?

26 out of 30 participating countries replied



Through which channels is the public informed about e-signatures?

25 out of 30 participating countries replied



Information obtained from 2019 eSignature Country Sheets

Los ciberdelincuentes
hoy salieron de pesca.

**Tus usuarios
caerán en
las trampas.**



Lanza simulaciones de Phishing y Ransomware, y conoce el
nivel de riesgo de tu empresa.



www.smartfense.com
info@smartfense.com



SMARTFENSE
HARDENING DE USUARIOS



Tuve la oportunidad de participar en una presentación a supervisores y a puerta cerrada de este análisis como parte del equipo que estaba redactando el esquema de acreditación/certificación eIDAS y solo puedo confirmar que, aparentemente, el ataque provenía de usuarios iraníes. Fuera quien fuera el atacante, tras identificar más de 500 certificados de DigiNotar falsos, los principales fabricantes de navegadores incluyeron en su lista negra todos sus certificados, iniciando lo que fue la rápida muerte de esta compañía.

Lo realmente importante es el impacto que tuvo este grave incidente en la seguridad jurídica y la fe pública de Holanda en tanto que DigiNotar emitía certificados no solo para los notarios sino además para la administración pública holandesa.²

Seguridades integradas

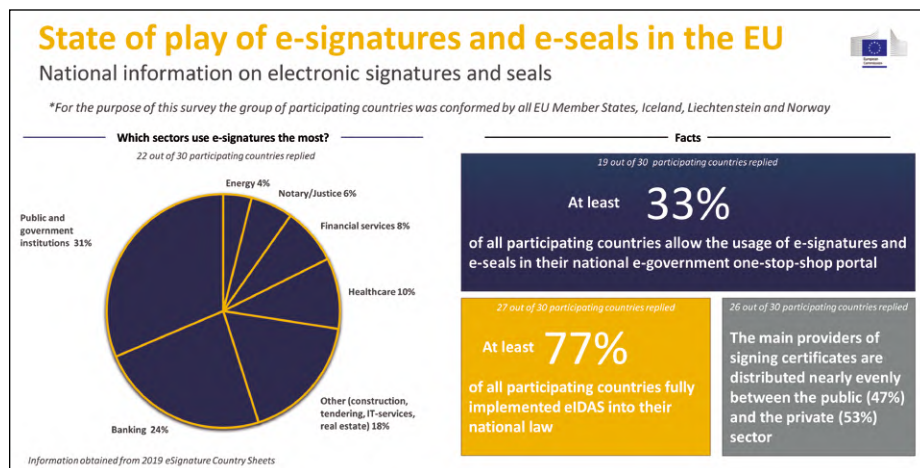
Las consecuencias del caso DigiNotar se llevaron al Reglamento eIDAS con toda su contundencia. La seguridad ahora es algo que compete a todos los sistemas involucrados, no

En la evaluación de un prestador de servicios de confianza se “heredan” las certificaciones cripto siempre que sean generalmente aceptadas, y de preferencia, las que cumplen con los estándares Common Criteria, en la revisión de aquellos controles de las normas que le resulten de aplicación.

solo al módulo criptográfico y sus aledaños, y la supervisión no depende de inspecciones aleatorias o de su total ausencia, sino de una evaluación bienal realizada por una tercera parte independiente y con capacidad técnica para extraer consecuencias.

Veníamos de la documentación de los *trustworthy systems*³, como parte nuclear de la seguridad de las Autoridades de Certificación conforme la Directiva, y de CEN como la entidad llamada a estandarizar este entorno, fuertemente basado en el convencimiento de que la criptografía subyacente a la prestación del servicio era más que suficiente para asegurar la seguridad del todo el sistema y, por ende, del servicio prestado.

Cuando, como editora de la EN 319 401 nos planteamos cómo acometer la regulación de los requerimientos de los *Trust Service Providers* (TSPs) o Prestadores de Servicios de Confianza (PSC) y tras no pocas discusiones y cejas levantadas, llegamos a la conclusión de que cualquier



servicio de confianza tenía que cumplir con unos requisitos básicos que pasaban, fundamentalmente, por el análisis de riesgo de la operación del servicio y de la organización que lo presta, la documentación básica (CPs, términos y condiciones) y una panoplia de controles de seguridad alineados con los controles de la IE/ISO 27002, lo que permitía la implantación integra-

esignature services” y acabaron incluidos en pie de igualdad junto con los servicios “pata negra” heredados de la Directiva. Para estos se diseñó el núcleo duro del Reglamento eIDAS de manera inicial y, por este motivo, a veces encaja con dificultad en estos servicios auxiliares o secundarios pero que no dependen de la criptografía ni de productos criptográficos propios para su prestación.

Así pues, el caso DigiNotar y la propia madurez del modelo, junto con la incorporación de expertos en los grupos de trabajo más cercanos a una visión holística de la seguridad, cambió el paradigma, pasando a certificar productos criptográficos y los *trustworthy systems*, muy pegados a la componente técnica de seguridad de alta granularidad, al prestador y el servicio que presta. Así, en la evaluación de un prestador de servicios de confianza se “heredan” las certificaciones cripto siempre que sean generalmente aceptadas, y de preferencia, las que cumplen con los estándares Common Criteria, en la revisión de aquellos controles de las normas que le resulten de aplicación.

La seguridad de un prestador de servicio de confianza y de los servicios que presta es tan robusta como cualquiera de los elementos de su operación. No se puede ser una entidad de confianza si no se es confiable. Esta es la principal lección aprendida de este caso y el por qué un esquema de certificación basado en la norma ISO/IEC 17065, aplicable a productos y servicios, no se centra en el producto criptográfico sino en la operación segura del servicio de confianza. ■

Evaluación de conformidad

En la evaluación de conformidad de un prestador de servicios de confianza que pretenda la cualificación, única vía para acceder a la TSL, el uso de herramientas y productos criptográficos es un componente esencial para algunos (CAs, ATS...) pero periférico en otros servicios que se diseñaron como “ancillary



PALOMA LLANEZA

Editora del esquema de certificación eIDAS (EN 319 403), y las normas EN 319 401, y EN 319 521 Directora técnica del esquema acreditado eIDAS de CERTICAR

¹ Schneier on Security. Effects of the 2011 DigiNotar Attack. https://www.schneier.com/blog/archives/2016/12/effects_of_the_.html. Josephine Wolff. How a 2011 Hack You've Never Heard of Changed the Internet's Infrastructure. Slate. <https://slate.com/technology/2016/12/how-the-2011-hack-of-diginotar-changed-the-internet-infrastructure.html>

² DigiNotar había emitido dos tipos de certificados: bajo su propio nombre (donde la CA raíz era “DigiNotar Root CA”) y los certificados para el programa PKIoverheid (“PKIgovernment”) del gobierno holandés. Así pues, DigiNotar era la CA de la administración pública holandesa.

³ EN 419 241-1: “Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements” (publicada por CEN).



WIFI DOMÉSTICA BLINDADA TELETRABAJO SEGURO

Dispositivo Plug&Play - Soporte 24/7 - Privacidad de datos



Conoce **el precio**
de Haunt Keeper





en **Construcción**



>> Jorge Dávila

Sobre la certificación de la seguridad en una Industria Digitalizada

Una de las consecuencias más directas del Cybersecurity Act europeo de 2019 es dotar a la Unión de un sistema ágil, eficiente y confiable de certificación de productos, sistemas y procedimientos en al ámbito de la Industria 4.0. La certificación no es algo nuevo, lleva entre nosotros desde el mismo principio de la industrialización y sin embargo eso no ha impedido múltiples desastres industriales de importantes consecuencias. Ahora le toca a la Industria Digitalizada que todos desean y promueven, pero no está claro que, en esta ocasión, las certificaciones y las normalizaciones puedan aportar algo tan volátil como la seguridad en los sistemas digitales y de información. Queramos o no el proceso está en marcha, y es tiempo de prestarle atención.

El esquema **Common Criteria** (CC) nace en 1990 como un intento de fusión de esquemas de certificación anteriores: el **ITSEC** europeo desarrollado por Francia, Alemania, Holanda y Reino Unido, el **CTCPEC** canadiense inspirado en su homólogo del Departamento de Defensa norteamericano y, por último, el **TCSEC** norteamericano del citado Departamento de Defensa llamado "the Orange Book" dentro de lo que se conoció como las "Rainbow Series".

La ventaja esencial de ese esquema de certificación es su vocación global plasmada en el Acuerdo de Reconocimiento Mutuo¹ que obliga a sus 31 miembros². Por ese acuerdo, todos los firmantes deciden reconocer la validez de los certificados emitidos por los demás.

En cada país firmante existe un responsable frente a los demás miembros y en el caso de España, ese cometido lo desempeña el **Organismo de Certificación de la Seguridad de las Tecnologías de la Información**³, que es parte del **Centro Criptológico Nacional (CNI)** actualmente adscrito al Ministerio de Defensa.

Para obtener alguna de las certificaciones, el cliente debe dirigirse a un Laboratorio de Certificación que, siguiendo una metodología común y aprobada por todos, se encargará de aplicar el procedimiento de evaluación que establece en cada nivel el esquema de los Common Criteria. En el mundo hay reconocidos 80 laboratorios de evaluación distintos operando bajo el esquema de Common Criteria⁴, y sólo seis de ellos son españoles y forman parte del conjunto de 33 laboratorios europeos.

En estos 30 años de funcionamiento el esquema de los **Common Criteria** ha demostrado muchas cosas, entre ellas, lo largas y costosas que se pueden hacer las certificaciones de productos. Aunque aumenta según la calidad de la certificación, incluso en sus formas más básicas, la certificación de productos ha supuesto duraciones, costes y dedicaciones de recursos

por parte del solicitante, que sin duda desmotivaban la adopción de esos estándares, sobre todo cuando no está del todo claro qué es lo que realmente se consigue con ello.

En el año 2020, se certificaron **Common Criteria** 388 productos⁵, mientras que en 2019 fueron 368. En concreto, en ese año, 187 (40%) de esas certificaciones correspondían a evaluaciones de alto nivel (de EAL4 a EAL7), de las cua-



La evaluación se hace siempre basándose en la información que aporta el fabricante y la que se pueda obtener de fuentes abiertas.

les 72 eran EAL4, 84 fueron EAL5, 30 en el nivel EAL6 y solo 1 de nivel EAL7. En el otro extremo, 82 productos (21,1%) siguieron evaluaciones más livianas (de EAL1 a EAL3), mientras que la evaluación más popular entre las de menor profundidad fue EAL2, con 57 productos certificados.

En cuanto a países solicitantes de certificación, los tres más activos en 2020 fueron los EEUU (81 certificados), Francia (77) y Holanda (59). Detrás vinieron Alemania (49), Canadá (24) y Suecia (19). Nuestro país sólo representa un 4% de la actividad certificadora total con sólo 17 productos.

Los laboratorios de evaluación más activos en 2020 fueron Brightsight (45 productos), SERMA (37), Acumen (29), Gossamer (25), TÜV y Thales (20). En cuanto a las compañías que solicitaban la certificación tenemos a Idemia con 31 productos certificados, NXP Semiconductors en segundo lugar con 28 productos, y en tercer lugar STMicroelectronics con 18 certificaciones, todas ellas seguidas de Infineon

(16) y Samsung (15). Entre los clientes de la certificación **Common Criteria** no resaltan las empresas de titularidad española.

En ese mismo año 2020, 265 productos (68%) de los 388 certificados, lo fueron a través de la modalidad conocida como **Protection Profile**⁷, tanto si tiene EAL asignado como si no lo tiene. La opción de evaluación armonizada conocida como **Collaborative Protection Profile**⁸ fue muy popular ese año y representó un 21% de todos los que optaron por la modalidad de certificación mediante evaluación del Protection Profile. El 83% de

¹ Ver <http://www.commoncriteriaportal.org/files/CCRA-July2,2014-RatifiedSeptember82014.pdf>

² Ver <https://www.commoncriteriaportal.org/ccra/members/>

³ e-mail: organismo.certificacion@ccn.cni.es URL: <https://oc.ccn.cni.es>

⁴ Ver https://en.wikipedia.org/wiki/Common_Criteria

⁵ Los laboratorios son Applus Laboratories, Brightsight Barcelona S.L., Instituto Nacional de Técnica Aeroespacial (INTA), Clover Technologies, DEKRA Testing and Certification, S.A.U., Layakk Seguridad Informática, S.L. Ver <https://oc.ccn.cni.es/acreditacion-de-laboratorios/laboratorios-acreditados>

⁶ Ver [https://www.itsec.es/files/2020 CC Statistics Report.pdf](https://www.itsec.es/files/2020%20CC%20Statistics%20Report.pdf)

⁷ Ver https://en.wikipedia.org/wiki/Protection_Profile

⁸ Un Collective Protection Profile (cPP) define los requisitos de seguridad IT que debe cumplir un TOE (Target of Evaluation) genérico y especifica las medidas que deberá asegurar el dispositivo a evaluar para conseguir la certificación.



todos los productos con estas modalidades fueron dispositivos de red⁹.

Aunque el gremio de la certificación *Common Criteria* no pone en duda su necesaria existencia, sí ha sido consciente de que su implantación está siendo muy limitada. Por ello algunos países han lanzado esquemas de certificación más ligeros, que intenten resolver el problema de costes y duraciones en el caso de los productos de garantías bajas (*low assurance products*). Francia fue uno de los primeros países en crear una metodología ligera (*CSPN*¹⁰) en 2008. Posteriormente, otros países han seguido esa misma senda, y en el caso de nuestro país, esa metodología se llama **LINCE**¹¹.

Esta ha sido diseñada para productos TI que requieran certificaciones y garantías medias o bajas en cuanto a su seguridad. El objetivo de una evaluación LINCE es que un laboratorio autorizado pueda comprobar que un producto tiene un determinado nivel de efectividad con las funcionalidades de seguridad implementadas en él. Cabe subrayar que la evaluación se hace siempre basándose en la **información que aporta el fabricante** y la que se pueda obtener de fuentes abiertas.

Se pretende que, con esas certificaciones, los productos de menor seguridad dispongan de un esquema de costes asumibles y de duraciones acotadas en el tiempo. Todas esas iniciativas son similares aunque utilizan metodologías con ligeras diferencias, pero no es impensable que con ellas se pueda crear una metodología común y única que sea aceptada por todos (o por muchos) dentro de Europa.



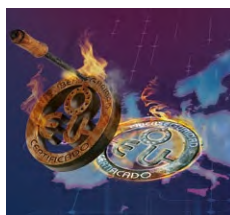
Tanto si la metodología es ligera como si es extremadamente farragosa, además de la pertinencia de ambas, también hay que prestar atención a las capacidades reales y procedimientos utilizados por los Laboratorios de Evaluación.

En general, esas metodologías ligeras consisten en varias fases: **1)** revisión de la documentación técnica del producto, **2)** evaluación funcional de su seguridad, **3)** búsqueda de vulnerabilidades conocidas, y **4)** ensayos de penetración.

Tanto si la metodología es ligera como si es extremadamente farragosa, además de la pertinencia de ambas, también hay que prestar atención a las capacidades reales y procedimientos utilizados por los Laboratorios de Evaluación. Aunque haya normas y certificaciones que pretendan homogeneizar las capacidades de las personas y metodologías que terminan

haciendo el trabajo, eso no quiere decir que los objetivos marcados por esas normas sean siempre los adecuados para aportar la seguridad necesaria en un sector, sistema o proceso en función del tiempo. La homogenización normativa implica rigidez, y la rigidez se adapta mal a la evolución de los riesgos y a las estrategias de ataque por parte de seres inteligentes.

La experiencia cuantitativa y cualitativa de tres décadas de certificación industrial bajo el esquema de los *Common Criteria* pone de manifiesto que no ha sido capaz de popularizar la certificación en ningún ámbito de la actividad



La homogenización normativa implica rigidez, y la rigidez se adapta mal a la evolución de los riesgos y a las estrategias de ataque por parte de seres inteligentes.

industrial o de servicios a nivel planetario, ni europeo. El nacimiento de las metodologías ligeras apunta a que las causas supuestas de ese raquitismo certificador pueden estar en los excesivos costes y tiempos de ejecución que siempre han tenido asociados la certificación en general, y la de *Common Criteria* en particular.

Todavía está por ver si este enfoque más ligero y local consigue algo significativamente distinto a lo anterior, pero es preciso dejar claro que estas nuevas aproximaciones no ponen en

evaluación independiente de los productos en el mercado. En muy pocas ocasiones tales certificaciones son obligatorias, y donde más éxito tiene la normalización es en sectores productivos industriales clásicos como el del automóvil, la aeronáutica y el transporte en general, donde esa obligación es *de facto*.

En el sector de las tecnologías de la información u otros derivados de ellas, la normalización brilla por su ausencia. Es verdad que el sector del automóvil y la aeronáutica tiene más de cien años de antigüedad, pero el sector TIC lleva unas décadas en boga con unos

crecimientos nunca antes vistos y, sobre todo, teniendo un impacto histórico sobre, no sólo la productividad, sino también sobre el individuo y la sociedad misma.

Está por ver que la agilidad de las tecnologías TIC permita algún tipo de normalización o certificación. En este gremio los productos son volátiles, efímeros, insustanciales, sobre todo si ponemos nuestra atención en que los más populares son servicios o *gadgets* que evolucionan, se consolidan y/o mueren en el propio uso de sus consumidores finales.

Es cuando ese tipo de tecnologías quiere entrar en el sector industrial cuando la consolidada tropa de la certificación y normalización quiere ponerle sus yugos. Está por ver que realmente lo consiga. Hasta ahora lo único que hemos visto es el surgir de una Internet de las Cosas (IoT) montándose sobre los mismos sillares que el comercio electrónico, las redes sociales, y el *streaming* de casi todo. No tengo muy claro que este fenómeno esté dispuesto a someterse al arbitraje de nadie y menos aún de los Señores de la Certificación.

Dos nuevos ámbitos: la Internet de las Cosas (IoT) y la Tecnología Operativa (OT)

La Internet de las Cosas¹² (IoT) y la Tecnología Operativa¹³ (OT) son dos nuevos ámbitos, dos nuevas fronteras donde la digitalización da la batalla a procedimientos previos netamente analógicos, continuos y derivables. Aunque ya llevan años en marcha, las seguimos viendo como nuevas porque es ahora cuando saltan al ágora en el que todos somos (in)formados.

La IoT ya estaba en marcha en 1992 con la primera máquina expendedora de Coca Cola de la Universidad de Carnegie Mellon, que informaba a través de Internet de su estado interno. Por su parte, la OT no es más que el apodo re-

⁹ Ver https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.1.pdf

¹⁰ Ver <https://www.ssi.gouv.fr/administration/produits-certifies/cspn/>

¹¹ LINCE Certificación Nacional

¹² Ver https://en.wikipedia.org/wiki/Internet_of_things

¹³ Ver https://en.wikipedia.org/wiki/Operational_technology



ciente de lo que mucho antes eran los Sistemas de Control Industrial¹⁴ (ICS).

Hace veintiocho años, en 1993, se publicaba IEC-1131, que posteriormente sería IEC-61131¹⁵, en el que la industria se mueve hacia una mayor estandarización del software de control para hacerlo independiente del hardware. Es el tiempo de entrada de la programación orientada a objetos en el software de control y del desarrollo de controladores lógicos programables¹⁶ (PLC) y los PCs industriales (IPC).

Escenarios industriales: vicios, debilidades, desastres...

Lo que es novedad es que todas esas tecnologías industriales, desarrolladas *ad initio* en escenarios netamente industriales, poco a poco han ido abrazando la idea de utilizar para sus fines productos y redes esencialmente desarrollados en el entorno TI. Esta tendencia se ve acompañada por una reducción de costes ya que van a comprar en un mercado TI donde el factor de enorme escala es esencial, pero también inoculan con ello los vicios y debilidades de las tecnologías de la Información en los escenarios industriales.

Puede que un fallo de un software pueda dejar expuestos los datos personales de millo-

olvidar que esta solución normativa sólo lo es frente a los fallos fortuitos, a los accidentes, a los imprevistos nacidos del capricho del azar y, sin embargo, **no hay nada en Ciberseguridad que sea culpa de la fortuna.**

No hay más que echar un vistazo a los incidentes más interesantes de la Ciberseguridad para concluir que **ninguno de ellos podría haberse evitado mediante normalización o certificación de procesos y productos.** Excluyo de esa lista de eventos "ciber-interesantes" las múltiples meteduras de pata de administradores y/o usuarios (80% de los casos), las configuraciones y cuentas por defecto, las no actualizaciones del software y del hardware, y los pésimos (o nulos) mantenimientos de los sistemas y productos, que han ayudado a que alguien se meta en los pagos²⁰ de otros y cause desastres varios.

"Ciber-inseguridades ontológicas"

Prefiero centrarme en aquellos escenarios en los que todo el sistema hizo lo que tenía que hacer (DigiNotar²¹, 2011), y el fallo era la misma existencia de cuentas de administrador verificadas con contraseñas fijas. Puestos a darle un nombre a estos casos de real interés, podríamos hablar de las **"ciber-inseguridades ontológicas"** de productos y sistemas. En estos casos

los (librerías, proceso, herramientas) que le ofrece el sistema operativo, ni siquiera tiene que llevarlo él como una pesada alforja (AKA "payload"). Si esto ocurre por la voluntad de un administrador, se le denomina **cifrado de ficheros**, si se hace de forma no autorizada y descontrolada, se llama **ransomware**. Ambas cosas son lo mismo, y permitida una se permite la otra. Otro ejemplo puede ser mandar un fichero adjunto por correo electrónico; si se hace con la voluntad legítima del titular del fichero, se habla de mandar un correo-e, si se hace sin ella, hablamos de "exfiltración de datos". Ningún proceso de certificación puede distinguir entre estas posibilidades duales.

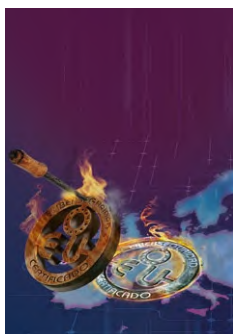
Otros ejemplos de ciber-inseguridades ontológicas o esenciales los podemos encontrar en las conexiones remotas²², en el acceso a través de redes virtuales privadas²³, en la migración de procesos²⁴ entre máquinas, en el arranque no autenticado de los equipos²⁵, en el uso de *caches* de datos^{26,27}, en la misma existencia de cuentas privilegiadas²⁸, en la no-autenticación de procesos que se están ejecutando²⁹ en cada equipo, etc.

Hoy en día, después de la entrada triunfal de China en la economía capitalista global, todos los países del mundo son partidarios de la certificación de productos en general, siempre y cuando beneficien a sus productos nacionales en particular. Los estilos certificadores y normativos franceses no suelen coincidir suficientemente con los estilos alemanes (sólo son dos ejemplos) como para que la construcción de cualquier esquema europeo de certificación sea un paseo idílico por la playa.

Después de todo, la certificación

1) impone costes (muchas veces muy importantes y no siempre estrictamente necesarios), a la vez que **2) excluye a otros** (los no certificados), por lo que la batalla

por ser el emisor de normas de certificación está servida. Hasta la fecha, la parte Occidental de las potencias económicas ha disfrutado de ese monopolio normativo, pero desde hace tiempo, la parte oriental también tiene cosas que decir³⁰.



La solución propuesta por Europa es más de lo mismo, recurrir a la certificación de los productos, y de los sistemas y procedimientos. Con todo, esta solución normativa sólo lo es frente a los fallos fortuitos, a los accidentes, a los imprevistos nacidos del capricho del azar y, sin embargo, no hay nada en Ciberseguridad que sea culpa de la fortuna.

nes de ciudadanos y no pase nada (aunque algo serio debería suceder), pero no está claro que se pueda aceptar que un software de control se vuelva loco (espontáneamente o con ayuda externa de alguien) y libere una nube tóxica de isocianato de metilo¹⁷ por ejemplo, tal y como ocurrió una noche de diciembre de 1984 en **Bhopal**¹⁸ (India) causando 25.000 muertos y medio millón de lisiados.

La lista de **desastres industriales**¹⁹ es larga y muy luctuosa, y debe ser consultada por todos y también enseñada en las escuelas para percatarnos de que éste es un asunto muy grave. La Historia nos ha llevado a un punto en el que deberíamos, ahora sí, tomarnos muy en serio la seguridad de los sistemas IoT, OT o cualesquiera que tengan que ver con la monitorización y el control automático de algo, ya sean humanos o procesos industriales.

La solución propuesta por Europa y el resto del planeta es más de lo mismo, recurrir a la certificación de los productos, y de los sistemas y procedimientos. Con todo, no podemos

la certificación de productos no sirve para nada.

Pongamos por ejemplo un proceso de cifrado de ficheros que autónomamente decide cifrarlo todo y encomendar la custodia de esas claves simétricas a una identidad RSA ajena al sistema. Para ello, utiliza los recur-

¹⁴ Ver https://en.wikipedia.org/wiki/Industrial_control_system

¹⁵ Ver https://en.wikipedia.org/wiki/IEC_61131

¹⁶ Ver https://en.wikipedia.org/wiki/Programmable_logic_controller

¹⁷ Ver https://en.wikipedia.org/wiki/Methyl_isocyanate

¹⁸ Ver https://en.wikipedia.org/wiki/Bhopal_disaster

¹⁹ Ver https://en.wikipedia.org/wiki/List_of_industrial_disasters

²⁰ Pago (segunda acepción) Del lat. Pagus: 1. Distrito determinado de tierras o heredades, especialmente de viñas u olivares. 2. Pueblo pequeño o aldea. 3. Lugar o región. 4. m. (en Arg., Bol. y Ur.) Lugar en el que ha nacido o está arraigada una persona.

²¹ Ver <https://en.wikipedia.org/wiki/DigiNotar>

²² Ver https://en.wikipedia.org/wiki/Remote_desktop_software

²³ Ver https://en.wikipedia.org/wiki/Virtual_private_network

²⁴ Ver https://en.wikipedia.org/wiki/Process_migration

²⁵ Ver https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface#Secure_boot

²⁶ Ver [https://en.wikipedia.org/wiki/Meltdown_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability))

²⁷ Ver [https://en.wikipedia.org/wiki/Spectre_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Spectre_(security_vulnerability))

²⁸ Ver https://en.wikipedia.org/wiki/Privilege_escalation

²⁹ Ver https://en.wikipedia.org/wiki/Trusted_execution_environment

³⁰ Ver https://en.wikipedia.org/wiki/China_Compulsory_Certificate

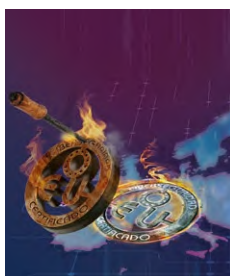


La propuesta europea de esquema de certificación

En Europa se ha propuesto implementar un esquema de certificación de la ciberseguridad de componentes industriales (*Industrial Automation & Control Systems Components, ICCS*) como parte del desarrollo del **EU Cyber Security Act**³¹. En principio, este esquema serviría como base de un futuro esquema europeo de certificación para los componentes de automatización y control industrial.

El Cybersecurity Act (CSA) fue publicado el 17 de abril de 2019 e introduce por primera vez la necesidad de una red paneuropea de certificación de la ciberseguridad para los productos, servicio y

procesos industriales. Esos componentes son: los dispositivos de automatización, los controladores lógicos programables (PLC), las unidades terminales remotas (RTU), los servi-



dores distribuidos que monitorizan y controlan los PLCs, las estaciones de trabajo desde las que operan los técnicos las RTUs y los PLCs, las redes telemáticas que lo conectan todo, sistemas supervisores de control y adquisición de datos (SCADA), y los registros históricos (*logs*) de la actividad SCADA.

El esquema ICCS³² **no pretende certificar todo el sistema industrial** (IACS³³) o sus sub-sistemas, ya que considera que esos son parte de un proceso de ingeniería más global y complejo que habrán de realizar los dueños del sistema o sus operadores/integradores. Por el contrario, **se centra en la certificación de los componentes** que después van a ser utilizados en el diseño y realización de los sistemas de control y operación industrial. Teniendo en cuenta que la seguridad es la del eslabón más débil, está claro que la certificación de los componentes sólo viene a reforzar las puertas, olvidándose de las murallas en las que están encastradas.

La granularidad del esquema ICCS no es muy fina, ya que sólo considera tres niveles de seguridad: Básico, Sustancial y Alto. Sólo en el caso del nivel Alto se evalúa realmente

la robustez del componente, y ello se hace en aras de poder preservar la soberanía nacional, y proteger al ciudadano y a la industria de los ataques de organizaciones criminales u otros estados. Sin embargo, la evaluación consiste, básicamente, en pruebas de penetración y la aplicación de ataques conocidos.

En el caso del nivel Sustancial, lo que se persigue prevenir es que los componentes puedan formar parte de ataques escalables con dispositivos de coste medio/alto. En este caso lo que se evalúa es la ausencia de vulnerabilidades conocidas. Por último, el nivel Básico persigue evitar la participación del componente en ataques masivos en dispositivos de bajo coste. En este último caso, la

El esquema ICCS no pretende certificar todo el sistema industrial o sus sub-sistemas, solo se centra en la certificación de los componentes que después van a ser usados en el diseño y realización de dichos sistemas. Teniendo en cuenta que la seguridad es la del eslabón más débil, está claro que la certificación de los componentes sólo viene a reforzar las puertas, olvidándose de las murallas en las que están encastradas.

evaluación se hace mediante la autoevaluación/revisión de la documentación técnica del componente por parte de su fabricante.

Esta fuerte asimetría en dos de los tres niveles de certificación quizás nazca de pensar que en cualquier sistema hay componentes menos críticos que otros, por lo que pueden ser evaluados de forma más liviana y rápida. Sin embargo, la realidad es que **la importancia de un componente nace del análisis de riesgos de la instalación de la que forma parte, y esa importancia no es inherente al componente**. Es más fácil para los reguladores y normalizadores centrarse en los componentes, pero la "Seguridad" seguirá estando difusa en todo el sistema.

Parece como si, con los niveles Sustancial y Bajo, lo único que preocupase a la comunidad certificadora fuera no alimentar las legiones de los futuros atacantes por denegación de servicio al estilo de la red Mirai³⁴ de septiembre de 2016³⁵. Preparar ahora esquemas de certificación para ataques de hace casi un quinquenio, quizás indique lo por detrás que vamos en la carrera hacia la ciberseguridad de nuestras vidas.

Aprender a tratar el todo

Desde hace tiempo se utilizan los sistemas IACS (*Industrial Automation & Control Systems*) y ahora quieren actualizarlos hacia un nuevo "el dorado"³⁶ que se llama Industria 4.0, que se estima supondría 150 billones de dólares americanos de negocio en el año 2025. Sin embargo, esa peregrinación global puede terminar exponiendo aún más a los sistemas industriales. Las vulnerabilidades de esa nueva industria podrán ser explotadas por adversarios y sus consecuencias tener un alto impacto en las infraestructuras de cualquier tipo y pronto afectar gravemente a la economía y de ahí al día a día de los ciudadanos.

Es curioso que, gracias al Covid-19, hayamos podido ver lo que pasa cuando, por algún motivo exógeno, la economía capitalista (la única disponible por el momento) se pone al ralenti durante bastante tiempo. Una gestión incorrecta o inmadura de la seguridad de los sistemas industriales sentaría las bases para futuras pandemias tecnológicas.

La certificación y la normalización de componentes es necesaria, pero también lo es la de los sistemas y los procesos, tanto si son industriales como si son de cualquier otra índole. La normalización y la certificación son necesarias, pero no son suficientes para asegurar los sistemas, procesos y servicios sobre los que vivimos. ¿Estaban certificados los sistemas que Stuxnet³⁷ logró penetrar y engañar? Probablemente estaban tan certificados como su usuario iraní podía certificar y, sin embargo, el ataque fue un éxito para sus promotores y un pequeño desastre para sus usuarios.

No creo que debamos perdernos en los detalles de los esfuerzos normativos y certificadores de las autoridades de siempre hasta que aprendan a tratar el todo y no sólo alguna de sus partes. A fin de cuentas, lo que sigue estando en juego es la seguridad, la felicidad y el futuro de los habitantes de este peculiar planeta, de esa "pálida mota azul"³⁸ de la que hablaba el entrañable³⁹ Carl Sagan⁴⁰. ■

JORGE DÁVILA

Consultor independiente

Director

Laboratorio de Criptografía

LSIIS - Facultad de Informática - UPM

jdavila@fi.upm.es

³¹ Ver <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act>

³² ICCS = IACS components Cybersecurity Certification Scheme Ver <https://op.europa.eu/s/oROt>

³³ IACS = Industrial Automation and Control System. Ver https://en.wikipedia.org/wiki/Control_system_security

³⁴ Ver [https://en.wikipedia.org/wiki/Mirai_\(malware\)](https://en.wikipedia.org/wiki/Mirai_(malware))

³⁵ Ver https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

³⁶ Ver https://en.wikipedia.org/wiki/EL_Dorado

³⁷ Ver <https://en.wikipedia.org/wiki/Stuxnet>

³⁸ Ver <https://youtu.be/GO5FwsblpT8>

³⁹ Ver <https://youtu.be/StRLkw7ZFVc>

⁴⁰ Ver https://en.wikipedia.org/wiki/Carl_Sagan

Queda por debajo de la media en políticas gubernamentales, atracción y retención de la fuerza laboral, motivación de la población e inclusividad

España, quinta del mundo en educación sobre riesgos digitales del Índice de Alfabetización sobre Ciberriesgos del Oliver Wyman Forum

Con todas las cautelas que este tipo de índices suponen y no sin sorpresa, cabe reseñar que según el Foro Oliver Wyman, España se sitúa a la vanguardia en educación en ciberseguridad, ocupando el quinto puesto a nivel mundial en esta categoría dentro de su Índice de Alfabetización y Educación sobre Riesgos Cibernéticos. En él, se valora la importancia que el país otorga a los planes de formación en primaria y secundaria, así como a la mejora de habilidades de los profesionales. No obstante, el índice también destaca la falta de políticas gubernamentales que ayuden a avanzar en la alfabetización digital de la población, y de planes activos de atracción y retención de la fuerza laboral, ubicándola en el puesto 26 de la clasificación general de 50 geografías analizadas.

España es uno de los países cuyos planes de formación en ciberseguridad se sitúan entre los primeros puestos a nivel mundial, tan solo por detrás de Singapur, Reino Unido, Suiza y Holanda. Así se desprende del 'Cyber Risk Literacy and Education Index', elaborado por el **Foro Oliver Wyman**, que ha evaluado 50 geografías (incluida la Unión Europea), a través de un exhaustivo análisis de la capacidad de la población para comprender los riesgos cibernéticos, así como de las estructuras actuales en los gobiernos, los sistemas educativos y las empresas para capacitar a las futuras generaciones con conocimientos y habilidades básicas en ciberprotección.

Los responsables de la investigación destacan "la fortaleza del país en cuanto al sistema educativo, que mide hasta qué punto se impulsa la educación en riesgos digitales, tanto en educación primaria y secundaria, como a la hora de mejorar las habilidades de los profesionales".

A pesar de este buen resultado, España se sitúa en una posición intermedia de la clasificación general en la que, además del sistema educativo, también se han valorado otros cuatro parámetros más a fin de obtener un mapa del



conocimiento completo sobre ciberseguridad de una población: la Motivación Pública, las Políticas Gubernamentales, la situación del Mercado Laboral y la Inclusividad.

Con la suma de todos ellos, en la que España ha obtenido un total de 535 puntos, nuestro país se queda en el puesto 26 del ranking, justo por detrás de Portugal y delante de Bélgica, situándose por debajo de la media.

Políticas gubernamentales insuficientes

Uno de los motivos que nos han lastrado a dicha posición reside en la baja puntuación obtenida

por la falta de políticas gubernamentales que determinen la visión y el compromiso a largo plazo del Gobierno para avanzar en la alfabetización digital de la población, así como de la falta de planes activos de atracción y conservación de fuerza laboral formada en riesgos digitales. Es este caso, España ocupa una modesta posición tanto respecto al conjunto de las geografías analizadas, como dentro de la Unión Europea, ocupando la posición 13.

Y, aunque, sin duda, unos países lo están haciendo mejor que otros, el informe llama la atención sobre los pocos esfuerzos que, en general, los gobiernos destinan a mejorar la ciberseguridad de la población a nivel mundial. "Durante la última década, los gobiernos de todo el mundo han comenzado a desempeñar un papel más activo

en ciberseguridad, lanzando estrategias nacionales, dedicando recursos a la ciberdefensa y estudiando métodos para equipar a las empresas con sistemas de protección más sólidos. A pesar de ello, la mayoría no han invertido lo suficiente para educar a sus ciudadanos sobre los riesgos cibernéticos, incluso teniendo en cuenta que casi el 95% de los problemas de ciberseguridad provienen de errores humanos", destaca el informe al mismo tiempo que alerta que, además, "los ciberataques costarán a las organizaciones más de 495.000 millones de euros al año, en 2021".

Falta de motivación

El Foro Oliver Wyman recuerda así que "la existencia de una población consciente de los ries-

ESPAÑA DENTRO DEL ÍNDICE DE EDUCACIÓN Y ALFABETIZACIÓN SOBRE CIBERRIESGOS

PARÁMETROS ANALIZADOS	RANKING
Sistema educativo	5º
Políticas gubernamentales	26º
Mercado de trabajo	31º
Inclusividad de la población	34º
Motivación de la población	42º



INTELIGENCIA

MÁS ALLÁ DE CIBERAMENAZAS

RASTREO DE AMENAZAS
CONTINUO Y AUTOMATIZADO

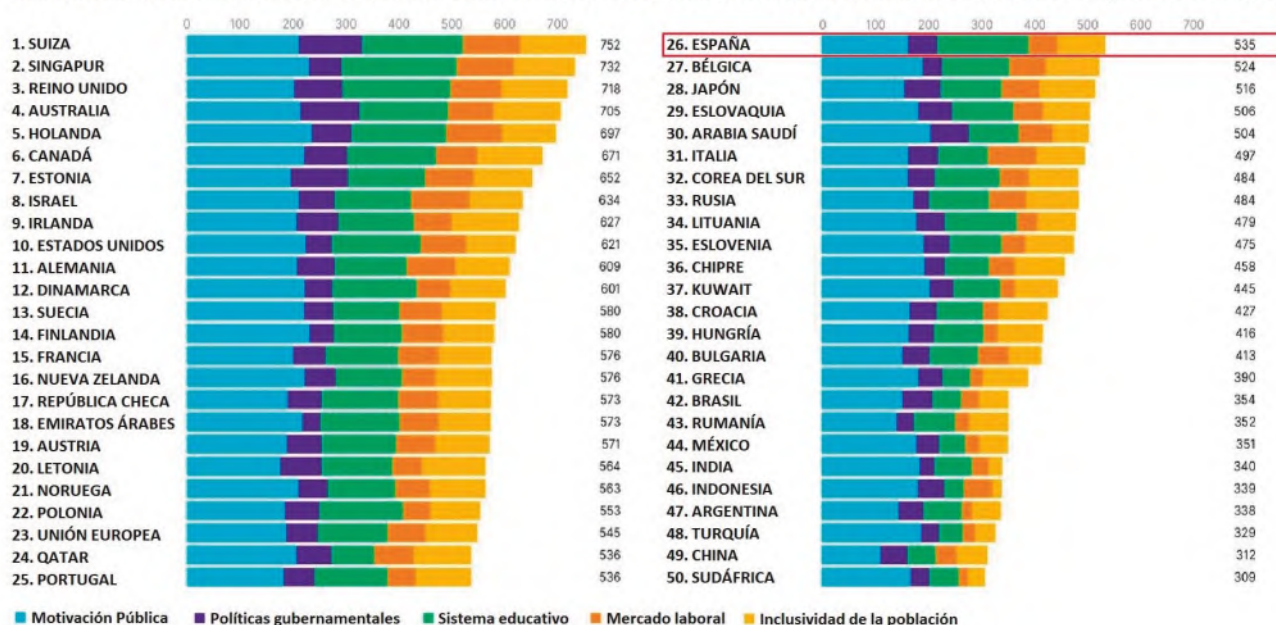
VALOR INSTANTÁNEO,
CONFIGURACIÓN MODULAR

computing
Security
Excellence
Awards
2018
Winner
Enterprise Threat
Detection Award

computing
Security
Excellence
Awards
2018
Winner
Enterprise Security Award



CLASIFICACIÓN DEL ÍNDICE GLOBAL DE EDUCACIÓN Y ALFABETIZACIÓN EN CIBERRIESGOS (Octubre 2020)



gos asociados a la era digital y motivada para afrontarlos resulta fundamental a la hora de implantar una cultura proclive a su mitigación”.

Pero, en lo que respecta a la ‘Motivación Pública’, España tampoco obtiene buena nota cayendo hasta los diez últimos puestos (41º), lo que indica que aún queda mucho camino por recorrer en este sentido. También, suspende en cultura de la población a la hora de ser capaz de tomar acciones específicas para reducir los riesgos de seguridad digital, descendiendo hasta la posición 43º. “Como parte de la Unión Europea, esta situación deja a España en el cuarto puesto por la cola, solo por delante de Italia, Bulgaria y Rumanía, y en claro contraste con Holanda y Finlandia, los dos mejor situados”, explican sus responsables.

De acuerdo con el informe, una de las posibles causas de la falta de motivación de la población española es el bajo nivel de ‘Inclusividad’, otro de los parámetros clave analizados en la investigación. España ocupa aquí la posición 34, lo que revela, según el informe, que el país “no está bien preparado en aspectos como el acceso a la tecnología y a la disponibilidad de programas y recursos dirigidos a la población vulnerable (como personas mayores)”.

Buena posición en I+D

España también se sitúa muy por debajo de la media en lo que respecta al Mercado Laboral. Con una puntuación de solo 343 puntos, el país ocupa el puesto 31 de la clasificación global, y el 16 dentro de los países europeos. Aunque, dentro de este parámetro, las diferencias en los aspectos valorados que lo componen son, no obstante, notables.

El informe destaca en este sentido la sorprendente circunstancia de que exista un bajo nivel de demanda de profesionales especializados en la materia (donde ocupa la posición 40) con la buena posición del país en lo referente a innovación en seguridad digital, que sitúan a España en un noveno puesto gracias al buen trabajo en I+D en este campo y a la colaboración entre gobierno y empresas. Gracias a ello, solo Holanda, Estonia e Italia están por delante de España a nivel europeo.

Suiza y Singapur, ejemplos a seguir

Para los responsables del estudio, por tanto, la clave del éxito reside en “la buena integración entre los niveles educativo, empresarial y gubernamental, que es lo que permite a los países obtener un mayor índice de alfabetización y educación en riesgos digitales”.

Este es el caso de Suiza, Singapur, Reino Unido, Australia y Holanda, que el Foro Oliver Wyman ha situado en los primeros puestos de la clasificación.

El informe indica que todos ellos han conseguido las mejores puntuaciones en casi todos los parámetros analizados, destacando la integración de medidas para conocer y mitigar los riesgos digitales en sus sistemas educativos, en el mercado laboral y en las políticas gubernamentales, así como en la motivación de la población para minimizarlos.

“Estos países apoyan una sólida educación en todos los niveles, poniendo énfasis en las habilidades cuantitativas y recomendando o exigiendo algún tipo de formación en ciberseguridad. Además, las empresas que operan en estas zonas geográficas son conscientes de los ciberriesgos y demandan trabajadores cualificados en esta materia. Incluso, sus políticas gubernamentales sobre formación son amplias y específicas, y con frecuencia son transparentes en cuanto a la financiación y las métricas utilizadas para evaluar su progreso y su éxito”, destaca el informe.

Así pues, Suiza, por ejemplo, el primer país del ranking, destaca por tener “un documento de implementación integral sobre ciberriesgos que establece responsabilidades específicas, junto

con la legislación nacional o provincial que se requiere. Además, se establecen hitos específicos y se crean medidas para garantizar la rendición de cuentas, independientemente de quién esté en el gobierno”, resalta el estudio.

Asimismo, Singapur, que ocupa el segundo lugar, “establece entre sus prioridades la educación en ciberseguridad, desde la infancia hasta las personas jubiladas. Además, la creación de la Agencia de Seguridad Cibernética de Singapur mantiene su ciberespacio seguro y protegido. Y, sus cursos de ‘bienestar cibernético’ se imparten en varios niveles y se centran en consejos de seguridad prácticos y sociales, como la importancia de conocer y reducir el ciberacoso”.

En el lado opuesto se encuentran aquellas regiones que, en general, carecen de una estrategia nacional de alfabetización digital y no priorizan la ciberseguridad en los planes de estudio de las escuelas. Este es el caso de Indonesia, Argentina, Turquía, China y Sudáfrica, que ocupan los últimos puestos de la tabla. El informe concluye que, no obstante, “si bien algunos gobiernos pueden no estar priorizando la ciberseguridad en este momento, al menos, dentro de su población sí que está comenzando a comprender la necesidad de asumir la responsabilidad para mitigar los riesgos cibernéticos a nivel personal”. ■



**Su información crítica
está en la nube.**

¿Y su seguridad?



Netskope.com/es

Uno de cada tres ejecutivos prevé invertir más en ciberseguridad y privacidad, según la encuesta mundial anual de PwC

El 58% de los CEOs españoles, extremadamente preocupados ante la amenaza de ciberataques

Un año después de declararse la pandemia mundial por parte de la OMS y con la progresiva vacunación de la población, 2021 se plantea como un año de transición hacia la recuperación del mundo 'pre-Covid'. Un momento que PwC ha querido analizar de forma especial en su 'XXIV Encuesta Mundial de CEOs' en la que ha puesto el foco, preguntando, entre enero y febrero de este año, a más de 5.000 presidentes y consejeros delegados de todo el mundo en su grado de confianza ante el futuro cercano, así sobre cómo consideran que evolucionará la economía y de qué dependerá. En este contexto, la ciberseguridad emerge por su decidida criticidad.

Fuerte optimismo

Entre las buenas noticias destaca que el 76% de los máximos responsables encuestados esperan una mejora de la economía mundial este año, una cifra muy por encima del 22% registrado en 2020 y del 42% de 2019, y que supone el mayor nivel de optimismo desde 2012, cuando se incluyó esta pregunta en el estudio.

No obstante, existe una gran variación entre sectores, lo que refleja los diferentes grados en que el comportamiento de los consumidores se ha visto afectado por la pandemia. Los CEOs de compañías de tecnología y las telecomunicaciones muestran los mayores niveles de confianza, con un 45% y un 43%, respectivamente. Mientras que los de transporte y logística (29%) y de hostelería y ocio (27%) son los que menos confían en su capacidad para aumentar los ingresos.

En España, los ejecutivos consultados también son partícipes de esta mejora de las expectativas: el 82% cree que la coyuntura económica mejorará (ya sea moderada –el 44%– o significativamente –el 38%–).



Necesidad de ciberprotección

En los últimos meses, ciberataques contra grandes organizaciones como Acer o el SEPE español siguen poniendo de manifiesto la necesidad de contar con la adecuada ciberseguridad pasando a ser una de las grandes prioridades de todas las compañías. No es baladí. Se calcula que cada 10 segundos una empresa sufre un ataque de este tipo por la fuerte apuesta en la digitalización de todas las organizaciones, más si cabe, por las restricciones operativas impuestas por la Covid-19.

los riesgos que escalan posiciones este año, encontramos la incertidumbre de las políticas fiscales (38%) y la desinformación (el 28% está 'extremadamente preocupado', en comparación con el 16% en 2020), debido a su impacto en los procesos electorales, en la crisis sanitaria y en el deterioro generalizado de la confianza de los ciudadanos. Por el contrario, los conflictos comerciales se diluyen en este ranking.

Estos datos suponen que la preocupación por los ciberataques haya escalado desde la cuarta a la segunda posición este año, a nivel mundial, y el 36% de los encuestados considera imprescindible

también destaca que el 26% la incluye entre sus últimas prioridades.

Más inversión en ciberseguridad

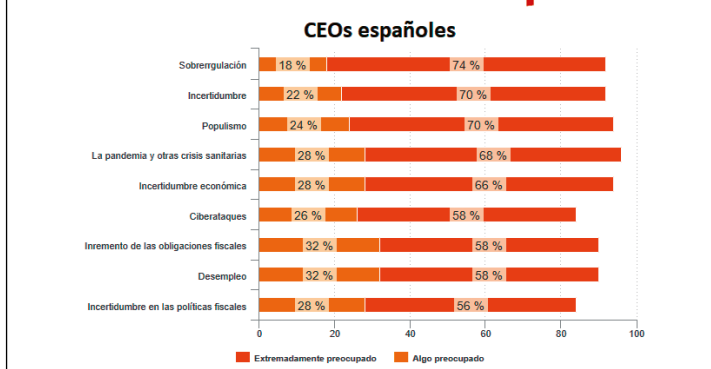
En cuanto a las principales riesgos para el crecimiento de sus empresas en 2021, la encuesta revela que el 36% de los CEOs priorizan la mejora de su productividad a través de la automatización y la incorporación de nuevas tecnologías, gracias a lo que casi la mitad (49%) espera incrementar sus inversiones en transformación digital en más de un 10% en los próximos tres años. Además, un 31% prevé también realizar estos incrementos en su inversión en ciberseguridad y privacidad. Si hablamos de los CEOs españoles, el 78% prevé aumentar su inversión en ciberseguridad y privacidad en los próximos tres años (30% estima incrementos por encima del 10%).

Estrategia y ciberamenazas

En cuestión de riesgos, el 59% de los CEOs (64% de los españoles encuestados) incluyen explícitamente las ciberamenazas en su gestión estratégica de riesgos y el 52% manifiesta estar focalizado en reevaluar la tolerancia al riesgo de su organización.

"La aceleración en la digitalización de las organizaciones conlleva importantes beneficios, aunque no exentos de la aparición de riesgos de ciberseguridad, gestionables desde una nueva perspectiva. Así lo ven ya el 78% de los CEOs españoles entrevistados, que tienen planificado un incremento de su presupuesto de ciberseguridad con el objetivo de mejorar su posición frente al riesgo tecnológico. Mediante esta transformación, la función de ciberseguridad funcionará como el habilitador necesario del nuevo escenario de negocio digital, protegiendo los activos de información y garantizando la continuidad del negocio", ha destacado el socio responsable de Business Security Solutions en PwC España, **Jesús Romero**.

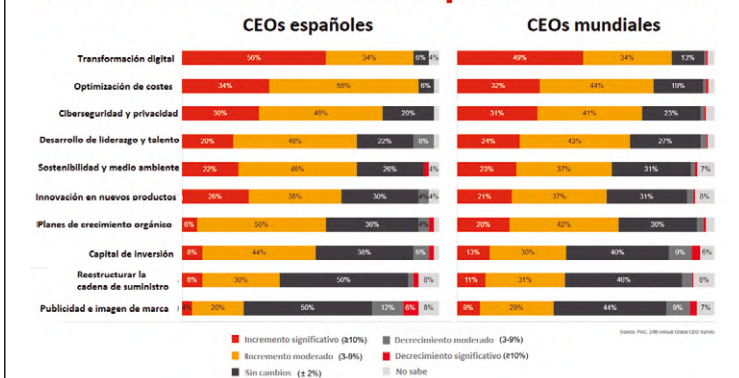
Principales amenazas para el crecimiento de las empresas



Así, se ha posicionado como una preocupación para los CEOs (47%, frente al 33% en 2020) como respuesta a la creciente digitalización, tan solo por detrás de volver a vivir una crisis sanitaria (52%). Entre

incrementar sus mecanismos de medición y detección en ciberseguridad. En nuestro país, el 58% de los CEOs encuestados se muestra extremadamente preocupado ante la amenaza de ciberataques, aunque

Previsión de inversión en los próximos tres años



Capacidades blandas y mayor 'inteligencia emocional' son ahora sus grandes retos, según una investigación de F-Secure

La pandemia refuerza el papel del CISO y su peso en la Junta, tanto por su perfil técnico como por su orientación al negocio

Desde que comenzara, en 1984, con la contratación por parte de **Citi Corp** del primer 'Director de Seguridad de la Información' (CISO), los roles, responsabilidades y capacidades de este tipo de profesionales han evolucionado mucho, madurando rápidamente.



Un puesto que ha cobrado una especial relevancia durante la pandemia y la popularización del teletrabajo, con el cambio de enfoque en protección que ha supuesto. Para analizar su cambio en 2020 y sus nuevos retos, **F-Secure** ha realizado un informe bajo el título '**Ciso: un nuevo amanecer**', emulando la conocida película de Star Wars, en el que describe cómo ha cambiado el trabajo de los CISO a través de entrevistas a 28 CISO, CTO, CSO, Directores de TI, etc. de grandes compañías de EE.UU. y Europa, de julio a septiembre de 2020.

"Si bien sus actividades y habilidades no han cambiado drásticamente, sus responsabilidades y prioridades sí se han alejado de la seguridad para integrarse más con las operaciones diarias", destaca el estudio. En él los participantes han subrayado que ahora el 'riesgo' se ha convertido en su principal reto, ganando en capacidades 'blandas' respecto a su perfil más técnico de hace tiempo, ya que se trabaja más integrado en la alta dirección. De hecho, el 65% de los CISO desvelaron que, el año pasado, incluso con todos los problemas que el mundo ha tenido que afrontar, están más afianzados en su puesto y sólo un 37% indicó considerar dejarlo. Eso sí, el 71% también manifestó haber sufrido niveles de agotamiento por su trabajo.

Entre los datos más significativos, destaca que tanto los CISO de EE.UU. (59%) como los de Europa (57%) han incrementado sus responsabilidades por la mayor presión regulatoria y de privacidad, sobre todo, cuando hay un riesgo de sanción que hace que aumenten los esfuerzos por "alinearse los riesgos de seguridad cibernética dentro de los marcos de gestión de riesgos empresariales (ERM) de una organización". Además, los encuestados destacaron que la pandemia les exigió "un mayor enfoque en las políticas de planificación de la continuidad del negocio (BCP) y su rela-

ción con la organización, operación y seguridad del negocio". Ello, también supuso que los responsables de ciberseguridad aumentaran su trabajo con mejores análisis de impacto empresarial (BIA) y teniendo muy en cuenta "la dependencia que las empresas tienen de la tecnología y evaluando qué controles de ciberprotección se precisan". Los CISO que ya tienen un asiento en el Consejo de Dirección manifestaron su confianza en que su rol es tan crítico para el negocio como otros puestos.

Preocupaciones en el colectivo

Eso sí, mucho también consideran que este rol no tiene el "nivel de importancia necesaria como una función comercial crítica", por lo que en muchos casos no cuenta con el respaldo que consideran que deberían tener, salvo en compañías en las que se esté directamente respaldado por el CEO. Para mejorar su "rentabilidad, capacidades y mejorar la experiencia del cliente", los CISO también se han educado "más allá de la seguridad cibernética, con la ayuda de sus pares para comprender el negocio de su organización y su trabajo en el mercado digital para atender a los clientes actuales y futuros".

Para la mayoría de los participantes, la inteligencia emocional (EQ) es más importante que la propia inteligencia (IQ) para lograr el éxito en sus vidas y carreras. Como individuos, los CISO son vistos en gran medida como muy inteligentes, pero algo inaccesibles, ya que son uno de los pocos perfiles técnicos en la Junta. "Este estereotipo puede ser solo eso, pero sigue siendo difícil

deshacerse de él en algunas culturas", dice el estudio.

Asimismo, se han visto obligados a "ver la nube desde una perspectiva más positiva tanto para la infraestructura de TI, como para las aplicaciones comerciales, algo imprescindible dada la creciente importancia de la nube para el éxito de muchas organizaciones. Además, gran parte de los participantes (71%) dedican tiempo a formarse sobre tecnologías emergentes (digitales) y operativa (OT) en las industrias de fabricación, como posibles superficies de ataque. Ello también incluye conocer bien nuevos marcos de trabajo del **NIST** y el de MITRE ATT&CK. De hecho, muchos mostraron su preocupación por "no estar al día y el posible impacto de ello en su carrera". También, vieron como uno de los mayores desafíos que plantearon los CISO fue el crecimiento de la TI en la sombra.

En este sentido, manifestaron una clara apuesta por la automatización y orquestación aplicando conceptos como SOAR y apostando

por planteamientos "más predictivos (SIEM, MDR, NDR, EDR, etc.) y su capacidad para brindar información procesable". Asimismo, los responsables de seguridad destacaron que "el crecimiento de la IA y el aprendizaje automático (ML) en OT y TI" les lleva a revisar continuamente si "realmente pueden agregar valor demostrable", ya que son conscientes de que "estas tecnologías han dejado su infancia".

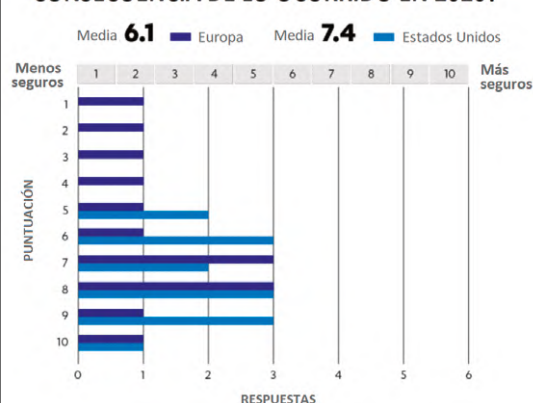
Orientación al negocio

En cuanto a su orientación al negocio, el 61% de los CISO confesaron su necesidad de mejorar sus habilidades comerciales, actualizándose "sobre nuevos desarrollos y riesgos identificados" con, entre otros objetivos, "anticipar y transmitir el impacto en el negocio en caso de que sufra un incidente cibernético". Igualmente, el 75% reconocieron que "su función se ha movido significativamente de un enfoque puro en el riesgo de la red a cubrir todos los aspectos de la tecnología que

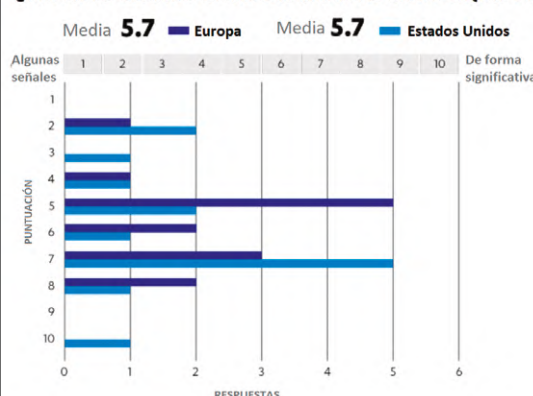
se está implementando ahora". Hay una salvedad: algunos de los encuestados más escépticos tienen preocupaciones sobre el valor a largo plazo de su función: creen que, a menos que su trabajo se entienda verdaderamente como parte del modelo operativo estándar, podría convertirse en un producto básico o consumirse en otra función, en lugar de ser reconocido como un activo estratégico.

En cuanto al presupuesto de ciberseguridad, entre el 53% y el 39% de los encuestados ven mejoras en él. De cualquier forma, los CISO "aceptan que, como miembros del equipo de alta dirección, deben cumplir con los objetivos comerciales, así como asegurarse de que sus responsabilidades para brindar un entorno operativo seguro en todas las cadenas de valor y suministro se puedan compartir entre sus propios equipos y otros". ■

¿SE SIENTEN LOS CISO MÁS REFORZADOS COMO CONSECUENCIA DE LO OCURRIDO EN 2020?



¿HA VISTO SIGNOS DE AGOTAMIENTO EN SU EQUIPO?



Enisa analiza cómo incrementar las sinergias entre los equipos de respuesta y los investigadores para mejorar su eficiencia

La obligación de reuniones virtuales facilita el intercambio de información entre CSIRT y entidades judiciales para luchar contra el ciberdelito

“La respuesta al ciberdelito requiere la cooperación de todos los actores involucrados”, destaca la **Agencia Europea de Ciberseguridad (Enisa)** en su informe titulado ‘Cooperación CSIRT LE: Un estudio de las funciones y las sinergias entre los Estados miembros de la UE’. Un documento en el que analiza cómo mejorar la relación, aprovechar sinergias y optimizar esfuerzos por parte de los equipos de respuesta a incidentes (CSIRT) nacionales y su coordinación con las instituciones que aplican la ley (LE) y el poder judicial (fiscales y jueces). Curiosamente, la Agencia reconoce que queda mucho por mejorar, sin embargo, destaca que “la pandemia ha tenido impacto significativo en la cooperación y los intercambios entre las tres comunidades y su capacidad para funcionar. La interacción incluso, aumentó en algunos casos”, gracias a la facilidad que dan las reuniones virtuales para el intercambio de información y conocimientos.

El informe, elaborado por nueve especialistas europeos en redes y seguridad de la información, ofrece una excelente visión de lo que se está haciendo en ocho países comunitarios -Chequia, Francia, Alemania, Luxemburgo, Noruega, Portugal, Rumania y Suecia- para incrementar la colaboración entre los CSIRT y las entidades judiciales que luchan contra el cibercrimen. Eso sí, quizá se echa de menos que España, el país con más número de CSIRT de la UE, según tiene registrado la propia Enisa, no esté presente en el estudio, aunque la Agencia deja abierta la puerta a que estén en futuras versiones más integrantes europeos. Entre otros ejemplos de buena colaboración, el documento pone en valor el trabajo del CSIRT de la policía judicial gala con su LE para apoyar



las investigaciones sobre ciberdelitos. O las reuniones periódicas que muchas fiscalías celebran con servicios de investigación policial especializados. Así como, el caso de Portugal donde los CSIRT y las LE realizan ejercicios conjuntos para mejorar su capacitación compartiendo metodologías, información y actividades de formación.

En definitiva, destaca el buen trabajo y capacidades de la comunidad CSIRT por su experiencia técnica necesaria para detectar y mitigar incidentes de ciberseguridad y restaurar entornos ciberseguros, unas capacidades muy valoradas por los expertos de LE y del poder judicial, ya que son “particularmente valiosas cuando se trata de ayudar con la recopilación, preservación y presentación de pruebas ante un tribunal de justicia”. De

ta a incidentes, de acuerdo con la Directiva NIS, todos los países analizados han establecido CSIRT nacionales. Sin embargo, aunque existen similitudes, la forma en que están organizados y el lugar que ocupan en la institucionalidad nacional varía de país a país. La forma que las LE, que se ocupan del ciberdelito, están organizadas también varía de un país a otro: algunos países tienen unidades centrales especializadas en ciberdelincuencia, mientras que otros tienen unidades especializadas descentralizadas o ambas.

Grupo de trabajo sobre ciberdelincuencia de la Unión Europea (EUCTF), el de **Conjunto de Acción contra la Ciberdelincuencia (J-CAT)** y la **European Judicial Cybercrime Network (EJCN)**, así como la Red de puntos de contacto en el marco del Convenio del Consejo de Europa sobre el ciberdelito. Además, “las comunidades deben desarrollar sus competencias y desarrollar habilidades organizativas e interculturales para establecer un enlace eficaz con sus homólogos de otros Estados miembros y países de la AELC”, explica el documento.

Metodología de referencia

Además, Enisa propone una metodología para mejorar el trabajo conjunto de los CSIRT con las entidades judiciales, basada tanto en investigación documental como en entrevistas con expertos en la materia y en una matriz de segregación de funciones (SoD),

Conclusiones

“La complejidad técnica y la naturaleza transfronteriza del delito cibernético ha desafiado las competencias (incluidas las habilidades, el conocimiento, los atributos y los comportamientos de los CSIRT, LE y el poder judicial), impulsando las tres comunidades

para perfeccionar su experiencia y establecer mecanismos de cooperación”, destaca el documento a la vez que recuerda que “pueden ocurrir interferencias durante el manejo de incidentes y las investigaciones de delitos cibernéticos, pero que las comunidades hacen esfuerzos para evitar tales interfe-

rencias, crear alianzas efectivas y aprovechar sus sinergias”.

Por ello, aunque se resalta la buena relación existente entre profesionales y organizaciones también lamenta que aún “pueden ocurrir interferencias en el proceso de manejo de incidentes e investigaciones de delitos cibernéticos, principalmente debido a la diferencia en el propósito y mandato de cada una de estas comunidades, es decir, mitigación de incidentes (CSIRT) en comparación con la preservación de pruebas y el enjuiciamiento penal (LE y el poder judicial)”. ■

Iniciativas de ENISA para mejorar la colaboración entre CSIRT y LE



hecho, varios participantes entrevistados confirmaron que el flujo de información entre CSIRT y LE ha sido fundamental para garantizar la conciencia operativa y estratégica de las ciberamenazas. De cualquier forma, reconoce que “los CSIRT, LE y el poder judicial desempeñan cada uno un papel diferente y buscan objetivos diferentes”, por lo que “ayudar a los CSIRT, LE y el poder judicial a comprender sus roles, deberes y competencias de forma recíproca permitirá una cooperación más estrecha al tiempo”.

Eso sí, el documento constata que, en términos de respues-

disponible en los repositorios del organismo europeo en **GitHub**, así como en la documentación del Grupo de Trabajo de Taxonomía de Incidentes de Seguridad de Referencia (RSIT).

Por último, debido a la naturaleza transfronteriza de la ciberdelincuencia, la Agencia recomienda que las tres comunidades conozcan en profundidad los diferentes marcos legales de la UE e internacionales (en particular, el Convenio sobre la Ciberdelincuencia **Consejo de Europa**, 2003) y los mecanismos y redes de cooperación (por ejemplo, la Red de CSIRT), el



¿Tus sistemas SAP y Microsoft están seguros?

Seidor,

multinacional líder en soluciones **SAP y Microsoft.**

Con **tecnología IBM, Microsoft Security**

y operado con **SERVICENOW** te ayuda a mantener

segura tu infraestructura y equipos de trabajo.

El 40% de las empresas atribuyen la responsabilidad del riesgo al CISO y un 35% al CIO, según un informe de BlueVoyant

La ambigüedad sobre quién es el propietario del riesgo cibernético de terceros propicia una falta de confianza y visibilidad de la seguridad de los proveedores

La falta de visibilidad, de monitorización continua y de un líder claro, además de la complejidad a la hora de implementar programas de gestión de riesgos de terceros son los principales retos a los que se enfrentan las empresas a la hora de minimizar los ataques a su red de proveedores. Así se desprende del estudio *Global Insights: Supply Chain Cyber Risk*, elaborado por BlueVoyant en el que también se vislumbran signos para la mejora. Y es que, aunque se necesita más inversión, los presupuestos destinados a solventar la situación están aumentando.

La gestión del riesgo de los proveedores se ha convertido en uno de los mayores desafíos de ciberseguridad. Los ataques



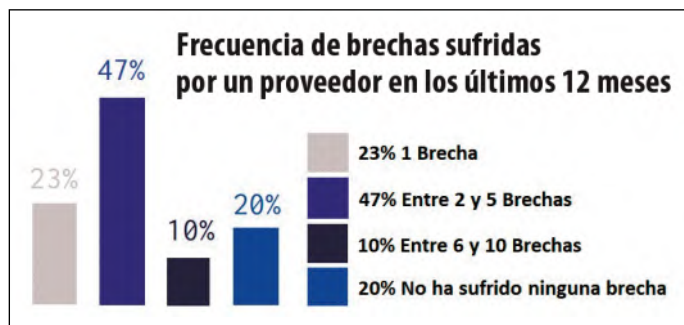
al mundo en los últimos 12 meses, según un estudio de BlueVoyant en el que han participado más de 1.500 CIO, CISO y CPO de Estados Unidos, Reino Unido, Suiza, México y Singapur.

a la cadena de suministro son cada vez más frecuentes y tienen un gran impacto. Un claro ejemplo lo encontramos en el ataque a **SolarWinds**, el cual, se estima que afectó a 18.000 empresas y organismos, entre ellos, la **NASA** y el **Pentágono**. Más recientemente, en febrero, el investigador y experto en seguridad, **Alex Birsan**, daba a conocer, de forma práctica, la facilidad para *hackear* 35 tecnológicas, entre ellas **Microsoft** y **Apple**, con un ataque a la cadena de suministro. Estas son 'solo' grandes pruebas testimoniales de un problema que han sufrido el 80% de las empresas en todo

y CPO de Estados Unidos, Reino Unido, Suiza, México y Singapur. De hecho, tal es su magnitud que el Presidente de EE.UU., **Joe Biden**, firmó a finales de febrero una orden ejecutiva exigiendo a las agencias federales llevar a cabo una revisión de los riesgos de seguridad de la cadena de suministro en los sectores con los que trabajan, incluido el de ciberseguridad.

Falta de visibilidad

Una de las causas de este problema, según el documento publicado por BlueVoyant bajo

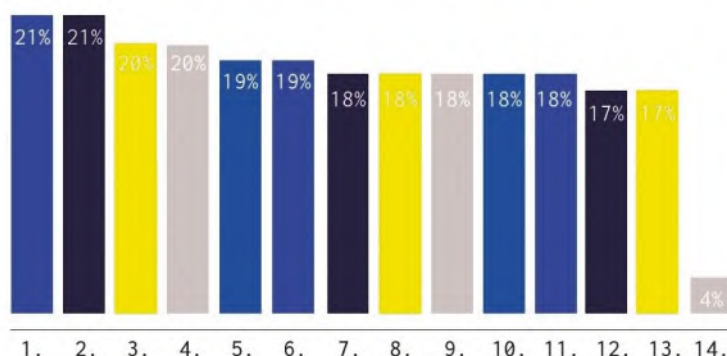


el título 'Global Insights: Supply Chain Cyber Risk', es el "sorprendente desconocimiento de la situación en las empresas". Una realidad que viene dada, en gran parte, debido a que casi un tercio no tiene forma de saber cuándo surge el riesgo y solo un 2% monitoriza de forma diaria o en tiempo real a sus proveedores. "Esto demuestra que una gran mayoría de las organizaciones no tiene visibilidad sobre cadena de suministro o, si la tienen, es con un retraso

significativo", subraya el informe.

La investigación, que analiza en profundidad la escala y el alcance del ciberriesgo en terceros, el impacto que está teniendo, así como los recursos y la forma en que las empresas están abordando este desafío, indica que esa falta de visibilidad del riesgo, lógicamente, limita la capacidad de las empresas para responder a amenazas emergentes. "Este hecho se convierte en la puerta de entrada para que los atacantes se

PRINCIPALES RETOS EN LA GESTIÓN DE RIESGOS DE TERCEROS



- Manejo del volumen de alertas - 21%
- Trabajar con proveedores para mejorar la seguridad - 21%
- Priorizar qué riesgos son urgentes - 20%
- Puntos ciegos en torno a los riesgos emergentes - 20%
- Demasiadas alertas de falsos positivos - 19%
- Tratar con proveedores que no responden - 19%
- Incorporación de proveedores de calidad contrastada - 18%
- Externalización de proveedores de calidad contrastada - 18%
- Comprensión sobre cómo penalizar a los proveedores - 18%
- Entendimiento interno con terceros - 18%
- Hacer cumplir los SLA de los proveedores - 18%
- Visibilidad en tiempo real de los proveedores - 18%
- Falta de recursos internos - 17%
- No tenemos ningún desafío - 4%



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

muevan lateralmente de una red a otra, conduciendo a hallazgos indeseados cuando se realizan auditorías, ya que muchas ciberamenazas han podido ampliar su profundidad y alcance si se identifican tarde”, puntualiza el estudio.

En este sentido, los responsables de la investigación destacan que, irónicamente, de los sectores analizados, los retrasos más prolongados en las auditorías se producen en los de fabricación y servicios públicos, “dos ámbitos con una larga experiencia en la administración de cadenas de suministro complejas que no se están adaptando a la naturaleza del riesgo cibernético actual”.

Estrategias difusas y complejas

El informe apunta que el retraso en el descubrimiento de los riesgos se debe también a la falta de una estrategia clara para atajar el problema. En este punto, pone de manifiesto la existencia de múltiples enfoques que no permiten contar con un programa de gestión de riesgos efectivo, suponiendo un reto, sobre todo, a la hora de integrar, valorar y priorizar la información disponible.

Por ejemplo, “a día de hoy, las prácticas estándar de la industria siguen involucrando el uso de cuestionarios y auditorías puntuales, que son útiles, pero ofrecen un contexto limitado sobre el estado actual de la ciberseguridad dentro de la red de socios y, por tanto, ya no son suficientes”, explica **Jim Rosenthal**, Director Ejecutivo de BlueVoyant. No obstante, casi la mitad de los encuestados (40%) indicaron que están evolucionando hacia una estrategia basada en datos y en el uso de herramientas de análisis de riesgos, transformando procesos manuales por otros más automatizados.

El informe destaca que, además, a la hora de implementar programas de gestión de riesgos de terceros, las empresas tienen

que lidiar con la complejidad y los múltiples desafíos que se presentan, como el manejo de un gran volumen de alertas y la dificultad de trabajar con los proveedores para mejorar el desempeño de la seguridad (ambos con un 21% de las respuestas). A ellos, les siguen la dificultad para priorizar qué riesgos son urgentes y cuáles no (20%), los

media, “las organizaciones están trabajando con una red de más de 1.000 proveedores”. Por este motivo, “comprender el riesgo en la cadena de valor es fundamental. Para ello, las empresas deben ampliar los programas de evaluación, monitorización y realización de informes para cubrir su larga lista de proveedores, inde-

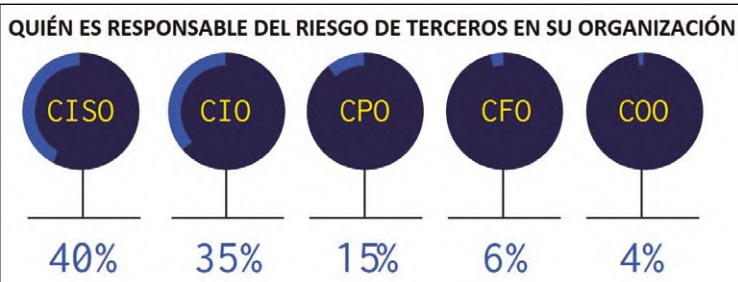
en un ‘silo’, con organizaciones que intentan dividirlo en diversas áreas de negocio”, señala el informe. En este sentido, BlueVoyant es claro y aboga por que “el ciberriesgo de terceros se integre completamente en el riesgo empresarial y sea propiedad de la junta, y que la tolerancia a él, de todas las partes interesadas, se incorpore en la gestión del riesgo cibernético para que exista un equilibrio entre la productividad, la protección, la continuidad y el cumplimiento”.

Aumentan los presupuestos

Los datos muestran, así pues, que aún queda un largo camino por recorrer antes de que las organizaciones puedan estar seguras de que cuentan con un programa de gestión de riesgos cibernéticos de terceros eficaz e integral. Sin embargo, también hay buenas noticias.

Según el informe, aunque la inversión aún no es suficiente, el dinero destinado a abordar este problema va en aumento. El 81% de los encuestados dijo que su presupuesto para la gestión del ciberriesgo de terceros se había incrementado en comparación con los últimos 12 meses. De media, creció un 40%, pero existen matices dependiendo del país y sector al que se pregunte. Por ejemplo, el Reino Unido y los EE.UU. destinaron un 45% más que la media, mientras que en Singapur el aumento planeado fue menor, del 28%. Por su parte, la industria de servicios financieros es la que hará la mayor inversión, ya que espera aumentarlo un 50%.

BlueVoyant también señala que, “dado que la frecuencia de las infracciones cibernéticas es un claro ejemplo de que los enfoques actuales se están quedando cortos, las inversiones en capacidades operativas, que reducen el riesgo día a día, son un área donde la concentración de la inversión produciría un rendimiento mayor”. ■

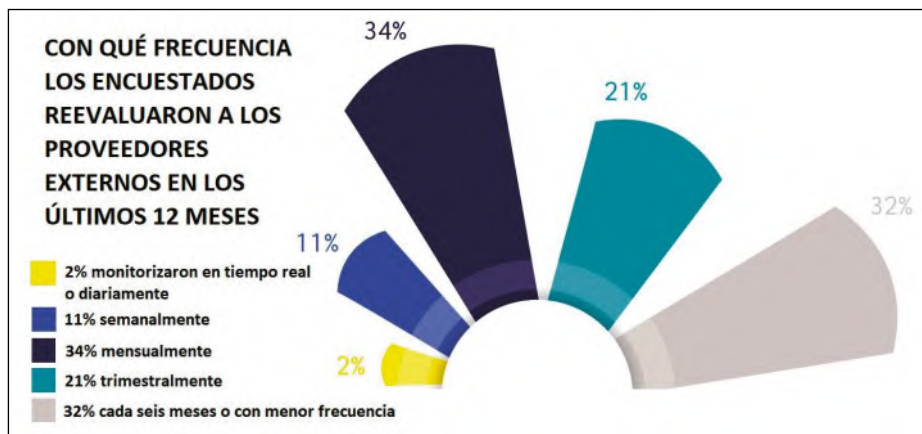


puntos ciegos donde no se tienen recursos y visibilidad para detectar riesgos emergentes (20%), así como tener que lidiar con demasiados falsos positivos (19%).

Asimismo, se suma el hecho de que “las organizaciones no siempre son sinceras con los proveedores cuando descubren un problema” y que “existe una falta de control y proactividad cuando se trata de proteger el negocio que son motivo de preocupación”. Y es que, solo en el 36% de los casos, se informa al proveedor y se espera a que él solucione el

pendientemente de su tamaño y no solo centrándose en los más críticos”. Una labor tan importante como “comprender quién es responsable de administrar estos riesgos”, señalan los responsables del estudio.

Precisamente, en este último aspecto, la investigación deja en evidencia también, “la ambigüedad que parece haber sobre quién es el propietario en última instancia del riesgo cibernético de terceros”. Para el 40% de las organizaciones encuestadas es el CISO, mientras que el 35% apun-



problema, mientras que el mismo porcentaje de encuestados afirma confiar en él para garantizar una seguridad adecuada.

La responsabilidad del riesgo

Sin duda, estos hallazgos son especialmente preocupantes teniendo en cuenta que, de

ta al CIO. Un 15% indica que es el CPO (Chief Product Officer), es decir, la persona encargada de los productos y servicios que ofrece la empresa; un 6% dice que es el responsable financiero (CFO); y un 4% el Jefe de Operaciones (Chief Operational Officer).

“Esta división expone un problema más profundo porque el riesgo cibernético está atrapado



CUENTAS DE SERVICIO PRINCIPAL OBJETIVO DE LOS CIBERATAQUES PARA GANAR PRIVILEGIOS Y ACCESO A INFORMACIÓN CONFIDENCIAL.

Las credenciales de aplicaciones, dispositivos y microservicios que se necesitan para autenticar y dar acceso a datos, están creciendo más que nunca: **más sistemas de control, más dispositivos y más aplicaciones.** Sin una gestión completa del ciclo de vida el número de cuentas de servicio se torna inmanejable, perdiendo control, visibilidad y gobierno.



Account LifeCycle Manager aporta **visibilidad total** sobre sus cuentas de servicio y permite la **gestión total del ciclo de vida** de las mismas:

- **Workflows** para un **control más estricto** sobre las cuentas de servicio.
- **Provisión, gestión y deprovisión** de cuentas de manera transparente y automática sin causar interrupciones
- Refuerza el **gobierno** de todas sus credenciales

GARTNER TOP #1 SECURITY PROJECT



www.thycotic.com

Mayor automatización y coordinación entre departamentos mejoraría el IAM, según la Identity Defined Security Alliance

Las empresas tardan, como poco, tres días en dar de baja los permisos de acceso de los empleados que abandonan la organización

Con el incremento 'explosivo' del número de identidades en las empresas, los procesos y las tecnologías, su gestión se ha vuelto cada vez más importante por el impacto que puede tener en las operaciones comerciales y el riesgo empresarial. Precisamente, la **Identity Defined Security Alliance (IDSA)** ha analizado en un reciente informe la situación de la gestión de identidades (IAM) y si realmente las empresas acometen una correcta política en este campo para reducir los ciberriesgos.

El estudio, con más de 310 encuestados de distintas áreas de negocio como Comercial, Recursos Humanos y la Alta Dirección, titulado 'Gestión de identidad y acceso: la perspectiva de las partes interesadas', alerta de forma especial del retraso con el que se conceden permisos de acceso y, también, con los que se revocan cuando un trabajador deja de pertenecer a una compañía. De hecho, sólo el 34% de los participantes reconocieron que retiraban los permisos de acceso el mismo día que alguien dejaba de estar en la empresa, con el riesgo que supone mantener dicho acceso a la información confidencial, así como el grave problema de cumplimiento normativo que se evidencia.

La mayoría de las empresas (72%) explican que tardan, de media, al menos una semana para dar acceso a los sistemas a un nuevo empleado. Algo chocante por cuanto la mitad confesó que les lleva como poco tres días revocar el acceso cuando deja la organización. Unos datos que, según casi todos los participantes (83%), han podido empeorar en el último año con la popularización del trabajo en remoto y otros factores relacionados con la Covid-19, lo que ha dificultado aún más "la administración del acceso a los sistemas corporativos", destaca el estudio. De hecho, el 56% de los gerentes de ventas explicaron que tenían constancia de personas que se habían llevado información cuando se fueron de la organización.

Además, a pesar de que los encuestados consideran



que este tema supone un problema de seguridad, la mayoría (62%) también reconoce que "dudaría en tomar medidas y cortar el acceso de los trabajadores ante un comportamiento preocupante". De hecho, solo dos de cada cinco encuestados (38%) destacaron que "cortarían inmediatamente el acceso a un trabajador que estaba accediendo a sistemas o datos de manera inapropiada, dejando la puerta abierta al riesgo debido a una amenaza interna o credenciales comprometidas".

Eso sí, siete de cada 10 (69%) encuestados confesaron haberse involucrado personalmente en solucionar problemas de 'comportamiento descuidados' relacionados con la identidad del sistema como, por ejemplo, cuando se detecta el uso del mismo nombre de usuario y contraseña para las cuentas laborales y personales, de dispositivos no autorizados o el intercambio de credenciales con personas que, incluso, no trabajan en la organización. Eso sí, dos tercios (68%) también reconocieron que prima más

hacer su trabajo diario, y que no se detenga el negocio, que la seguridad como tal.

Por ello, los responsables del estudio también destacan que tecnologías como los controles de seguridad con análisis del comportamiento del usuario (UEBA, por sus siglas en inglés) y las de puntuación de riesgo pueden revocar automáticamente el acceso, activar métodos de autenticación avanzados o iniciar revisiones de acceso, lo que limita el daño causado.

Compleja gestión

Dos de cada cinco participantes (39%) estuvieron de acuerdo en que el acceso al sistema en su empresa es "complicado" y la mayoría (83%) cree puede ser mejorable. Algo que se podría acometer, según el estudio, incrementando la automatización de accesos y gestión de identidades, ya que menos de una cuarta parte (23%) cuenta con esta forma de trabajar y solo una tercera parte (35%) tiene automatizado el dar de baja del sistema a los empleados que abandonan la compañía. Una situación complicada por cuanto estudios de

la asociación han destacado que la cantidad de identidades administradas en la empresa se está disparando (el 52% dice que las identidades se han multiplicado por cinco en los últimos 10 años), que las organizaciones luchan por alinear los equipos de identidad y seguridad (solo la mitad, un 53%, informa que la seguridad tiene algún nivel de propiedad para la fuerza laboral (IAM) y que el 94% de las organizaciones han tenido una violación relacionada con la identidad), que el 99% cree que podría haberse evitado. Además, los participantes destacaron que conseguir una identidad segura es "un esfuerzo de equipo" (el 81% cree que, sin importar su rol diferente, comparten la responsabilidad de los problemas de acceso).

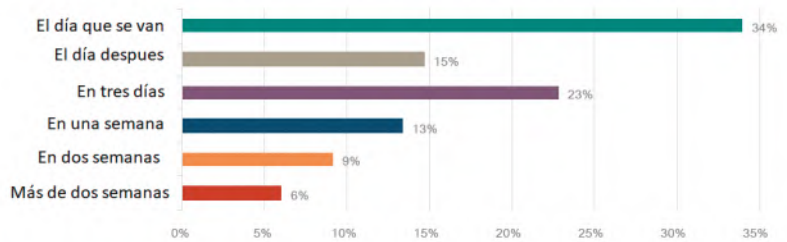
Importante margen de mejora

"La buena noticia para las empresas es que los riesgos destacados en el estudio pueden mitigarse incrementando la contratación de servicios y especialistas en este campo, que también quieren ser parte de la solución, a través del proceso de gobernanza, la automatización y las estrategias de seguridad centradas en la identidad" ha resaltado la Directora Ejecutiva de IDSA, **Julie Smith**.

En su apartado final, la Identity Defined Security Alliance también recuerda muchas de las buenas prácticas que recomienda en IAM, como el aprovisionamiento y desaprovisionamiento automatizado o poner marcha un comité de gobernanza de acceso, que fomente la colaboración entre los administradores de acceso al sistema y / o datos en toda la organización, así como fomentar la colaboración y la coherencia entre los que gestionan el acceso al sistema o a los datos en la organización.

De cualquier forma, como dato positivo, prácticamente todos los participantes (83%) consideran que los procesos de solicitud de acceso tienen un importante margen de mejora, por ejemplo, a través de la automatización y compartiendo las responsabilidades de los problemas de acceso entre departamentos. ■

Cuánto se tarda en revocar el acceso de los ex trabajadores



Qué conductas de riesgo, en gestión de identidades, confiesan haber hecho los trabajadores...



El 'síndrome del impostor', la falta de acuerdos flexibles y la mentorización, principales retos para promocionarse hacia puestos ejecutivos, según el Instituto SANS

La formación, la experiencia y la mentoría, decisivas para impulsar la presencia de la mujer en ciberseguridad, aún un 25% de la fuerza laboral

La carrera para aumentar la presencia femenina en ciencias, tecnología, ingeniería y matemáticas (más conocidas por las siglas STEM), está ganando fuerza y ya supone casi un 25%. En ciberseguridad, la más reciente edición del informe 'Women in Cybersecurity', realizado por la asociación (ISC)², destacó una presencia similar, duplicándose desde 2013, cuando ocupaban solo el 11% de los puestos de trabajo en la industria.

Una tendencia positiva que, sin embargo, también evidencia que queda mucho por hacer. Y es que, en la actualidad, un 35% de las mujeres que trabajan en este segmento de actividad sienten que no están progresando en sus trayectorias profesionales por cuestión de género. Así lo pone de manifiesto el estudio 'Mujeres en ciberseguridad: Abarcando el ciclo de vida profesional', realizado por el Instituto SANS y avalado por la compañía ThreatQuotient, a casi 500 mujeres que desempeñan funciones directivas en ciberseguridad, de ocho países de América del Norte, África, Europa y Asia. La investigación, que analiza la situación actual de estas mujeres y cómo ha sido su trayectoria laboral, destaca que el primer motivo por el que casi la mitad de ellas (un 40,8%) se han "ganado" sus puestos es "simplemente por estar en el lugar y en el momento adecuados", a pesar de que el 44,6% cuenta, al menos, con un máster.

La razón es que todavía "muchas mujeres experimentan una sensación del 'síndrome del impostor' y se resisten a ser consideradas 'líderes', a pesar de tener una gran experiencia y éxito en su carrera", señalan desde ThreatQuotient. A ello, se le une el hecho de que "sigue sin haber acuerdos de trabajo flexibles y un equilibrio realista entre el trabajo y la vida personal, lo que influye en su permanencia o en su decisión de quedarse en



un puesto de trabajo. Esto se traduce en una mayor indecisión a la hora de solicitar roles de responsabilidad, tal y como se muestra en el informe. Es por ello que, en el ámbito de la ciberseguridad, el índice de rotación es mayor en cualquier etapa de su trayectoria profesional que en el caso de los hombres", puntualiza la compañía.

Espacio para el cambio

No obstante, el esfuerzo y la dedicación están dando fruto. La formación combinada con la capacitación en el trabajo genera un impacto positivo en la carrera de cualquier profesional. En el caso de las mujeres encuestadas por Sans, destaca que, del 23% que tenía título universitario y el 12% un posgrado, lograron un puesto en ciberseguridad poco más de un año después de terminar su formación. Incluso un 16% consiguió un contrato tres meses después de conseguir su título. Además, un 14% fueron contratadas al año de terminar la escuela técnica, lograr una certificación u otra capacitación profesional similar.

El 19% de las encuestadas también atribuye su ascenso a posiciones de liderazgo a la formación continua y para el 34% las certifi-

caciones han sido una gran ayuda. De hecho, estas últimas cada vez tienen más valor dentro de las carreras profesionales de las mujeres en ciberseguridad. Por ejemplo, se constató que el 75% ya poseen varias certificaciones relacionadas con su área de actividad. Un 87% resaltaron, además, la importancia de la capacitación en el trabajo.

En cualquier caso, el informe también enfatiza que en este ámbito la experiencia es igual de importante. Alrededor del 47% de las encuestadas manifestaron contar con una experiencia en ciberseguridad de 10 años o más, y un 43% entre cinco y nueve años, consiguiendo acceder en este tiempo a una posición de liderazgo. Por su parte, un 37% de las participantes logró acceder a un puesto *senior* después de pasar entre uno y cuatro años en un nivel medio o *junior*. Solo el 5% de las encuestadas entró de inmediato a un puesto *senior* en su primer trabajo en ciberseguridad.

"Si tenemos en cuenta que los tres factores principales que influyen en la capacidad de ascender a una posición *senior* o de liderazgo son estar en el lugar correcto en el momento adecuado, tener diversas experiencias y obtener certificaciones, es posible controlar estos aspectos e impulsar el cambio", explica el informe, aludiendo al camino que seguir para potenciar la presencia femenina en el sector.

La ayuda de la mentoría, sin género

Sin duda, muchas mujeres con éxito en ciberseguridad pueden ser modelo a seguir para aquellas que esperan entrar en el sector y tener proyección de futuro en este campo. En este sentido, los programas de 'mentorización' o asesoría, tan en boga en la actualidad, son una buena herramienta para atraer, apoyar y aconsejar a una persona que está comenzando su carrera profesional, recuerda el estudio. "Una vez que las mujeres especializadas en carreras STEM se incorporan a una organización, es crucial proporcionar el apoyo adecuado, fomentar el crecimiento, la flexibilidad y el desarrollo de la trayectoria profesional", señalan también desde ThreatQuotient.

En ciberseguridad, solo el 7% de las mujeres han sido asesoradas por otra mujer, lo que supone "un porcentaje muy bajo", lamenta el estudio. En concreto, un 37% ha sido asesorada tanto por hombres, como por mujeres, mientras que el 31% solo ha sido mentorizada por hombres. No obstante, la investigación también destaca que "el género no juega un papel muy importante en este sentido", ya que los resultados obtenidos muestran que "la mentoría es neutral en este aspecto, como debería ser".

Eso sí, para el 33% de las encuestadas, lo que más le ha ayudado a escalar puestos en su trayectoria es contar con "un buen mentor", por delante del *networking* (22%) y de la reputación (20,8%).

Finalmente, el estudio recuerda que, tanto en el campo de las TIC como en ciberseguridad, en particular, existe una falta de expertos y de personal cualificado "que seguirá siendo un problema grave en el futuro". Por este motivo, "es importante que la brecha de género comience a cerrarse y más aún, cuando existen cada vez más mujeres relevantes y con una alta especialización en el sector", concluye. ■



Propone un marco de trabajo con 170 medidas defensivas, divididas en 20 actividades de protección

EL CENTER FOR INTERNET SECURITY de SANS presenta la nueva versión de sus 'Controles CIS' que permiten centrarse en las principales amenazas

El Center for Internet Security, fundado por el Instituto Sans hace dos décadas, presentó la séptima versión de su 'Modelo de Defensa Comunitaria' (CDM), que propone una serie de 'Controles CIS' para mejorar la protección de cualquier organización frente a las amenazas más probables y mayor impacto, dejando de lado las que no lo son para buscar la mayor eficiencia en las estrategias de ciberprotección y la inversión que se precisan para acometerlas con éxito.

Plasmados en más 170 medidas defensivas de ciberseguridad, denominadas salvaguardas, organizadas en 20 actividades de control, sus responsables aseguran que permiten hacer frente "aproximadamente, al 83% de todas las técnicas de ataque que se encuentran en el marco Mitre ATT&CK". De cualquier forma, desde CIS recuerdan que estos controles "no tienen decisiones basadas en riesgos como 'No mitigar'".

"Nuestro objetivo era crear un modelo abierto de alto nivel en el que las clases de contramedidas (sub-

controles o salvaguardas CIS) se organizaran en dos dimensiones: por un lado, en torno a los pasos que da el 'ciclo de vida del atacante' (similar al conocido Lockheed Martin Cyber Kill Chain) y, por otro, en torno a categorías de efecto defensivo".

"De acuerdo con nuestra misión, CIS se compromete a proporcionar a las organizaciones del sector público y privado las herramientas que pueden utilizar para ayudar a mitigar los ataques cibernéticos", explicó el Presidente y Director Ejecutivo de CIS, John Gilligan. "El mapeo de análisis riguroso y basado en datos de los controles CIS para el marco Mitre ATT&CK en nuestro modelo de defensa comunitaria es el paso más reciente que estamos dando para ayudar a todas las organizaciones a comenzar de manera segura y man-

tenerse seguras con higiene cibernética básica".

Patrones de ataque

El marco, precisamente, ha sido una de las fuentes más utilizadas por los responsables del CDM para "mapear fácilmente las salvaguardas más implementables y granulares con medidas defensivas ante las técnicas de ataque" que tiene registrado. Además, estos controles son independientes de la plataforma y el proveedor, por lo que pueden ser usadas para cualquier entidad como medida defensiva para mitigar cada fase de un ataque. En definitiva, su

Por último, se identifican las medidas que permiten mitigar cada fase de la intrusión.

Mientras que las primeras versiones del CDM, de hace casi una década, "se basaron en el juicio consensado de un número relativamente pequeño de personas con experiencia y se validaron con los comentarios del público de toda la industria", esta versión está basada en numerosas fuentes como los datos del informe de ciberamenazas de Verizon (DBIR) y el Mitre ATT&CK, entre otras. Se trata de que las organizaciones puedan responder de forma clara a dos cuestiones: qué tipos de contramedidas podrían ayudar a prevenir las primeras fases de los ataques y si se invierte en protección con eficiencia.

consideradas 'básicas' que permiten hacer frente al 79% de las técnicas de patrones de ataque, ante piratería de aplicaciones web (IG2) cubriendo el 100% de las posibles amenazas y con un 80% ante intrusiones dirigidas (IG3). Así, los tres IG de controles CIS corresponden a tres niveles diferentes de inversión en controles de seguridad que corresponden a la sofisticación esperada del atacante, la importancia de lo que se protege y el alcance del daño anticipado. Una empresa puede sopesar el costo de una salvaguarda en el contexto de todos los efectos de mitigación implementados para abordar una técnica de ataque. "Cualquier organización puede comenzar implementando IG1 para crear una base sólida para la defensa cibernética".

Y, en función del nivel de riesgo -valorando sobre todo las pérdidas que supondría un ataque con éxito-, invertir en salvaguardas adicionales como las IG2 e IG3. Y es que "cuantas más salvaguardas se asignen a una técnica, se obtendrá un valor más alto. Por lo tanto, los controles son más efectivos para defenderse de las técnicas con los valores más altos que se muestran en el gráfico. La

CINCO PRINCIPALES MITIGACIONES APLICADAS A LAS SALVAGUARDAS



implementación permite contar con 'higiene cibernética básica' frente a las técnicas de ataque presentes en los cinco patrones más usados por el cibercrimen, según el 'Informe de Investigaciones de Violación de Datos', de Verizon (DBIR) de 2019: ransomware, piratería de aplicaciones web, uso indebido de privilegios, malware e intrusiones dirigidas.

El modelo CDM se basa en tres pasos. El primero consiste en identificar los patrones de ataque más frecuentes y dañinos a partir de los informes de investigación actuales de la industria sobre incidentes e infracciones. El segundo conlleva normalizar los patrones de ataque usando el marco de trabajo Mitre ATT&CK con el conjunto de técnicas implementadas para lograr cada táctica para cada fase de un ataque.

10 TÉCNICAS APLICADAS A LAS SALVAGUARDAS



"Una vez que se identificaron y analizaron los patrones de ataque, se empleó el marco Mitre ATT&CK para seleccionar qué técnicas están asociadas con patrones específicos", explican sus impulsores. A través del mapeo de los Controles, el nuevo modelo también proporciona pasos específicos y concretos que todas las organizaciones pueden tomar para protegerse mejor contra los ataques cibernéticos, especialmente el malware y el ransomware, según el tipo de entidad, riesgo e inversión que quieran asumir.

Tres grupos, tres niveles

Por ello, el CDM muestra tres Grupos de Implementación (IG). En concreto ante malware (IG1), que supone poner en marcha las medidas

asignación de múltiples salvaguardas a una técnica también ayuda a ilustrar la defensa en profundidad. Muchas salvaguardas se asignaron a 20 o más técnicas", destacan sus creadores.

Retos futuros

CIS también destaca en la presentación de esta nueva versión de sus controles que ya trabaja en una nueva con importantes novedades de aspectos que no se pudieron 'mapear' relacionados con la capacidad de anticipación, como son la prevención del comportamiento en el endpoint, la detección de intrusos basados en host o capacidades similares y la puesta en marcha de un programa de inteligencia de amenazas. ■

10.342 fueron consideradas 'críticas' o de 'alta gravedad', según un estudio de Redscan

Con más de 18.000 vulnerabilidades parcheadas, 2020 marcó un nuevo récord en el número de las que se detectaron

El uso intensivo de la tecnología y dispositivos del Internet de las Cosas, ha hecho que el año pasado sea el más prolijo en detección de vulnerabilidades en todo tipo de sistemas. Sólo las consideradas 'críticas' o de 'alta gravedad', un 57%, supusieron 10.342 de las más de 18.000 detectadas –unas 50, cada día-. Una cifra preocupante teniendo en cuenta que, en 2010, su número apenas superaba las 4.600, según un estudio de la compañía **Redscan** en el que ha empleado, entre otras fuentes, el análisis de la 'Base de Datos Nacional de Vulnerabilidades' (NVD) y el repositorio de 'Vulnerabilidades y Exposiciones Comunes' (CVE), del **Instituto de Tecnología de Massachusetts** (NIST). "Las vulnerabilidades van en aumento, incluidas algunas de las variantes más peligrosas. Sin embargo, estamos viendo signos más positivos, por ejemplo, una caída en el porcentaje de las que no requieren privilegios de usuario para explotar", dijo el Jefe de Inteligencia de Amenazas en Redscan, **George Glass**, quien también destacó que "dado el creciente número de ECV que deben abordarse, se necesita un mayor contexto para facilitar una toma de decisiones más rápida y eficaz".

Y es que la situación es más que mejorable. Casi 4.000 de las vulnerabilidades descubiertas el pasado año –un 21% del total– pueden considerarse "lo peor de lo peor", por su alto impacto y facilidad de uso, según la investigación, que considera que "al analizar el riesgo potencial que representan, las organizaciones deben considerar más que solo su puntaje de gravedad. Muchas CVE nunca o rara vez se explotan en el mundo real porque son demasiado complejas o requieren que los atacantes tengan acceso a privilegios de alto nivel". De hecho, en la década de 1980 y principios de la de 1990, la gran mayoría de las vulnerabilidades eran de baja complejidad, pero el número disminuyó a menos del 50% en 2010. El número ha aumentado nuevamente en los últimos años y en 2020, las vulnerabilidades de baja complejidad representaron el 63% de todas.



El punto más positivo de la investigación es que las vulnerabilidades que no requieren privilegios de usuario para explotar disminuyeron, pasando del 71% en 2016, al 58% en 2020. Eso sí, también llama la atención que el 68% de las vulnerabilidades descubiertas "no requieren interacción del usuario para poderse explotar", facilitando aún más el trabajo de los ciberdelincuentes que sólo tienen que detectar qué sistemas las tienen y actuar. Un aspecto crítico cuando se trata, por ejemplo, de entornos como instalaciones energéticas, de transporte o de control industrial, ya que pueden ser explotadas fácilmente por atacantes poco sofisticados, resultando en ataques masivos. Este aspecto es preocupante teniendo en cuenta que el gran número que continuamente se reporta complica en exceso el trabajo de los equipos de ciberseguridad por proteger el entorno laboral

y la información más sensible de las organizaciones.

Por ello, muchos expertos recomiendan una actitud proactiva apostando por plataformas de detección basadas en el comportamiento de usuarios y aplicaciones como medida para detectar a los adversarios, además de implementar una política eficaz de parcheo, lo más automatizada posible, de vulnerabilidades. "Subestimar lo que parecen ser vulnerabilidades de bajo riesgo puede dejar a las organizaciones abiertas al 'encadenamiento', en el que los atacantes pasan de una vulnerabilidad a otra para obtener acceso gradual en etapas cada vez más críticas", resalta el informe.

La investigación resalta, asimismo, la importancia de comprobar que este tipo de políticas de seguridad se acometen por parte de proveedores de software y suministradores. En definitiva, recomienda que los proveedores asuman la responsabilidad de todo el código que incorporan a su producto y establecer una higiene

sostenible en la función de prueba, así como detectar las vulnerabilidades con anticipación. Hasta que eso suceda, las organizaciones deben asumir la responsabilidad del software que utilizan y realizar sus propias pruebas de vulnerabilidad y penetración para descubrir las vulnerabilidades entregadas por sus proveedores.

Entre las recomendaciones de los responsables de la investigación para hacer frente al incremento de vulnerabilidades, se recomienda acometer una "defensa en profundidad".

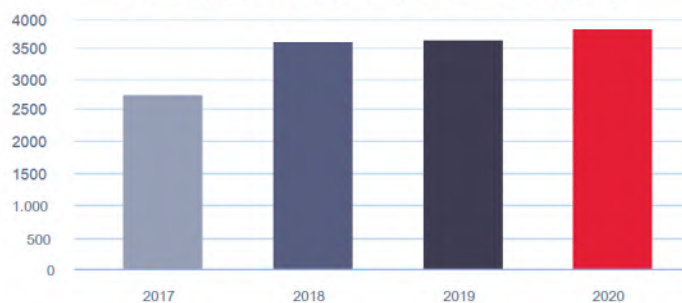
Así, desde Redscan aconsejan adoptar un enfoque de múltiples capas para la gestión de vulnerabilidades, incluyendo la realización de evaluaciones de vulnerabilidad internas y externas al menos una vez al mes, el uso intensivo de inteligencia de amenazas de código abierto para mantenerse informado sobre amenazas y vulnerabilidades emergentes, así como obtener un contexto de la vida real, además de realizar, ya sea con equipos propios o externos, pruebas de penetración para ayudar a identificar vulnerabilidades ocultas y comprender mejor cómo podrían ser explotadas por los ciberdelincuentes.

También, recomiendan supervisar de cerca las redes y los puntos finales en busca de evidencia de explotación de vulnerabilidades y realizar "ejercicios de modelado de amenazas de mesa" para obtener una descripción general de la ruta de ataque potencial de un atacante en el caso de que se explote una vulnerabilidad existente.

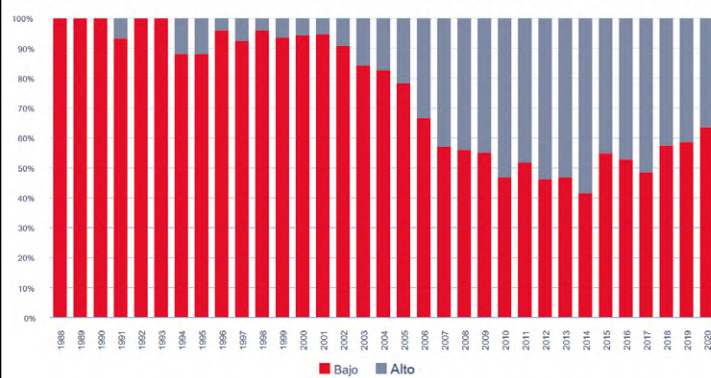
Eso sí, no todo es negativo: "por preocupante que pueda parecer el crecimiento de nuevas vulnerabilidades, tal vez no sea demasiado sorprendente y está en línea con el creciente número de dispositivos, productos y servicios digitales conectados a Internet que se utilizan a nivel mundial". Y es que, entre otras muchas causas, el crecimiento de vulnerabilidades también es atribuible a un aumento en el número de Autoridades de Numeración de CVE (CNA), de las cuales ahora hay más de 150 en todo el mundo (España cuenta con dos: el **Incibe** y **Alias Robotics**, participada por **Telefónica**). ■

NÚMERO DE VULNERABILIDADES MUY PELIGROSAS

Complejidad de ataque [Bajo] + Privilegios requeridos [Ninguno]
+ La interacción del usuario [Ninguno] + Confidencialidad [Alto]



PORCENTAJE DE VULNERABILIDADES (ECV) DE BAJA Y ALTA COMPLEJIDAD ENTRE 1988 Y 2020



Un informe de RiskRecon e Instituto Cyentia analiza el peligro de implementarlos en entornos corporativos

Tener dispositivos IoT sin una configuración y seguridad adecuada multiplica por 70 el riesgo de exponer activos críticos

Aunque están destinados a hacernos la vida más sencilla, la proliferación de dispositivos conectados está generando muchos ‘dolores de cabeza’ a los responsables de seguridad corporativos por los nuevos riesgos que conllevan. Se calcula que, en 2009, ya había más dispositivos conectados a Internet en el mundo que número de personas. **Gartner**, de hecho, calcula que actualmente hay unos 21.000 millones y otros analistas como **IDC** consideran que en sólo cuatro años superarán los 60.000. Para conocer cómo afrontar la seguridad frente a la popularización de estos dispositivos, la compañía **RiskRecon** y el **Instituto Cyentia** han analizado qué uso se hace de ellos y de los datos que generan en 35.000 organizaciones, prestando especial atención si se gestionan de forma segura.

Mala solución

Precisamente, eso es algo especialmente preocupante, ya que en el estudio se ha constatado que el 62% de las organizaciones que los utiliza tiene, generalmente, más problemas de seguridad que las que no. “Cuanto mayor sea la cantidad de dispositivos IoT expuestos, mayor será la probabilidad de que una organización experimente algún tipo de problema relacionado con el filtrado de red y la aplicación de parches de software”, recuerda el documento.

Además, el 86% de los problemas de seguridad en los dispositivos de IoT se consideran críticos. Unos problemas que “se agravan porque se resuelven más tarde en estos dispositivos que en otro software. Si añadimos a esto la incapacidad de parchear



fácilmente sus vulnerabilidades y su soporte inferior a otros artículos, es evidente que cualquier evaluación del riesgo de seguridad de una empresa debe contener una evaluación de los dispositivos de IoT”, destaca la investigación.

De cualquier forma, ya sea por su utilidad o por su falta de seguridad,

parte del 1% (0.038%) de todos los hosts escaneados de las empresas son dispositivos de IoT”. Eso sí, el estudio también explica que esta cifra pequeña se incrementa a medida que disminuye el tamaño de la empresa que son las que más “huella digital” generan con ellos.

No es un problema menor, ya que existen grandes diferencias entre su adopción por sectores. Por ejemplo, el estudio destaca que en el ámbito educativo su empleo es hasta 14 veces superior que la tasa media de los ámbitos analizados.

Primar la seguridad

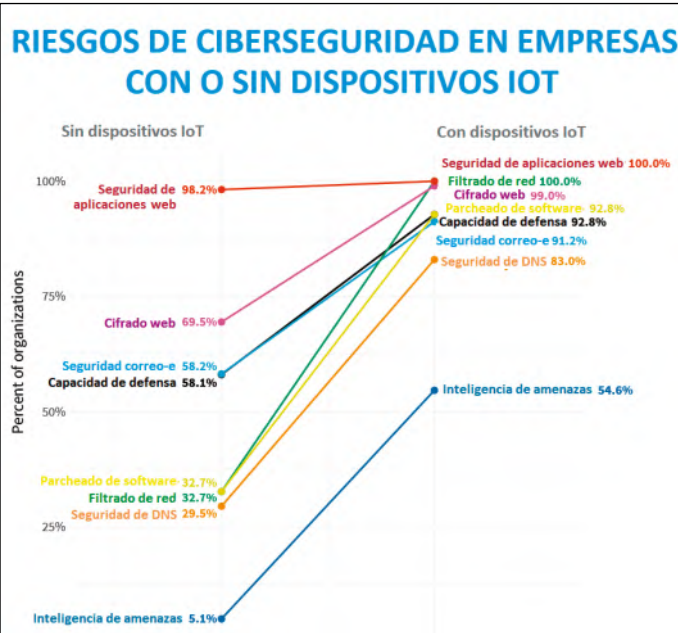
El informe también analiza en profundidad cómo anticiparse a las posibles amenazas que generen este tipo de dispositivos. “Conocer su cantidad y dónde es más probable que estén es un comienzo. Pero la siguiente pregunta es preguntarse qué tipos de dispositivos son y qué seguridad o inseguridad ofrecen”, explican los investigadores a la vez que destacan la necesidad de constatar que es vital comprobar que el software que utilizan es seguro. En cuanto a tipo de ‘cosas’ conectadas,

el documento identificó tres como los mayoritarios: cámaras (54%), interfaces de administración (30%) e impresoras (16%). De cualquier forma, “casi el 86% de los dispositivos de IoT tienen hallazgos de seguridad calificados como críticos”, explica el documento que también indica que, para ver lo preocupante de la situación, sirva tener en cuenta que “solo el 2% de los hosts que no son de IoT tienen hallazgos críticos”. O dicho de otra forma: “la gran mayoría de los dispositivos de IoT tienen fallos que probablemente resulten en un serio compromiso si se explotan”. Es más, la falta de seguridad en este tipo de cosas conectadas es tan preocupante que RiskRecon considera que debe seguirse el principio de ‘IoT como señal de humo’ reforzando la seguridad en caso de dar con uno de este tipo. De hecho, entre los problemas más habituales detectados con ellos están los asociados al filtrado de redes y el parcheo de software. Además, las compañías que los emplean multiplican por 70 los problemas de protección entre los activos de alto valor, según el documento.

Como conclusión, el informe anima a realizar en el entorno corporativo análisis continuos de seguridad y perfiles de TI para contar con “una visibilidad íntima de sus sistemas conectados a Internet, dónde están alojados, cuál es su configuración y si cumplen con los requisitos de seguridad”, recordando que la compañía realiza este tipo de servicios contemplando hasta 41 criterios de protección para “determinar automáticamente el valor de los activos en riesgo”, pudiendo “identificar fácilmente problemas, priorizar la respuesta y actuar de manera eficiente”. También, destaca la importancia de “realizar evaluaciones de terceros”, ya que carecer de su nivel de seguridad “supone una gran desventaja”, sobre todo, si las empresas con las que se trabaja o, en caso de fusión o absorción, no tienen bien configurados y protegidos este tipo de dispositivos. ■



dad, estos dispositivos conectados aún son minoritarios en el ámbito corporativo. Según los datos de RiskRecon, “menos de una vigésima



El gran número de tareas repetitivas provoca que dediquen hasta cinco horas de su jornada de trabajo al ocio

El exceso de carga de trabajo y la alta rotación hacen que los profesionales de ciberseguridad busquen otros retos laborales

Para conocer en profundidad la realidad del sector de ciberseguridad, **Kaspersky** ha elaborado un completo estudio, titulado 'Gestionar el equipo de seguridad TI', en el que ha preguntado a 5.266 responsables de la toma de decisiones de TI en 31 países, en junio de 2020. Entre sus conclusiones más llamativas que motivan el cambio de empresas más allá del estancamiento en el desarrollo profesional, la remuneración, los conflictos o la insatisfacción con el trabajo, un 42% destacaron la elevada carga de trabajo que sufren en el día a día. Un problema agravado por una alta rotación laboral, según destacaron el 45% de los participantes y que suma una "tensión adicional" al gran número de laborales diarias de los empleados existentes, ya que según el 61% supone más carga de trabajo. A ello se suma que la falta de políticas de ciberseguridad cuando un empleado se da de baja incrementa los ciberriesgos porque, por ejemplo, el 56% de los que dejan una compañía no devuelven sus dispositivos corporativos tras su marcha e, incluso, un 51% utiliza datos corporativos tras irse.

Distracciones en horario de trabajo

Además, el estudio destaca como motivo de cambio laboral que, cada vez más labores en ciberprotección son "rutinarias y repetitivas". Por ello, también ha identificado que el 80% del personal de seguridad TI en Europa confiese realizar actividades de ocio durante las horas de trabajo, en torno a cinco horas semanales. La razón, según el 43% de los participantes, es la necesidad de tener un descanso entre tarea y tarea, más que al aburrimiento o la falta de trabajo. Además, se ha constatado que el cambio al teletrabajo ha difuminado la línea entre el tiempo de trabajo y el personal, lo que supone, entre otros aspectos, que también se celebren más reuniones fuera del horario laboral tradicional -de 9 a 17 horas-. Curiosamente, el estudio ha identificado los principales 'pasatiempos' de los profesionales europeos en horas de trabajo: leer las noticias (34%) o publicaciones profesionales (33%), ver películas o series de televisión (29%) o videos en YouTube (28%). Además, algo más de un cuarto de los encuestados se las arregla para hacer ejercicio físico (28%) en ese tiempo, según destaca el estudio.

Trabajo por objetivos

"No creo que sea un problema que los empleados se distraigan del trabajo. La jornada laboral se ha alargado y se requieren descansos. La clave es controlar

el rendimiento de las tareas, no cuántas horas de trabajo se dedican a un pasatiempo. Además, puede ser normal que la gente vea videos, ya que puede dar ideas sobre cómo resolver un problema", comenta el Jefe de Seguridad de la Información de Kaspersky, **Andrey Evdokimov**. "Los empleados deben tener metas, KPIs, objetivos y métricas que describan la calidad y la velocidad de su trabajo. Si el rendimiento no se ve afectado, no hay problemas con el hecho de que una persona se distraiga del trabajo", destaca Jefe del Centro de Operaciones de Seguridad de Kaspersky, **Sergey Soldatov**.

Panorama de ciberseguridad corporativa

En cuanto a la situación de la ciberseguridad en las empresas, el estudio también ofrece una imagen nítida de la situación actual. Por ejemplo, la mitad de las compañías, un 52%, ya cuenta con un departamento de seguridad de TI dedicado e, incluso, un 20% tiene un centro de operaciones de seguridad interno, además de un equipo especial de análisis de *malware*, en un 14% de los casos. Unas capacidades que, en un 69%, consideran que podrían complementar con proveedores de servicios de seguridad gestionados en los próximos 12 meses, según el 69%. Entre las principales razones para ello está la necesidad

de conocimientos especializados y una mejor rentabilidad (41%).

Ciberinteligencia

Además, dada la mayor conciencia de contar con información sobre amenazas dentro del departamento de ciberseguridad, más de la mitad de los encuestados (66%) explicaron tener responsabilidades de análisis de inteligencia de amenazas. Para ello, consultan bases de datos de vulnerabilidades (61%), participan en foros y blogs profesionales (45%), además de recibir inteligencia sobre amenazas de *feeds* de pago (42%) y gratuitos (33%).

Eso sí, aún falta mucho por hacer para trabajar compartiendo información de ciberamenazas. La mitad de los encuestados (52%) dijo que sus responsables no les permitían compartir información sobre inteligencia de amenazas con comunidades externas. Esto significa que menos de la mitad (44%) había compartido conocimientos potencialmente críticos más allá de los límites de su propio negocio: el 77% de los que tenían permiso para hacerlo y el 8% de los que no.

Motivación de empleados

En el informe, la firma rusa da unas recomendaciones a las empresas para motivar a sus equipos de ciberprotección. Por ejemplo, propone contar con un empleado de ciberseguridad por cada 10 profesionales de TI, disponer de Centro de Operaciones de Ciberseguridad (SOC), que trabaje las 24 horas con, al menos, cinco empleados -dos como responsables de la monitorización; uno para investigación; una persona que combinará las funciones de arquitecto e ingeniero; un administrador; y un gerente de SOC-. "Además, en el SOC, el trabajo por turnos ayuda a evitar el exceso de trabajo. Las buenas condiciones de trabajo, que incluyen altos salarios y beneficios, programas sociales, una cultura corporativa saludable y relaciones en el equipo, también contribuyen a la retención", resalta el estudio.

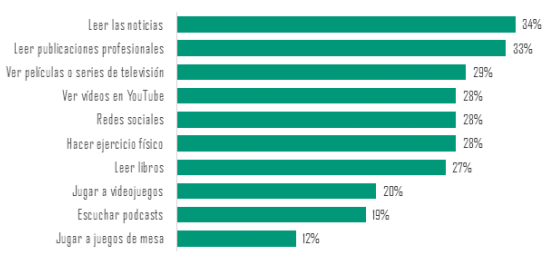
Asimismo, recomienda apostar por "externalizar las tareas típicas de seguridad TI. De este modo, los empleados internos tendrán más tiempo para centrarse en los requisitos específicos de la empresa y en la protección de la infraestructura TI heredada".

Para incentivar que estén motivados y no caigan en el aburrimiento también aconseja "asignar a los empleados tareas diferentes y no estándar para que no se queden estancados y puedan desarrollar sus habilidades". ■

¿PORQUÉ LOS PROFESIONALES DEL SECTOR QUIEREN CAMBIAR DE TRABAJO?



ACTIVIDADES QUE HACEN LOS EMPLEADOS DE SEGURIDAD TI EUROPEOS EN EL TRABAJO



Redes 5G, la ciberseguridad pasa a un primer plano por derecho propio

En el ámbito de las redes 5G, la ciberseguridad pasa a un primer plano por derecho propio. Todas las capacidades de esta tecnología unido a la mayor preocupación y concienciación con la confidencialidad y la privacidad hacen necesario repensar la visión, las políticas, las arquitecturas, las metodologías, los controles y las medidas de seguridad que venimos utilizando hasta el momento. En este sentido, ya hay mucho trabajo hecho que ha permitido disponer –a día de hoy– de unos buenos pilares para que las expectativas se puedan cumplir. Pero también es cierto, que nos queda el último sprint para acabar de aterrizar adecuadamente algunas cuestiones. Y en este contexto el enfoque holístico de la ciberseguridad 5G es el único camino posible.



Ignacio Pérez García / Óscar Díaz López

Ya han pasado unos cuantos años desde que se empezó a analizar la viabilidad y posibilidades de las comunicaciones 5G. Desde ese momento (finales de la primera década de 2000) hasta la crisis de la Covid-19, hubo un desarrollo paulatino de esas capacidades con el firme propósito de poder desplegar esta tecnología lo antes posible. Factores como la necesidad de inversión en infraestructuras, la falta de regulación o apuesta clara por los gobiernos, así como los posibles riesgos de seguridad para su despliegue, han sido algunos de los factores que han provocado que hoy en día todavía no sea una realidad más plausible.

La pandemia mundial ha puesto todo de vuelta y necesitamos sacar lecciones aprendidas, ser creativos e intentar revertir el terrible impacto socio-económico sufrido. La aceleración del despliegue y uso del 5G se ve claramente como una clara palanca tecnológica que puede ayudar a:

- **Reparar y reconfigurar todo lo que la Covid-19 ha interrumpido.** 5G ofrece a las empresas una plataforma de datos eficiente sobre la que puede ofrecer servicios nuevos y existentes, ayudando a restaurar ingresos y actividad económica perdidos durante la pandemia.

- **Repensar el futuro para adoptar nuevos modelos de negocio y casos de uso.** Con 5G, las empresas pueden tomar una nueva lupa donde mirar cómo operan, reconsiderar las ofertas de productos, enfoques de salida al mercado, e incluso las industrias y geografías en las que maniobran.

- **Reconfigurar el funcionamiento de las organizaciones.** Además de ser una tecnología poderosa por derecho propio, 5G puede unir y potenciar a otras tecnologías, incluyendo Inteligencia Artificial, Realidad Virtual o IoT. Todas estas tecnologías funcionan mejor y aportan más valor cuando se aplica en combinación con 5G, lo que ayuda a las empresas

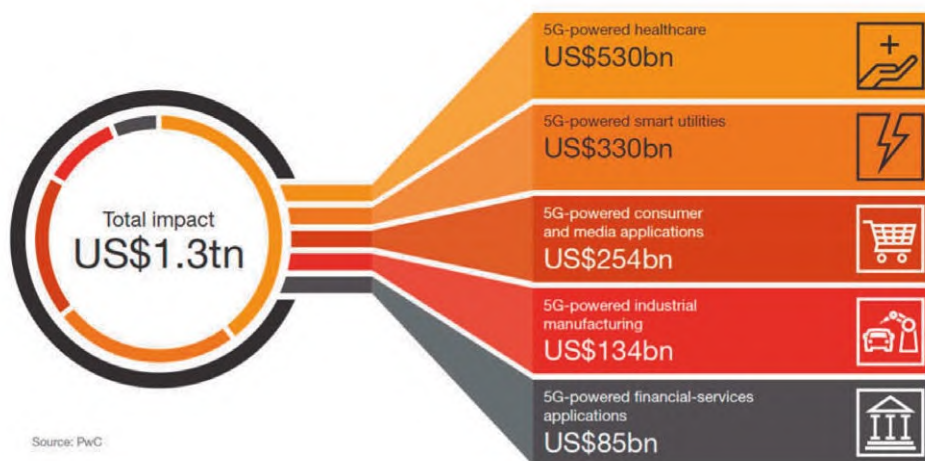
crean un “*volante tecnológico*”: el reprimido cuyo poder será aún mayor a raíz de la pandemia.

Y con los pasos de gigante que en este último año se están dando, sí podemos empezar a cuantificar el impacto potencial de la tecnología en términos económicos. Según el *Informe de PwC* recientemente publicado relativo al “*Impacto económico global de 5G*”, se prevé que para el año 2030 el impulso global sobre el PIB mundial sea de 1,3 trillones de dólares. Este estudio ha identificado cinco industrias (salud, servicios públicos inteligentes, consumidores y medios, manufactura industrial y servicios financieros) que pueden beneficiarse significativamente de la tecnología 5G.

Por todo ello, parece más que razonable

que todos aunemos esfuerzos para acelerar la digitalización en todos los sectores, donde la tecnología 5G pueda actuar como catalizador para que el bienestar social y económico pueda alcanzar niveles previos a la pandemia o incluso rebote con más fuerza.

En Europa, y por consiguiente en todos sus estados miembros, la apuesta es firme. Un claro ejemplo son los “fondos de recuperación Next Generation EU” (NGEU), que contribuirán a la reconstrucción de la Unión Europea después de la pandemia y apoyarán a la inversión en las transiciones ecológica y digital. A su vez, asociado al NGEU se encuentra el Mecanismo de Recuperación y Resiliencia (MRR), que es la piedra angular y distribuirá hasta un máximo de 312 500 millones en subvenciones y 360 000



Ya se ha definido una estrategia común, se han promulgado directrices y recomendaciones, y se apuesta por el desarrollo de un esquema de certificación de la ciberseguridad para redes 5G, teniendo en consideración algunos de los existentes actualmente, como por ejemplo NESAS.



Riesgos y retos ...



Previsible aumento de los ciberataques al haber muchos más puntos de entrada.



Actual dependencia de los operadores de redes móviles respecto a **un conjunto limitado de proveedores**, aumentando la exposición a una interrupción de suministro.



La **confidencialidad** como elemento clave debido al **aumento del riesgo de espionaje en las comunicaciones** de la ciudadanía y los gobiernos.



La **disponibilidad e integridad** de las redes se convierten en **graves preocupaciones** en materia de seguridad.



... originan un paradigma de seguridad

Se hace necesario **reevaluar y rediseñar un marco de seguridad y políticas** aplicables al sector de las telecomunicaciones y a su ecosistema.

millones en préstamos). Uno de los pilares sobre los que se estructura esas medidas financiadas es la digitalización. Los estados miembros tendrán que proponer medidas para digitalizar la administración pública y las empresas, y alinear las propuestas con las estrategias europeas -entre otras en lo referente al gobierno de los datos, la inteligencia artificial y la ciberseguridad.

A continuación, exponemos dos aspectos que entendemos claves desde el punto de vista de ciberseguridad, y que deberían estar muy presentes para favorecer la cuenta atrás del lanzamiento masivo de la tecnología 5G.

Enfoque holístico para la ciberseguridad 5G

Como probable infraestructura crítica, no cabe duda de que uno de los aspectos que más preocupa en el despliegue de la tecnología 5G es su ciberseguridad. Seguramente, cuando llegue el momento de despliegue masivo de esta tecnología siga habiendo fallos de seguridad; y es responsabilidad de todos los actores involucrados en su despliegue (gobiernos, operadores, suministradores y fabricantes), definir e implementar unos requisitos de seguridad que permitan a los usuarios finales confiar en un alto grado en esta tecnología. Por tanto, será necesario un **enfoque holístico para cubrir con garantías toda la cadena de suministro 5G**.

El potencial incremento de los ciberataques, la protección de los diferentes perímetros de exposición, el análisis de ingentes volúmenes de datos para la detección de incidentes, la identidad digital y autenticación, o la propia seguridad de los dispositivos de usuario, son algunas de las preocupaciones que se han analizado para definirlos requerimientos y buenas prácticas aplicables.

Y ahondando en las visiones de ese enfoque holístico, en primer lugar, **los gobiernos** -además de impulsar la disposición de frecuencias y el despliegue de la infraes-

tructura necesaria- tendrán que regular los roles y responsabilidades de cada uno de los actores en la 5G. En este sentido, sí que durante los últimos años ha habido grandes avances. Si nos fijamos en Europa, se quiere tomar una posición clara que acabe probablemente imponiéndose en el resto del mundo -más allá de vetos o posturas menos flexibles. En esa línea, se ha definido una estrategia común, se han promulgado directrices y recomendaciones, y se apuesta por el desarrollo de un esquema de certificación de la ciberseguridad para redes 5G (teniendo en consideración algunos de los existentes actualmente, como por ejemplo

garantizar la seguridad de la red de acceso, los componentes software / hardware y el propio terminal (y por consiguiente información del usuario). En lo relativo a objetivos de control, los aspectos donde habrá que prestar especial atención son los relativos a la autenticación y el acceso, la seguridad de la red virtualizada y la seguridad de la infraestructura. Adicionalmente, habrá que dar respuesta a un problema que reaparece cíclicamente en el tiempo, pero que esta vez generará mucho más esfuerzo. En este nuevo mundo digital hiperconectado, volverán a coexistir diferentes tecnologías (5G/4G/3G), que requerirán un nivel

homogéneo de control y seguridad; de nada servirá definir unos altos niveles de seguridad para el 5G si no se revisan algunos de los implantados sobre las anteriores tecnologías. De hecho, en las primeras fases de despliegue se emulan servicios 5G sobre parte de la infraestructura heredada, y, por tanto, es probable que los problemas de seguridad también se hereden. Por otro lado, todos los cambios tecnológicos asociados a su despliegue (virtualización de las infraestructuras, la computación al borde de la red o la mayor dependencia de componentes software) deberá traer un incremento en el número de suministradores. Y si de manera natural no sucede, los operadores tendrán que diseñar estrategias de diversificación que garanticen la no dependencia de ciertos suministradores y, por consiguiente, la continuidad de negocio. Estos últimos tendrán que justificar a los operadores y a los gobiernos la fiabilidad técnica y la seguridad de sus productos o servicios (por defecto y desde el diseño), así como su independencia de injerencias externas.

Por último, no hay que olvidar al **usuario**, quien como consumidor exigirá un nivel de seguridad en los servicios o productos que adquiera. En este sentido, es más que probable que se articulen procesos de homologación y/o certificación de terminales para garantizar los requisitos de seguridad.



Fuente: European 5G Observatory / IDATE DigiWorld Dic2020

NESAS). Como se indica en el Observatorio europeo de 5G, muchos de los estados miembros ya han definido una hoja de ruta para desarrollar localmente esa estrategia común europea. A nivel de España, somos uno de los estados miembros con mayor avance, disponiendo de una hoja de ruta clara y con un borrador de Anteproyecto de Ley que -con su entrada en vigor- permitirá regular los requerimientos para cada actor involucrado.

En segundo lugar, **los operadores y suministradores** deberán hacer foco en

Integrar la gestión de la seguridad en la gestión del riesgo de terceros

Como se ha comentado anteriormente, la gestión continua de riesgos vuelve a estar muy presente -también- en todo lo relativo a las redes 5G (como ha pasado en otros muchos ámbitos; como por ejemplo en el RGPD). Algunas iniciativas europeas que soportan esa trascendencia de la gestión de riesgos son, por ejemplo, la "recomendación 2019/534 de la Comisión" o la "EU Toolbox of risk mitigating measures". A nivel español, es el propio borrador de Anteproyecto de Ley quien de forma explícita exige análisis de riesgos de las redes y servicios al menos cada dos años y análisis de las prácticas de seguridad de los suministradores. Si a todo esto, le sumamos la obligación de diseñar -por parte de los operadores- estrategias de diversificación de suministradores, se puede ver claramente la **necesidad de integrar la gestión de la seguridad en la gestión del riesgo de terceros** (yendo hacia un enfoque de control y supervisión proactiva).

El objetivo de la gestión de la seguridad sobre terceros es asegurar que los servicios prestados y/o productos prestados cumplen unos niveles de seguridad adecuados, alineados con las expectativas del negocio y minimizando el coste. De este modo, se podrá:

- Gestionar los aspectos de seguridad de los contratos, desde su análisis hasta su terminación / renovación.
- Controlar y disminuir el riesgo asociado a los productos y servicios contratados, a través de cláusulas y medidas de seguridad.
- Evaluar y revisar periódicamente la seguridad de los productos y servicios prestados.
- Mantener un marco de control de seguridad actualizado y una herramienta de gestión que permite automatizar el proceso.

En resumen, la gestión de la seguridad, integrada en la gestión del riesgo de terceros, debe posibilitar la gestión eficiente de los riesgos de terceros, estableciendo un modelo de colaboración entre los diferentes interesados, incluyendo las áreas de seguridad, riesgos, aprovisionamientos, compras, IT, legal y las unidades de negocio.

Conclusión

En el ámbito de las redes 5G, la ciberseguridad pasa a un primer plano por

derecho propio. Todas las capacidades de esta tecnología unido a la mayor preocupación y concienciación con la confidencialidad y la privacidad hacen necesario repensar la visión, las políticas, las arquitecturas, las metodologías, los controles y las medidas de seguridad que venimos utilizando hasta el momento. En este sentido, ya hay mucho trabajo hecho que ha



Los operadores tendrán que diseñar estrategias de diversificación que garanticen la no dependencia de ciertos suministradores y, por consiguiente, la continuidad de negocio. Y estos tendrán que justificar a los operadores y a los gobiernos la fiabilidad técnica y la seguridad de sus productos o servicios (por defecto y desde el diseño), así como su independencia de injerencias externas.

permitido disponer -a día de hoy- de unos buenos pilares para que las expectativas se puedan cumplir. Pero también es cierto, que nos queda el último sprint para acabar de aterrizar adecuadamente algunas cuestiones. Desde nuestro punto de vista, algunas de las consideraciones más significativas en esta etapa final serán las siguientes:

- Como se ha comentado, el enfoque holístico de la ciberseguridad 5G es el único camino posible. Este nuevo mundo digital hiperconectado, hace necesario una buena dosis de *coordinación, gestión y supervisión de todos los actores implicados*. En este sentido tanto los gobiernos como las diferentes organizaciones internacionales en el sector de las telecomunicaciones, deberán seguir liderando para que así sea. Operadores, fabricantes, suministradores y asesores profesionales, deben tener una actitud muy activa en esos foros. Sólo de

esa manera conseguiremos la implantación homogénea del nivel de seguridad.

- Especialmente durante este año, todos los actores involucrados deben *identificar y comprender los requerimientos regulatorios aplicables* (algunos ya están definidos y otros llegarán firmemente en los próximos meses), analizar las posibilidades para aplicarlos y *planificar de forma proactiva su posible implantación*.

- A la hora de diseñar y definir procedimientos, arquitecturas, controles y medidas de seguridad, es importante *aplicar de forma contundente el principio de "seguridad desde el diseño y por defecto"*. Con algunos pilotos de 5G ya desplegados, quizás es conveniente dar un pequeño paso atrás para que los siguientes sean más consistentes. El análisis y la gestión de riesgos previa, vuelve postularse como la mejor herramienta para la aplicación de este principio.

- La integración de la gestión de la seguridad en el proceso de gestión del perfil de riesgo de terceros, será otra prioridad durante este año. Aquí, más allá de las obligaciones asociados a los operadores con sus suministradores (estrategias de diversificación requeridas), habrá que entenderlo como un enfoque más amplio,

siendo recomendable para todos los actores involucrados y considerando el ecosistema de proveedores.

Sin duda, muchos ojos estarán pendientes de cómo evoluciona la implantación de la tecnología 5G. Y viendo la trascendencia justificada que todos le estamos dando, se espera altura de miras de todos los actores involucrados (gobiernos e instituciones, operadores, suministradores y usuarios). Confiamos en que así sea. ■

IGNACIO PÉREZ GARCÍA

Director responsable de BSS para Cataluña y Andorra

ÓSCAR DÍAZ LÓPEZ

Senior Manager BSS

PwC

MVISION Unified Cloud Edge

Seguridad Nativa Cloud para Arquitecturas SASE.

- Visibilidad y Control del Dispositivo a la Nube
- Protección del Dato y Compliance Extremo a Extremo
- Protección Avanzada de la Navegación
- Protección de Entornos Cloud SaaS/PaaS/IaaS

www.mcafee.com/unifiedcloudedge



La convergencia de la CiberSeguridad con las CiberArmas y el nacimiento del “soldado” virtual

En el nuevo entorno hiperconectado por Internet de banda ancha en todos los entornos empresariales, la adopción de la nube, combinada con la llegada del 5G a todos nuestros dispositivos e infraestructuras, nos facilitarán un gran avance en la transformación digital y en la social y económica, sin duda. Este nuevo entorno hiperconectado es nuestra nueva superficie de Defensa, y cada dispositivo conectado se convierte en un elemento al que proteger, y lo que es peor, del que protegerse. En esta tribuna desarrollaremos los nuevos actores que tomarán un papel protagonista en la Ciberdefensa Nacional y, de igual forma, en las técnicas de Ciberataque entre naciones y estados.

CiberSeguridad y Armamento. La nueva realidad

He tenido la oportunidad de participar en la feria de Armamento y Defensa en Abu Dhabi, **IDEX**, hace unas semanas, donde se presentaron las novedades en sistemas de defensa terrestre más innovadoras de todos los países: carros de combate, vehículos blindados ligeros, misiles y todo tipo de armas de ataque y defensa. Nada fuera de lo común para una feria de armamento. Sin embargo, algo era distinto, había algo nuevo, había *stands* de empresas de ciberseguridad, de ciberprotección y defensa, de control de redes, de redes 5G de despliegue rápido en el campo de operaciones, anti-drones y sistemas de inhibición de drones y de destrucción.

Había **Ciberseguridad** en una feria de **armas**, y ¿por qué? Sencillamente, porque el 100 % de las armas tácticas, los sistemas de redes de comunicaciones, abastecimiento, logística, etc., están controladas por sistemas informáticos, lo que los hace vulnerables a un ciberataque. Y mediante un ciberataque se pueden destruir o dirigir hacia el propietario, y eso es mejor que tener la mejor arma, **poder controlar cualquier arma existente mediante un ciberataque**.

Malware: El enemigo y el aliado

El *malware*, virus o programas informáticos maliciosos se han convertido en una prioridad para los Gobiernos en los últimos años. Principalmente se han desarrollado en cuatro categorías de *malware* de defensa que se describen a continuación:

1.- Malware para Botnets. Como primera modalidad importante está la creación de redes de *Botnets*. Todo buen ejército digital debe contar con un número de integrantes lo más alto posible y una capacidad de “fuego” suficiente para derribar las barreras de su enemigo. Así que

diseñar *malware* militar para infectar redes de terceros anónimos en cualquier parte del mundo y estructurarlo para poder usar esos ordenadores contra nuestro enemigo es algo fundamental.

Adicionalmente, Rusia en 2016 desarrolló un nuevo modelo del uso de los *Bots* con fines de desinformación y alteración social, a través del uso de redes sociales de uso masivo como Facebook, Twitter o Instagram, entre otros. Este tipo de campañas son capaces de influir en la población del enemigo, desmoralizándole, creando confusión social, o llegando al punto de cambiar su liderazgo y/o gobierno, como ya concluyó el FBI en su investigación sobre las Elecciones de USA en 2016. (www.bbc.com/mundo/noticias-internacional-54640415).

2.- Malware de espionaje e inventario. Estos programas de ataque son muy comunes en el ámbito de la inteligencia y la defensa, su objetivo es recabar información del enemigo, personas, industrias, infraestructuras, capacidades, etc. Realizan la labor de los antiguos espías, nuestro querido 007 ahora se ha vuelto completamente digital. La clave del éxito de estos programas es no ser detectados, ser invisibles y poder moverse por las redes y sistemas del enemigo. En las versiones avanzadas pueden persistir y reprogramarse remotamente. Algunos ejemplos conocidos son el Octubre Rojo, software desarrollado por el gobierno de Rusia para espiar a las embajadas de occidente durante años. ([https://en.wikipedia.org/wiki/Red_October_\(malware\)](https://en.wikipedia.org/wiki/Red_October_(malware)))

3.- Malware de control e inventario. Este tipo de programas maliciosos son los exploradores del mundo de las ciberarmas. Su objetivo es el de hacer mapas de inventario de

sistemas de control críticos, tales como sistemas de control nuclear, eléctrico, de transporte aéreo, ferroviario, y cualquiera que pueda controlar infraestructuras críticas. Una vez identificado, normalmente se hibernan o se autodestruyen tras enviar la información de topología e inventario requerida.

4.- Malware de ataque a infraestructuras. Esta categoría también son las denominadas “ciberarmas”, serían los misiles de las ciberarmas. Son programas informáticos dirigidos a sortear las defensas del enemigo para inutilizar o destruir infraestructuras críticas de transporte, agua, energía o similares, y si no es posible destruir, bloquear o causar el mayor daño. Este es un *malware* dirigido, diseñado de forma específica para un \$S.OO., programa o sistema. Los objetivos principales son

to de ataque y defensa, autónomo e invisible.

El soldado virtual es un programa malicioso capaz de analizar las defensas del enemigo, reconfigurar su software para infiltrarse, establecer una vía de comunicación con su mando y recibir ordenes. Propagarse de forma dinámica y autónoma en el campo enemigo y ejecutar sus objetivos, bien de inventario, recopilación de información, destrucción o inhabilitación de sistemas e infraestructuras. Y todo esto sin ninguna interacción humana. Autónomo total.

Al igual que las armas controladas por robots e IA, son el siguiente paso en la evolución del armamento militar. Herramientas de un altísimo poder de defensa, ataque y destrucción. Si bien una vez estos nuevos soldados virtuales, o *malware* inteligente de defensa sean liberados, y

Las combinaciones de malware avanzado, con técnicas de ocultación, análisis y distribución de red, junto con IA, son los elementos necesarios para producir la siguiente generación de “malware militar”, el soldado virtual, un software perfecto de ataque y defensa, autónomo e invisible.

sistemas SCADA, sistemas de control y transporte, energía y suministro. Atacando la retaguardia del enemigo y sus sistemas principales de soporte a tropas y civiles. Los más conocidos de estos *malware* son los de la familia Stuxnet y Flame, y su operación más conocida la de la inutilización de los sistemas de enriquecimiento de Uranio de Irán en 2010. (<https://en.wikipedia.org/wiki/Stuxnet>)

Soldado Virtual: Automatización e IA combinados

Las combinaciones de *malware* avanzado, con técnicas de ocultación, análisis y distribución de red, junto con IA, son los elementos necesarios para producir la siguiente generación de *malware* militar, el soldado virtual, un software perfec-

el factor humano quede fuera de la cadena de control, estaremos ante un escenario desconocido e inquietante, la ciberguerra ejecutada por máquinas.

Y en este nuevo escenario de Ciberguerra debemos esperar que sus programadores no se olviden de incluir un botón de desconexión remoto, por lo que pueda pasar. ■



JUAN MIGUEL VELASCO
CEO
AIUKEN CYBERSECURITY

MUCHA INFORMACIÓN
SOBRE AMENAZAS, PERO...
¿ESTÁ PRIORIZANDO LAS
**REALMENTE
IMPORTANTES?**

PODEMOS AYUDARLE.

THREATQUOTIENT 

www.threatq.com



SOPHOS: ciberseguridad potente e intuitiva para una protección efectiva



Ricardo Maté

Sophos en 2021 sigue comprometido en proteger a todo el segmento de empresas, desde pymes con cinco usuarios hasta grandes corporaciones con decenas de miles de usuarios y puestos de trabajo desarrollando productos y servicios muy potentes e intuitivos que proporcionan la ciberseguridad más efectiva para organizaciones de cualquier tamaño.

Cuando en marzo de 2020 empezaron los confinamientos por la Covid-19, las personas y los lugares de trabajo iniciaron una rápida transición sin precedentes que continúa a día de hoy. Es posible que la forma en que trabajamos, vamos a la escuela, asistimos a eventos y conferencias y nos divertimos haya cambiado para siempre, y la informática en la nube es una parte fundamental de esta veloz evolución, pero presenta un gran número de desafíos. Unos permisos de acceso excesivos, una visibilidad limitada de los activos y los recursos en la nube y la falta de auditorías pueden contribuir a crear unos entornos en la nube más vulnerables a las ciberamenazas, y el *malware* es tan perjudicial en la nube como en cualquier otra ubicación. Además, muchas plantillas que teletrabajan desde múltiples ubicaciones han sufrido ataques de, por ejemplo, *ransomware*, en que los delincuentes bloquearon la infraestructura en la nube de la misma forma que atacaban los equipos físicos. A fin de cuentas, el *ransomware* puede cifrar un disco duro o un almacén de objetos virtual con la misma facilidad que un almacén físico. Las empresas cuya infraestructura en la nube sufre un ataque de *ransomware* pueden enfrentarse no solo a la factura de los ciclos consumidos por el cifrado de datos, sino también al pago del rescate o pago por la no publicación de sus datos.

La estrategia de Sophos para 2021 se compone de los siguientes pilares:

- Productos y Servicios líderes: Continuando el desarrollo de nuestros productos como el Endpoint y el Firewall, así como creando servicios de alto valor añadido como Rapid Response y Managed Threat Response.

- Sophos Central: Ofreciendo una protección y su gestión en modo *cloud* nativo. El cliente se debe sólo preocupar de su negocio.

- Plataforma Darwin: Creamos un ecosistema adaptativo y dinámico de Seguridad IT mediante la interconexión de distintos productos con una extensa API, incluso con la posibilidad de fabricantes

terceros, permitiendo que todos los productos hidraten un "lago de datos" del cual obtener información.

- IA y Automatización: Gracias al lago de datos antes comentado y sistemas de IA, poder procesar dichos datos y realizar acciones conjuntas de mitigación entre diversos productos.

- Modelo de negocio y operación sin fricciones.

- Un líder serio en tecnología en ciberseguridad.

- Channel first.

Con estos pilares en mente, Sophos en 2021 sigue comprometido en proteger a todo el segmento de empresas, desde

la empresa ante cualquier potencial amenaza. Para eso hace falta gestionar estas herramientas y ser muy proactivos para detectar estas posibles amenazas. Una gran empresa puede disponer de recursos especializados en ciberseguridad para gestionar los productos y herramientas, pero una pequeña y mediana empresa ni tiene los recursos ni grandes presupuestos para gestionar este entorno.

Teniendo esto en cuenta, nuestras soluciones destacadas este año y las que mayor crecimiento están demostrando son las siguientes:

Sophos EDR/XDR

Nuestro Endpoint, nacido en 1985 ha evolucionado, siendo líder en Gartner en los últimos 11 cuadrantes consecutivos. Si bien empezó siendo un antivirus basado en firmas, a día de hoy es un completo sistema de protección *endpoint* que engloba la protección tradicional (firmas), junto con protección "next-gen" (IA, anti *Exploit*, Comportamiento, anti-*ransomware* y anti-*hacking*) así como protecciones complementarias (control web, control de aplicaciones, cifrado, DLP, etc) y, por supuesto, EDR o, a día de hoy, XDR



pymes con cinco usuarios hasta grandes corporaciones con decenas de miles de usuarios y puestos de trabajo desarrollando productos y servicios muy potentes e intuitivos que proporcionan la ciberseguridad más efectiva para organizaciones de cualquier tamaño.

La ciberdelincuencia está cambiando y los ciberdelincuentes cada vez están más preparados y coordinados entre sí, utilizando herramientas muy sofisticadas y difíciles de detectar y de parar, por lo que ya no basta con tener los mejores productos de ciberseguridad, sino que hay que estar constantemente monitorizando y conocer cuál es la situación de

gracias a la integración cruzada de datos con nuestros *firewalls* y sistemas de protección *cloud*. Por tanto, lo convierte en un producto ideal para personal de Sistemas/IT como de Seguridad. Su gestión se realiza a través de Sophos Central, lo que permite la interacción con otros productos de Sophos y gracias a su API, con cualquier fabricante.

Sophos MTR, MTR-E y Rapid Response

Sophos Managed Threat Response (MTR), es un servicio gestionado de Respuesta frente a Amenazas, que ofrece a



**Pulsamos
la seguridad de
su empresa**

SECunit
by **mdtel**



**Solicite hoy mismo
una demostración
sin compromiso***

Conozca su riesgo y **prepare** su empresa
para recibir Ciberataques

Cuéntenos su caso

 **tenable**
www.tenable.com



*Mínimo 200 activos.

SECunit es la unidad de ciberseguridad de **mdtel**.



las empresas funciones de búsqueda, detección y respuesta ante posibles amenazas las 24 horas del día, 7 días a la semana. Está formado por un equipo de detección de amenazas y expertos en dar respuesta del más alto nivel, capaz de tomar medidas para neutralizar incluso las amenazas más sofisticadas. El factor diferencial de esa solución es que, cuando otros sólo notifican, Sophos puede dar respuesta, sin requerir un licenciamiento adicional, apoyándose en el agente de Sophos para realizar las acciones que el grupo de *Threat Hunting* considere oportunas para la detección y mitigación de la amenaza. Si bien este servicio se apoya sobre el Agente de Sophos, en los casos en los que no sea posible desplegarlo, se proporciona el servicio MTR-E, donde sin importar el sistema de protección desplegado en el cliente, Sophos puede dar este servicio.

Finalmente, si aún no es cliente de Sophos, cualquier empresa que sufra un ataque activo puede recurrir a **Sophos Rapid Response**. En el caso de que una empresa hubiera sido afectada por un ataque, ofrecemos un despliegue de productos y un equipo de expertos que son capaces de ver cuál es la situación dentro de la compañía, detener el ataque, si es posible, y detectar cómo ha venido, a quién ha afectado y limpiar para que pueda operar lo antes posible", comenta el director general de Sophos Iberia

Sophos ZTNA

Zero Trust comienza a sonar cada vez más como estrategia de seguridad y Sophos dispone de un ZTNA para securizar, siguiendo los pilares de nuestra estrategia, las conexiones de usuarios remotos, así como los accesos a servicios en nube. Todo ello gestionado centralizadamente desde Sophos Central, integrándose con el cliente de Seguridad Endpoint para facilitar los despliegues y adopción de las nuevas metodologías de conexión, evitando los problemas "habituales" de los sistemas VPN y SD-WAN tradicionales. El modelo Zero-Trust Network Access permite a los usuarios conectarse de forma sencilla a los recursos corporativos desde cualquier ubicación y al mismo tiempo mejora su seguridad al verificar de manera constante al usuario y validar el esta-



do y el cumplimiento del dispositivo, así como la red desde donde se conecta.

Seguridad Sincronizada

Sophos ha demostrado ser pionero en un concepto disruptivo en ciberseguridad: La sincronización. Muchos otros comienzan hoy a hablar de coordinación entre los sistemas *Endpoint* y los *Firewalls*, pero Sophos lleva ya más de cinco años conectando a través de su Seguridad Sincronizada los distintos sistemas de protección, compartiendo información. Si bien en su comienzo el punto final reportaba su es-



tado de salud al *firewall*, a día de hoy se extiende a todo el portafolio, así como la obtención de información avanzada para poder realizar acciones coordinadas. Nuestro proyecto Darwin, junto con la automatización y Sophos Central hacen posible nuestra seguridad sincronizada.

Sophos Cloud Optim

Conscientes de que el IT está migrando a la nube, Sophos fue uno de los primeros fabricantes mayoritarios en hablar de CSWP y CSPM gracias tanto al agente para servidores como a Cloud Optim, el cual audita los recursos que tengamos sobre proveedores de nube pública como AWS, Azure o Google Cloud, así como Kubernetes tanto en cualquiera de estos entornos como locales. Además, se integra tanto con la protección de instancias y servicios como MTR, lo que proporciona más visibilidad e información que será recogida en el DataLake antes comentado.

Sophos Firewall

La seguridad de red no queda desatendida en Sophos. Desde la compra de Astaro en 2008, los hemos seguido evolucionando hasta llegar a los modernos Sophos Firewall, gestionados de forma centralizada desde Sophos Central, integrándose con el Endpoint y servicios como MTR así como hidratando el lago de datos para permitir detectar, englobándose dentro de nuestra estrategia XDR.

Canal y MSP

El programa global de *partners* de Sophos está basado en tres pilares fundamentales de nuestro compromiso: rentabilidad, asociación y producto y está diseñado para adaptarse a las necesidades únicas de los distribuidores, proveedores de servicios administrados y expertos en ciberseguridad de última generación. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53.000 *partners* y proveedores de servicios gestionados.

Con un proveedor, un programa y un catálogo de soluciones de seguridad, nuestros *partners* pueden ofrecer a sus clientes una protección completa y probada que se gestiona desde una sola plataforma de administración. Se lo ponemos muy fácil a la hora de desplegar, gestionar y vender nuevos servicios de seguridad, lo que contribuirá a que crezcan sus ingresos y disminuyan sus costes.

Sophos combina los elementos necesarios de un entorno de seguridad por capas en una plataforma de fácil navegación que ofrece a nuestros *partners* visibilidad y protección escalable. Estas capas combinadas de seguridad dentro de Sophos Central también se sincronizan para compartir información entre productos a fin de detener las amenazas en tiempo real, convirtiéndolo en uno de los sistemas de ciberseguridad más eficaces y completos. Añadir el servicio Sophos Managed Threat Response a la pila tecnológica incrementan su oferta de seguridad como MSP y aporta a los MSP de cualquier tamaño la tranquilidad de un centro de operaciones de seguridad (SOC) de confianza. ■

RICARDO MATÉ
Director General
SOPHOS IBERIA

¿Si hubiera sabido que iba a pasar,
habría actuado de forma distinta?
Aún está a tiempo de hacerlo.

Sothis, Seguridad de la Información.

Gobierno de la Seguridad de la Información



Análisis de riesgos



Plan de tratamiento de riesgos



KPIs & KRIs



Metodología by Sothis



Plan director de seguridad



Oficina de seguridad



DPO as a service



CISO as a service



Cultura de seguridad

Ciberseguridad



Monitorización amenazas 24x7



Respuesta a incidentes



Arquitecturas de protección



Inteligencia de amenazas



Formación y concienciación



Análisis forense digital



Auditorías y red team



ISO 27001, ENS, NIST, LEY PIC...



Plan de continuidad TIC



Protección de datos



Clasificar información



Securitización de entorno industrial

A man with glasses and a dark jacket over a light blue shirt stands with his arms crossed in a server room. The background is filled with server racks and blue ambient lighting.

“ESET proporciona información sobre amenazas actualizada y comprensible para que pueda ser usada en operaciones de desmantelamiento de actividades delictivas”

Josep Albors

Director de Investigación y Concienciación de ESET España

> Por José Manuel Vera
> Fotografía: Eset y Jesús A. de Lucas

Desde joven, la tecnología, los videojuegos y, también la seguridad, han acaparado gran parte del tiempo de Josep Albors, Director de Investigación y Concienciación en España de la multinacional europea ESET, a la que llegó en 2005. Ocupado y preocupado por la creciente amenaza que supone el desbocado incremento de ataques —sobre todo con “ransomware por las consecuencias económicas tan negativas que puede llegar a tener en las empresas”—, su ‘expertise’ le aporta la mejor visibilidad para escudriñar lo que ocurre en la parte más oscura del ciberespacio y constatar cómo tecnologías como las desarrolladas por la firma eslovaca contribuyen a que el mundo sea más ciberseguro. Este hecho fue ya reconocido por esta revista, que destacó la labor de la empresa en 2017 otorgándole uno de sus Premios SIC anuales.

– ESET comenzó hace 30 años inspirando su nombre en una diosa egipcia (Isis, denominación griega de Ast). ¿Cómo han evolucionado? La atribución es uno de los grandes retos de la ciberseguridad...

– Nuestra función es la de proporcionar una información sobre amenazas actualizada y comprensible para que pueda ser usada en operaciones de desmantelamiento de actividades delictivas, siendo ese el motivo por el cual colaboramos

desde hace años con empresas y organismos oficiales. Hacer atribuciones alegremente, basándose únicamente en algunos indicadores de compromiso o líneas de código es algo arriesgado y, por eso, desde Eset preferimos dejar ese trabajo a las fuerzas de seguridad y organismos responsables de velar por nuestra seguridad.

– Actualmente, cuentan con más 110 millones de usuarios y 400.000 clientes corporativos en 200 países. ¿Qué marca la diferencia con la competencia?

– Somos la mayor empresa de ciberseguridad de la Unión Europea y destacamos por nuestro conocimiento sobre las amenazas y las tendencias del cibercrimen. Con equipos de investigadores en todo el mundo es posible identificar tanto amenazas globales como las dirigidas a objetivos concretos en una región específica. Esto nos permite ofrecer soluciones de seguridad muy efectivas sin consumir excesivos recursos en los sistemas en los que se instalan.

– ¿Cuál es su mercado actualmente en España y qué expectativas de crecimiento hay para 2021?

– Nuestro mercado lo conforman principalmente empresas, aunque tenemos un número importante de clientes que utilizan nuestras soluciones para el hogar. En cuanto a expectativas para este 2021, debido a la pandemia y al periodo de incertidumbre que estamos viviendo, nos hemos centrado en escuchar a nuestros clientes y distribuidores –contamos con una red de más de 5.900 *partners*–, para conocer sus necesidades e intentar ayudarlos en todo lo que nos sea posible. Por ejemplo, el año pasado lanzamos una campaña para nuestros clientes mejorándoles la protección de forma gratuita mientras pasábamos los meses más duros de la pandemia, proporcionamos de manera altruista nuestra herramienta de inteligencia de amenazas a los CERTs más importantes de España y participamos conjuntamente con el CNI para proporcionar licencias gratis a empresas de sectores críticos que lo necesitaran, y si este año la situación empeora, seguiremos en este camino de intentar ayudar en todo lo que podamos.

– En el ámbito de la ciberprotección corporativa, ¿cuál es el área en la que más invierten?

– El aumento de los riesgos y la profesionalización de los ciberdelincuentes provocan que mejoremos nuestras soluciones a diario, para intentar ofrecer siempre la mejor seguridad a nuestros clientes sin afectar al rendimiento. La protección para *endpoint* y servidores es, sin duda, donde más invertimos. Nuestro reto, desde nuestros orígenes, es ofrecer un producto eficaz y potente, sin mermar el funcionamiento de los equipos.

– Y la innovación de la que están más orgullosos...

– Nuestro EDR avanzado, Eset Enterprise Inspector, una solución muy sofisticada de detección y respuesta ante incidentes que permite monitorizar de forma integral, continua y a tiempo real toda la actividad de los equipos, además de tener la capacidad de analizar procesos sospechosos para ofrecer una respuesta inmediata. Además, permite detectar amenazas persistentes avanzadas (APTs), descubrir y detener ataques sin archivos, bloquear amenazas de tipo '0-day' y *ransomware*, entre otras. Esta herramienta, junto con los servicios ofrecidos desde Eset España, nos permite proporcionar a nuestros usuarios la tranquilidad de poder realizar sus tareas diarias sin preocupaciones.

– Honda, Mitsubishi Motors, Allianz Suisse, Greenpeace, Canon o T-Systems son algunos de sus grandes referencias

internacionales... ¿Cuáles son los más significativos en España?

– Sí, y también contamos con otros como Google a la que proporcionamos nuestra tecnología para proteger, por ejemplo, a sus usuarios de Google Chrome o de Google Play Store. Aquí, en España, contamos con clientes muy significativos casi en todos los sectores y, también, en la Administración Pública, desde entidades locales a ministerios que confían su ciberseguridad en Eset. Pero por citar a algunos, trabajamos con ayuntamientos como el de Valencia o Vigo, con universidades como las de Vigo o León, así como con la Federación Española de Baloncesto, Hissense o la cadena Spar, entre



“Cuando se trata de amenazas complejas contra objetivos específicos, el factor humano del analista de *malware* resulta crucial, ya que su experiencia y capacidad no es equiparable a ningún sistema de estas características”.

otras entidades. Hay bastantes más, aunque no podemos dar muchos más nombres por temas de confidencialidad.

– ¿Qué es lo que más demandan vuestros clientes en España?

– Sobre todo, cuatro aspectos: compatibilidad con sus sistemas, eficiencia en la detección de ataques, que consuma pocos recursos y un buen servicio. Desde Eset estamos orgullosos de la valoración que dan nuestros clientes tanto a las diferentes soluciones como a los servicios de ciberseguridad que prestamos, y esto es gracias a todo el trabajo realizado desde que comenzamos hace tres décadas, siempre centrados únicamente en la protección de usuarios y empresas de todo el mundo.

– ¿En qué ha cambiado el enfoque de Eset con la pandemia y la popularización del teletrabajo?

– Con el incremento del trabajo en remoto también han aumentado cierto tipo de ataques relacionados con las conexiones remotas. Sirva como ejemplo, que entre el primer trimestre y el último de 2020, encontramos un crecimiento del 768% en intentos de ataque al Protocolo de Escri-

torio Remoto (RDP). Por ese motivo, desde Eset nos hemos centrado en concienciar a los usuarios y empresas para que puedan seguir trabajando desde cualquier lugar de forma segura, estando al tanto de las amenazas existentes, su evolución y como contrarrestarlas con nuestro catálogo de soluciones.

– Como responsable de Laboratorio, en un momento donde la automatización está en crecimiento –cuenta con un motor propio de aprendizaje automático (Eset Augur)–, ¿qué valor tiene la persona en ciberseguridad?

– Todo lo relacionado con el aprendizaje automático va muy bien para automatizar procesos, pero cuando se trata de complejas amenazas contra objetivos específicos, el factor humano del analista de *malware* resulta crucial, ya que su experiencia y capacidad no es equiparable a ningún sistema de estas características.

– Un aspecto más desconocido en el mundo corporativo quizá sea la labor que realizan desde los laboratorios de investigación... ¿Qué valor tienen para ser proactivos?

– La investigación es fundamental para

adelantarse o detectar campañas de *malware* en sus fases iniciales. Mediante la monitorización de indicadores de compromiso y el análisis de muestras recientes se pueden observar cambios o tendencias para la detección prematura de otras amenazas o de nuevas campañas de propagación de software malicioso, ayudando a mitigar sus consecuencias o bloquearlas por completo.

– **¿Por qué fracasa la industria de la ciberprotección, incapaz de encontrar una fórmula consistente para frenar en seco al *ransomware*, recayendo la responsabilidad en última instancia en el usuario y en su ‘dedo’ desatador de la infección?**

– Hablar de fracaso no sería lo adecuado cuando ahora disponemos de soluciones capaces de detectar estas amenazas de forma efectiva e, incluso, antes de que lleguen a causar un daño irreparable. Otra cosa es que estas medidas de seguridad no se configuren y utilicen de forma adecuada e intervengan otros factores como la falta de concienciación y de adopción de medidas básicas de seguridad que solo dificultan el trabajo de estas soluciones.

– **Han participado en varias acciones notables como la Operación Stealthy-Trident o la SignSight del grupo Lázarus, que al igual que el mediático caso**

complejos o en los más cotidianos.

– **También, se centran en proteger la Unified Extensible Firmware Interface (UEFI), antes conocida como BIOS... ¿Qué aporta?**

– Seguridad frente a un tipo de amenazas concretas que tienen como objetivo principal infectar y modificar estas UEFI para conseguir persistencia y tratar de dificultar su detección. En los últimos años, hemos descubierto ataques de este estilo y es una tendencia que se extenderá, cada vez más, por las posibilidades que ofre-



“No basta con instalar las soluciones de seguridad en las diferentes capas previamente establecidas, además se deben monitorizar por personal especializado y configurar de forma adecuada para que resulten efectivas”.

SolarWinds aprovechaban fallos en cadena de suministro... ¿Qué importancia tiene la inteligencia de amenazas a través de sistemas como su LiveGrid?

– La inteligencia sobre amenazas es un pilar básico a la hora de detectar todo tipo de ataques, no solo los más avanzados. Respecto a qué puede haber fallado cuando se descubre un ataque como el de SolarWinds, hay que tener en cuenta que no basta con instalar las soluciones de seguridad en las diferentes capas previamente establecidas, sino que además se deben monitorizar por personal especializado y configurar de forma adecuada para que resulten efectivas. De hecho, seguimos viendo fallos en medidas de seguridad básicas como la autenticación de los usuarios, la gestión de permisos o la segmentación de redes, algo que los atacantes no dudan en aprovechar para conseguir su objetivo, ya sea en ataques

ce a los atacantes de pasar desapercibidos en un sistema infectado durante largos periodos de tiempo.

– **En el último lustro firmaron varias alianzas: con Xopero, para recuperación de información; con Safetica para evitar fugas de datos... ¿continuarán las alianzas en 2021?**

– Sí, nos hemos centrado en cubrir las necesidades de protección de nuestros clientes, con doble autenticación a través de Eset Secure Authentication, con cifrado, *backup*, DLP, etc. Asimismo, el año pasado lanzamos la solución Cloud Office Security, de servicio (SaaS) que ofrece protección preventiva avanzada para los usuarios de las aplicaciones de Microsoft 365, además de lanzar las soluciones de protección avanzada como nuestra *sandbox* en la nube llamada Dynamic Threat Defense y nuestro EDR, Enterprise Inspector.

– **¿Qué capacidades novedosas son su prioridad de cara a 2021?**

– Nuestro objetivo es seguir incorporando novedades en estas soluciones que hemos comentado y centrarnos en ofrecer servicios de seguridad en la nube.

– **Como responsable de concienciación, ¿Qué hace falta para que el talento patrio tenga más recorrido? ¿Y para crear más empresas de proyección internacional?**

– Algo tan sencillo como valorar adecuadamente el talento patrio. Ya sería un gran avance ofrecer salarios y condiciones laborales adecuadas, involucrándose también en la formación de los futuros profesionales como ya hacemos en Eset en varios países, incluyendo España. Recientemente, hemos visto como Google ha apostado por Málaga para establecer su nuevo centro de ciberseguridad, reconociendo el talento existente. Si esto se hace bien, las empresas exitosas y con proyección internacional vendrán.

Sin embargo, observamos de forma casi continua declaraciones quejándose de una supuesta falta de talento cuando lo que realmente se está pidiendo es gente altamente formada (incluso en perfiles *junior*) a cambio de condiciones laborales manifiestamente mejorables. Esto explicaría la dificultad que tienen muchas empresas españolas para atraer talento en ciberseguridad extranjero y, cómo gracias al auge del teletrabajo, son

cada vez más los que optan por hacerlo en compañías de fuera pero quedándose a vivir en España.

– **Colabora, a través de Eset, con diferentes foros internacionales como el Grupo de Asesores sobre Seguridad en Internet de Europol o Google Chrome, ¿Qué se echa de menos en España que se hace en otros países?**

– Sin duda un mayor número de recursos asignados a la ciberseguridad. Hay talento de sobra tanto en empresas privadas y organismos públicos como en cuerpos y fuerzas de seguridad del Estado, pero la mayoría de las veces no se cuenta con los recursos necesarios para desempeñar su labor de la forma adecuada. Si se dejase de ver la ciberseguridad como un gasto y se considerase una inversión que puede evitar una quiebra de la empresa tras sufrir un ciberataque, otro gallo nos cantaría... ■

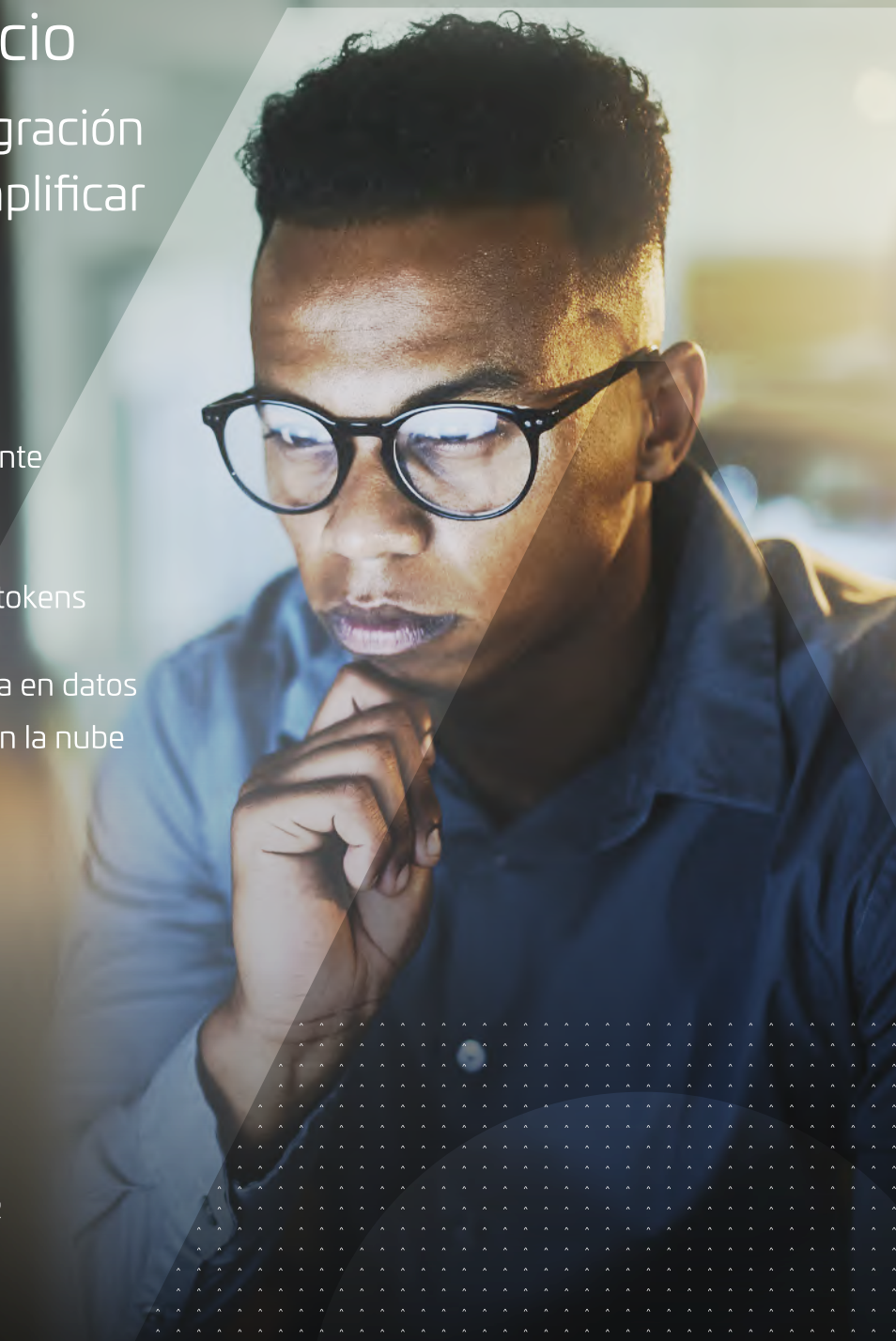


SafeNet Trusted Access

Gestión de accesos en la nube como servicio

Prevenir brechas / Migración segura a la nube / Simplificar el cumplimiento

- Smart Single Sign-On
- Motor de políticas flexible y potente
- Mitiga riesgos con métodos de autenticación universales
- Gestión y aprovisionamiento de tokens automatizados
- Informes con información basada en datos
- Soporta las aplicaciones web y en la nube que utilizas



cpl.thalesgroup.com

Ajoomal Asociados
Your Security. Our Responsibility

Contacta con nosotros: +34 91 382 17 10
www.ajoomal.com \ comercial@ajoomal.com

PenTera o cómo validar la postura de Ciberseguridad y el Nivel de Riesgo de forma automática, continua y consistente

PenTera de Pcysys ayuda a los equipos de Red Team a automatizar las tareas más repetitivas, más tediosas y más automáticas para poder realizar esos ejercicios en mucho menor tiempo y que el Pen Tester se centre en ataques más complejos, en situaciones más complicadas donde podrá aportar mucho más valor a la empresa. Así mismo PenTera ofrece unos Reports Automáticos siempre con los mismos parámetros para que la organización conozca cómo evoluciona su postura de seguridad en el tiempo, priorizando la Remediación en función de la criticidad de las vulnerabilidades en esa Red en concreto, ahorrando tiempo y recursos en el proceso de Remediación y cerrando las Brechas de Seguridad para evitar el objetivo final, la fuga de información.

Han pasado poco más de cinco años desde que en noviembre de 2015 el fundador y CTO de **Pcysys** (Proactive Cyber Systems) y líder del equipo de Red Teaming del Ejército Israelí, **Arik Liberzon** tuviera la visión de que el software, si se diseñaba de forma inteligente y segura, podría hacer un trabajo mucho mejor de Pen Testing que el realizado manualmente. Desde entonces, más de 200 clientes en todo el mundo, y la propia Gartner, han refrendado su visión, convirtiendo a PenTera en la primera solución mundial de Análisis de Riesgo y validación de la postura de ciberseguridad de las empresas de forma continua y consistente gracias a la automatización del *Pen Testing* desde la perspectiva y conocimientos de un ciberdelincuente.

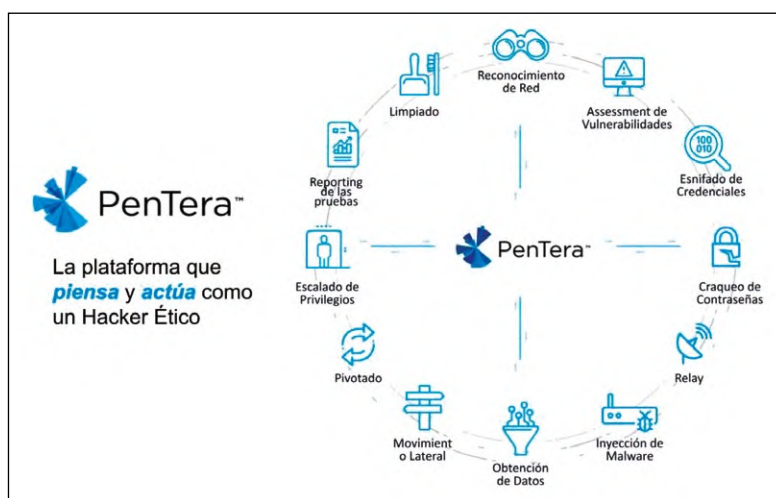
El reto al que se enfrentan las empresas hoy en día es conocer su nivel de exposición al riesgo antes de que sea demasiado tarde, antes de sufrir una brecha de seguridad. No es suficiente una gestión tradicional de Vulnerabilidades, con una lista interminable de CVSS basados en un *score* general que no sabemos qué consecuencias tiene para nuestra empresa, o si se podrán explotar o no dentro de nuestro entorno. Por otro lado, herramientas tipo BAS (*Breach and Attack Simulation*), como su propio nombre indica, realizan simulaciones, no ataques reales, y extrapolan los resultados al resto de la red.

Mientras tanto, ¿qué haría un atacante real?

Un atacante real permanece en silencio en la red mientras reconoce los activos y busca las vulnerabilidades que realmente sean explotables en ese entorno en concreto. Un ciberdelincuente suele utilizar en muchas ocasiones vulnerabilidades NO críticas pero que aún así le ofrecen un

alto beneficio al explotarlas, ya que justamente al no ser críticas, están en menor prioridad en el proceso de remediación. Además, esnifa credenciales que cruzan la red, las *crackea*, las utiliza en otras máquinas, pivota, se mueve lateralmente, escala privilegios, trata de infiltrar malware que le permita nuevas acciones, todo ello con el objetivo de exfiltrar la información deseada.

Eso es exactamente lo que realiza **PenTera** de forma Automática y Continua. Sin desplegar ningún agente en la Red, simplemente conectando



la máquina que albergue PenTera a un punto de red, podremos realizar escenarios de ataque tipo:

- **Black Box**, donde no proporcionamos ninguna información a la Plataforma.
- **Grey Box**, donde podremos incorporar información, como unas credenciales, un nombre de fichero, una dirección a atacar, etc.
- **Ataques dirigidos.**
- **Análisis del Active Directory** para comprobar cómo de fuertes son las contraseñas existentes, incluso aunque cumplan con la política corporativa.
- **Análisis de Vulnerabilidades** basado en los CVSS tradicionales.
- **Búsqueda de una Vulnerabilidad** conocida para saber si el proceso de Remediación ha sido realizado correctamente en toda la Red.

Y todo ello configurando además el **Nivel de Ruido** con el que queremos realizar el ataque. Desde una enumeración total con un nivel de descubrimiento ruidoso hasta una enumeración muy ligera con un nivel de descubrimiento extra silencioso... ¿Por qué?

Porque es la única forma de comprobar si los mecanismos de Seguridad existentes se están comportando como esperamos se comporten.

¿Cuándo saltan las alarmas en mi EPP? ¿Me está detectando el NDR cuando realizo un ataque? ¿Los *firewalls* están protegiendo correctamente? ¿Están llegando las alertas a mi SIEM? ¿Está respondiendo en tiempo y forma mi SOC?

¿Por qué es tan importante el concepto de Continuidad y Consistencia?

Todos somos conscientes de que las Redes están 'vivas'. Los usuarios transmiten información con mayor o menor protección, existen fallos humanos, se añaden nuevos equipos a la red cada día que amplían la superficie de ataque, aparecen nuevas vulnerabilidades, existen requerimientos regulatorios que solicitan una prueba permanente de los sistemas de Seguridad...

Por eso un **Pen Testing anual**, quizás dos en los mejores casos, **no es suficiente**.

De esta forma tendremos una foto puntual en el tiempo, y posiblemente de un escenario no completo de la Red, ya que en muchas ocasiones, al ser un Proyecto limitado en el tiempo, el Pen Tester tratará de lograr el mayor logro aprovechando una brecha... pero ¿podrá replicar esas mismas Técnicas, Tácticas y Procedimientos en toda la Red en el tiempo que dura el proyecto?

PenTera de Pcysys ayuda a los equipos de Red Team a automatizar las tareas más repetitivas, más tediosas y más automáticas para poder realizar esos ejercicios en **mucho menor tiempo** y que el Pen Tester se centre en ataques más complejos, en situaciones más complicadas donde podrá aportar mucho más valor a la empresa.

Así mismo PenTera ofrece unos Reports Automáticos siempre con los mismos parámetros para que la organización conozca **cómo evoluciona su postura de seguridad en el tiempo, priorizando la Remediación en función de la criticidad de las vulnerabilidades** en esa Red en concreto, ahorrando tiempo y recursos en el proceso de Remediación y cerrando las Brechas de Seguridad para evitar el objetivo final, la fuga de información. ■

RAÚL GORDILLO
Regional Sales Manager – Iberia
PCYSYS



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

ThreatQ, plataforma de inteligencia sobre amenazas abierta para acelerar las operaciones de ciberseguridad

La plataforma ThreatQ, de la compañía ThreatQuotient, ha irrumpido con fuerza en el mercado. Está específicamente orientada a optimizar las operaciones de ciberseguridad centradas en las amenazas, y muy especialmente diseñada para paliar las dificultades que plantea a los SOC's y CSIRT's la toma de decisiones en base a informaciones proporcionadas por los sistemas de ciberseguridad y fuentes externas, proporcionando una mejora en la orquestación y automatización de la gestión de riesgos de ciberseguridad. En consecuencia, ayuda en el proceso de inteligencia, reduciendo la carga de trabajo no productivo, aumenta la eficiencia y la eficacia de la operación y reduce costes.

Como un experto en seguridad dijo “**prevé lo que puedas, detecta lo que no puedas prevenir y caza lo que no puedas detectar**”. Y para hacer esto, actualmente contamos con la ayuda de diferentes fuentes de inteligencia: 1) **Inteligencia de los productos de seguridad** (ayuda a prevenir la mayoría de los ataques más conocidos); 2) **Inteligencia Externa** (da información de Adversarios, Técnicas, Herramientas y Procesos que usan, objetivos, etc., y nos brinda esa visión más estratégica que los productos de seguridad no cubren, además de ayudar a anticiparnos); y 3) **Inteligencia Interna**, la parte más importante, quizás. (Es toda la información que recolectamos de la detección que hacemos con nuestros sistemas, SIEM, etc.).

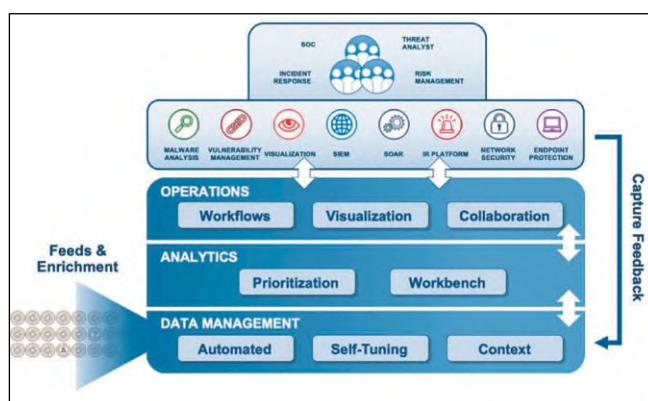
La plataforma ThreatQ le centra en automatizar la ingestión, correlación, normalización, contextualización y priorización de estas fuentes para decidir qué es realmente importante y así **convertir esta cantidad de datos en Inteligencia actuable**. Esto último es esencial, ya que la plataforma también **automatiza la diseminación de esta inteligencia en los sistemas de protección** de la compañía (NGFW, EDR's, DNS, Email, etc.) de forma que, independientemente de la Inteligencia que tengan definida por el fabricante, se pueda asegurar la detección de las amenazas relevantes.

ThreatQ también permite que la información esté visible para las personas que participan en las labores de Ciberseguridad, de forma que cada vez que alguna de ellas —o proceso— cambie o enriquezca la información, automáticamente se harán visibles dichos cambios en el resto de la organización. La Threat Intelligence Platform (TIP), se pone en el centro de la tecnología, personas y procesos, haciendo que la información fluya entre ellos y convirtiéndose en la “**fente de la verdad**” sobre las amenazas importantes para la empresa. Además, provee de mecanismos para automatizar procesos en base a datos (“**Data Driven SOAR**”, esto es automatización que aprende y mejora con cada iteración).

Cada euro invertido en la plataforma TIP, retor-

na muchos euros en el resto de las operaciones de seguridad, en:

- **Gestión de Vulnerabilidades**, priorizando y siendo proactivo con el parcheo de vulnerabilidades que sabemos que nos pueden afectar más teniendo en cuenta todo el contexto, no solo la criticidad genérica que indica el fabricante.
- **Gestión de políticas de seguridad**, permitiendo automatizar en la plataforma la actualización de los elementos de protección de forma inteligente y proactiva.



• **Gestión del SIEM**, reduciendo la cantidad de información a correlar y priorizando las amenazas críticas. De esta forma se es más eficaz y se reducen radicalmente los falsos positivos.

• **SOAR**. Un SOAR ejecuta *playbooks*, tareas repetitivas y si ejecuta tareas sobre información no relevante, el ruido en la empresa (*tickets* abiertos, alertas escaladas, etc...) se amplifica. Con lo que el SOAR sin inteligencia, pierde mucha efectividad. En este caso Gartner ya posiciona el SOAR como la unión de la automatización con una plataforma de Inteligencia que de foco y sentido a esta automatización. **La plataforma TIP pasa a ser parte indispensable del SOAR.**

El TIP permite dar el salto hacia la anticipación (sin inteligencia las operaciones del SOC son siempre reactivas). Y si se enfocan las ventajas desde otra perspectiva, se observa que su uso trae ventajas y ROI en las siguientes áreas: **Mayor ratio de bloqueo de ataques, mayor eficiencia operacional y mejor planificación.**

Plataforma ThreatQ

ThreatQ actúa como una plataforma de inteligencia sobre amenazas abierta, que acelera las operaciones de seguridad. Los componentes integrados y autoajustables (Threat Library, Adaptive Workbench, ThreatQ Investigations y Open Exchange) permiten comprender rápidamente las amenazas, tomar decisiones y acelerar la detección y la respuesta. Integra información de toda fuente de amenazas, Personas que necesitan y actúan sobre esa información (CIO, CISO, Incident Responders, SOC Managers), Procesos (VA, IR, TH, etc...) y Tecnologías (SIEM, NGFW, Helpdesk, etc.); prioriza amenazas en función de todo el contexto en tiempo real; automatiza procesos y tareas basándose en Datos; y colabora al hacer accesible la información a las personas, procesos y tecnología, de forma dinámica.

Módulos

1. THREAT LIBRARY. El repositorio de inteligencia contextualizada y compartida entre sistemas, personas y procesos. Esta biblioteca de amenazas puntúa y prioriza automáticamente la inteligencia en función de los parámetros que se definan. La priorización se calcula al relacionar muchas fuentes distintas, tanto externas como internas, para ofrecer mediante el contexto acumulado una única fuente de verdad. De esta forma, se eliminan los resultados irrelevantes y se reduce el riesgo de falsos positivos.

2. ADAPTIVE WORKBENCH: es una combinación de automatización e inteligencia humana, que permite articular una detección y respuestas proactivas. El flujo de trabajo personalizable y el enriquecimiento facilita optimizar el análisis de los datos y eventos de las amenazas con el fin de agilizar la investigación y la automatización del ciclo de vida de la inteligencia.

3. OPEN EXCHANGE. Arquitectura abierta y ampliable para tener un ecosistema robusto. Importa y agrega fuentes de datos externos e internos, integra la información con herramientas de enriquecimiento y análisis existentes, y exporta la inteligencia adecuada a las herramientas apropiadas, en el momento justo, para acelerar la detección y la respuesta.

4. THREATQ INVESTIGATIONS, la primera sala de análisis de ciberseguridad del sector. ThreatQ Investigations resuelve el problema de la descoordinación y las ineficiencias en las operaciones de seguridad con el fin de acelerar la detección y la respuesta. Esta solución optimiza las investigaciones y mejora la colaboración activa entre los equipos. ■

EUTIMIO FERNÁNDEZ

Regional Sales Manager – Spain & Portugal
THREATQUOTIENT

Su fuerza laboral ahora es remota. Mantengamos su negocio a salvo.

Aseguremos sus
correos electrónicos,
datos, redes y
aplicaciones.

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

 **Barracuda**
Your journey, secured.

Los EDR, XDR y MDR... y la búsqueda del Santo Grial

Sin la pretensión de entrar en la antropología de la profesión, les tengo que hacer una confesión: he observado a varios compañeros que trabajan en la ciberseguridad y creo que muchos de ellos se sienten como los caballeros de una nueva orden que viven para luchar contra el mal, ahora el ciber-mal. E, igual que los Caballeros de la Mesa Redonda, estamos todos en búsqueda de un Santo Grial –la seguridad completa–, que pueda con todo: con el *ransomware* dirigido y los atacantes avanzados, con las APT y la ingeniería social a la vez, dejando nuestras infraestructuras pulcras y nuestros datos intocables. Todo esto no es noticia, estoy convencido que usted lector lo ha observado también; la noticia es que creo que este Santo Grial existe y está a su alcance, y voy a mostrarles aquí un mapa para conseguirlo. En Bitdefender nos esforzamos mucho para poder acompañarle en cada una y en todas estas etapas del camino hacia el Santo Grial de la ciberseguridad.

“Un viaje de mil millas comienza con el primer paso” dijo el sabio chino y en el camino hacia la ciberseguridad creo que muchos ya hemos dado este paso: no creo que haya probablemente en España una sola organización que no tenga alguna medida básica de protección, un antivirus, un cortafuego, o un *Gateway* de seguridad. A lo mejor hablamos de alguna solución un poco más avanzada, como un antivirus de nueva generación, o una solución que incorpore *Machine Learning* para poder protegerse frente a los códigos desconocidos. Y si a la tecnología le hemos añadido algunas buenas prácticas y procesos, creo que ya tenemos la primera parte del viaje cubierta.

El siguiente tramo –el más difícil– es darse cuenta de que este primer nivel no es suficiente porque nos enfrentamos a amenazas más complejas y a atacantes fuertes. Los últimos años han puesto en evidencia muchas debilidades de “los castillos grandes”, incidentes donde la protección no ha resistido ante el *ransomware* dirigido o ante los ataques avanzados. Así que llegamos a entender que se necesita algo más junto a las tecnologías de protección / prevención, algo que actúe de otra manera, en el ámbito de la detección y respuesta. Hablamos de la necesidad de identificar si hay un ataque en desarrollo a través de síntomas –indicadores de compromiso (IoC) y de ataque (IoA)– o de técnicas, tácticas y procedimientos (TTPs) específicos. Y luego de la posibilidad de visualizar, identificar quién te ataca, cómo y con qué, para extraer la causa raíz y dar la respuesta adecuada. Y después remediar los daños y aprender de la incidencia. Como ya muchos se habrán dado cuenta, estoy hablando de las tecnologías de *Endpoint Detection and Response* (EDR).

A medida que avanzamos por el camino, nos damos cuenta de que a lo mejor se necesita más información. O de que si esperamos obtener más seguridad por la integración de nuestro EDR con un SIEM o SOAR a lo mejor los resultados no llegan a ser los deseados porque lo que ganamos en con-

texto, lo perdemos en tiempo de reacción –que es esencial hoy en día, cuando en término de horas un atacante te puede cifrar o robar los datos críticos. Y entonces aparece la necesidad de tener e integrar inteligencia de ciberseguridad a varios niveles (*endpoints*, red, nube, usuarios, *e-mail*, móviles, IoT etc.) en una plataforma unificada de analíticas y gestión de la seguridad, una XDR (XDR –eXtended Detection and Response–, acompañada por un equipo de analistas expertos agrupados en un *Security Operations Center* (SOC) como los caballeros alrededor de la Mesa Redonda.



Llegados en este punto, nos damos cuenta de que ya hemos avanzado bastante y podemos entender mejor el reto; probablemente hayamos librado muchas batallas, algunas perdidas, algunas ganadas, pero lo más importante es aprender de todas estas experiencias y darse cuenta de sus límites. Como en cualquier ámbito, a medida que profundiza, uno se da cuenta de lo mucho que no llega a saber, por varios motivos: no todos se permiten tener un SOC con personal experto, o no lo tienen 24/7, o incluido si lo tienen se dan cuenta de que hay puntos que no cubren como puede ser el análisis de códigos, o entender algunos indicadores muy especializados (por ejemplo, incrementos extraños de los IOPS para algunas instancias en la nube, o crecimiento del tráfico entre unas máquinas virtuales...). Es el momento en el cual un caballero piensa que a lo mejor no le vendría mal un acompañante por el camino. Y por suerte se pueden encontrar tales acompañantes: los proveedores de servicios de *Managed Detection and Response* (MDR). Ellos aportan la experiencia y

el conocimiento de los expertos que han estado en la primera línea de la lucha durante muchos años, pero también aportan la perspectiva externa, intentando detectar ataques avanzados por señales que a lo mejor sus analistas o sus tecnologías no hayan detectado o no hayan puesto en evidencia.

Están haciendo esto identificando sus activos críticos (las joyas de la corona), construyendo escenarios de ataques y buscando rastros de que la imaginación coincida con la realidad –servicio de *Threat Hunting* (o buscando información privilegiada en la *Dark Web* para confirmarle si está o va a devenir blanco de un ataque dirigido.) Son servicios de alto valor añadido que pueden acompañar las tecnologías, los procesos y los equipos internos dedicados a la ciberseguridad.

Como hemos visto, el camino es largo y muchas veces empinado... y en un final el caballero llega a entender que el Santo Grial es algo que ya tenía y lo ha tenido al alcance durante todo el camino. Porque en la ciberseguridad el Santo Grial es la actitud de estar siempre en alerta y siempre abierto a aprender. Es el empeño de encontrar recursos financieros y humanos para luchar con los ciberdelincuentes. Es la conciencia de que necesitas buscar aliados que cumplan con tus expectativas, acompañantes de confianza durante este viaje.

En Bitdefender nos esforzamos mucho para poder acompañarle en cada una y en todas estas etapas del camino hacia el Santo Grial de la ciberseguridad:

- Para los que buscan una solución fácil de implementar y gestionar, enfocada a la prevención, basada en *Machine Learning* y una estructura resiliente de más de 36 capas de protección, nos enorgullece seguir proporcionando nuestra galardona-da gama Endpoint Protection.
- Con las soluciones de Endpoint Detection and Response (EDR) aportamos visibilidad y categorización de todas las fases

del ataque avanzado, alertas tempranas, herramientas de DFIR y la posibilidad de responder en un solo clic.

- Con la nueva gama XDR aportamos una gran riqueza de información, monitorización a nivel de *endpoint*, red, nube, *e-mail* y los usuarios, analíticas de seguridad extensas y la posibilidad de intervención inmediata.
- Y no últimamente, con los servicios MDR aportamos la experiencia y los conocimientos de nuestros *Threat Hunters* –caballeros de nuestro SOC– para detectar ataques que usan técnicas y procedimientos desconocidos, para identificar los robos de datos que aún no han descubierto y para poder decirles antes si van a llegar ser atacados.

Como han podido ver, tenemos las armas para poder ser su escudero y acompañante durante este tremendo viaje. ¿Empezamos? ■

HORATIU BANDOIU
Channel Marketing Manager España y LATAM
BITDEFENDER



Conozca la calificación de ciberseguridad de su organización

Conocer su calificación de riesgo de ciberseguridad le permitirá ver si los activos críticos de su organización son vulnerables a un ataque, lo que podría conducir a la pérdida de datos. RiskRecon dispone de tecnología líder en el mercado para descubrir todos los activos de su organización de manera automática y desasistida. Su informe de riesgo es solo el comienzo para mejorar su gestión de riesgos de ciberseguridad. Visite www.riskrecon.com/know-your-risk-es y obtendrá GRATIS el informe completo de su Rating de Ciberseguridad.

Para obtener más información sobre el enfoque de RiskRecon, o solicitar una demostración, visite el sitio web www.riskrecon.com



NOVEDADES

CLOUD FOUNDATION 4.2., LA APUESTA DE VMWARE PARA ASEGURAR LAS IMPLEMENTACIONES DE CONTENEDORES Y EQUIPOS VIRTUALES A GRAN ESCALA

VMware ha dado a conocer su **Cloud Foundation 4.2**, una actualización de su herramienta para ayudar a los usuarios a mejorar el almacenamiento, la conexión de redes, la gestión y la seguridad de las implementaciones de contenedores y equipos virtuales a gran escala en la plataforma. Además, la empresa anunció la disponibilidad de la plataforma para la persistencia de datos vSAN, incluidos los *plug-ins* de almacenamiento de ob-

simplicidad el consumo de las conexiones de red y las construcciones de seguridad. En definitiva, permite realizar una gestión centralizada, conexiones de red consistentes y configuración de políticas de cumplimiento, así como un estado operativo sincronizado en los despliegues NSX-T federados a gran escala. Además, los clientes pueden utilizar redes ampliadas y políticas de seguridad unificadas que abarcan despliegues de VMware Cloud

Foundation en varias regiones. La actualización, también supone la consolidación de la seguridad de SDDC Manager. Con ella, la

firma pretende proteger las comunicaciones entre SDDC Manager y los subcomponentes para minimizar las amenazas a VMware Cloud Foundation durante las fases operativas.

La nueva versión también tiene una plataforma para la persistencia de datos vSAN, que permite gestionar el almacenamiento de objetos compatibles con S3 para datos no estructurados con la Plataforma HCI. Además, con vSAN HCI

Mesh ofrece un enfoque basado en el software para el desglose de recursos informáticos y de almacenamiento que ayuda a los clientes a reducir el CAPEX. Se espera que Cloud Foundation 4.2 esté disponible durante el primer trimestre del año fiscal 2022 de la firma.

La compañía también ha actualizado su **vRealize Cloud Management** de software como servicio y de entorno local. Su objetivo es ayudar a los clientes a optimizar, proteger y modernizar los entornos de nube híbrida y *multicloud* que usen. A esta novedad se han sumado otros lanzamientos como VMware vRealize Automation 8.3, VMware vRealize Operations 8.3, VMware vRealize Log Insight 8.3, vRealize Suite Lifecycle Manager 8.3, VMware vRealize Network Insight 6.1 y VMware Skyline, junto con mejoras en VMware vRealize Operations Cloud, VMware vRealize Log Insight Cloud y VMware vRealize Network Insight Cloud para adaptarse al entorno cambiante que viven las empresas gracias, entre otras tecnologías, a la aplicación de la Inteligencia Artificial para disponer de más ciberseguridad.

VMWARE

www.vmware.com/es



jetos Cloudian HyperStore y MinIO. "Todo ello, conforma una plataforma de almacenamiento unificada e híbrida preparada para la nube, válida para aplicaciones modernas y tradicionales con consistencia y simplicidad operativa", destacan desde la compañía.

Entre otras novedades, en esta nueva versión se incluye el NSX-T 3.1 Federation, un modelo operativo tipo nube para administradores de red que

SOPHOS PRESENTA SU ZERO TRUST NETWORK ACCESS Y SE ALÍA CON QUALCOMM PARA PROTEGER DISPOSITIVOS 5G CON SU SNAPDRAGON

Antes de la pandemia, ya se estaba produciendo un cambio en las redes, con un porcentaje cada vez mayor de personas que trabajaban desde casa. Esta tendencia se aceleró drásticamente en el último año. Ello ha supuesto un desa-

fío para muchas organizaciones de TI, que han estado luchando para implementar el acceso VPN para sus trabajadores remotos. Sirva como ejemplo que el uso de soluciones como VPN Sophos Connect con XG Firewall se ha multiplicado por 10. Precisamente, para mejorar la seguridad del teletrabajo, la firma británica ha presentado su propuesta **Zero Trust Network Access (ZTNA)**, que dio a conocer en un webinar a través de su Presales Engineer para España, **Alberto Ruiz**, quien destacó que esta solución busca mayor simplicidad y seguridad a la hora de conectar a los usuarios con aplicaciones y

datos importantes. Su ZTNA se basa en el principio de confianza cero y trata de verificar al usuario. Así, aprovecha la autenticación de múltiples factores para evitar que las credenciales robadas sean una fuente de compromiso, luego

valida el estado y el cumplimiento del dispositivo para garantizar que esté registrado, actualizado y protegido adecuadamente. Posteriormente, ZTNA utiliza esa información para tomar decisiones basadas en políticas para determinar el acceso y los privilegios a las aplicaciones en red.

Por otro lado, Sophos ha firmado un acuerdo con **Qualcomm Snapdragon** para dar protección a puntos finales, con capacidades 5G, a través de la plataforma 'Sophos Intercept X'.

SOPHOS

www.sophos.com



LAS NUEVAS CAPACIDADES DE WATCHGUARD CLOUD FACILITAN LA GESTIÓN DE LA SEGURIDAD PARA LOS MSP Y SU ADOPCIÓN DEL ENFOQUE DE CONFIANZA CERO

WatchGuard ha presentado nuevas funcionalidades de su **WatchGuard Cloud**, su plataforma de seguridad para proveedores de servicios gestionados (MSP). Entre otras mejoras, ahora sus clientes dispondrán de una nueva interfaz única y centralizada para ofrecer y gestionar la seguridad de red, la detección avanzada de amenazas y la autenticación multifactor (MFA), entre otros muchos elementos. Los MSP se beneficiarán así de una gestión simplificada de los clientes al tiempo que permiten un crecimiento rápido, eficiente y rentable.

Además, incorpora las funciones de ThreatSync de WatchGuard, las capacidades avanzadas de gestión de políticas de Firebox y las políticas de autenticación que permiten aplicar el enfoque de Zero Trust. Con WatchGuard Cloud, los MSP pueden crear plantillas de políticas para realizar despliegues de seguridad fáciles y repetibles en muchas cuentas de

suscriptores. La plataforma simplifica la gestión y los informes sobre los entornos de seguridad de Firebox y las implementaciones de AuthPoint MFA desde un único panel de control.

A diferencia de otras alternativas, los creadores de WatchGuard

Cloud destacan que está diseñada desde cero con la simplicidad y la facilidad de uso en su núcleo. Además,

la herramienta de configuración RapidDeploy, basada en la nube, ofrece a los usuarios un método optimizado, ágil y sin intervención para configurar fácilmente nuevos entornos de seguridad. La plataforma también da capacidades de gestión multinivel y *multi-tenant*, permitiendo a los MSP crear y gestionar un número ilimitado de cuentas de clientes con facilidad. Asimismo, les permite demostrar su valor a los clientes con más de 100 paneles e informes personalizables.

WATCHGUARD

www.watchguard.com





El antivirus se queda anticuado

Sustituya la seguridad tradicional de terminales por VMware Carbon Black Cloud™ y disfrute de ventajas para la empresa

Para más información visite:
www.vmware.com/es





EL CCN PRESENTA ADA, CARLA Y ELENA PARA LA DETECCIÓN DE AMENAZAS, PROTECCIÓN DINÁMICA Y EN TIEMPO REAL DE DOCUMENTACIÓN Y MEJORA DE LA CIBERINVESTIGACIÓN

El CCN-CERT, del Centro Criptológico Nacional (CCN) presentó en febrero su nueva solución de análisis avanzado de código dañino: **Ada**, una plataforma con la que se mejora la detección de ciberamenazas de tipo *malware* en archivos, ficheros (.zip, pdf, documentos de office, etc.) y URLs.

Ada integra las funcionalidades de detección de las soluciones Marta y María.

Mediante la combinación de análisis dinámicos y estáticos de las muestras, y con el empleo de herramientas de análisis forense, esta solución incrementa las capacidades de identificación de vectores de ataque e infección y de amenazas tanto conocidas como desconocidas. Además, permite controlar, gestionar y acceder a los resultados de todas las tecnologías de análisis que integra desde un solo interfaz unificado.

Carla, seguridad de documentos

También, presentó **Carla** una herramienta “que nace para que las organizaciones tengan su información y documentos siempre prote-



gidos y bajo control en cualquier ubicación”. Así, permite disponer de protección “dinámica y capaz de modificarse en tiempo real”. Gracias a ella, el usuario podrá impedir el acceso a un documento, aunque este ya haya sido compartido y se encuentre en una red o equipo fuera del control de la entidad. Asimismo, la solución incluye una completa auditoría de acceso a la información, dando visibilidad sobre quién ha accedido a un documento y con qué permisos, monitorizando intentos de acceso bloqueados. El CCN ofrece Carla como un servicio gestionado en la nube en dos modalidades: **Carla**, pensada para un servicio limitado a un subconjunto de usuarios de la organización; y **Carla-Global**, diseñada para su despliegue en toda la organización y con todos los módulos opcionales.

Ciberinvestigación de amenazas

El CCN también dio a conocer su herramienta **Elena**, “para adentrarse en el ámbito y las labores de la ciberinvestigación sobre ciberamenazas” y ayudar a “la capacitación de profesiona-

les en tácticas, técnicas y procedimientos de ciberinvestigación para la prevención y análisis de ciberamenazas”. La solución ofrece diferentes itinerarios mediante escenarios simulados en un entorno de laboratorio digital aislado y los usuarios adoptan el rol del analista —en la plataforma el participante adopta la identidad de un personaje bautizado como ‘CCN-Warrior’— teniendo que superar diferentes retos.

Por otro lado, el CCN celebró en marzo, en la Universidad EAN, de Bogotá, en Colombia, su ‘I Jornada STIC’ en el país bajo el lema “Ciberseguridad el compromiso que nos une”.

CCN

www.ccn.cni.es

ES-CIBER APUESTA POR MÁS CULTURA DE CIBERSEGURIDAD PARA REDUCIR EL RIESGO DE CIBERATAQUES EN 2021

Alrededor del 95% de los ciberataques que sufren las empresas tienen su origen en el factor humano, ya sea por desconocimiento o error, según varios informes. Sin embargo, esta situación choca con la realidad: sólo se invierte un 9% del presupuesto anual de Seguridad en concienciar a los empleados. Por ello, desde la compañía **Es-Ciber**, de **Áudea**, se han marcado diferentes retos para 2021 para generar cultura de ciberseguridad, ya que consideran que “mejorarla debería ser uno de los objetivos más importantes para todas las compañías que no quieran tener más sorpresas desagradables”.

Según destacan desde Es-Ciber, “la concienciación es una carrera de fondo en la que la constancia es una pieza fundamental. Nunca podremos conseguir que nuestro equipo interiorice buenas prácticas y cambie su comportamiento habitual realizando sólo una acción”. Por ello, considera fundamental poner los medios para lograr que un usuario cambie su forma habitual de realizar algo tan simple como abrir un correo o responder a



una llamada de teléfono y que lo haga de forma natural.

Entre los principales beneficios que aporta implementar una cultura de ciberprotección en la empresa están desde minimizar el riesgo corporativo ante ciberataques de todo tipo con foco en usuario, hasta lograr que los usuarios conozcan y eviten las principales amenazas, una reducción de gastos y posibles multas por brechas de seguridad y, también, mejorar la concienciación y el nivel de madurez de la misma entre los empleados. Así pues, Es-Ciber recomienda implementar “un plan estratégico continuado en el tiempo que sea capaz de identificar riesgos, diseñar y desarrollar acciones, evaluar y medir el nivel de concienciación”, a través de soluciones integrales como la que ofrece la compañía con diferentes servicios en función de sus necesidades y tomando como punto de partida, el conocimiento de las conductas y comportamientos de los empleados.

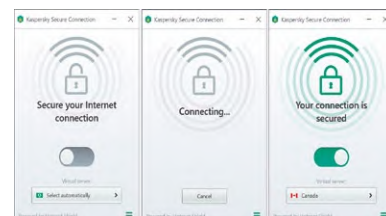
ES-CIBER

www.es-ciber.com

KASPERSKY REFUERZA SU VPN SECURE CONNECTION CON UNA VERSIÓN PARA EQUIPOS MAC CON EL NUEVO PROCESADOR APPLE SILICON

El uso de las redes privadas virtuales (VPN) ha crecido este año debido al aumento del trabajo a distancia. Consciente de la necesidad de privacidad cuando se explora la web, **Kaspersky** ha apostado por actualizar, de forma constante, sus soluciones para que funcionen sin problemas con las plataformas más innovadoras, desarrollando soporte nativo para las novedades hardware. Ahora, la firma rusa ha presentado la primera de sus soluciones de seguridad, **VPN Secure Connection**, para ejecutarse de forma nativa en los Mac con tecnología M1, su nuevo procesador.

El chip SoC (*system on chip*) Apple M1 ofrece un mayor rendimiento y eficiencia a los usuarios de Mac. Y con la última actualización de Kaspersky VPN Secure Connection, los usuarios de los últimos MacBook Air, MacBook Pro y Mac mini, todos con M1, podrán disfrutar de la mayor velocidad a la hora de transferir datos a través



de una VPN segura, manteniendo la privacidad durante su actividad online y ocultando su dirección IP y ubicación. Podrán conectarse a más de 2.000 servidores en 40 ubicaciones en más de 35 países de todo el mundo, incluyendo Estados Unidos, Alemania, y Singapur, entre otros muchos. Asimismo, la versión premium de Kaspersky VPN Secure Connection ofrece la funcionalidad ‘Kill Switch’, que cancela automáticamente todo el tráfico de un dispositivo si se pierde la conexión VPN.

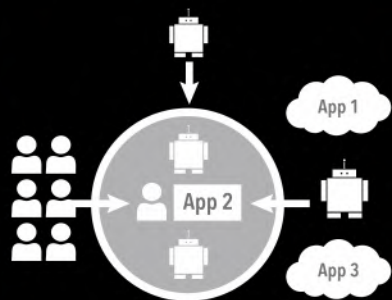
La solución actualizada funciona tanto en los Mac con tecnología M1 como Intel y está disponible como versión gratuita o premium.

KASPERSKY

www.kaspersky.es

Edge Security:

Es hora de adoptar un perímetro en la Nube



ZERO TRUST



- No hace falta distinguir entre tráfico externo o interno
- Todo es externo, igual que en Internet

- Verifíquelo todo, no confíe en nada
- Distribuya aplicaciones y datos solo a usuarios y dispositivos autenticados y autorizados

- Verifique siempre todo con registros completos y análisis de comportamiento
- La visibilidad es vital, es necesario entender lo que es "normal"

¿CÓMO PUEDE AYUDARLE AKAMAI?

Akamai ha desarrollado la plataforma más segura, fiable, escalable y de mayor rendimiento del mundo para ayudarle a afrontar un ecosistema tan lleno de riesgos y poco fiable como el actual.

Obtenga más información en akamai.com/zerotrust

o llámenos al 91 793 31 64



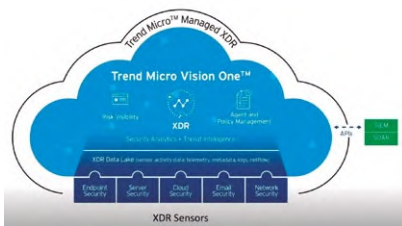


NOVEDADES

TREND MICRO PROPORCIONA MÁS CONTEXTO Y REDUCE EL 'RUIDO' DE LAS ALERTAS CON VISION ONE PLATFORM

Trend Micro ha dado un paso más en su apuesta por identificar y reducir el riesgo cibernético mediante la correlación de alertas en todo el entorno de TI. Hasta ahora contaba con la solución XDR, presentada en 2019 y, ahora, presenta la plataforma **Vision One**, con una XDR mejorada, mayor visibilidad de los riesgos, nuevas integraciones de terceros y una respuesta simplificada a las amenazas en todas las capas de seguridad.

Entre sus características destaca su capacidad para ofrecer visibilidad e inteligencia sobre amenazas, que permiten a las empresas ver ataques complejos y puntos concretos de riesgo que las soluciones aisladas pasan por alto. "En la vista previa, hay nuevos conocimientos sobre el uso de las aplicaciones SaaS, sus niveles de riesgo y las tendencias a lo largo del tiempo", puntualiza la compañía. Vision One también puede ajustar las políticas de seguridad y dirigir las acciones de respuesta en todas las capas de seguridad desde una única consola, simplificando



soluciones de terceros que ya se utilizan para complementar los flujos de trabajo.

Asimismo, los clientes pueden conectar esta plataforma a otras tecnologías de seguridad, como plataformas de protección para puntos finales de terceros y soluciones SIEM y SOAR, incluyendo nuevas integraciones con Fortinet, Microsoft Sentinel y Splunk. Incluso, con cortafuegos, soluciones de *ticketing*, así como con soluciones de gestión de identidades y accesos.

Además, la compañía ha presentado su plataforma **Cloud One** en el Marketplace de Amazon Web Services (AWS), que se ofrecerá en modelo de autoservicio y pago por uso

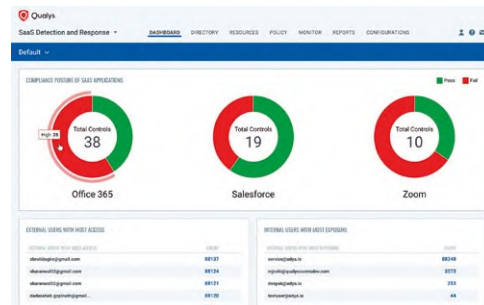
TREND MICRO

www.trendmicro.com/es_es

las tareas de gestión.

Asimismo, permite integraciones nativas con el *stack* de seguridad de Trend Micro en las capas de protección más importantes, además de disponer de APIs listas para usar con las

QUALYS REFUERZA LA SEGURIDAD Y LA GESTIÓN DE RIESGOS EN LAS 'APPS COMO SERVICIO' CON SAAS DETECTION AND RESPONSE



Bajo el nombre **SaaS Detection and Response** (SaaS-DR), **Qualys** ha dado a conocer una solución que permite que los equipos de seguridad y TI obtengan de forma continua visibilidad, seguridad y cumplimiento para las aplicaciones SaaS críticas, desde una única consola.

Con ella, la compañía ofrece un control exhaustivo con un inventario automatizado y actualizado sobre todas las aplicaciones, carpetas y documentos SaaS con el fin de evitar la exposición malintencionada o involuntaria de información confidencial. Con ello, ofrece también una comprensión profunda de la postura de cumplimiento para estas aplicaciones. De hecho, la solución identifica las debilidades de seguridad de las aplicaciones SaaS, así como sus posibles permisos incorrectos, archivos en riesgo, cambios en los archivos, problemas de configuración, vulnerabilidades críticas o *exploits*, utilizando una inteligencia de amenazas avanzada. Además, recopila información detallada sobre los puntos finales, su ubicación, servicios en ejecución y el software instalado.

También, dispone de controles de acceso robustos y realiza evaluaciones continuas y automatizadas de la configuración y políticas de seguridad para estar al día con las exigencias del cumplimiento normativo, entre otras funciones.

La versión inicial de SaaS-DR proporcionará soporte nativo para Google Workspace, Microsoft Office 365, Zoom y Salesforce aunque, durante la segunda mitad de año, incluirá también soporte para soluciones como Slack, GitHub y Microsoft Teams. Además, la compañía ha adelantado que ofrecerá controles personalizados para permitir evaluaciones de políticas de seguridad específicas, capacidades de respuesta proactiva, como alertas sobre exposición de datos y corrección automatizada. Su objetivo es que los clientes puedan solucionar problemas de cumplimiento y exposición corrigiendo automáticamente configuraciones erróneas, vulnerabilidades y amenazas con un solo clic.

Seguridad extendida a Android e iOS

En paralelo, la compañía ha ampliado las capacidades de **Qualys VMDR** (de gestión integral, detección y respuesta en vulnerabilidades) a dispositivos móviles con soporte para Android, así como iOS/iPadOS, proporcionando una solución de extremo a extremo para la seguridad de estos dispositivos.

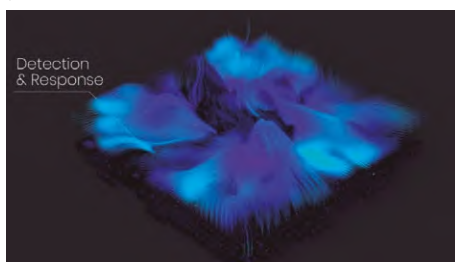
QUALYS

www.qualys.com

SENTINELONE Y ACKCENT AÚNAN SUS CAPACIDADES DE PROTECCIÓN, DETECCIÓN Y RESPUESTA EN EL SERVICIO HYPERAUTOMATED MDR

SentinelOne ha alcanzado un acuerdo para integrar su solución de protección de puntos finales, **Singularity Complete**, en el servicio avanzado de detección y respuesta (Managed Detection and Response) de **Ackcent**. Fruto de esta unión, ambas compañías han lanzado el servicio **hyperautomated MDR**.

En concreto, SentinelOne aporta un enfoque único basado en la inspección profunda de todos los procesos del sistema, combinado con capacidades avanzadas de aprendizaje para aislar de forma rápida comportamientos maliciosos, protegiendo los dispositivos contra amenazas dirigidas avanzadas en tiempo real. Este enfoque aplica también técnicas de detección basadas en el comportamiento de las amenazas, con herramientas forenses y de remediación automatizada para lidiar contra ataques que emplean una combinación de técnicas avanzadas dentro del *malware*, *exploits* o *scripts* inseguros. Con su plataforma Singularity, SentinelOne consigue una protección de dispositivos basada en Inteligencia Artificial sin necesidad de firmas, cubriendo los equipos, sistemas IoT y las cargas de trabajo en la nube. Con un solo agente, además, consolida



toda la funcionalidad "con un impacto mínimo en el rendimiento", indica la compañía.

Por su parte, Ackcent ofrece una gama de servicios gestionados de detección y respuesta 24/7 con un enfoque de 'hiperautomatización' en la detección, respuesta y remediación. Asimismo, aprovecha su experiencia en ciberseguridad para integrar de forma eficaz servicios y soluciones que ayuden a las empresas a resolver los retos de ciberseguridad complejos, tanto en entornos de nube pública como privada.

SentinelOne en la F1

Por otro lado, SentinelOne ha sido nombrada socio oficial de ciberseguridad del equipo Cognizant Formula One de **Aston Martin**. La escudería seleccionó su plataforma Singularity XDR impulsada por Inteligencia Artificial en 2018 para proteger la carga de trabajo en la nube, los dispositivos de IoT y los puntos finales del equipo. Un aspecto crítico durante las carreras.

SENTINELONE

www.sentinelone.com

SOC Managed Security Services



MONITORIZACIÓN IT/OT



CIBER INTELIGENCIA



GESTIÓN DE VULNERABILIDADES



RESPUESTA A INCIDENTES Y ANÁLISIS FORENSE

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

Ibermática

Ibermática es una compañía global de servicios TI que lleva operando en el mercado desde 1973, con presencia multinacional en más de 10 países en Europa y América.



- MÉXICO
- ECUADOR
- PERÚ
- CHILE
- ARGENTINA
- BRASIL
- EEUU
- UK
- ESPAÑA
- ANDORRA



Ciberseguridad IT/OT

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



TF-CSIRT
Trusted Introducer



CSIRT.es



CONTACTA
CON NOSOTROS:

+34 902 102 655
+34 902 413 500

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



CHECK POINT REORGANIZA SU PORTAFOLIO EN TRES FAMILIAS DE PRODUCTO PARA PROTEGER LAS REDES CORPORATIVAS, LAS IMPLEMENTACIONES EN LA NUBE Y EL TELETRABAJO DE LOS EMPLEADOS

Por primera vez, **Check Point** tuvo que celebrar su gran evento anual CPX360 de forma virtual. En él, la compañía dio a conocer su estrategia para 2021 que pasa por reorganizar su cartera de soluciones en tres grandes familias: **Harmony**, **CloudGuard** y **Quantum**, para proteger las redes corporativas, las implementaciones en la nube y a los empleados en cualquier lugar.

Precisamente, la primera de ellas responde al gran impacto que el teletrabajo está suponiendo para las empresas. Para ello, **Check Point Harmony** se presenta como solución unificada que permite la conectividad segura a cualquier recurso desde cualquier lugar ofreciendo protección en todos los dispositivos y *endpoints*, así como en las conexiones a Internet, a la vez que proporciona acceso bajo el enfoque Zero Trust a las aplicaciones corporativas

y al correo-e (como GSuite y Microsoft Exchange).

CloudGuard engloba las soluciones para proteger la nube que, “en la actualidad, utilizan más de 3.000 clientes”, según la compañía.

Dentro de esta familia, destacó la presentación de **CloudGuard Application Security (AppSec)**, una solución de protección de aplicaciones web nativas de la nube y de API, totalmente automatizada, que proporciona protección contra ataques conocidos y de día cero.

Por su parte, la familia Quantum, pensada para dar seguridad a los centros de datos, el perímetro corporativo y los dispositivos IoT, también cuenta con algunas innovaciones como **Quantum Flash**, un *firewall gateway* ultrarrápido para grandes em-



presas. Por otro lado, para las pymes y las sucursales que trabajan en red, la compañía presentó **Quantum Spark**, con una gama de seis *gateways*. Y para los dispositivos OT e IoT, ha creado **Quantum IoT**, basado en el enfoque de Confianza Cero.

El elemento que conecta a las tres grandes familias de soluciones es **Infinity-Vision** que, en 2021, va a disponer de una nueva generación basada en la nube, aunque va a seguir teniendo soporte en local, unificando la gestión de la inteligencia de amenazas y la administración de todos los productos de Check Point.

CHECK POINT

www.checkpoint.com

GMV CREA UTILE PET PARA FACILITAR EL USO DE DATOS GESTIONADOS CON IA SALVAGUARDANDO LA PRIVACIDAD

Con el objetivo de dar respuesta al difícil equilibrio entre la privacidad y la confidencialidad de los datos, especialmente, en sistemas de Inteligencia Artificial (IA), **GMV** ha desarrollado **uTile PET** (Privacy-Enhancing Technologies), una solución que permite realizar cálculos de forma segura y privada sobre datos distribuidos, sin exponerlos ni moverlos de las organizaciones.

uTile permite aprovechar también los datos confidenciales para mejorar los algoritmos de aprendizaje automático y modelos analíticos, cumpliendo en todo momento con los requisitos organizativos, garantizando la privacidad de los datos, así como con las normativas vigentes.

GMV da respuesta así al problema que se crea en un mundo donde, por un lado, cada vez se generan más datos que contienen información sensible y privada y, por otro, las organizaciones incrementan el uso de analítica avanzada cuyos algoritmos utilizan datos, con



buena y mala calidad, con sus restricciones de seguridad y privacidad, etc., y los científicos de datos tienen problemas para acceder a esa información. Con esta solución, “no es necesario elegir entre privac-

idad de los datos y la posibilidad de utilizarlos, ya que aprovecha métodos criptográficos avanzados que mantienen los datos cifrados mientras se realizan todos los cómputos necesarios”, explica el Director de Inteligencia Artificial y Big Data de Secure e-Solutions de GMV, **José Carlos Baquero**. Y es que, uTile habilita la posibilidad de que los datos sensibles de las organizaciones nunca sean ni expuestos ni transferidos a través de departamentos, organizaciones o distintos países. Es más, ni siquiera los propietarios de los datos tienen que confiarlos a terceros, ya que permanecen protegidos tras los controles internos de las organizaciones, ya sea en local o en la nube.

GMV

www.gmv.com/es

RECORDED FUTURE MEJORA SU SOLUCIÓN THIRD-PARTY INTELLIGENCE PARA MITIGAR EL RIESGO EN LA CADENA DE SUMINISTRO

Recorded Future

ha introducido varias mejoras significativas en su solución de inteligencia de terceros, **Third-Party Intelligence**, para permitir que los equipos de seguridad y gestión de riesgos puedan evaluar a terceros “hasta un 50% más rápido y mitigar el riesgo de manera proactiva”, destaca la compañía.

Entre las nuevas características está una visibilidad más profunda de diferentes fuentes de datos, que incluyen desde foros de la Dark Web, sitios de extorsión de *ransomware* y una biblioteca de volcado de datos y credenciales filtradas masivamente, con el fin de ofrecer la imagen más completa del riesgo cibernético.

Las mejoras en la solución permiten a las compañías alinearse con el marco de ciberseguridad del NIST, así como contar



con mayores detalles de evidencia sobre credenciales filtradas y otros indicadores de riesgo, que permite investigaciones más rápidas, la colaboración de terceros y la mitigación de riesgos.

Cabe destacar además que, gracias al motor de recopilación de datos de la compañía, su **Intelligence Graph**, la solución ofrece información en tiempo real sobre las amenazas emergentes de terceros de las organizaciones, lo que permite una evaluación rápida de riesgo del proveedor y la monitorización continua.

RECORDED FUTURE

www.recordedfuture.com

BREVES



■ En el marco de su evento Universe 2021, celebrado de forma virtual a finales de marzo, **Micro Focus** dio a conocer **OPTIC**, una Plataforma de Operaciones para la Transformación, la Inteligencia y la Nube. Su objetivo es acelerar las operaciones de TI aprovechando la inteligencia y la automatización integradas para poder explotar la nube de manera eficaz, superando la complejidad de la transformación de TI.

Durante el encuentro, la compañía también anunció su integración con **Snowflake**. Gracias a ello, los clientes de Micro Focus Voltage SecureData podrán cambiar las cargas de trabajo de manera segura a la plataforma de Snowflake sin comprometer los datos confidenciales y cumpliendo con los requisitos de privacidad. Los clientes de Snowflake, por su parte, se beneficiarán de las capacidades de análisis de datos seguras de Voltage.

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa
estés donde estés.



CYBERSECURITY
EXPERTS ON
YOUR SIDE



go.eset.es/sic

EN CONSTRUCCIÓN. La ciberseguridad insegura: sacando los colores a la sociedad digital



Autor: Jorge Dávila
Prólogo: Luis Jiménez
Editorial: Ediciones CODA
Año: 2021 – 792 páginas
www.revistasic.com

El profesor y director del Laboratorio de Criptografía de la Facultad de Informática de la UPM, **Jorge Dávila**, es uno de los grandes referentes académicos en ciberseguridad y nuevas tecnologías. Desde el año 2000, su sección 'en Construcción', en Revista SIC, se ha erigido como una de las atalayas del pensamiento digital sobre los riesgos y parabienes de las nuevas tendencias que presumen con cambiar el mundo, ya sea la inteligencia artificial, la identidad, la analítica de datos masiva, la automatización y, por supuesto, el cómo aportar ciberprotección a un mundo cada vez

más hiperconectado. Ahora, Ediciones Coda, editora de la Revista, ha querido celebrar sus 30 años de vida agrupando sus 101 artículos durante más de 20 años en una recopilación que, por su profundidad, didactismo y, también, reflexión, son de obligada lectura para los que quieren saber qué hay detrás de toda esa tecnología que usamos cada día y cómo, empezando por las personas, podemos ayudar a que sea más segura. La obra, prologada por el Subdirector del CCN, del CNI, **Luis Jiménez**, además del editor de Revista SIC, **Luis Fernández**, y su director, **José de la Peña**, no dejará indiferente a nadie siendo de 'lectura obligatoria' para los que buscan desasnar. **Revista SIC** inicia 2021 con la celebración de sus 30 años de vida regalando esta obra recopilatoria, que se puede solicitar en PDF o ePUB en www.revistasic.com



BUG BOUNTY: De profesión cazarrecompensas

Autor: Pablo García
Editorial: Oxword
Año: 2021 – 258 páginas
ISBN: 978-84-09-25909-0
Oxword.com

Pablo García está especializado en Auditoría de Cuentas, pero su pasión en su tiempo libre es, desde hace años, reportar vulnerabilidades. De hecho, forma parte del 'Salón de la Fama' de compañías como Netflix, Xiaomi o Pinterest, entre otras. Precisamente su experiencia –y la escasa bibliografía en la materia– le ha llevado a publicar esta obra sobre los programas de recompensas (conocidos como *Bug Bounties*) que cada vez más empresas y organismos incorporan a sus sistemas de seguridad para que investigadores en la materia (especialmente, *hackers*) puedan buscar y reportar vulnerabilidades. Un negocio al alza: Sirva como ejemplo que, sólo entre 2019 y 2020, siete investiga-

dores obtuvieron un total de más de 950.000 euros de recompensa, a través de la plataforma HackerOne.

Para ofrecer una visión realista, con sus claros y sombras, y facilitar a los menos expertos en este campo un 'paso a paso' sobre cómo comenzar, García aborda los aspectos básicos de estos programas, como pueden ser su estructura, las principales herramientas, ciertas metodologías o las vulnerabilidades más comunes. Todo ello, desde un punto de vista práctico analizando reportes públicos realizados por *hackers* de la comunidad. Una obra que, sin duda, por ser de las primeras en castellano, aspira a ser una de las referencias.

DESINFORMACIÓN Y GUERRA POLÍTICA



Autor: Thomas Rid
Editorial: Critica
Año: 2021 – 552 páginas
ISBN: 978-84-91-992776
www.planetadelibros.com

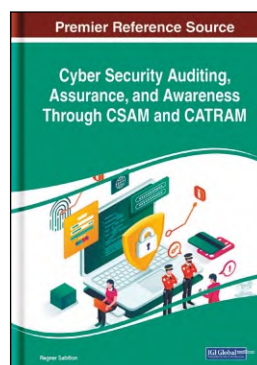
Apasionante obra sobre la información y desinformación como estrategia durante todo el siglo XX y, también, el XXI. Rid, reconocido experto sobre tecnología y espionaje, fue uno de los primeros en alertar de la posible injerencia rusa en las elecciones estadounidenses, en 2016.

En este libro, desgana y lleva al lector a la 'trastienda' de los servicios secretos y de cómo realizan muchas de sus operaciones en el ciberespacio hackeando, filtrando información y falsificando datos para minar "nuestra confianza en la información y debilitar la base misma de la democracia". La obra, escrita

de forma amena y con abundante información y bibliografía sobre la materia, ofrece un asombroso viaje por "un siglo de guerra psicológica secreta" con algunas de las operaciones más significativas de la historia a través de las que cómo los espías comenzaron a explotar la cultura emergente de Internet mucho antes del caso WikiLeaks.

En cierto modo, como explica su autor, el libro "conduce, como si de una visita guiada se tratara, por lo más profundo de un vasto salón de espejos, antiguos y nuevos, apuntando a un futuro de polarización diseñada, pero también nos ofrece las herramientas para superar este engaño". Sin duda, una obra que se convertirá en breve en lectura obligada para los que quieren saber de la desinformación, sus técnicas y qué impacto tiene y tendrá en la sociedad.

CYBER SECURITY AUDITING, ASSURANCE, AND AWARENESS THROUGH CSAM AND CATRAM (Auditoría, garantía y concienciación de ciberseguridad a través de CSAM y CATRAM)



Autor: Regner Sabillón
Editorial: Igi Global
Año: 2021 – 260 páginas
ISBN: 9781799841623
www.igi-global.com

cíficamente el Modelo de Auditoría de Ciberseguridad (CSAM) y el Modelo de Capacitación en Concienciación sobre Ciberseguridad (CATRAM).

Además, presenta estudios de múltiples casos sobre el desarrollo y la validación de estos modelos y marcos, y analiza su implementación y capacidad para sostener y auditar las estrategias nacionales de ciberseguridad. Con cobertura sobre un amplio abanico de temas como análisis forense, evidencia digital y gestión de incidentes, este libro está pensado, especialmente, para investigadores, desarrolladores, legisladores, funcionarios gubernamentales, estrategas, profesionales de la seguridad, educadores, analistas de seguridad y auditores, entre otros.

Regner Sabillón, profesor en la Escuela de Computación de la canadiense Athabasca University y doctorando de la UOC, explora en este libro, reconocido como mejor recomendación para 2021 sobre ciberseguridad según la web BookAuthority, los aspectos prácticos de reevaluar las medidas de ciberseguridad actuales dentro de las organizaciones y los gobiernos internacionales y mejorarlas utilizando modelos de capacitación en auditoría y concienciación, espe-



Modelo de seguridad SASE y Zero Trust

Las soluciones de ciberseguridad de SASE permiten a sus usuarios que accedan de forma segura y sin importar donde estén, a la web, las aplicaciones en nube y las aplicaciones internas.

25 TÉCNICAS APLICADAS A CAMPAÑAS DE RED TEAM Y HACKING



Autor: Daniel Echeverri Montoya
Editorial: Independiente
Año: 2021 – 318 páginas
ISBN: 979-8706390662
www.amazon.es

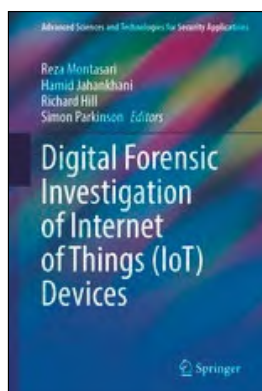
los procedimientos aplicados para luchar contra el cibercrimen en casos reales y, sobre todo, los detalles más relevantes que tienen en cuenta los equipos profesionales de pruebas con intrusiones de seguridad, tanto sus métodos, como procedimientos y mejores herramientas.

La obra está dividida en dos apartados para ofrecer una mejor comprensión de los aspectos más técnicos. Por un lado, concentra una parte teórica con los conceptos básicos que hay que tener y, por otro, una explicación detallada de las tácticas aplicadas por atacantes y ciberdelinquentes para perpetrar ataques contra empresas y organizaciones de cualquier tipo. El libro también tiene un componente altruista: el dinero recaudado con su venta irá destinado de forma íntegra a Unicef.

Daniel Echeverri, conocido en el mundo técnico de la ciberseguridad por 'Adastra' y autor del blog 'The Hacker Way', es un profesional con gran experiencia en Red Team en España. Este libro, de carácter técnico, nace de su afán por dar a conocer los aspectos más desconocidos del día a día de su trabajo como consultor en ciberprotección. Así, en él, explora cada una de las etapas involucradas en una campaña de Red Team. Además, ofrece una completa visión de

DIGITAL FORENSIC INVESTIGATION OF INTERNET OF THINGS (IoT) DEVICES

(Investigación forense digital de dispositivos de internet de las cosas)



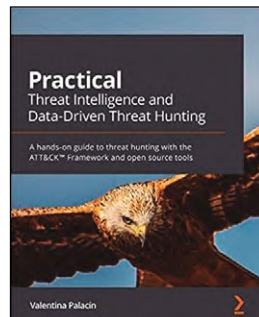
Autores: Montasari R., Jahankhani H., Hill R., Parkinson S.
Editorial: Springer
Año: 2021 – 285 páginas
ISBN: 978-3-030-60424-0
www.springer.com

que pueden usarse para triangular e identificar a las personas y sus acciones. Como tal, el interés y la evolución de los vehículos autónomos", destacan sus impulsores.

Para ayudar en la lucha contra el cibercrimen para los profesionales que quieran especializarse en análisis forense de IoT, tanto como parte de los cuerpos de seguridad o como miembros de los equipos de detección y respuesta a incidentes, este libro proporciona una referencia valiosa para contar con amplios conocimientos sobre la materia. De hecho, cada capítulo está escrito por un experto, de referencia internacional, con amplia experiencia en la aplicación de la ley, la industria y el mundo académico.

La creciente popularidad de los dispositivos de IoT para actividades delictivas denota que hay disciplina y una industria en torno a la ciencia forense en esta área. A medida que la tecnología se vuelve más barata y más fácil de implementar en un mayor número de objetos cotidianos discretos, el alcance para la creación automatizada de huellas digitales personalizadas aumenta con lo que supone dejando un "rastro de datos

PRACTICAL THREAT INTELLIGENCE AND DATA-DRIVEN THREAT HUNTING: A hands-on guide to threat hunting with the ATT&CK framework and open source tools



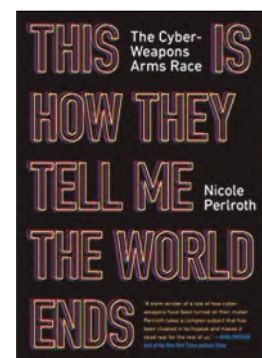
(Inteligencia práctica sobre amenazas basada en datos con el marco ATT&CK y herramientas de código abierto)

Autora: Valentina Palacín
Editorial: Publicación independiente
Año: 2021 – 398 páginas
ISBN: 978-1838556372
www.amazon.com

Valentina Palacín es una analista de inteligencia de amenazas (CTI), especializada en APTs, utilizando el marco Mitre ATT&CK, y fundadora de la comunidad BlueSpaceSec. En este manual, con un enfoque práctico, ofrece información detallada de métodos, herramientas y cómo trabaja aplicando la inteligencia a la búsqueda de amenazas (TH) basada en datos, con abundantes consejos y técnicas de expertos que participan en él. Por eso, esta obra no es una mera introducción para los que carecen de conocimiento en CTI, ni el mundo del TH, sino que se pre-

senta como una guía para aquellos los que, con un conocimiento más avanzado de otros campos de la seguridad cibernética, buscan mejorar los suyos en este ámbito. Así pues, ofrece un paso a paso que parte sobre cómo comenzar a explorar en busca de amenazas cibernéticas para ofrecer conocimientos avanzados de cómo detectarlas y prevenirlas a través de herramientas de código abierto. Incluye ejemplos prácticos y una amplia explicación de cómo usar el marco de trabajo Mitre ATT&CK para "conseguir las habilidades necesarias".

THIS IS HOW THEY TELL ME THE WORLD ENDS: THE CYBERWEAPONS ARMS RACE



(Así me dicen que acaba el mundo: La carrera armamentista de las ciberarmas)

Autora: Nicole Perlroth
Editorial: Bloomsbury Publishing
Año: 2021 – 528 páginas
ISBN: 978-1526629852
www.bloomsbury.com/uk

La especialista en ciberseguridad del New York Times, **Nicole Perlroth**, profundiza en esta obra en los aspectos menos contados "del mercado de armas cibernéticas, el mercado más secreto, invisible y respaldado por el gobierno en la tierra, y un primer vistazo aterrador a un nuevo tipo de guerra global". Un mundo que la autora plasma en una trepidante novela llena de "espías, hackers, traficantes de armas y algunos héroes anónimos". El *thriller* está documentado

en los años de informes y cientos de entrevistas que su autora ha realizado para el rotativo estadounidense desvelando con asombrosa nitidez la amenaza cibernética global que se cierne sobre el mundo. Se trata, en definitiva, de una forma de sacudir de su letargo a los que aún no son conscientes de los riesgos que acarrea el mundo digital a través, en muchos casos, de los propios estados. Y es que pone como ejemplo el 'arsenal' de fallos 'de día cero' que países como EE.UU. han acumulado pagando por ellos millones de dólares y que, en ocasiones, han sido robados por "naciones hostiles y mercenarios".

MÓNICA NGSIEM

**La solución del CCN-CERT
para la gestión de eventos e
información de seguridad en
la Administración Pública**

Tecnología española

Recoge en una única plataforma toda la información existente sobre amenazas potenciales permitiendo no solo reaccionar ante los ataques, sino adelantarse a ellos para remediarlos antes de que sucedan.

Cursos SANS INSTITUTE

- **SEC401 Security Essentials Bootcamp Style**
12/23-4-2021
- **SEC504 Hacker Tools, Techniques, Exploits and Incident Handling**
12/23-7-2021
- **FOR578 Cyber Threat Intelligence**
29-11/4-12-2021
Organiza: One eSecurity
Formato Live Online.
Tel.: 911 011 000
Correo-e: sans@one-esecurity.com
Sitio: www.one-esecurity.com

CyberICON

Organiza: Deloitte
Fecha: 13-4-2021
Evento en línea.
Sitio: <https://cutt.ly/rxGRtad>

Cursos de ISACA Madrid

- **Preparación al examen CRISC**
19/30-4-2021.
- **Preparación al examen CISM**
17/28-5-2021.
- **Preparación al examen CISA**
17/31-5-2021
Organiza: ISACA Madrid
Tel.: 91 639 29 60
Correo-e: administracion@isacamadrid.es
Sitio: www.isacamadrid.es

RSA Conference 2021

Organiza: RSA Security
Fechas: 17/20-5-2021
Evento digital.
Correo-e: information@rsaconference.com
Sitio: rsaconference.com

Curso OSINT: Inteligencia de Fuentes Abiertas en Internet.

Organiza: Alianza española de seguridad y crisis. AESYC
Fecha de inicio: 20-5-2021
Curso online.
Correo-e: coordinacion@aesyc.com
Sitio: aesyc.com

Congreso y Expo ASLAN 2021

Organiza: Asociación @ASLAN
Fechas: 2/3-6-2021
Lugar: IFEMA Palacio Municipal. Madrid
Sitio: aslan.es

II Foro de Ciberseguridad y Negocio

Organizan: Deloitte CyberSOC e ISMS Forum
Fecha: 25-6-2021
Sitio: ESADE Madrid.
Tel.: 629 407 729
Correo-e: mmartincirujano@deloitte.es
Sitio: <https://cutt.ly/gxT9JVA>

VIII WiCyS Conference

Organiza: Women in Cybersecurity
Fechas: 8/10-9-2021
Lugar: Denver. Estados Unidos.
Sitio: www.wicys.org/events/wicys-2021/

UNITE Conference EMEA

Organiza: One Identity-Quest
Fechas: 4/8-10-2021
Lugar: Barcelona
Sitio: oneidentity.com/unite-conference

SECURMÁTICA 2021

Seguridad digital: todo se transforma

Organiza: Revista SIC
Fechas: 5/7-10-2021
Lugar: Hotel Novotel Campo de las Naciones. C/ Ámsterdam, 3. Madrid
Tel.: 91 575 83 24
Fax: 91 577 70 47
Correo-e: info@securmatica.com
Sitio: securmatica.com

Cursos ES-CIBER

Organiza: Escuela Superior de Ciberseguridad, ES-CIBER
Correo-e: info@es-ciber.com
Sitio: www.es-ciber.com

IDENTI::SIC 2021

Cara a cara... con la identidad

Organiza: Revista SIC
Fechas: 16/17-11-2021
Formato mixto: presencial y retransmitido.
Lugar: Hotel Novotel Campo de las Naciones. C/ Ámsterdam, 3. Madrid.
Tel.: 91 575 83 24
Correo-e: info@codasic.com
Sitio: revistasic.es/identisic

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 M2i formación

Organiza: Alhambra-Eidos
Tel.: 91 787 23 00
Fax: 91 787 23 01
Sitio: m2iformacion.com

AENOR Formación

Organiza: AENOR
Tel.: 91 432 61 25
Sitio: aenorciberseguridad.com

INDICE DE ANUNCIANTES

EMPRESA	PAG.	EMPRESA	PAG.	EMPRESA	PAG.
ADVANTIO	23	IDENTISIC	11	QUALYS	141
AENOR	73	INGENIA	53	RECORDED FUTURE	21
AIUKEN	13	ITS	175	RISKRECON	169
AKAMAI	173	JTSEC	17	S2 GRUPO	165
ALL4SEC	77	LEET SECURITY	109	S21 SEC	105
ARROW	65	LOGICALIS	45	SAILPOINT	41
BARRACUDA	167	MCAFEES	153	SECURMÁTICA	Contraportada
BITDEFENDER	47	MDTEL	157	SEIDOR	139
BLUELIV	133	MICROSOFT	Documentos SIC	SENTINEL ONE	9
BOTECH	63	MNEMO	59	SMARTFENSE	125
CCI	69	NETSKOPE	135	SOPHOS	113
CHECK POINT	4	NETWITNESS (RSA)	25	SOTHIS	159
CIPHER	61	NOVARED	71	STORMSHIELD	37
CYTOMIC-WATCHGUARD	43	NUNSYS	67	TARLOGIC	27
DOT FORCE	51	OKTA	103	THALES	163
ENTELGY INNOTECH	7	ONE ESECURITY/		THREATQUOTIENT	155
EPIC BOUNTIES	29	SANS INSTITUTE	183	THYOCOTIC	143
ES-CIBER	57	ONE IDENTITY	81	TREND MICRO	31
EXCLUSIVE NETWORKS	107	ONESEQ	75	VMWARE	171
EY	49	ONTINET-ESET	177	V-VALLEY	2-3
FACTUM	121	OYLO	39	WESTCON	33
FASTLY	95	PALO ALTO NETWORKS	15	WISE SECURITY	127
FORCEPOINT	179	PCYSYS	85	ZEROLYNX	35
GMV	55	PROOFPOINT	83	ZSCALER	117
ICA	181	PWC	19		



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
Jess García y Carlos Fragoso.

Nuevo 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)*

*Excepto el curso FOR578 que dura una semana.

CALENDARIO 2021



SEC401 | GSEC |
Security Essentials Bootcamp Style

12-23/04/2021 | 15h a 21h CEST
De Lunes a Viernes



SEC504 | GCIH |
Hacker Tools, Techniques, Exploits,
and Incident Handling

12-23/07/2021 | 15h a 20h CET
De Lunes a Viernes



FOR578 | GCTI |
Cyber Threat Intelligence
29/11 - 04/12/2021 | 9h a 17h CET
De Lunes a Sábado



Carlos Fragoso



Jess García

El precio de los cursos es de 6.595 € + 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

The background of the poster is a dark space filled with vertical columns of binary code (0s and 1s). In the upper right corner, there is a small, reddish-orange planet. In the lower left corner, there is a statue of a person in a thinking pose, rendered in a metallic, textured style. The main title 'SECURMÁTICA' is written in a large, glowing orange-outlined font across the top.

SECURMÁTICA

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

**Seguridad digital:
todo se transforma**

**5 • 6 • 7
OCTUBRE
2021**

www.securmatica.com

Ciberprotección consistente, integrada y resiliente



Pablo Vera

Sr Sales Manager
Cybersecurity Solutions
Microsoft

**“Zero Trust: un enfoque
holístico con capacidades
únicas”**

**Microsoft: ADN de ciberseguridad para
contar con una protección anticipativa**

**Seguridad en la nube:
*Swift security to the left***

**Gestión del riesgo
y cumplimiento inteligente**

Modern SOC



ENTREVISTA

Alberto Pinedo

National Technology
Officer (NTO) de Microsoft



Su apuesta por la IA, el principio de seguridad por defecto, 3.500 especialistas y una inversión millonaria convierten a la compañía en un gran referente mundial

Microsoft: ADN de ciberseguridad para contar con una protección anticipativa

La ciberseguridad forma parte del ADN de Microsoft. Con una inversión de más 1.000 millones de dólares al año en ella, su reto es ofrecer protección basada en el principio de 'Confianza Cero' y un enfoque holístico a través de la gestión de identidades y de accesos, la detección proactiva y avanzada de amenazas, la protección del dato y la monitorización unificada, una apuesta que le ha llevado a facturar globalmente en estos segmentos más de 10.000 millones de dólares en su último ejercicio.

La seguridad está en el ADN de **Microsoft** desde que hace más de dieciséis años **Bill Gates** formulara la 'Trustworthy Computing Initiative', por la que la seguridad se promueve por diseño. Ahora, con más de 3.500 profesionales dedicados a la protección

de sus productos, sus servicios y la de sus clientes y una inversión de más de 1.000 millones de dólares (840 millones de euros) cada año, apuesta por una aproximación holística, integrando la ciberseguridad como servicio horizontal en todos sus productos y servicios para ayudar a "simplificar y reforzar la protección de las organizaciones".

Para conseguirlo cuenta con equipos de expertos especializados en diferentes ámbitos de la ciberseguridad, entre los que están desde su **Digital Crimes Unit (DCU)** hasta el **Microsoft Threat Intelligence Center (MSTIC)**, especializado en el seguimiento de adversarios avanzados, su **Detection and Response Team (DART)** centrado en la Respuesta a Incidentes y, por supuesto, su centro de operaciones, el **Microsoft Cyber Defense Operation Center (CDOC)**, desde el que monitoriza toda la actividad 24x7. Gracias a ellos, se analizan ocho billones de 'señales' diarias a través de una red de monitorización mundial que otorga a la compañía una posición privilegiada para detectar y remediar amenazas.

Para apoyar la seguridad proactiva, la compañía ha apostado por la IA, que permite tener a punto sistemas de alerta temprana muy efectivos para enfrentarse a los crecientes riesgos de ciberseguridad que, en 2022, supondrán un coste de más de ocho billones de dólares a escala mundial. "La IA hace posible que los profesionales de ciberseguridad se centren en tareas que aporten el



máximo valor, reduciendo labores administrativas y repetitivas para ayudarles a procesar grandes cantidades de alarmas, detectar anomalías y responder en el menor tiempo posible". Además, la compañía con sede en Redmond destaca por la combinación de uno de los mayores repositorios de inteligencia de seguridad del mundo (Microsoft Intelligence Security Graph) con sus capacidades en IA y el contexto humano, proporcionado por los expertos de DCU, MSTIC, DART y el CDOC para adaptar los modelos predictivos de *Machine Learning* a los cambios en el entorno de amenazas.

Cuatro pilares

Así, su apuesta es lograr una protección de 360° a través de cuatro grandes pilares: la gestión de identidades y autenticación, la detección proactiva y avanzada de amenazas, la protección del dato y la monitorización unificada, todo un reto en el que juega un papel destacado su Plataforma XDR que

integra, de forma nativa, controles de seguridad para los sistemas, la colaboración en Microsoft 365 y la nube de Azure (con más de 60 regiones y utilizada por el 95% del Fortune 500), tanto para IaaS, PaaS y SaaS, extendiendo su cobertura a múltiples plataformas

y con un enfoque *multicloud*. A sus capacidades se suma que es una plataforma abierta a la integración de soluciones de terceros, fruto de su colaboración con los más de 200 socios de la **Microsoft Intelligent Security Association**.

Cumplimiento

Su objetivo es que, a través de ella, los clientes de Microsoft puedan desarrollar una estrategia Zero Trust basada en asumir que pueden sufrir un incidente de seguridad en cualquier momento.

Dado que la privacidad es de forma creciente un imperativo de negocio, la multinacional también ha apostado por ofrecer una nube segura y preparada para la adaptación continua al marco regulatorio, facilitando el cumplimiento de normas internacionales tan exigentes como el RGPD, la ISO 27001, HIPAA, FedRAMP, SOC 1 y SOC 2 o, en España, la certificación con el Nivel Alto del Esquema Nacional de Seguridad (ENS). ●

Microsoft posee uno de los mayores repositorios de inteligencia de seguridad del mundo (Microsoft Intelligence Security Graph), que combinado con sus grandes capacidades en IA y el contexto humano proporcionado por sus expertos en diferentes áreas, es capaz de adaptar los modelos predictivos de Machine Learning a los cambios en el entorno de amenazas.

Zero Trust: un enfoque holístico con capacidades únicas

La transformación digital y las nuevas formas de trabajo remoto híbrido, que van a formar parte de nuestra realidad presente y futura, están forzando a las organizaciones a cambiar el concepto de seguridad tradicional a un modelo de desconfianza total, en la que todos los accesos desde todas las ubicaciones no deben ser confiables por defecto. Unimos a esta situación que los adversarios cada vez buscan más usar identidades comprometidas para entrar en los sistemas, haciéndose pasar por usuarios legítimos, lo que nos obliga a poner en la identidad el nuevo plano de control de la seguridad. Es precisamente la identidad uno de los pilares fundamentales de la propuesta Zero Trust de Microsoft.

Zero Trust es, en términos prácticos, una transición de la confianza implícita —suponiendo que todo dentro de una red corporativa es seguro— al modelo que asume la brecha y verifica explícitamente el estado de seguridad de la identidad, el dispositivo utilizado, la red y otros recursos en función del análisis de todas las señales y datos disponibles. Pero para establecer una estrategia sólida de Zero Trust se debe adoptar un enfoque holístico que tenga en cuenta todos los aspectos que consideramos fundamentales: identidades, dispositivos, redes, infraestructura, aplicaciones y datos.

Cada uno de estos seis elementos principales sirve como fuente de señales para la detección y el análisis de anomalías, establece un plano de control para su aplicación y constituye un recurso crítico a defender. La Plataforma de Seguridad XDR de Microsoft, Microsoft Defender, proporciona controles nativos, integrados, multiplataforma y *multicloud* para todos estos elementos, simplificando la aplicación efectiva de la estrategia Zero Trust, reduciendo los tiempos de implementación, los riesgos y la complejidad de las operaciones de seguridad.

La aproximación Zero Trust de Microsoft se basa en tres principios:

1. Nunca confiar, verificar siempre. Independientemente de dónde se origine la solicitud o a qué recurso se acceda, Zero Trust nos enseña a “nunca confiar y verificar siempre”. Saber quién está solicitando acceso es esencial. Antes de concederlo, cada solicitud debe autenticarse fuertemente, autorizarse

dentro de las restricciones de las directivas y monitorizarse en tiempo real en busca de anomalías. El proceso, basado en *Machine Learning*, comprueba todo el contexto y otorga una puntuación de riesgo a cada conexión, desde la identidad del usuario, su ubicación, el estado del dispositivo desde el que se accede y su postura de seguridad, el comportamiento de la aplicación, las directivas organizativas, la clasificación de la información accedida hasta el entorno de hospedaje de la aplicación para evitar una infracción. A partir de ese veredicto, se

más fácil de mantener (al tener menos elementos que los atacantes puedan explotar), sino que además el modelo basado en la nube permite recopilar una gran cantidad de señales que, junto con procesos de análisis avanzados, hace posible la detección de anomalías muy sutiles y sólo detectables en conjuntos de datos muy grandes.

3. Asumir el incidente de seguridad. Zero Trust también significa que se debe asumir que se podrían producir incidentes de seguridad en cualquier momento, incluso que podríamos estar sufriendo una situación crítica

ahora mismo. Una mentalidad siempre vigilante ayuda a tener un comportamiento proactivo que permita minimizar y prevenir los movimientos laterales. También, deben utilizarse técnicas como microsegmentación, ci-

frado fuerte y análisis de la telemetría para detectar más rápido las posibles brechas. Siguiendo este comportamiento, además de mejorar las capacidades de detección y respuesta, también se reducirá el impacto cuando se produzcan los incidentes. La preparación para la respuesta a un incidente es una tarea fundamental. Desde Microsoft disponemos de servicios profesionales específicamente diseñados para ayudar a nuestros clientes a identificar donde están sus áreas de mejora, en cuanto a herramientas, procedimientos y necesidades formativas de sus equipos de respuesta. Mediante la realización de ejercicios prácticos de simulación usando ejemplos de situaciones de crisis reales, el cliente pone a prueba a sus equipos y sus procesos, verificando qué elementos funcionan bien y cuáles necesitan ajustes de mejora. Las empresas que operan bajo el modelo Zero Trust de Microsoft son más resilientes, consistentes y reaccionan mejor y más rápido ante nuevos ataques.

Para facilitar a nuestros clientes el inicio de este camino disponemos de guías de implementación de Zero Trust, de acceso público, a través del portal <https://docs.microsoft.com/en-us/security/zero-trust>



desencadenan una serie de procesos: dar el acceso, concederlo limitado, bloquearlo completamente, solicitar una autenticación multifactor (MFA) o pedir al usuario que restablezca sus credenciales y vuelva a solicitar el acceso. Todo ello, realizado de forma automática o de forma autónoma por el usuario, reduciendo la carga de trabajo sobre los equipos del *Help Desk*.

2. Privilegios mínimos para los usuarios. Otro principio fundamental de Zero Trust, el acceso con privilegios mínimos, otorga acceso a los usuarios sólo cuando lo necesitan, por el tiempo que lo precisan y para la tarea específica en cuestión. El control de acceso utiliza políticas adaptativas basadas en el riesgo de cada conexión protegiendo los datos, sin comprometer la productividad del usuario.

Microsoft proporciona herramientas para la verificación de los accesos para limitar, al mínimo, el número de usuarios privilegiados, estableciendo un modo de trabajo basado en solicitudes de escalada de privilegios temporales. Igualmente, dispone de herramientas integradas para la gestión de las identidades privilegiadas (PIM), de los accesos privilegiados (PAM) y para la implementación de máquinas específicas para accesos privilegiados (PAW), que facilitan una gestión de los accesos privilegiados completa y robusta.

La utilización de un modelo de identidad moderno basado en la nube, como Azure Active Directory (Azure AD), es más sencillo y seguro que usar mecanismos de federación con las identidades locales. No solo es



PABLO VERA
Sr Sales Manager
Cybersecurity Solutions
Microsoft

Desde hace casi dos décadas en Microsoft es uno de los referentes en tecnología y, también, en ciberseguridad. De hecho, ha sido el responsable en la compañía de llevar a cabo grandes proyectos en sectores tan diversos como *retail*, finanzas... Además, ha liderado la renovación del Esquema Nacional de Seguridad para Azure, Microsoft 365 / Microsoft 365 Education y Dynamics 365. Especializado en IA, Datos, Computación en la Nube, Identidad Digital, Innovación y Transformación Digital, Alberto Pinedo explica las claves que han llevado a Microsoft a tener la ciberprotección como un pilar fundamental en sus productos y servicios, además de colaborar con gobiernos en la lucha contra el cibercrimen.

“El camino hacia la resiliencia en la automatización de los negocios lo marcan la adopción del modelo Zero Trust y la aplicación de Inteligencia Artificial”

– ¿Qué lema resumiría mejor la estrategia de Microsoft en ciberseguridad?

– Nuestra estrategia es única en la industria, por un lado, con un enfoque integrado y, por otro, aprovechando la Inteligencia Artificial y la automatización. Además, contamos con una aproximación holística sobre aspectos fundamentales de la ciberprotección como la seguridad de la identidad y la administración de acceso; los puntos de acceso, el correo electrónico y la seguridad de las aplicaciones; la prevención de la pérdida de datos y la seguridad en la nube y nuestras soluciones de SIEM/SOAR hacen que nuestro enfoque sea de extremo a extremo.

– ¿Qué capacidades de ciberseguridad les demandan sus clientes en España?

– Contamos con clientes a los que proporcionamos servicios de defensa proactiva en todos los sectores. Ninguna empresa debe bajar la guardia y, en consecuencia, tomar medidas para minimizar su área de exposición. Entre las capacidades más demandadas en el último año están las relacionadas con las plataformas de trabajo confiables, debido a que el perímetro de seguridad de las empresas se ha ampliado. Por ello, es más necesario que nunca adoptar el modelo Zero Trust, para el que contamos con una evaluación *online*, que permite a las empresas determinar en qué etapa de madurez están y cómo mejorar.

– En los últimos años han firmado acuerdos relevantes con entidades como el CCN...

– Son una prueba fehaciente de la apuesta de Microsoft por la seguridad en todos sus servicios y garantiza a las

empresas los máximos estándares a la hora de adoptar nuestras soluciones. Microsoft cumple con un amplio abanico de normas internacionales tan exigentes como el RGPD o la norma ISO/IEC 27001, entre otras muchas. En el caso concreto del Centro Criptológico Nacional, fuimos el primer gran proveedor de soluciones *cloud* en obtener el certificado de conformidad con el ENS, con categoría ALTA, en 2018. Actualmente, hemos renovado los certificados para Microsoft Cloud (Microsoft 365, Dynamics 365 y Microsoft Azure) con categoría ALTA en todos nuestros servicios. Además, también colaboramos con este organismo, a través de su ecosistema de *partners*, en la elaboración conjunta de guías de seguridad alineadas con el cumplimiento del ENS.

– ¿A qué nuevas amenazas se están enfrentando las empresas?

Las actividades de los ciberdelincuentes se han vuelto más oportunistas, es un modelo de negocio en sí. El volumen y la complejidad de los

ciberataques ha crecido de forma notable en los últimos tiempos. En este contexto, es necesario tener una estrategia sólida y confiar en proveedores que ofrezcan una ventaja competitiva para afrontar los riesgos ciber. Entre otras capacidades, el Microsoft Cyber Defense Operation Center (CDOC) nos permite monitorizar la actividad mundial 24x7, analizando billones de señales diarias. A ello hay que sumar la combinación de uno de los mayores repositorios de inteligencia de seguridad del mundo, con nuestra tecnología de IA y la adaptación de los modelos predictivos de *machine learning* a los cambios en el entorno de amenazas.

– **Su compañía apuesta hoy por adoptar un modelo Zero Trust...**

Sí; y lo hacemos en cada uno de los cuatro grandes frentes que permiten la protección de 360 grados de nuestros servicios: gestión de identidades y autenticación, detección proactiva y avanzada de amenazas, protección del dato y monitorización unificada. Además, nuestra propuesta de soluciones de seguridad se basa en una plataforma XDR (Extended Detection & Response), que integra de forma nativa controles para todos los sistemas y que está abierta a la integración con soluciones de seguridad de terceros, gracias al trabajo de la Microsoft Intelligent Security Association, que cuenta con más de 200 socios.

– **¿Qué aporta Microsoft a un CISO que quiere tener un nivel aceptable de riesgo de ciberseguridad en sus entornos multinube?**

– Una base tecnológica que cumple con los estándares más exigentes de la industria, manuales para su despliegue elaborados en colaboración con el CCN, una filosofía DevSecOps para proteger todo el ciclo de vida de desarrollo de software y una red de monitorización global para actuar proactivamente ante los riesgos. A ello se suma una red de *partners* especializados que proponen las soluciones más adecuadas a cada situación. En entornos *multicloud* es necesario obtener una vista holística para correlacionar las amenazas y evaluar cómo una amenaza puede afectar a otro recurso. Soluciones como Microsoft Cloud App Security brindan herramientas para detectar aplicaciones en la nube y supervisarlas y protegerlas, mientras que con Azure Sentinel recopilamos y analizamos datos en todas las instalaciones y en varias nubes.

– **¿Cuál es la tecnología de protección digital de Microsoft más desconocida por los clientes corporativos?**

– Es difícil apostar por una, pero sí destacaría Microsoft Intelligent Security Graph API, que permite conectar productos y servicios de seguridad Microsoft, así como de nuestros *partners* para optimizar las operaciones de seguridad y mejorar la protección, detección y respuesta ante ciberamenazas. Es una gran aproximación y da excelentes resultados.

– **El ‘Modern SOC’ se basa en una combinación de herramientas SIEM nativas de la nube, con IA y aprendizaje automático... ¿Qué marca la diferencia con otras aproximaciones?**

– La misión principal del SOC es identificar rápidamente situaciones de compromiso y responder a los incidentes. En medio de un ataque, los minutos importan. En este contexto, en un SOC moderno la IA y el aprendizaje automático juegan un papel clave y su uso permite a los expertos reducir el ‘ruido’ y centrarse en las cuestiones relevantes. De este modo, se cuenta con una importante ventaja competitiva. Es nuestro caso, con Azure Sentinel, donde la IA y el *machine learning* analizan cantidades masivas de datos para detectar con mayor precisión los modelos de comportamiento que indican un riesgo.



“Soluciones como Microsoft Cloud App Security brindan herramientas para detectar aplicaciones en la nube, supervisarlas y protegerlas, mientras que con Azure Sentinel podemos recopilar y analizar datos en todas las instalaciones y en varias nubes”

– **Ataques contra la cadena de suministro han evidenciado la necesidad de incrementar los esfuerzos en esta área, ¿Cómo aborda el problema Microsoft?**

– Es una de las tres amenazas más importantes a las que nos enfrentamos, no sólo como compañía, sino también como sociedad, tal y como lo reflejó nuestro presidente, Brad Smith, pidiendo una respuesta fuerte y global en materia de ciberseguridad. Los ataques-nación se han vuelto más sofisticados y de una mayor determinación. En nuestro caso, disponemos de un programa denominado ‘Government Security Program’ con el que damos información a más de 45 países, entre ellos España, sobre vulnerabilidades, código fuente de nuestros productos y amenazas. Adicionalmente, mantenemos línea directa con los equipos que investigan dichos ataques a escala mundial. El objetivo es ofrecer la mayor información posible, de forma transparente y con una comunicación proactiva, a los responsables de ciberseguridad a nivel nacional.

– **¿Cuál diría usted que es la gran novedad en materia de ciberseguridad de Microsoft en lo que llevamos de 2021?**

– Uno de los grandes anuncios en Microsoft Ignite, nuestro evento anual para Profesionales de TI y desarrolladores, fue el lanzamiento de la autenticación sin contraseñas en Azure Active Directory. Las organizaciones ya pueden hacer uso de esta funcionalidad y beneficiarse de una mayor seguridad y simplicidad apoyándose en tecnologías como Windows Hello, la aplicación Microsoft Authenticator y llaves FIDO2.

De hecho, ya contamos con más de 200 millones de usuarios que se autentican sin contraseña en nuestros servicios de consumo y empresa. En 2021, esperamos que el *passwordless* se convierta en una tendencia. ●

SEGURIDAD EN LA NUBE: SWIFT SECURITY TO THE LEFT

Dictar las normas ya no es suficiente: de las políticas como documentación a las políticas como código

Comparar la ciberseguridad con el sistema inmunológico no es novedoso, pero no por ello deja de ser fascinante. Se trata de un punto de vista que plantea la ciberprotección como un proceso evolutivo, de resiliencia y, también, de adaptabilidad.

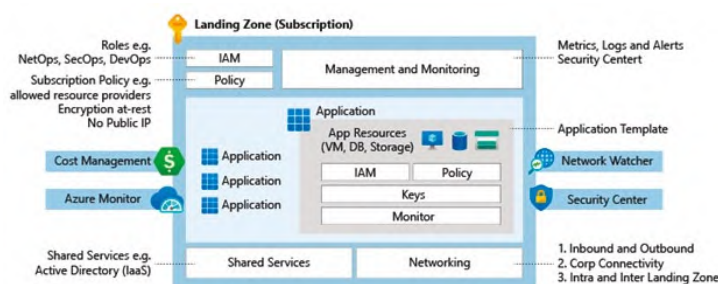
Un claro ejemplo son las citoquinas, uno de los métodos usados por las células y el sistema inmunitario para comunicar que están siendo atacadas y, tras recibir esta señal, activar en el organismo el 'modo protegido', deshabilitando comportamientos no vitales o reforzando medidas de protección. Esto ha inspirado a Microsoft para diseñar sus aplicaciones para que, en caso de verse comprometidas, detecten que son incapaces de cumplir sus indicadores de confidencialidad, integridad o disponibilidad, alertando de la situación y activando un proceso que supone suprimir capacidades no imprescindibles e implementar medidas adicionales.

Sin duda, la nube proporciona una gran plataforma sobre la que desarrollar aplicaciones con las características esperadas sin necesi-

dad de controlarlas individualmente. Se trata de una apuesta por implementar en la nube de Microsoft, Azure, un principio fundamental como es el uso de los llamados Blueprints, que definen políticas y roles, así como la existencia (o ausencia) de ciertos componentes en todo despliegue.

Estas políticas pueden ser utilizadas para

minantes. Además, como componente básico también se apuesta por una arquitectura en la que toda aplicación tenga asociada una 'caja fuerte' donde guardar secretos, se cuente con un WAF protegiendo la salida a Internet, se habilite un espacio donde se hagan copias de seguridad, etc. De esta forma, la multinacional consigue dotar a cada una de las aplicaciones de una inmunidad innata frente a amenazas.



múltiples propósitos entre los que están desde mejorar la ciberseguridad, hasta el gobierno y, también, el cumplimiento. Gracias a ello, Microsoft logra que todo disco esté cifrado, que cada servicio envíe su telemetría a un sistema central, que ningún componente desplegado tenga IP pública o prohibir desplegar en ciertos países, entre otros aspectos deter-

Valor diferencial

El valor para la seguridad de la aproximación DevOps en la nube emerge usando repositorios de código como única fuente de verdad, así como *pipelines* continuos automatizados de testeo y despliegue en

todos los entornos, desde desarrollo a producción. Eso sí, para garantizar su eficacia este modelo debe usarse tanto para el desarrollo de las aplicaciones como en la definición de la infraestructura general. Así, Microsoft no solo se adapta mejor a las nuevas amenazas, sino que permite recuperarse de cualquier incidente con solo pulsar el botón de 'Redesplegar todo'.

Gestión del riesgo y cumplimiento inteligente frente a un entorno normativo dinámico global

La gestión y protección del dato se ha convertido en uno de los grandes retos para las empresas, especialmente cuando se trata de garantizar el cumplimiento, con un marco normativo tan cambiante como el actual. Solo en 2020 se registraron más de 215 actualizaciones de regulaciones al día, de más de 1.000 organismos en todo el mundo, según el informe 'Coste del cumplimiento 2020. Actualización de la Covid-19', de Thomson Reuters. A ello, se le suma el hecho de que los datos no son estáticos. Tienen un ciclo de vida desde el momento en que se crean, comparten y almacenan en un amplio abanico de plataformas y servicios, tanto en la nube, como en las instalaciones o en entornos híbridos.

En la mayoría de los casos, las organizaciones disponen de recursos y herramientas limitados para identificar y mitigar los riesgos derivados de su falta de seguimiento y control en toda la empresa, al tiempo que se tiene que cumplir con los estándares de privacidad del usuario. Por ello más de la mitad de las compañías (54%) reconocen estar preocupadas por la falta de visibilidad de su ecosistema digital.

Ante estos desafíos, Microsoft ofrece un portafolio de soluciones de cumplimiento inteligente y gestión de riesgos que proporcionan capacidades integradas en cuatro áreas clave:

1.-Gobierno y protección de los datos donde quiera que se encuentren.

Los clientes disponen de la flexibilidad necesaria para implementar los

controles precisos para cumplir con los requisitos de cumplimiento y seguridad internos y externos, enriquecidos por una plataforma inteligente.

2. Identificación de los riesgos internos críticos y aplicación de medidas sobre ellos. Microsoft ha potenciado su solución Insider Risk Management para aprovechar el repositorio Microsoft Graph, entre otros servicios, y poder obtener señales de terceros y nativas en tiempo real para identificar los riesgos internos, controlar el anonimato y permitir la colaboración entre TI, RR.HH. y legal.

3. Investigación y reacción con datos relevantes. Microsoft ha llevado a cabo un gran esfuerzo para desarrollar su solución de eDiscovery Avanzado, que proporciona un flujo de trabajo de extremo a extremo para preservar, recopilar, analizar, revisar y exportar contenido para asuntos legales o investigaciones internas de una organización.

4. Simplificar el cumplimiento. La compañía cuenta con su Compliance Manager, que permite evaluar y monitorizar los controles de protección de datos, con la capacidad de puntuación de cumplimiento para reducir los riesgos. Además, ofrece más de 150 plantillas personalizables, para cumplir con las normativas internacionales, locales y sectoriales. En todas ellas, la compañía aplica su experiencia en IA y aprendizaje automático. Se trata de que las organizaciones puedan, incluso, escalar estos procesos y flujos de trabajo, reduciendo, en gran medida, el riesgo.

Modern SOC: aplicando la teoría de la gravedad de los datos para protegerlo todo

Los equipos de seguridad aún están viviendo en 2021 el impacto del repentino cambio al teletrabajo. A la par, las amenazas son constantes y los adversarios han incrementado rápidamente su sofisticación, usando técnicas que dificultan su detección y que ponen en peligro, incluso, a las empresas e instituciones mejor preparadas. Y una vez que los atacantes están dentro, los daños pueden escalar rápidamente.

Modern SOC

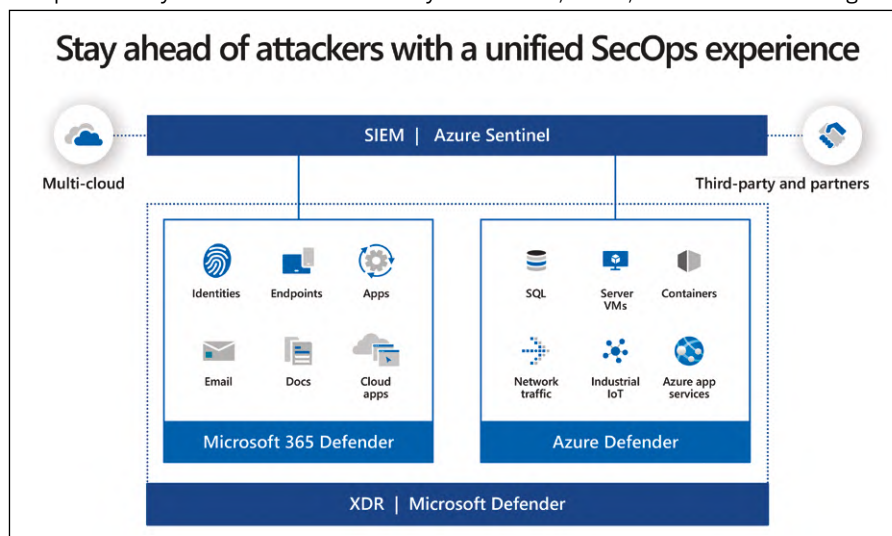
El escenario descrito es un gran reto al que se suma el hecho de que se está redefiniendo el modelo de seguridad hacia a un enfoque Zero Trust. Los principios de Zero Trust obligan a tener una profunda visibilidad de todo el entorno para contar con el mayor contexto posible, analizar una ingente cantidad de señales y automatizar la respuesta. Sin embargo, el SOC tradicional no está preparado para la ingesta y análisis de grandes volúmenes de datos de los actuales escenarios (Cloud, IoT, Zero Trust). A mayor número de señales, más ruido, mayor tiempo de respuesta y, también, mayor dificultad para atender todas las alertas.

Por ello, Microsoft propone implementar un nuevo modelo de SOC (“cloud ready”, “IoT ready” y “Zero Trust ready”) apoyado en las capacidades que la nube ofrece para manejar grandes volúmenes de datos, aplicar analítica avanzada y automatizar procesos. Precisamente, cuando se habla de analizar grandes volúmenes de señales, se tiende a pensar en traerlas todas al SIEM del SOC y aplicar allí la analítica. Una aproximación que Microsoft ve como “poco adecuada” por lo costoso de mover e ‘ingestar’ todos los datos (o en su defecto renunciar a traer todas las señales perdiendo el valioso contexto), y por la latencia introducida en el proceso, que va en contra de una detección y respuesta rápida. Por ello, la multinacional propone apostar por el concepto de la ‘gravedad de los datos’ (‘data gravity’), acuñado por **Dave McCrory**, en 2010. Se basa en considerar que a medida que los conjuntos de datos crecen, son cada vez más difíciles de mover por lo que se quedan estáticos. Frente a esta situación es la gravedad lo que atrae aplicaciones y servicios donde está el dato. ¿Cómo se debe construir un SOC moderno? Pues respetando la ‘ley de data gravity’. Si se puede aplicar la analítica cerca de dónde ya está el dato, se puede incrementar la velocidad de detección y respuesta. Esto no supone

el fin de la agregación. Un SOC moderno realiza una aproximación híbrida, aplicando la analítica tan cerca del dato como sea posible, para luego extender la visibilidad y el conocimiento, en un repositorio central del SOC para el análisis y el conocimiento adicional a lo largo de otros centros de gravedad. Además, hay que incorporar analítica avanzada (ML & UEBA) para permitir a los SOCs modernos detectar peligros que antes pasaban desapercibidos y automatizar la detección y

Al contrario que otras aproximaciones, estas herramientas no trabajan en silos, sino que están ya integradas en la plataforma XDR Microsoft Defender, que cubre dominios como el punto final, la identidad, aplicaciones de colaboración, aplicaciones cloud e infraestructura (almacenamiento, contenedores, redes, VMs, etc.) sea on-premise o multinube.

Adicionalmente Azure Sentinel (SIEM nativo-cloud, SOAR, UEBA & Threat Intelligence



la respuesta de amenazas commodity (autocuración), permitiendo a los analistas centrarse en las tareas de más valor, como el *hunting* de amenazas avanzadas, sólo realizables por humanos.

La propuesta de valor de Microsoft

Partiendo de este planteamiento, Microsoft ofrece una aproximación para modernizar las Operaciones de Seguridad única en la industria a través de una plataforma integrada, apoyada en las potentes capacidades AI/ML que ofrece Azure, y alimentadas por un ingente y diverso número de señales de seguridad de sus plataformas y servicios (*Intelligence Security Graph*).

Así, sus equipos de seguridad definen los modelos analíticos avanzados en base a su conocimiento de los adversarios, modelos que son entrenados y refinados en el *Intelligence Security Graph*. Además, esta analítica avanzada se embebe en cada una de las herramientas de detección y respuesta, y es aplicada cerca del dato o servicio que monitorizan, proporcionando profundidad en la detección, análisis y respuesta a lo largo de múltiples dominios.

Hub) proporciona amplitud en la detección, análisis y respuesta, habilitando un nivel superior de agregación de alertas y señales para mayor contexto, no solo de la plataforma XDR Microsoft Defender sino también de fuentes de terceros y otras nubes, mejorando la fiabilidad de las alertas.

En definitiva, Microsoft ofrece una solución integrada XDR + SIEM (+SOAR, UEBA, TI Hub) que brinda una experiencia de operaciones de seguridad unificada, y proporciona: **Efectividad**, reduciendo drásticamente los tiempos de resolución al eliminar tareas manuales y maximizando el uso de ML y automatización.

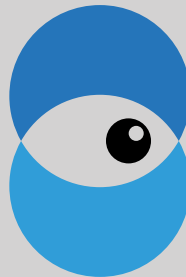
Eficiencia, haciendo un mejor uso del presupuesto de seguridad, consolidando herramientas, reduciendo tiempos de despliegue y optimizando los costes de operación.

Agilidad, a la hora de monitorizar el modelo *Zero Trust* y los entornos modernos que el negocio está fomentando.

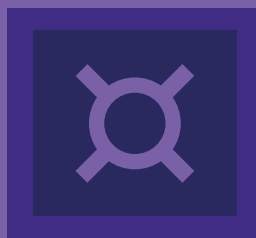
Esta solución integrada no sólo cubre su plataforma, sino que abarca múltiples sistemas operativos y otras nubes, ofreciendo a sus clientes una solución completa a lo largo de todo su ‘estado digital’.



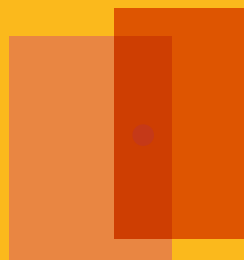
Seguridad inteligente
que mejora tu organización.



Desbloquea la innovación
de manera segura



Transforma los servicios
al ciudadano de manera
segura



Tecnología segura que
mejora los servicios al
paciente.

