Nº 140 Junio 2020
Año XXIX

www.revistasic.com

SiC

Revista
Ciberseguridad, seguridad de la información y privacidad

ENTREVISTA

Jess Garcia
CEO
ONE eSECURITY

PROYECTOS
PROSEGUR

EN CONSTRUCCIÓN
Tras el Cuarto Jinete

ESTRATEGIA
La visión de DXC en un contexto de amenazas creciente

SECURMÁTICA 2020
CISOS:
Cómo están protegiendo sus empresas

¡Tengan cuidado ahí dentro!

TELETRABAJO

LAS
OPORTUNIDADES
YA NO
LLAMAN
A LA
PUERTA.

Somos la compañía que ha innovado digitalmente
a las corporaciones mas exigentes del mundo.
Tu futuro potencial llama a la puerta.
Abrámosla juntos.
Transformación digital por DXC Technology.

dxc.technology/digitaljourney

DXC.technology | THRIVE ON CHANGE.

Proteja su nube con confianza

Una solución completa de seguridad y automatización de cumplimiento de normativas para sus nubes públicas

checkpoint.com/es

Check Point
SOFTWARE TECHNOLOGIES LTD

ARROW V-Valley the Value of esprinet Westcon

SiC
Nº 140
Junio 2020

>> Sumario

>> en este número

• **Securmática.** A tenor de cómo se están desarrollando hasta la fecha la pandemia, las sucesivas prórrogas del estado de alarma y el denominado proceso de "desescalada" en curso, los miembros del equipo organizador de esta reunión profesional han creído prudente reiniciar en pocos días los procesos conducentes a su celebración.

Así pues, en las mañanas de los días 29 y 30 de septiembre y 1 de octubre, y con las medidas sanitarias y de higiene especiales que estén prescritas en esas fechas, tendrá lugar de forma presencial y en su sede habitual del Campo de las Naciones de Madrid, la XXXI edición del Congreso global de Ciberseguridad, Seguridad de la Información y Privacidad, cuyo programa se encuentra disponible en www.securmatica.com.

• **PEPP-PT.** A raíz de la pandemia, en el marco del Pan-European Privacy-Preserving Proximity Tracing se están estudiando en Europa dos propuestas de monitorización automática de proximidad de personas. En dichas propuestas juegan un papel determinante las redes de telefonía celular, los móviles, el *bluetooth* y la criptografía.

No son pocas las voces que se han alzado contra este tipo de iniciativas, principalmente porque pueden vulnerar el derecho a la intimidad. Y lo cierto es que, como todo sistema con base TIC, tendrá vulnerabilidades, y su descubrimiento, aprovechamiento o explotación para fines ilegales, dejaría además en entredicho la salvaguarda del derecho a la protección de datos personales.

En la presente edición de SIC, Jorge Dávila trata con profundidad técnica y crudeza, en su sección "En construcción", el problema que plantean estas iniciativas, especialmente tras el oportuno ofrecimiento de Apple y Google para modificar, respectivamente, iOS y Android.

• **León.** El Gobierno español ha aprobado la candidatura de la ciudad de León para acoger la sede del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Seguridad (European Cybersecurity Industrial, Technology and Research Competence Center). Dicho Centro, junto con la red de centros de competencia prevista, constituye una de las apuestas de la UE en ciberseguridad, área en la que España ocupa una buena posición a través del INCIBE, dirigido hoy por Rosa Díaz y cuya sede se encuentra en la capital leonesa.

A fecha de cierre de esta edición, los países que más han apostado por acoger este Centro, además de España, han sido Bélgica y Rumanía, aunque no se descartan nuevos candidatos como, por ejemplo, Francia, que también ha mostrado interés. La decisión política para elegir la sede se espera que esté tomada antes de final de año para que la Red comience a funcionar en 2021.

• **ENS.** El Centro Criptológico Nacional ha decidido celebrar el 24 de este mes el II Encuentro del ENS. La ocasión lo merece, porque este año el Esquema Nacional de Seguridad ha cumplido 10 años. Cuando se promulgó, su contenido afectaba a la administración electrónica; en su siguiente actualización, allá por 2015, se fijó su alcance al sector público.

Hoy, y con base en la experiencia de su aplicación efectiva (que está siendo más lenta de lo deseable por, entre otras, razones presupuestarias), estamos a la espera del refinamiento de una norma que, ya desde su aparición, fue un hito para la gestión de la ciberseguridad y la protección de la información con espíritu de mejora permanente y ánimo de apoyo a los profesionales, la industria y los servicios especializados.

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:** Eduard Alegre, Carlos Bachmaier, Alejandro Becerra, Santiago Campuzano, Jorge Dávila, Federico de Dios, Vicente de la Morena, Boris Delgado, Raúl Dopazo, Carlos Manuel Fernández, Pablo Fernández, Juan Carlos Gómez, Alejandro González, Paula González, Israel Hernández, Alfonso Martínez, Rubén Muñoz, Mariano Ortiz, Alberto Partida, Ramsés Pascual, Prasanna Kumar, Antonio Ramos, Rafael Rosell, Mikel Salazar, Nelson Sánchez, Daniel Solís, Israel Zapata **Departamento de Marketing/ Publicidad:** Rafael Armisén Gil, Fernando Revilla Guijarro **Administración y suscripciones:** Susana Montero, Maite Montero, Mercedes Casares **Fotografía:** Jesús A. de Lucas **Producción, diseño y maquetación:** MSGráfica **Imprime:** Monterreina **ISSN:** 1136-0623

Identi::SiC

Organiza:

Revista SiC

www.revistasic.com/identisic

Madrid_
14 y 15 de octubre_2020
Hotel Novotel Campo de las Naciones

OSTIA para los políticos

José de la Peña Muñoz
Director
jpm@codasic.com

No sea malpensado el lector: la Ostia del título no va con falta de ortografía. Lamentablemente es sin "h", porque se refiere al acrónimo de la Online Safety Tech Industry Association, entidad constituida en Reino Unido por expertos en ciberseguridad y empresas del gremio con la finalidad, entre otras, de informar a los responsables políticos sobre la ciberseguridad en redes e influir en las políticas y elaboración de regulaciones. El invento cuenta con el apoyo de la GCHQ (Home Department) y del Minister for Digital and Culture. Y eso induce a pensar que OSTIA seguirá sin la "h" si hay suficientes libras esterlinas para financiar iniciativas de interés.

"Ostias" hay en muchos países. Y suelen actuar, con mayor o menor fortuna, a modo de correa de transmisión del motor de la colaboración público-privada.

> "No pocos CISOs y colaboradores, a caballo entre la primera y la segunda línea de defensa –e implacablemente auditados por la tercera–, están desfallecidos por el enorme esfuerzo realizado durante jornadas interminables de teletrabajo".

Apliquémonos esto a nosotros, y formulémonos algunas preguntas; por ejemplo: ¿Cómo andamos en España de "Ostias"? ¿Tenemos una, varias o demasiadas? ¿Qué rasgos diferenciales presenta o presentan? ¿Si no disponemos de ninguna, sería conveniente o no crearla? Ahí queda.

Teleagotados

Mientras reflexionamos sobre el particular, bien merece plantear otras cuestiones de gran interés. Empiezo por la que me parece más humana; a saber: que la mayoría de responsables de seguridad de la información y colaboradores con los que he tenido oportunidad de hablar, a caballo entre la primera y la segunda línea de defensa –e implacablemente auditados por la tercera–, están (literalmente) desfallecidos por el enorme esfuerzo que les está suponiendo culminar jornadas interminables de teletrabajo, en ocasiones a salto de mata. La responsabilidad ante la contingencia, las reuniones y más de doce horas diarias de gestiones en remoto, dejan a cualquiera tocado. Y posiblemente a otras personas de otras áreas de la empresa, les esté sucediendo lo mismo.

Ahora que el Gobierno dice que se propone regular el teletrabajo (no se sabe si mediante una legislación específica o reformando el estatuto de los Trabajadores), merecería la pena que antes de tomar decisiones en el terreno normativo y legislativo con base preponderante en criterios laborales tradicionales, tuvieran en consideración los efectos que el entorno digital tiene o puede tener en las personas (de cualquier generación) y en las organizaciones que dan empleo. Y en las pólizas de seguros.

Expertos

Mientras tanto, aquellos que, pese a vivir en países democráticos, siguen convencidos de que hay que sustituir las leyes por algoritmos, se han topado a raíz de la pandemia con eso que se llama derechos fundamentales. Los más concernidos, como el de la intimidad y el de la protección de datos personales son, a medida que avanza la "transformación", más tangibles. La sustanciación del cumplimiento legal en el aparato tecnológico de la dimensión digital (incluido el que afecta a la ciberseguridad), va a proseguir su escalada, no su "desescalada".

Y en este terreno, hay un detalle que conviene valorar: la ciberseguridad de los productos TIC legales (dejémoslo ahí) tiene que poder verificarse. Para eso están la evaluación y la certificación, que son la apuesta no solo de la UE. Esto significa que los laboratorios de evaluación deben disponer de personal técnico muy experto y muy especializado. Si esto no se puede contrastar, no se les debería dejar operar en el mercado. ●

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

Every breath you take

Luis Fernández Delgado
Editor
lfernandez@codasic.com

Estas fechas tan normalmente anormales a uno le ponen nostálgico. Y ante el inoperante espectáculo de tanto preboste del globo frente a la pandemia, uno no deja de recordar con cariño a los geniales Gila, y Martes y Trece, con sus antológicas citas a "La Guerra" y a la malograda Encarna Sánchez, respectivamente. Y, tirando de imaginario, casi da la risa en medio de esta desoladora coyuntura, evocar sus genialidades pretéritas trasladándolas a la realidad actual, en la que tanto timonel perdido trataría de contactar, cual añorado cómico de casco, con el enemigo y le diría "¿Oiga, es ahí la Covid-19? Sentémonos a hablar" o, autoparódicamente, telefonearía a la estrella radiofónica para decirle: "¿Encarna, cómo están de hechas esas mascaradillas?

Pero lo cierto es que el espectáculo, tan poco edificante, golpea igualmente a nuestro pequeño mundo, ese de la ciberseguridad y, su inseparable compañera de viaje, la privacidad. A fecha de cierre de esta edición, algunos de los principales ministerios de nuestros lares seguían tirándose los trastos a la cabeza por las polémicas apps de trazabilidad, solicitadas de manera precipitada, sin consenso y chapuceramente diseñadas. Su puesta en servicio, de manera caótica y caprichosa, no ha hecho más que inquietar al frágil ecosistema sanitario, temeroso de ser colapsado con inundaciones de falsos positivos. Ya trascenderá en estas fechas la abultada espantada de 'expertos' renuentes a seguir en una secretaría de estado que diseña futuros y que no aprende ni del pasado.

Por cierto, que este caos en pos del rastreador de Fierabrás no se circunscribe solo al ámbito cañí, sino que también en la vecina Francia, por ejemplo, la aplicación descargable "StopCovid", –en modo anónimo *bluetooth* mediante– también viene causando revuelo por su fútil carácter voluntario y por 'tomarse' ciertas libertades improcedentes.

Este fundamentado recelo ante un brumoso despliegue de apps defectuosas 'de fábrica' –no *made in China* precisamente– y su grosera colisión con importantes derechos, como el de la intimidad, parecen abocarnos a una deriva acaso arteramente pergeñada por quién sabe qué intereses (¿gubernamentales? ¿de las *majors* tecnológicas?), tan fascinados ellos por nuestra 'movilidad' y nuestro 'estado físico', augurando tiempos '*riesgosos*' para nuestra salud democrática. Este temor lo aflora de manera muy precisa nuestro colaborador Jorge Dávila en su certero artículo de esta edición, que no hay que perdérselo.

Que sombríamente se nos ciernan nubarrones de vigilancia digital, no es ya solo por la dichosa pandemia sino, además, por ese elefante que estrena cacharrería irrumpiendo desbocado en un *tsunami* telelaboral aún sin contornear.

> "Se nos ciernen nubarrones de vigilancia digital, no ya solo por la dichosa pandemia sino, además, por ese elefante que estrena cacharrería irrumpiendo desbocado en un tsunami telelaboral aun sin contornear".

En este revuelto escenario y a colación de lo hasta ahora expuesto, bien cabe recordar las palabras de Thierry Breton, el comisario europeo de Mercado Interior –con anterioridad ministro francés y Ceo de Atos–, quien, a propósito del 'seguimiento' a los europeos, ha demandado que en estas 'prácticas' hayan la adecuada "anonimización, voluntariedad, descentralización, temporalidad, seguridad y transparencia".

Prosiguiendo con mi nostalgia, y en este desconcierto global de hoy, no dejo de tararear la premonitoria canción de Sting compuesta en 1983: "Every breath you take", interpretada por su emblemática banda –casualmente bautizada como "La Policía"–, resonando en estos días como nunca. Su letra, tal vez, haya invitado a que algunos se la tomaran al pie de la letra, valga la redundancia. He aquí un afamado fragmento:

"Cada aliento que tomes,
cada movimiento que hagas,
cada atadura que rompas, cada paso que des,
te estaré vigilando.
Todos y cada uno de los días,
y cada palabra que digas,
cada juego que juegues,
cada noche que te quedes,
te estaré vigilando.
Oh, ¿no puedes ver que tú me perteneces?"

Inquieta pensar que otros también se estén deleitando con ella pero por otros motivos, antagónicos a nuestro legítimo derecho a que exista una supervisión legal y garantista de este asunto y haga buena la lapidaria sentencia de Jeremy Bentham: "Cuanto más te observo mejor te comportas". ●


CITRIX®
¿Te preocupa el trabajo en remoto?
Prepara y capacita a tus empleados
Más información en citrix.es

El Gobierno aprueba la candidatura de León como sede del Centro europeo de Competencia en Ciberseguridad

El Consejo de Ministros, en su reunión de 2 de junio, ha aprobado la candidatura de la ciudad de León para acoger la sede del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Seguridad (European Cybersecurity Industrial, Technology and Research Competence Center).

El Centro Europeo de Ciberseguridad es un instrumento de la UE para poner en común las investigaciones en materia de ciberseguridad, un área en la que España ocupa una posición de referencia a través del Instituto Nacional de Ciberseguridad (INCIBE), dirigido por **Rosa Díez** y cuya sede se encuentra en León.

Precisamente, el Centro Europeo de Ciberseguridad reforzaría a León, a la comunidad autónoma de Castilla y León, y a España como un 'Cibersecurity Innovation Hub' a nivel europeo, ya que, en la actualidad, la ciudad es ya un importante nodo en materia de tecnologías de la información y ciberseguridad.

Tanto la Red de Competencia en Seguridad Cibernética de la UE como la elección del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Seguridad (con base en la denominada "ley" de Ciberseguridad de la UE de 2019) se ha puesto en marcha, de nuevo, en junio, basándose en una nueva propuesta que, entre otros aspectos, es más flexible en lo que toca a cómo financiará la sede el país que la albergue, ya que se calcula que podría rondar los 90 millones de euros.

De momento, los países que más han apostado por acogerlo, además de España, han sido Bélgica y Rumania, aunque no se descartan nuevos candidatos como, por ejemplo, Francia, que también ha mostrado interés.

La decisión política para elegir la sede, se espera que esté tomada antes de final de año para que la Red comience a funcionar en 2021.

INCIBE pone foco, en sus nuevas guías, en cómo notificar incidentes correctamente y usar dispositivos IoT de forma segura

El **CERT del Instituto Nacional de Ciberseguridad** (**Incibe**) ha actualizado su 'Guía Nacional de Notificación y Gestión de ciberincidentes', con el objetivo de ofrecer a cualquier entidad, pública o privada, ciudadano u organismo, un esquema y la orientación precisa acerca de a quién y cómo debe reportar un incidente de ciberseguridad.

La guía proporciona a los Responsables de Seguridad de la Información las directrices para el cumplimiento de las obligaciones de reporte de ciberincidentes ocurridos en el seno de las Administraciones Públicas, las infraestructuras críticas y los operadores estratégicos de su competencia, así como en el resto de entidades comprendidas en el ámbito de aplicación del Real Decreto-Ley 12/2018, de seguridad de las redes y sistemas de información.

Como complemento a esta actualización, Incibe-Cert también publicó un anexo sobre su documento 'Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía', con la intención de servir de apoyo en dichas tareas y como referencia de qué mecanismos y canales hay que usar para notificar posibles amenazas al **Centro de Respuesta a Incidentes de Seguridad** de Incibe, cuando sea necesario.

Impulso a la formación

Además, el Instituto actualizó en abril sus publicaciones sobre formación en ciberseguridad a nivel nacional. En concreto, el 'Catálogo de másteres en ciberseguridad en España' recopila un total de 72 programas de máster y cuatro grados, mientras que el 'Catálogo de instituciones que ofrecen formación en ciberseguridad en España' reúne 129 centros donde se puede realizar algún estudio en ciberprotección, en varias modalidades.

También presentó su nueva guía 'Seguridad en la instalación y uso de dispositivos IoT', que recoge las principales medidas de seguridad que una empresa debe incorporar para reducir riesgos. Entre sus recomendaciones prioritarias están desde la utilización de criptografía para proteger la información, hasta la necesidad de implementar programas de actualizaciones automatizadas y gestión de parches de seguridad.

La AGENCIA DE CIBERSEGURIDAD DE CATALUÑA renueva su imagen tras su puesta en marcha por el Govern

La **Agencia de Ciberseguridad de Cataluña**, antiguo **Cesicat** (Centro de Seguridad de la Información de Cataluña), ha estrenado una imagen corporativa acorde al cambio de marca, tras su puesta en marcha el 1 de enero y después de que el Gobierno catalán diera luz verde a su creación en octubre de 2019. La Agencia, que absorbió los activos y el personal del Cesicat y pasó de ser una Fundación a ser una agencia gubernamental, tiene entre sus objetivos prevenir y detectar incidentes de ciberseguridad, garantizar la protección de la Administración catalana, ejercer las funciones de equipo de respuesta a emergencias (CERT) e impulsar una cultura de ciberseguridad de ámbito nacional.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

En este compromiso, "es necesario que la nueva Agencia de Ciberseguridad de Cataluña se dote de una nueva identidad visual propia, que permita la interlocución con sus públicos: instituciones, empresas, ciudadanía, administraciones locales, universidades, así como otros centros de ciberseguridad y organismos de ciberseguridad de ámbito internacional", aseguran desde la Agencia a través de un comunicado.

La nueva marca, alineada con el Programa de Identificación Visual (PIV) de la Generalidad de Cataluña, debe permitir, por tanto, "potenciar la Agencia como un referente nacional e internacional en el ámbito de la ciberseguridad".

tranxfer | secure file exchange

La forma más segura y sencilla de enviar y recibir archivos

Evita los riesgos de ciberataque y pérdidas de información propios de los entornos colaborativos y del shadow IT

- Identificación unívoca de los archivos
- Prevención de malware entrante
- Encriptación end-to-end
- Antivirus y DLP
- Doble factor de autenticación
- Eliminación automática de los archivos
- Integración en los sistemas corporativos

Establece con Tranxfer el canal corporativo seguro de entrada y salida de ficheros

Powered by:

aws

Google Cloud Platform

Microsoft Azure

Made in EUROPE

También se considera prioritario poner en marcha una identidad digital europea

La UE desarrollará la nueva Estrategia de Ciberseguridad integrada con el plan 'Next Digital' para contar con hegemonía tecnológica

Para hacer frente a las consecuencias de la pandemia de la Covid-19, la Comisión Europea presentó, a finales de mayo, un amplio plan de recuperación bajo el nombre **'Next Generation EU'.** Tendrá una dotación específica de 750.000 millones y formará parte de un ambicioso plan de inversión a largo plazo, hasta 2027, en todo tipo de campos, por valor de 1,85 billones de euros. Su objetivo será ayudar a los estados a recuperarse, relanzar la economía y apoyar la inversión privada, aprendiendo de las experiencias puestas en marcha para hacer frente a la crisis sanitaria, una iniciativa en la que tendrá un peso especial la ciberseguridad para contribuir a dar "forma al futuro digital de Europa". En concreto, el documento aprobado por la Comisión, bajo el título "El momento de Europa: Reparar y prepararse para la próxima generación" dedica en su capítulo cuarto, un amplio apartado a lo digital y la ciberseguridad bajo el título "Un mercado único más profundo y digital**".** En él resalta que la pandemia ha evidenciado la "importancia de la digitalización en todas las áreas de la economía", reconociendo que esta situación, a la larga, provocará "cambios permanentes y estructurales en la vida social y económica" popularizando el teletrabajo, la formación en línea, el comercio electrónico y la Administración digital. Por eso, considera prioritario importante, "desarrollar una identificación electrónica universalmente aceptada" y que Europa cuente con una "identidad digital pública que permita un acceso simple, confiable y seguro a los servicios públicos digitales transfronterizos".


EUROPEAN COMMISSION

Brussels, 27.5.2020
COM(2020) 456 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Europe's moment: Repair and Prepare for the Next Generation

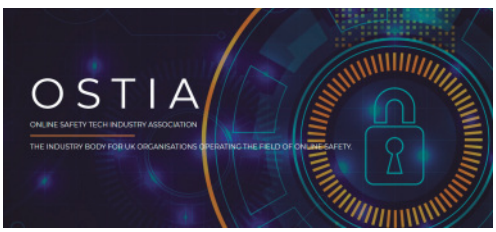
{SWD(2020) 98 final}

Para la recuperación digital el documento fija cuatro pilares: en primer lugar, invertir más y mejor en conectividad, impulsado el despliegue de las redes 5G –antes del 30 de junio los estados presentarán sus propuestas para hacerlo seguro–. En segundo, mejorar la presencia industrial y tecnológica en aspectos estratégicos, teniendo especial relevancia la "seguridad de la tecnología". Precisamente en este punto destaca que la inversión para la recuperación se canalizará hacia capacidades digitales estratégicas, incluyendo la inteligencia artificial, la ciberseguridad, las comunicaciones seguras, las infraestructuras de datos y la nube, así como las tecnologías cuánticas y el *blockchain*, entre otras. Además, en tercer lugar, se considera importante "construir una economía de datos reales como motor de innovación y creación de empleo", avanzando la aprobación de una Ley de Datos que dé respuesta a las necesidades existentes.

Finaliza avanzado que, para hacer frente a los ciberataques, se creará una nueva **"Estrategia de ciberseguridad"** que estudiará "cómo impulsar la cooperación, el conocimiento y la capacidad en este campo en la UE". Entre sus retos está que deberá ayudar "a Europa a fortalecer sus capacidades industriales y asociaciones, y alentar la aparición de nuevas pymes en la industria de ciberseguridad". Esta estrategia también será acompañada de "la revisión de la Directiva sobre seguridad de redes y sistemas de información (NIS)", así como de una "propuesta de medidas adicionales sobre Protección de Infraestructuras Críticas". Y es que la Comisión ve vital "asegurar la red y los sistemas de información en la UE para mantener en funcionamiento la economía en línea y garantizar la prosperidad", cobrando especial importancia el concepto de ser, digitalmente, ciberresilientes ante crisis cibernéticas a gran escala.

Se crea en Reino Unido la asociación OSTIA para asesorar a los políticos de cómo mejorar la ciberprotección

Con el apoyo de la **Agencia Nacional contra el Delito** (**GCHQ**), del **Ministerio del Interior** (NSPCC) y liderada por **Cyan Forensics y Public**, una asociación de analistas expertos en ciberseguridad y empresas del sector, se ha presentado en Reino Unido la **Asociación de la Industria de Tecnología de Seguridad en Línea** (**OSTIA**), que une analistas expertos y empresas innovadoras con la misión conjunta de mejorar la seguridad en línea.



La iniciativa, que ha contado con el respaldo de la Ministra de Estado del área Digital y Cultura del Departamento de Digital, **Caroline Dinenage**, se centrará en tres objetivos: "proporcionar una voz de esperanza informando a los responsables políticos, a los proveedores de tecnología y al público en general sobre las tecnologías de seguridad en línea, influir en las políticas y la regulación al respecto, de forma que esté apoyada por el sector, y proporcionar un foro de encuentro para las empresas que buscan la ciberseguridad *online*".

Nace una alianza de expertos para proteger los hospitales y a los sanitarios de los ciberataques derivados de la Covid-19

La firma de inversión británica, **C5 Capital,** especializada en compañías de seguridad de datos, ha impulsado una alianza de empresas para proteger a los hospitales y al sistema de salud de varios países europeos, incluido España, del incremento de ciberataques que se han producido (hasta un 150%), sobre todo, al principio de la pandemia, contra instalaciones hospitalarias. La iniciativa, denominada **'Ciberalianza para defender nuestra atención sanitaria'** ('Cyber Alliance to Defend our Healthcare') es proteger "los sistemas sanitarios, a los proveedores de servicios de salud y los laboratorios frente a los actores maliciosos".

Además de ayudar a parar las amenazas, también ofrecen buenas prácticas y consejos de ciberprotección para actuar de forma segura en sus dispositivos de trabajo y en las redes corporativas. De momento, la alianza ya ha llegado a acuerdos con casi 90 entidades sanitarias, además de cinco servicios de salud nacionales (de España, Italia, Reino Unido, Alemania y Suecia), y su siguiente objetivo es ampliar estos acuerdos a entidades de Estados Unidos. Además, también forman parte de la iniciativa diversas organizaciones de seguridad como son **ITC Secure, IronNet Cybersecurity, Haven Cyber Technologies, Enveil, 4iQ, Blue Cedar, Hazelcast, SAP NS2, Modex, Telos, OneVinn, TruSTAR Technology, Privitar, Cynamics, SOSA's Global Cyber Center** y **Klaatu IT Security.**

Proteja a su organización ante el riesgo de amenazas internas.

El 52% de los incidentes de seguridad son originados por los propios empleados, habiéndose duplicado su coste en los últimos 3 años.

Proofpoint Insider Threat Management facilita a los equipos de seguridad la detección de amenazas internas, simplifica la investigación y protege frente a la fuga de datos.

Más información sobre ObserveIT Insider Threat Management, contacte con nosotros **info-spain@proofpoint.com**.

proofpoint. | La protección empieza por las personas

También prohibirá la compra de equipos extranjeros para la red eléctrica a fin de evitar incidentes

EE.UU. aprueba una inversión de casi 2.400 millones de euros en ciberseguridad para 2020-2021, buscando más protección, incluso, en el Espacio

Estados Unidos tiene la ciberseguridad como una de sus grandes prioridades estratégicas y ello abarca todo tipo de campos, incluso, el espacial, donde la recién creada **Fuerza Espacial de los Estados Unidos** (USSF) ha abierto una oferta de empleo entre las que hay numerosas plazas para expertos en ciberprotección.

A ello se suma que su Presidente, **Donald Trump,** firmó en mayo una orden ejecutiva para evitar los riesgos ante las posibles amenazas extranjeras al sistema eléctrico del país en caso de "emergencia nacional". A través de ella, el gobierno prohíbe "la adquisición, importación, transferencia o instalación" de equipos de electricidad que sean fabricados por gobiernos extranjeros. "El sistema de energía masiva es un objetivo de aquellos que buscan cometer actos maliciosos contra Estados Unidos y su gente, incluidas actividades cibernéticas peligrosas", destaca la orden ejecutiva.

La medida cuenta con 150 días de estudio, ya que tiene que ser puesta en marcha por el Secretario de Energía, **Dan Brouillette,** coordinándose con los secretarios de Defensa y Seguridad Nacional, el Director de Inteligencia Nacional y los jefes de otras agencias, tras lo que se publicarán los reglamentos que implementen la orden. Algo similar a lo que se aprobó en 2019, prohibiendo la compra de equipos extranjeros para desplegar las redes 5G en el país.

Éstos son dos de los ejemplos que dan cuenta de la importancia que está cobrando este campo en el país. De hecho, para el año fiscal 2020-2021, el Departamento de Seguridad Nacional (DHS) propuso un gasto en ciberprotección de 2.343 millones de euros, el segundo presupuesto más grande para las agencias gubernamentales.

De esa cantidad la mayor partida es para el Departamento de Defensa (DoD), con una solicitud de 8.857 millones de euros.

Estrategia Nacional de Ciberseguridad

El país ha incrementado notablemente la inversión en protección cibernética desde que en 2018 la Casa Blanca aprobara su nueva Estrategia Nacional de Ciberseguridad. Sin embargo, excepto el DoD, el resto de agencias podrían sufrir recortes presupuestarios en esta materia. De cualquier forma, se pasaría de una inversión por parte de la Administración de 15.426 millones de euros en 2019 a 17.111 en 2020. La razón es que las agencias federales son uno de los grandes objetivos de los ciberataques en el país con más de 31.107 incidentes cibernéticos reportados en 2018, y un 5,6% de las brechas que comprometieron datos.

GASTO PREVISTO EN LA ADMINISTRACIÓN DE EE.UU. EN CIBERSEGURIDAD PARA 2020/2021
(en millones de euros)

	2020	2021
Departamento de Agricultura	207,7	206,8
Departamento de Comercio	462,3	340,1
Departamento de Defensa	9.063	8.857
Departamento de Educación	149,3	145,7
Departamento de Energía	494,6	598,08
Departamento de Salud y Servicios Asistenciales	427,3	466,9
Departamento de Seguridad Nacional	2.315	2.343
Departamento de Vivienda y Desarrollo Urbano	61,2	62,08
Departamento de Justicia	809,8	835,9
Departamento de Trabajo	82,7	80,1
Departamento de Estado	365,4	439,3
Departamento del Interior	109,1	119,7
Departamento de Tesorería	529,3	620,2
Departamento de Transporte	235,8	224,2
Departamento de Asuntos de Veteranos de Guerra	472,6	414,2
Agencia de Protección Ambiental	28,9	42,3
Administración de Servicios Generales	73,9	71,2
Administración Nacional de Aeronáutica y del Espacio	149,5	147,5
Fundación Nacional de Ciencia	203,5	190,8
Comisión de Regulación de la Energía Nuclear	24,5	23,6
Oficina de Administración de Personal	42,3	48,6
Administración de Pequeños Negocios	13,6	14,4
Administración de la Seguridad Social	186,5	184,6
Agencia de los Estados Unidos para el Desarrollo Internacional	37,9	38,8

© Statista 2020

BREVES

■ **El Instituto Nacional de Estándares y Tecnología**, de EE.UU., está buscando empresas y asociaciones que permitan implementar estándares de ciberprotección en la tecnología de redes de quinta generación para publicar un documento con las mejores prácticas. "El resultado esperado demostrará cómo los componentes de la arquitectura 5G pueden proporcionar capacidades de seguridad para mitigar los riesgos identificados y cumplir con los requisitos de cumplimiento de los sectores de la industria", destaca el NIST, que contará con un presupuesto de casi 1,1 millones de euros para ello. Este proyecto conformará una 'Guía de Prácticas de Seguridad cibernética NIST', que se plasmará en una serie de publicaciones especiales y una guía de implementación, detallada, con los pasos prácticos necesarios "para implementar la seguridad cibernética".

■ **Marco de teletrabajo para la Administración**. Las Agencias federales, de EE.UU., centradas en TI y seguridad, están elaborando un marco de trabajo y casos de uso con las mejores prácticas de ciberprotección para los empleados federales que teletrabajan y precisan de un acceso remoto seguro para su labor. Una política de seguridad que ha sido denominada '*Trusted Internet Connection 3*'. De momento, la **Agencia de Seguridad de Ciberseguridad e Infraestructura** (**CISA**) ha emitido varios borradores con una posible arquitectura de referencia. Su objetivo es crear lo que se denomina como "zonas de confianza". Sin embargo, estas primeras sugerencias también han despertado críticas frente a lo que algunos creen que debería ser el camino aplicando el concepto de 'Confianza Cero'.

■ **La Oficina del Censo** estadounidense ha publicado recientemente una '**solicitud de información'(RFI)** para comenzar a estudiar las compras que precisará en ciberseguridad, en la próxima década, para transformarse digitalmente, ya que a pesar de su centenario de vida quiere informatizar sus registros para lo que se calcula que destinará 14.200 millones de euros, siendo consciente de que ello también conllevará nuevas vulnerabilidades. El documento de la Oficina del Censo destaca, por ejemplo, que la Oficina es consciente de que "mediante el uso de la inteligencia artificial y el aprendizaje automático de próxima generación, el objetivo es establecer una conciencia situacional casi en tiempo real de la tecnología de alto valor y los activos de información".

The Capgemini Effect

Capgemini

When customers **trust** your cibersecurity, business runs more **efficiently**

#trusticient

La autoridad de control recibió y analizó 95 notificaciones de incumplimiento, en 2019

El SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS evalúa y alerta de que hay demasiados fallos en la aplicación del RGPD en las instituciones de la UE

A pesar de que la administración debería ser la primera en dar ejemplo en cumplir las normativas que se aprueban, lo cierto es que aún queda mucho por hacer en el entorno comunitario. Así lo destaca el Informe Anual, de 2019, del **Supervisor Europeo de Protección de Datos** (**SEPD**), en el que analizó si las instituciones y organismos de la Unión Europea respetaron las principales normativas vigentes tanto de privacidad como de protección de datos, incluyendo el Reglamento 2018/1725, sobre el tratamiento seguro de datos personales por parte de las instituciones, órganos y organismos de la UE.

Violaciones de datos personales

El informe, en el que se destaca el trabajo del SEPD junto con los Oficiales de Protección de Datos (DPO) en las instituciones de la UE, explica que el año pasado el organismo recibió y evaluó 95 notificaciones de incumplimiento de datos personales, la gran mayoría relacionadas con brechas de confidencialidad. Exactamente un 62% se debieron a un error humano, seguidas de las de fallos técnicos (13%) y las causadas por ciberataques (9%). "En 24 casos, el controlador informó a las personas interesadas", puntualiza el informe.

El SEPD también detalla los resultados de su primera ronda de inspecciones remotas de las web de las instituciones europeas, destacando que varios de ellas no cumplían con el Reglamento 2018/1725, ni con las disposiciones aplicables de la Directiva sobre privacidad electrónica. Es más, tampoco seguían las Directrices del SEPD sobre servicios web. Entre los problemas encontrados destaca el seguimiento de terceros a los usuarios, sin consentimiento previo, lo cual es particularmente problemático en los casos de empresas cuyo modelo de negocio se basa en la elaboración de perfiles de usuarios y de sus comportamientos en los sitios web. Además, el SEPD resaltó la buena colaboración en su trabajo con la **Junta Europea de Protección de Datos** (EDPB) para proporcionar y apoyar las iniciativas destinadas a garantizar la aplicación del RGPD en toda la UE. Fruto de ello, emitieron el primer dictamen conjunto sobre el procesamiento de datos de pacientes y el papel de la Comisión dentro de la infraestructura del Servicio Digital de eSalud (eHDSI).

50 millones para ciberseguridad y privacidad

Por otro lado, la UE destinará cerca de 49 millones de euros para impulsar la innovación en sistemas de ciberseguridad y privacidad. A finales de mayo anunció que dedicaría casi 41 millones de euros, a través de 'Horizonte 2020', para apoyar nueve proyectos de soluciones innovadoras de ciberseguridad y privacidad. Cinco de ellos se centrarán en soluciones para ciudadanos y pymes y los otros cuatro buscarán mejorar los sistemas de seguridad críticos, como las infraestructuras sanitarias y los sistemas de transporte multimodal. Además, se financiarán 21 proyectos de ciberseguridad a través del Mecanismo Conectar Europa (CEF), con un total de 7,6 millones de euros. Las solicitudes se admitirán hasta agosto.

FIRST actualiza los principios de coordinación y divulgación de vulnerabilidades que afectan a múltiples partes

El **Foro de Respuesta a Incidentes y Equipos de Seguridad** (**FIRST**), que reúne a un amplio número de CERTs internacionales para el intercambio de información y la cooperación, ha publicado un conjunto actualizado de principios de coordinación y divulgación de vulnerabilidades para mejorar la comunicación entre las diferentes partes afectadas cuando ocurre un problema de seguridad.

Hasta ahora, sus recomendaciones y guías de actuación se habían centrado, principalmente, en la coordinación bilateral, es decir, entre un investigador de seguridad y un proveedor. Por ello, este documento, elaborado junto con la **Administración Nacional de Telecomunicaciones e Información** (**NTIA**), está dirigido a mejorar la comunicación de vulnerabilidades que afectan a varios proveedores y tecnologías al mismo tiempo (como ocurrió con el grave fallo de seguridad HeartBleed), a través de mejores prácticas, políticas y métodos actualizados. Y es que, en una primera versión del texto, según explica el FIRST, "no se abordaron de forma adecuada las complejidades actuales de la coordinación de este tipo de comunicaciones".

Las recomendaciones incluyen el establecimiento de relaciones sólidas entre las partes interesadas y los investigadores mediante la publicación de "políticas y expectativas de divulgación y coordinación de vulnerabilidades públicas 'accionables', incluidos plazos y umbrales para la comunicación".

CHINA impone nuevas medidas de evaluación para la compra de equipos tecnológicos extranjeros, para reforzar su seguridad nacional

En un movimiento para reforzar la ciberseguridad del país, **China** ha implementado nuevas reglas para adquirir equipos tecnológicos que requieren que los operadores de infraestructura de información crítica se sometan a una revisión de cualquier producto o servicio tecnológico que pueda afectar a la seguridad nacional.

Las nuevas normas fueron anunciadas por la **Administración del Ciberespacio China** (CAC), en abril, y entraron en vigor este 1 de junio dentro de la Ley de Ciberseguridad del país.

El gobierno chino define los operadores de infraestructura de información crítica a aquellas empresas que se incluyen dentro de los sectores energético, telecomunicaciones, transporte, finanzas, defensa, gestión militar, así como la computación en la nube, *big data* e Internet de las Cosas.

Según la nueva regulación, estas empresas deben presentar documentos de adquisición, acuerdos de compra y un análisis del impacto potencial de la seguridad nacional del acuerdo para su revisión por parte del gobierno antes de firmar un contrato. Se espera que un proceso de revisión tarde entre 45 días hábiles y tres meses. La normativa no ha estado exenta de críticas, ya que que las compañías chinas pueden comprar productos locales en lugar de correr el riesgo de recibir largas revisiones, situando los productos tecnológicos extranjeros en desventaja. Además, la redacción de esta regulación dice que el gobierno chino considerará "factores políticos, diplomáticos y comerciales".

¿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?

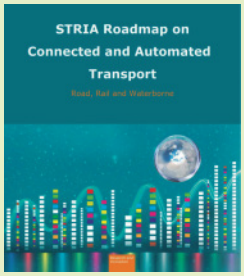
Somos Ciberseguridad OT e IoT, Confíe en oylo

hello@trustoylo.com

El proyecto piloto contará con 70 especialistas de marcas, organismos y centros de investigación de toda la UE

La protección de los sistemas de transporte inteligente, una prioridad para la COMISIÓN EUROPEA

La **Comisión Europea** ha creado un subgrupo de trabajo que buscará desarrollar procesos comunes de ciberseguridad en infraestructuras y vehículos del llamado 'transporte inteligente' que, entre otras capacidades, puedan interactuar de forma colaborativa. Para ello, se pondrá en marcha un programa piloto en toda la UE en el que se buscarán protocolos y procesos para contar con comunicaciones seguras y confiables tanto entre los vehículos, como con los equipos de su entorno (carretera, sistemas de señalización, etc). La idea es que tanto el conductor como los propios transportes cuenten, de forma automatizada, con información y mensajes que les permitan actuar con mayor seguridad y, también, se mejore la gestión del tráfico.



Por eso, este subgrupo también servirá como foro para intercambiar experiencias ya realizadas (fabricantes como Volvo o Mercedes tienen varios programas en marcha desde hace años), y acordar un conjunto de buenas prácticas en el campo de los Sistemas Cooperativos de Transporte Inteligente (C-ITS), como destaca el llamamiento de la UE para crear el grupo de expertos.

En principio, según explica el documento, estará formado por un máximo de 70 expertos pertenecientes a autoridades nacionales y locales de los estados miembros, así como especialistas de marcas de vehículos, de suministradores de equipos de este tipo, organizaciones independientes y centros de investigación. En definitiva, de las principales entidades que estén trabajando alineadas con la Estrategia Europea sobre Sistemas de Transporte Cooperativo e Inteligente.

Asesorar a la Comisión

La idea es que este foro se convierta en uno de los principales asesores de la Comisión en las áreas relacionadas con los C-ITS para permitir identificar nuevos requisitos (funcionales, técnicos, de seguridad y legales), que se pueden utilizar para garantizar que los servicios de C-ITS funcionen sin interrupciones y bajo los protocolos del llamado Sistema de Gestión de Credenciales de Seguridad de C-ITS de la UE (CCMS de la UE), con el fin de garantizar la máxima protección. Por eso, entre sus labores también estará apoyar la implementación de cualquier cambio que mejores los requisitos (en el certificado y en las políticas de seguridad) para poner en marcha los sistemas C-ITS y los CCMS.

Para tener un carácter eminentemente práctico también se prestará especial atención a los incidentes que se ya se produzcan en este tipo de entornos, de alta gravedad, y que puedan impactar en todo el sistema de confianza C-ITS (por ejemplo, una situación de 'recuperación de desastres' donde el algoritmo criptográfico está comprometido).

Por último, está previsto que juegue un papel activo en la redacción, publicación y mantenimiento de la Política Europea de Seguridad C-ITS (SP) y la Política de Certificado C-ITS (CP), además de tomar parte en el desarrollo de la infraestructura de clave pública para estos entornos, incluyendo desde su definición, hasta su plasmación final y la publicación de los de auditoría de la **Autoridad de Certificación y Certificación** (CA) de la Declaración de Práctica del Certificado (CPS), que permiten validar los equipos, procesos y tecnologías que se implementen para garantizar la máxima seguridad.

VMWARE crea una 'Alianza SOC de nueva generación' para mejorar las capacidades y visión de los entornos de los equipos que trabajan en ellos

Con el fin de desarrollar mejores capacidades y contexto a los equipos que trabajan en los Centros de Operaciones de Ciberseguridad (SOC), **VMware** ha impulsado la creación de la 'Alianza SOC de Nueva Generación',de la que forman parte compañías como **Splunk, IBM Security, Google Cloud's Chronicle, Exabeam** y **Sumo Logic,** entre otras, que integrarán en ella sus tecnologías.

"La alianza aportará una masa crítica de contexto y capacidades XDR (*eXternal Data Representation*) a los SOC, de una forma totalmente intrínseca", ha explicado el Vicepresidente de Alianzas para VMware Carbon Black, **Tom Barsi**. "En asociación con los principales actores SIEM/SOAR de la industria, estamos estableciendo una fuerte visión para el SOC moderno, ofreciendo más visibilidad y capacidades de remediación a través de *endpoints*, redes, cargas de trabajo y contenedores".

Su idea es que, a través de la alianza, los equipos de los SOC puedan también aprovechar la red de VMware, simplificando la gestión de su trabajo con numerosas herramientas y productos en sus labores de prevención, detección y respuesta, y disponiendo de un "contexto mucho más rico sobre la infraestructura y las aplicaciones que se protegen". Además, mejorará la eficacia de los expertos del SOC gracias a que contarán con más herramientas de automatización y orquestación que, junto a las capacidades XDR, permitirá escalar y estandarizar sus procesos de investigación y respuesta.

CYBEREASON desembarca en España ofreciendo su plataforma de defensa, basada en la nube

La multinacional estadounidense, **Cybereason** acaba de abrir oficinas en España, tras un fuerte crecimiento en EMEA (Europa, Oriente Medio y África), donde ha duplicado sus ingresos en sólo un año. Al frente de la filial ibérica estará un ejecutivo con amplia experiencia en compañías del sector y en su arranque en el mercado ibérico, **Vesku Turtia**.

Cybereason ofrece servicios de prevención, detección, respuesta y vigilancia activa ante ciberataques a través de su plataforma de protección de puntos finales (EPP), basada en una nube propia, para dar una prevención de extremos de múltiples capas utilizando distintas técnicas para evitar amenazas conocidas y desconocidas, a la vez que pone en funcionamiento técnicas de comportamiento y engaño para responder a ataques de *ransomware* y de *malware* sin archivos. "Nuestra tecnología protege de las constantes amenazas cibernéticas a algunas de las marcas más importantes de la región, ayudando a nuestros clientes a encontrar y eliminar brechas más rápido que cualquier otra plataforma en el mundo", explicó en su presentación en España el CEO de la compañía, **Lior Div**.

Entre sus recientes novedades destaca Cybereason Mobile, una herramienta basada en la nube, diseñada para ayudar a las empresas a prevenir, detectar y responder tanto a los riesgos de los dispositivos móviles, como a los de los puntos finales tradicionales. Se ha presentado junto con su nuevo Mobile MDR contra amenazas móviles, totalmente gestionada y creada para detectar y prevenir actividades sospechosas antes de que se produzcan daños.

bidaidea

CYBERSECURITY &
INTELLIGENCE

- Líderes en infraestructuras críticas
- Líderes en convergencia IT / OT/ IoT
- Transformación digital de la seguridad
- Inteligencia en materia de Ciberseguridad

- Servicios de Inteligencia
- GRC & BC
- Auditoría Técnica
- Centro de Servicios 24x7 (iSOC)
- Industria 4.0 (iLAB)
- I+D+i
- Productos Especializados
- Outsourcing
- Formación y Concienciación

España – Portugal – Brasil – México – Colombia - Perú

Telf +34 918 71 93 59 – info@bidaidea.com

El MANDO CONJUNTO DE CIBERDEFENSA dará paso al del CIBERESPACIO

El **Ministerio de Defensa** ha acometido una reorganización de la estructura de las Fuerzas Armadas (FAS) "hacia un modelo centrado en el conocimiento y las personas" y teniendo en cuenta que una "adecuada transformación digital debe permitir a las Fuerzas Armadas gestionar y distribuir convenientemente la información, así como mejorar la eficacia y agilidad interna".

Entre otras novedades, en el Real Decreto aprobado por el Consejo de Ministros el pasado 19 de mayo, destaca que en esta nueva estructura hay que "fomentar el desarrollo de capacidades y talento en el personal militar que forma parte de ella, de manera que se aprovechen al máximo las nuevas tecnologías digitales y se logre la debida adaptación al cambio para estar siempre en vanguardia".

Además, el **Mando Conjunto de Ciberdefensa**, encuadrado en el Estado Mayor de la Defensa (EMAD), modifica su denominación y pasa a ser del **Ciberespacio,** encargado de "la dirección, coordinación, control y la ejecución de las acciones conducentes a asegurar la libertad de acción de las FAS en el ámbito ciberespacial", siendo de su responsabilidad planear, dirigir, coordinar, controlar y ejecutar las operaciones militares en el ciberespacio y, en este ámbito, las acciones necesarias para garantizar la supervivencia de los elementos físicos, lógicos y virtuales críticos para la Defensa y las FAS".

La modificación que, al cierre de esta edición estaba pendiente de ser desarrollada y publicada en el BOE, podría conllevar no sólo el cambio de nombre sino, también, nuevas atribuciones o la

integración en el Mando de otros departamentos de Defensa. Además, supondría considerar a esta unidad como un 'mando componente' con lo que actuaría, en los ejercicios de entrenamiento, al mismo nivel que Tierra, Armada y Aire. Eso sí, al parecer, el logotipo se mantendrá con su imagen actual, simplemente adaptando sus iniciales a la nueva denominación.

AIUKEN prosigue su expansión en Arabia Saudí para consolidarse como referente en Oriente Medio

A pesar de las fuertes restricciones que ha generado la pandemia de la Covid-19 a nivel mundial, la multinacional española, **Aiuken Cybersecurity** continúa con su plan de crecimiento a nivel internacional con el objetivo de ampliar su presencia, especialmente, en la región de Arabia Saudí, entre otros mercados internacionales ampliando también su equipo de especialistas.

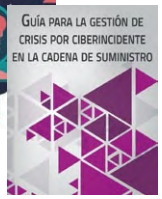
Fuentes de la compañía, que ya cuenta con una fuerte presencia en Kuwait, Bahrein y Emiratos Árabes Unidos (UAE), han explicado su apuesta por reforzar las operaciones que lleva a cabo en Arabia Saudí, incrementado su actividad a diferentes ciudades del país desde su sede en Riyadh, donde también alberga uno de los ocho Centros de Operaciones de Seguridad (SOC) que ha abierto a nivel mundial. Para apoyar este crecimiento, Aiuken incorporará a su plantilla, tanto a nivel nacional como internacional, casi una decena de profesionales y expertos para reforzar las áreas de preventa, ciberinteligencia, así como de sus Centros de Operaciones de Ciberseguridad (SOCs), sumándose así a los más de 110 ingenieros de ciberprotección certificados con los que ya cuenta. "Seguir con los planes trazados, nos permite encarar esta situación actual como un desafío.

Juan Miguel Velasco

Las empresas deben continuar con sus objetivos estratégicos, en materia de seguridad, y nosotros, más que nunca, tenemos la obligación de acompañarlos y ofrecerles nuestros mejores profesionales y nuestra tecnología innovadora", ha comentado su CEO, **Juan Miguel Velasco**.

Presentadas la "Guía de Buenas Prácticas en Auditorías RGPD" y la "Guía de Gestión Crisis Ciberincidentes en la cadena de suministro"

La Asociación **ISMS Forum** ha presentado dos amplios documentos, con más de un centenar de páginas cada uno, bajo el título 'Guía de Buenas Prácticas en Auditorías RGPD' y 'Guía para la gestión de crisis por ciberincidentes en la cadena de suministro'. El primero tiene como objetivo establecer una serie de pautas generales para los responsables del tratamiento de los datos, en relación con la realización de auditorías de cumplimiento con la normativa vigente de protección de datos, dando respuesta a las dudas más frecuentes, en particular, relativas a la necesidad de llevar a cabo dichas auditorías, las obligaciones que forman parte del alcance de la auditoría y la periodicidad de realización de las mismas.



La segunda, que ha contado con el apoyo del **CCN, DSN, Incibe, CNPIC** y de la **Agencia de Ciberseguridad de Cataluña**, ofrece recomendaciones y buenas prácticas sobre cómo deben abordar las empresas una estrategia de protección y respuesta a incidentes de ciberseguridad con origen en proveedor que pueda llegar a provocar una amenaza grave para la propia empresa, así como las convenientes medidas de monitorización, contención y vuelta a la normalidad en la propia Entidad. Este trabajo complementa al ya publicado "Protocolo de actuación frente a incidente en proveedor".

BIDAIDEA pone en marcha un servicio de asesoramiento a las empresas para la nueva certificación de medidas de seguridad 'anti Covid-19'

Tras la aparición de la crisis sanitaria son muchos los retos a los que se enfrentan las empresas, sobre todo, desde el comienzo de la desescalada, en junio, y la transición hacia la 'nueva normalidad'. Para facilitar la labor de las compañías en este escenario, **Bidaidea** ha puesto en marcha un 'Servicio de asesoramiento, definición e implantación de los protocolos y medidas de seguridad para la Covid-19', orientado a poder obtener la nueva certificación de protocolos Covid-19, que **Cámara Certifica**, **Aenor**, **Bureau Veritas**, etc, entidades acreditadas por la **Entidad Nacional de Acreditación** (ENAC) han desarrollado, y que permite a una organización demostrar que cuenta con procedimientos de actuación y medidas de seguridad ante el coronavirus.

Así, Bidaidea propone con este servicio la puesta en marcha en cada organización de medidas basadas en las recomendaciones de las autoridades sanitarias y las buenas prácticas recogidas a lo largo de los años por la consultora.

En definitiva, se trata de "proteger a todas las personas que representan el motor de negocio de las organizaciones, dar una herramienta a las empresas para garantizar la salud y seguridad integral de sus empleados, afianzar la confianza de los clientes con evidencias de cumplimiento de las máximas medidas de seguridad posibles y, también, preparar a las organizaciones ante nuevos posibles rebrotes", destacan desde Bidaidea. El certificado se obtiene a través de cinco pasos que van desde el análisis y gestión de riesgos, hasta de zonas y espacios de trabajo, gestión de los empleados y contingencias, implementando, finalmente, un plan de continuidad de negocio.

Asimismo, desde la empresa recuerdan que "contar con este nuevo certificado permite generar confianza entre todos los colectivos, aspecto clave para asegurar los planes de continuidad del negocio y fortalecer las políticas internas de gestión de la seguridad, de salud laboral y de prevención de riesgos".

Entelgy Innotec
SECURITY

Live confident,
be (cyber) secure

VPN Cloud

Trabaja en remoto de forma segura

- Seguridad
- Privacidad
- Flexibilidad
- Monitorización

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

innotec.security

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

FIRST · TF-CSIRT Trusted Introducer · Centro de Ciberseguridad Industrial · CSIRT.es · ISACA Madrid Chapter · isms forum spain

También, ha actualizado su catálogo de Productos STIC y mejorado su plataforma de retos Atenea

El CCN se centra en incrementar la protección de las entidades locales y presenta microClaudia, su nueva herramienta anti*ransomware*

Uno de los retos planteados desde el **Centro Criptológico Nacional (CCN)** para este 2020 es conseguir una mayor seguridad en los sistemas de las entidades locales (desde diputaciones, hasta cabildos, consejos insulares y ayuntamientos). Para ello, el CCN está llevando a cabo todo tipo de iniciativas que les permitan cumplir las exigencias del Esquema Nacional de Seguridad (ENS), en función de las características de cada una de ellas.

Con este objetivo, y a través de la nueva sección de su web 'Adecuación de las Entidades Locales al ENS', el Centro está publicando abundante material en el que destaca la actualización de su guía CCN-STIC 883, donde muestra un Plan de Adecuación a esta normativa, así como el conjunto de medidas de seguridad a adoptar, tanto desde el punto de vista organizativo, operacional y de protección.

Además, fruto de su trabajo con entidades locales, la Secretaria de Estado, Directora del Centro Nacional de Inteligencia (CNI), **Paz Esteban,** y la Directora de la **Agencia para la Modernización Tecnológica de Galicia (AMTEGA)**, **Mar Pereira,** firmaron, en abril, un 'Convenio General de Actuación' para impulsar, en el ámbito de las competencias de la Xunta y el CCN, la ciberprotección a través del "intercambio de información, la formación especializada y el desarrollo de proyectos tecnológicos".

Anti*ransomware*

Además, para proteger a organismos frente al *ransomware*, la entidad presentó en abril su nueva herramienta **microClaudia.** Se trata de un sistema que utiliza un 'agente 'para ejecutar vacunas en equipos Windows y prevenir infecciones y que complementará las funcionalidades de los antivirus frente a dichos tipos de ataques.

También, se han realizado importantes mejoras en Atenea, la plataforma de retos del CCN-CERT, abierta cualquier persona que quiera poner a prueba sus conocimientos en ciberseguridad. Ahora, los usuarios podrán realizar competiciones privadas entre ellos y solicitar pistas sobre cierto tipo de retos. Estas solicitudes se agruparán y, al llegar a cierto umbral, se incluirá una pista en el desafío correspondiente.

Por último, el organismo ha actualizado su Catálogo de Productos STIC y ha dado a conocer lo que denomina el **Entorno de Superficie de Exposición (ESE**) para mejorar las capacidades de vigilancia y reducir la superficie de exposición de los sistemas frente a las amenazas del ciberespacio, en tiempo real. Se trata de una red neuronal que proporciona una capa de acceso al resto de contenidos y recursos del organismo. Debido a la pandemia, la entidad también ha realizado una labor intensa de formación y concienciación con numerosos documentos e, incluso, ha abierto un canal de Telegram.

ZIUR y LEET desarrollan un proyecto para impulsar la ciberseguridad en el tejido empresarial de Guipúzcoa

Con el fin de reforzar y desarrollar las capacidades en ciberseguridad de las empresas industriales de Guipúzcoa, el **Centro de Ciberseguridad Industrial Gipuzkoa ZIUR** ha alcanzado un acuerdo de colaboración con la agencia de calificación de ciberseguridad española, **Leet Security.**

Gracias a esta alianza, las empresas industriales del territorio contarán con una solución innovadora de autoevaluación, calificación y definición de las directrices e itinerarios en materia de ciberseguridad. Estas soluciones estarán basadas en estándares, normativas y buenas prácticas internacionales para sistemas de información y control industrial. De esta manera, las empresas de este sector podrán conocer, de manera global, sus niveles de ciberseguridad y tomar las medidas oportunas para mejorarlos a través de una aplicación adaptada a sus características.

"Hoy en día, una empresa cibersegura es una empresa competitiva", subraya el Director General de ZIUR, **Carlos Abad,** a la vez que añade que "contar con una solución de autoevaluación permitirá conocerse mejor, potenciar fortalezas y poner solución a debilidades en ciberseguridad". "Somos los únicos en Europa que realizamos calificaciones específicas del nivel de protección de los servicios TIC e ICS", resalta el CEO de Leet Security, **Antonio Ramos**, recordando la necesidad clara de que "las empresas deben contar con avales que aporten confianza y valor al sector industrial".

Por otra parte, Leet Security ha renovado la calificación de **Unysis** para servicios de soporte y mantenimiento de aplicaciones y sistemas de información, conservando el nivel global BBB. Además, también ha obtenido 'Nivel A' para algunas de las secciones correspondientes a la Operación de los Sistemas, Seguridad del Personal, Resiliencia y Desarrollo Seguro.

El GOBIERNO VASCO y GRUPO SPRI ponen en marcha el programa de ayudas a la ciberseguridad industrial 2020

Un año más, el **Gobierno Vasco**, a través del **Grupo SPRI** y el **Centro Vasco de Ciberseguridad** (BCSC, por sus siglas en inglés), han puesto en marcha el programa de ayudas de Ciberseguridad Industrial 2020. "Ante la situación actual generada por la pandemia de la Covid-19, la ciberseguridad está considerada como un elemento clave para el desarrollo de la economía. Debido a la situación actual y al firme compromiso del Gobierno Vasco, en 2020, se amplía el presupuesto inicial hasta 1,3 millones de euros", destacan sus impulsores.

Ayudas con un objetivo muy claro

Así, en línea con los objetivos del Departamento de Desarrollo Económico e Infraestructuras del Gobiernos Vasco, plasmadas tanto en la Estrategia Industria Vasca 4.0, como en la Agenda Digital de Euskadi 2020, el objeto de este programa es impulsar la ciberseguridad industrial, especialmente proyectos que aborden la convergencia e integración de los sistemas de protección ante ciberataques para entornos IT/OT.

Dicho programa contempla subvenciones de hasta 18.000 euros para cubrir hasta el 50% de la inversión y se puede pedir hasta el 27 de noviembre, estando limitados a empresas en el País Vasco.

ADVANTIO

SU SOCIO DE CONFIANZA EN CIBERSEGURIDAD

SPAIN@ADVANTIO.COM
+34 91 418 58 17

ADVANTIO.COM/ES

10 AÑOS DE EXPERIENCIA

13 UBICACIONES
15 IDIOMAS

SIEMPRE A TIEMPO Y DENTRO DE PRESUPUESTO

ACREDITACIONES PCI

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

OTROS SERVICIOS

RGPD
CMMI
SOC2
ISO 27001 / 22301
PRUEBAS DE PENETRACIÓN
ANÁLISIS FORENSE
ANÁLISIS DE MALWARE
SEGURIDAD EN LA NUBE
SERVICIOS ADMINISTRADOS

ABORDE SU ESTRATEGIA EN SEGURIDAD CIBERNÉTICA CON UN SOCIO DE CONFIANZA

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

Seguridad en medios de pago, más allá del cumplimiento normativo

PCI 3DS

PCI PIN

PCI P2PE

Servicios gestionados de seguridad en la nube. Una manera de reducir los recursos en infraestructuras sin perder el control de la seguridad de los sistemas críticos.

PRESENTAMOS aGUARD

aGUARD MDR

Detecta brechas de seguridad y responde en el momento

aGUARD VULN

Gestiona tu programa de vulnerabilidad

aGUARD CLOUD

Acelera tu migración a la nube pública

Las compras de empresas de protección en la nube y para el trabajo en remoto, protagonistas del mercado en tiempos de Covid

A pesar de la crisis sanitaria global, el mercado de la ciberseguridad, con gran demanda en ciertos segmentos para dar protección a millones de trabajadores en remoto, ha continuado su acentuada tendencia de fusiones y adquisiciones, gran parte de ellas relacionadas con la seguridad en la nube.

Como se veía venir, la industria de la ciberseguridad ha experimentado un súbito y fuerte crecimiento en ciertos segmentos derivado por la crisis de la Covid-19, ya que la generalización del teletrabajo ha obligado a muchas empresas a apostar por servicios de ciberprotección en la nube y gestionados para dar protección a sus plantillas en remoto.

Aunque, en este sector, el mercado español no ha experimentado grandes operaciones tras un comienzo de año agitado con la compra de SIA por parte de Minsait, el internacional sí ha vivido operaciones de calado. Quizá, una de las más interesantes por los participantes es la compra, por parte de la plataforma de videoconferencias **Zoom** de la empresa **Keybase,** un servicio de mensajería cifrada. Una operación que forma parte de su estrategia para fortalecer su plataforma de videoconferencia que pasó de 10 a 200 millones de usuarios en 90 días, y su popularización sacó a la luz numerosos fallos de seguridad.

Zoom se hace con Keybase, Zscaler compra Cloudneeti y Edgewise Networks, Palo Alto finaliza la operación de CloudGenix, Rapid7 adquiere DivvyCloud, CyberArk a IDaptive, VMware a Kubernetes Octarine y Microsoft a CyberX en tanto que Atos refuerza su negocio de datos e IA con Miner & Kasch.

Sin embargo, algunos analistas, como **ResearchAndMarkets,** pronostican en sus informes que el mercado global de seguridad cibernética crecerá a una tasa promedio más lenta de 6,2% por año, hasta 2023, debido a las consecuencias económicas de la pandemia, tras estudiar 46 tecnologías y disciplinas de ciberseguridad, 39 de las cuales aún se encuentran en una etapa temprana en su ciclo de vida del producto (caracterizadas por un alto crecimiento, baja saturación de clientes y grandes ecosistemas de proveedores).

"La seguridad se ha convertido en un problema cada vez más estratégico y las empresas son menos capaces de prescindir de ella cuando se reducen los costes. Sin embargo, las compañías tendrán dificultades con el flujo de caja y las congelaciones presupuestarias en 2020 y es probable que los aplazamientos de proyectos se generalicen, retrasándose la inversión en nuevos", destaca la investigación del analista de mercados.

También, en Estados Unidos, **Zscaler** anunció su intención de adquirir **Cloudneeti,** una compañía de Cloud Security Posture Management (CSPM) y también se ha hecho con Edgewise Networks, de seguridad en aplicaciones para las nubes públicas y centros de datos.

Palo Alto Networks completó la adquisición de **CloudGenix** por 390 millones de euros para hacer frente a competidores como **Cisco, VeloCloud** de **VMware o SD-WAN** de **Dell**, entre otros, en el mercado de redes seguras SD-WAN. La tecnología de CloudGenix se integrará en la plataforma SASE de Palo Alto, conocida como Prisma Access.

Por su parte, **Rapid7** se hizo con **DivvyCloud**. Se trata de una nueva compra dentro del conjunto de soluciones CSPM, cuya operación se ha cifrado en 132 millones de euros, y espera cerrarse en el segundo trimestre del año.

CyberArk adquirió **IDaptive,** centrada en la identidad como servicio. "La adquisición ampliará el valor de la gestión del acceso privilegiado y su innovación en seguridad de la identidad digital". Entre sus aspectos más relevantes destaca que contará con un enfoque integral basado en la Inteligencia Artificial (IA), en una gestión de identidades que sea adaptable y que tenga en cuenta el contexto, y que esté basado en los principios de Zero Trust y en el acceso con privilegios mínimos, entre otras características.

VMware se hizo con la *startup* de seguridad **Kubernetes Octarine** y la incorporará a Carbon Black. La operación encaja con lo que esta última llama su "estrategia de seguridad intrínseca", es decir, proteger el contenido y las aplicaciones donde sea que se encuentren. Asimismo, el proveedor de protección de identidad **Venafi** compró **Jetstack,** una empresa especializada en software de protección de identidades de máquina de código abierto para Kubernetes.

Además, **Microsoft** anunció su intención de hacerse con la israelí **CyberX** por 150 millones de euros, especializada en ciberseguridad industrial para IoT y protección de comunicaciones de máquina a máquina mediante la identificación de anomalías.

Además, la también estadounidense **Smarsh,** focalizada en cumplimiento y ciberseguridad en las comunicaciones, sobre todo, para el sector financiero, ha comprado la compañía de software y gestión de riesgo, **Entreda.**

En Europa, **Atos** compró **Miner & Kasch,** una firma de consultoría en inteligencia artificial (IA) y ciencia de datos con sede en EE.UU.

Rondas de financiación

En cuanto a las rondas de financiación, la española **Ironchip**, especializada en productos ciberseguridad basados en geolocalización, cerró con éxito su primera ronda, liderada por **Invereadу** y **EASO Ventures**, por 500.000 euros, que se destinará a mejorar el producto y comenzar la comercialización internacional de su plataforma Ironchip Location Based Security (LBS) en Iberomérica, Europa y EE.UU.

La británica **CyberOwl** recaudó 1,9 millones de euros para continuar con el desarrollo de su plataforma de seguridad para sistemas de transporte e infraestructura. En concreto, dedicará esta nueva inyección de capital para ganar presencia en el sector marítimo. Un aspecto de relevancia, ya que la Organización Marítima Internacional ha ordenado a los operadores de flotas que aborden su seguridad cibernética antes del 1 de enero de 2021.

La *startup* israelí de ciberseguridad, **Secret Double Octopus,** obtuvo, por su parte, 12,7 millones para ayudar "a las empresas, a deshacerse de las contraseñas" gracias a su herramienta de autenticación de usuario corporativo que no las requiere.

1. SERVE THE PUBLIC TRUST
2. PROTECT THE INNOCENT
3. UPHOLD THE LAW

SECURA by factum

BLUE TEAM - SOC

WWW.SECURA.ES
info@secura.es
t_ 91 157 07 04

Víctima de Covid-19, cuando se matriculó en Oxford, en 1943, sólo había cinco mujeres en ciencias exactas

Muere la criptoanalista Ann Mitchell, referente femenino en ciberseguridad que ayudó a romper el cifrado de Enigma en Bletchley Park

La historia de las matemáticas, la informática y, sobre todo, la criptografía y la ciberseguridad ha estado llena de mujeres que, en la sombra, contribuyeron decisivamente a lograr hitos sorprendentes. Es el caso de Ann Khaterine Mitchell que falleció en mayo, fruto del Covid-19, a los 97 años y ayudó, en 1943, a romper los códigos de la máquina Enigma nazi, desde las instalaciones británicas de Bletchley Park. Un ejemplo inspirador del espíritu que ha de impregnar hoy a iniciativas como la de WiCS –la asociación española Women in Cybersecurity of Spain–, en pos de dotar a la sociedad de toda la diversidad, representatividad y talento posibles.

"Cuando fui a Oxford en 1940, había cinco mujeres en toda la universidad que en esa promoción estudiaban matemáticas", explicaba **Ann Mitchell,** en una entrevista. Su vida destacó por su 'espíritu **WiCS'**, la iniciativa española que busca dar visibilidad a la mujer en el sector de la tecnología y la ciberseguridad.

Natural de Oxford, Mitchell destacó desde pequeña en matemáticas aunque la directora de su escuela le llegó a decir a sus padres "que no era una asignatura femenina". Fruto de su pasión, fue una de las pocas estudiantes en este campo que consiguió matricularse en la Universidad de Oxford en 1940. Tras graduarse en ciencias exactas, en 1943, fue llamada por el Ministerio de Asuntos Exteriores para trabajar en una villa victoriana, a las afueras de Londres, Bletchley Park, también conocida como 'Estación X'.

Allí, en el más absoluto secreto, durante dos años, un verdadero 'ejército' de casi 7.000 mujeres junto a algunos de los matemáticos y criptógrafos más importantes del momento, como **Alan Turing, Dilly Knox, Tony Kendrick, Peter Twinn** y **Gordon Welchman,** trabajaron para desarrollar máquinas que permitieran descifrar los mensajes en clave que el ejército nazi enviaba a través de sus máquinas Enigma, reto que alcanzaron cuando Turing diseñó la 'Bomba', el que es considerado el primer ordenador electromecánico del Reino Unido. Mitchell fue destinada a uno de los lugares más secretos de Bletchley Park, la 'Sala de Máquinas' (Hut 6), donde junto con otras mujeres conformaron un equipo encargado de idear las instrucciones sobre cómo instalar las 'Bombas' y configurarlas para que pudieran descifrar de forma automática los códigos. De hecho, era desde donde se descifraban los códigos de "alta prioridad" del Ejército alemán y la Fuerza Aérea. Curiosamente, no todas las que trabajaban en ese decisivo equipo femenino eran matemáticas o criptógrafas, ya que era preciso que lo hicieran por turnos, las 24 horas del día, y al no dar con suficientes matemáticas –por la noche no estaba bien visto que trabajaran con hombres– también fueron contratadas economistas y abogadas. Se calcula que gracias a la labor de los 'rompedores de códigos' de Bletchley Park, los aliados consiguieron ganar la guerra dos años antes.

Ann Mitchell en 2020. Fuente: The Scotsman



Graduación de Ann Mitchell en 1943
A la derecha la "sala de máquinas" donde trabajó

En la 'Hut 11' estaban las máquinas de La Bomba

Finalizado el conflicto, la instalación fue cerrada y su material destruido. Sin embargo, a partir de los años 70, cuando se dio a conocer la máquina Enigma, su labor comenzó a reconocerse en público. Finalmente, el equipo de Bletchley fue, en 2009, galardonado con una medalla de la agencia británica de inteligencia 'ciber' **GCHQ**.

"Estoy orgullosa de lo que hicimos", destacó Mitchell, que el año pasado formó parte del Proyecto de Computación '*Forgotten Women* of Oxford', que celebró la historia, hasta ahora oculta, del papel pionero de las mujeres de la universidad en la informática.

Es de justicia y de agradecer que en las últimas décadas, por fin, el trascendental trabajo de este equipo femenino que rompió los códigos de Enigma, haya salido a la luz y sus protagonistas obtuvieran público reconocimiento. Entre estas pioneras del criptoanálisis y ya indiscutibles referentes figuran, junto a la mentada Ann Mitchell, **Pamela Rose, Margaret Rock, Mavis Lever, Joan Clarke, Pat Davies** o **Charlotte Webb**, entre otras.

Un enriquecedor ejemplo de la auténtica visibilidad que se precisa para estimular el atractivo de emprender una trayectoria profesional en el ámbito de la ciberprotección por parte del aún escaso y renuente colectivo femenino a las especialidades técnicas.

SIC

Liderada por la gallega Gradiant, también la integran los centros tecnológicos Fidesol, Ikerlan y Vicomtech

Nace ÉGIDA, la primera Red Nacional de Excelencia en tecnologías de seguridad y privacidad, para la protección de la privacidad de la información

Con una inversión de 3,3 millones de euros y formada por **Gradiant** (Vigo), **Fidesol** (Granada), **Ikerlan** (Gipuzkoa) y **Vicomtech** (San Sebastián), se ha puesto en marcha en España, **Égida,** la primera red de centros tecnológicos dedicada a tecnologías de seguridad y privacidad e integrada por centros tecnológicos de excelencia. Creada en el marco del Programa Cervera, del **Ministerio de Ciencia e Innovación y el Centro de Desarrollo Tecnológico Industrial** (CDTI), su objetivo es "fortalecer la investigación aplicada, reforzando las capacidades tecnológicas de los centros y fomentando la colaboración con las empresas".

Cuatro campos

En concreto, esta iniciativa abordará la investigación en tecnologías de seguridad y privacidad desde cuatro ámbitos, pero siempre con un objetivo común: la protección de la privacidad de la información. Así, los centros que forman el consorcio de Égida trabajarán centrados en tecnologías de criptografía aplicada, para la protección de información confidencial; en datos personales o sensibles, etc.; en identidad digital y privacidad para la prevención del fraude a través de la creación, verificación y uso de identidad digital; en seguridad en sistemas distribuidos, para mejorar la seguridad en tecnologías disruptivas y su utilización con tecnologías IoT, 5G o DLT/blockchain; y en el desarrollo de sistemas de información seguros, que permitan aumentar la confianza en los sistemas de información frente a ataques cibernéticos.

"La alianza que hemos forjado nos permite ser plenamente conscientes del papel transformador que juega la innovación tecnológica en seguridad y privacidad tanto para las personas, como para las empresas, y es un gran reto situar a España en el mapa internacional", apunta el Director de Égida, responsable de Seguridad

y Privacidad en Gradiant, **Juan González.** Entre otras aportaciones, desde Fidesol, la Fundación I+D del Software Libre, "buscará mejorar el análisis e inferencia de conocimiento a partir de las distintas fuentes de información que ocurren en un ataque a una red corporativa y su posterior *re-up* (puesta de nuevo en funcionamiento), además de presentar diferentes soluciones de ciberprotección orientadas a redes IoT, así como servicios de contratos inteligentes (*smart contracts*)", destaca su Director Técnico, **Miguel A. López Montellano**. Desde Ikerlan, el centro tecnológico de la Fundación Mondragón, el responsable de Área de Ciberseguridad Industrial, **Salvador Trujillo,** destaca que la apuesta de su organización es aportar a Égida "tecnologías de ciberseguridad y privacidad con impacto en los sistemas industriales del futuro, ya que la digitalización y la ciberseguridad son cada vez más relevantes en la sociedad y en la industria".

Generación de talento

Asimismo, otro de sus objetivos es la generación de empleo cualificado en I+D+i. Durante los tres años de duración de la red (2020-2022), 80 ingenieros e investigadores trabajarán para alinear estrategias y acciones en investigación y desarrollo, captar y retener talento. Además, Égida facilitará la definición de carreras profesionales a largo plazo, contribuirá a la especialización de los investigadores y promoverá el intercambio internacional de los profesionales tecnológicos.

La red también contará con el apoyo de organismos públicos y el sector privado, ya que en su comité científico están desde el **Instituto Nacional de Ciberseguridad (INCIBE)**, hasta **Alastria, AEI Ciberseguridad, AENOR, IDC Research España, Vector ITC Group, la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), ElevenPaths** (unidad global de ciberseguridad de Telefónica), **BBVA** y el **Centro Criptológico Nacional (CCN).**

La AEPD sólo sancionó a un 5% de las notificaciones por fallos de seguridad en 2019

La **Agencia Española de Protección de Datos (AEPD)** publicó, en mayo, su 'Memoria 2019', en la que hace un balance del Plan Estratégico de la Agencia, el cual, ha supuesto la realización de más de 150 acciones, desde 2015. En la memoria se ha dado a conocer que, en total, el año pasado se presentaron ante la Agencia 11.590 reclamaciones, un 33% más que en 2017. Las reclamaciones planteadas con mayor frecuencia por los ciudadanos en 2019 hicieron referencia a servicios de internet (13%) y videovigilancia (12%). En cuanto a las notificaciones de "quiebras de seguridad" ante la Agencia, como indica el RGPD, la Unidad de Estudios y Evaluación Tecnológicos (UEET) recibió y analizó 1.459 notificaciones en 2019, una cifra que supone casi triplicar las que recibió el año anterior (547). En este punto, es necesario mencionar que sólo 79 se han remitido a Inspección al requerir de una investigación en profundidad, lo que supone poco más del 5%.

En 2019, se dictaron también 338 resoluciones sancionadoras en materia de videovigilancia (287), servicios de Internet (58), publicidad a través de correo electrónico o teléfono móvil (32), telecomunicaciones (21) y administración pública (15). Las áreas con mayor importe global de multas fueron los directorios (2,9 millones de euros), telecomunicaciones (641.000), contratación fraudulenta (620.620) y quiebras de seguridad (460.000). Además, la memoria destaca que en España ya hay reconocidos 50.326 Delegados de Protección de Datos (44.069 del sector privado y 6.257 del sector público).

Privacidad vs coronavirus

También en mayo, la AEPD publicó un estudio en el que analizó distintas tecnologías para luchar contra el coronavirus y sus riesgos para la privacidad cuando se utiliza la geolocalización. En el documento, la Agencia pone de manifiesto "que nos encontramos en un punto de inflexión crítico, no solo por la pandemia, sino por nuestro modelo de derechos y libertades", y recuerda que "la utilización de la tecnología debe ser entendida en el marco de un tratamiento de datos personales con un propósito claramente definido".

Además, el organismo ha publicado un informe que aborda diversas cuestiones relacionadas con la seguridad privada, entre ellas, si es lícito incorporar sistemas de reconocimiento facial en los servicios de videovigilancia. Un aspecto en el que la AEPD recuerda que estas técnicas suponen un tratamiento de categorías especiales de datos en el RGPD, exigiéndose garantías reforzadas y estando justificado si hay un "interés público esencial".

McAfee. The device-to-cloud cybersecurity company.

¿Sabías que la nueva McAfee...

....ofrece una plataforma de seguridad abierta integrada?

....protege todo tipo de dispositivos?

....posee la mejor solución CASB del mercado?

....proporciona un entorno de SecOps moderno y escalable?

Encuentra tus respuestas aquí **www.mcafee.com/device-to-cloud**

McAfee™
Together is power.

La valenciana LAYAKK, nuevo laboratorio de evaluación español de Common Criteria

El **Centro Criptológico Nacional** ha acreditado a un nuevo laboratorio**, Layakk Seguridad Informática,** de Valencia como centro de evaluación de la seguridad de las tecnologías de la información, conforme a la metodología 'Common Criteria' (ISO/IEC 15408). En concreto, hasta el nivel 'EAL2', tras certificar su competencia técnica la **Entidad Nacional de Acreditación (ENAC)**, para la realización de ensayos de "Evaluación de la Seguridad de las Tecnologías de la Información", con alcance suficiente para los niveles solicitados. Así lo ha hecho constar el CCN en la Resolución A0/38122/2020, de 13 de abril, publicada en el BOE, recordando que la empresa ya contaba con el reconocimiento para certificaciones en ciberseguridad, más básicas, como la tipo Lince (Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad), dentro del Esquema Nacional de Evaluación o la Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI).

Layakk es una empresa española dedicada a servicios de seguridad, fundada, en 2013, por **David Pérez** y **José Picó**. Entre otras iniciativas, la compañía se apoya en sus actividades de investigación y el conocimiento de su equipo para realizar servicios de seguridad avanzados. Sus fundadores han sido ponentes habituales en el congreso técnico de ciberseguridad **RootedCON,** con intervenciones muy valoradas sobre seguridad en redes 2G, 3G, 4G y 5G. Precisamente, sobre las posibles vulnerabilidades en esta última también participaron en el especial 'Pillar el punto al 5G', en el nº 134 de **Revista SIC.**

El CCN-CERT actualiza su catálogo de productos, CPSTIC, tras la evaluación LINCE y las pruebas complementarias de JTSEC

El **Catálogo de Productos de Seguridad TIC**, **CPSTIC**, recomendados por el **Centro Criptológico Nacional** (CCN), ha sido actualizado gracias, entre otras, a las nuevas evaluaciones, con metodología de certificación y evaluación LINCE, para analizar la capacidad de un producto TIC en cuanto al tratamiento de la información de forma segura. Se trata de una de las vías para incluir productos en él, siendo identificados como aptos para sistemas que deban cumplir con el Esquema Nacional de Seguridad (ENS). Un aspecto al que ha contribuido la empresa granadina **JTSEC**, primer laboratorio acreditado por ENAC y el CCN para este tipo de evaluaciones, "trabajando codo con codo para mejorar la seguridad de los productos de sus clientes".

Entre las novedades del nuevo catálogo destaca la inclusión de: SoCe System on Chip engineering, de **Novatronic Sistemas,** para protección de comunicaciones; **Eset** Endpoint Security, especializado en seguridad de punto final; **McAfee** Data Loss Prevention (DLP) Endpoind; y el **Stormshield** Network Security UTM/NG-Firewall, entre otros.

MASTERCARD y ENEL X abrirán un laboratorio de ciberseguridad en Israel dedicado a tecnologías fintech

Las multinacionales **Mastercard** y **Enel X** abrirán un nuevo centro de investigación, en el que se invertirá casi 3,5 millones de euros, para investigaciones sobre ciberseguridad en tecnologías financieras (*fintech*). Apoyado por la **Autoridad de Innovación** de Israel, la **Dirección Nacional de Ciberseguridad (DNC)** y el **Ministerio de Finanzas,** el objetivo es que el nuevo centro de investigación también facilite la labor de emprendedores y de empresas que desarrollen nuevas tecnologías en ciberseguridad para el sector financiero de la nación.

De hecho, la Autoridad de Innovación financiará el 85% del coste (en torno a 130.000 euros) que suponga para las empresas incorporarse al laboratorio, siempre que lo justifiquen con una 'prueba de concepto'. Además, las compañías que se integren en las instalaciones tendrán acceso a datos de ciberseguridad y financieros de las entidades del país que les faciliten el desarrollo de sus productos, procesos y servicios. "Esta colaboración hará que la información y las posibles ciberamenazas que conoce el sector estén disponibles para desarrollar mejores ciberdefensas frente a ellas por la acelerada digitalización de los sistemas financieros", ha destacado el Director General de la **DNC**, **Igal Unna.**

La adaptación es seguridad

Adaptar tu modelo de seguridad a los retos que plantean las nuevas tecnologías es fundamental para tu negocio. En Omega Peripherals nos mimetizamos con cada entorno para proteger tus datos.

¿Quieres saber más? Descubre nuestras soluciones de seguridad en www.omega-peripherals.com

Hacemos seguridad, creando seguridad

OMEGA
PERIPHERALS

www.omega-peripherals.com

ISO actualiza su ISO/IEC 27009 para permitir a las empresas abordar la ciberseguridad y privacidad de forma más coherente

La **Organización Internacional de Normalización (ISO**) actualizó en mayo su ISO/IEC 27009 "para proteger la privacidad de personas y empresas, así como su ciberseguridad". El estándar aporta en su nueva versión "tranquilidad" a través de "un enfoque coherente y reconocido internacionalmente".

Como se recordará, la ISO/IEC 27009, fue desarrollada por un grupo de expertos del comité técnico ISO/IEC JTC 1/SC, centrado en la seguridad de la información, la ciberseguridad y la privacidad. Su objetivo es definir los requisitos para el uso del estándar ISO/IEC 27001, el más usado en ciberprotección, en cualquier sector específico (campo, área de aplicación o sector de mercado). Así, la ISO/IEC 27009 define con claridad cómo incluir requisitos adicionales, así como 'refinar' cualquiera de sus requisitos de este e incorporar controles o conjuntos de control, además de los marcados por la ISO/IEC 27001.

Entre sus novedades destaca que añade dos definiciones adicionales: por un lado, de la interpretación como "explicación (en forma de requisito u orientación) de una exigencia del estándar ISO/IEC 27001 en un contexto específico del sector que no invalida ninguno de los requisitos del estándar ISO/IEC 27001". Por otro, la de 'Refinamiento', considerándose como tal "la especificación del sector de un requisito del estándar ISO/IEC 27001 que no elimina ni invalida los requisitos de dicho estándar".

Además, el estándar ISO/IEC 27009 asume que todos los requisitos del estándar ISO/IEC 27001 que no se refinan o interpretan, y todos los controles en el estándar ISO/IEC 27002 que no se modifican, se aplicarán en el contexto específico del sector sin cambios.

HORNETSECURITY finaliza el proceso de compra de SPAMINA

A principios de 2019, la empresa de seguridad informática **Spamina** fue adquirida por el proveedor alemán de seguridad de correo electrónico en la nube, **Hornetsecurity.** Durante un año, los expertos de ambas empresas trabajaron en la adaptación de los procesos y servicios de Spamina al entorno técnico de Hornetsecurity tras lo que, ahora, el negocio continuará bajo una marca común, quedando ambas compañías bajo la marca Hornetsecurity.

Esto permitirá a los clientes de Spamina disfrutar de "oportunidades completamente nuevas", destacan desde la compañía. "Gracias a la migración al entorno de Hornetsecurity, ampliamos los servicios que podemos ofrecer a nuestros clientes. Juntos somos ahora capaces de dar soporte 24/7 y hemos obtenido acceso a recursos técnicos aún más amplios, ya que ahora contamos con nueve centros de datos redundantes en todo el mundo", ha explicado el Head of Channel Management Iberia y Latam de Spamina, **Leonardo Rodríguez,** a la vez que ha recordado que Hornetsecurity 365 Total Protection Suite ahora también está disponible para el mercado Ibérico y Latinoamericano. Esta herramienta ofrece una protección efectiva, dependiendo del alcance habilitado: desde la protección contra el *spam* y el *malware* hasta la protección avanzada contra amenazas, pasando por el cifrado de datos.

"La fusión nos convierte en una unidad poderosa que nos proporciona la fuerza necesaria para los próximos desafíos", ha destacado el Director General de Hornetsecurity Iberia, **Daniel Blank.**

El GRUPO WALLIX llega a España focalizado en servicios PAM, albergando el centro de investigación de la compañía para protección de puntos finales

El **Grupo Wallix** ha acelerado su internacionalización y, en abril, presentó su filial en España. Con presencia en más de 85 países y con más de 1.000 clientes corporativos, el lanzamiento de Wallix Ibérica representa una apuesta solida de la compañía por España, Portugal e Iberoamérica, que se realiza en el marco del plan de expansión Ambition 21. En éste se enmarca la compra, en 2019, de **Simarks** en España y **Trustelem** en Francia.

De momento, nuestro país contará con un equipo de una docena de personas, con sede en Las Rozas (Madrid) divididas en dos departamentos: un centro de conocimiento y desarrollo de tecnologías, especializada en protección del punto final para todo el Grupo y, por otro lado, un área dedicada al desarrollo de negocio, soporte y marketing, que es similar a la que la organización tiene en otros países.


Jean-Noël de Galzai

La entidad está especializada en desarrollar y proveer Productos y Soluciones de ciberseguridad, todas de desarrollo propio, en las áreas de *Privileged Access Management* (PAM), Protección del Endpoint (EPM), Federación de Identidades (IdaaS) y Soluciones de ciberseguridad OT/Io. "España es un mercado prioritario para el Grupo, ya que la ciberseguridad es una de las principales preocupaciones de las empresas", explicó en rueda de prensa el CEO del Grupo, **Jean-Noël de Galzai**. Durante la presentación de la filial ibérica, que contó con el responsable de desarrollo de negocio de la filial española, **Luis Miguel García,** los responsables de la empresa dieron a conocer sus productos de última generación en protección PAM, como Wallix Bastion, y en EPM, como Wallix BestSafe.

RISK4ALL y OESÍA unen fuerzas en el ámbito de la ciberseguridad y privacidad

Ante un entorno de creciente complejidad para gobernar, evaluar riesgos y demostrar el cumplimiento de normativas y estándares de seguridad y privacidad, se hace cada vez más necesario el uso de herramientas que permitan aprovechar sinergias y ahorren tiempo y recursos. Por eso, **Risk4All,** dedicada al desarrollo, comercialización y distribución de su herramienta GRC, y **Grupo Oesía,** multinacional española de alta tecnología y productos de ingeniería electrónica para seguridad y aeroespacial, han cerrado una alianza para facilitar a las empresas la evaluación de riesgos y demostrar el cumplimiento de normativas y estándares, mediante una solución global a nivel internacional en el soporte del cumplimiento normativo de privacidad y seguridad de la información. "Las soluciones tecnológicas son cada vez más complejas y requieren de conocimientos específicos en las áreas de diseño, instalación y mantenimiento", han destacaron sus impulsores.

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, las organizaciones necesitan un nuevo enfoque en su gestión de los riesgos tecnológicos, desde la estrategia a la ejecución.

En PwC no te decimos cómo hacerlo. Lo hacemos contigo.

www.pwc.es/bss

pwc

Los investigadores de Trend Micro Research han llegado a identificar, de media, 230 millones cada día

La configuración incorrecta es el riesgo número uno para los entornos en nube

Gartner estima que para 2021, más del 75% de las organizaciones, medianas y grandes, habrán adoptado una estrategia de TI *multicloud* o híbrida. Sin embargo, su protección será uno de los grandes retos. **Trend Micro**, de hecho, destaca que los errores humanos y los despliegues complejos abren la puerta a una amplia variedad de ciberamenazas, según los resultados de su última investigación bajo el título, 'Desenredando la red de amenazas de seguridad en la nube'.

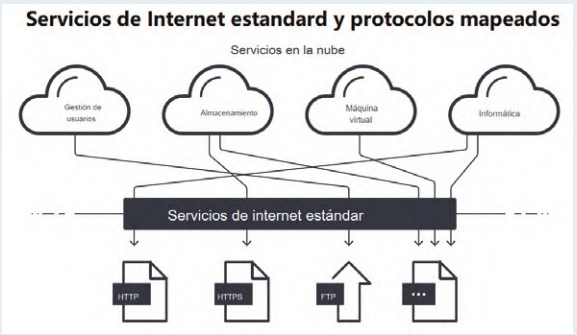
En ella explica que, "a medida que las plataformas en la nube se vuelven más frecuentes, los equipos de TI y DevOps se enfrentan a preocupaciones e incertidumbres adicionales relacionadas con la seguridad de sus instancias *cloud*". Prueba de ello es que los responsables del estudio han identificado, cada día, una media de 230 millones de configuraciones erróneas, "lo que demuestra que este riesgo es frecuente y generalizado".

La investigación encontró amenazas y debilidades de seguridad en varias áreas clave de la computación basada en la nube, que pueden poner en riesgo las credenciales y los secretos de la empresa. Los delincuentes que aprovechan las configuraciones erróneas se han dirigido a las empresas con *ransomware, cryptomining, e-skimming* y filtrado de datos.

"Creemos que la migración a la nube puede ser la mejor manera de solucionar los problemas de seguridad, redefiniendo el perímetro TI y los *endpoints* corporativos. Sin embargo, eso solo puede ocurrir si las organizaciones siguen el modelo de responsabilidad compartida para la seguridad *cloud*", explica el Vicepresidente de Ciberseguridad de Trend Micro, **Greg Young**.

Entre las buenas prácticas que recomienda el estudio también están desde emplear controles de privilegios mínimos, supervisar los sistemas mal configurados y expuestos e integrar la seguridad en la cultura DevOps.

Por otro lado, Trend Micro Research, junto con la **Universidad Politécnica de Milán,** publicó, en mayo, un estudio sobre los métodos críticos de ataque a la Industria 4.0. En él se describen los principales escenarios de ataque avanzados y recomendaciones para los operadores OT. Entre ellas está poner en marcha inspecciones en profundidad de paquetes que soporta los protocolos OT, para identificar cargas útiles anómalas a nivel de red, usar controles para identificar cualquier componente de software alterado, contar con la firma de código en los dispositivos IoT y realizar análisis de riesgos que vayan más allá de la seguridad física.



El CENTRO DE CIBERSEGURIDAD INDUSTRIAL analiza la situación actual del sector en Galicia y Cataluña con dos estudios específicos

El **Centro de Ciberseguridad Industrial (CCI)** ha publicado dos guías de interés para conocer la situación y madurez de la ciberseguridad en Galicia y Cataluña. La primera, 'Estudio sobre el estado de la Ciberseguridad Industrial en Galicia', presenta los resultados de la investigación realizada a gestores de 27 empresas industriales de Galicia y ofrece una interpretación de los mismos basada en el conocimiento y experiencia de sus redactores y de los participantes en el proceso de revisión. Entre otros aspectos, se valoran la Organización de la Ciberseguridad Industrial (Responsabilidad y Grado de Capacitación), su gestión (evaluación de Riesgos, Gestión de Incidencias y Planificación); sus aspectos técnicos (conexión de Redes, Accesos Remotos, Uso de Normas y Medidas), así como el mercado ofreciendo una previsión de Nuevas Actividades, Requisitos para Nuevos Proyectos, Contratación de Proyectos y Certificados Profesionales".

Por su parte, el 'Estudio sobre el estado de la Ciberseguridad Industrial en Cataluña' muestra los resultados de un análisis realizado a gestores de 43 empresas del sector en la región y ofrece "información focalizada y completa" para valorar el nivel en el que se encuentra la industria catalana respecto a la ciberprotección, valorándose aspectos similares a los analizados en la publicación sobre Galicia.

Ambos estudios permiten "pensar en la necesidad de desarrollar, de forma planificada, la ciberseguridad industrial contemplando aspectos como el organizacional, el plano técnico y la respuesta a los incidentes", según destacan sus responsables, que también recomiendan estas guías a cualquier emprendedor que quiera abrir negocio en este campo en estas regiones.

HITEC, el CONSEJO EJECUTIVO HISPANO DE TI incluye a los españoles Santiago Moral y Gloria Lorenzo dentro de tu 'Top50 global 2020'

El **Consejo Ejecutivo Hispano de Tecnologías de la Información (HITEC),** una entidad formada por ejecutivos del sector de la tecnología y la empresa, ha reconocido a **Gloria Lorenzo**, Directora Senior de Soluciones de Lenguaje de **Oracle,** y **Santiago Moral,** Vicepresidente de Innovación y Ciberseguridad de **OpenSpring**, como dos de los 50 especialistas tecnológicos más influyentes y notables de América Latina, España y Portugal, en 2020, en su 'Hitec 50', un ranking mundial que se publica desde 2011.

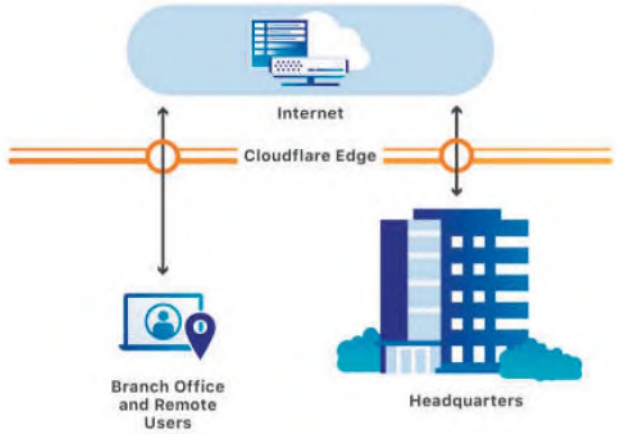
En el caso de Moral, se trata de un reconocimiento a su carrera profesional como científico de datos y experto en ciberseguridad. En su trayectoria, Moral ha ejercido como CISO del Grupo **BBVA** durante más de 15 años y, anteriormente, desempeñó distintos cargos en la compañía tecnológica Atos. Además, es antiguo miembro del grupo de Ciberseguridad para las Ciencias de la Computación y la Inteligencia Artificial del Instituto Tecnológico de Massachusetts, (MIT) y es Fundador y Codirector del **Institute for Data, Complex Networks & Cybersecurity *Sciences*** (DCNC) de la **Universidad Rey Juan Carlos.**

Lorenzo, por su parte, se ha convertido en un referente en el mundo de la globalización de aplicaciones SW, con un trabajo enfocado en el desarrollo de tecnologías relacionadas con la traducción y soluciones informáticas en idiomas, aplicando técnicas de *Machine Learning* y NLP. Además, es Vicepresidenta de la **Delegación Española del Global Summit of Women**.

Cloudflare for Teams

Proteja cada conexión, sin compromiso.

Su sede central puede tener puertas y cerraduras, pero Internet hace que su negocio no tenga fronteras. Eso significa que se accede a sus activos principales todo el tiempo, desde cualquier lugar. Aquellos controles para los accesos estáticos del pasado y los perímetros con redes cerradas en las que se establecía la confianza y la verificación, no son adecuados para el modelo actual de Empresa abierta. ¿Cómo protege a su equipo y sus datos en un mundo sin perímetros?



PROTEGE TUS CONEXIONES A INTERNET

Permite a los empleados navegar Internet sin miedo a perder datos confidenciales. Cloudflare es una red global que filtra todas las peticiones, bloqueando las solicitudes maliciosas. La tecnología de aislamiento de navegador remoto asegura que el código malicioso no llegue nunca a los dispositivos de los empleados.

ACCESO ULTRA RÁPIDO

Enruta las conexiones a través de Cloudflare y elimina así la necesidad de mantener configuraciones y redes MPLS. Mejora la experiencia de navegación del usuario, al eliminar el reenvío de tráfico a ubicaciones centralizadas para su procesamiento.

CONTROL DE ACCESO A APLICACIONES POR USUARIO

Permite a los usuarios, ya sea contratista o empleado remoto, acceder a aplicaciones internas de forma rápida y segura. Administra el acceso a aplicaciones específicas on a per-user basis, con reglas fáciles de crear y gestionar.

ADOPTA LA ARQUITECTURA ZERO TRUST

Moderniza el acceso a aplicaciones internas que tradicionalmente requieren una VPN. Asegura conexiones autenticadas y verifica que los dispositivos sean conocidos y fiables antes de permitir el acceso.

CLOUDFLARE®

www.cloudflare.com

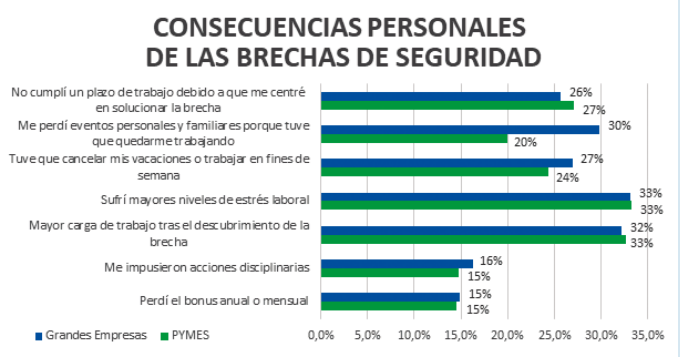
V-Valley the Value of esprinet

Contacto:
enterprise@cloudflare.com
+34 518 880 290

También ha detectado el número más alto de ciberincidentes contra cajeros en los últimos años

KASPERSKY detecta el doble de vulnerabilidades en sistemas industriales que el año pasado, además de alertar sobre la sobreocupación de los CISOs

La nueva investigación del ICS CERT de **Kaspersky** sobre las amenazas que afectan a los sistemas de control industrial (ICS), destaca 103 nuevos fallos encontrados en 2019, que podrían ser potencialmente explotados en ciberataques contra estos entornos. La mayoría se localizaron en las herramientas de administración remota (34), Scada (18), software de *backup* (10), así como en los productos de IoT, soluciones para edificios inteligentes, PLC y otros componentes industriales.



Lo preocupante, según el documento, es que el número de fallos de seguridad casi se duplicó respecto a 2018, con 61. "El éxito de la respuesta ante estas y otras amenazas puede depender del grado de conocimiento por parte de los equipos de seguridad de OT", destacan los responsables del informe.

Ciberseguridad vs conciliación familiar

La firma rusa también ha dado a conocer su informe 'El cuidado de la seguridad corporativa y la privacidad del empleado: por qué la ciberprotección es vital tanto para las empresas, como para sus trabajadores'. Un interesante estudio en el que destaca el "lado humano" de los incidentes de ciberseguridad, al examinar la incomodidad y las pérdidas que sufren los empleados a causa de las brechas de datos.

Por ejemplo, constata que alrededor de un tercio (30%) de los que se ven involucrados en este tipo de casos quitaron tiempo de ocio, trabajaron toda la noche (32%) o sufrieron estrés adicional (33%). Incluso, más de una cuarta parte tuvo que cancelar sus vacaciones (27%).

Objetivo: cajeros automáticos

También, ha sido especialmente relevante la alerta de Kaspersky cuyos analistas han constatado que los ataques contra los cajeros automáticos han alcanzado, en los últimos años, su mayor nivel de actividad. De hecho, entre 2017 y 2019, el número de dispositivos ATM/PoS únicos protegidos por la marca, en los que se encontró malware creció casi 2,5 veces, según las estadísticas de su Security Network. Las áreas donde se registró mayor actividad en 2019 fueron Brasil y Rusia, aunque también tuvieron mucho impacto, en los últimos tres años, en Alemania, Italia, Estados Unidos, Turquía, India y Vietnam.

Protección OT

Por otra parte, la compañía proveedora de energía, **Alperia,** ha elegido a Kaspersky para la protección de los sistemas de control remoto de sus centrales eléctricas y la red de distribución que da energía a 280.000 usuarios en Tirol del Sur (Italia). Para ello, utilizará la solución Kaspersky Industrial Cybersecurity for Nodes, especializada en protección OT para evitar el riesgo de interrupción de servicio.

ÁUDEA apuesta por la concienciación en ciberseguridad con un nuevo blog técnico

Áudea, consultora en ciberseguridad, privacidad, GRC y formación, ha presentado su nuevo proyecto para impulsar la cultura en protección cibernética. Se trata de su blog 'Ghost Line Security' (www.ghostlinesecurity.com), en el que participarán de forma muy activa los expertos de su Equipo Técnico del Área de Ciberseguridad, integrado por investigadores y analistas que han dado luz a esta iniciativa durante el estado de alarma de la crisis de la Covid-19, con el "objetivo de enriquecer a la Comunidad".

De momento, 'Ghost Line Security' tendrá formato de repositorio y en él se publicarán las investigaciones propias del Equipo de Ciberseguridad, además de compartir avances de los nuevos servicios de la compañía. Esta publicación "supone para Áudea un paso más para continuar creciendo en la línea de la I+D técnica, aportando, a la vez, nuestro granito de arena en esta era digital en la que vivimos compartiendo conocimiento con la Comunidad", destacan sus responsables.

EVOLUTIO se desgaja en España de BT, de la mano del fondo Portobello Capital, con gran foco en seguridad

El mercado de las comunicaciones en España cuenta con un nuevo actor tras la presentación de **Evolutio,** *spin off* de BT. La nueva marca es fruto de la venta del negocio de la compañía británica al grupo inversor **Portobello Capital**, por una cifra que se estima en los 200 millones de euros, y que hereda buena parte del equipo profesional y directivo de BT España, así como de su negocio.


Jacinto Cavestany

Evolutio gestionará los activos correspondientes a los servicios de telecomunicaciones, de computación en la nube, ciberseguridad y de tecnologías de la información propios de los clientes españoles, tanto con alcance internacional como doméstico, lo que supone más de un 85% de la cartera de clientes de la empresa en el país. La compañía tiene el objetivo de ser el socio estratégico en la integración de servicios *cloud* para compañías globales del mercado español, de la mano de socios como **Akamai, Avaya, AWS, Google Cloud, HPE, IBM, McAfee, Microsoft, NetApp, Nokia, Oracle, Salesforce** o **Zoom**, entre otras.

Para ello, Evolutio contará con una plantilla de casi 1.000 profesionales, casi todos ellos procedentes del anterior equipo profesional de la filial británica en nuestro país, al frente de la que continuará **Jacinto Cavestany**, hasta ahora responsable de BT España y que pasará a ser CEO de Evolutio. "Las necesidades de nuestros clientes evolucionan y, con ellas, nosotros también. Queremos seguir impulsando su innovación digital y maximizar el valor de sus negocios, conectando, gestionando y protegiendo sus datos y aplicaciones, gracias a toda nuestra experiencia como integrador de servicios *cloud*. Esperamos y confiamos en que este salto adelante les ayude a ganar agilidad, flexibilidad y capacidad de innovación y disrupción", ha destacado Cavestany.

CIBERSEGURIDAD

Diagnóstico Express de Seguridad

¿TE GUSTARÍA TENER UNA VISIÓN ACTUALIZADA DEL RIESGO ASOCIADO A TUS SISTEMAS DE ACCESO REMOTO EN 5 DÍAS?

Debido a la situación provocada por el COVID19, muchas empresas se han encontrado con la necesidad de proporcionar acceso remoto a sus empleados con el fin de garantizar la continuidad de las operaciones.

Existe el riesgo de que este despliegue de contingencia haya introducido vulnerabilidades en los sistemas de accesso remoto. Específicamente, en los sistemas VPNs y escritorios virtuales (VDIs).

Nuestro objetivo es proporcionar a los responsables de seguridad un DIAGNÓSTICO RÁPIDO DE SEGURIDAD de los sistemas de acceso remoto enfocado en la identificación de las vulnerabilidades más relevantes.

RÁPIDO, CONFIABLE Y A COSTE REDUCIDO

marketing.TIC@gmv.com

gmv.com

gmv®
INNOVATING SOLUTIONS

EXCLUSIVE amplía su cartera integrando soluciones de HYCU y aliándose con CHRONICLE

Exclusive Networks ha llegado a un acuerdo de distribución con **Hycu,** especialista en software empresarial para copia de seguridad, recuperación y monitorización de datos para la próxima generación de nubes empresariales.

Esta alianza, que inicialmente se circunscribía a Reino Unido, los países nórdicos y Oriente Medio, se ha ampliado a Iberia para ofrecer a miles de socios un acceso más rápido a las soluciones para infraestructuras multinube locales e hiperconvergentes de Hycu. Así, los socios de canal de Exclusive Networks podrán disponer de una oferta tecnológica integral que, además, es apta para trabajar con los clientes de Nutanix Enterprise Cloud, incluyendo la recientemente presentada Nutanix Mine con Hycu, una solución de almacenamiento secundario integrada y diseñada para esta colaboración.

Como parte del acuerdo, Exclusive ya ha puesto en marcha un conjunto de iniciativas comerciales encaminadas a acelerar el desarrollo de mercado de esta empresa.

Acuerdo con Chronicle

Además, Exclusive Networks también ha firmado de un contrato de distribución con **Chronicle**, del grupo **Google Cloud**, que cubre la región del sur de Europa. Con esta asociación, brindará a su red de socios acceso a la plataforma de análisis de seguridad de esta compañía. Con Chronicle, los clientes pueden almacenar y monitorizar continuamente sus registros para investigación, detección de ataques y respuesta a incidentes mucho más rápido gracias al poder del motor de búsqueda de Google. Chronicle recopila, normaliza, indexa, correlaciona y enriquece los datos de seguridad de fuentes heterogéneas (en las instalaciones y en la nube) y proporciona análisis instantáneos y contextualización de actividades riesgosas.

ARSYS renueva la certificación ENS en su apuesta por la seguridad del sector público

Arsys ha renovado la certificación del ENS (Esquema Nacional de Seguridad) de **Aenor**. Esta certificación, conseguida en su nivel medio, la habilita para seguir trabajando con cualquiera de los organismos vinculados a la Administración Pública en el territorio español con las altas garantías en seguridad de los sistemas de información. De este modo se acredita, con una validez de dos años, que Arsys cumple con un Esquema que establece los principios básicos y requisitos mínimos de seguridad de los sistemas de información que exigen las Administraciones Públicas con el objetivo de generar confianza en dichos sistemas.

Arsys proporciona así soluciones de infraestructura IT basadas en Servidores Cloud y Servidores Dedicados con los niveles de servicio, seguridad y disponibilidad que las entidades públicas requieren para tratar, procesar y almacenar datos.

Además, la compañía cuenta con el SAP Certified in Cloud and Infrastructure Operations, el Certificado de Buenas Prácticas para el Comercio-e de Aenor, Seguridad ISO 27001 y Calidad ISO 9001.

MINSAIT y BANKIA suman fuerzas para reducir el fraude bancario y las anomalías

Bankia y **Minsait** han firmado un acuerdo de colaboración con el fin de convertirse en el principal referente frente a la lucha contra el fraude bancario y las anomalías de ciberseguridad. El acuerdo tiene como objeto desarrollar, implantar y comercializar una solución antifraude, basada en IA, por un lado, capaz de prevenir, detectar y contener tendencias o patrones de fraude y, por otro, detectar anomalías en el ámbito de la ciberseguridad.

Esta solución permitirá así optimizar la seguridad, confianza y experiencia de los clientes de las entidades financieras y empresas de otros sectores de actividad.

El considerable aumento del número de transacciones en el entorno digital y la necesidad de dotar de mayor protección a las operaciones realizadas en servicios de venta en línea, pago sin contacto o transferencias, entre otros, propicia el riesgo de ciberdelitos como el fraude, algo que constituye un auténtico desafío para entidades financieras y empresas dentro de su entorno multicanal.

Esta alianza implica la combinación de algoritmos, inteligencia y explotación de datos históricos de ambas instituciones y contempla el desarrollo de una solución antifraude con capacidad de respuesta rápida y confiable que permitirá abordar los desafíos presentes y futuros en este campo. **SIA**, adquirida recientemente por Indra, aportará sus capacidades para desarrollar las iniciativas contempladas en el marco del acuerdo. La solución utilizará motores de detección basados en técnicas de aprendizaje automático, redes neuronales con IA, niveles de procesamiento *in memory computing* y la creación de patrones apoyados en conocimiento experto sobre actividades fraudulentas.

WATCHGUARD completa la compra de PANDA

La estadounidense **WatchGuard Technologies,** especializada en inteligencia y seguridad de red, *wifi* seguro y autenticación multifactor acaba de cerrar la compra de la española **Panda Security**, por entre 200 y 300 millones de euros, según fuentes del sector.

Con ello, Panda ha pasado a ser subsidiaria al 100% de WatchGuard, formando una empresa combinada que permitirá a los partners y clientes de ambas acceder a sus soluciones de seguridad. Así, se beneficiarán de funcionalidades de detección y respuesta avanzada de amenazas, impulsadas por IA, de técnicas de elaboración de perfiles de comportamiento y de correlación de eventos de vanguardia.

También, les permitirá contar con beneficios operativos adicionales como una gestión centralizada de la seguridad de red y del punto final. "Creemos que el equipo y la tecnología de Panda encajan perfectamente en la cultura de WatchGuard y la complementa. Nuestros clientes y *partners* necesitan acceso a una seguridad, de nivel empresarial, creada para los requerimientos del mercado. WatchGuard se centra en proporcionar estos servicios de protección, a través de una plataforma de seguridad enfocada en MSP, que simplifica todos los aspectos del suministro de seguridad, y consolida nuestra posición como la solución de seguridad, de facto, para el mercado medio", explica el CEO de WatchGuard, **Prakash Panjwani**.

Como parte de la transacción, **Investing Profit Wisely (IPW)** se unirá a **Vector Capital** y **Francisco Partners,** como accionista de WatchGuard Technologies, y el CEO de Panda Security, **Juan Santamaría,** se unirá al consejo de administración de la compañía estadounidense.

SCAN ME

Para desarrollar de forma óptima los programas PAM, las organizaciones necesitan unas directrices estratégicas. El modelo de CyberArk ayuda a reducir el riesgo siguiendo tres reglas de oro que responden a las últimas iniciativas de transformación digital.

Obtenga más información y apúntese a una sesión sobre el modelo en https://www.cyberark.com/es/blueprint/

CYBERARK

AURIGA adquiere la solución de cajeros automáticos Lookwise Device Manager a S21SEC

Auriga, proveedor de soluciones tecnológicas para los sectores de la banca omnicanal y de pagos, adquirió Lookwise Device Manager (LDM), una histórica plataforma de seguridad modular y unidad de negocio de **S21sec,** especializada en servicios de seguridad gestionada, que forma parte de la cartera de Sonae IM, una empresa corporativa de capital de riesgo que invierte en compañías de tecnología de ciberseguridad, *retail* y telecomunicaciones.

Mediante la integración de LDM en el paquete de software WWS de Auriga, sus clientes podrán contar con mayor protección, gracias a la monitorización de la seguridad, y beneficiarse del control de sus dispositivos de red críticos para el negocio, como cajeros automáticos, terminales de punto de venta y sistemas de control de infraestructuras críticas. Además, diseñada como una solución de seguridad integrada, proporciona las capacidades de contramedidas más avanzadas y eficaces para detener la nueva generación de ataques. Y es que, se trata de una plataforma de seguridad modular que ofrece funcionalidades para garantizar estos tres aspectos y adecuarlos a los dispositivos críticos.

Tras la adquisición, Auriga continuará invirtiendo en la investigación y desarrollo de LDM e impulsará mejoras, entre ellas, una mayor rapidez de comercialización para la implementación.

TELEFÓNICA logra el estatus de Competencia en Seguridad de AWS, a través de ELEVENPATHS, y protegerá los entornos TI/OT junto con SIEMENS

ElevenPaths ha alcanzado el estatus de Competencia en Seguridad de **Amazon Web Services** (AWS). Un reconocimiento fruto de la capacidad de ElevenPaths en ayudar a proporcionar seguridad en la nube para entornos corporativos, alineados con las mejores prácticas y guías de seguridad de AWS combinadas con la experiencia de la compañía de ciberseguridad de Telefónica en el diseño de plataformas de protección y procesos para la adecuada gestión de la seguridad en la nube.

AWS brinda soluciones escalables y flexibles dirigidas tanto a *startups* como a empresas globales. Para apoyar la integración y el despliegue continuo de estas soluciones, AWS estableció el Programa de competencias con vistas a ayudar a los clientes a identificar a los socios consultores y tecnológicos de su Red, APN Network, con gran experiencia y pericia en la industria.

Lograr esta Competencia en Seguridad, así pues, distingue a ElevenPaths brindando servicios de consultoría especializados para ayudar a las empresas a adoptar, desarrollar y desplegar proyectos complejos de seguridad que permiten proteger sus entornos en AWS para establecer y mantener una adecuada postura de seguridad en la nube en AWS. Además, **Telefónica Tech,** mantiene una colaboración estratégica con Amazon Web Services para hacer más fácil la transición a la nube.

Asimismo, Telefónica ha creado un **Centro de Excelencia Cloud** en España y Brasil, a los que se sumarán el resto de los países de la región de Telefónica Hispam.

Acuerdo con Siemens

Telefónica, además, ofrecerá junto con Siemens, soluciones integrales de ciberseguridad TI/OT para ayudar a sus clientes en su transformación digital. Así, Siemens Digital Industries aportará su tecnología y servicios de consultoría y auditoría, incorporando productos tanto en el terreno de los componentes de red industriales, como en el área de los controladores y sistemas de visualización.

Por su parte, Telefónica ofrecerá su portafolio de servicios de seguridad y la experiencia en el ámbito IT para complementar el diseño del plan de seguridad del cliente y actuar en el caso de que se detecte cualquier vulnerabilidad.

BREVES

■ **Víntegris**, perteneciente a **Euronovate Group**, ha sido validada como prestadora para emitir durante el estado de alarma certificados electrónicos cualificados mediante videoconferencia. Este reconocimiento en concreto se centra en su solución Tap-ID, una plataforma de identidad digital (ID) para particulares, empresas y organizaciones que permite recopilar, verificar y acceder de forma fácil, segura y certificada a las identidades de los usuarios, vía Blockchain. Además, el Ministerio de **Asuntos Económicos y Transformación Digital** también la ha incluido en su lista de "prestadores de sistemas de expedición de certificados electrónicos cualificados mediante videoconferencia".

■ **Varonis** se ha unido al portafolio de fabricantes de ciberseguridad del mayorista **Ingecom**. Especializada en detección de amenazas y clasificación de la información corporativa, esta alianza abarca todos los países donde el distribuidor tiene presencia –España, Portugal e Italia–. "Las compañías se están moviendo desde redes on premise a plataformas de colaboración y almacenes de datos en la nube. Mientras que, por una parte, la conectividad remota impulsa los negocios en cualquier lugar, al mismo tiempo proporciona a los ciberdelincuentes un mayor espectro de ataques. Para dar respuesta a esta situación con Varonis es posible identificar y proteger los datos sensibles de las empresas con el mínimo privilegio", ha explicado el Channel Manager de Varonis para Iberia e Italia, **Juan Gosálvez**.

■ La **Red Europea para la Seguridad Cibernética** (ENCS) sumó en mayo dos nuevos socios, la **National Grid Gas Transmission** (NGGT) y la **National Grid Electricity Transmission** (NGET), del Reino Unido. Se trata de una organización de la que forman parte las principales compañías eléctricas y de gas del Viejo Continente, siendo España representada por **Iberdrola.** Su objetivo es compartir información sobre amenazas cibernéticas y debatir sobre cómo proteger mejor el sector energético europeo contra los ciberataques.

■ Nace la primera **Alianza Europea de la Industria de Pagos Digitales** (Edpia). Creada por cuatro de las empresas referentes en el sector, **Ingenico Group, Nets, Nexi** y **Wordline**, tendrá como fin "participar en los debates sobre políticas" que afecten al sector de los pagos de la UE, según informaron en un comunicado. La alianza espera impulsar el papel de esta industria "a través de un diálogo constructivo con los responsables políticos y otras partes interesadas que determinan el panorama de los pagos en Europa". Edpia considera que un marco normativo europeo "sólido y debidamente aplicado" podrá garantizar una competencia justa entre soluciones de pago transparentes, que conozcan el mercado y que busquen la confianza de los usuarios de estos servicios. Además, considera que la UE debería basarse en el proyecto SEPA, que hará que progresen nuevas tecnologías como los pagos de cuenta a cuenta, incluso entre cuentas de diferentes países.

LOGICALIS
Architects of Change

es.logicalis.com

QRadar, seguridad inteligente para su negocio

QRadar lleva la seguridad a un nuevo nivel con su analítica avanzada de amenazas, una solución ajustada al negocio, actual y futuro, de cada empresa.

Una plataforma flexible que permitirá a su equipo de seguridad afrontar todo tipo de potenciales peligros y retos que comprometan su compañía.

Potencie la seguridad de su organización con QRadar, escale sus defensas y analice automáticamente millones de amenazas potenciales.

¿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

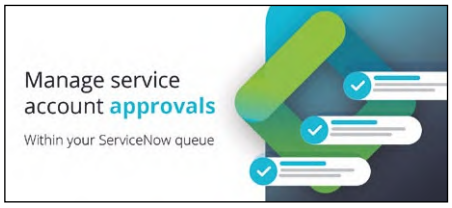
Si quiere saber más sobre los desafíos comunes y mejores prácticas descárguese el siguiente QR

La integración de THYCOTIC y SERVICENOW elimina cuellos de botella para la aprobación de cuentas de servicio

Thycotic, proveedor de soluciones de gestión de acceso privilegiado (PAM) se integrará en la plataforma **ServiceNow,** de servicios de TI. Exactamente lo hará a través de su solución Thycotic Account Lifecycle Manager para la gobernanza de las cuentas de servicio. Con ello, espera ofrecer una buena opción para resolver las aprobaciones de flujo de trabajo, un cuello de botella común que genera frustración para muchos equipos de TI que administran cuentas de servicio privilegiadas.

Más supervisión

Las cuentas de servicio privilegiadas, que conectan aplicaciones, bases de datos, cuentas raíz y otros



sistemas de TI, comparten información confidencial y realizan procesos críticos para el negocio, a menudo automáticamente. Sin supervisión humana, las cuentas de servicio pueden quedar fácilmente sin administrar y olvidarse, abriendo la puerta a los ataques cibernéticos. Para evitarlos, la herramienta de Thycotic busca garantizar que cada cuenta de servicio esté vinculado a un propietario que tenga los niveles adecuados de responsabilidad y supervisión.

Un flujo de trabajo típico para configurar o proporcionar acceso a una cuenta de servicio privilegiado de alto riesgo a menudo requiere una segunda capa de aprobación. Sobre todo, cuando los trabajadores en remoto o contratistas externos solicitan acceso privilegiado, las aprobaciones son críticas para mantener la seguridad sin interrumpir la productividad. La solución integrada entre Thycotic Account Lifecycle Manager y ServiceNow acepta una solicitud de cuenta, identifica el equipo de respuesta correcto y activa las comunicaciones dentro del flujo de trabajo existente. Los que aprueban la solicitud la ven en el mismo sistema de gestión de servicios que utilizan el resto de peticiones, por lo que se atienten todas de forma coordinada. Como resultado de la integración, cada paso en el proceso de aprobación se acelera y se rastrea.

En cientos de solicitudes de aprobación de cuentas de servicio, los ahorros pueden ser sustanciales. La sinergia Thycotic-ServiceNow también proporciona la capacidad de rastrear la finalización del ticket de aprobación y demostrar el cumplimiento de los acuerdos de nivel de servicio de TI.

ALHAMBRA IT presenta su solución de medición térmica y es reconocida Gold Partner de SOPHOS

Alhambra IT ha integrado en su catálogo soluciones de medición térmica a distancia y control de aforos para combatir la Covid-19, y dar respuesta a la necesidad de las organizaciones por garantizar la salud de trabajadores, clientes y proveedores, durante la 'nueva' normalidad. La medición de temperatura es una solución que puede instalarse en los puestos de control de los edificios o en zonas altamente transitadas para conocer la temperatura de la persona en tiempo real y sin contacto entre las partes.

Además, Alhambra IT ha reforzado su área de ciberseguridad, OneseQ, creada en 2016, convirtiéndose en Gold Partner de Sophos, por su "expertise, a nivel técnico y comercial, así como por sus garantías de calidad".

NOMBRAMIENTOS

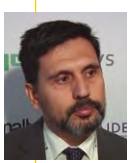
● **BBVA** ha designado a **Antonio Ávila** como Head of Corporate Security para Perú. Ingeniero informático, hasta ahora venía siendo el CISO Corporate Functions Engineering en la entidad. También ha trabajado, entre otras, para la Sociedad Estatal de Loterías y Apuestas del Estado y Fon Wireless.

● **Prosegur Alarmas** ha promocionado a CISO desde el pasado abril a **Walter Santiago Dobal.** Titulado en TI por la Universidad de San Luis, lleva 18 años en la compañía donde comenzó en el departamento de soporte técnico y en la que ha desempeñado diferentes roles de responsabilidad.

● El CEO y Analista de Seguridad de **One eSecurity, Jess García,** ha sido distinguido por **Sans Institute** como Senior Instructor, uno de los más altos reconocimientos en esta institución formativa con la que colabora desde 2002. También es Presidente de Insectra Technology Services y ha trabajado para organismos de referencia, como el Instituto de Técnica Aeroespacial (Inta). Es ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid y Premio SIC.

● **Áudea Seguridad de la Información** ha incorporado recientemente a **Isabel María Gómez** en calidad de Directora de Ciberseguridad y a **Angélica Zamora** como Responsable del Área GRC (Gobierno, Riesgo y Cumplimiento). Con más de 18 años de experiencia, Gómez ha trabajado para Medtronic y Bankia, entre otras organizaciones. Por su parte, Zamora, ingeniera de Sistemas, cuenta con una trayectoria profesional de más de 19 años como responsable de seguridad, CISO y jefe de proyecto en empresas como Prosegur, Oesia, Azertia y Grupo Financiero de Interacciones, entre otras. Cuenta con certificaciones como CISA, CISM, QSA PCI-DSS, Lead Auditor ISO 22301 y un MBA especialidad en *eBusiness.*

● **Antonio Sahagún** ha sido promocionado a Head of Internal Cybersecurity Sales y **Rames Sarwat** a Chief Revenue Officer en **ElevenPaths**. Sahagún es cofundador de Cheefy y ha trabajado para compañías como Oesia, Matchmind, Germinus y Everis, entre otras. Sarwat ha sido responsable del programa de partners y CSA en la compañía de Telefónica desde 2016, además de haber trabajado para Smart Access, la Asociación Aslan y Microsoft Ibérica, entre otras.



● **Transmit Security** ha promocionado a **David Navarro** como Vicepresidente de Ventas de Iberia y Latinoamérica. Navarro es titulado en Administración de Empresas por el ESIAE de París y ha ocupado puestos de responsabilidad en IBM, Trusteer, RSA y EMC, entre otras.

SailPoint

Rethink identity.

Descubra cómo el Gobierno de la Identidad puede ayudar a su organización

- Automatizar las certificaciones de acceso
- Modelar los accesos con AI
- Recomendar accesos
- Analizar los accesos de todos los usuarios

sailpoint.com/es

MCAFEE y ZYXEL aúnan esfuerzos para proteger de forma integrada a la pyme

Zyxel Networks, especializado en soluciones empresariales de seguridad basadas en IA y la nube, y **McAfee** abrirán una nueva línea de negocio para ofrecer una solución de seguridad integrada en un solo dispositivo a pequeñas y medianas empresas. Con ella se quiere ayudar a estos negocios, que en España suponen la mayor parte del tejido empresarial, a contar con "soluciones de seguridad robustas y fáciles de implementar y gestionar que se ajusten a su tamaño", destacan ambas compañías recordando los datos del informe Data Breach Investigation de Verizon de 2019, que resalta que más del 40% de los ciberataques que se realizan actualmente se dirigen a pymes. La integración de la tecnología anti*malware* de McAfee en la familia de *firewalls* ATP (Advanced Threat Protection) de alta gama de Zyxel proporcionará a las pymes soluciones con seguridad contrastada para la detección de software malicioso, rendimiento en seguridad y filtrado web. Todo ello en un solo dispositivo llegando, a través dicha integración, a ofrecer una defensa frente a ataques de 'día cero' a las redes corporativas.

Zyxel también ha anunciado la incorporación de los modelos ZyWall ATP100W y ATP700 a la serie de cortafuegos ATP para pymes. Estas soluciones 'todo en uno' integran *sandboxing* basado en nube con múltiples capas de seguridad adicionales para detectar y bloquear amenazas conocidas y desconocidas.

ONE IDENTITY logra la certificación Common Criteria para su solución Identity Manager 8.1

One Identity, proveedor de seguridad de identidades, ha logrado la Certificación Common Criteria que otorga la **National Information Assurance Partnership** (NIAP) para su solución de gestión y administración de identidades (IGA) Identity Manager 8.1. Dicha certificación, para la Gestión de la Seguridad de la Empresa (Identity and Credential Management v2.1) ha requerido que One Identity cumpla con rigurosos requisitos de seguridad para demostrar su eficacia tanto para las instituciones gubernamentales, incluidas entidades autonómicas, estatales y locales, como empresariales. La certificación CC de NIAP incluye pruebas independientes para satisfacer requisitos precisos y rigurosos de seguridad y garantía, y de conformidad con la normativa de la Organización Internacional de Normalización (ISO) y el estándar 15048 de la Comisión Electrotécnica Internacional (IEC) para la evaluación de la Seguridad TI.

Una protección de datos e identidades robusta

La mayoría de las violaciones de datos de alto perfil son el resultado del acceso inapropiado, bien externo de manos de los ciberdelincuentes, o bien de recursos internos que acceden a datos, sistemas o procesos sin autorización. Según una reciente encuesta de One Identity, realizada entre los asistentes a la Conferencia RSA 2020, el 49% de las entidades no confían en que su organización cumpla con las últimas normas de privacidad y seguridad de datos.

De este modo, la certificación Common Criteria es una medida que los fabricantes de seguridad deben adoptar para mejorar su capacidad de ayudar a las organizaciones a evitar este tipo de deficiencias de seguridad.

NOMBRAMIENTOS

● **Bitdefender** ha fichado a **Emilio Román** como Vicepresidente para la región de EMEA para impulsar los objetivos de crecimiento de la compañía. Con más de 20 años de experiencia liderando equipos, Román tiene un amplio conocimiento en ciberseguridad y en el área *cloud*. Ha desempeñado distintos cargos de responsabilidad en Samsung, Fortinet y Scality. Es ingeniero de telecomunicaciones y cuenta con un MBA por la IE Business School.

● **Iván Sanz de Castro** ha sido designado por **Wise Security Global** como Head of Cybersecurity. Ingeniero de Telecomunicaciones, cuenta con un Máster por la Universidad Europea en Tecnologías de la Información y, con anterioridad a esta incorporación, trabajó para organizaciones como PwC, Telefónica y Axa Seguros. Cuenta con el certificado CSX, de Isaca.

● **Vesku Turtia** ha sido fichado por **Cybereason** como Regional Sales Director en Iberia. Licenciado en Administración de Empresas por la Universidad Europea, cuenta con más de 20 años de experiencia en diferentes cargos de responsabilidad en multinacionales del sector. Comenzó su carrera profesional en el ámbito de las materias primas, en los mercados españoles y de Oriente Medio, para trabajar en ciberseguridad a partir del 2000, desempeñando diferentes roles en organizaciones como Stonesoft, Nozomi Networks, FireEye, F-Secure Corporation, y Fortinet.

● **Alsid** ha designado a **Jesús Barrajón** Country Manager para España y Portugal. Ingeniero de Telecomunicaciones por la Universidad de Vigo, Barrajón ha trabajado para Aerohive Networks, Exclusive Networks y Polycom, entre otras. También, cuenta con sendos MBAs por el UCF College of Business y la EOI Business School.

● **Forescout** ha promocionado a Country Manager para España y Portugal a **José Antonio Sánchez Ahumada**, que lleva en la compañía desde 2013, donde ha desempeñado diferentes responsabilidades. Con anterioridad, también trabajó para compañías como Juniper Networks, Afina y Accenture, entre otras.

● **Pablo Vera** ha sido contratado como Enterprise Security Executive en **Microsoft.** Con más de 20 años de experiencia en multinacionales de telecomunicaciones y de cibrerseguridad, Vera ha trabajado para empresas como Symantec, FireEye, McAfee y Network General, entre otras. Es Ingeniero de Telecomunicaciones por la Politécnica de Madrid.

● **RavenLoop** ha designado como Director Comercial a **Ángel Castellanos**. Con más de 15 años de experiencia en gestión de ventas en Iberia, en ciberseguridad y redes, ha trabajado para compañías como Ingecom, Allot Communication y Trend Micro, entre otras.


VSOC AIUKEN
TODAS LAS CLOUD EN UN SOLO SOC
POWERED BY
Google Cloud
POWERED BY
Microsoft
POWERED BY
amazon
Aiuken
Cybersecurity

ESET ayuda a los CERT de la UNIÓN EUROPEA, dándoles soporte, para mejorar la protección frente a las ciberamenazas durante la pandemia

Eset ha ofrecido, desde que comenzara la pandemia, un plan de refuerzo a los CERT (Computer Emergency Response Teams, o Equipos de Respuesta ante Emergencias Informáticas) de la **Unión Europea** para ayudar a reducir el impacto de las ciberamenazas durante estos meses. Una labor que lleva haciendo también con otras organizaciones de la UE, como **Europol** o la iniciativa 'NoMoreRansom', para proteger y garantizar la seguridad *online* de los ciudadanos europeos. En esta ocasión ofrecerá medio año de acceso, sin coste, a los datos del motor de inteligencia de amenazas de la compañía con información sobre dominios, URLs y archivos maliciosos, así como también a información actualizada sobre las *botnets* activas.

El motor de Inteligencia contra Amenazas de Eset utiliza la información recopilada desde más de 110 millones de sensores para compartir la toma de decisiones inteligentes con los usuarios de la compañía. Gracias a sus datos, los CERT podrán mejorar su capacidad para monitorizar posibles amenazas con el objetivo de reducir los riesgos de posibles ataques y de potenciar sus defensas. La colaboración es una parte esencial de la inteligencia frente a amenazas y ESET ha contactado con 46 CERT de toda Europa para ofrecerles sus servicios gratuitos.

"Creemos que todos los ciudadanos tienen el derecho a disfrutar de un uso seguro de la tecnología y eso significa que el sector público debe estar equipado con los recursos que protejan tanto a las personas, como a las infraestructuras", ha explicado el Director de Negocio de Eset, **Ignacio Sbampato**.

ARROW distribuirá las soluciones de FORCEPOINT para la seguridad en la nube

Arrow ECS distribuirá las soluciones de **Forcepoint** dedicadas a la protección de aplicaciones y usuarios basados en la nube, la seguridad de datos y redes, así como la defensa frente amenazas internas. Gracias a ellas, las empresas pueden proteger las interfaces entre usuarios, sistemas y datos. Entre el portafolio de soluciones que comercializa Forcepoint se encuentran también sus cortafuegos de última generación y las soluciones Secure Web Gateway para la protección de redes empresariales. Además, cuentan con soluciones de protección de datos como Data Loss Prevention (DLP) y Cloud Access Security Broker (CASB).

"Forcepoint ofrece una plataforma orientada a dar servicio de monitorización y análisis de comportamiento de usuario, hacer seguras las conexiones de los usuarios y proteger los datos de las empresas, cubriendo así una amplia gama de necesidades entre los clientes, por lo que cobrará un especial interés para nuestra comunidad de canal", ha comentado el Director General de Arrow ECS para España y Portugal, **Ignacio López Monje.** "Los usuarios son el nuevo perímetro, el enfoque de protección orientado al comportamiento del usuario que ofrece Forcepoint constituye la mejor estrategia para proteger las conexiones de los usuarios y proteger los datos críticos, ayudando a las organizaciones en su recorrido de la transformación digital", ha añadido la Directora General de Forcepoint para España y Portugal, **Elena Cerrada**.

NOMBRAMIENTOS




● **Zscaler** continúa fortaleciendo su equipo en España con la incorporación de **Juan Carlos Peña** y **Jorge Perez,** ambos como Regional Sales Manager, así como de **Pablo Valenzuela** y de **David Díez,** como Systems Engineer. Peña, ingeniero, ha trabajado para compañías como Symantec, Nortel Networks y Banesto, entre otras. Pérez, ingeniero de Telecomunicaciones, ha desempeñado diferentes roles en Alhambra Eidos, Check Point y Symantec. Por su parte, Valenzuela, con una experiencia de más de 20 años en preventa, ha trabajado para Symantec, Buguroo, Imperva y Exclusive Networks, entre otras. Díez, ingeniero informático, cuenta con más de 15 años de experiencia en el sector en empresas como Blue Coat, Symantec y Palo Alto Networks, entre otras.


● **SailPoint** ha reforzado su equipo local en Iberia con la incorporación de **Fernando de los Ríos** y **Miguel Hormaechea** como Sales Engineer y Territory Sales Manager, respectivamente. Ambos provienen de Micro Focus, donde el primero fue International IAM Practice Lead, Senior Sales Engineer y Technical Account Manager, entre otros roles. Es licenciado en Informática y en Estadística. Por su parte, Hormaechea cuenta con siete años de experiencia en el área de ventas, habiendo dedicado los últimos años a los portafolios de dicha compañía de modernización y seguridad para *mainframe* y AS/400 para Iberia, Turquía y Grecia.



● **Proofpoint Iberia** ha fichado a **Jorge Burgoa** como Business Development Representative, **Pedro Alamo** como Senior Named Account Manager, para el Sector Público, y **Javier Baquero** en calidad de Senior Channel Manager. Burgoa, graduado en Economía por la Universidad de Valladolid, ha trabajado para CIS21 en tareas de venta e integración de software ERP, así como de asesoramiento en materia de ciberseguridad. Álamo, Ingeniero Superior de Telecomunicación por la Politécnica de Madrid, lleva 20 años vinculado al mundo TIC en compañías como Telindus, Unitronics y Huawei y Baquero, que cuenta con más de 27 años en el mercado español de las Telecomunicaciones y la ciberseguridad, tiene una larga trayectoria profesional en multinacionales como Nortel Networks, Juniper, Bluecoat y Symantec, donde fue, en los últimos ocho años, Director de Canal y Distribución para Iberia.

● **Pablo Estevan** ha sido fichado por **Palo Alto Networks** como Senior Systems Cortex Presales. Hasta ahora, Estevan había ocupado el puesto de Senior Systems Engineer en RSA. Con anterioridad, también desempeñó cargos de responsabilidad para compañías como Masternaut, Innovae y Secuware, entre otras. Es licenciado en Informática por la universidad Complutense.

BITGLASS integra la tecnología de aprendizaje automático de CROWDSTRIKE ante amenazas avanzadas de día cero en la nube

Bitglass y **CrowdStrike** han firmado una alianza que permitirá proporcionar una solución de protección contra las amenazas avanzadas (ATP) sin agentes. Esta herramienta identifica y repara las amenazas conocidas y de día cero en cualquier aplicación o servicio en la nube, así como en todos los dispositivos que accedan a los recursos de TI corporativos (incluidos los dispositivos personales).

Las políticas de aplicaciones en la nube y uso de dispositivos personales en el trabajo (BYOD) proporcionan a las compañías una mayor flexibilidad y eficiencia; pero también, pueden servir como puntos de proliferación para el *malware* si no se protegen adecuadamente. La tecnología de CrowdStrike utiliza el aprendizaje automático y la inspección profunda de los archivos para identificar el software malicioso y otras amenazas. Junto con la solución de acceso seguro a la nube de próxima generación (CASB) de Bitglass, permite responder automáticamente a las amenazas de acuerdo con las políticas preestablecidas.

El CASB de Bitglass aprovecha los *proxies* en línea sin agentes para monitorizar e intermediar en el tráfico entre las aplicaciones y dispositivos en la nube, con el fin de aplicar políticas de seguridad granulares en los datos que se transmiten.

Al incorporar las capacidades de detección de CrowdStrike directamente en el *proxy* sin agentes de Bitglass, la integración permite identificar y bloquear el *malware* en tiempo real a medida que los archivos infectados se cargan en aplicaciones *cloud* o se descargan en dispositivos (incluidos los personales), sin la necesidad de instalar software. Además, la integración con interfaces de programación de aplicaciones (API) posibilita la detección y puesta en cuarentena del *malware* que ya está alojado en la nube.

BOTECH presenta ISOPH: tecnología gratuita orientada a empresas, pymes y autónomos para que puedan conocer la seguridad de sus equipos

La cuarentena ha disparado el uso de Internet y, en consonancia, la ciberseguridad ha cobrado más protagonismo que nunca para proteger del cibercrimen la labor de los trabajadores en remoto, sin importar si pertenecen a empresas grandes o pequeñas. Entre sus mayores vulnerabilidades estuvo, precisamente, que muchos usaron sus dispositivos personales para teletrabajar con lo que esto supone: menos seguridad y descarga de programas que no son 100% fiables.

Para ayudar en su protección, **Botech** ha ofrecido durante la crisis, de forma gratuita, su tecnología ISOPH, orientada a empresas, pymes y autónomos para que puedan conocer la seguridad de sus equipos. Descargable desde www.botechsolutions.com, esta herramienta permite conocer las vulnerabilidades que presenta el equipo en el que se instala y proporciona información de gran valía para conocer su estado de seguridad, permitiendo tomar medidas para evitar incidentes.

Además, facilita el 'diagnóstico' de equipos para que se puedan tomar las medidas adecuadas y solucionar sus vulnerabilidades.

"En esta complicada situación que nos ha tocado vivir, tan solo hemos querido poner nuestro 'granito de arena' para ayudar a trabajar en un entorno más ciberseguro y que los incidentes no sean un motivo de preocupación para el trabajador", ha destacado el CEO de Botech, **Ángel Rojo.**

NOMBRAMIENTOS

Mikel Rufián ha sido promocionado a Socio Global en **Bidaidea**, donde está al frente del área de Seguridad & Inteligencia a nivel global. Con una trayectoria de más de 14 años, su formación en Telecomunicaciones e Informática, Derecho y Criminología (CEU), Inteligencia y su MBA por el IESE le han permitido combinar una visión técnica con una de negocios, que ha puesto en práctica en compañías como KPMG, Entelgy Innotec y The Coca-Cola Company, entre otras. Además, compagina su actividad profesional como profesor Universitario Internacional, instructor y mentor de *start-ups*.

Felipe San Román y **Samir Zerizar** se han incorporado a **Okta** como Ingeniero Preventa y Channel Account Manager para Iberia, respectivamente. San Román, licenciado en Físicas, se ha dedicado a la preventa en integradores tecnológicos como Telefónica y Vodafone y en fabricantes de software o equipamiento hardware como Zebra, AirWatch y VMware. Zerizar ha trabajado durante más de una década para CA Technologies y ha ocupado diferentes puestos de responsabilidad en mercados internacionales de Europa, Rusia, África y Oriente Medio.

Botech FPI ha incorporado a **Daniel Vivar** como Consultor PCI. Ingeniero de Sistemas, Vivar posee más de 20 años de experiencia en ciberseguridad y posee un Máster Executive en Dirección y Gestión de Tecnologías de la Información y en Seguridad Informática. Además, ha dirigido equipos y proyectos para la adecuación al cumplimiento normativo (ISO 27.000, ENS, RGPD), de auditorías, planes para la gestión de vulnerabilidades y de creación de requerimientos técnicos para la gestión de éstas.

Twilio ha designado a **Pedro García Milicua** como Security Incident Response Manager. Con gran experiencia en riesgos tecnológicos y de gestión de proyectos desde el punto de vista operacional, ha trabajado para organizaciones como DXC, Deloitte España y Telefónica, entre otras. García es Ingeniero en Informática por la Politécnica de Madrid.

Trend Micro ha nombrado a **Xavier Clará** como Territory Manager, **Agustín Jerez** como Customer Success Manager y a **Iñaki Zarate** como Sales Engineer. Clará, que cuenta con un Master en Gestión Tecnologías de la Información, ha desempeñado diferentes roles en compañías como Symantec, Veritas Technologies e ID Grup. Por su parte, Jerez, Ingeniero en Informática por la Pontificia de Salamanca, ha estado en Telefónica e Nfq Advisory, Solutions, Outsourcing. En cuanto a Zarate es Técnico Superior en Informática, y ha trabajado para empresas como ID Group, donde fue Responsable de Ciberseguridad, así como en Oesia y Davinci Group, entre otras.

XXXI Edición del Congreso global de Ciberseguridad, Seguridad de la Información y Privacidad

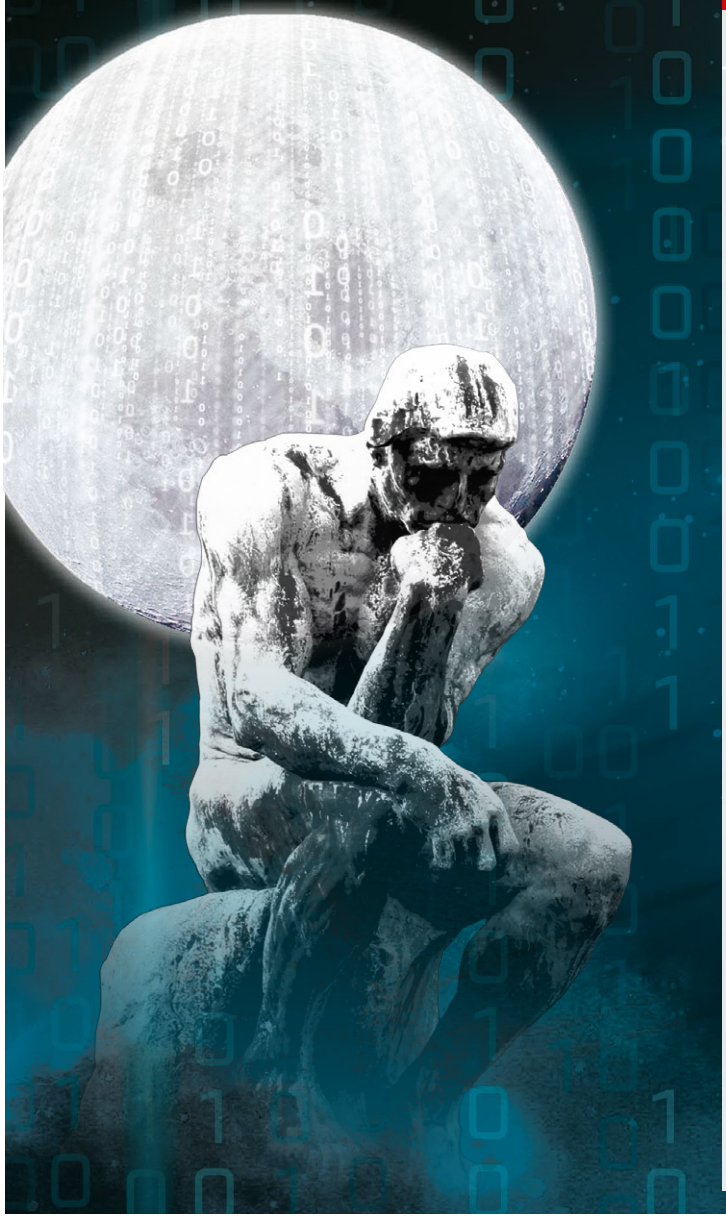
El equipo de organización reiniciará a finales de junio las acciones encaminadas a la celebración de SECURMÁTICA 2020

Con motivo de la declaración de pandemia por la Covid-19 y posterior declaración del estado de alarma en España, la organización de **Securmática** comunicó a los interesados la posposición de la celebración presencial del congreso a los días 29 y 30 de septiembre y 1 de octubre del presente en su habitual sede del Campo de las Naciones en Madrid, siempre y cuando las circunstancias lo permitan.

A fecha de cierre de esta edición, y a tenor de las informaciones disponibles, en esas fechas, presumiblemente, España se encontrará en plena fase de 'retorno' a la normalidad, por lo que hay que presumir que, tomando las medidas de higiene y salud pública pertinentes, el congreso podrá celebrarse. Y en base a esta hipótesis está trabajando la revista SIC.

La gestión de riesgos de ciberseguridad en las compañías más avanzadas, se fundamenta en la colaboración de sus equipos internos de expertos –comandados por el CISO– con prestatarios de servicios especializados. Este proceso, muy asentado en otros sectores del mercado, se ha ido sistematizando en el de seguridad de la información. Y pese a los desajustes en algunas áreas de actividad en materia de precios y escasez de recursos humanos capacitados, está dando sus frutos.

Securmática, fiel a su ideario, va pretende aportar nuevamente en esta edición, una muestra actual de los proyectos, iniciativas y enfoques en los que están embarcados los actores empresariales más adelantados en todos los frentes concernidos por la seguridad digital: personas, procesos y tecnologías, y que pueden servir como guía y ejemplo para avanzar.



AVANCE DE PROGRAMA

PRIMER MÓDULO, 29 DE SEPTIEMBRE

Ceremonia de apertura

Conferencia de inauguración

Ponencia: **El rol del CISO: claves y futuro**
Ponente: **Daniel Barriuso**, CISO Global. Grupo SANTANDER

Ponencia: **"Don't Panic: We have MIGSE"**
Ponentes: **Borja Parada**, Responsable Global de Gestión de Crisis. Grupo SANTANDER
Antonio Requejo, Director de Consultoría en Ciberseguridad para el sector Financiero. EY

Ponencia: **Cloud Security: una visión integral**
Ponentes: **Miguel Ángel Galán**, Responsable Global de Ciberseguridad. Grupo SANTANDER
José Luis Domínguez, VP Customer Business Development. ELEVENPATHS, Unidad de Ciberseguridad de TELEFÓNICA

Ponencia: **"Adversary & Attack Intelligence": así haremos Red Team en 2030**
Ponentes: **Carlos Capmany**, Head of Global Red Team. BBVA
Alberto Cuesta, Head of Global Red Team Missions. BBVA
Aurora García, Coordinadora de Inteligencia Global del Global Red Team en BBVA. MNEMO

Ponencia: **De la concienciación al riesgo humano en ciberseguridad**
Ponentes: **Roberto Ortiz**, Global Head of People Information Security. BBVA
Andrés Núñez, Director de Desarrollo de Negocio. S2 Grupo

SECURMÁTICA 2020

NUEVAS FECHAS

29 Y 30 DE SEPTIEMBRE, Y 1 DE OCTUBRE DE 2020

SEGUNDO MÓDULO, 30 DE SEPTIEMBRE

Ponencia: **La (in)seguridad en los procesos electorales de EE.UU. ¿Hasta qué punto la realidad supera la ficción?**
Ponentes: **Jordi Puiggalí**, Gerente de Seguridad y Director del Departamento de Investigación. SCYTL (SCO)
Gerard Cervelló, Director de Operaciones. BLUELIV

Ponencia: **GLOBALVIA: de Madrid a Pocahontas: retos de la ciberseguridad en una organización multinacional**
Ponentes: **Fernando Vallejo**, Director de IT, Innovación y Transformación. GLOBALVIA
Carlos Cortés, Gerente del área de Servicios Gestionados y Ciberseguridad. INGENIA

Ponencia: **NATURGY: Protección de Amenazas Avanzadas (PPA)**
Ponentes: **Carlos Manchado**, CISO. NATURGY
Alejandro Belón, Cybersecurity Sales Executive. DXC

Ponencia: **RENFE: el Centro de Coordinación de Ciberseguridad: presente y futuro de un CERT en un operador crítico**
Ponentes: **Francisco Lázaro**, CISO y DPO. RENFE
Jorge Hurtado, Chief Sales and Marketing Officer. S21sec

Ponencia: **FERROVIAL: la contrainteligencia digital como una nueva Estrategia de defensa**
Ponentes: **Daniel Aparicio**, Gerente de Arquitectura y Operaciones de Ciberseguridad. FERROVIAL
César Tascón, Socio de Ciberseguridad en Business Security Solutions. PwC

Ponencia: **GRUPO SANTILLANA: transformando la seguridad**
Ponentes: **Rodrigo Nalda**, CISO. Grupo SANTILLANA
Óscar Riaño, Responsable de GMV-CERT. GMV

Cena de la Ciberseguridad y entrega de los XVII Premios SIC

TERCER MÓDULO, 1 DE OCTUBRE

Ponencia: **RIA FINANCIAL: evolución del sistema NAC para mayor visión, control y cumplimiento de dispositivos conectados**
Ponentes: **Adrián García**, Infrastructure Manager de EMEA. RIA FINANCIAL
Alejandro Alcaide, CISO para el área EMEA. RIA FINANCIAL
Israel Zapata, Director de Operaciones de Ciberseguridad. SECURA by FACTUM

Ponencia: **CEPSA: SOC Cloud hacia el SOC 3.0**
Ponentes: **Rafael Hernández**, CISO. Grupo CEPSA
Juan Miguel Velasco, CEO. AIUKEN Cybersecurity

Ponencia: **Thin Cybersecurity: eficacia y eficiencia en SINGULAR BANK**
Ponentes: **Damián Ruiz**, CISO. SINGULAR BANK
Enrique Domínguez, Director Estratégico. ENTELGY INNOTEC Security

Ponencia: **BANKIA: transformando el sistema de gestión para la protección de la información estructurada y no estructurada**
Ponentes: **Pedro Joaquín Feu**, Director de Prevención y Recuperación de Ciberseguridad. BANKIA
Jaume Soler, Responsable de las prácticas Data Security & Data Privacy. ACCENTURE Security para la región de Iberia

Sesión de clausura:
Luis Saiz, Responsable de Innovación en Seguridad. BBVA.
Ponente por determinar

Fin del tercer módulo y de la XXXI edición de Securmática

esprinet® V-Valley the Value of esprinet vinzeo®

Para nosotros, la ciberseguridad es un factor importante que debe estar en el ADN de todas las organizaciones. Nuestro equipo de profesionales compacto, competente, especializado en marcas y tecnologías específicas, y al servicio del canal, es el valor único para que la seguridad sea un facilitador más del negocio.

¡La ciberseguridad es nuestra pasión!
Hablamos tu idioma:
Seguridad, Cloud y Networking Enterprise

Enterprise Security

McAfee
IPS | CASB | EPP | Mobile | ATP | Sec Content | EDR | SIEM | DLP

Microsoft
CASB | EPP | IAM | IRM

Check Point SOFTWARE TECHNOLOGIES LTD.
NGFW | IPS | DDoS | Este/Oeste | vSec | CASB | EPP | Mobile | ATP | VPN | Encryption | Sec Content

A10
DDoS | ADC | SSLi

PulseSecure
IdP | Mobile | ADC | VPN | NAC | SDP

BROADCOM connecting everything
Management IT | IAM | SSO | Intelligent Automation

CounterCraft
Honey Pot | Deception | Threat Hunting

kaspersky
EPP | Mobile | ATP | EDR | Sec Content | Encryption

SONICWALL
NGFW | IPS | vSec | ATP | EDR | Sec Content | VPN | WIFI

CLOUDFLARE
DDoS | DNS SEC | CDN | WAF

CIPHER™
HSM | Secure PKI | Digital Sign

BACKBOX
Intelligent Automation

solarwinds
Management IT

aruba a Hewlett Packard Enterprise company
VPN | UEBA | WIFI

NETWORK SECURITY | ENDPOINT SECURITY | SECURITY MANAGEMENT
CLOUD SECURITY | IDENTITY SECURITY | INFORMATION SECURITY
DIGITAL SIGN & PKI | CONTENT SECURITY | INFRASTRUCTURE SECURITY

www.v-valley.com Tel. + 34 690 756 403 seguridad@v-valley.com
BARCELONA | BILBAO | MADRID | LISBOA | SEVILLA | ZARAGOZA

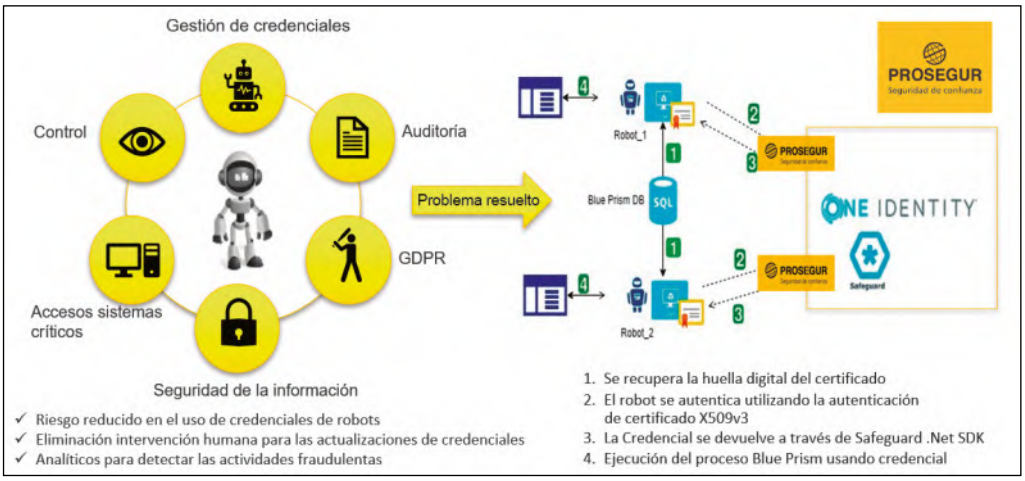
PROSEGUR y ONE IDENTITY: 'securización' de entornos RPA

Hace aproximadamente un año y medio, el departamento de RPA de Prosegur se encontraba ante la necesidad de cumplir diferentes normativas de seguridad debido al aumento significativo en los procesos de negocio que se estaban automatizando, con la consiguiente criticidad del sistema y confidencialidad de los datos que se estaban manejando en estos procesos. Después de evaluar diferentes alternativas, One Identity fue seleccionada para ayudar a cumplir estos requerimientos de protección. Prosegur utiliza RPA para transformar su negocio mientras reduce el riesgo de los accesos privilegiados utilizando One Identity Safeguard.

Prasanna Kumar / Raúl Dopazo

Prosegur está en un proceso de transformación digital, automatizando muchas de las tareas administrativas mediante la tecnología RPA de BluePrism, permitiendo así a sus trabajadores centrarse en aquellas que aportan más valor a la empresa y logrando el objetivo de reducir costes y de facilitar y agilizar la transición.

En solo dos años, la multinacional ha multiplicado el número de trabajadores digitales en 14 áreas de negocio, como son las de recursos humanos, finanzas, aspectos jurídicos, marketing, servicios informáticos y operaciones. El programa ha permitido ahorrar 350.000 horas.



El riesgo existente en esta transformación es evidente, ya que el software de RPA interactúa directamente con las aplicaciones empresariales, reproduciendo la forma en la que las aplicaciones y las personas utilizan las credenciales y los permisos. Esto puede conllevar ciertos riesgos cuando los trabajadores digitales se embarcan en procesos que requieren acceso a credenciales privilegiadas, y estos a su vez a datos confidenciales y críticos.

Por eso, para Prosegur era fundamental poder gestionar las credenciales privilegiadas de forma segura y proteger los accesos para reducir el riesgo de infiltraciones al objeto de garantizar que BluePrism pudiese acceder de forma segura a las credenciales privilegiadas, siendo esto de vital importancia para su iniciativa de RPA.

La primera vez que la compañía implementó una solución de RPA, esta no ofrecía las funciones necesarias para automatizar el control ni garantizar que los accesos privilegiados se concedían de forma segura. La empresa realizó una prueba de concepto (POC) con una de las principales soluciones de gestión de acceso privilegiado (PAM), pero no fue capaz de integrar la solución de RPA mediante la API de la que disponía de manera satisfactoria y rápida. Por esta razón, desde Prosegur se decidió hacer otra POC, utilizando, en esta ocasión, **Safeguard de One Identity**.

Con esta decisión los problemas relativos a la API desaparecieron de un plumazo. Resultó muy sencillo trabajar con la API de One Identity, que es un producto basado en el concepto de API First, con una completa REST-API y un conjunto de SDK en diferentes lenguajes de programación. Además, como la asistencia brindada resultó magnífica, la prueba de concepto con Safeguard y la solución de RPA fueron todo un éxito.

La potencia del API de Safeguard proporciono toda la flexibilidad requerida, y de forma inherente los controles de seguridad necesarios para el control y gestión de las cuentas privilegiadas y las sesiones de los desarrolladores.

Mediante la implementación de un sistema PAM integrado en su plataforma de RPA con BluePrism, Prosegur ha conseguido de una manera sencilla:

- Reducir el riesgo del uso inapropiado de cuentas privilegiadas por parte de los desarrolladores del equipo de RPA.
- Controlar el uso de credenciales de manera segura por trabajadores digitales mediante el uso de certificados seguros y restricciones de acceso, sin exponer en ningún momento estas credenciales.
- Trazabilidad absoluta en el uso de estas credenciales.
- Análisis del comportamiento de los desarrolladores durante las sesiones para la resolución de incidencias, suplantando su identidad por la de los trabajadores digitales sin conocer estas contraseñas.
- Cumplimiento normativo, lo que le ayuda a verificar que cumple el reglamento general de protección de datos (RGPD) de la Unión Europea.

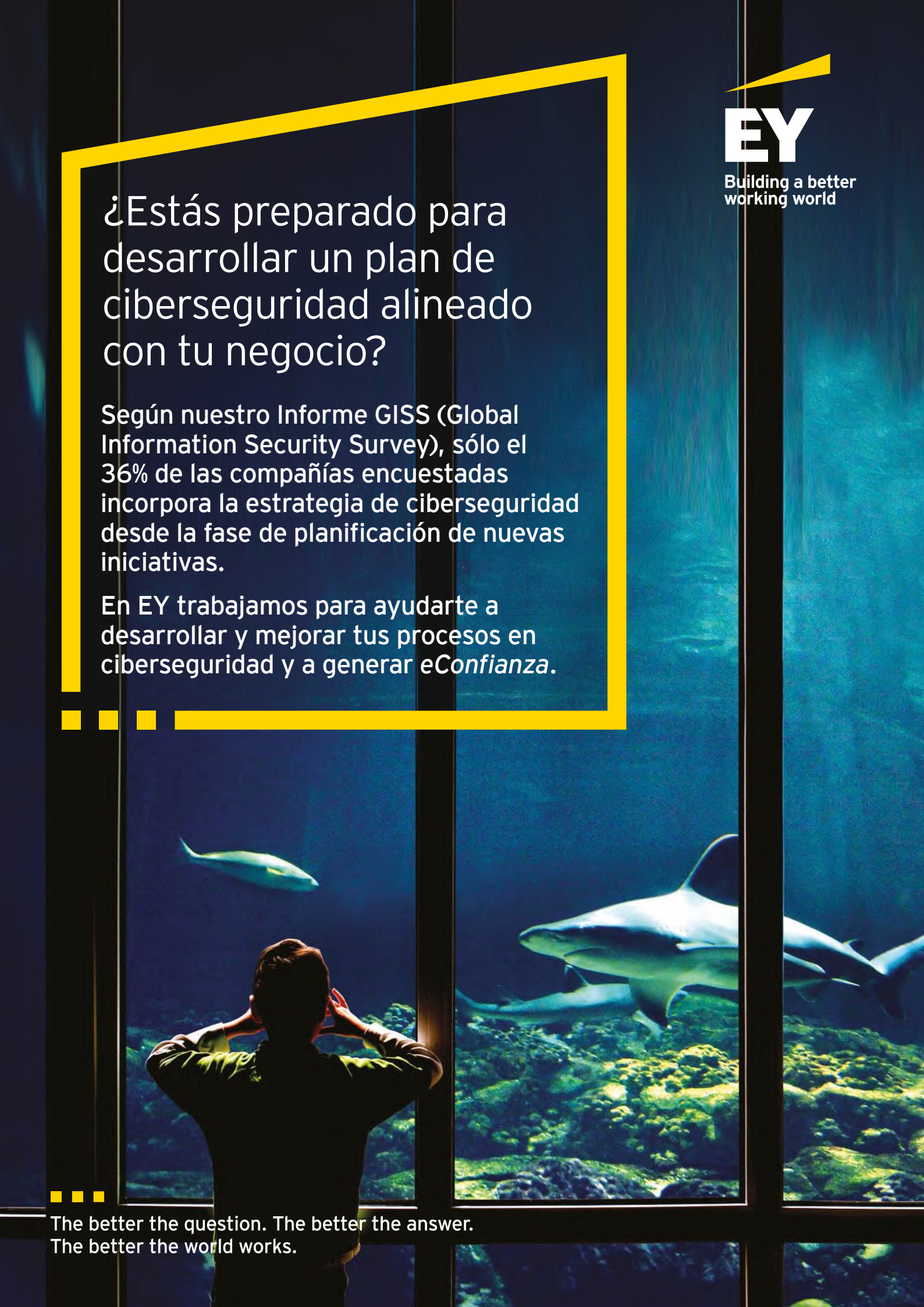
Con estas acciones en Prosegur somos capaces de ver lo que pasa en nuestro entorno en todo momento. Ahora, gracias a Safeguard de One Identity, ya no tenemos que preocuparnos por los accesos privilegiados y nos será más fácil acelerar nuestro programa de RPA.

Con los objetivos cumplidos, la colaboración entre ambas compañías no se ha quedado simplemente en una mera transacción comercial. Actualmente Prosegur y One Identity colaboran en distintas iniciativas empresariales de manera conjunta, en un claro ejemplo de *Win-Win*.

A su vez, Prosegur está incrementando su oferta de servicios para ayudar a otras compañías en esta transformación digital mediante el uso de tecnologías RPA y Safeguard desde el concepto de Security by Design. ■

Prasanna Kumar
Arquitecto TI
PROSEGUR

Raúl Dopazo
Sales Engineer
ONE IDENTITY



EY
Building a better working world

¿Estás preparado para desarrollar un plan de ciberseguridad alineado con tu negocio?

Según nuestro Informe GISS (Global Information Security Survey), sólo el 36% de las compañías encuestadas incorpora la estrategia de ciberseguridad desde la fase de planificación de nuevas iniciativas.

En EY trabajamos para ayudarte a desarrollar y mejorar tus procesos en ciberseguridad y a generar *eConfianza*.

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

“El buen hacer, el afán de conocimiento y el esfuerzo nos dan credibilidad para vencer reticencias y competir internacionalmente con cualquiera”

Jess Garcia

CEO de One eSecurity

>Por **Luis Fernández Delgado**
>Fotografía: **One eSecurity**

Tras algunos años previos de ‘calentamiento’ sectorial y con una creciente y consolidada trayectoria, One eSecurity es hoy, tras una década a sus espaldas, una de las compañías españolas de mayor proyección internacional en ciberseguridad. Y no solo por haberlo logrado en un sector incomprendido e infravalorado, sino además por sobresalir en especialidades nada triviales como son las de ‘forensía’ digital y respuesta a incidentes (DFIR), en las cuales sus servicios y desarrollos tecnológicos son referencia. En la siguiente entrevista su CEO y fundador, Jess Garcia, explica las razones de su reconocido ‘savoir faire’.

"Hoy en día cualquier empresa utiliza de forma proactiva esta disciplina en procesos como Threat Hunting o Ciberinteligencia; me gusta mucho este mestizaje porque nos fuerza a innovar y a abordar problemas tradicionales desde prismas innovadores".

– ¿Cuál es el origen y momento de nacimiento de One eSecurity?

– One eSecurity nació en 2007, hace ya camino de 14 años, como consecuencia natural del deseo de hacer cosas nuevas y emocionantes en el ámbito de la ciberseguridad. Yo venía de gestionar las redes, sistemas y seguridad del LAEFF (Laboratorio de Astrofísica y Física Fundamental) del INTA (Instituto de Técnica Aeroespacial), un Laboratorio donde la seguridad era un componente tremendamente crítico, dado que estábamos dentro de las redes de la Agencia Espacial Europea (ESA) y operábamos radiotelescopios de la NASA. Allí, además de compartir unos años maravillosos con mentes brillantísimas, pude aprender y desarrollar mis conocimientos de ciberseguridad desplegando y operando una red de altísima seguridad. Pasados 10 años sentí que era hora de abrirse a otras experiencias y proyectos y me establecí como consultor independiente. Tuve el honor de aprender a ser "consultor/proveedor" de la mano de mi gran amigo Víctor Chapela, otra mente brillantísima, con quien pude trabajar en fascinantes proyectos e investigaciones en Estados Unidos y México. Pasada esa etapa decidí que era hora de emprender mi propia andadura y así nació One eSecurity, un proyecto que surgió en un "chiringuito con wifi" en Marbella, con mi gran amigo e impresionante profesional Carlos Fragoso.

– Dentro del amplio espectro de actividades que cobija la ciberseguridad tecnológica, ¿dónde encuadra a su compañía y cómo la definiría?

– Nuestro foco ha sido muy específico desde nuestros orígenes: Detección y Respuesta. Nuestros clientes acuden prioritariamente a nosotros cuando buscan un servicio personalizado y de alto *expertise* técnico. Me enorgullece decir que con los años hemos conseguido convertirnos en una empresa con una sólida reputación, forjada a base de infinitas horas de trabajo (y muchas noches sin dormir) al lado de nuestros clientes. "Together as ONE" como reza nuestro eslogan.

Lo que nos definen son unos pocos principios básicos: pasión por lo que hacemos, alta especialización técnica, alto grado de exigencia con nosotros mismos, aproximaciones realistas, innovadoras y pragmáticas, y sobre todo -como decía- el trabajar con nuestros clientes codo a codo, como si fuéramos compañeros dentro de una misma empresa.

– A día de hoy, ¿cuánto personal la conforman y cuál es su implantación internacional?

– En este momento nuestro equipo consta de más de 50 personas, lo que para una empresa especializada en DFIR (*Digital Forensics & Incident Response*) es un tamaño bastante considerable.

Desde nuestros orígenes nuestra proyección ha sido internacional, con clientes globales que nos han llevado a hacer investigaciones y proyectos por medio mundo. Desde nuestros dos centros neurálgicos en España y México servimos a nuestros clientes de EMEA y América, y proporcionamos servicios 24x7. Además, tenemos oficinas comerciales en otros países, como Reino Unido o Alemania. Con el objeto de reducir nuestros tiempos de respuesta estamos en proceso de abrir nuevos centros técnicos en Oriente Medio, Sudamérica y Estados Unidos. Pero lo cierto es que hoy la mayor parte de nuestros servicios se pueden prestar en remoto, lo cual ha significado una gran ventaja para nuestros clientes, que no han visto interrumpidos sus negocios por la presente crisis del COVID-19.

– ¿Podría precisar qué es y qué no es la 'forensía' digital?

– Tradicionalmente la 'forensía' digital se define como la disciplina que aborda el análisis de dispositivos e información tecnológica a través de herramientas y procedimientos específicos siguiendo un conjunto de buenas prácticas que preserven la integridad de la evidencia para responder a una serie de preguntas como "qué pasó", "quién lo hizo", "cuándo pasó", "dónde pasó", "cómo pasó" y potencialmente "por qué". No obstante, poco a poco esta disciplina ha ido tomando una presencia cada vez mayor en el ámbito de la ciberseguridad y hoy en día cualquier empresa la utiliza de forma proactiva en procesos como *Threat Hunting* o Ciberinteligencia. Personalmente me gusta mucho este mestizaje porque nos fuerza a innovar y abordar problemas tradicionales desde prismas innovadores.

– ¿Qué rol y límites le augura a la 'forensía' en el emergente mercado de las pólizas frente a riesgos de ciberseguridad y si las compañías que las suscriben o intermedian están adecuadamente desempeñando su papel?

– El rol de la 'forensía' en los CiberSeguros es crítico porque ésta es quien determina en última instancia la causa del incidente. Desde nuestra experiencia, y trabajando con aseguradoras que dirigen sus soluciones al mercado *corporate* (grandes empresas), es un mercado más desarrollado en EEUU y en fase de maduración en Europa. En el sur europeo –usualmente denominado EMEA– podríamos decir que estamos mayormente en la fase de "adolescencia" construyendo y mejorando la oferta a medida que los clientes finales van demandando estas pólizas.

Nuestra experiencia como proveedor en este sector es que para clientes que no tengan proveedor de DFIR de confianza o unos procesos de Respuesta ante Incidentes adecuado, las aseguradoras pueden facilitar la vida proporcionando lo que el asegurado necesita cuando lo necesita. Nuestra relación con clientes y sus aseguradoras está creando sinergias muy positivas para los afectados, especialmente cuando podemos trabajar con ellos de manera proactiva.

– En su apuesta por el talento y la ac-

tividad industrial en nuestro país cuentan con una delegación en Málaga para asuntos de I+D. ¿Cuál es su foco?

– Como mencionaba anteriormente, no se puede entender a One sin innovación tecnológica. Desde muy temprano apostamos por desarrollar nuestra propia tecnología, y ello nos ha permitido abordar investigaciones o procesos de *Threat Hunting* en miles de máquinas y diversos países, interaccionando con tecnologías y productos diversos de una forma tremendamente potente a la vez que simple. Nuestros sistemas de Forense/*Threat Hunting* Automatizado (FOREST) y de Laboratorio Forense Automatizado (SKY) son una piedra angular de nuestros servicios de Forense Gestionado/en la Nube, de Threat Hunting o de EIR, y nos diferencian de otros proveedores por la enorme potencia de fuego que nos proporcionan. Aunque nuestro equipo de desarrollo se encuentra bastante deslocalizado (como el resto de nuestra empresa), nuestro centro principal de desarrollo se encuentra efectivamente en Málaga, una ubicación privilegiada que proporciona un entorno inspirador y tranquilo para desarrollar nuestra tecnología alejados (hasta cierto punto) de la frenética realidad de nuestros servicios DFIR. Es un honor estar tan cerca de otros centros de enorme talento, como VirusTotal/Google.

– Como compañía de origen español, ¿está usted satisfecho o echa en falta mayores acciones y compromiso de los actores públicos concernidos de nuestro país para apoyar y dar mayor visibilidad a nuestra industria en el exterior, más allá de las consabidas y casi siempre fútiles exhibiciones en ferias internacionales?

– La verdad es que en One hemos tenido muy poco contacto con este tipo de actores públicos a lo largo de nuestra historia. Sólo recientemente hemos entrado en contacto con ciertos organismos (Icex, Incibe ...) y aunque su disposición ha sido fantástica, la verdad es que en lo que a nuestro tipo de servicios atañe el llegar a que un cliente internacional se interese en ellos y decida contratarlos, tiene un recorrido muy distinto. Por tanto, voy a responder a esta pregunta desde otro ángulo, explicando cuál ha sido la clave para nosotros de una razonablemente exitosa estrategia internacional. Hay algunos factores tremendamente importantes a la hora de crear una oportunidad de negocio fuera de España (especialmente en el mundo de habla no hispana), que es convencer al cliente de que eres capaz de prestar tus servicios con la misma calidad que otros competidores de Estados Unidos o Reino Unido. Nosotros nos hemos encontrado a lo largo de toda nuestra andadura con una enorme reticencia a contratar nuestros servicios por ser una empresa española de DFIR. España se asocia a nivel internacional con ciertos segmentos comerciales, pero la ciberseguridad no es uno de ellos, y DFIR menos. Por eso hemos tenido que vencer dichas reticencias demostrando que podemos hacer el trabajo igual de bien (o mejor) que otros, y que además estamos dotados de ciertas características muy españolas (capacidad de improvisación, capacidad de hacer largas jornadas, capacidad de empatizar, etc.) que nos benefician mucho en el ámbito específico de DFIR, donde se viven situaciones de tensión extrema.

Por otro lado, One eSecurity se creó con proyección internacional desde su origen, inicialmente construyendo sobre mi trayectoria como instructor de SANS, pero además apostando por dotarse de unas estructuras flexibles para poder operar desde cualquier sitio, por tener un equipo mayormente bilingüe y diversificado internacionalmente, adoptando el inglés como nuestra lengua vehicular tanto externa como interna, etc. Todos estos factores, junto por supuesto con el buen hacer, el afán de conocimiento y el esfuerzo, crean un paraguas de credibilidad que permite vencer dichas reticencias. Con todos estos factores en una ya larga trayectoria hemos conseguido labrarnos una reputación internacional y una cartera de clientes globales que permiten que dichas reticencias pasen ya a ser menores en muchos casos.

"Desde muy temprano apostamos por desarrollar nuestra propia tecnología, permitiéndonos abordar investigaciones o procesos de Threat Hunting en miles de máquinas y diversos países, interaccionando con tecnologías y productos diversos de una forma tremendamente potente a la vez que simple".

– SANS Institute, uno de los entes internacionales de formación en ciberseguridad más consolidados viene contando con usted en Europa como uno de sus expertos pioneros. Su empresa cuenta también con otros reputados especialistas... ¿Cómo viene funcionando en España en su ideario de erigirse en el ente por excelencia en la formación en ciberseguridad y que rasgo singular le diferencia de otras opciones, digamos, clásicas, y de esos otros 'competidores', subidos más recientemente al carro', con nulo 'pedigrí'?

– Para mí SANS ha sido el motor que me ha permitido desarrollarme profesionalmente de forma exitosa y satisfactoria, y creo firmemente que la formación de calidad es la clave del éxito, tanto para individuos como empresas. Yo tomé mi primer curso de SANS en Estados Unidos en 1998 y aquella experiencia cambió mi vida. En 2002 fui nombrado instructor y hace sólo unos días me promocionaron al reducido grupo de Senior Instructors, un verdadero honor teniendo en cuenta el enorme talento que hay en SANS.

SANS me ha permitido dar clase a profesionales en decenas de países de los cinco continentes, y en instituciones tan prestigiosas como el FBI, lo que sin duda ha marcado mi vida. Creo que deben existir diversas opciones de formación para aquellos que no se puedan permitir los precios que sin duda no son asequibles a cualquier bolsillo. Pero sin duda mi recomendación para todo el que quiera desarrollar su carrera profesional en ciberseguridad es que invierta en formación de calidad, no se arrepentirá.

El culmen de este proceso fue la posibilidad de traer por fin los cursos de SANS a España en español hace unos años, estableciéndonos como *partner* exclusivo de SANS en nuestro país (un privilegio que muy pocas empresas tienen a nivel mundial). Esto fue un sueño cumplido, ya que era uno de mis objetivos primordiales desde que allá por 2002 cargué sobre mis hombros establecer a SANS en EMEA. Hoy ambos objetivos se han cumplido, lo cual me hace enormemente feliz.

– Siguiendo con la formación, las nuevas dimensiones de la operativa de cibersegu-

Seguridad Evolutiva

Defensa adaptativa y conectada

España | México | Colombia

www.mnemo.com info@mnemo.com

MNEMO

ridad auguran la necesidad imperiosa de atender especialidades nuevas, ciberecosistemas inéditos, algunos de ellos aún por delimitar. ¿Cómo plantea SANS atender esta crítica necesidad de formar en capacidades y habilidades inéditas y por definir?

– Acompañar a SANS durante 18 años en ese viaje a la excelencia formativa me ha hecho ver cómo el equipo profesional de instructores, autores y negocio de SANS constituyen una maquinaria de relojería perfecta, que favorece la flexibilidad y la innovación en formación. SANS produce todos los años varios cursos con contenido novedoso, y recicla por completo el contenido de todos sus cursos cada 2 o 3 años, lo que asegura la rabiosa actualidad de los contenidos. El secreto está en que los que desarrollan dichos contenidos son profesionales que están en las trincheras, lo que garantiza su calidad y la relevancia de los contenidos.

"Nuestros sistemas de Forense/Threat Hunting Automatizado (FOREST) y de Laboratorio Forense Automatizado (SKY) son una piedra angular de nuestros servicios de Forense Gestionado/en la Nube, de Threat Hunting o de EIR, y nos diferencian de otros proveedores por la enorme potencia de fuego que nos proporcionan".

– En el reciente monográfico que esta revista dedicó a cómo evolucionarán las ciberamenazas en el presente año usted declaraba a este 2020 como de consolidación y evolución de las estrategias vistas el año anterior: ataques multifase, aumento de la agresividad de los grupos 'esponsorizados' por gobiernos tanto en el ámbito del cibercrimen como del ciberespionaje, abogando por estar preparados para incidentes sofisticados con un plan y un potente equipo de respuesta a incidentes...

– Aunque aún es pronto, y la pandemia que estamos viviendo con la revolución del teletrabajo asociada todo lo puede cambiar, se puede decir que en lo que va de año se confirman dichas predicciones. Un ejemplo está siendo cómo ciertos estados están robando propiedad intelectual a empresas farmacéuticas que están desarrollando medicamentos relacionados con el COVID. Y otro cómo los ataques de secuestro (*ransom*) efectivamente están derivando en venta de datos. Sin duda es hora de prepararse, y puedo decir que en general estamos viendo que los devastadores ataques de *ransom* están siendo una palanca favorecedora de la ejecución de proyectos proactivos y suscripción de *retainers* en el ámbito DFIR.

En lo que se refiere a cómo esta pandemia ha cambiado esas predicciones, creo que los ataques al nuevo paradigma de teletrabajo, expresado de forma muy visible por el caso de Zoom, han sido una interesante adaptación de los actores de cibercrimen al medio de una forma prodigiosamente ágil. De forma adicional, creo que ha sido especialmente infame observar los ataques sufridos por hospitales durante la situación extrema de crisis sanitaria, poniendo de manifiesto la falta de escrúpulos de ciertos actores.

Esta crisis seguramente va a ser la palanca para afianzar una transformación hacia un trabajo distribuido apoyado en servicios *Cloud,* que nos arrastrará a adaptar nuestros procesos de ciberseguridad asociados. En el ámbito DFIR que nos incumbe, por ejemplo, muchos clientes nos están pidiendo ayuda para adaptar sus procesos de Respuesta a Incidentes de forma nativa en la Nube, o a equipos comprometidos de teletrabajadores, en el contexto de ataques ya existentes como los de *ransomware*, o de nuevas variaciones más creativas.

– Sin desvelar al pecador, ¿puede decirnos el pecado más curioso y/o inquietante que haya constatado últimamente en su interminable periplo internacional de 'ciberbombero'?

– Por mencionar un par de ellos, un caso que recuerdo que me impactó es el de un cliente que, tras comunicarle (después de sólo una semana de investigación) que un actor había comprometido totalmente toda su infraestructura durante meses en más de 10 países, que había tenido acceso a todas sus credenciales y datos (propios y de clientes), que había incluso cambiado la configuración de sus *firewalls* para operar de una forma más cómoda..., la respuesta por parte del Comité de Dirección fue "que no lo consideraban un incidente relevante", no le dieron importancia y ni siquiera lo investigaron más allá. Impresionante.

Por otro lado, con respecto a la realidad del espíritu humano, tuvimos un incidente de *ransomware* en el que al preguntarle al empleado sobre cómo había sucedido la infección nos explicó que había abierto un adjunto malicioso, a pesar de que sabía perfectamente que era malicioso, y que el antivirus le avisara en tres ocasiones seguidas de que el *ransomware* iba a cifrar todos sus archivos. Al preguntarle por qué lo hizo, respondió con una absoluta sinceridad, normalidad y estupefacción: "no lo sé".

En el ámbito de lo inquietante diría que una de las cosas que me preocupa es ver cómo las operaciones Estado-contra-Estado (o contra las empresas de dichos Estados) se están volviendo algo totalmente cotidiano, y de una forma incrementalmente más agresiva. Hace unos años hacer una investigación en la que estuvieran involucrados actores relacionados con servicios de inteligencia era algo relativamente poco habitual, hoy es el pan nuestro de cada día.

– Es sabida la intensa colaboración que mantiene One eSecurity con los Cuerpos y Fuerzas de Seguridad del Estado español y equiparables en otros países, en las materias que nos ocupan. ¿Cómo valora la cualificación de estos colectivos, su disposición de medios, apoyo institucional, retos internacionales?

– En One tenemos el enorme privilegio de colaborar con diversas fuerzas del orden, tanto en España como fuera, y yo personalmente he formado a centenares de profesionales de este ámbito de todo el mundo. Bajo esta privilegiada perspectiva puedo decir que hay un enorme talento y pasión en nuestro país, equiparable o superior al existente en cualquier otro. Las fuerzas del orden españolas tienen una excelente reputación internacional, y están presentes en foros de primera línea. Tenemos diversos miembros de nuestras fuerzas del orden en destacados puestos en organizaciones internacionales, como Europol o Interpol. No obstante, sí es cierto que existen importantes diferencias de inversión frente a otros países de nuestro entorno. No entraré a valorar las causas, que supongo que son muchas y complejas, pero sí creo que es algo que debería corregirse habida cuenta que todo investigación civil o criminal hoy en día tiene un componente tecnológico. ■

ágoraSIC Centro de Conocimiento en Ciberseguridad

TELETRABAJO

¡Tengan cuidado ahí dentro!

La declaración de pandemia por la Covid-19 y las medidas de confinamiento adoptadas por los estados han propiciado la puesta en marcha del mayor despliegue de entornos activos de teletrabajo que la Humanidad recuerde para salvaguardar la continuidad de actividades y negocios, y una valiosa experiencia para que empleados, empleadores y legisladores pacten con conocimiento unas reglas del juego para esta relación laboral acordes con la transformación digital.

En estas páginas especiales, se brinda una visión multidimensional del acceso remoto seguro aplicado al trabajo por cuenta ajena desde el domicilio particular con medios TIC.

SUMARIO

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

PROTECCIÓN DE DATOS, SISTEMAS Y TRATAMIENTOS

Teletrabajo seguro, el catalizador digital de la transformación socioeconómica

Tras la declaración de la pandemia por la Covid-19, en nuestro país se pasó de una fuerza laboral que trabajaba en remoto de poco más del 5% a elevarse a un 30%, con grandes multinacionales tecnológicas y entidades financieras con sus plantillas desplazadas. El teletrabajo ha avanzado en tres meses más que en dos décadas. Una consecuencia ha sido el incremento de los ciberataques en más de un 300%, mientras que los CISOs y responsables de ciberprotección han tenido que implementar, a contrarreloj, un entorno seguro con VPNs, redes de confianza cero y gestión de identidades, aprovechando la nube. Revista SIC plantea en este especial qué supone el teletrabajo, qué riesgos y ventajas tienen las tecnologías y servicios para el acceso remoto seguro, ofreciendo recomendaciones de los que saben realmente de ello para una fuerza laboral en remoto que, hasta 2021, se presume como la tendencia habitual.

Ana Adeva y José Manuel Vera (equipo SIC)

Parece que el teletrabajo es una fórmula laboral nueva, pero el concepto fue acuñado por el físico estadounidense, **Jack Nilles**, en 1973, cuando buscaba una solución para ahorrar carburante en los desplazamientos laborales, en plena crisis del petróleo. De hecho, él lo aplicó trabajando de forma remota en un sistema de comunicación de la NASA.

Con la pandemia de la Covid-19, más de 500 millones de personas se han visto obligadas a trabajar desde casa popularizándose el concepto de 'oficina digital colaborativa' gracias a plataformas de trabajo compartido, videoconferencia y, por supuesto, acceso remoto seguro, una situación que está dando un empujón al replanteamiento de la ciberseguridad en la búsqueda de una protección 'más allá del perímetro' y dispensable de forma masiva en un medio heterogéneo.

En España, empresas como por ejemplo **Repsol, Iberdrola** o **Microsoft** –entre otras– tienen un activo plan de teletrabajo, aunque hasta la pandemia el porcentaje de personas que lo pedían era relativamente bajo. Por otro lado, algunas multinacionales tecnológicas, como **WordPress, Buffer, Invision, Gitlab** o **Zapier,** tienen desde hace años al 100% de su plantilla trabajando en remoto.

Lo que está claro es que la crisis sanitaria está marcando un antes y un después, ya que muchos expertos aseguran que esta forma de colaboración en remoto ha venido para quedarse, de forma granular, y será tendencia en lo que queda de año y 2021. Casi un 25% de las empresas han destacado, en una investigación de **Gartner,** que consideran que, pasada la crisis, el 20% de sus trabajadores pasarán a desempeñar sus tareas en remoto.

Sus defensores consideran que con él se ofrece una jornada más flexible, productiva, conciliadora con la vida personal y, además, ahorra costes en desplazamientos, oficinas e, incluso, permite compartir entre departamentos a trabajadores según sus capacidades. También, ha permitido acelerar la automatización, ya que puede aumentar la confiabilidad, mejorar la seguridad y el bienestar, y manejar picos repentinos en la demanda.

El reto de la ciberseguridad

Pero no todo es favorable. Un 49% de los 300 expertos en TI encuestados por la compañía **xMatters**, destaca que, con la popularización del teletrabajo, las personas "actualmente trabajan más horas y experimentan una disminución de la conciliación laboral". Además, la pandemia ha sacado a relucir la ciberseguridad como un problema para el que muchas organizaciones nunca tuvieron un plan para un cambio tan drástico.

El ya discutido con anterioridad concepto del perímetro, como protección, 'ha caído' obligando a los CISOs y a la industria de ciberseguridad a proteger los sistemas para el trabajo corporativo, desde el hogar, así como miles de accesos que hasta ahora eran poco significativos.

De hecho, un reciente estudio de **Check Point**, realizado a 411 profesionales de TI y seguridad de organizaciones de más de 500 empleados en todo el mundo, destaca que un 61% estaba preocupado por los riesgos de tener que hacer cambios rápidos para permitir el trabajo remoto. Y es que, la distribución de *malware* y los ataques de *ransomware*, las aplicaciones fraudulentas que se hacen pasar por herramientas populares, así como sitios web maliciosos, *spyware*, *adware* y el *phishing* -este último que se

Fuente: Federico Wengi, Paua Ventures

mantiene como la principal ciberamenaza para suplantar a entidades, como las de la Organización Mundial de la Salud, la ONU o empresas privadas y sector público- se han reinventado y han aumentado exponencialmente, aprovechando la pandemia y el confinamiento, las vulnerabilidades del teletrabajo y del eslabón más débil de la cadena: los empleados. Incluso, **Úrsula von der Leyen**, la presidenta de la **Comisión Europea**, advirtió, el 24 de marzo, que el "delito cibernético" en la UE había aumentado por el brote de la Covid-19.

A ello se le suma que solo el 7% de los empleados había recibido capacitación específica de ciberseguridad en línea cuando se implementaron las medidas de bloqueo y que solo el 19% de los que trabajan desde casa con sus equipos, como resultado de las medidas de bloqueo de la Covid-19, había verificado si su solución antivirus estaba actualizada, según un estudio de **Avast Business.** Los investigadores también descubrieron que casi una quinta parte (18%) de los que actualmente trabajan desde su hogar lo hacen desde sus propios dispositivos desprotegidos, y ni siquiera la mitad, el 45%, trabajan en dispositivos seguros proporcionados por su empresa.

Sin duda, el teletrabajo ha sacudido todos los cimientos de la ciberseguridad, llegando a las pólizas de seguros que cubren daños causados por ciberataques, que no tenían contemplado este uso intensivo del trabajo en remoto. De hecho, según la correduría **Marsh & McLennan**, las aseguradoras "están intensificando el escrutinio de los acuerdos de seguridad de los asegurados. Estos esfuerzos podrían resultar en políticas más costosas, o incluso negaciones de cobertura para las compañías". Prueba de que el riesgo tiene que volver a reconsiderase es que se calcula que seis de cada 10 trabajadores remotos están usando dispositivos personales para hacer el trabajo, y casi todos esos trabajadores creen, ingenuamente, que sus dispositivos son seguros, según un estudio de **CrowdStrike**.

Por eso, a medida que las organizaciones trabajan para actualizar sus sistemas tecnológicos e infraestructura para apoyar a la creciente fuerza de trabajo en remoto, es imperativo que la ciberseguridad no se quede atrás.

Herramientas de colaboración

De cualquier forma, las herramientas de colaboración en línea se están convirtiendo en un elemento vital para el teletrabajo. No existe una definición consensuada para describir este tipo de tecnologías mucho más allá del *groupware*, como se designó originalmente al software colaborativo en la década de los 80, estableciendo su razón de ser en "situar la computadora directamente en medio de las comunicaciones entre gerentes, técnicos y cualquier otra persona que interactúa en grupos, revolucionando su forma de trabajar". Bajo este concepto, a principios de los años 90, **Lotus Notes** se convirtió en uno de los grandes ejemplos de esta categoría de productos, permitiendo la colaboración y la comunicación grupal de forma remota en los comienzos de la Internet.

Desde entonces, el entorno de trabajo ha experimentado una gran transformación como resultado de los avances de las TIC, los dispositivos móviles y las redes de comunicación y, a día de hoy, el número de propuestas tecnológicas en este frente resulta abrumador.

El mercado actual abarca desde aquellas herramientas que intentan virtualizar la comunicación física, como las reuniones de equipo, eventos o foros, hasta plataformas que ofrecen estilos de comunicación típicos del mundo digital, como los seminarios web o *webminars*, las nativas de la nube (como Dropbox y Slack), y, en otro orden de categorización, aquellas que permiten una comunicación sincrónica, donde la comunicación ocurre en tiempo real, como las de videoconferencia, o una comunicación asíncrona, como las de correo-e.

El auge de las videoconferencias y las VPN

El paso súbito al trabajo en remoto ha aumentado de manera exponencial el uso del software de colaboración a escala mundial, especialmente, de las aplicaciones de videoconferencia. Así se desprende, por ejemplo, de un estudio elaborado por **Okta** a cerca de 8.000 clientes, entre febrero y marzo. En él sitúa a **Zoom** como la aplicación de más rápido crecimiento, con un sorprendente aumento del 110% en usuarios únicos, cuando en el mismo periodo de 2019 solo creció un 6%. Y es que su base de usuarios aumentó de 10 millones en diciembre a más de 300 millones de usuarios conectados a fecha de mayo.

Junto con Zoom, **Microsoft Teams** y **Google Meet** se han convertido en otros de los servicios más utilizados para el trabajo en remoto los últimos meses. La primera con más de 75 millones de usuarios activos diarios en mayo, aumentando un 90% desde el mes de marzo. Y Google Meet con más de 30 millones de usuarios durante el mes de abril (siendo a fecha de cierre de esta edición de SIC una aplicación de pago).

El estudio de Okta también revela un gran aumento del número de usuarios de entornos con seguridad para red, como las VPN, a medida que las organizaciones iban trasladando a gran escala su fuerza de trabajo a la nube. En este sentido, **Palo Alto Networks** GlobalProtect mostró un crecimiento del 94% entre febrero y marzo, en comparación con el 20% en el mismo período de 2019. **Cisco** AnyConnect (86%) y **Citrix** ADC (56%) también han experimentado una gran demanda, y no solo de estas soluciones de seguridad, sino también de aquellas que acompañan a dichas tecnologías y que facilitan el teletrabajo, como Cisco Webex o las soluciones de Citrix: Digital Workspace, Networking y Analytics. ■

CAVILACIONES SEGURAS

El patito feo de la seguridad

La actual pandemia está cambiando nuestra forma de trabajar. Esta sentencia se repite una y otra vez desde mediados de marzo de 2020. Ya no es nada novedosa. Las semanas de confinamiento se sucedieron una tras otra y todos tuvimos que aprender a interactuar y a trabajar en una "nueva normalidad".

Las tres archiconocidas propiedades básicas de la seguridad de la información son *confidencialidad*, integridad y *disponibilidad*. Tradicionalmente las dos primeras han constituido el objetivo más atractivo de gran parte de las soluciones de protección en el mercado. La disponibilidad, en ocasiones, no se veía siquiera como parte de la seguridad: era el "elefante rosa" en la "habitación de la ciberseguridad" que no acertábamos a ver y a tratar con claridad. El patito feo de la tríada.

El confinamiento por la pandemia ha supuesto una verdadera puesta de largo de la "disponibilidad" en nuestros sistemas y datos como valor esencial de la seguridad.

Estos nuevos tiempos han servido para darnos cuenta de que "la garantía de disponibilidad de nuestros servicios" es mucho mayor si pueden ser proporcionados de forma remota. Indefectiblemente, hoy en día, el adjetivo remoto viene asociado al adjetivo digital si hablamos de servicios prestados por las empresas. Y si hablamos de servicios digitales, la ciberseguridad es un requisito necesario para su prestación con garantías suficientes.

La disponibilidad del acceso remoto a nuestros sistemas y datos ha cobrado una importancia vital: ha sido una verdadera puesta de largo de la "disponibilidad" como valor esencial de la seguridad. En estos días, la confidencialidad y la *integridad* acompañan a la disponibilidad de los sistemas *online* sólo si la empresa, grande o pequeña, tiene capacidad para ello.

Las redes privadas y los escritorios virtuales ya eran herramientas en uso entre desarrolladores, analistas, etc. El cambio actual las hace presentes en muchas otras funciones profesionales que antes no entraban en la ecuación del teletrabajo. Los centros de atención a clientes y la asistencia médica primaria son dos ejemplos.

Los profesionales de la ciberseguridad tenemos la oportunidad de innovar en este nuevo paradigma de relación profesional en nuestra sociedad. El lugar físico desde el que trabajamos de forma segura ya no es relevante en nuestros equipos y organizaciones.

Alberto Partida
Analista en Ciberseguridad
itsecuriteer@gmail.com
@itsecuriteer en twitter
https://linkedin.com/in/albertopartida

Productividad en remoto y privacidad

El teletrabajo plantea, al mismo tiempo, retos de privacidad y confianza entre los profesionales y los responsables de las compañías, ya que algunas han optado por implementar medidas de vigilancia y monitorización sobre la actividad de los trabajadores a través de diversas herramientas (en ciertos casos, también, encaminadas a identificar patrones anormales de comportamiento en el tráfico de red para tratar de evitar la propagación de *malware* por la red corporativa, y el acceso y uso no autorizado de recursos).

Este hecho es y ha sido motivo de debate, especialmente ante la llegada de tecnologías de control cada vez más sofisticadas. En la gran mayoría de casos, su uso es legítimo, pero, como toda medida susceptible de atentar contra ciertos derechos fundamentales, la legislación apunta que cualquier medida de control sobre la actividad de los trabajadores debe superar el test de idoneidad, necesidad y proporcionalidad en sentido estricto.

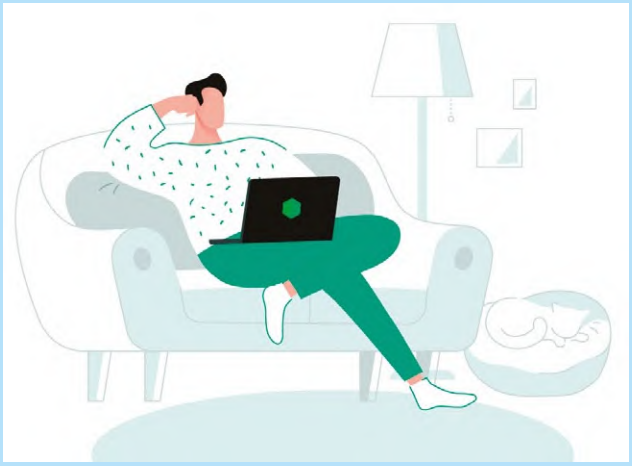
En el caso de España, los mecanismos de monitorización implementados en el contexto de acceso remoto a recursos corporativos en situaciones de movilidad y teletrabajo deben respetar también los derechos digitales establecidos en la LOPDGDD, en particular, el derecho a la intimidad y uso de dispositivos digitales y el derecho a la desconexión digital en el ámbito laboral.

La **AEPD** emitió un documento, en abril, haciendo referencia a ello con motivo del aumento del teletrabajo por el estado de alarma, titulado *'Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo'*. En él se establece que "se debe informar al personal, en la política de protección de la información para situaciones de movilidad, sobre la existencia y el alcance de actividades de control y supervisión".

Si las actividades de monitorización se usan para verificar el cumplimiento de las obligaciones laborales del personal, la Agencia indica que "el responsable del tratamiento deberá informar con carácter previo, y de forma clara, expresa y concisa a las personas empleadas y, en su caso a sus representantes, de la medida adoptada en el marco de las funciones de control previstas en el Estatuto de los Trabajadores que han de ejercerse dentro de su marco legal y con los límites inherentes al mismo". Al tiempo, recuerda que "la configuración definida para acceder a los recursos de forma remota debe ser revisada de forma periódica para garantizar que no ha sido alterada ni desactivada sin autorización, además de permanecer actualizada y adaptada a un entorno externo de riesgo que evoluciona de manera continua".

Qué se considera legalmente teletrabajo

El teletrabajo, como tal, no cuenta en España con una regulación que haga frente a las lagunas legales que genera el acuerdo entre partes, como quién pone el equipo de trabajo, cómo se controla la jornada laboral en remoto o, en caso de que el trabajador use un dispositivo propio, hasta qué punto puede instalarse software de la empresa en él para supervisar su labor diaria. En definitiva, el trabajo en remoto aún debe demostrar que es tan seguro como el presencial y respeta de igual forma la privacidad de las personas y otros derechos laborales.



Y eso que no es un tema nuevo. En Europa, la **Comisión** sentó sus bases, en julio de 2002, aprobando el Acuerdo Marco Europeo sobre Teletrabajo. En España, también hay numerosas referencias de la pasada década, y esta posibilidad está recogida en el Estatuto de los Trabajadores, en su actualización de 2015, que incluye un artículo específico sobre él: "los trabajadores a distancia tendrán los mismos derechos que los que prestan servicio en el centro de trabajo de la empresa y que el empresario deberá establecer los medios necesarios para asegurar el acceso efectivo de estos trabajadores a la formación profesional para el empleo". Además, está la Orden APU/1981/2006, de 21 de junio, por la que se promueve la implantación de programas piloto de teletrabajo en los ministerios, considerando que es "una nueva fórmula basada en las tecnologías de la información que posibilita que los empleados de una organización puedan desarrollar total o parcialmente su jornada laboral desde un lugar distinto al de su centro de trabajo".

Aprovechando su popularización en la pandemia, países como Alemania, han anunciado que están preparando una normativa específica para trabajar en remoto, según anunció el ministro de Trabajo, **Hubertus Heil**. Y en España también el Gobierno ha manifestado, a través de su homónima ministerial, **Yolanda Díaz**, su determinación a garantizar por ley el derecho al teletrabajo, afirmando que con prontitud verá la luz la la denominada Ley Reguladora del Trabajo a Distancia.

Radiografía del teletrabajo en España

El 30% de los trabajadores podría teletrabajar tras la pandemia, según un informe del **Banco de España** en el que analiza, de forma exhaustiva, cuál es su situación, destacando que el incremento potencial futuro del teletrabajo "es asimétrico y no todos los trabajadores se van a aprovechar de él, dado que aquellos con menor nivel educativo tienen dificultades para poder beneficiarse de esta forma de trabajar".

De hecho, su uso era residual en 2019, ya que el porcentaje de personas que, al menos ocasionalmente, trabajaban desde su residencia ascendía al 8,3%. Solo 2,4% más que hace una década, según la Encuesta de Población Activa (EPA). Así, España se sitúa por debajo de la media europea, con un 7,5%, un 6% menos que el promedio europeo y muy alejada de países como Francia (20,8%) o Alemania (11,6%).

Además, el Banco de España explica que el perfil de este tipo de empleados es de personas de entre 35 y 65 años y de trabajadores con formación universitaria. Por tipos de ocupación, "el trabajo a distancia es más frecuente entre los autónomos, en las empresas pequeñas y entre las ocupaciones cualificadas". En cambio, en sectores como las manufacturas, las Administraciones Públicas, el transporte y el almacenamiento, las actividades administrativas, el comercio y otros servicios, la implantación del teletrabajo es baja.

Por tipo de trabajo, las actividades cualificadas –realizadas en la actualidad por alrededor del 80% del total de ocupados que llevan a cabo parte de su trabajo a distancia– son las que también presentan mayor margen de mejora. En concreto, los trabajadores con teletrabajo en las ocupaciones de técnicos y profesionales de apoyo y en las de empleados contables, administrativos y otros empleados de oficina podrían incrementarse en más de un 40% su participación en el número total de empleados de cada una de estas ocupaciones.

Las ocupaciones incluidas en las categorías de directores y gerentes, y técnicos y profesionales científicos e intelectuales, podrían aumentar el porcentaje de trabajadores con teletrabajo en un 32% y 37%, respectivamente.

Según el Banco de España, Madrid (+28%), el País Vasco (+26%) y Cataluña (+25%) serían las comunidades autónomas en las que se podría registrar el mayor aumento en el porcentaje de empleados que trabajan desde su domicilio.

Teletrabajo flexible y seguro: principales tecnologías y enfoques

El trabajo en remoto supone un gran reto dentro de una situación para la que muchas empresas no estaban preparadas, requiriendo de capacidades, tanto de personal como de infraestructura, que no siempre están disponibles. Así, en poco más de un mes se desplegaron todo tipo de 'capas' de seguridad a través de soluciones que van desde las de protección de punto final (como EDRs), hasta el despliegue de VPNs, implementación de autenticación multifactor (MFA), sistemas de gestión de identidades y acceso combinadas con la administración de los accesos privilegiados (PAM) y agentes de seguridad de acceso a la nube (CASB). Los más maduros, incluso apostaron por enfoques como SASE o los de confianza cero, como ZTNA.

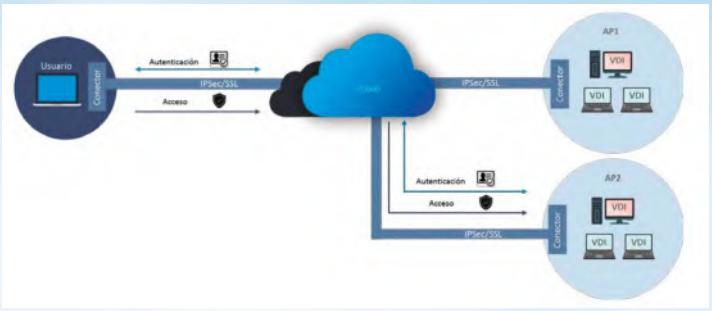
La actual situación de teletrabajo masivo, a nivel mundial, ha desafiado a las empresas a fortalecer, ampliar y encontrar nuevas formas de proteger datos, usuarios y organizaciones, sin importar su ubicación. Pero no resulta sencillo, ya que todo depende de muchos factores, como por ejemplo quién es el usuario y cuál es su función laboral (los usuarios críticos como la alta dirección, por su acceso a información privilegiada, necesitarán de análisis de datos superiores a la media); qué tipo de dispositivo se utiliza y si es propiedad de la empresa o del empleado o a qué tipo de aplicaciones y datos necesitan acceder cuando están en una nube.

VPN como rápido aliado del teletrabajo

Sin duda, las VPN con mecanismos de confidencialidad e integridad se han convertido en la medida más utilizada para el teletrabajo durante la crisis. Se trata de una tecnología que ha mejorado notablemente en los últimos años y que ofrece un abanico de posibilidades. De hecho, al principio del confinamiento, su demanda creció en 75 países, llegando a duplicarse en 21 de ellos, con Francia, Estados Unidos y Reino Unido a la cabeza, según la firma de investigación **Top10VPN**. En España, aumentó un 75% en las primeras semanas del estado de alarma, según el estudio.

Sin embargo, la necesidad de dotar de VPN a gran cantidad de empleados para permitir una conexión más 'segura' a los recursos corporativos ha sacado a la luz desafíos que habían caído en el olvido, como su limitación física o el reto de cómo admitir a tantos usuarios. De cualquier forma, muchos expertos consideran que las VPN se quedan cortas a la hora de satisfacer la demanda de una fuerza laboral moderna, que suele acceder en remoto a las redes corporativas y desde todo tipo de dispositivos y aplicaciones.

El aumento exponencial del uso de las VPN también ha suscitado el interés de los ciberdelincuentes provocando que su uso, sin medidas adicionales de protección, incremente los riesgos cibernéticos para las compañías. Y es que, en los



últimos años, las VPN han servido como puerta de entrada a las redes corporativas para ataques persistentes avanzados (APT) contra infraestructuras críticas y activos estratégicos. Google, por ejemplo, tuvo que eliminar una de las aplicaciones VPN más populares en su 'Play Store' debido a una vulnerabilidad que facilitaba los ataques de hombre interpuesto ('*man in the middle*') contra los usuarios que la empleaban, pudiendo exponer datos corporativos. Por eso, organismos como la **Agencia de Ciberseguridad e Infraestructura** (CISA) de EE.UU., emitió varias alertas instando a las empresas a tomar medidas para reforzar sus VPN corporativas. En España, el **Incibe-CERT** también publicó, en abril, una guía sobre las VPN con recomendaciones de seguridad para el teletrabajo. Y con antelación lo hizo, efectos de acceso remoto seguro y vigilancia el **CCN-CERT**.

Muerte de las VPN

De cualquier forma, a pesar del debate sobre su futuro, en el que algunos auguran su "muerte", las redes privadas virtuales son críticas hoy para facilitar y proteger el acceso remoto. Su pervivencia dependerá, según expertos de la industria, del grado de automatización e inteligencia que incorporen, además de que la funcionalidad VPN cada vez reside menos en las manos de los usuarios y más en el *back-end* de la red. Ello conllevaría a que las VPN tradicionales fueran reemplazadas por aquellas con un perímetro definido por software (como SDNs) y con avances en el 'túnel' (que tenderán a ser híbridos) y el cifrado. De hecho, y en este último sentido, el **Ministerio Federal de Educación e Investigación** alemán puso en marcha el proyecto QuaSiModO, en septiembre de 2019, para investigar y estandarizar algoritmos de resistencia cuántica, es decir, aquellos que no pueden ser atacados por una computadora cuántica en las implementaciones de VPN. Se espera que los primeros resultados se muestren en 2022.

De momento, su crecimiento actual es tal que también se están comercializando las *VPN as a Service* (VPNaaS), con una nueva arquitectura VPN diseñada para la nube. Con ella, las organizaciones pueden proporcionar acceso seguro a los empleados a las aplicaciones y recursos de la compañía en *cloud* y viceversa

Enfoque de confianza cero

Una alternativa a la seguridad en el acceso remoto que proporcionan las VPN, sobre todo en entornos donde tener medidas y políticas de seguridad vinculadas a un perímetro de red se ha vuelto difícil, son los enfoques de 'Confianza Cero' (Zero Trust). Expertos del **NIST**, de **Gartner** y **Forrester** son algunos de los muchos que ya recomiendan su adopción como principio de seguridad por diseño.

Los avances tecnológicos están haciendo que su relevancia esté aumentando en la actualidad a pesar de que la lectura moderna de este concepto date de 2004, cuando CISOs del Reino Unido lo introdujeron después de observar cómo cambiaba el paradigma en los accesos y la autorización ante la revolución de la computación móvil y la nube.

La clave de estos enfoques es que

"funcionan bajo el supuesto de que cada solicitud de acceso, ya sea desde dentro de la red empresarial o desde fuera, es hostil" y "se centra en proteger los recursos (no segmentos de red), puesto que la ubicación de la red no se ve como el componente principal de la postura de seguridad". Así lo destaca el NIST estadounidense en un documento, publicado en febrero en fase de 'borrador', bajo el título 'What the NIST Zero Trust Architecture Means for Business Continuity' (cuya lectura es altamente recomendable).

BeyondCorp: el ejemplo de Google

Entre los ejemplos más documentados de una implementación de Zero Trust, está el modelo de **Google** 'BeyondCorp', una de las primeras en adoptar esta arquitectura de red para su seguridad corporativa hace ya una década y que ha comenzado a comercializar, en abril, como parte de su cartera 'Google Cloud' para que los empleados de las empresas puedan trabajar en remoto y acceder a aplicaciones internas, basadas en web, sin necesidad de VPNs.

Los pilares de esta solución, según publica el **Consejo Asesor de Tecnología e Industria** de EE.UU., se cimientan, especialmente, sobre tres principios: "la conexión desde una red en particular no debe determinar a qué servicios puede acceder; el acceso a los servicios se otorga en función de lo que sabemos sobre el usuario y su dispositivo; y todo el acceso a los servicios debe ser autenticado, autorizado y cifrado".

Acceso a la red de confianza cero

No obstante, una de las tendencias que está ganando más auge dentro de los enfoques de confianza cero es el ZTNA o *Zero Trust Network Access*, cuyo mercado "es incipiente, pero está creciendo rápidamente", según un reciente informe de **Gartner**. En él, se aventura a predecir que, para 2023, "el 60% de las empresas eliminarán la mayoría de sus VPN de acceso remoto a favor del ZTNA".

El objetivo se focaliza, *grosso modo*, en otorgar acceso a aplicaciones y servicios en función de la identidad del usuario y de otros atributos y contextos (como la hora, fecha, geolocalización y la postura del dispositivo), y ofrece de forma 'adaptativa' la confianza apropiada requerida en ese momento, independientemente de la ubicación. "El resultado es un entorno resistente con mayor flexibilidad y mejor monitorización", destaca Gartner.

La identidad, más allá del acceso, y la autenticación

La identidad y su gestión también ha sido determinante en los accesos que ha exigido el teletrabajo. Cuando se construye un modelo de confianza cero, uno de los principios esenciales se basa en situar la identidad en el centro de la red. De hecho, muchas empresas y fabricantes de seguridad llevan años situando la identidad como "el nuevo perímetro".

Por ello, alianzas como la **Identity Defined Security Alliance** (IDSA), formada por más de 20 compañías, entre las que se encuentran Atos, BeyondTrust, CyberArk, SailPoint, Okta y VMware, entre otras, proponen dotar de un acceso en tiempo real, basado en inteligencia, datos y aplicaciones al integrar la infraestructura de IAM con otras tecnologías de ciberseguridad empresarial.

Para la IDSA, en la creación de un modelo de confianza cero basado en una arquitectura de seguridad definida por la identidad, lo que se conoce como Identity Defined Security (IDS), hay que tener en cuenta cuatro principios: 1) la identidad se basa en una autenticación dinámica y continua o 'adaptativa' (vigilando los cambios en el comportamiento o el contexto), apoyándose en un sistema gestionado y centralizado que administra la autenticación de todos los recursos, en función del riesgo de la transacción. 2) Es imprescindible autenticación de múltiples factores (MFA) que, durante la 'explosión' del teletrabajo, tanto se ha destacado como medida de seguridad adicional para cualquier tipo de acceso remoto. 3) Se basa en un inicio de sesión único (SSO) federado, y 4) Los servidores *proxys* cobran relevancia para proteger todos los recursos mediante la ejecución de políticas centralizadas.

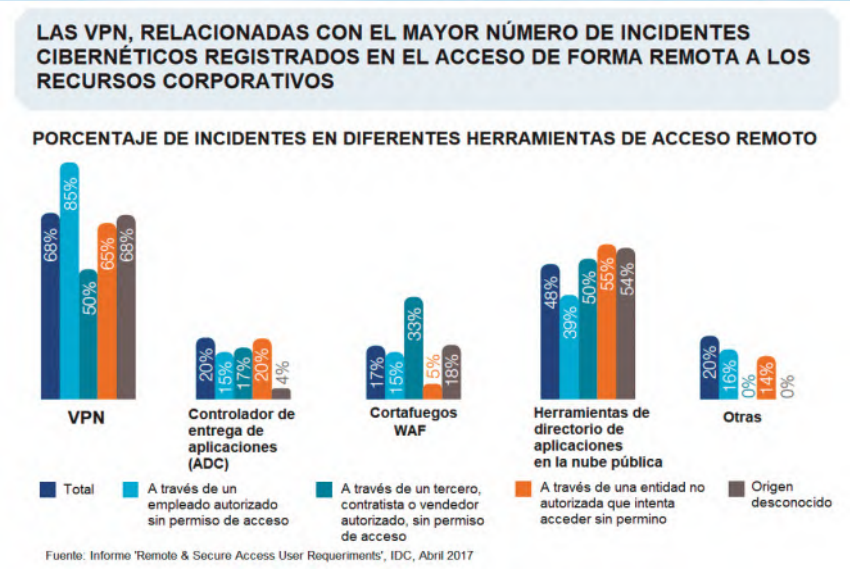
Este enfoque tendrá que ser tenido en cuenta a medida que el número de identidades digitales se dispara, cobrando más relevancia las soluciones de IAM. Entre los aspectos más destacados de una futura identificación/autenticación de los empleados estarán, sin duda, las soluciones biométricas, no solo a través de la huella dactilar, sino del reconcomiendo facial y la voz.

SASE: acceso seguro nativo de la nube

Junto a ello también está creciendo la apuesta por intentar proporcionar un acceso seguro con independencia de la ubicación de los usuarios, los datos, las aplicaciones o los dispositivos. Un problema que intenta resolver el *Secure Access Service Edge* (SASE).

Este modelo de provisión de ciberseguridad, cuyo concepto fue acuñado por Gartner en noviembre de 2019, destaca porque unifica múltiples defensas de seguridad web, en la nube, de datos y frente a amenazas, además de ofrecer funciones de red, en un potente 'edge' en la nube para respaldar a los usuarios, los datos y las aplicaciones en cualquier lugar. Por ejemplo con la combinación de tecnologías de seguridad (como CASB, SWG, ZTNA, protección de DNS y FWaaS) con tecnologías de WAN (como SD-WAN). Y, una vez más, la identidad del usuario y de los recursos (no solo una dirección IP), determinan la experiencia de la red y el nivel de los derechos de acceso.

Un ejemplo de la gran apuesta por esta solución se encuentra en el interés de grandes fabricantes de ciberseguridad que han invertido en ello, como **McAfee** y **Palo Alto Networks** al adquirir a principio de año las firmas **Light Point Security** y **Cloud-Genix**, respectivamente, para fortalecer su cartera de productos en este frente. ■



Qué nos dicen los informes

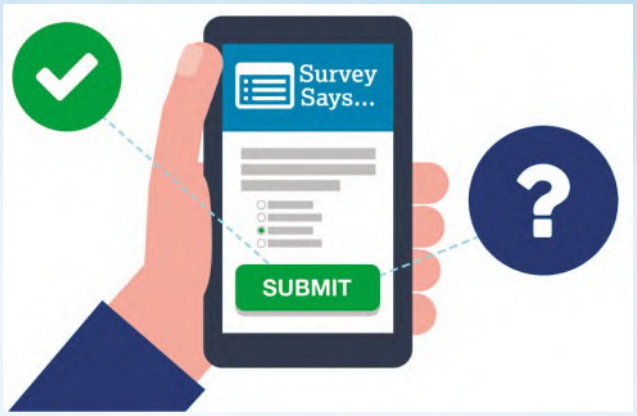
Desde la Agencia Nacional de Ciberseguridad de EE.UU. (NSA), hasta el CCN y el Incibe, en España, las principales asociaciones internacionales del sector, como Isaca e (ISC)² y, por supuesto, los fabricantes y prestadores de servicios han analizado, desde que comenzó la pandemia, las consecuencias de la generalización del teletrabajo y cómo garantizar un acceso remoto seguro. Para ello, cada entidad ha preguntado a miles de ejecutivos, asociados y clientes sobre su experiencia y qué lecciones aprendidas se pueden obtener para mejorar la ciberprotección global. Estas han sido sus conclusiones a través de los informes de referencia.

Cómo lo ven las asociaciones

La declaración del estado de alarma ha hecho que los CISOs y sus equipos tengan que ofrecer accesos remotos seguros en entornos desconocidos como son los hogares y, a veces, con equipos personales sin seguridad contrastada. ¿Cómo lo han acometido con éxito? Para conocer la respuesta, el **Consorcio internacional de Certificación de Seguridad de Sistemas de Información, (ISC)²**, que ha certificado a más de 60.000 profesionales en 135 países, realizó una encuesta titulada 'COVID-19 Cybersecurity Pulse Survey', sobre a qué dedicaron su tiempo los profesionales de ciberseguridad. En concreto, preguntaron a 256 expertos en ciberprotección durante su labor en las primeras semanas de la crisis sanitaria para "proporcionar una instantánea actual de los problemas y desafíos que sus miembros tuvieron", en esta situación.

El 81% de los encuestados destacó que su función laboral cambió durante la crisis, además de trabajar en remoto en un 90% de los casos. Una situación motivada porque, casi un tercio (32%), sufrieron la falta de compañeros por estar infectados, lo que provocó que el 96% de las empresas cerraran sus instalaciones físicas apostando por el teletrabajo, situación que ha supuesto que se detecten hasta el doble de incidentes, incrementándose, al menos, en un 23% por la transición de la oficina física al trabajo en remoto, un proceso en el que también destaca que un 81% de las compañías consideraron fundamental "la ciberseguridad", para acompañar esa evolución. Eso sí, también recordaron que, por la urgencia en dotar de equipos a su fuerza laboral en remoto, un 47% tuvieron que trabajar para el departamento de TI dejando de realizar sus funciones de ciberseguridad.

Un 34% destacó que, durante estas semanas, contaron con los medios y equipos necesarios para dar ciberprotección al trabajo en remoto, mostrando su malestar por carecer de ellos apenas un 15%. Eso sí, un 50% también confesó que "podrían estar haciendo más". De hecho, entre los temas por los que más preocupación mostraron los encuestados estuvieron también la falta de hardware, para soportar un mayor número de trabajadores remotos, la lucha entre las prioridades de la organización para el despliegue rápido de tecnología remota y el nivel proporcional de seguridad para proteger los sistemas, así como el reto de tener que ayudar a los usuarios finales a comprender y cumplir con políticas de seguridad fuera de la oficina y evitar que sean 'el eslabón más débil'.



Entre las 'lecciones aprendidas' los participantes destacaron que la pandemia fue una "una oportunidad para mejorar el proceso en el futuro". Entre los siguientes pasos que darán resaltan que, ahora, las compañías deberán "hacer lo que deberían haber hecho mucho antes: promulgar planes de contingencia para el trabajo remoto a gran escala debido a desastres naturales o provocados por el hombre" y "permitir el trabajo en remoto, que también puede ser beneficioso para los equipos de ciberseguridad, ya que, sus atractivos, pueden atraer a expertos en un mercado con déficit de profesionales", puntualiza el informe.

Por su parte, la asociación **Isaca** realizó un amplio estudio denominado 'Covid-19', para analizar "el impacto de la crisis en sus organizaciones y el trabajo en ciberseguridad". Para ello, preguntó a 3.700 profesionales de 123 países, especializados en auditoría de TI, gobernanza y seguridad. "Las empresas están evolucionando rápido hacia nuevas formas de hacer negocios, lo que es positivo, pero también puede hacerlas más vulnerables", destacó el CEO de Isaca, **David Samuelson**. "Un incremento en el número de trabajadores en remoto significa que hay una mayor superficie de ataque. El trabajo en remoto es de vital importancia en este momento, por lo que la seguridad debe estar a la vanguardia junto con la educación de los empleados", añadió.

Así, un 59% consideraba que contaba con los medios adecuados para hacer su trabajo de ciberprotección desde casa. De hecho, el 51% de los ejecutivos de tecnología reconoció estar "muy seguro" de que sus departamentos de ciberseguridad disponían de capacidades suficientes para afrontar esta situación y, en un 41% de los casos, se mostraron satisfechos con que los empleados contaran con las "herramientas y los recursos necesarios en su hogar para realizar sus trabajos con eficacia". Curiosamente, un 87% de los encuestados también destacó que esta situación había "incrementado la protección de datos y la gestión del riesgo de privacidad".

Estos resultados difieren ligeramente de la realidad en Europa. **Revista SIC** ha contado con las conclusiones específicas de la encuesta en el Viejo Continente, facilitadas por Isaca. Entre sus aspectos más llamativos resalta la buena preparación de las empresas, ya que el 60% de los preguntados sí destacó haber contado con las herramientas y recursos necesarios para realizar su trabajo desde casa de manera efectiva. Eso sí, un 83% también expuso que, nada más comenzar el confinamiento, se compartieron mejores "prácticas de riesgo cibernético". De hecho, el 86% vió positiva esta situación, que consideran que ha mejorado la "protección de datos y la privacidad". Como nota negativa también han confesado que la pandemia ha supuesto una reducción de las ventas (46%), una reducción de la productividad general (41%), así como problemas en la cadena de suministro y en el cierre de operaciones en curso (19%).

Qué ve la industria

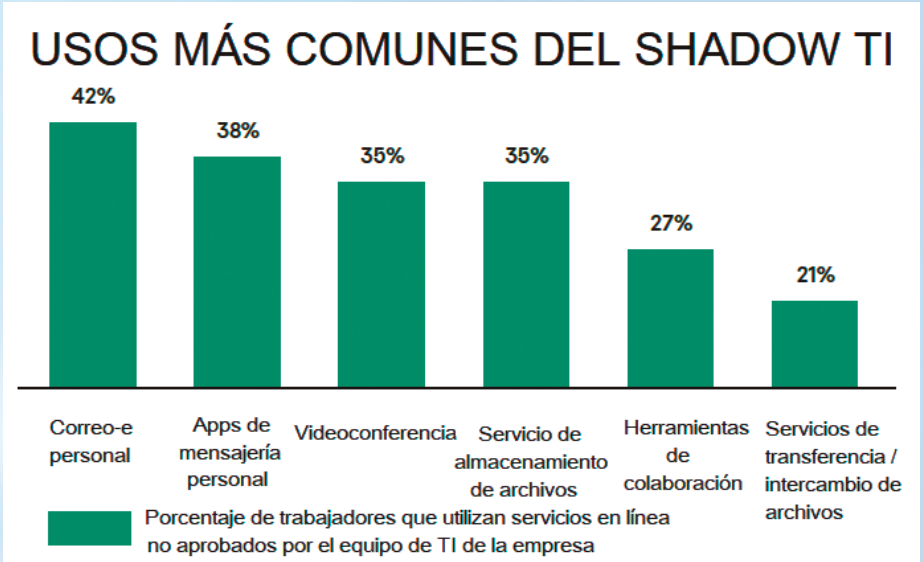
Durante los meses más intensos de la crisis, varias compañías de referencia en ciberprotección investigaron, con encuestas multitudinarias, el impacto de la pandemia en la ciberseguridad.

Quizá uno de los trabajos más interesantes sea el realizado por **Barracuda,** en colaboración con **Censuswide**, en el que preguntó a más de 1.000 ejecutivos de Reino Unido, EE.UU. Francia y Alemania sobre su experiencia en ciberprotección estos meses. Más de la mitad (51%) destacó un importante aumento de los ataques de suplantación (*phishing*) por correo-e, desde el 'minuto cero' en el que la fuerza laboral comenzó a trabajar en remoto. Además, el 51% dijo que sus trabajadores "no están capacitados adecuadamente en los riesgos cibernéticos asociados al teletrabajo". A ello, se suma que un 46% de los expertos en protección encuestados reconoció no confiar en la seguridad de sus aplicaciones web y que, por la situación, se han adoptado malas prácticas: por ejemplo, la mitad de ellos reconoció haber permitido a los empleados utilizar su dirección de correo-e personal y dispositivos propios para trabajar.

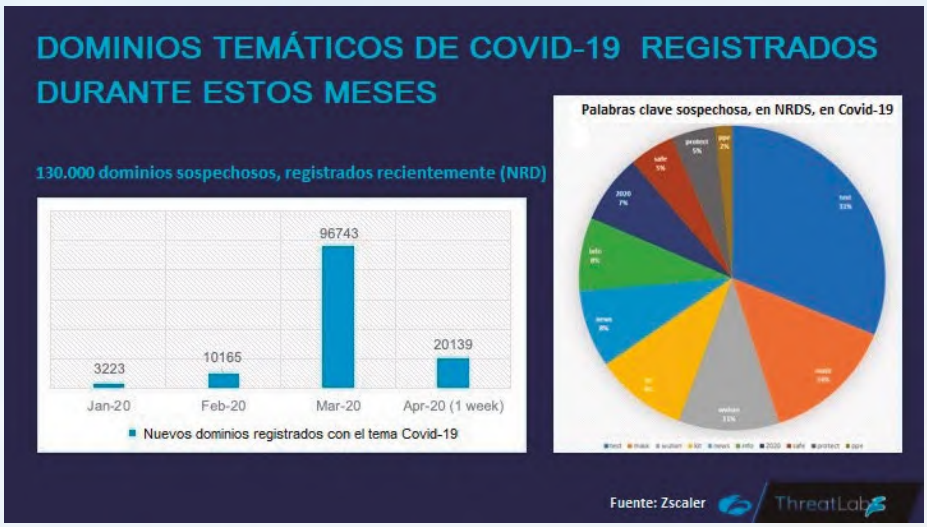
Zscaler también ofreció abundante información sobre la situación de la ciberprotección en la pandemia. Sus expertos alertaron que, desde enero, habían detectado un incremento de los ataques de suplantación con un desmesurado incremento del 30.000%, pasando de bloquear 1.200 ataques en enero a 380.000 en marzo. Además, destacó que desde el principio de la pandemia se detectaron 130.000 dominios sospechosos de reciente registro (NRD). "Los ciberdelincuentes registran nuevos dominios para aprovechar palabras, como prueba, máscara, Wuhan, kit... y debido a que los dominios son nuevos, no aparecen en ninguna lista de sitios web sospechosos".

Por su parte, **Proofpoint** alertó del incremento de campañas que utilizan como gancho el auge de las videoconferencias para el trabajo en remoto y cómo a través de ellas se roban las credenciales que son vendidas en el mercado negro. Según la compañía, estas acciones no atacan directamente al *software* de videoconferencia, sino que emplean como cebo los nombres de estas plataformas para *phishing* de credenciales, instalar *malware* u obtener datos con los que falsificar cuentas.

A pesar del incremento de ataques, el 40% reconoció que su empresa redujo los presupuestos de ciberseguridad para "ayudar en la crisis del Covid-19" y un 50% destacó que podría valorar, incluso, reducir su personal si consiguiera ofrecer



El 42% de los trabajadores dice que usa cuentas de correo-e personales para su labor y casi la mitad (49%) han admitido que cada vez más. Además, el 38% utiliza servicios de mensajería personal para asuntos profesionales, incluso un 60% reconoce que con más frecuencia que antes, ahora que trabaja desde casa. Los servicios de intercambio de archivos que no han sido aprobados por los departamentos de IT también se están empleando mucho, con un 53% de los encuestados que confiesa utilizarlos desde su hogar. El empleo de estos servicios ofrece grandes beneficios para la fuerza laboral en remoto pero también puede tener un coste inesperado si son objetivo de los ciberdelincuentes. Fuente: Kaspersky



con menos equipos el mismo grado de protección y seguridad.

Pero la realidad no es *halagüeña*: un 46% confesó haber tenido, al menos, un incidente de importancia desde que cambió a un modelo de trabajo remoto. Además, la transición ha sido tan agresiva, que un 55% destacó que no habría implementado la forma de trabajo en remoto, al menos, en los próximos cinco años de no haber sido por esta crisis sanitaria. Eso sí, ya comenzado este proceso, el 56% dijo que continuará con el teletrabajo una vez haya pasado la pandemia. Incluso, más de la mitad de los encuestados explicó que ha acelerado sus planes de migración para dar seguridad al trabajo en remoto apostando, casi en un 100%, por modelos basados en la nube.

Otras investigaciones, como la realizada por **CrowdStrike**, también resaltan que la nube va a ser cada vez más importante para garantizar la seguridad en remoto de los trabajadores, ya sea con una infraestructura pura o híbrida.

BrightSight, una compañía de calificación de seguridad con sede en los Países Bajos, preguntó a más de 41.000 empresas sobre los problemas que han sufrido por tener que trabajar desde casa. El resultado es desalentador: acostumbrados a manejar un riesgo aceptable en la protección diaria corporativa, se conoció que el 45% de los encuestados reconoció haber detectado software malicioso (*malware*) en sus redes domésticas, frente al 13,3% de las redes de las empresas. Además, se constató que el 25,2% de las redes domésticas tenían uno o más servicios expuestos en Internet.

De ellos, el 61,2% presentaba una interfaz de control de módem por cable expuesta, uno de los canales más habituales para realizar ciberataques por Internet. Según los responsables de la investigación, "es fundamental", en este sentido, "que el equipo de gestión de activos se asegure de que su empresa tiene políticas y procedimientos específicos por escrito para los empleados que trabajan desde casa", ya que "si bien no se puede eliminar todo el riesgo asociado con los empleados remotos, la higiene básica de seguridad puede reducir un gran porcentaje de los ataques más comunes y básicos".

Por su parte, **Kaspersky**, en su informe 'Cómo el Covid-19 está cambiando el trabajo de la gente', en el que entrevistó a más de 6.000 trabajadores de todo el mundo, también destacó la importancia de tener claro cómo se conectan los empleados a las redes corporativas. Y es que, "desde principios de marzo, los ataques en puertos abiertos a RDP, el protocolo de conexión remota más popular, se disparó en todo el mundo". Además, "cuando se produce una conexión en remoto a una red corporativa desde casa, los empleados no suelen tener en cuenta al resto de equipos que pueden estar vinculados a su *router* doméstico y que podrían ser vulnerables".

Cómo lo ven los centros y agencias

Las principales agencias de ciberseguridad y centros nacionales de inteligencia, que también velan por la protección del ciberespacio, han trabajado a contrarreloj durante la crisis de la Covid-19, tanto para anticiparse a posibles incidentes en sus infraestructuras críticas, sobre todo hospitales, como para publicar todo tipo de informes con alertas y actualizaciones sobre posibles vulnerabilidades en las herramientas de trabajo en remoto más utilizadas, sobre todo para videoconferencias, además de dar a conocer buenas prácticas que reduzcan el riesgo en esta situación.

Especialmente activo ha sido el **Centro Criptológico Nacional** (**CCN**), que ha venido publicando varias guías y documentos sobre herramientas y políticas para un acceso remoto seguro, tanto a través de la nube como para sistemas en local. Precisamente, sobre este último aspecto publicó un útil 'Abstract' titulado 'Medidas de seguridad para Acceso Remoto', en el que analiza cómo proteger, en remoto, correos electrónicos, salas de reuniones virtuales, conexiones con proveedores o procedimientos de actuación de las personas o equipos que estén trabajando en su casa. Entre sus recomendaciones más importantes están desde la de realizar pruebas de conectividad de los diferentes usuarios que puedan usar el acceso remoto, comprobando su funcionalidad y registrando sus direcciones IP, hasta tener actualizado el puesto de trabajo con los últimos parches de seguridad (sistema operativo, herramientas de seguridad, aplicaciones, etc.), cerrar todas las conexiones que no sean estrictamente necesarias y todas las aplicaciones cuando no se estén utilizando y realizar análisis programado de los antivirus (exhaustivos) a los puestos de trabajo. Además, en él recomienda tener un listado de las direcciones IP de los posibles orígenes remotos de las conexiones y contar con listados de personas, teléfonos, correos-e corporativos y alternativos, relacionados con el acceso a los sistemas de forma remota.

El CCN, incluso, habilitó una sección específica en su web, que sigue activa a fecha de cierre de esta edición, bajo el nombre 'CiberCOVID19', para prevenir riesgos cibernéticos. En ella, incluye los trabajos de algunas comunidades autónomas y organismos, así como informes sobre concienciación, acceso remoto seguro, alertas y avisos.

Por su parte, el **Instituto Nacional de Ciberseguridad** (**Incibe**) publicó varias recomendaciones para teletrabajar de forma segura con pautas básicas, como el uso de VPNs y comunicaciones cifradas, entre otros.

También, han emitido informes para proteger los datos y garantizar la privacidad de los usuarios los principales organismos nacionales como la **AEPD** o su homóloga gala, **CNIL**, que facilitaron a las empresas orientaciones sobre cómo implementar las mejores prácticas en este contexto. Su objetivo fue garantizar la privacidad de los trabajadores y la protección legal de los datos de los clientes asegurándose de que tienen en marcha una "una política de seguridad informática o de seguridad de la información que cubra el teletrabajo o, como mínimo, un conjunto de reglas mínimas que cada empleado en remoto debe cumplir, de carácter vinculante".

En Estados Unidos, los principales organismos que velan por la ciberseguridad en la Administración Federal, también fueron muy activos en la elaboración de informes y documentos sobre teletrabajo. Incluso la **Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA)** creó una plataforma web específica (www.cisa.gov/telework) con recomendaciones en todos los ámbitos, también el educativo. Su informe de referencia fue la 'Guía de Teletrabajo Provisional TIC 3.0', presentada en abril con el apoyo de la **Agencia Nacional de Ciberseguridad (NSA)** y el **Departamento de Seguridad Nacional**

(DHS), basada en las recomiendas para el trabajo en remoto del **Pentágono** (en su documento 'DoD Cyber Exchange Telework').

Uno de los aspectos más interesantes es que ofrece diferentes consejos, según el tipo de conexión, para trabajar en remoto: desde para los trabajadores a distancia que acceden directamente a los recursos del proveedor de servicios en la nube, hasta para los que se conectan a través de VPN y las redes de una organización, a los recursos de la nube y los que lo hacen a través de un CASB para acceder a recursos CSP aprobados por la CISA.

Precisamente, priorizar los productos y servicios certificados para organismos oficiales ha sido una de las principales recomendaciones de todas las entidades públicas, como también lo hizo la **Dirección Digital Interdepartamental (DINUM)** y la **Agencia Nacional de Ciberseguridad de Francia** (ANSSI), llegando a no recomendar la plataforma de videoconferencia **Zoom** en favor de **Jitsi.**

En Estados Unidos, también destacó la guía conjunta que emitieron la **Comisión Federal de Comercio (FTC)**, el **Instituto Nacional de Estándares y Tecnología (NIST)** y la CISA sobre trabajos seguros de teletrabajo e infraestructura crítica, además de la que el Instituto hizo sobre teletrabajo seguro, acceso remoto y soluciones *Bring Your Own Device* (BYOD). El boletín resume los conceptos clave y las recomendaciones del documento 'NIST SP 800-46' aconsejando a las organizaciones valorar el "equilibrio entre los beneficios de proporcionar acceso remoto a recursos adicionales y el impacto potencial de un compromiso de esos recursos". Para mitigar los riesgos asociados con la provisión de acceso remoto, NIST cree que lo mejor es "limitar el acceso al mínimo necesario".

Desde Reino Unido, el **Centro Nacional de Seguridad Cibernética (NCSC)** publicó también varios informes y guías para el trabajo en remoto seguro en el país, prestando atención especial a las pymes, a las que da varias recomendaciones para detectar correos-e sospechosos, así como para el establecimiento de una política de gestión de riesgos.

Por último, es reseñable el trabajo del **Centro de Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC)**, que también dio indicaciones para los teletrabajadores del sector, entre los que destacan "alertar a sus MSP y MSSP del cambio en los modelos operativos para que puedan ajustar y adaptar sus notificaciones y ajustar sus actividades de monitorización". ■

La industria de la ciberseguridad en 'ayuda' del trabajo en remoto

Fabricantes y proveedores de servicios de ciberseguridad han aumentado la oferta de este tipo de soluciones para proteger el acceso remoto durante el teletrabajo, junto con otras herramientas, como las de gestión de la seguridad de los puntos finales (dispositivos móviles, servidores, máquinas virtuales y aplicaciones en la nube), a través de tecnologías EDR, que complementan y amplían las funcionalidades de los antivirus, la monitorización de la actividad de red, hasta servicios de consultoría de seguridad, análisis forense, etc.

PRINCIPALES EMPRESAS DE PRODUCTOS DE CIBERPROTECCIÓN PARA EL TELETRABAJO

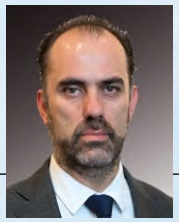
Agari	Cloudflare	ICA	Pulse Secure	Symantec (Broadcom)
Akamai	CrowdStrike	Kaspersky	Qualys	Tenable
Barracuda Networks	CyberArk	McAfee	Radiant Logic	Thycotic
BeyondTrust	DinoSec (Telefónica)	Microsoft	RiskRecon (Mastercard)	Transmit Security
Bitdefender	ESET	Microfocus	RSA	Tranxfer
Blueliv	Extrahop	Okta	SailPoint	Trend Micro
Check Point	Extreme Networks	One Identity	SonicWall	Víntegris
Cisco	Forcepoint	Oracle	Sophos	Wise Security Global
Citrix	ForgeRock	Palo Alto Networks	Stormshield	

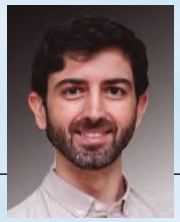
PROVEEDORES DE REFERENCIA DE SERVICIOS DE CIBERSEGURIDAD PARA EL TELETRABAJO

Accenture Security	CMC	ITS-Ibermática	Orange	Tarlogic
Aiuken	DXC	Logicalis	Oylo	Telefónica
All4Sec	Entelgy Innotec	Mdtel	Cytomic (Panda)	Tranxfer
Áudea	EY	Mnemo	PwC	Wise Security Global
Bidaidea	GFI	Netskope	S2 Grupo	Zerolynx
Blueliv	GMV	Nunsys	S21Sec	Zscaler
Botech	IBM	Omega Peripherals	Secura by Factum	
Capgemini	ICA	One eSecurity	SmartFense	
Cipher	Ingenia	OneseQ	Sothis	

El cumplimiento regulatorio en el teletrabajo como modelo operativo presente y futuro: el análisis de riesgos

El futuro post COVID-19 es incierto aún, pero si algo es seguro es que la cultura de las empresas va a cambiar. De la noche a la mañana, la mayoría de las compañías ha tenido que dar un giro de 180º en la manera en que venía desarrollando su actividad con una aceleración no planificada de su transformación digital y cultural. Los beneficios de esta transformación son muchos, al igual que los riesgos y obligaciones. Aprovecharemos este espacio para analizarlos y descubrir cómo sacar el máximo partido de ellos para las empresas y sus empleados, entendiendo las barreras de lo permitido y la necesidad del cumplimiento regulatorio (*compliance*) tomando buena nota de que específicamente dentro del *compliance*, el análisis de riesgos es el "perejil de todas las salsas".





Israel Hernández / Pablo Fernández Burgueño

Un pequeño análisis de riesgos para ir cubriendo el expediente

La gran mayoría de las empresas españolas contaban con infraestructura de teletrabajo normalmente para la administración de CPD, la gestión de incidencias, el soporte técnico remoto, etc. Las compañías más maduras también habían implantado, con mayor o menor intensidad, el teletrabajo. Pero ninguna de ellas alcanzaba a adivinar, hasta hace menos de cinco meses, que la solución debería ser desplegada de forma masiva como medida de contingencia, para salvar la continuidad de las operaciones y el negocio.

Conviene precisar que existe una evolución en las normativas en los últimos tres o cuatro años que consiste en un cumplimiento responsable (diligencia debida) basado en un enfoque de control *taylor made,* según el resultado de tus propios análisis de riesgos. Así que, remontándonos a principios de marzo, un gran número de empresas abordaron un análisis exprés de riesgos en el que se plantearon algunas de una manera más o menos formal (**Figura 1**).

Otras tantas empresas ni siquiera tuvieron tiempo para hacer este análisis exprés y se vieron obligadas a improvisar medidas tales como permitir extraer equipos fijos de la sede empresarial para que los empleados se los llevasen a sus casas o tener que asumir que sus empleados no pudiesen trabajar durante varios días hasta la adquisición de equipos portátiles, entre otras muchas situaciones.

Dos meses después del inicio del teletrabajo forzado y con perspectivas a su normalización, es fundamental identificar el riesgo real para la empresa, el *compliance* sobre la materia y, por tanto, las **modificaciones** del **ambiente de control** sobre los servicios, los procesos de negocio, la tecnología que los soportan y las personas.

Ya sea a priori o a posteriori es necesario realizar este análisis de riesgos *ad hoc* que el contexto de teletrabajo tiene en esta 'nueva normalidad'. El uso de estándares que son *best practice*, como la ISO, NIST, Magerit, CRAMM, etc., puede estar recomendado siempre y cuando su implementación sea adecuada en coste *vs* resultados rápidos; si no, elegiremos una implementación inteligente solo cogiendo las partes del estándar que apliquen en el análisis.

¿Qué debe contener este análisis de riesgos?

El análisis de riesgos debe contemplar todas las derivadas y debe ser un *artefacto* vivo.

Igualmente ha de contemplar todos los planos, entre los que destaca la continuidad de las operaciones, la protección de activos empresariales y la protección de datos personales.

• **Continuidad de las operaciones**: Con respecto a la continuidad de negocio,

El análisis de riesgos debe contemplar todas las derivadas y debe ser un artefacto vivo. Ha de contemplar todos los planos, entre los que destaca la continuidad de las operaciones, la protección de activos empresariales y de datos personales.

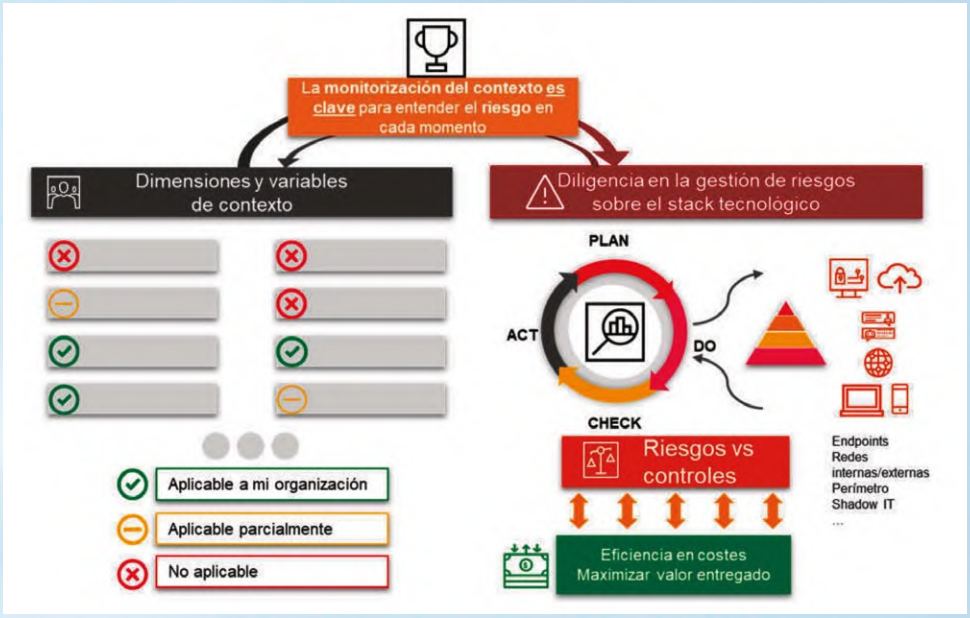
existen múltiples regulaciones sectoriales, así como mejores prácticas (*best practices*) que especifican la necesidad de contar con planes de continuidad y un *Disaster Recovery* Plan a nivel tecnológico. Estos planes tienen que contar con un escenario añadido *ad hoc* de pandemia que debe estar integrado en el Plan de Continuidad de Negocio, haciendo una actualización de los BIAs (Business Impact Analysis) y, con base en ello, priorizar los procesos de teletrabajo, adecuando las personas, tecnologías y medidas de protección.

Especial atención han tenido los servicios esenciales durante la pandemia y la protección de sus infraestructuras críticas **(LPIC)**.

• **Protección de activos empresariales**: La empresa debe prestar también especial atención a la protección de sus **"secretos empresariales"**, que es toda información generalmente desconocida o de difícil acceso, que tiene valor precisamente por ser secreta y que la empresa protege con medidas razonables de seguridad. Si la empresa se despreocupa y deja sus secretos desprotegidos, estos contarán con menos protección legal, conforme nos indica la **Ley de Secretos Empresariales, de 2019**. Por tanto, incluso las medidas que salvaguardan aquello que no contenga datos personales deben ser objeto de revisión en situaciones de teletrabajo.

Por otro lado, diferentes normas sectoriales también determinan los objetivos de seguridad y confidencialidad que se han de lograr en muchas profesiones. Estas normas complementan a las generales aumentando el nivel de *compliance*. Así, por ejemplo, el **Código Deontológico de la Abogacía Española, de 2019**, establece que el secreto profesional ampara las comunicaciones y negociaciones orales y escritas de todo tipo, con independencia del medio, lo que obliga a los bufetes a analizar previamente cada una de las herramientas que vayan a usar con el fin de determinar su conveniencia y, en su caso, las medidas adicionales que se deben desplegar para garantizar la seguridad y el secreto profesional. De igual manera, se debe preservar la confidencialidad para las fuentes de origen de la información en el marco del periodismo (**Ley de Prensa, de 1966**) y para los datos de salud de los pacientes en el de los servicios sanitarios (**Ley de Autonomía del Paciente, de 2002**).

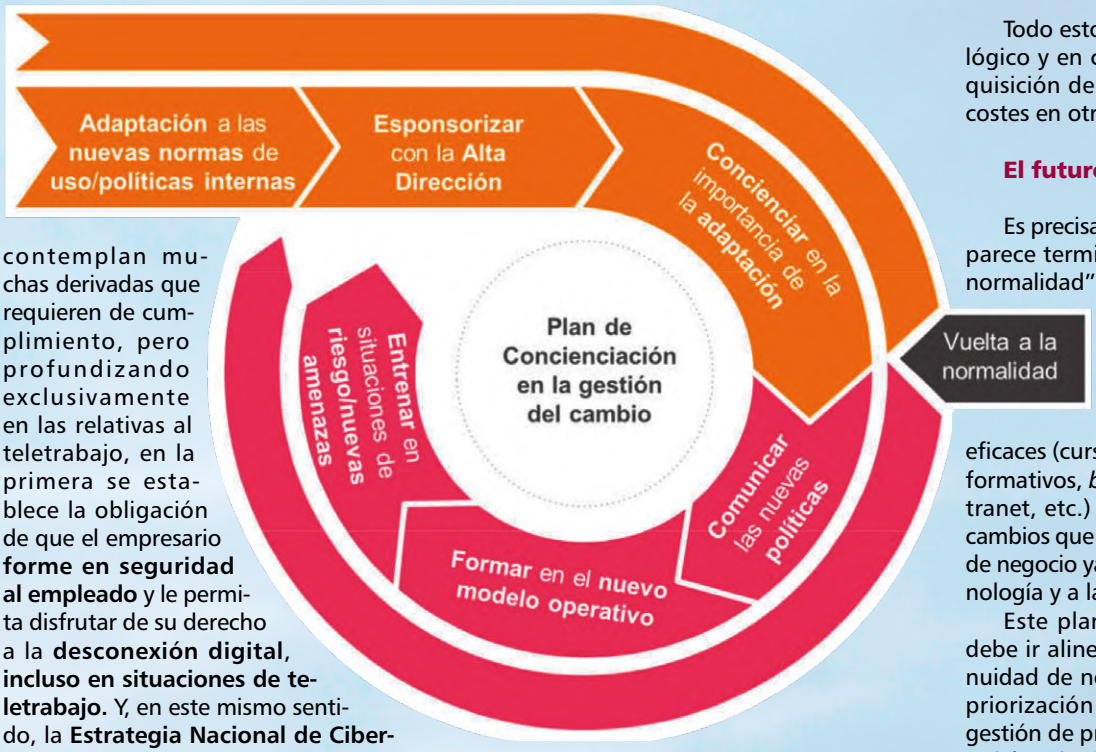
Además, hay otras regulaciones transversales concretas como **NIS, PCI–DSS, SWIFT, SCIIF** que requieren establecer medidas diligentes en la protección de la información, junto con los controles generales aplicables.



La gestión y monitorización de los empleados con la excusa de medir su performance no solo abre el dilema de la legitimación del tratamiento y los derechos encontrados entre compañía y empleado, sumado a los considerandos de desconexión digital versus conciliación, sino que también supone nuevos retos y oportunidades en el campo de la seguridad empresarial.

• **Protección de datos personales:** Por otro lado, también la información que permita identificar y concierna a empleados, usuarios, clientes y proveedores debe permanecer debidamente resguardada en todo momento frente a accesos, manipulaciones o borrados que deseen realizar personas no autorizadas. En este sentido, el **RGPD** así como la **normativa local de desarrollo** establecen la obligación de desplegar y mantener actualizadas en todo momento las medidas técnicas y organizativas apropiadas para garantizar la seguridad sobre el dato y los tratamientos. Las **empresas están obligadas a cumplir y a poder demostrar que han cumplido**, que se han planteado el cambio y han realizado los análisis, las evaluaciones de impacto y los despliegues necesarios para proteger los procesos asociados a los tratamientos y los datos, como uno de sus principales activos.

• *Compliance* **hacia las personas**: La norma española de desarrollo en materia de protección de datos personales y el propio **RGPD**



contemplan muchas derivadas que requieren de cumplimiento, pero profundizando exclusivamente en las relativas al teletrabajo, en la primera se establece la obligación de que el empresario **forme en seguridad al empleado** y le permita disfrutar de su derecho a la **desconexión digital, incluso en situaciones de teletrabajo.** Y, en este mismo sentido, la **Estrategia Nacional de Ciberseguridad**, en su última versión publicada (2019), establece como objetivo lograr una mayor ciberseguridad de ciudadanos y empresas adaptada a la situación que se viva en cada momento. El **conjunto normativo** exige la **revisión** y **actualización continua** de los **planes formativos**, para empleados y clientes con orientación al riesgo.

Estos planes de concienciación se basan en **campañas** de transformación y gestión del cambio, que **deben focalizarse** en mitigar fugas de información y mal uso de los sistemas. Durante el **teletrabajo los empleados** están **expuestos** a un **mayor número** de **amenazas**, tanto técnicas como de ingeniería social por lo que **no se trata de una acción puntual** para tener un ***tick the box* en el *compliance***. En un plan de concienciación a empleados debemos:

- **Concienciar** de las amenazas para combatir los sesgos, hábitos y costumbres.
- **Comunicar** las nuevas normas, políticas y *best practices* que la empresa quiera implementar para familiarizar a los empleados con las soluciones y evitar rechazo.
- **Formar** con los conocimientos necesarios para que los empleados puedan ejecutar los procesos y nuevos procedimientos sin poner en peligro a la empresa.
- **Entrenar** a los empleados y directivos para que la respuesta a incidentes se pueda considerar parte de la operativa habitual, la cual estará soportada por las políticas internas.

El resultado

Como base del análisis de riesgos, se esperan respuestas y controles sobre varias dimensiones:

- Revisión y uso de los riesgos y obligaciones mediante un **cuerpo normativo actualizado completo** y **robusto** del nuevo entorno.
- Los **patrones de seguridad** del acceso de empleados y colaboradores.
- **Medidas extra a nivel de infraestructura y arquitectura de protección**: uso de dispositivos portátiles plataformados, VPNs, dobles factores de autenticación, antivirus, MDM, gestión del ciclo de vida de parcheado, *read team* continuo, etc.
- Control del **Shadow IT** y los **aplicativos de mensajería instantánea** (WhatsApp, Telegram, etc.) y la convivencia de su uso con propósito profesional y personal.
- Las **lecciones aprendidas** durante este periodo de confinamiento y patrones identificados de acceso remoto.
- Los casos de **incidentes, incidencias** y distintos **patrones de fraude** identificado en la empresa.
- El **% de personal** asociado a **procesos críticos** que requieren mejoras de niveles de servicio.
- El **% de colaboradores** que requieren acceso en relación **con los que no**.
- Control de que las **medidas implantadas** por mis **terceros** estén **alineadas** con las **medidas** desplegadas **internamente**.

Todo esto impactará en el *stack* tecnológico y en costes de licenciamiento, adquisición de tecnologías, decremento de costes en otras partidas, etc.

El futuro

Es precisamente ahora, que la reclusión parece terminar y la vuelta a "una nueva normalidad" se acerca, cuando las empresas deben seguir concienciando en su "plan de vuelta a la normalidad".

Será necesario establecer canales de comunicación eficaces (cursos, correo electrónico, vídeos formativos, *blogs* de dudas, noticias en intranet, etc.) para informar de los nuevos cambios que afectarán tanto a los procesos de negocio ya mencionados, como a la tecnología y a la protección de activos.

Este plan de vuelta a la normalidad debe ir alineado con los planes de continuidad de negocio de la empresa para la priorización de colectivos y procesos, la gestión de proveedores, la compra de material sanitario etc.

Se debe incluir una importante campaña de concienciación sobre las medidas de cumplimiento adoptadas para empleados y colaboradores, que les permita conocer los servicios disponibles y las obligaciones que deben cumplir.

Además, se debe incluir una importante **campaña** de **concienciación** sobre las **medidas de cumplimiento adoptadas** para empleados y colaboradores**,** que les permita conocer los servicios disponibles y las obligaciones que deben cumplir**.** Así, se establece la necesidad de adecuar los antiguos puestos de trabajo para un servicio local adaptado o establecer sistemas seguros, física y lógicamente, para el teletrabajo, con plenas garantías de cumplimiento normativo y de protección de activos.

En este sentido la gestión y monitorización de los empleados con la excusa de medir su *performance* no solo abre el dilema de la legitimación del tratamiento y los derechos encontrados entre compañía y empleado, sumado a los considerandos de desconexión digital versus conciliación, sino que también abre nuevos retos y oportunidades en el campo de la seguridad empresarial. ■

Israel Hernández
Socio Business Security Solutions

Pablo Fernández Burgueño
Abogado of counsel de PwC Tax and Legal Services

PwC

riskrecon

mastercard

www.riskrecon.com

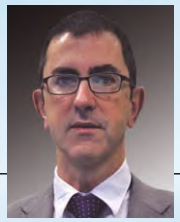
La gestión de riesgos de terceros es esencial para el éxito de su negocio.

RiskRecon es el único sistema en el mundo en el que los riesgos priorizan de forma automática los problemas en función del valor de los activos y la gravedad del problema, lo que proporciona una verdadera visibilidad del riesgo real IT de un proveedor.

Para obtener más información sobre el enfoque de RiskRecon, o solicitar una demostración, visite el sitio web www.riskrecon.com

El acceso remoto orientado al teletrabajo, un reto para el CISO

Casi todas las empresas tienen desde hace tiempo y desde un punto de vista técnico un entorno de teletrabajo, al menos desde que los empleados pueden leer el correo en el móvil o utilizar un navegador para acceder a los servicios en nube de turno. Si los servicios en *cloud* han roto el perímetro del centro de proceso de datos, el impulso del teletrabajo ha terminado por romper el perímetro de seguridad tradicional de las oficinas.



Juan Carlos Gómez Castillo / Alejandro Becerra González

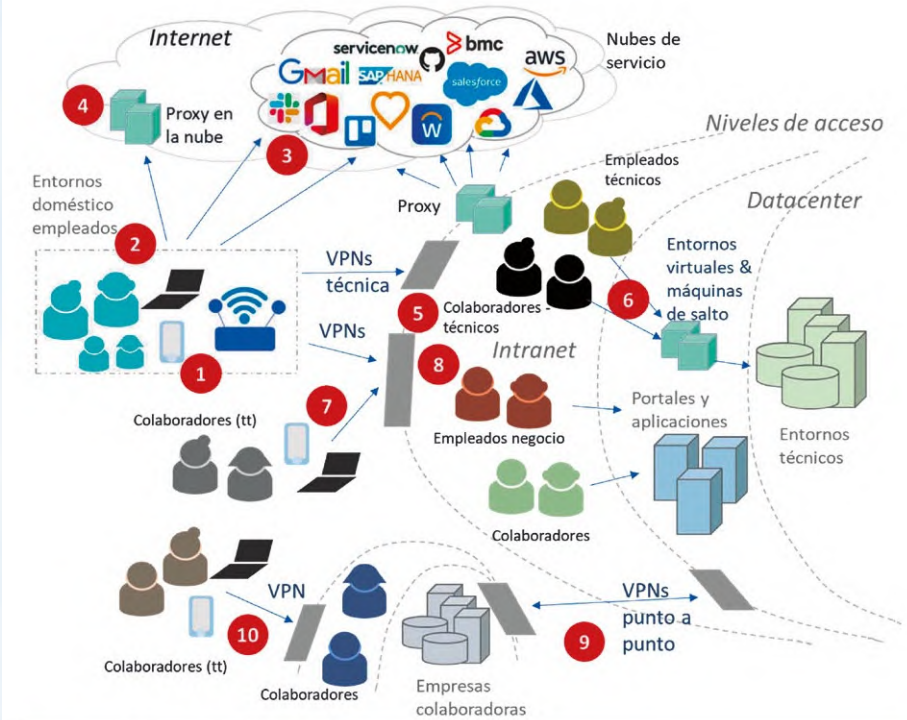
La seguridad en el teletrabajo abarca tanto la **seguridad de los servicios que facilitan y hacen posible el teletrabajo** (servicios de videoconferencias, colaboración en grupo, redes sociales empresariales, almacenamiento, compartición y edición de documentos colaborativa, etc.) como la **seguridad de los dispositivos electrónicos desde los que se teletrabaja** (ordenador, móvil, etc. tanto corporativos como personales).

Desde la perspectiva de la seguridad de los dispositivos electrónicos desde los que se teletrabaja, **al responsable de seguridad se le plantean una serie de interrogantes**, como son: ¿hay que tratar Internet como si fuera la Red Corporativa o la Red Corporativa como si fuera Internet? ¿Se permite sólo trabajar en dispositivos plataformados y controlados por la empresa o también desde cualquier dispositivo personal o ajeno (controlado por un hotel, el vecino, una *botnet*…)?

La contestación a estas preguntas entraña **desafíos relativos a la seguridad de los dispositivos utilizados para el teletrabajo y que no están conectados a la Red Corporativa**. Algunos de estos desafíos son:

- Proteger la navegación hacia Internet.
- Proteger los dispositivos de las amenazas que se propagan por Internet.
- Actualizar los parches de seguridad (ya no siempre posible desde repositorios internos).
- Actualizar las firmas y políticas de antivirus/antimalware/EDR.
- Asegurar la identidad del usuario y del dispositivo fuera de la Red Corporativa, tanto en el acceso remoto por VPN como a los servicios en nube.
- Monitorizar la actividad maliciosa.
- Evitar la suplantación de los servidores y servicios de la empresa o en nube a los que acceden los empleados.
- Dar soporte remoto en caso de que el usuario tenga problemas con el dispositivo.
- Reaccionar frente a la posible pérdida o robo del dispositivo en los desplazamientos.
- Limitar y asegurar el acceso de colaboradores externos y proveedores desde sus propios dispositivos.
- Prever y reducir los riesgos de intercepción y desviación de tráfico de los dispositivos.
- Suplir la falta de formación de los empleados en este contexto más aislado.

Es necesario desplegar medidas de seguridad que minimicen el riesgo que introduce el teletrabajo. A continuación, se hacen **reflexiones sobre algunas de las principales medidas de seguridad** que cubren parte de los desafíos planteados anteriormente.



Los principales puntos de atención a proteger son:

1. Dispositivos empleados
2. Entorno hogar empleados
3. Herramientas colaborativas
4. Navegación empleados
5. VPNs de acceso
6. Accesos privilegiados
7. Accesos de colaboradores
8. Segmentación de accesos
9. Conexiones con redes de proveedores
10. Teletrabajo colaboradores

Proxy de navegación en nube

Dentro de la Red Corporativa la navegación a Internet está protegida por el *proxy* de salida, pero no es así para los dispositivos remotos (y conectarse por VPN sólo para esto puede resultar un cuello de botella).

Como alternativa podemos pensar en un *proxy* en la nube, en un modelo SaaS de pago por uso o por usuario, en un modelo de nube pública o privada. En cualquiera de los modelos habrá que sopesar el rendimiento, el ancho de banda y el control sobre el entorno.

También existe la opción de reutilizar la inversión del *proxy* que da servicio a los dispositivos de la Red Corporativa y permitir su uso desde Internet, pero con cuidado en la penalización del tráfico de entrada y salida.

En cualquier modalidad, habrá que prestar especial atención a los siguientes aspectos:

– La autenticación de los usuarios frente al *proxy* y del *proxy* frente a los usuarios, bien por doble factor de autenticación en el primer caso como por el uso de certificado en ambos.

– El cifrado de las comunicaciones entre el dispositivo y el *proxy*, que si bien en un entorno de Red Corporativa no tenía mayor importancia, en un entorno de teletrabajo sería casi obligatorio.

– La obligatoriedad de utilizar el *proxy* en los dispositivos, bien por políticas en los dispositivos controlados por la empresa o por que no quede más remedio para acceder a las aplicaciones de la empresa, abriendo así la posibilidad de utilizar el *proxy* como "VPN" de acceso a las aplicaciones de la empresa, si todas son aplicaciones web.

La disponibilidad del servicio, que adicionalmente debe estar respaldado por una solución de contingencia.

Antimalware/EDR

Una solución de antimalware/EDR es fundamental para poder proteger los equipos que están en un entorno hostil fuera de la Red Corporativa. Es necesario que la solución pueda actualizarse a través de Internet casi en tiempo real y que permita a los equipos de respuesta a incidentes disponer de una telemetría y la capacidad de poder realizar investigaciones en remoto.

Esta solución puede incorporar o completarse con funcionalidades propias de un cortafuegos, cifrado de disco, protección de la navegación (como complemento o sustitutivo del *proxy*), etc.

Muchas de estas soluciones incorporan potentes funcionalidades que exceden, incluso, el objetivo para el que fueron pensadas, convirtiéndolas en "navajas suizas". Hay que extremar el cuidado en el mantenimiento y administración de las mismas porque "un gran poder conlleva una gran responsabilidad".

Escritorio virtualizado

Los escritorios virtualizados en los que se controla lo que los usuarios pueden hacer tienen ventajas desde el punto de vista de seguridad, mantenimiento y soporte. Incluso, tienen ventajas para la monitorización y respuesta efectiva de incidentes.

Sin embargo, suelen ser soluciones costosas y no muy amigables para ciertos colectivos, que por funcionalidad o por rendimiento las terminan rechazando.

En el caso de que los usuarios sean personal externo en labores de mantenimiento o administración remota, la obligatoriedad del uso de estas soluciones la determina el cliente para el que trabajan y las razones de seguridad tienen un peso importante.

Es un mecanismo que simplifica en extremo aislar las circunstancias de los puestos desde los que se accede, asegurando que se cumplen todas las políticas de seguridad de la organización. Es, de alguna forma, la vuelta al 'buen viejo terminal tonto'…

Además, el despliegue de soluciones de *deception* en estos entornos virtualizados puede abrir un campo muy interesante para los equipos de ciberinteligencia.

Identidad

La identidad es el nuevo perímetro. Y más cuando el perímetro tradicional se pierde con el teletrabajo. Puertas para las VPNs, aplicaciones en la nube, credenciales del correo…

Y la llave más simple pero más efectiva es el doble factor de autenticación y la primera que hay que perseguir. No es perfecta, pero ninguna otra da más por tan poco.

Las identidades de los usuarios (en cualquiera de los sistemas, infraestructuras o aplicaciones, en la nube o en infraestructura propia) es lo primero que busca un atacante, por lo que su supervisión cuidadosa siempre rendirá valor para evitar que un robo de identidad tras un *phishing* o por algún otro medio, resulte en un incidente de *ransomware* o una fuga de datos.

Especial cariño hay que rendirles a las cuentas privilegiadas, y éstas entendidas en su sentido más amplio (la de los administradores, las de la Alta Dirección que llevan a un típico 'fraude de CEO'). Doble motivo para que estén protegidas con doble factor, sean objeto de una monitorización dedicada, certificación frecuente, etc. La generalización de soluciones para gestión de credenciales privilegiadas, lejos ya de reservarse para aplicaciones muy sensibles, hoy día se aplican a una diversidad de credenciales de acceso a aplicaciones de lo más diverso.

Monitorización

Lo que no se mide, no se puede gestionar… lo que no se monitoriza, no se puede cuidar. La monitorización de seguridad, si bien no es fácil y muchas veces poco efectiva, es imprescindible.

La extensión del trabajo a los hogares amplía también los puntos a vigilar. Las conexiones remotas son un básico. Pero es importante la trazabilidad integrada, correlada, que de forma efectiva facilite el seguimiento de la actividad de los usuarios desde su acceso remoto hasta sus actuaciones en infraestructuras y aplicaciones.

La aplicación de reglas de detección simples (p.e. los saltos imposibles) es más actual que nunca, pero no es suficiente. Quizás algún día llegue a ser cierto que los algoritmos de inteligencia artificial nos avisen donde los ojos de los analistas no lleguen, muchas veces por cansados o aturdidos por seguir el sol.

Y si los servicios, aplicaciones e infraestructuras en la nube han venido para quedarse, habrá que monitorizarlas también… implicará, además de preparar presupuesto, un reciclaje importante de los equipos de seguridad, desde los encargados del diseño de controles a los analistas de seguridad, pasando por los responsables de gobierno de la seguridad, que en el caso de la nube adquiere una nueva importancia.

Adicionalmente a las medidas comentadas, tenemos la concienciación de los empleados (más fundamental si cabe), la actualización de parches fuera de la Red Corporativa, soluciones seguras de soporte remoto, etc. que quedan para otro artículo.

En definitiva, los empleados van a teletrabajar como sea y como puedan (el estado de alarma de la pandemia nos lo ha demostrado) y la anticipación es la clave del éxito si queremos que lo hagan de forma ordenada sin poner en riesgo la seguridad de la empresa. Las circunstancias actuales (pandemia, productividad, conciliación, etc.) nos están empujando a tener un **entorno de teletrabajo versátil que exige una adaptación valiente, imaginativa y decidida de los responsables de seguridad de las empresas** de todo tipo de actividad y tamaño. ■

Juan Carlos Gómez Castillo
Director de Seguridad Digital

Alejandro Becerra González
Director Global de Seguridad de la Información

TELEFÓNICA S.A.

El papel del DPD ante el auge del trabajo a distancia

"El trabajo en remoto presenta desafíos particulares a la protección de datos personales, en muchos casos no pequeños, y cada actor (el responsable del tratamiento, el CISO, el delegado de protección de datos) tiene su particular función para salvaguardar los derechos y libertades de los interesados". El autor de este artículo, brinda su opinión profesional documentada –y no exenta de fina y sana ironía– sobre el papel del DPD y su organización ante el hecho del tratamiento de datos personales llevado a cabo por teletrabajadores.

Carlos Bachmaier

Comenzaré recordando que no todas las organizaciones tienen obligación de designar un delegado de protección de datos personales, pero sí todas ellas tienen responsabilidades dimanantes del tratamiento de datos personales, que conllevan actuaciones diferenciales cuanto se traslada un tratamiento a trabajo a distancia; también, indicando que no abordaré la problemática sobre el tratamiento de datos de salud que pueda conllevar una epidemia que sea la impulsora del trabajo a distancia, ni de los aspectos GDD de LOPD@2018, ni hablaré de teletrabajo (que parece vincularse a aspectos laborales) sino de trabajo en remoto (*humpty dumpty, where are you?*), y ello bien por no ser asuntos del DPD o por no tener relación biunívoca con el trabajo a distancia.

SIC me ha dado el honor de invitarme a contestar a una pregunta aparentemente inocua y no compleja, y, ya se sabe: SIC nunca lanza preguntas o retos cuya respuesta no resulte un tanto comprometedora… Diríase que no es así en esta ocasión… Y, dando una respuesta sencilla a una pregunta sencilla, la respuesta sería que "**el papel del delegado de protección de datos personales no cambia porque se expanda el trabajo a distancia**". Pero, probablemente, esta fuera una lectura y contestación mecanicista a la cuestión del título ;-) Lo intentaremos de nuevo, reinterpretando la pregunta para anular la anfibología que presenta, acudiendo a la pragmática.

(Pero antes no puedo resistirme a incluir un chascarrillo que siempre gustaba contar mi difunto socio en GMV, el Profesor Dr. Martínez García. Ahí va: dos amigos viajando en globo se adentran en la niebla y se encuentran perdidos. Descienden hasta casi el suelo y le vociferan a un hombre en tierra: "Disculpe, ¿dónde estamos?". El hombre se pone a pensar…, sigue pensando… Y, al fin, dice: "Están ustedes en un globo aerostático a escasa altura del suelo y rodeados de un banco de niebla". Del globo contestan: "Debe ser usted matemático (sustitúyase por ingeniero, científico, informático, etc.): ha tardardo un montón en darnos una contestación que, si bien es absolutamente precisa y exacta, resulta verdaderamente inútil". Y el del suelo replica: "Ustedes deben ser consultores…").

En una situación donde, por los motivos que sea, se traslada una parte significativa del tratamiento de datos personales de entornos situados en dependencias del responsable del tratamiento a ser tratados en entornos diferentes y otras dependencias (tales como la vía pública o la vivienda de trabajadores y, en ocasiones, equipos propiedad de los empleados), si bien el riesgo (inherente) para los derechos y libertades de los interesados no varía, los activos de información tratados se enfrentan a amenazas distintas, que deben ser analizadas y gestionadas mediante las correspondientes medidas, fundamentalmente de ciberseguridad y de sensibilización y formación a las personas.

DPD: cambio de foco

Las funciones del DPD en nada cambian, si bien el foco de alguna de sus actividades sí ha de cambiar. Fundamentalmente, el delegado de protección de datos debe prestar una atención especial a los cambios de riesgos, y, en concreto, a los que supone supervisar que se identifican y protegen **nuevos tratamientos** que ocurran por trabajar en remoto, tales como los derivados de participación en teleconferencias, asesorando debidamente al responsable sobre estos aspectos. Un caso de especial relevancia son los sistemas de registro horario remoto y la prohibición de uso de métodos biométricos de contacto en algunas circunstancias. La normativa laboral exige la llevanza del registro horario también en trabajo en remoto, y el interés legítimo del empresario de medición del desempeño y de cumplimiento de la jornada laboral, esto es, en controlar que se presta un trabajo adecuado en el horario pactado. Ello puede llevar al empleo de técnicas como geolocalización,

En una situación donde, por los motivos que sea, se traslada una parte significativa del tratamiento de datos personales de entornos situados en dependencias del responsable del tratamiento a ser tratados en entornos diferentes y otras dependencias (tales como la vía pública o la vivienda de los trabajadores y, en ocasiones, en los equipos propiedad de los empleados), si bien el riesgo (inherente) para los derechos y libertades de los interesados no varía, los activos de información tratados se enfrentan a amenazas distintas, que deben ser analizadas y gestionadas.

supervisión de pantalla y teclado y control de presencia mediante video, todo lo cual debe ser exquisitamente estudiado en términos de proporcionalidad.

Si bien, como se ha dicho, el tratamiento de datos en trabajo en remoto no cambia los riesgos para los derechos y libertades de los interesados, probablemente, debido al cambio de amenazas sobre los activos de información, sea necesario desplegar medidas de protección de los activos de información adaptadas a la situación, por lo que **el delegado de protección de datos debe informar y asesorar al responsable del tratamiento que efectúe una revisión de los correspondientes análisis de riesgo sobre los activos de información**, y medidas a tomar, labor que todo CISO competente se encuentra en perfectas situaciones de acometer con el apoyo de la AEPD[1]; y **supervisar las correspondientes acciones de despliegue y adaptación**.

A título de ejemplos evidentes, vayan estos: asegurar la integridad del equipo remoto de acceso, la autenticidad del usuario remoto, establecer comunicaciones cifradas, asegurar la integridad y protección de la confidencialidad de equipos en tránsito, asegurar el empleo adecuado de la nube, estructurar las salvaguardas de copias de seguridad y, sin duda los aspectos más complejos: asegurar que en el equipo remoto de acceso se asegura la integridad, disponibilidad y confidencialidad de los datos – taponando cualquier vía de escape de información (frente al riesgo interno y el externo); y mediante acciones de concienciación y formación con los trabajadores en remoto. Al ser estos últimos problemas complejos, pues dichos equipos remotos de acceso en ocasiones pudieran ser personales del empleado, resulta conveniente revisar en los sistemas *on premise* el nivel de acceso a datos, restringiéndolo a lo más mínimo viable (no solo en amplitud de datos de un interesado sino, aún más, en cuanto a número de interesados y necesidad del acceso). Tampoco puede desatenderse la detección de brechas de seguridad en los equipos remotos.

El DPD también debe supervisar que los sistemas de tratamiento en las dependencias del responsable de tratamiento tengan niveles de protección adecuados acompasados a circunstancias extraordinarias de amenazas que puedan surgir.

"Mayordomo de datos personales"

Lo anteriormente descrito, responde al papel, *stricto sensu*, que corresponde con las funciones asignadas al DPD por la normativa vigente, si bien, puede tener asignadas –lo que no es infrecuente– funciones asociadas a las responsabilidades del responsable del tratamiento, que podríamos designar como de gestor de la protección de datos, coordinador de la protección de datos, o, como personalmente me gusta designar, mayordomo de datos personales (mayordomo en el sentido contemplado en https://es.wikipedia.org/wiki/Mayordomía, esto es, en llevar adelante la gestión responsable de los datos personales tratados por el responsable del tratamiento. Estas funciones no corresponden al DPD pero adecuadamente planteadas pueden, dentro de ciertos límites, no ser incompatibles con las mismas.

Si bien la normativa vigente establece las responsabilidades del (sic) responsable del tratamiento, que define como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento", no desciende al suelo a la hora de matizar cómo se materializan las mismas en una organización. Siendo positivo dar libertad a las organizaciones para establecer delegaciones de autoridad y responsabilidad, tal vez hubiera de haberse establecido una cierta obligación de que las personas jurídicas especificaran la obligación de designar una persona física como delegada de dichas responsabilidades. A falta de tal hecho, se deberá estar a lo que cada organización desee llevar a cabo o entenderse que los poderes asignados el máximo ejecutivo de la misma le asignan tal delegación. Parece de cajón de cama para niños de madera; pero indefectiblemente muchos de los DPD con los que hablo tienen dificultades para enseñar un papel que lo ponga y apuntar con el dedo al representante en la tierra del ente jurídico, a efectos de cumplimiento.

Las funciones del DPD en nada cambian, si bien el foco de alguna de sus actividades sí ha de cambiar, ya que debe prestar una atención especial a los cambios de riesgos, y, en concreto, a los que supone supervisar que se identifican y protegen nuevos tratamientos que ocurran por trabajar en remoto, tales como los derivados de participación en teleconferencias, asesorando debidamente al responsable sobre estos aspectos.

Dependiendo de dicha cascada de delegaciones, alguna(s) persona(s) física(s) tendrá(n) encomendada(s) diversas funciones relativas a asegurar las responsabilidades del (sic) responsable del tratamiento, que podrán corresponder al CISO (en cuanto al análisis de riesgos de activos de información y como protegerlos), a un "oficial de cumplimiento" (tal vez de los aspectos más legales de la normativa) o incluso a figuras como el antedicho mayordomo de datos personales.

Las actividades de estas funciones sí se ven más impactadas por un traslado de tratamientos de datos personales a entornos de trabajo en remoto, en los términos que se han indicado anteriormente, especialmente en analizar los riesgos de activos de información y desplegar medidas.

Funciones del DPD

Puede merecer la pena recordar cuales son las funciones asignadas al DPD por el RGPD, Artículo 39, "Funciones del delegado de protección de datos". Las mismas, para despejar toda incógnita,

[1] Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteger-datos-teletrabajo.pdf

las podemos resumir en (remplácese responsable por encargado cuando corresponda):

• Informar y asesorar (al responsable) del tratamiento (y a los empleados que se ocupen del tratamiento) de las obligaciones que les incumben.

• Supervisar el cumplimiento de las obligaciones normativas y de las políticas (que el RGPD ni define, ni prescribe explícitamente) del responsable en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

No resulta infrecuente encontrar a DPDs que tienen funciones asociadas a las responsabilidades del responsable del tratamiento, que podríamos designar como de gestor de la protección de datos o coordinador de la protección de datos, y llevan adelante la gestión responsable de los datos personales tratados por el responsable del tratamiento. A este tipo de figuras podría corresponderles funciones de análisis de activos, protección y cumplimiento.

• Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

• Cooperar con la autoridad de control; y actuar como punto de contacto de la autoridad de control.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Como se ve, las funciones no se alteran en presencia o ausencia de trabajo en remoto, si bien varían en su foco por el distinto riesgo (operativo) del tratamiento.

Algunos claroscuros hay, y tal vez sea conveniente poner sobre la mesa ciertas limitaciones. Quizás si D.R. Hofstadter hubiera sido expuesto a los influjos de la primera década del siglo XXI, su libro de 1979, Gödel, Escher, Bach: un Eterno y Grácil Bucle (Gödel, Escher, Bach: an Eternal Golden Braid), tal vez lo hubiera centrado, y titulado, STEM, Arte y Legislación (SAL): un homomorfismo Atemporal, Sincronizado y Lagrangiano… Tras ello, nosotros hubiéramos traspasado un punto Jombar (¿sobre 27 de abril de 2016?) donde la plasmación de la normativa de protección de datos abandonó el homomorfismo SAL, produciéndose una disrupción de coherencia espacio-temporal que trata de 'apañarse' (i.e., *arrange*) mediante diversos mecanismos de expansión, explicación, parcheo y sincronización, en ocasiones orquestados como recomendaciones de grupos de sabios. Pero hay un conjunto de conceptos jurídicamente indeterminados que merece la pena repasar.

WP 243 rev.01: algunas luces sobre las funciones

El WP 243 rev.01 aporta algunas luces sobre las funciones. Entre las relevantes al caso, el WP precisa la cuestión de que el delegado de protección de datos debe actuar de manera **autónoma, independiente y sin conflicto de interés. Nada cambia en esto haya o no el trabajo a distancia**. Y continúa indicando que, no obstante, la autonomía del DPD no significa que tenga poder para adoptar decisiones más allá de sus funciones, ya que el responsable del tratamiento sigue siendo responsable del cumplimiento de la normativa de protección de datos y debe ser capaz de demostrar dicho cumplimiento. La claridad queda reforzada con el texto que indica que "si el responsable del tratamiento toma decisiones que son incompatibles con el RGPD y el consejo del DPD…", texto que evidencia que ello puede ocurrir.

Relativo a la supervisión, se cita que el considerando 97 especifica además que, "al supervisar la observancia interna del presente Reglamento, el responsable debe contar con la ayuda" del DPD. Y abunda en "como parte de esas obligaciones de supervisión de la observancia, el DPD puede, en particular: recabar información para determinar las actividades de tratamiento; analizar y comprobar la conformidad con la normativa de las actividades de tratamiento; informar, asesorar y emitir recomendaciones al responsable.

También remarca que "supervisar la observancia no significa que el DPD sea personalmente responsable de cualquier caso de inobservancia. El RGPD establece claramente que es el responsable y no el DPD quien está obligado a aplicar "medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento". El cumplimiento de las normas en materia de protección de datos es responsabilidad corporativa del responsable del tratamiento, no del DPD". **Los DPD no son personalmente responsables en caso de incumplimiento** del RGPD. El RGPD deja claro que es el responsable del tratamiento quien está obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza de conformidad con sus disposiciones (artículo 24, apartado 1); el cumplimiento de las normas sobre protección de datos es responsabilidad del responsable.

También indica que "el DPD desempeña un papel fundamental en la promoción de una cultura de protección de datos dentro de la organización y contribuye a la aplicación de elementos esenciales del RGPD, como los principios relativos al tratamiento de datos, los derechos de los interesados, la protección de los datos desde el diseño y, por defecto, el registro de las actividades de tratamiento, la seguridad del tratamiento y la notificación y comunicación de las violaciones de la seguridad de los datos".

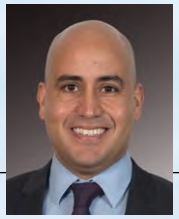
Se va precisando más explícitamente el alcance de las funciones del DPD, que corresponden de forma un tanto controvertida con más de una de las diversas líneas de defensa clásicas, al mezclar asesoramiento/consultoría con supervisión. ■

Carlos Bachmaier
ABAPLLC (además de empleado por cuenta ajena)
Para contacto sobre este artículo, escribir a sic202006@abapllc.33mail.com (buzón que se decomisionará en sep. 2020)


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.

Gestión de Identidades y Accesos: la receta para el teletrabajo seguro

La situación excepcional que se ha generado como consecuencia del COVID-19 ha propiciado una transformación en el modo de operar de las organizaciones donde el teletrabajo es fundamental. Evidentemente, el asumir el trabajo remoto de forma masiva requiere de un análisis más profundo y medidas de ciberseguridad aún más robustas. Para la mitigación de los riesgos asociados al acceso remoto, es fundamental la implantación de políticas, procedimientos y soluciones tecnológicas para la gestión de identidades y accesos que incluyan, entre otras cosas, mecanismos de autenticación fuerte y apliquen el principio de mínimos privilegios controlando todavía más a los usuarios con accesos especialmente sensibles.



Nelson Sánchez Vera

Éramos conscientes de que más temprano que tarde las organizaciones asumiríamos el teletrabajo como una forma habitual de operar, lo que no imaginábamos es que adoptaríamos este modo de trabajo de una manera tan abrupta debido a una situación tan extraordinaria como una pandemia global causada por un virus desconocido.

El día a día de una empresa con un gran porcentaje de sus empleados (o subcontratados) trabajando de manera remota no sólo se traduce en facilitar el acceso al correo electrónico, agenda o intranet corporativa desde internet mediante el uso de dispositivos móviles, también supone, entre otras muchas cosas, facilitar el acceso remoto a transacciones críticas para el negocio por parte de altos directivos o el acceso de los operadores, desarrolladores y personal de soporte a su entorno tecnológico con los accesos privilegiados que suelen necesitar.

Como no podía ser de otra forma, **si se conectan más personas para realizar nuevas y más intervenciones en los sistemas de información de manera remota, mayor será el grado de exposición a los riesgos derivados de este tipo de accesos.** Las amenazas y vulnerabilidades asociadas a estos riesgos son viejas conocidas. Podemos destacar las siguientes:

- Aumento de los ataques de *ransomware* y *phishing*.
- Aumento del robo de credenciales.
- Despliegue de nuevos *malware*.
- Uso de roles que no han sido diseñados para el teletrabajo.
- Trabajo desde entornos físicos poco seguros.
- Al ser una situación generalizada se heredan los riesgos de proveedores y terceros a la organización.
- La fuga de datos se convierte en un problema creciente (tanto si es intencionada como accidental).
- Asignación de roles sin el control necesario como consecuencia de las crisis.
- No se lleva a cabo un seguimiento adecuado de las alertas de seguridad debido al aumento del número de alertas y/o por falta de la infraestructura/mecanismos adecuados para hacerlo de forma remota.

El tratamiento de estos riesgos es un tema en el que se viene trabajando desde hace ya mucho tiempo; de hecho, organismos ampliamente aceptados y reconocidos han publicado recomendaciones y buenas prácticas específicas aplicables al teletrabajo. Por ejemplo, el NIST propone una guía para el teletrabajo y el acceso remoto (Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security); por su parte ISO/IEC proponen, en su archiconocida serie de guías de buenas prácticas de técnicas de seguridad para las tecnologías de la información (ISO/IEC 27000), una buena cantidad de controles que aplican al teletrabajo. A nivel local, el Centro

Si se analizan las recomendaciones, buenas prácticas y controles necesarios para la mitigación de los riesgos ligados al teletrabajo nos damos cuenta de que muchos de ellos están asociados a soluciones de Gestión de Identidades y Accesos (IAM), Gobierno de la Identidad (IGA), Control de Accesos y Gestión de Cuentas Privilegiadas (PAM).

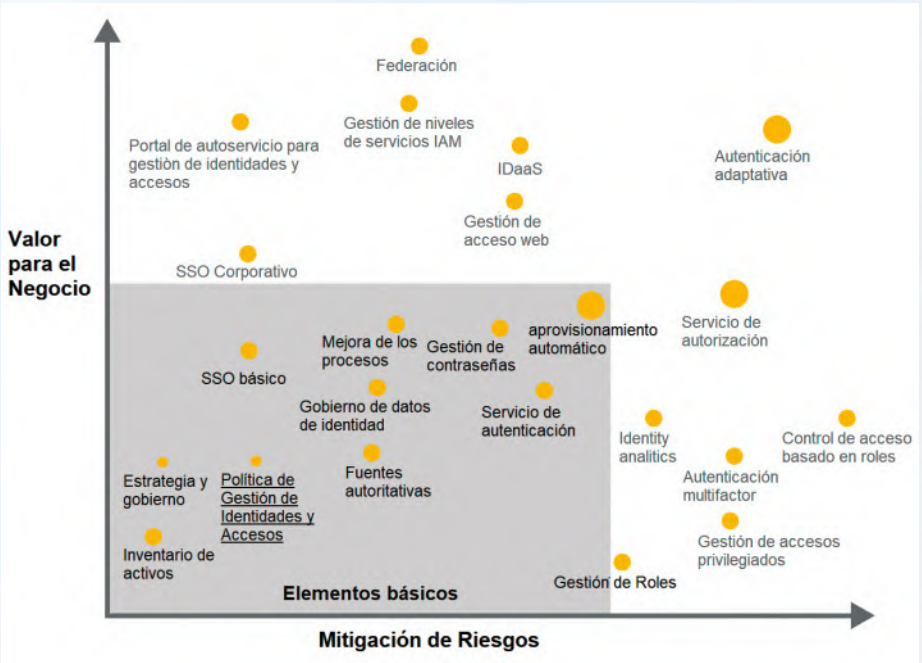


Figura 1.- Elementos básicos.

Criptológico Nacional (específicamente el CCN-CERT) ha publicado un documento que lleva por título "Medidas de seguridad para Acceso Remoto".

La implantación de medidas para controlar el acceso remoto podría no ser opcional, ya que son requisito en regulaciones como por ejemplo SOX, GDPR o ENS.

Si analizamos las recomendaciones, buenas prácticas y controles necesarios para la mitigación de los riesgos ligados al teletrabajo nos damos cuenta de que muchos de ellos están asociados a soluciones de Gestión de Identidades y Accesos (IAM), Gobierno de la Identidad (IGA), Control de Accesos y Gestión de Cuentas Privilegiadas (PAM).

En la **Figura 1** se muestran los elementos que EY ha incluido dentro de su ecosistema NextGen IAM. Se podría escribir un libro sobre la relación de cada uno de estos elementos y el teletrabajo. A continuación se desarrollan los siguientes.

Control de accesos

En lo que se refiere al **control de acceso en el teletrabajo, lo que se busca es validar la identidad del usuario y aplicar políticas de acceso basado en la criticidad de los sistemas a los que se conecta** o bien basado en el riesgo que supone desde dónde, cómo y cuándo se está estableciendo la conexión.

En mi opinión, es en los mecanismos de autenticación de usuarios donde **se observan los avances más significativos o que más repercusión pueden tener sobre los usuarios finales.** Hace ya mucho tiempo quedó en evidencia que sólo el uso de usuario y contraseña no es un método suficientemente seguro de autenticación, por lo que empezamos a utilizar un segundo o tercer factor (MFA), como podrían ser contraseñas de un sólo uso (OTP) provistas a través de medios alternativos como teléfonos móviles (SMS o llamada) o *tokens* (físicos, apps, etc.); otro factor muy expandido en estos tiempos, gracias a las funcionalidades de los *smartphones*, es el uso de la biometría. Factores más avanzados de autenticación se basan en el análisis de la información aportada por los dispositivos desde donde se establece la conexión; por ejemplo, desde hace algún tiempo hay herramientas que analizan la manera en que los usuarios interactúan con el teclado como un factor adicional.

Finalmente, estamos viviendo un cambio de paradigma, y todo indica que en un futuro cercano no tendremos que memorizar contraseñas para acceder de forma remota o presencial a los sistemas corporativos. Como era de esperar, ante un cambio como este existen miles de opiniones a favor y en contra, pero algo que está claro es que los fabricantes de soluciones de control de acceso están trabajando en este sentido.

Gestión del uso de cuentas de accesos privilegiadas de manera remota

Si bien es cierto que el uso de cuentas con accesos privilegiados (por ejemplo: administradores de sistemas u otros usuarios con permisos para tratar información sensible o procesos críticos del negocio) siempre se ha tenido que controlar con medidas especiales, **el uso continuado de este tipo de accesos fuera de un entorno físico controlado supone aún más riesgo.**

Figura 2

Si bien es cierto que el uso de cuentas con accesos privilegiados (por ejemplo: administradores de sistemas u otros usuarios con permisos para tratar información sensible o procesos críticos del negocio) siempre se ha tenido que controlar con medidas especiales, el uso continuado de este tipo de accesos fuera de un entorno físico controlado supone aún más riesgo.

Sin entrar en detalle de todas las funcionalidades de una herramienta PAM (permisos de acceso granulados, control de acceso basado en roles, MFA, monitorización/grabación de sesiones, gestión de cuenta compartidas, rotado de contraseñas, cifrado de sesiones, etc.), destacan dos funcionalidades fundamentales para el teletrabajo: por un lado, **la protección que aportan estas soluciones ante amenazas tipo *ramsomware*,** al no permitir que se establezcan sesiones directamente con el dispositivo que está siendo gestionado de forma remota; y por otro, **la posibilidad de implementar flujos de aprovisionamiento dinámico,** que permitirían a un usuario la ejecución de acciones específicas sólo cuando sea necesario.

Gestión y gobierno de la identidad

Con el uso masivo del teletrabajo hay que **analizar si son suficientes las políticas, procedimientos, y mecanismos de alta, baja, modificación y certificación de los accesos de los usuarios**, dando por hecho que son correctos para el trabajo presencial. Por ejemplo, deberíamos hacernos las siguientes preguntas: **¿los riesgos asociados al acceso a unos datos críticos para el negocio son los mismos si se realiza desde la red corporativa o se accede de forma remota?** ¿La definición de roles y la matriz de segregación de funciones de mi organización se ve afectada si tomamos en cuenta que los accesos se pueden hacer de forma remota? ¿Las campañas de recertificación deberían llevarse a cabo más a menudo si los accesos se realizan de forma remota?

Es en este punto es donde **la integración entre las herramientas de control de acceso y las de gestión de identidades nos permite implementar medidas más exhaustivas para controlar las actuaciones sobre los datos y sistemas de información**. Las herramientas IAM de última generación permiten definir niveles de riesgos para los accesos, usuarios o roles. Y mediante una correcta integración con las herramientas de autenticación se podrían requerir mecanis-

mos adicionales dependiendo de las acciones que se quieran realizar y desde dónde, cómo y cuándo se está realizando la conexión. Lo mismo aplica si integramos la herramienta de control de acceso remoto con herramientas DLP o IRM.

Monitorización y respuesta

La monitorización y respuesta a incidentes de seguridad es fundamental cuando se masifica el uso del teletrabajo en una organización; adicionalmente a todos los eventos que están siendo evaluados por los mecanismos de vigilancia, se debe prestar especial atención a la **integración de las herramientas que forman parte del ecosistema IAM y a la correlación con los registros generados por los dispositivos de red, aplicaciones, sistemas operativos**, etc. Las herramientas de IAM/PAM de última generación cuentan con módulos de **análisis de comportamiento de usuarios que buscan patrones y correlacionan eventos a nivel global para generar alarmas que permitirían tomar acciones antes que se materialicen las amenazas**.

Actualmente, la mayoría de las herramientas IAM/PAM están disponibles en entornos Cloud y desde EY las ofrecemos como un servicio gestionado (IDaaS), compatible con el entorno tecnológico que tenga la organización (Cloud, on-premise o híbridas).

Aunque los fabricantes de soluciones IAM/PAM aseguran que prestar este tipo de servicios desde la nube es totalmente seguro, el mercado local aún se resiste, no así el mercado norteamericano, donde se conocen casos de éxito en empresas que se han atrevido a dar el paso.

Todas estas soluciones forman parte de **NextGen IAM, un ecosistema de referencia desarrollado por EY, que combina personas, procesos, datos y tecnología orientados a la mitigación de riesgos, al mismo tiempo que aporta eficiencia y reduce los costos asociados a la gestión de usuarios, sus identidades, atributos y credenciales**.

Figura 3

Conviene realizar un análisis del estado en el que se encuentra la organización, definir cuál es la situación ideal que debería alcanzar en el ámbito del teletrabajo y, tras una evaluación de los recursos tecnológicos y humanos con los que se cuenta, establecer una estrategia y un plan detallado eficiente que esté alineado con los objetivos del negocio.

Conclusiones

Hoy en día las recomendaciones son claras, disponemos de cientos de nuevas tecnologías con la capacidad para proporcionar un acceso remoto seguro para que las organizaciones puedan operar con sus trabajadores (empleados o contratados) de manera no presencial. Pero **las nuevas tecnologías por sí solas no son suficientes para alcanzar los niveles de seguridad necesarios para mitigar los riesgos que supone esta transformación que ha llegado de forma abrupta y para quedarse**.

Entonces, ¿qué pueden hacer las empresas para aprovechar al máximo las soluciones tecnológicas y hacer un uso eficiente de los recursos? Una de las respuestas podría ser, **realizar un análisis del estado en el que se encuentra la organización, definir cuál es la situación ideal que la organización debería alcanzar en el ámbito del teletrabajo y tras una evaluación de los recursos tecnológicos y humanos con los que se cuenta, establecer una estrategia y plan detallado eficiente que esté alineado con los objetivos del negocio**, cuya columna vertebral sea una política sólida de acceso remoto y que no esté basado únicamente en el despliegue de soluciones tecnológicas. La correcta implantación de un programa de gestión de identidades y accesos supone una transformación tecnológica crítica para el negocio, cuyos factores esenciales se pueden observar en la **Figura 3**.

En EY no sólo contamos con la experiencia y las capacidades necesarias para la definición de la estrategia, el desarrollo de procedimientos y el despliegue de herramientas tecnológicas para la transformación o implantación de un acceso remoto seguro para el teletrabajo; también **contamos con un equipo multidisciplinar para acompañar a las organizaciones en la evolución hacia una cultura de *Smart Working***. ■

Nelson Sánchez Vera
MED & Spain IAM Services Leader
Cybersecurity Services
nelson.sanchez.vera@es.ey.com
EY

risk4all

Ante un entorno creciente para gobernar, **evaluar riesgos y demostrar el cumplimiento de normativas y estándares,** se hace cada vez más necesario el uso de herramientas que permitan aprovechar sinergias y ahorren tiempo y recursos.

Risk4All es un software creado por y para profesionales de la seguridad de la información y privacidad, **que automatiza y unifica la gestión y las tareas de cumplimiento de normas de privacidad y seguridad desde un enfoque de gestión de riesgo y continuidad de negocio.**

Alineada con las mejores guías, estándares o regulaciones como **RGPD, LOPD-GDD, ISO 31000, ISO/IEC 27001, ISO 27701 o ENS.** Permite incorporar otras normas y catálogos para evaluar su cumplimiento y analizar el riesgo de los activos y las organizaciones, así como otras muchas funcionalidades.

Conviértete en **partner**

Solicita una **demo** en **info@risk4all.com**

www.risk4all.es

El reto del Coronavirus a la tecnología: el Acceso Remoto Seguro

En medio de todos los retos humanos, políticos, económicos, sociales y tecnológicos que la situación actual está deparando, la seguridad informática se antoja como la pieza clave para poder engranar todos los elementos de la forma correcta. Este enfoque es la visión propugnada por Citrix, compañía de la que su director regional para Iberia, desgrana en las siguientes líneas la necesidad de disponer de soluciones de Acceso Remoto Seguro para poder adaptarse y obtener los beneficios ofrecidos por el nuevo paradigma, sin sacrificar la usabilidad, la productividad y la experiencia de usuario.

Santiago Campuzano

Quizás sonará a tópico decir que un virus cambió el escenario tecnológico del entorno laboral que conocíamos. Sin embargo, no era un virus informático, en diciembre del año 2019 un nuevo virus con origen en China ha bloqueado el mundo tal y como lo conocíamos. Siendo el correcto uso de la tecnología, quizás, la mejor medida preventiva para nuestra salud y para nuestra economía.

Cuando en el mes de marzo se decretó el Estado de Alarma y el Gobierno de España imponía el confinamiento nos enfrentamos a la realidad: durante los próximos meses sería obligatorio teletrabajar para todos los puestos de las organizaciones que estuvieran capacitados para ello. Desde ese momento las compañías tuvieron dos prioridades resumidas en una: la continuidad de negocio en un entorno seguro, o lo que es lo mismo, cómo permitir que la gente pudiera trabajar desde casa cumpliendo la legislación vigente desde el punto de vista de gestión de los datos y minimizando el riesgo desde el punto de vista de seguridad. He aquí un nuevo dilema, otrora minusvalorado o, al menos, no considerado prioritario: ¿Cómo ofrecer la alternativa adecuada de Acceso Remoto Seguro en tiempo record y de uso general dentro de las organizaciones?

Ya con anticipación CCN-CERT había lanzado su guía de teletrabajo el día 13 de marzo. Un día antes de la declaración del Estado de Alarma. El objetivo era que las administraciones públicas tuvieran una guía de cómo abordar el teletrabajo, en cualquier organización pero especialmente en los organismos públicos. Una de las alternativas consistía en "desplegar una solución de servicio en la nube como la ofrecida por 'Citrix Cloud' en modalidad de pago por uso". Evidentemente, la situación adecuada para cada caso iba a depender del escenario inicial y de los objetivos que se querían conseguir.

En los siguientes días fue necesario definir la solución para las organizaciones, tanto públicas como privadas, cómo abordar los distintos retos a los que se enfrentaban. Y, lógicamente, las soluciones de cada caso dependían de la situación inicial de cada uno. Cuestiones como, ¿qué dispositivos están al alcance de los usuarios, portátiles, de sobremesa o personales? ¿qué soluciones de virtualización de aplicaciones o escritorios disponemos? ¿cuál es el acceso estándar de redes privadas virtuales tenemos? ¿a qué tipo de aplicaciones hay que ofrecer acceso? ¿qué infraestructura tenemos? ¿cuál es nuestra capacidad de desbordamiento en la nube? Y debemos ser conscientes del plazo en el que esto ocurrió; desde el día 10 hasta el final del mes de marzo las compañías cambiaron radicalmente sus prioridades y objetivos, se produjeron compras por procedimientos de urgencia, se asignaron presupuestos extraordinarios y se implementaron modelos de Acceso Remoto Seguro en tiempo record. Lo que hemos vivido ha sido equivalente a montar en el mundo sanitario un hospital de campaña en tiempo record.

La realidad a la que nos enfrentamos es que muchas entidades –la mayoría de las grandes empresas y gran parte de la administración pública–, tenían ya soluciones de virtualización del puesto y/o de las aplicaciones, quizás limitando la capacidad de trabajar desde el exterior, pero ya estaban preparados; otras entidades contaban con soluciones de acceso remoto basadas en VPN, aunque limitados por el número de dispositivos portátiles corporativos; otras no tenían directamente la posibilidad de ofrecer acceso y debían buscar alternativas para que se pudiera trabajar de alguna forma desde los dispositivos corporativos. En decir, un escenario diferente para cada organización.

En definitiva, diferentes alternativas para distintos escenarios. Sin duda, la más segura, fácil y transparente para el trabajador se producía en compañías que ya habían empezado a trasformar el puesto de trabajo previamente, donde el acceso a aplicaciones y escritorios a través de un portal único ya estaba implementado. Dicho escenario ha sido muy usado en las entidades financieras, aseguradoras y en compañías energéticas.

Posiblemente uno de los casos más exitosos de movilizar de forma rápida y segura a los usuarios haya sido el del Grupo Comdata. La compañía, hace casi dos años, inició un proyecto a nivel mundial de transformación del puesto de trabajo virtualizando cientos de aplicaciones de diferentes tipologías y, en distinto grado, habían implementado el teletrabajo parcialmente aunque ahora el reto era hacerlo a nivel global y de forma inmediata. Como bien explica **José Luis García de los Ríos**, CIO del Grupo Comdata –uno de los principales call centers a nivel mundial–: "Nuestro proyecto de transformación del puesto se inició hace casi dos años y uno de sus objetivos, evidentemente, era la flexibilidad laboral. La solución, basada en la virtualización de aplicaciones y escritorios con Citrix, nos ha permitido garantizar la continuidad del negocio sin impacto y con seguridad. Además, la productividad tampoco se ha visto afectada ni hemos requerido grandes inversiones adicionales pues la experiencia digital del empleado se ha mantenido intacta independientemente del dispositivo que los empleados estuvieran utilizando desde sus hogares durante el confinamiento".

Otra alternativa bastante eficiente ha sido el uso de modelos híbridos, donde los usuarios con dispositivos móviles corporativos han accedido a través de soluciones VPN; mientras, los usuarios sin dispositivo corporativo han recibido acceso remoto a través de puestos o aplicaciones virtualizadas, manteniendo en muchos casos la experiencia digital del usuario intacta.

En cuanto a rapidez de reacción creo que hay dos ejemplos significativos. El primero es la utilización como alternativa a la virtualización del acceso a PCs remotos (Remote PC), la cual ha sido segura, eficiente y muy rápida. La solución se ha basado en acceder directamente a los PCs de las oficinas del mismo modo que si se accediera a un VDI en un *datacenter* o en la nube. Aquí el diferencial tecnológico ha venido por la gestión de la seguridad en el acceso y el protocolo de acceso ICA/HDX, que permite optimizar la experiencia del usuario. Hay que tener en cuenta que la alternativa para ofrecer algo equivalente con una VPN requería, en muchos casos, llevarse el PC de la oficina a casa del trabajador. El segundo es un proyecto en modo nube híbrida con un proveedor de servicios (Citrix Service Provider) para una entidad de sector público en el que se hizo el despliegue de 5.000 puestos integrando tecnologías en la nube con infraestructura *on premise* en menos de una semana desde cero; en un entorno donde la tecnología llevaba ya probada desde hacía meses pero donde ni siquiera estaban diseñadas las maquetas de los puestos que se tenían que desplegar.

Smartworking y teletrabajo

Evidentemente, es fácil de argumentar que somos la compañía que más tiempo lleva hablando de *smartworking* y teletrabajo en España o que nuestra base instalada y nuestra experiencia son factores diferenciales. Sin embargo, cuando movilizas cerca de 500.000 personas de medianas y grandes empresas y de las principales entidades de sector público, los motivos también son tecnológicos. Centrándonos en la seguridad, todos los datos y aplicaciones permanecen dentro del perímetro digital de protección de las organizaciones, interactuando los usuarios con el espacio de trabajo a través del protocolo de presentación cifrado ICA/HDX. El mismo nos permite limitar la descarga de datos o comunicación entre unidades de almacenamiento locales y el espacio de trabajo. Además, Citrix permite limitar otras amenazas controlando las capturas de pantalla desde ese equipo de acceso o limitando que un *keylogger* pueda intentar capturar la información que escribamos en nuestro espacio de trabajo, facilitando que puedan usarse dispositivos personales de forma segura (*Bring Your Own Device* o con capacidades de instalación y uso personal).

Por otra parte, Citrix adopta la aproximación de seguridad "Zero Trust", con una monitorización continua de los riesgos y propuestas de mitigación tras el *login* inicial. Con este proceso se limitan las vulnerabilidades, permitiendo las conexiones remotas sin necesidad de las complejidades que representa una VPN, especialmente con dispositivos no controlados. También se contextualizan los accesos y se evita el denominado "Traffic back-hauling", que daña la experiencia de usuario. Esta seguridad no se ve menoscabada por el interés alrededor de la experiencia del usuario, ofreciendo un análisis inteligente sobre el comportamiento de los usuarios para obtener una protección proactiva (*User Behavior Analytics*). En definitiva, la visión está centrada completamente alrededor del usuario y su necesidad de tener que trabajar en un entorno seguro con una experiencia digital óptima.

Experiencia digital en entorno seguro y sin impacto para el usuario

Por supuesto, hay otras alternativas tecnológicas pero ninguna tan completa que permita mantener la experiencia digital del usuario en un entorno seguro y sin impacto para el usuario. Además, la flexibilidad del entorno y la rapidez para garantizar la continuidad de negocio eran factores críticos.

No debemos olvidar ese aspecto relevante que es la falta de una legislación que cubra las necesidades reales del teletrabajo y que se antoja más crítico que nunca.

Por último, la gran duda a la que se enfrentan las compañías ahora es si este nuevo concepto de movilidad, teletrabajo o *smartworking* ha llegado para quedarse. Recientemente desde Citrix realizamos una encuesta en distintos países de Europa sobre el impacto del teletrabajo con la crisis de la COVID-19; del mismo sacamos varias conclusiones relevantes, como que más del 70% de los encuestados pensaba que el teletrabajo sería una realidad desde ahora o que más del 60% pensaba que su capacidad productiva no estaba mejorando, lo cual se puede considerar normal puesto que el reto no es solo tecnológico sino también cultural y de liderazgo. Estamos en medio de la definición de un nuevo paradigma en la forma de trabajar de las empresas, donde a veces no apreciamos lo que no conocemos. Desde el punto de vista de las organizaciones los criterios de medición de la productividad cambiarán o los requerimientos en las infraestructuras físicas asociadas a las oficinas cambiarán. Desde el punto de vista de las personas, ahora se va a valorar más la conciliación laboral, aprovechar el tiempo y no perderlo en atascos, mejoras en la alimentación por comer en casa, etcétera. No debemos olvidar que otro de los aspectos relevantes es la falta de una legislación que cubra las necesidades reales del teletrabajo y que se antoja más crítico que nunca; ya está empezando a trabajar no solo en nuestro país sino también en otros países, considerados en algunos aspectos más avanzados, como Alemania.

Revolución Sociotecnológica

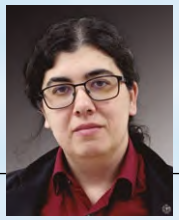
Desde hace siete u ocho años vengo utilizando el concepto de la 'Revolución Sociotecnológica' para explicar que la evolución tecnológica, que siendo una realidad, se unía a una serie de cambios sociales como eran las nuevas costumbres, la incorporación de nuevas generaciones al entorno laboral y un concepto muy pragmático, trabajamos como vivimos. Las personas estaban preparadas y las compañías e instituciones lo han hecho con eficiencia y rapidez. Es un clásico alrededor de la tecnología, especialmente en la era de la transformación digital, utilizar la frase de Charles Darwin en la que se explica que no sobrevive el más fuerte o el más inteligente, sino el que tiene más capacidad de adaptación al cambio. Creo que donde más sentido tiene utilizarse es, en concreto, alrededor del *workplace* ya que realmente es donde la tecnología se une al comportamiento humano.

Y en medio de todos estos retos humanos, políticos, económicos, sociales y tecnológicos, la seguridad informática se antoja como la pieza clave para poder engranar todos los elementos de la forma correcta. Más que nunca se requieren soluciones de Acceso Remoto Seguro para adaptarnos y obtener los beneficios ofrecidos por el nuevo paradigma, sin sacrificar la usabilidad, la productividad y la experiencia de usuario. ■

Santiago Campuzano
Director regional Iberia
CITRIX

Teletrabajo: diagnósticos de ciberseguridad según la tecnología utilizada

La autora muestra en este artículo las diferentes soluciones tecnológicas y las amenazas propias de cada una de ellas en un escenario donde el teletrabajo no ha sido una opción, sino una necesidad. Además –y como ella misma afirma–, "estamos en una situación donde debe tenerse en cuenta que la seguridad que rodea a los usuarios no es la misma que en condiciones normales: a las redes corporativas les estamos añadiendo los problemas de seguridad de las redes domésticas, que es donde están trabajando los usuarios en este momento".[1]



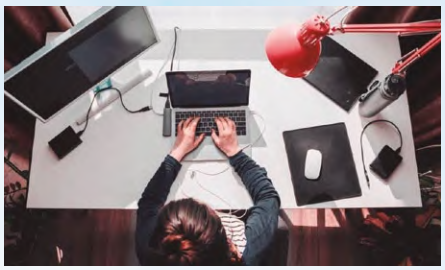
Paula González Muñoz

Uno de los grandes avances gracias a Internet consiste en la posibilidad que tenemos los distintos tipos de profesionales de trabajar de manera remota. Ya no es necesario estar físicamente presente en el lugar donde tenemos que desarrollar nuestra actividad para poder realizarla. No obstante, la incidencia del teletrabajo siempre ha sido bastante desigual entre países: si consultamos los datos de 2017 observamos que el teletrabajo en la Unión Europea sólo era utilizado de manera habitual por un 5% de los empleados (según fuentes de Eurostat)[2].

La llegada de la COVID-19 ha cambiado este panorama totalmente. Se ha pasado de un escenario en el que, en el mejor de los casos, el teletrabajo habitual llegaba a un 15% de los trabajadores por cuenta ajena a uno en el que, para todas las actividades que lo permitan, se ha pasado a un teletrabajo total. Este cambio de paradigma, junto con las circunstancias en las que se ha dado, presenta bastantes retos tanto desde el punto de vista puramente técnico como desde el punto de vista social. En este artículo nos centraremos en cómo afecta también a la seguridad de las organizaciones, ya que este nuevo escenario ha forzado a que, en la mayoría de los casos, se haya tenido que elegir entre continuidad y confidencialidad.

¿Qué entornos y esquemas hay?

Lo primero que hay que tener en cuenta al hablar de teletrabajo es que existen distintos esquemas que podemos utilizar para teletrabajar. Suponiendo que todos nuestros empleados dispongan de equipos corporativos, podemos proporcionarles acceso a nuestra red de manera que puedan trabajar desde cualquier lugar con el mismo tipo de acceso que si estuvieran físicamente en la oficina de la organización mediante VPN. Si, por el contrario, existen empleados que no tienen estos equipos se pueden utilizar dos



esquemas distintos: escritorios virtuales (VDI) o estrategias orientadas a la gestión de dispositivos mediante la creación de espacios virtuales dentro de un mismo dispositivo (MaM).

Aparte de los tipos de soluciones mencionados, también podemos distinguir entre dos situaciones que han influido en las implantaciones del teletrabajo dentro de la situación actual. Por un lado, tenemos a aquellas organizaciones donde, por diversos motivos, el teletrabajo continuado no estaba contemplado como parte de sus procedimientos. Este tipo de organizaciones han tenido que hacer un especial esfuerzo para desplegar la solución que hayan seleccionado como óptima para su plantilla, así como para facilitarles el acceso a aquellos recursos que necesitan para desarrollar su día a día. Por contra, aquellas organizaciones que ya tenían a una parte de su plantilla teletrabajando de manera habitual, su principal esfuerzo se ha centrado en aumentar la capacidad de sistemas ya existentes.

En ambos casos, e independientemente de la tecnología, la necesidad de garantizar la continuidad de la actividad puede haber supuesto fallos en la implantación de los nuevos sistemas, además de un incremento de la superficie y la información expuesta más allá de las dependencias físicas de la organización. Es por ello que resulta especialmente interesante tener en cuenta las amenazas para cada uno de los esquemas.

VPN

La primera solución técnica que nos viene a la mente al hablar de teletrabajo se trata de la implantación de Redes Privadas Virtuales (VPN). Las VPN son conexiones que utilizan redes públicas, como internet, para conectar usuarios remotos como si de redes punto a punto se tratase. Por norma general, este tipo de soluciones tienen tres amenazas fundamentales: debilidades en el cifrado, que se puedan utilizar para ataques de tipo Man in the Middle, debilidades en el control de acceso a la VPN y el riesgo de que un equipo de usuario infectado por *malware* pueda infectar a toda la red al conectarse.

El uso de diagnósticos de ciberseguridad puede permitirnos analizar si la red VPN de nuestra organización es vulnerable a cualquiera de estas amenazas. Mediante distintos tipos de pruebas sobre el cifrado podemos comprobar su robustez. Para el control de acceso se deben comprobar principalmente la seguridad en el *login* así como la correcta utilización de los dobles factores de autenticación. Finalmente, el riesgo de que una amenaza puntual se extienda por toda la red debe basarse en la validación de la segmentación de la red, así como en la de las medidas de protección de los *endpoint* ya que, recordemos, estos esquemas deberían utilizarse cuando todos los empleados disponen de equipos corporativos.

VDIs

Para aquellas organizaciones cuya estrategia se basa en el uso de escritorios virtuales (VDIs), parte de la problemática es común a la de las VPNs pero también tiene peculiaridades propias. Este tipo de soluciones son utilizadas normalmente en dos posibles escenarios. El primero de ellos es aquel en que los empleados no tienen un equipo corporativo propio. El otro escenario habitual es aquel en el

[1] https://threatpost.com/enterprise-security-woes-explode-home-networks/155280/
[2] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20180620-1

que los equipos corporativos no pueden ejecutar programas necesarios para la actividad de la organización, generalmente por problemas de compatibilidad, licenciamiento o potencia. En cualquiera de las opciones, cuando el usuario ingresa en el VDI, puede ejecutar las aplicaciones corporativas y trabajar como si físicamente estuviera en su organización.

De nuevo, la primera de las amenazas a tener en cuenta es la exposición a Internet del acceso a la plataforma: puertos expuestos innecesariamente y debilidades en el control de acceso son dos puntos de entrada típicos para un atacante. En caso de que se consiguiera acceder al VDI, se suele limitar el tipo de operaciones que se pueden realizar, así como la visibilidad de red que tienen estos sistemas.

Los primeros pasos para una intrusión a través de un VDI suelen ser tanto ejecutar la línea de comandos como subir algún tipo de fichero malicioso al mismo. Si el VDI tiene bien configuradas las restricciones este tipo de acciones no serán posibles. Por último, si el objetivo del atacante no es controlar el VDI sino exfiltrar información, se debe de comprobar que no es posible descargar ningún tipo de archivo desde la plataforma y que se han tomado las medidas pertinentes para evitar que se obtenga utilizando medios tales como el correo electrónico.

Los VDI son una herramienta muy potente para el teletrabajo pero requieren una especial atención al detalle en su configuración para tener en cuenta todos los casos anteriormente expuestos. Por ello, la realización de diagnósticos que aseguren que las restricciones del VDI están correctamente configuradas resulta muy interesante. También es importante validar que las medidas de control de acceso son las adecuadas.

Finalmente, siempre se debe validar que al implantar este tipo de sistemas no se han expuesto otros al exterior: un atacante siempre preferirá acceder, por ejemplo, a las consolas de administración de los sistemas a tener que realizar una intrusión a través de un VDI.

MaM

La última de las tecnologías a tratar en este artículo es en la que se basan las soluciones de gestión de aplicaciones móviles (MaM por sus siglas en inglés). Este tipo de soluciones permite a aquellas organizaciones donde sus empleados no tienen equipos corporativos, bien por la situación actual bien porque se haya optado por una política "bring your own device" (BYOD), gestionar la seguridad de los datos corporativos a nivel de aplicación. Imaginemos un usuario en una organización con política BYOD: el empleado tiene que trabajar desde su propio dispositivo mientras que la organización tiene que ser capaz de garantizar tanto la privacidad del usuario como la seguridad de su información corporativa. Es en este tipo de esquemas dónde el MaM es una solución muy interesante.

Las soluciones MaM permiten la creación de dos espacios de datos dentro de un mismo dispositivo físico. Por un lado, toda la información que pertenece al usuario y, por otro, la de las aplicaciones corporativas que pertenecen a la organización. De esta forma es posible gestionar la seguridad de los datos corporativos a nivel de aplicación sin impactar a los datos personales que haya en el mismo dispositivo. No obstante, y de manera parecida a como ocurre con los VDI, una correcta implantación de un MaM requiere una configuración muy detallada para evitar que un atacante pueda realizar acciones no permitidas.

En el caso de las soluciones MaM, el principal riesgo reside en el uso de aplicaciones corporativas en dispositivos no corporativos que pueden contener cualquier tipo de *malware*. Por tanto, es crítico que se garantice tanto que no se puede exfiltrar información confidencial como que no es posible que un *malware* de un dispositivo personal se expanda a otros usuarios de la organización. El tipo de diagnóstico para poder validar que el MaM cumple con estas características es especialmente sofisticado, aunque crítico, ya que en este escenario se debe garantizar el aislamiento entre la capa personal y la corporativa.

A lo largo de este artículo se han mostrado diferentes soluciones tecnológicas y las amenazas propias de cada una de ellas en un escenario donde el teletrabajo no ha sido una opción, sino una necesidad. Además, estamos en una situación donde debe tenerse en cuenta que la seguridad que rodea a los usuarios no es la misma que en condiciones normales: a las redes corporativas les estamos añadiendo los problemas de seguridad de las redes domésticas, que es donde están trabajando los usuarios en este momento (https://threatpost.com/enterprise-security-woes-explode-home-networks/155280/).

Si todos los empleados disponen de equipos corporativos, se les puede proporcionar acceso a la red para que puedan trabajar desde cualquier lugar con el mismo tipo de acceso que si estuvieran físicamente en la oficina de la organización mediante VPN. Si existen empleados que no tienen estos equipos se pueden utilizar dos esquemas distintos: escritorios virtuales (VDI) o estrategias orientadas a la gestión de dispositivos mediante la creación de espacios virtuales dentro de un mismo dispositivo (MaM).

Esta realidad hace que sea de especial importancia comprobar que, independientemente de la tecnología utilizada para habilitar el teletrabajo, las medidas de seguridad implantadas funcionan correctamente y que todas las restricciones para el acceso a la información sensible son robustas. Debe tenerse en cuenta que, en esta situación, se debe validar la seguridad en ambas direcciones, ya que todas las organizaciones han tenido que aumentar su exposición para asegurar que su actividad no se vea impactada. En este aspecto, e independientemente de su nivel de madurez en ciberseguridad, todas las organizaciones deben establecer un plan de diagnósticos que asegure que las distintas medidas que han tomado funcionan correctamente. ■

Paula González Muñoz
Jefa de sección de Auditoría
GMV

Teletrabajo: por dónde crecen las amenazas

Ante la más que previsible instauración del teletrabajo como una modalidad laboral de carácter estructural y permanente, las organizaciones deberán adaptar su sistema de ciberseguridad a estos entornos, en tanto que a los empleados "se les exigirá un uso más responsable de sus medios digitales al quedar potencialmente más expuestos a los riesgos y amenazas habituales", porque el cibercrimen y los actores hostiles habituales buscarán ahora maneras concretas de rentabilizar las vulnerabilidades potenciales y brechas de seguridad que, en el sistema corporativo y en cada usuario en particular, se puedan derivar del recurso al teletrabajo.

Mariano Ortiz / Alejandro González

El teletrabajo, como modalidad laboral generalizada y de aplicación consolidada en el tiempo, parece haber llegado con (o verse impuesto por) la pandemia del coronavirus. Con independencia de cómo evolucione esta pandemia y más allá de que se encuentren vacunas y medicamentos que permitan superarla, sí que parece claro que a partir de ahora el teletrabajo se va a incluir como modalidad laboral de empresas y organizaciones en un porcentaje superior a cómo venía haciéndose hasta ahora, aquellas que no lo utilizaban comenzarán a hacerlo y las que sí lo hacían intensificarán su uso. Un paso más en la Transformación Digital de la economía y de los mercados.

Todo apunta a que el teletrabajo podrá implantarse más en aquellos sectores con alto valor añadido y elevado componente tecnológico, entre una población laboral que cuente con una alta cualificación profesional, ámbitos todos ellos que tradicionalmente han de ser objeto de una especial vigilancia y protección en el ámbito digital. El teletrabajo puede contribuir a acelerar la competitividad de las empresas, pero por el camino no puede dejar de lado la seguridad.

El factor humano

Hay que volver a insistir sobre el componente personal que la ciberseguridad tiene, más allá de la seguridad con la que se dotan dispositivos, sistemas y redes. El teletrabajador está "solo", los soportes de mantenimiento, IT y seguridad de su organización seguirán funcionando y no dejarán de existir, pero pueden ser percibidos de una manera lejana, difusa o casi virtual. En estos entornos, la concienciación, formación y disciplina del "teletrabajador" seguirán conformándose como auténticos primeros escalones de ciberseguridad de las organizaciones. De nuevo el factor humano.

Trabajar de manera continuada desde casa, en un entorno en el que casi conviven ocio y negocio puede provocar una relajación en el uso de las reglas de seguridad a medida que la situación se prolongue en el tiempo. También puede producir descoordinaciones internas en la organización o dar nuevas oportunidades a actores del tipo *Insider Threat*.

Trabajar de manera continuada desde casa, en un entorno en el que casi conviven ocio y negocio puede provocar una relajación en el uso de las reglas de seguridad a medida que la situación se prolongue en el tiempo. También puede producir descoordinaciones internas en la organización o dar nuevas oportunidades a actores del tipo Insider Threat.

Por otro lado, la forzosa necesidad de teletrabajo ha puesto de manifiesto entre otras cosas, que los mecanismos de mitigación (salvaguardas y controles de seguridad) existentes, pueden y deben mejorarse, con el objetivo de reducir al máximo la ciberexposición de la compañía en todo su conjunto, otorgando una mayor sensación de control y seguridad.

Cuando hablamos de los principales actores de las ciberamenazas, tales como ciberatacantes aislados, mafias, o incluso estados, olvidamos que dentro del abanico de las amenazas y riesgos de ciberseguridad existe el factor de intencionalidad, y es sabido que en muchos casos el factor humano es el origen (intencionado o no), de la creación de una vulnerabilidad, que puede estar presente en el activo tangible como, por ejemplo, a través de una mala configuración o en el intangible, con la exposición de información.

Por todo ello es recomendable que frente al aumento del teletrabajo y con vistas a futuro, exista un equilibrio entre la usabilidad de las aplicaciones, la estabilidad de los entornos de trabajo e infraestructuras tecnológicas, y la seguridad de los activos y usuarios, estando presente dentro de los procesos de gobernabilidad, cumplimiento normativo, políticas, estrategia y conciencia de la ciberseguridad corporativa, y respaldado por la dirección desde el inicio.

Amenazas

Desde el ámbito de la Ciberinteligencia y Riesgos Digitales se aprecia que algunos riesgos y amenazas pueden ser más susceptibles de producirse al poder aprovechar los actores hostiles que sus objetivos están funcionando en modalidad de teletrabajo. Analicemos las amenazas que probablemente se verán también potenciadas por el muy previsible complicado escenario económico que se generará a raíz de la pandemia:

• **Fraude del CEO y otras formas de fraude**. Pueden producirse nuevas oportunidades de explotación de las tradicionales brechas de seguridad que son el origen del fraude. Al trabajar en remoto distintos elementos de una misma organización, la descoordinación entre ellos, el retraso en sus comunicaciones o una mala verificación entre sí a la hora de confirmar operaciones financieras y transferencias, puede propiciar una mayor tasa de éxito para los defraudadores que en circunstancias de funcionamiento normales, en las que la modalidad de trabajo presencial proporciona una mayor agilidad y seguridad en la comunicación. En caso de duda es conveniente revisar (y actualizar a la realidad del teletrabajo si ello fuera necesario), para asegurar, los protocolos existentes con los que operan

las organizaciones y ejecutan sus pagos y transferencias.

• ***Insider Threat***. Cabe esperar un incremento de este tipo de amenaza, tanto en su modalidad consciente como inconsciente. Para el inconsciente porque el teletrabajo implicará una relajación en el empleo de sus medios digitales, que se agudizará por la no proximidad de soportes IT cercanos que tendrán que apoyarle en remoto en caso de dudas o de tener que reparar o mantener sus equipos. Todo ello se traducirá en brechas de seguridad. En el caso del consciente habrá que prestar especial atención a todas las medidas contempladas en el Plan de Insiders con que cuente la organización y comprobar que los accesos en remoto a datos, archivos, cuentas y aplicaciones que los teletrabajadores llevan a cabo están justificados y tienen sentido.

• **Exposición Digital de Directivos y Personal Crítico de las compañías**. el teletrabajo continuado, más aún durante unas circunstancias emocionalmente duras y excepcionales como las que estamos viviendo, se traducen en incremento de comunicaciones y uso masivo de Redes Sociales y en una posible relajación del rigor y de la seguridad con las que habitualmente hay que actuar. Los actores hostiles que en circunstancias normales recopilan informaciones de tipo personal y personal / corporativo con las que montar posteriormente sus ataques, pueden tener ahora un acceso a datos que desconocían o confirmar / complementar otras informaciones que conocen de forma parcial.

• **Campañas de *phishing* y *spear phishing***: aprovechan la situación de incertidumbre y la multitud de fuentes de información disponibles para inundar a usuarios y clientes finales con noticias falsas relacionadas con la pandemia, utilizando las redes sociales, aplicaciones de mensajería instantánea y el envío de *emails* con información acerca de medidas preventivas, recaudación de fondos para la lucha contra el virus o solicitudes de ayuda de cualquier tipo, con el objetivo de robo de credenciales y fraude.

• **Reconocimiento y modelado de ciberataques**, que si bien podríamos decir que no se trata estrictamente de una ciberamenaza como tal, sino más bien una fase dentro de una metodología de intrusión estándar, sí que se debe tener en cuenta, ya que puede suponer que con motivo del teletrabajo expongamos cierta información referente a la organización, información como versiones de software de aplicaciones, tipos de arquitectura tecnológica desplegada, rangos de IP utilizados, nombres DNS registrados, tipos de accesos remotos para empleados, fabricantes de tecnología utilizados, etcétera, y que sirva a los ciberatacantes para recopilar información acerca de la organización.

• **Aplicaciones móviles fraudulentas**, que fingen un aparente seguimiento de los casos detectados, e incluso la falsa posibilidad de rastrear infectados, y que están dirigidas principalmente al robo de información.

Tras la pandemia del coronavirus empresas y organizaciones van a entender el teletrabajo como una modalidad laboral de carácter estructural y permanente más que como una forma coyuntural y limitada de que sus empleados puedan conciliar vida laboral y personal / familiar. Además, el teletrabajo podrá hacer más competitivas y eficientes las organizaciones e incrementará su componente digital.

La ciberseguridad deberá adaptar su diseño y reforzarse a esa realidad del teletrabajo porque ninguna empresa será capaz de mantenerlo sacrificando su seguridad y, por tanto, su supervivencia como negocio. Además, los teletrabajadores deberán adaptarse también a un ámbito laboral que será más descentralizado y disperso, que les dotará con mayor autonomía, pero que les exigirá un uso más responsable de sus medios digitales al quedar potencialmente más expuestos a los riesgos y amenazas habituales. ■

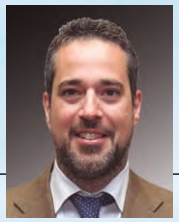
Cabría esperar un incremento de amenazas tipo Insider Threat, tanto en su modalidad consciente como inconsciente. En el caso de la inconsciente, porque el teletrabajo implicará una relajación en el empleo de sus medios digitales, que se agudizará por la no proximidad de soportes IT cercanos, que tendrán que apoyarle en remoto en caso de dudas o de tener que reparar o mantener sus equipos. Todo ello se traducirá en brechas de seguridad.

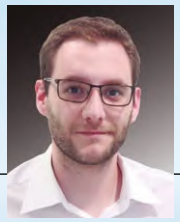
Ante el teletrabajo, es recomendable que exista un equilibrio entre la usabilidad de las aplicaciones, la estabilidad de los entornos de trabajo e infraestructuras tecnológicas, y la seguridad de los activos y usuarios, estando presente dentro de los procesos de gobernabilidad, cumplimiento normativo, políticas, estrategia y conciencia de la ciberseguridad corporativa, y respaldado por la dirección desde el inicio.

Mariano Ortiz
Global Digital Risk Director
Alejandro González
Cybersecurity Manager
TARLOGIC

¿'Mascarillas virtuales' para el acceso remoto y el teletrabajo?

En estos momentos de pandemia y COVID-19, ha sido necesario acelerar la famosa transformación digital que estaba en boca de todas las compañías y de la sociedad, pero por lo que se ha demostrado en la mayoría de casos, poco se estaba preparado. La forzosa transición al teletrabajo de la mayoría de negocios, ha acarreado una fuerte carga de datos a las redes corporativas, concentradores VPN y demás componentes de la electrónica de red, por lo que se han tenido que realizar cambios con la máxima celeridad, así como despliegues a toda prisa. Dentro de estos cambios, se ha tenido que usar herramientas cloud, conexiones remotas y software de chat y videoconferencia. Por esta inminente necesidad, que ha pillado a muchos por sorpresa, se han dejado de tener en cuenta aspectos muy importantes de la ciberseguridad tales como las actualizaciones de la política de seguridad, la concienciación a los usuarios sobre el teletrabajo y los accesos remotos, o aún peor, con las prisas se han obviado activar medidas para proteger a los empleados y a su trabajo, ante el ataque del creciente cibercrimen. En definitiva, no nos hemos puesto las mascarillas virtuales u otras medidas de ciberprofilaxis con la suficiente celeridad y de forma más seria.





Daniel Solís / Ramsés Pascual

¿Pero qué es lo que está pasando?

Dicho en otros términos, estos motivos han sido caldo de cultivo para que la industria del cibercrimen se haya frotado las manos y esté expandiendo su gran catálogo de *servicios* y, por ende, amenazas contra la ahora más extendida superficie de ataque.

El aumento del trabajo en remoto y por tanto de la ampliación de los puntos o vectores de ataque ha traído consigo la proliferación de las siguientes amenazas:

- Incremento de ataques contra las compañías, siendo el *phishing* el más usado por su efectividad y sencillez.
- Mercadeo de credenciales de servicios de videoconferencia, accesos remotos y/o otros servicios expuestos, vinculados al teletrabajo.
- Fuerte subida del espionaje y del robo de información confidencial o sensible.
- Comercialización de *exploits* y/o *phishing kits* que afecten a cualquiera de los software o aspectos anteriormente mencionados.

Siendo Blueliv los ojos de las compañías en Internet, el *dark* y *deep* web, así como su experiencia en entender el cibercrimen, seguidamente se desarrollan los anteriores puntos con los datos obtenidos en los últimos meses durante la pandemia.

Incremento de ataques: *phishing*

Aunque parezca mentira, el *phishing* sigue siendo el vector de engaño –y en consecuencia de distribución de *malware*– que mejor sigue funcionando mediante campañas masivas. Resulta evidente que los chicos malos hayan adaptado los mensajes maliciosos sobre noticias vinculadas a COVID-19, curas y material médico. La cantidad de *phishing* con contenidos sobre el coronavirus o el confinamiento han ido incrementando, a medida que los países han entrado en estado de alarma, ampliando de esta manera las posibilidades y objetivos que tiene el atacante. La industria del cibercrimen ha sabido seleccionar las distintas regiones que aplicaban medidas de confinamiento y que, por ello, debían incrementar las conexiones remotas a sus redes, así como desplazar a sus empleados a teletrabajar.

Todo ello con el objetivo de suplantar portales para robar credenciales o para infectar mediante archivos adjuntos a miles de usuarios, y así poder infectarles los equipos con *malware* tipo *ransomware* u otro uso de *malware* como RATs, o *credential grabbers* que puedan robar credenciales de acceso, sesiones de videoconferencia, etc.

Si a estas crecientes campañas les añadimos el hecho de que, a pesar de tenerse políticas de protección de los dispositivos, la mayoría de teletrabajadores no tienen grandes medidas de protección en sus hogares –a excepción de las que disponen propiamente sus portátiles corporativos– y, además, que la mayoría de tráfico que se dirige hacia plataformas *cloud* no siempre pasa por VPNs, cortafuegos y/o demás controles de contenidos corporativos, no es de extrañar que el éxito de este tipo de ataques haya sido muy alto.

Es curioso constatar cómo ha crecido la curva de correos de *phishing* en este periodo de pandemia. Mientras que en diciembre el virus era prácticamente una simple noticia en todo el mundo, en enero ya se vieron los primeros *phishing* relacionados, coincidiendo con su expansión alrededor del mundo. A partir de febrero, momento en el que China entra en estado de alarma, se detecta un incremento de un 600% del *phishing* relacionado con el evento mundial. Marzo marca la gran diferencia, es cuando la mayoría de países empiezan el confinamiento, y eso implica que muchos negocios empiezan a enviar a sus empleados a trabajar desde casa dentro de sus posibilidades. Durante este mes, se aprecia una subida de casi un 1000% del *phishing* del coronavirus respecto al mes anterior. Pero la culminación de este tipo de *phishing* llega en abril, cuando sube un 300% respecto a marzo. Y finalmente, en el momento de la redacción de este artículo (mediados de mayo), el *phishing* detectado durante este mes se estabiliza igualando los números de abril.

Mercadeo de credenciales

La situación global actual ha provocado que el coronavirus sea un tema recurrente, tanto por los medios de comunicación y las conversaciones en los grupos de WhatsApp como, por supuesto, los foros y *markets* de la *clearnet* y la *darknet*. La industria del cibercrimen ha crecido en los foros con actores que quieren vender sus hallazgos o resultado de sus hazañas, actores interesados que intentan conseguir accesos o credenciales u otros actores que intentan conseguir reputación en este mundillo compartiendo de forma gratuita parte de sus logros.[5]

Los *productos* que forman parte de esta compraventa, mayoritariamente, son las credenciales de servicios de accesos remoto y VPN, videoconferencia y mensajería

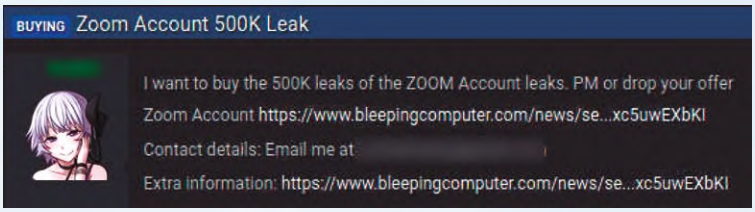


Fig. 1.- Criminal solicitando la compra de credenciales de Zoom.

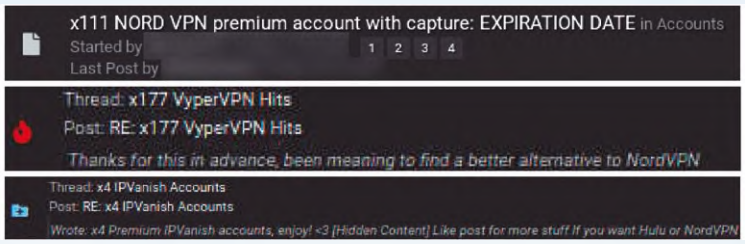


Fig. 2.- Venta de credenciales de accesos VPN.

,que se han empezado a utilizar de forma más extendida desde el confinamiento. A modo de ejemplo, se muestran dos grupos de estos *productos* del cibercrimen:

El primer grupo se basa en la extracción, ya sea por *phishing* o por *malware*, de las credenciales de servicios como Zoom, Discord, Skype, Microsoft Teams o Slack en su mayoría. Estas son difundidas por los cibercriminales en foros o expuestas en pequeñas cantidades para ganar reputación y para que sirvan de prueba de la calidad y veracidad de sus datos, para así vender grandes cantidades de credenciales robadas [1] o, por lo contrario, están interesados en comprar dichas credenciales, como se puede ver en la **Figura 1**.

En el segundo grupo, nos encontramos con los foros y *markets* que están llenos de actores que realizan compra-venta de credenciales y accesos a VPN, permitiendo accesos a redes internas de organizaciones. Por ejemplo, encontramos foros con hilos de tecnologías específicas como el que se muestra en la **Figura 2** para NordVPN, VyprVPN y IPVanish.

En este contexto desde Blueliv hemos detectado un incremento exponencial de las credenciales robadas de estos servicios desde marzo, momento clave del confinamiento, con casos mediáticos como el de Zoom. Las credenciales de estos servicios siempre han sido objetivo de muchos cibercriminales, pero especialmente en esta histórica situación, ha despertado el interés tanto de cuentas personales como profesionales. La **Figura 3** muestra un ejemplo del crecimiento de las detecciones de robo de credenciales de servicios de videoconferencia y mensajería.

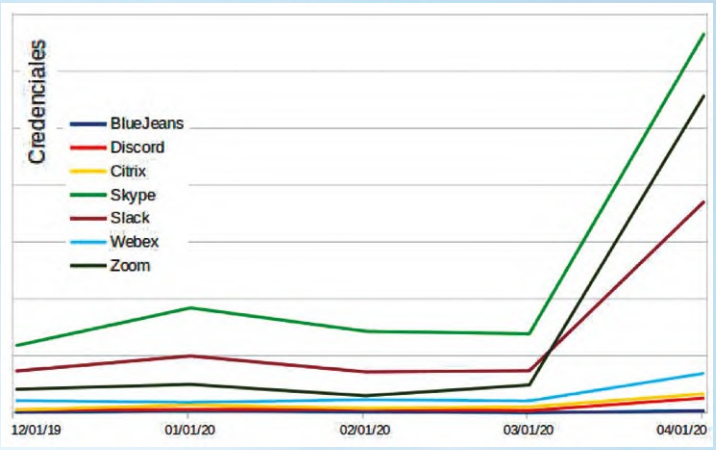


Fig. 3.- Incremento de credenciales de todas las plataformas desde el inicio de Covid-19.

Aumento del espionaje y del robo

Se han extendido los casos de robos de datos y extorsión sobre las compañías, como se puede ver en el incremento de víctimas en la página publicada por Maze [2], la de Clop de TA505 o la actividad detectada por otros grupos de cibercriminales como APT10, APT18 y APT41, Dridex o Trickbot, entre otros. Por otra parte, se han hecho públicos diversos ataques a grandes compañías, y se han visto atacantes interactuar en distintos foros y mercados de la *darknet* intentado conseguir herramientas –algunas de ellas vistas ya en campañas previas– para extorsionar económicamente o robar información.

Aprovechando la actual situación de vulnerabilidad de los sistemas informáticos de la mayoría de los teletrabajadores y la falta de adaptación de los sistemas y su seguridad, estos Threat Actors están realizando ataques dirigidos con *spear-phishing* a entidades y organizaciones, para luego cifrar documentos y descargar gigas de información, siendo utilizados como reclamo para la realización de un pago que, en caso de no producirse, dicha información y documentos se harían públicos.

En este caso, el sector *target* no ha influido en la decisión de los actores, dado que existen casos que han afectado tanto a hospitales como a organizaciones privadas internacionales [3]. Uno de los sectores que más llamó la atención a Blueliv, ha sido la industria farmacéutica [4], en dónde diferentes grupos de *Threat Actors*, algunos de ellos vinculados a gobiernos, se están focalizando para robar datos sobre COVID-19, ya sean vinculados a potenciales medicamentos, fórmulas, estudios o cualquier dato que les permita tener una ventaja, no solo financiera, sobre la pandemia.

Comercialización de *exploits*

En el mercado negro de *0 days* y *exploits* [5], se ha observado un notable crecimiento en la demanda. En los foros de compra de kits de *malware* se puede apreciar cómo han aumentado, en las últimas semanas, los hilos preguntando por el funcionamiento de algunas muestras que sirven para explotar vulnerabilidades o pidiendo consejo para escoger el tipo de *malware* que se va a utilizar, contra diferentes tipos de verticales o tecnologías que afecten a los servicios de videoconferencia o accesos remotos. Es por ello que se ha empezado a comercializar con vulnerabilidades como el *0-day* de Zoom [6], a precio de medio millón de dólares, para así conseguir el acceso y control de la máquina remota que ejecute dicho software, o los casos de Pulse Secure VPN o Citrix, las cuales evidenciaron tener vulnerabilidades capaces de ser explotadas de forma remota [7], entre otros.

Cabe destacar que el seguimiento de la compra-venta en el mercado negro es complicado y requiere de un gran nivel de conocimiento del cibercrimen y de infiltración en distintos grupos de cibercriminales. Esto ocurre porque es frecuente que el contacto entre comprador y vendedor se realice a través de mensajes privados, utilizando canales como Jabber o correo electrónico.

Conclusiones

Esta nueva situación mundial está generando cambios a grandes pasos, tanto en nuestras vidas personales como en las profesionales. Por ello hace falta una adaptación más dinámica, sin olvidar la ciberseguridad, ni dejar de estar al corriente de lo que está pasando en el mundo del cibercrimen que nos pueda afectar.

Por estos motivos, y cuando el despliegue de tecnología no ha podido seguir todas las medias de profilaxis y protección pertinentes, ya sea por la situación de alta emergencia o por no estar preparados, deben invertirse más recursos en hacer que los usuarios nos echen una mano y se pongan mascarillas virtuales. Para enseñarles a hacerlo, nada mejor que realizar formaciones y concienciaciones de las amenazas y riesgos a los que están expuestos y recordarles que es esencial su colaboración en un momento tan dinámico.

Por otra parte, aunque en una primera instancia no se haya podido realizar la correcta implementación u optimización de la infraestructura tecnológica actual, es esencial establecer medidas de control y monitorización a los equipos que operan en remoto.

Por último, uno de los grandes retos de las grandes empresas, y ahora si cabe aún mayor, es que desde que ha entrado la variable de la distancia en la ecuación, resulta esencial mantener los sistemas actualizados de los empleados en teletrabajo. Las nuevas actualizaciones contienen los parches de seguridad que evitan la ejecución de código malicioso y, por lo tanto, principalmente el robo de datos y extorsión. ■

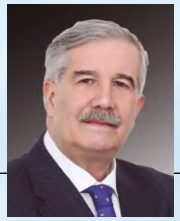
Daniel Solís
CEO
Ramsés Pascual
Analista de Ciberinteligencia
BLUELIV

REFERENCIAS

[1] https://www.blueliv.com/the-credential-theft-ecosystem/
[2] https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/escape-from-the-maze/
[3] https://unaaldia.hispasec.com/2020/03/campana-de-phishing-a-hospitales-aprovechando-la-crisis-del-coronavirus.html
[4] https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/sounding-the-pharma-alarma/
[5] https://www.blueliv.com/threat-intelligence-dark-commerce-report-part-i/
[6] https://www.bleepingcomputer.com/news/security/exploit-for-zoom-windows-zero-day-being-sold-for-500-000/
[7] https://nakedsecurity.sophos.com/2020/05/15/top-10-most-exploited-vulnerabilities-list-released-by-fbi-dhs-cisa/

Las mejores prácticas ISO contra el COVID-19 y crisis futuras

Con base en las normas internacionales ISO 22301, ISO 27001 y 27002, e ISO 20000-1, los autores, dos reputados expertos de AENOR, evidencian en las siguientes líneas la forma en que puede implementarse de forma sistemática el teletrabajo construyendo un marco de gestión certificable que abarca la protección de la privacidad, la ciberseguridad, los servicios TIC y la continuidad de negocio.



Boris Delgado / Carlos Manuel Fernández

En los últimos años la evolución de las TIC no ha cesado y su vertiginoso desarrollo ha sido de tal magnitud que la 4ª revolución industrial (tecnológica) y la Transformación Digital han ido teniendo un profundo impacto en las organizaciones, en las industrias y en la sociedad en general.

Y, mientras las organizaciones pensaban y abordaban su transformación digital, sucedió lo inesperado: aquello que solo algunas voces habían vaticinado, como si de una novela de ciencia ficción se tratara, una terrible y demoledora pandemia global impacta a todos los países del mundo. Asia, Europa, América se veían afectados por el coronavirus o COVID-19. Y como medidas para minimizar esta propagación, los diferentes gobiernos han establecido, entre otras, el confinamiento de la población en sus hogares.

Este escenario ha obligado a tomar decisiones para dar continuidad a la actividad laboral, lo que en muchos ha acelerado la adopción de soluciones TIC en las organizaciones y empleados, para poder trabajar en remoto (teletrabajo) a través de herramientas colaborativas.

Sin embargo, esto ha generado a la misma velocidad, riesgos en los sistemas de información de las organizaciones que deben ser debidamente gestionados para que la seguridad y privacidad de las organizaciones (empleados, clientes y *stakeholders*) se vean lo menos afectadas posible, para ser productivos y eficaces, cumpliendo los objetivos de negocio.

Datos que llaman la atención

Según datos del INE, en 2019 en España, solo el 4,8% de los trabajadores utilizaban el teletrabajo. En el momento actual, según datos del Banco de España, el 80% de las organizaciones han aumentado el teletrabajo.

Según la OCDE, 62,5% de los servicios de banda ancha en España están conectados por fibra óptica, lo que permite colocar a España como el sexto país del mundo por fibra óptica implantada.

No obstante, aún quedan por cubrir 9.400 municipios de esa "España vaciada", que no tienen esa cobertura.

El avance de las redes móviles 4G y 5G y la implantación masiva de fibra óptica hasta los hogares facilita enormemente que los empleados puedan teletrabajar o realizar sus funciones desde casa. Además, las herramientas colaborativas, como las videollamadas, videoconferencias o reuniones virtuales, o los entornos *cloud*, hacen que con cualquier terminal u ordenador conectado a Internet, dispongamos de un puesto de trabajo móvil sin la necesidad de estar presencialmente en las instalaciones de la organización.

Confianza en los estándares ISO

Las empresas necesitan más que nunca trasmitir confianza plena sobre sus servicios y forma de actuar, y los compradores -desde los consumidores a las grandes corporaciones e instituciones- necesitan confianza para la toma de decisiones. Sólo así es posible producir y poner en el mercado con la rapidez y seguridad que el mercado exige.

Pero los riesgos de una crisis sanitaria junto con las medidas de confinamiento que los diferentes gobiernos han adoptado para evitar la expansión del COVID-19, son los que afectan directamente a las personas; las cuales y por esta situación, no pueden acceder a sus puestos de trabajo y deben realizar, en el mejor de los casos, su actividad desde sus casas.

Concretamente los principales riesgos y amenazas TIC, a los que los empleados y trabajadores se enfrentan en la actual crisis, cuando realizan teletrabajo y se utilizan herramientas colaborativas son, entre otros:

- No utilizar dispositivos corporativos, y usar dispositivos personales (BYOD-Bring Your Own Device)
- No utilizar accesos seguros a los sistemas corporativos (VPNs corporativas) en la conexión a la red con WIFI doméstica.
- No realizar *backup* de la información en repositorios corporativos.
- No actualizar con los parches de seguridad, conforme a las políticas establecidas por las áreas de TI de cada organización.
- Pérdida de confidencialidad y privacidad en las comunicaciones.

AENOR diseñó el Modelo de Ciberseguridad y Privacidad para la nueva era digital (ver **Figura 1**) basado en estándares internacionales ISO que son buenas prácticas (best-practices) como la ISO 27001, ISO 20000-1 o ISO 22301 que ayudan a las organizaciones a hacer frente a los riesgos y amenazas TIC; y en el escenario actual y futuros, los indicados anteriormente relacionados con

AENOR ha desplegado toda su capacidad para ayudar a gestionar el proceso de auditoría de las organizaciones y llevarlas a cabo en remoto (teletrabajo), garantizando la confianza de los sistemas, así como la calidad y adecuación de los procesos. Esta alternativa permite no retrasar el proceso de auditoría y coloca a las organizaciones en una mejor posición para recuperar lo antes posible la actividad normal una vez superada la crisis del coronavirus.

el teletrabajo, con el objetivo de generar y devolver la confianza a las organizaciones. Y son muchas organizaciones certificadas por AENOR en los anteriores sistemas, y que han ayudado dando una respuesta eficaz a esta crisis, al disponer de un sistema de gestión auditado anualmente por AENOR.[1]

Así, el modelo descrito, propone tres soluciones (sistemas de gestión) relacionadas entre sí basadas en normas internacionales ISO, a los riesgos y amenazas anteriores:

La primera es la Resiliencia y Continuidad de Negocio con ISO 22301, cuyo objetivo es la identificación de los procesos críticos de la organización (a través del BIA-Business Impact Analysis), considerando los tiempos máximos de recuperación, y a los empleados, clientes, proveedores críticos y *stakeholders*, para que, ante incidentes disruptivos, se tomen la decisiones más adecuadas por el comité de crisis ejecutando los correspondientes planes de continuidad para no parar la actividad de la organización.

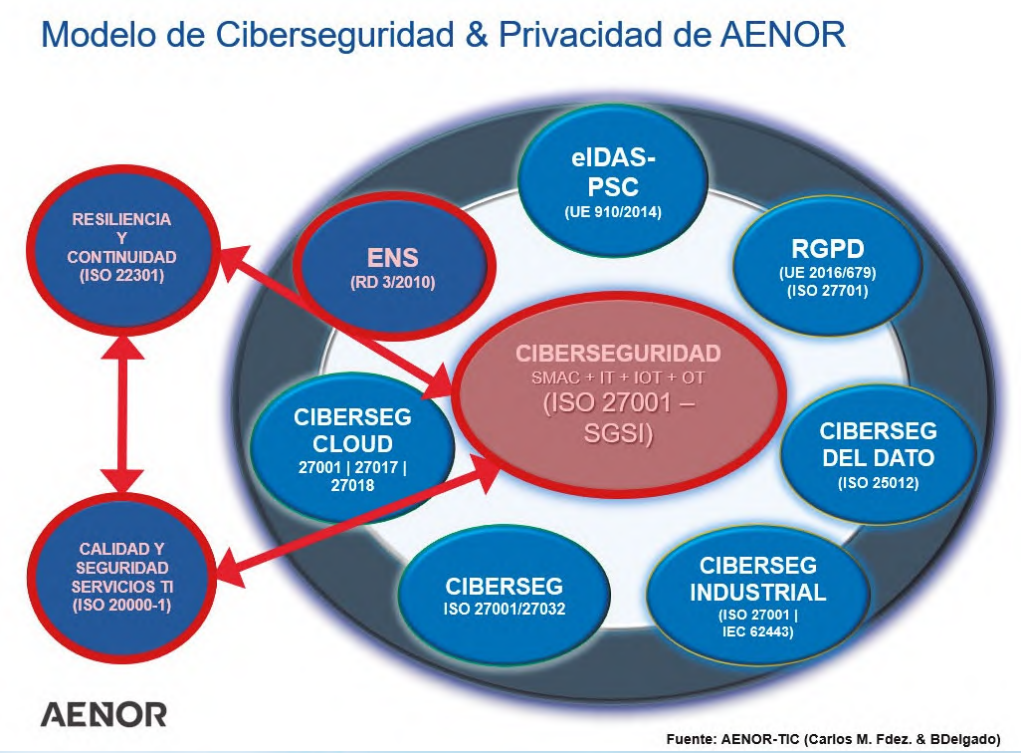


Figura 1

Ante escenarios como el de COVID-19, donde los empleados no pueden acceder físicamente a sus instalaciones (o no todos), es crucial disponer de un sistema de gestión como ISO 22301, que dote a la organización los planes de continuidad que permitan a los empleados realizar su actividad de forma remota (teletrabajo).

En segundo lugar, la Ciberseguridad y teletrabajo seguros con ISO 27001/ISO 27002 y ENS. El objetivo, a través del análisis y gestión de riesgos de los procesos de negocio/servicios de TI y sus activos de información, hardware, software, es aplicar un set de controles para mitigar dichos riesgos.

Por ejemplo, el **dominio A.6.2 Dispositivos móviles y teletrabajo (ENS – Art 21. y medidas como org.2; op.acc.7)**, donde la correcta aplicación del control garantiza la seguridad en dispositivos móviles y en las condiciones del teletrabajo. O el dominio **A.13 Seguridad en las comunicaciones (ENS – medidas como mp.com.2 y mp.com.3), garantizando** comunicaciones seguras a través de VPNs, asegurando la confidencialidad y privacidad de la información intercambiada con los sistemas corporativos. También los controles relacionados con la privacidad **A.18.1.4 Protección de datos y privacidad de la información personal (ENS – medidas como mp.info.1)**. Además, dispone de los controles para la contingencia/continuidad TIC, lo que permite que la organización sea "ciberresiliente".

Y no menos importante, **la gestión de incidencias de seguridad**, que en estos tiempos se incrementan precisamente por los accesos remotos a los recursos corporativos.

En tercer y último lugar, la Calidad, Disponibilidad y Continuidad de servicios TIC con ISO 20000-1. El fin es la prestación de los servicios de TIC, como pueden ser las herramientas colaborativas para el teletrabajo, garantizando la capacidad, la disponibilidad y continuidad de estos servicios TIC y plataformas colaborativas utilizadas por las organizaciones para el desempeño eficaz de la actividad de sus empleados y la relación con sus clientes. Por ejemplo, los procesos de gestión de la capacidad (demanda actual y futura en relación a un servicio TIC, como puede ser escritorio remoto, videoconferencia, o acceso a espacios compartidos), proceso de disponibilidad y continuidad del servicio TIC, o proceso de gestión de incidentes; incluso el proceso de gestión de acuerdos de nivel de servicio con proveedores. Estos procesos son relevantes para garantizar la operativa de la organización.

En definitiva, estos tres sistemas de gestión, basados en buenas prácticas ISO, abarcan los siguientes aspectos clave:

- **El análisis, gestión y mitigación de los riesgos y ciberriesgos** en las TIC de las organizaciones. Y sus controles/procesos para una protección (seguridad y privacidad) adecuada de la información, los servicios y sistemas de la organización.
- **El ciclo de mejora continua** (PDCA-Plan, Do, Check, Act), que, como es sabido, es el motor de mejora continua orientado a objetivos de negocio.
- **La gestión de incidencias de seguridad** y de los servicios de TIC.
- **Compromiso de la Dirección**, que toma decisiones en base a la información que le proporciona los sistemas de gestión anteriores.
- **Concienciación y formación** a los empleados en materia de Continuidad, Ciberseguridad y servicios TIC. Hay que destacar que la privacidad y confidencialidad de la información en un entorno doméstico, se pueden garantizar gracias a la correcta aplicación de acciones de concienciación y formación de los empleados.
- Y de forma particular para **continuidad de negocio, el Business Impact Analysis (BIA),** la gestión de crisis ante un incidente disruptivo y los planes de continuidad; para ciberseguridad, la gestión de incidencias de seguridad; para la provisión de servicios de TI, los acuerdos de nivel de servicio, la gestión de incidencias, la seguridad y la disponibilidad/continuidad de los servicios TIC.

[1] Datos obtenidos mediante técnica Delphi por expertos (equipo auditor de AENOR).

Figura 2

Momento para ofrecer soluciones: auditorías en remoto

En AENOR hemos perseguido, todavía más en estos momentos, encontrar soluciones seguras y factibles para nuestros clientes, y agilizar los procesos de auditoría y seguir llevando a cabo nuestro trabajo de forma que se permita verificar la correcta implantación de los sistemas de gestión con las mejores condiciones de seguridad.

Para ello, AENOR ha desplegado toda su capacidad para ayudar a gestionar el proceso de auditoría de las organizaciones y **llevarlas a cabo en remoto (teletrabajo)**, garantizando la confianza de los sistemas, así como la calidad y adecuación de los procesos. Esta alternativa, permite no retrasar el proceso de auditoría y coloca a las organizaciones en una mejor posición para recuperar lo antes posible la actividad normal una vez superada la crisis del coronavirus.

AENOR ha descrito 10 claves que se deben considerar, en las auditorías en remoto (ver **Figura 2**):

- Identificación de los interlocutores.
- Análisis de tecnologías disponibles y selección de herramientas (considerando la seguridad de las mismas).
- Solicitud de la documentación necesaria para la auditoría y sistema de intercambio de archivos.
- Gestión de horarios y reuniones por áreas o procesos de la organización.
- Pruebas previas, clima laboral (condiciones y tener en cuenta los posibles imprevistos (incidencias, disponibilidad, etc.)

Las auditorías remotas realizadas por nuestros auditores siguen los procedimientos adecuados que garanticen el rigor, imparcialidad e independencia. Dichos auditores, además, se preocupan por que los sistemas de gestión certificados, les estén ayudando en esta crisis, interesándose por su capacidad para continuar tele-trabajando de forma segura, las incidencias de seguridad relacionadas con este escenario, etc.

A modo de conclusión, podemos decir que la actual crisis sanitaria plantea nuevos retos y desafíos urgentes, que deben ser abordados con el máximo rigor y seguridad para seguir contribuyendo, como lo ha hecho AENOR desde su creación, a generar confianza entre organizaciones y personas.

Ejemplo claro de esta vocación por ofrecer servicios y productos tangibles que aporten confianza es la certificación de protocolos frente al COVID-19, que cubre diferentes aspectos, entre los que está la continuidad de negocio.

Actualmente hay más de 800 organizaciones certificadas por AENOR en sistemas como son ISO 22301, ISO 27001 e ISO 20000-1, lo que les ayuda a poder desempeñar sus actividades con resiliencia, calidad y seguridad, en las TIC, siendo precisamente, las que permiten que el teletrabajo sea una realidad. Pero se tiene que seguir trabajando para que las nuevas amenazas y riesgos no impidan continuar trabajando. En AENOR seguimos expectantes para aportar procesos que generen y devuelvan confianza a las organizaciones de hoy y las del futuro, siendo necesario que las organizaciones se puedan estabilizar para continuar con la transformación digital abordada durante estos años.

Un apunte final: no olvidemos por la situación actual, el siguiente reto que tenemos sobre la mesa (de nuestros hogares): el *blockchain*, BigData y su relación con la Inteligencia Artificial, modelos matemáticos y algoritmos, que decidirán sobre cómo actuar ante una crisis como la actual y las que puedan venir. ■

Boris Delgado
Riss. CISA, CISM
Gerente de TIC
bdelgado@aenor.com

Carlos Manuel Fernández
MBA, CISA, CISM
Asesor Estratégico de TI
cmfernandez@fidesol.org

AENOR

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

thycotic

www.thycotic.com

Calificación: teletrabajo seguro a un click de distancia

En estos tiempos que nos han tocado vivir, además de la obvia preocupación por la salud de todos los que nos rodean, muchos hemos tenido que trabajar, y duro, en asegurar la continuidad de las operaciones de nuestras organizaciones con todo el personal desplazado en sus domicilios en teletrabajo, durante un largo período de tiempo y, además, con poco tiempo para tomar decisiones sobre soluciones a adoptar en cuanto a la contratación de nuevos servicios que nos permitan trabajar en estas condiciones tan excepcionales.

Antonio Ramos

En estas circunstancias, son muchas las preguntas que nos habrán surgido en relación con la seguridad, entre otras:

¿Supone este escenario de teletrabajo un mayor riesgo que la situación habitual? ¿Nuestro grado de exposición es ahora mayor? ¿Tendría que adoptar medidas adicionales? ¿Podemos asegurar la disponibilidad de los servicios para nuestros clientes?

En caso de haber implementado soluciones de manera urgente, ¿cumplen con los requisitos de seguridad aprobados?

El impacto del nivel de riesgo de los proveedores

LEET Security es una agencia de calificación y como tal no proporciona servicios de protección con el fin de evitar cualquier potencial conflicto de intereses y, por lo tanto, nuestra contribución en esta situación se focaliza en proporcionar información objetiva y homogénea para una buena toma de decisiones de manera ágil y eficaz, en especial, en lo relativo a los terceros que acceden a nuestros sistemas o que manejan nuestra información en sus propios sistemas. No debemos olvidar que estos terceros, al igual que nosotros mismos, también están trabajando en un escenario excepcional en el que las medidas adoptadas no tienen por qué ser equivalentes a las habituales.

Es decir, las preguntas que ayudamos a responder serían, en línea con las anteriores:

¿Supone este escenario de teletrabajo que mis proveedores [por simplificar] tienen un mayor nivel de riesgo que en la situación habitual?

¿El grado de exposición de mis proveedores es ahora mayor?

¿Tendrían que adoptar/están adoptando mis proveedores medidas adicionales?

¿Me pueden asegurar mis proveedores la disponibilidad de sus servicios?

En caso de que hayan tenido que implementar soluciones de manera urgente, ¿cumplen esos nuevos servicios con los requisitos de seguridad que nosotros necesitamos?

Las respuestas a todas estas preguntas las podemos fundamentar en tres cuestiones principales:

1. La existencia de un dominio específico dedicado al teletrabajo.
2. La supervisión de los proveedores calificados que lleva a cabo la propia agencia.
3. La necesidad de que los proveedores calificados evalúen, a su vez, a sus proveedores.

Dominio específico de teletrabajo

Para saber si los terceros suponen un mayor nivel de riesgo ahora por las circunstancias propias del teletrabajo, caben dos posibilidades: que el servicio calificado en cuestión haya incluido el dominio de teletrabajo en su evaluación o no. ¿Cómo podemos saberlo? Muy sencillo,

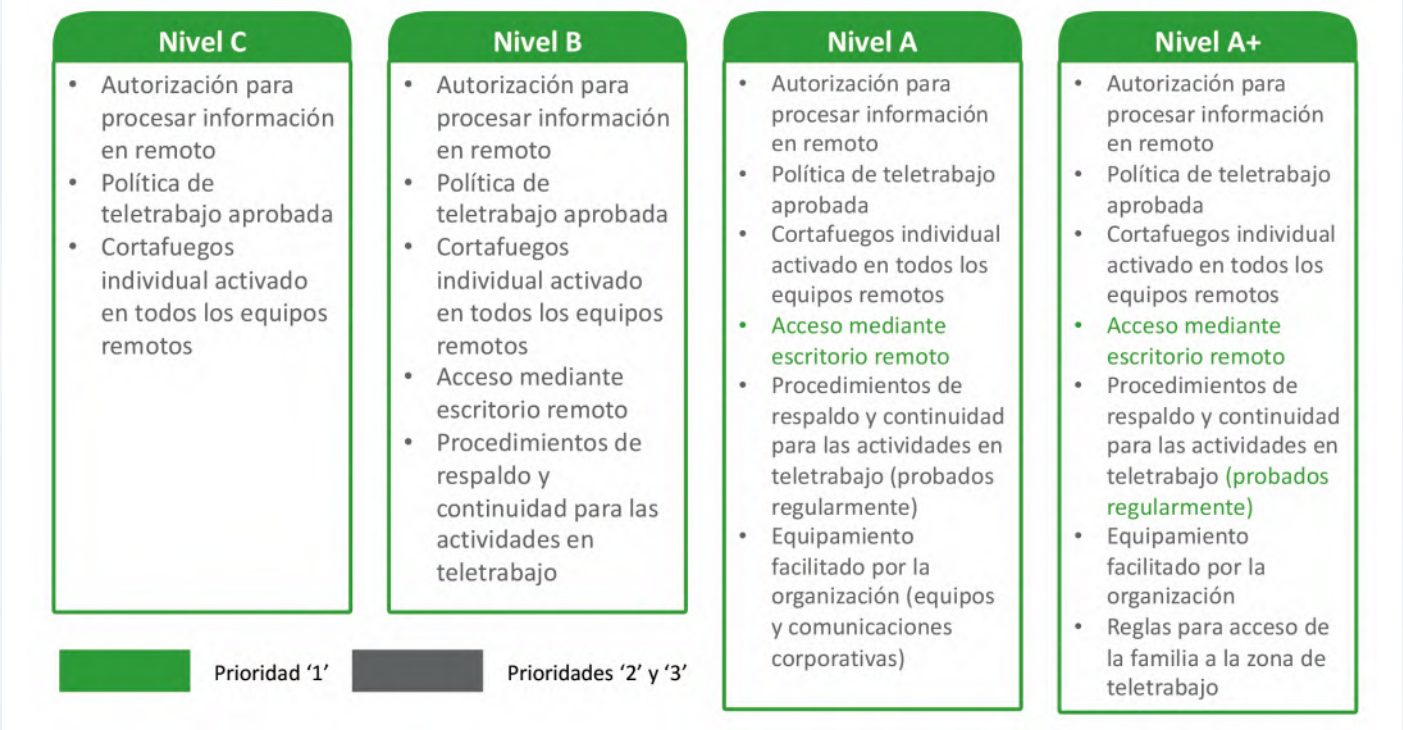


Figura 1.- Medidas de seguridad por nivel de calificación.

NO PENSAR EN LOS RIESGOS PUEDE SER FATAL PARA TU NEGOCIO

NUESTRA MISIÓN ES PROTEGERLO

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

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

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

S·C PREMIOS 2017

el dictamen de calificación detallado con el que cuentan todos los servicios calificados detalla el nivel de seguridad obtenido por dominio y sección y, en particular, en el resultado del dominio [SO.07], que está específicamente dedicado al teletrabajo.

Como se puede ver en la **Figura 1** existen requisitos (incrementales) para el teletrabajo desde el nivel C hasta el nivel A+, de forma que, simplemente consultando el nivel obtenido por el servicio en esta sección podremos entender las medidas incorporadas para la protección del teletrabajo.

Hay que tener en cuenta que no todas las organizaciones tenían previsto el teletrabajo como una opción, aunque la práctica totalidad contaba con mecanismos para conexión desde el exterior (lo que no debe confundirse con el teletrabajo, aunque solo sea por el carácter esporádico de uno y continuado del otro). La evaluación de los mecanismos de seguridad para las conexiones desde el exterior, se pueden consultar en la sección dedicada al control de acceso desde el exterior (NC.04).

En resumen, para saber si en esta situación el servicio supone un nivel de riesgo mayor o no, bastaría con consultar el nivel de seguridad obtenido en las secciones indicadas (teletrabajo y acceso remoto).

Supervisión continua del nivel de seguridad

El servicio de calificación incorpora mecanismos de supervisión para garantizar que el nivel de seguridad publicado es el adecuado. En particular, se mencionan a continuación los más pertinentes para esta situación:

• Un sistema de monitorización externo no intrusivo basado en las IPs asignadas al servicio / proveedor del servicio. Este sistema es utilizado como disparador de alertas, puesto que nos permite detectar variaciones significativas de la huella en Internet de la organización y/o cambios significativos en el grado de exposición de sus activos a potenciales vulnerabilidades y/o problemas de seguridad de todo tipo (configuraciones erróneas, sistemas no protegidos, etc.). En nuestro caso, hacemos uso del servicio de MrLooquer [2] Rating para llevar a cabo esta supervisión (**Figura 2**).

• La propia labor proactiva del equipo de monitorización [3]. Desde que empezó esta situación se están realizando solicitudes a los proveedores calificados que no habían incluido el teletrabajo inicialmente para incorporar la evaluación de los mecanismos de protección en el mismo a la calificación final.


LEET SECURITY
ICT Services Rating Agency

Informe de monitorización mensual

Este informe, incluido en el servicio que desde LEET Security le ofrecemos, es el resultado de una monitorización externa y constante de los puertos de entrada expuestos en la red, realizada con la herramienta de Mr Looquer.

Informe Nº: AC000373829
Fecha: 29 de febrero de 2020

SOBRE EL INFORME

Este informe es un resumen del riesgo detectado, referido al rango de IPs públicas facilitadas por el cliente relacionadas con el servicio calificado.

Es importante reseñar que estas vulnerabilidades se tienen en cuenta a la hora de mantener la calificación de LEET Security, por lo que cualquier variación debe ser comunicada para valorar su efecto sobre los servicios evaluados.

SU PUNTUACIÓN

La puntuación obtenida por **ACME S.A.** es de **400** puntos sobre 1000, tal y como se indica en el diagrama de la izquierda. Como referencia, la herramienta establece un **nivel mínimo deseable (700 puntos)**, así como un **nivel recomendado (900 puntos)**.

En el diagrama de la derecha se muestra la variación del score monitorizado semanalmente, desde la fecha de su primera auditoría o, en su defecto, los últimos 12 meses.

Puntuación
400
Mínimo
Recomendado

EVOLUCIÓN DE LA PUNTUACIÓN
400 400 400 400 400
375
Oct Nov Dic Ene Feb Mar

ACTIVOS

Se monitorizan un total de 25 activos, distribuidos de la siguiente forma:

- 0 activos IP6
- 8 activos IP4
- 17 dominios y subdominios.

De estos 25 activos, 13 están afectados por incidencias con distintos niveles de criticidad (un 52% del total de activos).

Activos afectados
52%

LEET Security

Figura 2.

Evaluación de las cuartas partes

Para responder a la duda sobre si los servicios adicionales que hubieran tenido que contratar los proveedores de los servicios para hacer frente a la situación excepcional de teletrabajo sobrevenido suponen un riesgo adicional, la solución que aporta la calificación es, además de los distintos mecanismos de monitorización mencionados anteriormente, un dominio entero dedicado a la seguridad de la cadena de suministro; es decir, la manera en la que nuestros proveedores evalúan a sus proveedores forma parte del nivel de calificación total que el servicio obtiene.

Dicho de otra manera, el servicio obtendrá un nivel de calificación tan alto como el nivel de seguridad que pueda garantizar de sus proveedores, ya que, al contar con controles obligatorios en esta sección, actúan también como factores limitantes del resultado final.

Es decir, de nuevo, consultando el nivel de calificación del servicio y, en particular del dominio dedicado a las terceras partes, se puede **saber** si el proveedor está supervisando adecuadamente a sus respectivos proveedores.

La actual situación nos obliga al teletrabajo y ante esto, surgen preguntas sobre su seguridad. La existencia de un dominio específico que aborda el teletrabajo en la calificación de servicios, la supervisión de los proveedores calificados y la calificación a su vez de los proveedores de estos proveedores, disipan estas dudas.

En nuestra opinión, la supervisión de proveedores tiene dos componentes evidentes: un componente estático (que es, por ejemplo, cuando hacemos una *due diligence* previa a la contratación mediante una auditoría) y otro dinámico (más relacionado con una supervisión continua y que se parece más a una labor de monitorización típica de un SOC) y se debe hacer uso de ambas para poder tener un entendimiento adecuado del nivel de riesgo de los terceros.

Esta labor de supervisión que realiza la Agencia para los servicios calificados nos permite estar tranquilos sobre si el nivel de seguridad ha aumentado o no, puesto que en caso de que así fuera, el nivel de seguridad publicado sería modificado para reflejar la situación real.

Conclusión

La calificación de un servicio, dada la metodología, cómo se construye y los mecanismos de supervisión utilizados, permite **saber,** en estos momentos tan agitados, de manera ágil y eficaz, si el nivel de riesgo que suponen mis terceros se ha incrementado o se mantiene estable y, todo ello, a la distancia de un clic [1]. ■

Antonio Ramos
CEO
LEET SECURITY

REFERENCIAS

[1] Disponemos de un registro público de los servicios calificados accesible para consulta en: https://www.leetsecurity.com/servicios-calificados/

[2] https://mrlooquer.com/rating.html

[3] Sirva como ejemplo la entrada publicada en el blog de la agencia en relación a las medidas de seguridad relacionadas con el teletrabajo disponible en https://www.leetsecurity.com/blog/teletrabajo/

Porque la seguridad de la información no es solo cosa del firewall y del antivirus, nos complace presentar:

Bitdefender®

NETWORK TRAFFIC SECURITY ANALYTICS

- Detección de las amenazas en tiempo real, para cualquier dispositivo conectado en la red. Visibilidad 360° sobre los ataques o intentos contra cualquier endpoint, independientemente de su tipo (tanto para los dispositivos corporativos como para los BYOD o IoT).

- Ahorro de trabajo con prioridades destacadas por el Automated Security Incident Triage que permite el enfoque del equipo de respuesta a las incidencias y mejora la eficiencia de los equipos de Threat Hunting

- Información detallada para la investigación forense digital y un curso de acción sugerido para la respuesta y preservación de los datos.

Para más información, por favor, visite nuestro sitio web:

https://www.bitdefender.es/business/enterprise-products/network-traffic-security-analytics.html

o contacte con uno de nuestros Channel Partners

Ciberseguridad industrial: reflexiones derivadas de la COVID-19

La irrupción de la COVID-19 ha supuesto un cambio repentino y no previsto en las condiciones de operación de muchas compañías e infraestructuras que dependen para su negocio o la prestación de sus servicios de sistemas de control industrial. En particular, la declaración del estado de alarma y las restricciones de movimiento consecuencia de la misma pueden haber supuesto un incremento en el nivel de riesgo a que estos sistemas se encuentran expuestos. Ahora que parece que vemos la luz al final del túnel (al menos temporalmente), puede tener sentido realizar un primer análisis, necesariamente muy básico, que nos permita extraer algunas lecciones para un futuro que no está demasiado lejano.

Rafael Rosell

Es difícil realizar una estimación directa de algo tan difícil de cuantificar como esto, pero existen algunos indicadores que pueden ser de utilidad para tratar de valorar el impacto en la ciberseguridad de esta situación excepcional. Uno de ellos es el uso de los accesos remotos a los sistemas. Otro indicador es la gestión de los incidentes de ciberseguridad.

Si bien no nos es posible aportar todavía datos precisos al respecto, sí que podemos realizar una valoración cualitativa a partir de nuestra experiencia en los servicios que S2 Grupo CERT presta en este tipo de operadores.

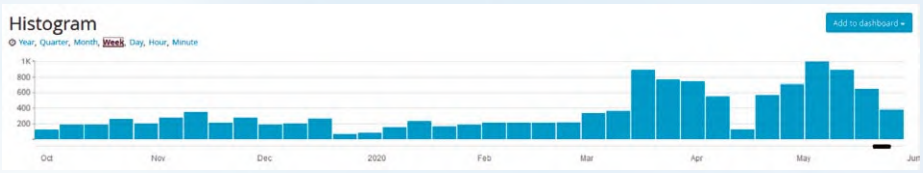
En primer lugar, hemos percibido en algunos casos un incremento notable en los accesos remotos a sistemas de control industrial. Si bien el uso de este tipo de accesos es habitual, la situación de incertidumbre previa a la declaración del estado de alarma el 14 de marzo motivó la habilitación de mecanismos de acceso remoto "de emergencia", desde ubicaciones y por personal que no se habían considerado previamente. En algún caso sí nos ha sido posible cuantificar un incremento en un factor 4 en el uso de accesos remotos ya habilitados previamente a partir del día 12 de marzo, con un regreso paulatino a niveles habituales en la segunda quincena de mayo.

Por otra parte, también hemos constatado un incremento en el tiempo de respuesta ante notificaciones de ciberseguridad por parte de las organizaciones, principalmente en aquellos casos en lo que no existe personal específico asignado a este tipo de actividad. Esto podría ser atribuible al esfuerzo extra requerido para la gestión de la situación de contingencia, preparación y despliegue de medios para el trabajo remoto de un buen número de empleados que habitualmente no hacen uso de esta opción.

La combinación de estos tres factores:

- El despliegue a marchas forzadas de accesos remotos sin tiempo para llevar a cabo una validación técnica y el establecimiento de procedimientos de gestión.
- El incremento en el uso de estos accesos.
- El descenso en la disponibilidad del personal encargado de la gestión de incidencias supone en cualquier caso un riesgo adicional que no se ha gestionado adecuadamente en todos los casos.

Además de estos aspectos tecnológicos, durante la crisis de COVID-19 y especialmente al principio de la misma se dieron otras situaciones que han incrementado el riesgo sobre la continuidad de las operaciones, y que han puesto al límite a las organizaciones y sus planes de contingencia, en muchos casos activados por primera vez desde la aprobación de la LPIC. Entre ellos tiene especial importancia la gestión del personal. Podemos decir que la crisis ha evidenciado la dependencia que se tiene de cierto personal difícilmente sustituible, sobre todo en tiempos de reducción de costes de mantenimiento y externalización de servicios. En sistemas críticos solemos contar equipos redundados para asegurar la continuidad pero esto es mucho más difícil con las personas, ya que distribuir el conocimiento es más complejo que duplicar sistemas.



Registros asociados al acceso remoto a los sistemas industriales de una infraestructura. Es notorio el incremento experimentado a partir de la mitad de marzo.

También se ha evidenciado que muchas infraestructuras dependen necesariamente de la presencia de personal *in situ*, habiéndose dado por sentado en algunos casos que siempre sería posible acceder a las instalaciones. Este supuesto se puso a prueba cuando hubo que gestionar la emisión y gestión exprés de los salvoconductos para los empleados que tenían que desplazarse hasta las infraestructuras en que desempeñaban su actividad. Hay que recordar que la orden de confinamiento total se produjo en fin de semana, cuando los recursos necesarios son más difíciles de movilizar, y más todavía en esta situación.

También ha sido evidente la dificultad para proporcionar protección sanitaria al personal: garantizar distancias de seguridad en los puestos o adquirir y distribuir equipos de protección individual en cantidad suficiente para abastecer a los empleados (ya hemos visto lo que ha ocurrido en un servicio esencial como es el sanitario). Es evidente que no disponer de un criterio claro no ha ayudado, pero… ¿qué hubiese ocurrido de haberse considerado imperativo el uso de mascarillas u otros EPIs? De no haberse podido proveer a todos los empleados de infraestructuras críticas, ¿podrían estos haberse negado a acceder a su puesto de trabajo? Imaginemos qué habría ocurrido si este virus hubiese combinado su capacidad de contagio con una letalidad más elevada.

Realizando una valoración final, cabría decir que el resultado no ha sido tan malo como potencialmente podría haber sido. Pero precisamente por eso, reconociendo el estrés a que se han visto sometidos los sistemas y el personal de servicios esenciales, es el momento de acometer algunas acciones antes de que un posible rebrote otoñal se materialice. Sin ánimo de ser exhaustivos, me atrevería a señalar dos.

Acciones a acometer

En primer lugar, todos los sistemas desplegados para permitir el acceso remoto deben ser sistemáticamente evaluados. No hay nada más permanente que aquello que se plantea de forma provisional, por lo que el riesgo de que errores de configuración y gestión debidos a la premura queden de forma permanentes y puedan ser aprovechados con fines maliciosos en el futuro es bien real. Es más, debe revisarse el propio concepto de acceso remoto, ya que lo que antes se preveía en algunos casos como una herramienta de contingencia va a convertirse, como hemos visto, en parte de la 'nueva' normalidad.

En segundo lugar, el funcionamiento de los planes de contingencia durante la crisis debe revisarse sistemáticamente, y estos deben actualizarse para ser adaptados a este nuevo escenario, un escenario en que el conocimiento y habilidades de ciertos empleados deben ser considerados tan críticos como otros elementos tecnológicos. A modo de conclusión, y tratando de ser positivos, en realidad deberíamos plantearnos esto como una oportunidad. ■

Rafael Rosell
Director Comercial
S2 GRUPO

La llave física que vela por su seguridad digital

Impida los robos de cuentas, y modernice su MFA (autenticación de múltiples factores). Obtenga la llave de seguridad líder en el mundo para mejorar la seguridad, la experiencia de usuario y el retorno de inversión.

Mayor seguridad: las credenciales de autenticación de empleados protegidas únicamente con un YubiKey y FIDO U2F han experimentado un aumento significativo en el nivel de seguridad con cero robos de cuentas.

Mayor productividad de los empleados: los empleados vieron una reducción de casi un 50 por ciento del tiempo para autenticarse usando un YubiKey en comparación con el uso de una contraseña de un solo uso (OTP) a través de SMS. Los inicios de sesión fueron casi cuatro veces más rápidos al comparar YubiKey con Google Authenticator. El tiempo ahorrado se debe principalmente a la característica única de YubiKey, que requiere un único toque para que el propio YubiKey inserte el código de autenticación por el usuario en el campo de OTP en milisegundos.

Soporte reducido: en comparación con el uso de un teléfono para la autenticación, los YubiKeys son fáciles de usar, de diseño robusto, impermeables y no se rompen fácilmente—Al no tener pila, pueden durar de por vida. Estos atributos permitieron a Google emitir múltiples copias de seguridad de YubiKey para cada empleado y aún así ahorrar costes. Las llamadas de soporte bajaron con una reducción de incidencias de un 92%, ahorrando miles de horas por año en soporte.

dotforce
Your Source for innovative Cybertech

Para más información visite:
https://www.dotforce.es/yubico/
o bien llame al 914 230 991.

DotForce – Mayorista de soluciones de ciberseguridad y optimización de operaciones TIC.
https://www.dotforce.es

yubico

>> Jorge Dávila

Tras el Cuarto Jinete[1]

Llegó la hora de poner a prueba los Planes de Contingencia nacidos de múltiples Análisis de Riesgo previos, y en cierta medida vemos que han fallado todos. El virus que ahora nos (pre)ocupa no aparece en Virus Total, sino que ataca a nuestros sistemas vitales más que a nuestros sistemas operativos que, por otra parte, han pasado a un distante segundo plano. El miedo, una vez más, ha despertado la insolidaridad darwiniana de algunos humanos y ya claman voces para que se marque, para que se distinga a sanos de enfermos, a inocuos de infecciosos. Esto no sería una gran noticia si no fuese porque ahora, por primera vez en la Historia, sí es posible y hay tecnologías que permitirían hacer exactamente eso, marcar a unos y otros haciendo saltar por los aires la intimidad del individuo, y muchos otros de sus derechos fundamentales. Es hora de plantear si es posible que un Coronavirus orgánico engendre un virus tecnológico oportunista que nos etiquete y, de algún modo, nos condene a todos (o a casi todos) a la vigilancia y al sometimiento eternos.

El nitrophenyl-pentadienal[2], NPPD[3], o METKA ("marca" en ruso) es lo que coloquialmente se conocía durante la guerra fría como "*spy dust*". Esa sustancia se utilizó, entre otras, para el marcado de agentes extranjeros por parte del KGB soviético. Con esta sustancia, las autoridades eran capaces de seguir el movimiento de los agentes occidentales aplicándoles, sin que se diesen cuenta de ello o por mera transferencia cuando tocaban ciertos objetos, esta sustancia como un polvo invisible en su ropa, suelas de zapato, asientos de coche, pomos de puerta y cualesquiera otros objetos. Algunas variantes de "*spy dust*" incluyen al luminol[4] (famoso por series televisivas como CSI), que fluoresce cuando se le ilumina con luz ultravioleta.

Las primeras noticias de esta sustancia se las dio a la CIA, en 1963, el desertor del KGB Alexander Chrepanov y su uso fue detectado durante la década de 1970. En 1984, el oficial del KGB que actuaba como espía de la CIA, Sergei Vorontsov, les entregó una muestra de METKA, posteriormente y éste fue delatado por el espía ruso en la CIA Aldrich Ammes, por lo que terminó siendo ejecutado por traición.

El KGB lo aplicaba en las suelas de los zapatos de los espías occidentales para poder saber por dónde habían ido gracias al uso de perros entrenados. "Podía ser muy útil para coger a un individuo en concreto dentro de una multitud, incluso de noche y con mal tiempo"[5]. Se llegó incluso a utilizar isótopos radioactivos como sustancias marcadoras invisibles, que eran detectadas con contadores Geiger-Müller escondidos en los *checkpoints* que debían cruzar cuando intentaban regresar a occidente.

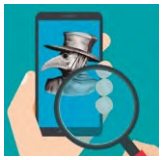
Infecciosos y No-Infecciosos

Una situación parecida se ha vuelto a plantear con la llegada de la pandemia del SARS-CoV-2[6], o Covid-19 para los amigos, en la que algunos quieren poder clasificar de forma masiva a toda la población mundial para poder catalogarla, en tiempo real, en **Infecciosos** y **No-Infecciosos**. Cualquier clasificación se hace por algo, y no sería de extrañar que los promotores de esta nueva "caza de brujas" estén pensando en confinar a los infecciosos quieran o no ser confinados.

Lo de clasificar a la gente, sobre todo cuando es en contra de su voluntad, siempre ha traído problemas bastante profundos a la Humanidad y, desde luego, no es propio de los sistemas democráticos occidentales. China y Corea son otra cosa. Todavía nos podemos acordar de las clasificaciones que algunos hicieron en Alemania, en la primera mitad de Siglo XX, utilizando triángulos de distintos colores[7] y números tatuados en el antebrazo.

¿Qué nos ha llevado a tener que estar hablando de esto al final de la segunda década del Siglo XXI? La razón de ello es que, aparentemente sin aviso previo, se ha desatado una pandemia planetaria de magnitudes no vistas en los últimos cien años. El caso más próximo es la pandemia de la **Gripe Española**[9] de 1918 que durante 36 meses infectó a 500 millones de personas, y la más conocida por todos son los diferentes episodios de **Peste Bubónica**[10] del 1348, que se llevó por delante a un tercio de la población europea de entonces. La gripe fue un Virus (Orthomyxoviridae[11] H1N1), la Peste, una bacteria (Yersinia Pestis[12]); pero en ambos casos la Humanidad no estaba preparada para ello.

La evolución de las pandemias se parecen bastante a los estados de agregación de la materia: sólido, líquido y gaseoso.



A diferencia de pandemias anteriores, en el mundo actual de las comunicaciones, la globalidad y la movilidad "Urbi et Orbe", han surgido propuestas e incluso exigencias, de que se utilicen los siempre bien identificados teléfonos móviles para trazar el deambular (líquido) de los ciudadanos y ser capaces de identificar a quienes estuvieron cerca de cualquiera de nosotros en el pasado inmediato.

[1] Ap 6:8
[2] Notación IUPAC: (2*E*,4*E*)-5-(4-Nitrophenyl)-2,4-pentadienal
[3] Ver https://en.wikipedia.org/wiki/Nitrophenyl_pentadienal
[4] Ver https://en.wikipedia.org/wiki/Luminol
[5] Antonio Mendez; "*Spy Dust: Two Masters of Disguise Reveal the Tools and Operations That Helped Win the Cold War*", Simon Pulse Ed., September 1, 2003. ISBN-13: 978-0743428538
[6] SARS-CoV-2 = Severe Acute Respiratory Syndrome CoronaVirus 2
[7] Ver https://en.wikipedia.org/wiki/Nazi_concentration_camp_badge
[8] Pandemia: proviene del griego πᾶν, pan, "todo" y δῆμος, demos, "gente", que afecta "a todos los humanos".
[9] Ver https://en.wikipedia.org/wiki/Spanish_flu Lista de epidemias https://en.wikipedia.org/wiki/List_of_epidemics
[10] Ver https://en.wikipedia.org/wiki/Black_Death
[11] Ver https://en.wikipedia.org/wiki/Orthomyxoviridae
[12] Ver https://en.wikipedia.org/wiki/Yersinia_pestis

Estado sólido: el virus existe y se cría viviendo/infectando a un número cerrado y limitado de individuos (huéspedes) que suelen haber desarrollado algún tipo de resistencia/inmunidad frente al virus. En ese estado, la comunidad se encuentra espacialmente limitada dentro de su hábitat, que no solapa con los humanos, y por ello no se propaga fuera del espacio que le es propio.

De aquí nace el convencimiento de que alterar la ecología y los hábitats del planeta nos acaba pasando factura a todos. La Peste Negra es una enfermedad de roedores del campo que es transportada por las pulgas (Xenopsylla cheopis) que viven en y de ellos. En un entorno urbano, cuando ya no hay ratas de las que vivir, porque entre otras causas la infección las ha matado, las pulgas saltan a vivir en los humanos, y ya fue cuestión de tiempo que la bacteria Yersinia Pestis que llevaban en sus estómagos infectara a los hombres y entrara así en la historia de la Humanidad.

Las infecciones también pueden tener una fase que recuerda al **Estado líquido**: el virus infecta a individuos que se mueven libremente pero con cierto roce, viscosidad, entre individuos también infectables. En este caso, la velocidad de desarrollo de la pandemia depende sólo de lo que le cueste al virus saltar de un individuo a otro. Al ser un medio fluido el de los portadores, el virus puede terminar ocupando todo el hábitat de esos individuos y hacerlo de forma homogénea, ya que el riesgo de contacto es isotrópico.

Las velocidades con las que pueden darse esas infecciones recuerdan al frente de detonación[13] en un material explosivo. En este caso la **Velocidad de Detonación** depende de muchas cosas pero, entre ellas, del tamaño de las partículas de explosivo; a partículas más pequeñas, con más superficie de contacto, mayor velocidad de detonación. En el caso de las pandemias, su velocidad aumenta al aumentar la **intensidad y el número de relaciones sociales por unidad de tiempo**, que hace apreciablemente diferente el carácter latino o mediterráneo respecto al carácter nórdico. Además de la intensidad y la frecuencia de contacto, la velocidad de propagación de las infecciones depende de la **adyacencia** y **contigüidad** de los sujetos infectados e infectables por lo que, necesariamente, **aumenta con la densidad de población** de esas sociedades.

Por último, las pandemias, cuando se agotan, pasan por una fase similar al **Estado gaseoso**. En este caso, el virus vive en individuos infectados que se mueven libremente y con escasa interacción entre ellos, como ocurre en el estado gaseoso, pero en esta circunstancia, la mayoría de los individuos que interactúan ya han desarrollado **inmunidad** y **no-son-transmisores** del virus. En este estado de agregación, la mayoría de los individuos son inertes desde el punto de vista del virus, ya que ni se infectan ni pueden infectar.

Aunque en este estado haya todavía individuos susceptibles de ser infectados, su concentración es baja respecto a los inmunes y por ello se requiere de bastante tiempo y muchos encuentros (contactos sociales) para que el virus pueda saltar de un individuo infectado a un individuo infectable. En este caso, la velocidad de contagio (como la de cualquier reacción química ordinaria) será directamente proporcional al producto de las concentraciones de individuos infectables e infectados; y solo la baja concentración de unos y otros disminuirá, tanto la velocidad de avance de la infección como para que pueda darse por terminada la Pandemia.

Dicho de otro modo, la única forma de terminar con una pandemia es conseguir **1)** que la inmensa mayoría de la población sea inmune a ella (inmunidad de grupo o rebaño) porque han superado la enfermedad o se les ha vacunado y ha desarrollado sus propias defensas inmunológicas, **2)** que desaparezcan prácticamente todos los infectados, o **3)** que se infecte toda la población.

Ahora sabemos por los estudios serológicos que sólo ha desarrollado inmunidad menos de un 10% de la población, lo que está muy lejos del umbral necesario para hablar de inmunidad de grupo (estado gaseoso), por lo que habrá que esperar a la creación de una vacuna efectiva.

Gestión y control de pandemias

Desde el punto de la gestión y el control de pandemias, se pueden probar varias aproximaciones:

1) Evitar que se funda el estado sólido. En este caso, habría que erradicar aquellas acciones o conductas humanas que (I) destruyen hábitats de otras especies y empujan a sus patógenos a buscar nuevos mundos en los que vivir e infectar, y (II) disminuir la permeabilidad de las fronteras de los humanos con esos otros seres vivos y sus patógenos (menos mascotas exóticas, menos medicinas tradicionales chinas, dejar en paz y felices al pangolín o a los murciélagos de la fruta en sus hábitats).

2) Si se funde el estado sólido, congelarlo inmediatamente. Esto es lo que se ha intentado con el confinamiento del mundo en los primeros meses del año 2020 y que pasará a la Historia. Fijando los individuos al terreno como si fuesen plantas, se disminuye el contacto entre personas (Distanciamiento Social) y el desplazamiento geográfico (Difusión) de los infectados.

Google y Apple se han asociado para ofertar al planeta su apoyo para el desarrollo de sistemas de trazado de personas a través de los móviles que están por todo el mundo (desarrollado), ya que o corren Android o iOS. Proponen meter lo esencial de las aplicaciones de seguimiento y trazado de cada uno de esos artefactos, directamente en el sistema operativo, de manera que sean indisolubles con él. En su propuesta, si quieres tener un smartphone y datos, tienes que aceptar estar potencialmente monitorizado "around the clock".

Los individuos infectados por virus sólo tienen, simplificando, dos posibles futuros: desarrollar algún grado de inmunidad y acabar con todo el virus activo, o morir por la excesiva proliferación de virus y sus efectos negativos sobre los sistemas vitales del paciente. La "**congelación social**", el **confinamiento** y el **aislamiento**, sólo persiguen **1)** que los infectados que haya, sobrevivan o perezcan sin interactuar con otros, y realmente esto no es una solución de la enfermedad, ya que se carece de medicina para ello, y **2)** que la **velocidad de contagio/propagación** de la pandemia esté limitada y, desde algún punto de vista (capacidades del sistema sanitario), sea manejable (tratamiento farmacológico, ingreso en UCIs, gestión de las defunciones, etc.).

Dado que el distanciamiento social es un **estado muy inestable y peligroso** si se gestiona inadecuadamente, tarde o temprano la sociedad volverá a un **estado meloso** en el que la libertad de movimientos estará todavía muy limitada pero se

[13] Detonación: Tipo de combustión que sigue un frente exotérmico y supersónico que se acelera a través del medio y que genera una onda de choque que viaja justo delante de él.

dará, con lo cual aumentará de nuevo la velocidad de contagios, su número y sus consecuencias.

Otra posibilidad es que **la densidad de Infectados y/o No infectados disminuya**. En este escenario estamos ante **dos reactivos** (Infectados y No infectados) disueltos en un **solvente** (los Inmunes) que necesitan encontrarse entre sí para que la Pandemia progrese. Si la concentración de uno u otro es baja, **la pandemia se lentifica**, lo cual no quiere decir que no llegará a su **meta final**, que es **haber infectado a todos los individuos posibles** y haberse con ello cobrado su botín en vidas humanas.

Este escenario es en el que se habla de la **inmunidad de rebaño** y en él, la velocidad de propagación de la enfermedad es suficientemente lenta para no poder considerarla como una Pandemia; pero, como decía Galileo de la tierra, "*E pur **si muove***", y la infección sigue propagándose. El final de la enfermedad sólo es posible cuando la velocidad de propagación sea tan lenta que la dinámica del virus termine en todos los infectados sin que haya nuevos contagios.

La ventaja de disminuir la velocidad de propagación es que se gana tiempo. Dado que, en la mayoría de los casos, la infección de individuo sólo puede durar cierto tiempo, a menos que se convierta en huésped asintomático (portador) de la misma. El paso del tiempo corre en contra del interés del virus y a favor de la Humanidad. En esta fase realmente no se ha terminado con la enfermedad, sino que se ha disminuido su velocidad de propagación. Para terminar con una enfermedad hay que **erradicarla**, y eso significa **que no haya ningún infectado**.

Son pocas las enfermedades erradicadas[14]; de hecho, todavía hoy existen focos en Madagascar, la República Democrática del Congo y en el Perú de la misma Peste Bubónica que barrió Eurasia en 1348 y que, tarde o temprano, se ha terminado dando en todo el mundo[15] excepto en Oceanía.

3) Precipitar/eliminar el componente no deseado. En la Química que, entre otras, es el arte de las disoluciones, cuando se quiere disminuir la presencia de usa sustancia en una disolución lo que se busca es encontrar el modo de **precipitar selectivamente** ese componente y volverlo al estado sólido. Para ello hay que encontrar otro reactivo, que sea especifico y que forme con el componente que se quiere retirar de la solución un producto que sea insoluble en ella. Si eso se consigue, la operación final de separación será tan sencilla como colar/filtrar la disolución turbia que se forma, para así dejar el precipitado en el filtro y recuperar una disolución homogénea y transparente donde la concentración del elemento que queríamos quitar puede ser inmensamente baja.

Para cualquier operación de extracción o purificación es necesario un reactivo que sea selectivo y que reaccione de algún modo útil (por ejemplo, formando un sólido) con el componente que se quiere retirar (por filtrado mecánico) de la disolución. Para ello, ese nuevo componente debe poder **clasificar** los componentes de la solución es reactivos (que precipitan) y no reactivos (que se van a quedar disueltos).

Infectados y no infectados + inmunes

No se pueden separar cosas que son indistinguibles entre sí, como por ejemplo las partículas elementales[16] o cualquier objeto digital. Por ello, estos días han surgido voces que claman por poder **distinguir a los infectados** (enfermos o portadores asintomáticos) **de los no infectados** (inmunes y no-infectados) y por ello todo el revuelo mediático que hay sobre los ensayos serológicos de las inmunoglobulinas M y G, y la ya famosa y extremadamente precisa "**Polymerase Chain Reaction**", o PCRs para andar por casa.

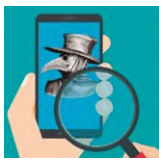
El problema de la PCR es que te dice si un individuo está o no está infectado **en ese momento**, pero nada dice de si puede estarlo después o ya lo ha superado, por lo que habría que estar haciendo pruebas a toda la población y de forma continua. Esa prueba sólo sería una solución si **1)** se hiciesen **simultáneamente** a toda la población confinada dentro de un territorio cerrado (adiabático), e inmediatamente después **2)** se separase y confinase sólo a los que hayan sido identificados como infectados (enfermos y asintomáticos).

Para detectar a los No-infectados e inmunes, además de la PCR hay que recurrir a los ensayos de inmunoglobulinas (IgM y IgG) que determinan la presencia o no de anticuerpos específicos para la Covid-19. Si el resultado es un claro positivo, se puede tener cierta confianza en que ese individuo no volverá a infectarse, al menos durante cierto tiempo.

Aun así, estas soluciones son bastante "académicas" porque se necesitaría **que la tasa de falsos negativos en las prueba de infección fuesen cero**, lo cual sólo se da en las pizarras de las Universidades. En Biología, unos pocos especímenes (asexuados, eso sí) pueden terminar conquistando todo el planeta si hay alimento y hábitat proclive a ello. Casi con que se escape un solo huésped infectado[17], la Pandemia volvería a darse hasta que desaparezcan todos los organismos infectables.

Cuando no se pueden hacer **pruebas eficaces** de algún tipo **a toda la población**, en cualquier enfermedad el único aviso son unos síntomas suficientemente bien marcados. Cuando los síntomas son suficientemente escandalosos o la virulencia de la enfermedad es muy alta, las Pandemias pueden ser controlables porque: **1)** la aparición de síntomas permite una rápida clasificación de los individuos en enfermos y no-enfermos (sanos y asintomáticos), y con ello poder **separarlos antes de que de difunda la enfermedad**, o **2)** una extrema virulencia termina con los pacientes enfermos antes de que el virus haya podido saltar a nuevos huéspedes, como suele ser el caso del Ébola y enfermedades hemorrágicas similares en entornos rurales (en las ciudades sería muy distinto).

En el caso del Covid-19 sus características más significativas para su propagación son dos: **1)** es un virus muy infeccioso, por lo que un solo infectado acaba infectando a un número significativo de individuos con los que interacciona por unidad de



En estos días han surgido dos propuestas en el ámbito europeo que tienen mucho en común, pero con algún detalle diferencial muy interesante. En ambas se trata de sistemas que se consagran al Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), donde lo sustantivo es el Proximity Tracing y con el prefijo Privacy-Preserving pretenden quitarle hierro a la amenaza que supone el primero para la intimidad y derechos fundamentales de todos los que viven en la UE. Lo de Pan-European marca la escala global a la que se quiere llevar este tipo de iniciativas.

[14] Enfermedades erradicadas gracias al uso de vacunas en el Siglo XX: Difteria, Tétanos, Tosferina, Poliomielitis, Sarampión, Rubeola, Parotiditis, Varicela y el Papiloma Humano.

[15] Ver https://www.who.int/csr/disease/plague/Plague-map-2016.pdf

[16] Ver https://en.wikipedia.org/wiki/Identical_particles

[17] Esto es una licencia literaria porque en realidad hace falta una cantidad mínima de patógeno para que tenga alguna posibilidad de subsistir en unas condiciones ambientales dadas.

tiempo, y **2)** el tiempo en el que no presenta síntomas (asintomático) pero es infecciono es muy largo (14-20 días). Por todo ello, su velocidad de propagación ha sido muy alta en sociedades densas, no confinadas y en las que no se practica el aislamiento social.

Hay una tercera característica que no afecta a la propagación de la Pandemia pero que es importante para las sociedades modernas desarrolladas, y es la letalidad y especificidad de la Covid-19 con las personas de edad avanzada o débiles por patologías anteriores, lo cual la catapulta al pódium de las grandes pestes.

Móviles y trazabilidad

A diferencia de Pandemias anteriores, en el mundo actual de las comunicaciones, la globalidad y los dispositivos móviles "*Urbi et Orbe*", han surgido propuestas e incluso exigencias, de que se utilicen los siempre bien identificados teléfonos móviles para trazar el deambular (líquido) de los ciudadanos y ser capaces de identificar a quienes estuvieron cerca de cualquiera de nosotros en el pasado inmediato. El razonamiento, bastante simplista es que, si podemos saber con quiénes interactuó un infectado en los últimos quince días, podremos saber a quiénes ha podido infectar (no necesariamente que lo haya hecho), y con ello marcarlos para su retirada (precipitación) inmediata fuera de la sociedad (fluida).

El sistema parece sencillo y eficaz, pero desde luego se lleva por delante varios derechos fundamentales de las personas por, para empezar, **1)** la pérdida temporal de la libertad de movimiento sin haber cometido ningún delito, **2)** la pérdida (posiblemente definitiva) del derecho a la intimidad al ser directa o indirectamente vigilada de forma continua sin razones penales para ello, y **3)** sufrir las muchas discriminaciones sociales que con seguridad acompañarían al ser marcado dentro de un grupo.

Los promotores de estas medidas dicotómicas dicen que, a falta de razones penales para poder hacer todo lo anterior, bien valen las razones de la Salud Pública (a ver si también se las aplican al tabaco, el alcohol y al sedentarismo que induce la propiedad de un automóvil), y puede que tengan razón puesto que el interés general siempre debe estar por encima del interés individual.

El momento es proclive para que se autoricen, y el pueblo soberano acepte, sistemas de vigilancia si no planetarios, por lo menos nacionales o de ámbito europeo. El problema de fondo es que la autorización seguro que tendría un carácter transitorio, pero los sistemas de información y de vigilancia o monitorización montados para ello no, y vendrían para quedarse.

Tal es el caso que Google y Apple se han asociado para ofertar al mundo su apoyo para el desarrollo de sistemas de trazado de personas a través de los móviles que están por todo el planeta (desarrollado) ya que o corren Android o iOS. Su propuesta ni siquiera pretende disimular y parecer respetuosa con los derechos individuales; ellos proponen meter lo esencial de las aplicaciones de seguimiento y trazado de cada uno de esos artefactos, directamente en el sistema operativo, de manera que sean indisolubles con él. En su propuesta, si quieres tener un smartphone y datos, tienes que aceptar estar potencialmente monitorizado "*around the clock*".

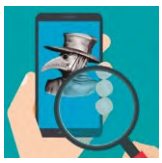
Las tecnologías que se están proponiendo se engloban dentro de lo que se llama Personal Tracking Technologies[18] y son el santo grial de todas las Agencias de Inteligencia, su nuevo *spy dust*. Por otra parte, está el subgrupo de las Proximity Tracing Technologies que no son nada nuevas para el mundo de márquetin dirigido, y que persigue poder pastorear a los clientes que van a sus tiendas o que incluso pasan cerca de ellas o miran sus escaparates.

Muchos alcanzan a sospechar que estas tecnologías y prácticas desde luego afectan y pueden ofender al derecho a la intimidad de las personas, tanto como individuos (libertad de movimiento) como colectividades (derecho de reunión), y ello ha alimentado cierta resistencia en los ámbitos ejecutivo, legislativo y judicial. Sin embargo, con una pandemia ya establecida y con el enemigo vírico instalado en centenares de miles de personas, esas resistencias pueden saltar por los aires y desarrollarse comportamientos totalitarios.

Ya ocurrió algo parecido con Quinto Fabio Máximo cuando, en la víspera de la Batalla de Cannas, fue nombrado Dictador[19] en junio de 217 a.C. tras el desastre (romano) del Lago Trasimeno[20]. Este nombramiento suspendía los derechos ciudadanos y el poder del Senado de la Republica de Roma, pero **aquella dictadura fue muy deseada por la aristocracia romana porque tenían miedo a desaparecer**. En la campaña del año 211 a. C. de la Segunda Guerra Púnica, el ejército de Aníbal llegó y acampó a tan solo tres millas de las murallas de Roma, lo que sembró el pánico en la metrópoli y fue entonces cuando los romanos acuñaron la famosa y amenazante frase "*Hannibal ad portas*"; **tenían miedo y eso lo justificaba todo**.

Suerte tuvo Roma de que Quinto Fabio Máximo realmente no tuviese ansias de poder y, ganada la segunda Guerra Púnica, devolviera el poder al Senado y sus derechos a los ciudadanos. Quinto Fabio es un personaje histórico muy peculiar ya que fue dictador en dos ocasiones, y en los dos casos abandonó la dictadura sin que nadie le presionase para ello. Otro ejemplo posterior y muy distinto fue el de Julio César, que llegó a ser nombrado dictador permanente por sus devotos, y optó por liquidar la República e instaurar el Imperio presidencialista, que se mantuvo después de su asesinato.

Dicho de otro modo, no es de paranoicos o conspiranoicos pensar que el establecimiento ahora de un sistema de monitorización con la excusa de la Pandemia del Coronavirus, hará que se levanten estructuras y sistemas de monitorización y vigilancia automáticos y nada democráticos, que terminen durando más que el propio virus. La posibilidad de poner en marcha sistemas de monitorización continua, universal y automática atenta directamente contra las esencias del sistema democrático y los derechos humanos fundamentales.



Bien puede pensarse que el establecimiento ahora de un sistema de monitorización con la excusa de la Pandemia del Coronavirus, hará que se levanten estructuras y sistemas de monitorización y vigilancia automáticos y nada democráticos, que terminen durando más que el propio virus. La posibilidad de poner en marcha sistemas de monitorización continua, universal y automática atenta directamente contra las esencias del sistema democrático y los derechos humanos fundamentales.

[18] Ver https://behavioranalyticsretail.com/technologies-tracking-people/ y https://medium.com/@RonnyMax/12-technologies-to-track-people-f39d9473c1ae

[19] Un dictador en el Roma era un magistrado de la República al que se le confería la plena autoridad del Estado para hacer frente a una emergencia militar o para emprender una tarea específica de carácter excepcional. Todos los demás magistrados estaban subordinados a su *imperium* y la posibilidad de que los tribunos de la plebe vetaran sus acciones o de que el pueblo apelara contra ellas era muy limitada.

[20] Ver https://en.wikipedia.org/wiki/Battle_of_Lake_Trasimene

Sin embargo, con el "*Covid ad portas*" la idea de poder discriminar entre infectados, infecciosos y gente sana resuena bien dentro de una sociedad asustada que no recuerda que **no se puede discriminar a las personas por cuestiones de salud**. La idea de "*cortar las cadenas de propagación del virus*" le suena bien a una mayoría asustada, poco informada, poco formada y en estado de shock[21], por lo que nuestra sociedad global podría estar a punto de comulgar con que "*el fin justifica los medios*", que tanto daño ha hecho siempre.

Iniciativas de monitorización automática

En esta tesitura han surgido varias iniciativas dirigidas a la monitorización automática de las proximidades de las personas y la Comisión Europea ha tenido que salir a la palestra para dar recomendaciones[22] de cómo deberían hacerse estos sistemas si se quiere seguir cumpliendo con las leyes europeas, especialmente las de privacidad.

En estos días han surgido dos propuestas en el ámbito europeo que tienen mucho en común, pero con algún detalle diferencial muy interesante. En ambos casos se trata de sistemas que se consagran al Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), donde lo sustantivo es el *Proximity Tracing* y con el prefijo *Privacy-Preserving* pretenden quitarle hierro a la amenaza que supone el primero para la intimidad y derechos fundamentales de todos los que viven en la Unión Europea. Lo de *Pan-European* marca la escala global a la que se quiere llevar este tipo de iniciativas.

En el trazado de proximidad se busca generar **indicios digitales** que permitan, *a posteriori*, reconstruir con quien se ha estado dentro de un radio de acción (algunos metros) y durante un cierto tiempo (algunos minutos), lo que pone de manifiesto algún tipo de relación entre ambas personas y, según el baremo/algoritmo que se acuerde para ello, establecer una probabilidad de infección entre ellas.

Ambas propuestas tienen elementos en común y se organizan en cuatro fases:

1. Instalación. Se instala una aplicación específica en el teléfono móvil del ciudadano y cada una de ellas, en su instalación y de forma local, genera un **valor secreto del cuál va a ir derivando una serie de claves efímeras**, cada cierto tiempo, y las radiará por Bluetooth de forma que actuaran como identificadores de ese ciudadano. Si ese secreto realmente se genera al azar, en secreto y de forma homogénea entre todos sus posibles valores, nadie excepto esa aplicación podrá saber cómo generar las identidades efímeras que van a estar irradiando por Bluetooth para todo el que quiera escucharla. **Si ese número no es secreto e inimaginable, la privacidad de todo el sistema desaparece**.

2. Operativa Diaria. Cada teléfono móvil radia a todos los que tiene alrededor el identificador efímero que le corresponde en ese momento del tiempo. A la vez, ese mismo teléfono escucha y toma nota de los identificadores de otros teléfonos que logra oír por encontrarse en su vecindad. La intensidad y sensibilidad de las radios Bluetooth determinan la distancia efectiva de esa vecindad.

Cada aplicación cambia su identificador efímero cada cierto tiempo, por ejemplo cada 5 minutos, lo que supondrían 288 identidades efímeras distintas al día para cada individuo/teléfono. La generación de esos identificadores es criptográfica, y puede de hacerse que sea razonablemente difícil descubrir los identificadores pasados y futuros a partir de un conjunto de identificadores conocidos. Dicho de otra forma, la próxima vez que te cruces con esa misma persona, su identificador será otro y que, aparentemente, no tiene nada que ver con ninguno de los ya vistos, ni con los que se podrán ver más adelante.

La Agencia Española de Protección de Datos ha tenido que tomar posición sobre las tecnologías propuestas y no le ha quedado más remedio que establecer públicamente que ninguna de ellas respeta y protege realmente los datos personales. Al margen, claro, de que puedan presentar vulnerabilidades aprovechables.

3. Gestión de los Infectados. Si una autoridad sanitaria confirma que un ciudadano ha resultado infectado, ésta emite un *token* que autoriza/capacita a la aplicación de ese usuario para subir sus identidades efímeras de los últimos días, a un servidor accesible para todos (publico) o a unos pocos, y aquí está la diferencia esencial entre los sistemas centralizados o descentralizados.

Con la subida de sus identidades efímeras, el usuario muestra sus cartas al sistema y se declara infeccioso, a la vez que da permiso explícito para utilizar esa información para calcular el riesgo de infección en el resto de usuarios. **Este índice de riesgo se calcula para todos los demás usuarios del sistema** y marcará quiénes sí y quiénes no habrán podido haber sido infectados por quien entrega sus identidades efímeras.

El que publica estará perfectamente identificado frente al servidor; sin embargo, lo que se publica para todo el mundo son las identidades efímeras, por lo que el recién identificado paciente sigue siendo anónimo para todos los demás usuarios. Si el que publica no estuviera bien autenticado frente al servidor, se podrían perpetrar ataques como **1)** los de publicar identificadores aleatorios, que envenenarían el sistema restándole eficacia y sensibilidad, ya que aumentaría la probabilidad general de que cualquiera pueda ser considerado infectado potencial, o **2)** que alguien siga a alguien durante un cierto tiempo y luego mande los identificadores que haya recabado, como identificadores de infecciosos; con esto es muy probable, prácticamente seguro, que en la evaluación del riesgo causado por esa persona acosada va a salir el confinamiento urgente y automático de todos los que hayan estado en su vecindad ya que, en ese caso, se han metido todas sus papeletas en el sistema. Sería una forma fácil de confinar a cualquiera y a sus allegados.

Los identificadores efímeros que se publican son los que han identificado a ese paciente infectado a través de su aplicación en el teléfono móvil durante un determinado intervalo de tiempo, por ejemplo, de cinco a catorce días antes de que se le haya diagnosticado como portador del virus Covid-19.

En principio, esta liberación de identidades efímeras no permite identificar concretamente al paciente infectado porque, en principio, todos los datos derivan de una **semilla secreta y aleatoria** que no tiene nada que ver con el titular del móvil en el que se ejecuta. Sin embargo, **este anonimato desaparecería si esa semilla dejase en algún momento, presente o futuro, de ser secreta o no fuese generada realmente al azar**.

Todos móviles que contengan alguna

[21] Ver https://es.wikipedia.org/wiki/La_doctrina_del_shock , Naomi Klein: "*The Shock Doctrine: The Rise of Disaster Capitalism*". Macmillan USA. (2008). ISBN-13: 978-0312427993

[22] Ver https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670, https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf y https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_670/IP_20_670_EN.pdf

Busque o escriba un comando

Actividad
Chat
Equipos
Calendario
Llamadas
Archivos
...

08:59 | Solicitar control

Aplicaciones
Ayuda

Z A B

Chat de la reunión

15:02
Buenas tardes equipo, os envío el enlace al borrador del informe sobre el Pentest al entorno Cloud realizado esta semana a Petrolnovalty. Revisadlo por favor, y lo comentamos en unos minutos.

B Bob 15:02
Gracias, le echamos un vistazo... ;)

A Alice 15:09
Puff, otra filtración de claves de acceso a los buckets de S3, todos los datos comprometidos...

15:12
Es crítico y ya van varias, Alice. ¿Te animas a explicar cómo solucionarlo en el blog de www.flu-project.com? Así, tal vez podamos visibilizar el problema...

Escribe un mensaje nuevo

de esas identificaciones en sus ficheros de evidencias recogidas, sólo podrán haberlas conocido **1)** porque hayan estado en la vecindad de teléfono móvil emisor que sí sabe generarlas, lo cual está bien, o **2)** porque alguien se las haya reenviado a modo de puente (*bridge*), lo que sería un serio *bug* del sistema.

4. Modelo Centralizado. Consiste en que todos y cada uno de los ciudadanos **previamente identificados** suban, por ejemplo cada día, a un único Servidor Central (Administración, Autoridad Sanitaria y/o Empresa) los datos de los **identificadores exógenos que han oído ese día**. Si los usuarios no se identificasen en la subida de datos, el sistema podría ser víctima, entre otros, de un ataque DoS por **envenenamiento de la base de datos** con identidades que realmente no representan a nadie y que nadie ha podido oír/registrar, por lo que la identificación sería necesaria y ahí desaparece en anonimato de cada participante.

Al identificar quién hace el depósito, los que tienen acceso a ese servidor identifican todas y cada uno de las identidades efímeras que (supuestamente) ha oído y registrado cada ciudadano. Solo sabiendo cuantas identidades entrega cada cual, ya podemos saber qué tipo de vida hace, si son pocas identidades, ello apuntará a un/a solitario/a, y si son muchas, apuntaran al "*hombre de la multitud*"[23]. Si el usuario pudiese alterar la aplicación que le representa, quizás podría introducir identidades efímeras falsas, lo que "diluiría" su contacto con todos los que realmente ha frecuentado. Esa dilución podría afectar, a la baja, el cálculo de su riesgo de haber sido infectado y librarse del confinamiento.

En este punto, el que accede al servidor no sabe con quienes ha estado cada uno de los participantes, pero en cuanto un ciudadano concreto es calificado como infeccioso, y declara cuáles han sido sus identificadores efímeros, el que tenga acceso a esa base global de datos, podrá identificar qué otros usuarios concretos han estado en su vecindad, ya que habrán subido en sus cargas periódicas alguna o algunas de las identidades ahora desveladas.

Así quedan identificados con nombre y apellidos tanto el ciudadano infeccioso, como los ciudadanos que podrían haberse infectado con él/ella. La idea de estos promotores de este tipo de **sistemas de alerta temprana** es avisar a los sospechosos de estar infectados y someterlos a cuarentena ¿forzosa? (modelo coreano).

5. Modelo Descentralizado[24]: En este caso, los únicos datos que se suben a un servidor central y abierto al público son las identidades efímeras de ciudadanos que han sido diagnosticados como infecciosos. En este servidor sólo se mantienen accesibles los indicios digitales de los últimos días, pero al ser de acceso público, cualquiera puede reconstruir (backup) la base de datos completa, con todos los identificadores desde que se puso en pie el sistema (**¡Internet nunca olvida!**).

En este escenario, es cada usuario el que tiene que descargarse de ese servidor público todos los identificadores efímeros de todos los pacientes en activo y clasificados como infecciosos (o actualizar su copia local). Lo que hace a continuación cada usuario del sistema es ver si en esa lista están algunos de los identificadores efímeros que su aplicación recolectó de su vecindad. Si encuentra alguno podrá, mediante un baremo que está por aclarar, determinar la probabilidad de haberse infectado, pero en ningún momento sabrá si fue por un donante o por varios, ni cuál es la identidad de los mismos, ya que sólo conoce identidades efímeras.

Si existe el **riesgo de haber sido infectado**, el que se acaba de enterar de ello deberá decidir qué hacer; (1) no decir nada y seguir como siempre, con lo que todo el sistema gana en el respeto a los derechos humanos en cuanto a no ser discriminado por cuestiones de salud, pero pierde como herramienta de monitorización de pandemias, o (2) ponerse en manos del sistema de salud para que después de su triage[25], decida o aconseje sobre su confinamiento y/o aislamiento. Para establecer el grado de respeto real de los derechos humanos individuales es necesario saber si la decisión de confinamiento sería voluntaria u obligatoria (modelo coreano).

Nadie lo comenta pero puede ser **que la aplicación delate automáticamente el resultado de la evaluación de riesgo** de cada ciudadano al servidor central, en cuyo caso las consecuencias de la posible infección escapan de la voluntad y civismo del ciudadano mismo. En este caso, el sistema **es descentralizado pero no es anónimo** y actúa como una espada de Damocles sobre todos y cada uno de los ciudadanos que participen en el sistema de seguimiento.

Consumo en comunicaciones y capacidad de almacenamiento digital de datos

En ninguna de las fuentes consultadas hasta el momento se ha tratado el asunto del tamaño que supone la operación de trazado de la adherencia en la población[26] de la Unión Europea (513,48 millones), en España (46,94 millones) o incluso en las comunidades autónomas más afectadas por el Covid-19, que son la de Cataluña (7,57 millones) y la de Madrid (6,64 millones).

Si hacemos caso a los expertos estadísticos y se lograse **1)** que un 60% de la población participase en este experimento sociológico, **2)** que se genera una identidad efímera por persona y hora, **3)** que el periodo de retención fuese solo de 14 días, estaríamos hablando de que, en la UE de 28 miembros, el volumen de identidades efímeras seria de 103,5 mil millones, en España serían de 9.463 millones de identidades efímeras, 1.526 y 1.343 millones en Cataluña y en la Comunidad de Madrid, respectivamente.

Supongamos ahora que **se infecta el 30% acumulado de la población**, que es un valor muy probable para una primera ola de la Pandemia, pero en realidad los estudios serológicos dicen que en España ha sido netamente inferior al 10%; y que lo hace **en seis meses** (183 días). Si las medidas de control de la Pandemia consiguiesen frenar su crecimiento exponencial intrínseco y hacer que la velocidad de infección fuese constante, estaríamos hablando de 842 mil infecciones diarias en la UE, de **77 mil infecciones diarias en España**, y de 12 mil y 11 mil infecciones diarias en Cataluña y en la Comunidad de Madrid.

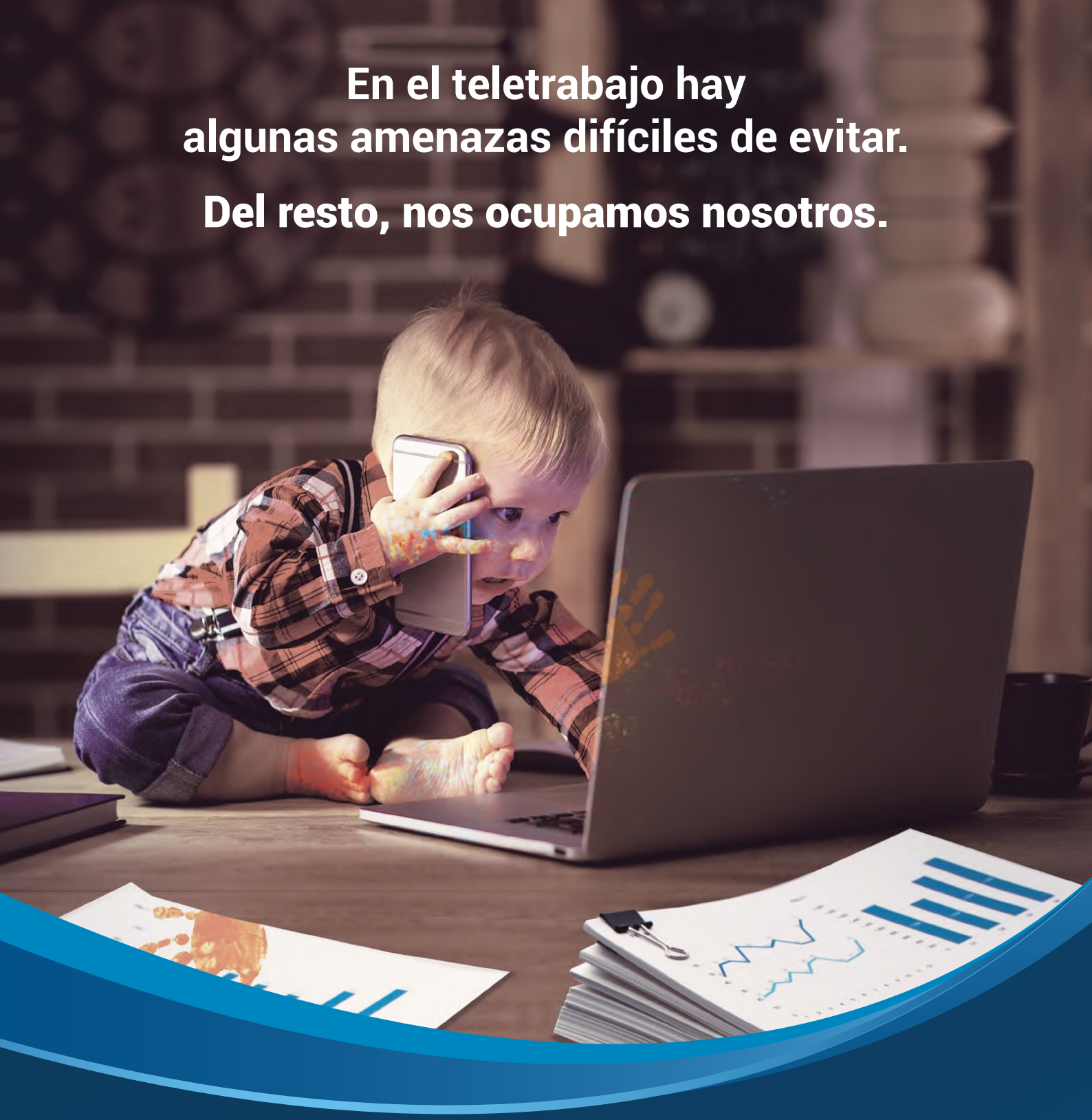
En el escenario UE-28, tanto el modelo centralizado como descentralizado, requieren que cada ciudadano europeo (513,48 millones) consulte, en cada actualización diaria de su riesgo de contagio, 283 millones de identidades efímeras de contagiados comprobando a ver si se ha cruzado con alguna de ellas en los últimos 14 días. En lo que toca a España esas consultas serian 25,9 millones, o 4,2 y 3,7 millones respectivamente si los movimientos estuvieran restringidos al interior de las comunidades de Cataluña y Madrid.

En el escenario España y siguiendo el modelo centralizado, los ordenadores de la autoridad pertinente tendrían que comparar 25,8 millones de Identidades de infectados con los registros entregados por cada uno de los 28,2 millones de personas participantes en el experimento. El resultado de esa comparación sería un total de $7{,}28 \times 10^{(14)}$ cruces de información. En cuanto un afectado publicase sus identidades efímeras, la autoridad central tendría identificadas a todas las personas que se

[23] Ver https://en.wikipedia.org/wiki/The_Man_of_the_Crowd
[24] Ver https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/
[25] El triage es un sistema de selección y clasificación de pacientes en los servicios de urgencia, basado en sus necesidades terapéuticas y los recursos disponibles. Esto permite una gestión del riesgo clínico para optimizar la atención y la seguridad de las personas.
[26] Datos correspondientes al año 2019.

En el teletrabajo hay algunas amenazas difíciles de evitar.

Del resto, nos ocupamos nosotros.



En **S2 Grupo** somos conscientes de que el teletrabajo ha llegado para quedarse y es fundamental que se realice en entornos ciberseguros. Por este motivo, le proponemos una solución acorde a las necesidades de su negocio, que permitirá a todos y cada uno de los empleados de su organización teletrabajar de una forma robusta y ágil, sin que suponga un problema en la experiencia de usuario. Además, tendrá a su disposición un CERT con más de 200 profesionales especialistas, cuyo objetivo será que su organización esté siempre a salvo de los riesgos actuales.

Es el momento de actuar y no quedarse atrás.

Póngase en contacto con nosotros en info@s2grupo.es y nos pondremos en marcha.

Síguenos en: • @s2grupo • s2grupo.es

S2 GRUPO

Anticipando un mundo **ciberseguro**

han cruzado con él/ella en los últimos 14 días, y ahí están todos sus círculos sociales y familiares, además de los laborales y de ocio.

En el escenario España y siguiendo el modelo descentralizado, cada uno de nuestros teléfonos móviles tendría que descargarse y mantener actualizados, los datos correspondientes a 9.463 millones de identidades efímeras (que supondrían 303 GB si cada ID efímera fuese de tan sólo 32 bytes) y ver si entre ellas están las que ese teléfono haya recopilado en nuestro deambular social durante los últimos 14 días.

Con estos resultados está claro que los modelos propuestos suponen un consumo en comunicaciones y una capacidad de almacenamiento digital de datos muy considerable, y quizás por ello no sean realizables. Está claro que los teléfonos móviles de los españoles no suelen tener 303 GB de memoria interna ni tolerarían consumo diario de 827 MB para la descarga diaria de los 77 mil identificadores efímeros de los nuevos ciudadanos contagiados identificados.

Atendiendo al volumen de datos que generan, los modelos propuestos de *Personal Tracing* sólo serían posibles (1) si fuesen **centralizados** (y con recursos ilimitados), o (2) si la **movilidad** de los ciudadanos estuviese **muy restringida** y, por ejemplo, cada ciudadano no puede salir de su correspondiente Comunidad Autónoma.

Con estos cálculos es fácil ver que este tipo de sistemas sólo se han implementado cuando el número de participantes no es tan amplio (12% en Corea del Sur) y no alcanzan el que se precisa (60%) desde el punto de vista sanitario, o cuando la movilidad de la población está seriamente restringida, lo cual reduce el grado de anonimato de sus usuarios.

Objetivo: la identificación continua

La Agencia Española de Protección de Datos, ha tenido que tomar posición sobre estas tecnologías[27] y no le ha quedado más remedio que establecer públicamente que **ninguna de estas tecnologías respeta y protege realmente los datos personales**.

Hasta aquí los detalles técnicos de los que se ha hablado y sobre los que se ha querido que se hable. Lo que no he visto comentar es que los sistemas de comunicación digital están plagados de identificadores únicos. Existen los Machine Access Code (MAC) que son únicos para cada dispositivo de red, y los Universal Unique Identifications (UUID) del protocolo Bluetooth. Esos elementos son esenciales para establecer la comunicación (sea del tipo que sea) por lo que las aplicaciones podrían guardar también de forma no documentada, dichos identificadores; por lo que el baile de identidades efímeras sería un paripé, una columna de humos para tapar lo que realmente se está haciendo, identificar continuamente a la gente y a sus entornos mediante sus móviles.

Otro de los detalles que no parecen haber sido entendidos es el por qué de la sorprendente unión temporal de intereses de Apple y Google para supuestamente colaborar con la lucha contra el Covid-19. Esa operación lo que realmente representa es aprovechar la oportunidad que aporta la calamidad generalizada para hacer saltar una medida de seguridad que hasta ahora hemos (casi siempre) disfrutado. La medida básicamente consiste en que el dueño del móvil puede decir qué aplicaciones acceden a todos sus servicios (red, ubicación, sensores, etc.) y que ello se haga desde una aplicación que corra en primer plano y este bajo su control y voluntad mediante una interfaz adecuada.

Para el combate del Covid-19 alguien ha colado inexplicadamente que la aplicación "*corra continuamente en segundo plano*" (en *background*) y para ello es necesario que los dueños de los sistemas operativos habiliten su acceso directo a esos servicios básicos.

Hasta ahora eso se hacía con aplicaciones espías muy sofisticadas (*Remote Access Trojans* o RATs), que engañan tanto al sistema operativo (haciéndose *root*) como al usuario (siendo invisible y corriendo en segundo plano); pero a partir de ahora ya no van a hacer falta, pues su función la hace directamente el sistema operativo. Quizás desde la última actualización de nuestros teléfonos móviles ya no seamos realmente soberanos para decir qué se comunica, a quién se comunica y qué se mide/ve/oye a través de nuestros teléfonos.

Hace años perdimos la capacidad de quitarle la batería a cualquier teléfono móvil, y con ello **perdimos la potestad de poder apagarlos**, con esta modificación **perderíamos la posibilidad de decidir lo que nuestro teléfono dice de nosotros** y a quién se lo dice.

Atendiendo **1)** a este descontrol efectivo de lo que hace el móvil, **2)** al no-anonimato del hardware que utilizamos, **3)** a su difícil escalamiento que hace que estas propuestas de trazado de personas **4)** no sean realmente útiles para lo que se declara –combatir un Pandemia–, y **5)** que no respeten necesariamente la protección de datos personales, **estas aplicaciones de vigilancia deberían prohibirse**, especialmente en una época donde, en todas partes, reina la preocupación y algunas veces el miedo.

No dejemos que el miedo de ahora abra la puerta a lo que se ha propuesto porque en el fondo son sistemas de vigilancia continua, global y automática que tanto gustan a los sistemas autoritarios (no necesariamente gubernamentales) para poder hacer que todos sus enemigos sean siempre pequeños, sean siempre individuales. Las mujeres y hombres libres de Sion no tendrán teléfonos móviles.

Hay que tener cuidado porque el miedo es un potente disuasor, pero casi siempre es una compañía muy peligrosa. **Por miedo uno es capaz de aceptar cualquier cosa**. Como decían las sacerdotisas Bene-Gesserit[28] en la novela *Dune*[29] de Frank Herbert: "*El miedo mata la mente. El miedo es la pequeña muerte que conduce a la destrucción total*"[30].

No dejemos que el miedo de ahora abra la puerta a lo que se ha propuesto porque en el fondo son sistemas de vigilancia continua, global y automática que tanto gustan a los sistemas autoritarios (no necesariamente gubernamentales) para poder hacer que todos sus enemigos sean siempre pequeños, sean siempre individuales. Las mujeres y hombres libres de Sion no tendrán teléfonos móviles. ■

[27] Ver páginas 8 a 10 de https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf
[28] Ver https://en.wikipedia.org/wiki/Bene_Gesserit
[29] Ver https://en.wikipedia.org/wiki/Dune_(novel)
[30] Frank Herbert. "*Dune*", Ed. Debolsillo. Colección: Las crónicas de Dune (2017). ISBN-13: 978-8497596824
[31] Zion, en español Sion, es una ciudad subterránea y ficticia de las películas de Matrix. Es la última ciudad humana en el planeta Tierra, producto de la guerra de la humanidad contra las máquinas que dijeron formas de vida inteligente y artificial que pugnaban por dominar el mundo. Ver https://en.wikipedia.org/wiki/Zion_(The_Matrix)

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

POR HAUNT KEEPER

TELETRABAJO BLINDADO

UN DISPOSITIVO WI-FI CONECTADO AL ROUTER DOMÉSTICO DISEÑADO PARA SECURIZAR TOTALMENTE LAS REDES DOMÉSTICAS

HAUNT KEEPER

- ✔ Haunt Keeper es **plug&play** real y no requiere configuración previa
- ✔ No necesita ningún tipo de hardware adicional
- ✔ Respaldado por el soporte de Wise Security Global

HAUNT KEEPER HOME	HAUNT KEEPER PRO	HAUNT KEEPER ENTERPRISE
(19,95 € / MES)	(24,95 € / MES)	(29,95 € / MES)

haunt-keeper.com

info@haunt-keeper.com

+34 910 700 549

by wisesecurity GLOBAL

La visión de DXC en un contexto de amenazas creciente

DXC Technology es una multinacional puntera en la provisión de servicios de IT, que cuenta hoy con más de 130.000 empleados en más de 70 países. En materia de Servicios de Seguridad, la compañía dispone de más de 4.000 empleados en todo el mundo, con 10 SOCs distribuidos a escala global donde lleva entregando servicios gestionados desde hace más de 30 años. Esto nos ha permitido conocer de primera mano las exigencias concretas (y su evolución) en materia de ciberprotección y adaptarse a ellas para garantizar ese proceso de transformación. En Iberia, DXC cuenta con un equipo de más de 150 profesionales en ciberseguridad altamente especializados y ubicados en 5 localizaciones (Madrid, Barcelona, Avilés, Zaragoza y Lisboa).

Mikel Salazar / Rubén Muñoz

En el contexto de la transformación digital, muchas organizaciones se apresuran a modernizar su infraestructura de TI sin una comprensión de las implicaciones del riesgo de la transformación digital de sus negocios. El panorama de amenazas digitales está evolucionando rápidamente aumentando en complejidad y los ciberdelincuentes están intentando explotar cualquier debilidad y vulnerabilidad a medida que buscamos transformar el negocio. El paradigma defensivo ha cambiado; el escenario de movilidad, con la nube acelerando la forma de hacer negocios, y la nueva ola de IoT soportada por el progresivo despliegue del 5G, han hecho que el perímetro se haya difuminado.

Adicionalmente, la situación generada con la crisis de la pandemia de COVID-19 ha llevado esto al extremo generando la tormenta perfecta. En este entorno tan complejo, en DXC nos apoyamos en la combinación de **dos modelos de seguridad** para ayudar a nuestros clientes en su viaje seguro a la transformación digital: *Zero trust* y *Defensa en profundidad.*

Zero Trust representa un cambio radical en el contexto de relación entre objetos accesibles y usuarios demandantes de acceso. El principio fundamental es **nunca asumir un escenario de confianza, incluso si el usuario es confiable**. Esto se consigue robusteciendo la fase de autenticación del usuario, al mismo tiempo que se añade como variable de dicho proceso de autenticación un elemento externo al usuario, como es el dispositivo desde el que se intenta autenticar.

Incluso tras este nuevo proceso de autenticación, Zero Trust incide nuevamente en la fase de autorización buscando minimizar el posible impacto de un usuario por defecto no confiable, otorgándole los privilegios mínimos necesarios para realizar las acciones solicitadas. Por último, el modelo impone una capa de verificación que permita detectar acciones indebidas o anomalías en el comportamiento por parte del usuario.

DXC ha utilizado su experiencia en la transformación a la nube para adaptar al nuevo paradigma un modelo de seguridad que durante años ha sido la base de las arquitecturas defensivas.

Defensa en Profundidad es un modelo que despliega diferentes capas de protección, partiendo de la base de un diseño y gobierno de la seguridad efectivo. Dichas capas articulan **medidas de protección escalonadas y complementarias** desde los contextos más "externos" a la nube, como pueden ser los puntos de conexión a la misma y el control del acceso (y aquí entrelazamos con Zero Trust), hasta el corazón de todo entorno tecnológico, la información.

Debido a la variedad de estrategias cloud (IaaS, PaaS, SaaS) y las correspondientes diferencias en la compartición de responsabilidades entre proveedor y cliente en la nube en cada una de ellas, DXC ha aprovechado su experiencia para diseñar distintas arquitecturas de referencia de defensa en profundidad que puedan adaptarse a la complejidad de cada cliente.

SEGURIDAD: solo con un *partner* de confianza

El objetivo de DXC es convertirse en el socio de seguridad de sus clientes, proveyendo un *end to end* en su hoja de ruta segura de una manera agnóstica y totalmente personalizada según las necesidades:

1. Proveer **advisory para revisar su estrategia de seguridad**, comprender su postura y crear una hoja de ruta para ayudarlo a realizar una transformación segura de su negocio, minimizando el riesgo de una manera eficiente y efectiva.
2. Optimizando su postura de seguridad actual con soluciones y proyectos específicos para los desafíos clave de la seguridad, apoyándonos en los cuatro dominios de transformación de la seguridad: **Identidad digital, Ciberdefensa, Infraestructura Segura y Protección del dato.**
3. Proveyendo **servicios gestionados de seguridad** desde nuestro SOC de Iberia, respaldados por la inteligencia global de nuestra red de 10 SOCs a lo largo de los 5 continentes.

Identidad Digital

La gestión de la identidad es un habilitador clave para la transformación digital**.** En un momento en el que el robo de credenciales está en la diana de los ciberdelincuentes es vital gestionar y verificar el acceso a toda la información de la empresa, controlar las identidades privilegiadas y estar protegidos mediante controles de acceso multifactor. En DXC estamos especializados en la implementación y servicios gestionados de soluciones alineados con Zero Trust, como son la **gestión de la identidad, identidad privilegiada y el control de acceso** (MFA, acceso condicional…). DXC cuenta con numerosas referencias en la implementación de proyectos complejos de Identidad Digital, así como servicios gestionados

desde su SOC, que aseguran la evolución de estos sistemas, así como el mantenimiento de las diferentes plataformas.

Ciberdefensa

Nuestros servicios de ciberdefensa permiten prevenir, detectar y responder al actual panorama de amenazas donde observamos un gran incremento, tanto en el volumen como en la complejidad de los incidentes de seguridad:

Concienciación. El empleado es la primera línea de defensa. Gracias a nuestros servicios de concienciación nuestros clientes pueden formarles y prepararles para evitar ser víctimas en las numerosas campañas de *phishing*, o enseñarles a hacer un uso adecuado de la información según el marco normativo y legal vigente.

En el ámbito de la **detección y respuesta** contamos con experiencia en la implantación de diferentes soluciones (SIEM, UEBA, anti-Fraude y Vigilancia digital) que permiten a detectar y responder rápidamente a las amenazas. Nuestras operaciones de seguridad inteligentes brindan detección y respuesta proactivas de eventos e incidentes de seguridad, así como gestión y recuperación de incidentes, a la vez que minimizan las interrupciones, daños y pérdidas con los servicios entregados 24X7.

Gestión de **vulnerabilidades en infraestructura (TVM) y aplicaciones (S-SDLC).** Con la implementación de soluciones TVM, nuestros servicios gestionados establecen un proceso mediante el cual se identifican y clasifican las vulnerabilidades de los activos, priorizando y evaluando el riesgo asociado a ellas. Por otra parte, nuestros servicios de ciclo de vida del desarrollo seguro (S-SDLC) permiten asegurar un código sin vulnerabilidades en producción desde las fases de análisis y diseño hasta las fases de puesta en producción, incluyendo el desarrollo de aplicaciones en escenarios DevOps. Esta evaluación conduce a un proceso de eliminación o mitigación de los riesgos detectados.

Automatización, orquestación y respuesta mediante SOAR. Los servicios de ciberdefensa se apoyan en la plataforma GO; se trata de una plataforma SOAR (Security Orchestration Automation and Response) diseñada y desarrollada por la unidad de Ciberseguridad de DXC Iberia, y cuya implementación sigue los siguientes principios básicos: minimizar tiempos de respuesta, ser una plataforma "agnóstica" tecnológicamente, garantizar la escalabilidad y evolución funcional, así como ser una plataforma multicliente que permita consolidar datos de manera efectiva durante la operativa del SOC, pero que garantice el consumo por parte de cada cliente siendo rigurosos desde los criterios de confidencialidad y privacidad.

Infraestructura Segura

Nuestros servicios de infraestructura segura incluyen el diseño, instalación, integración y posterior servicio gestionado en **seguridad perimetral, red, endpoint, aplicaciones, web y protección del correo electrónico**.

Cloud Security. En muchos casos la transición a la nube se puede definir como un viaje inesperado en el que los primeros pasos suelen ser improvisados. Por ello, DXC ha desarrollado un itinerario de seguridad para el viaje a la nube, mediante el cual se asegura esa transición. DXC acompaña con los servicios especializados de **Cloud Advisory,** así como la implementación de soluciones asentadas como el CASB, o más recientes como el CSPM (Visibilidad de postura de seguridad) y CWPP (Protección de cargas).

Protección avanzada del *endpoint* y entornos obsoletos: el panorama creciente en número y tipología de amenazas hace necesaria de una evolución en la seguridad del *endpoint* (EDR), así como como la protección de entornos obsoletos mediante implementación de soluciones de Virtual Patching.

Protección del Dato

El dato es el activo corporativo más valioso. En un ámbito como el actual – y ahora más, si cabe, con COVID19 –, donde el riesgo de fuga de información aumenta con la operación remota y en movilidad, desde DXC podemos ayudar con la implantación de soluciones de **clasificación y prevención de fuga de datos**. Nuestras soluciones y servicios de protección de datos ayudan a desarrollar una estrategia de protección para reducir el riesgo de divulgación no intencional o no autorizada de datos confidenciales y el cumplimiento de las regulaciones y leyes nacionales e industriales relacionadas con la protección de datos.

"SOC AS A SERVICE"

La experiencia de DXC Technology como proveedor global de servicios de seguridad nos ha demostrado que lo que el cliente requiere es un servicio de seguridad que le asegure el cumplimiento y mejora constante de sus indicadores de seguridad, minimizando el impacto en su operativa IT, que sea ágil para adaptarse y habilitar a las nuevas necesidades del negocio y cuya facturación siga un modelo de pago por uso con *drivers* de consumo estándares.

Para cumplir con estas expectativas, es necesario disponer de una plataforma tecnológica de seguridad con cobertura "end to end", que sea lo menos invasiva posible con la arquitectura IT existente en el cliente y con capacidad de crecimiento/decrecimiento bajo demanda en ecosistemas heterogéneos híbridos y multicloud. Toda esta plataforma tecnológica deber ser gestionada de manera efectiva por personal altamente cualificado y entrenado, con un *know how* generado por la experiencia y articulado según procesos definidos a partir de las mejores prácticas del sector.

Buscando cumplir las expectativas del mercado en este sentido, y gracias a la alianza Global con Microsoft, DXC ofrece dentro de su portafolio de servicios una plataforma **"SOCaaS" sobre tecnología Microsoft** (M365 y Azure).

DXC dispone de un equipo humano formado, certificado y con la experiencia necesaria para realizar las implantaciones de las soluciones de seguridad M365 y Azure de Microsoft, así como los servicios gestionados de éstas desde nuestro SOC, siguiendo los modelos de 'securización' más implantados en el mercado (Zero Trust, Defensa en Profundidad) y con un enfoque SecOps integral (orientado a minimizar tiempos de respuesta ante las ciberamenazas, maximizando la eficacia y eficiencia de dicha respuesta). Y todo manteniendo nuestro rasgo distintivo de prestar servicios personalizados y diseñados "a la carta". ■

Mikel Salazar,
Head of Cybersecurity for Iberia
Rubén Muñoz
Cybersecurity Sales Executive

A pesar de ello, el 40% ve la nube pública más segura que sus centros de datos, según un estudio de Oracle y KPMG

Sólo uno de cada diez CISOs confía en que la nube corporativa está bien protegida, viéndose incapaces de seguir, con seguridad, su ritmo de adopción

A medida que las empresas migran sus cargas de trabajo y datos corporativos a la nube para optimizar costes y dar paso a nuevos entornos de trabajo, los responsables de ciberseguridad siguen luchando por mantenerse al día. Y es que aunque el *cloud* se está ganando la confianza de las compañías, en la mayoría existe una brecha importante entre la rapidez en la que se está adoptando y el grado de madurez de los programas de ciberseguridad que la protegen, una situación que está provocando grandes quebraderos de cabeza a los responsables de ciberseguridad.

Así se desprende del informe '*Cloud Threat Report 2020*', realizado por **Oracle** y **KPMG**, para el que han encuestado a 750 responsables de ciberseguridad (CISO) y de TI de organizaciones, tanto del sector público como del privado, de América del Norte (EE.UU. y Canadá), Europa occidental (Reino Unido y Francia) y de Asia-Pacífico (Australia, Japón y Singapur).

En él se destaca que el 40% de las compañías perciben la nube, incluso, más resistente y segura que los sistemas que usan en sus propias instalaciones, un 13% más que en 2019. Sin embargo, nueve de cada 10 encuestados (92%) no confía en que su organización esté bien preparada para proteger estos servicios, especialmente, los de nube pública, los más utilizados por la gran mayoría (en un 88%).

La principal preocupación de los responsables de ciberseguridad y de TI es la capacidad de acompasar el ritmo de adopción de la nube con su capacidad para evaluar y gestionar el riesgo empresarial, y ofrecer la protección adecuada.

Serias dificultades

Por un lado, para el 78% de los encuestados las diferencias entre la infraestructura y las aplicaciones locales y las que residen en la nube requieren un conjunto diferente de políticas y procesos de seguridad. Además, tienen serias dificultades para llevar a cabo un programa adecuado de parcheo para la seguridad de los datos, gestionar los servicios mal configurados y, la mayoría confiesa sufrir una gran confusión en torno a los nuevos modelos de seguridad en *cloud*.

Esta situación está generando que los responsables de ciberseguridad lleguen a "estar más preocupados por la protección de la información de su empresa, sobre todo, la financiera y de propiedad intelectual, que por la seguridad de su propio hogar o del país", destaca el estudio. A ello se suma que, para muchos encuestados, existe cierta inquietud cuando se trata de confiar en los proveedores de servicios en la nube (CSP). En concreto, el 80% de los participantes confesaron su preocupación por que los proveedores de servicios en la nube con los que hacen negocio se conviertan en sus competidores. "Ahora que los clientes se han acostumbrado a la seguridad de las nubes publicas, los responsables de ciberseguridad y de TI quieren asegurarse de que los CSP se mantengan vigilantes y comprometidos con fuertes medidas de ciberseguridad", destaca el informe.

Responsabilidad compartida

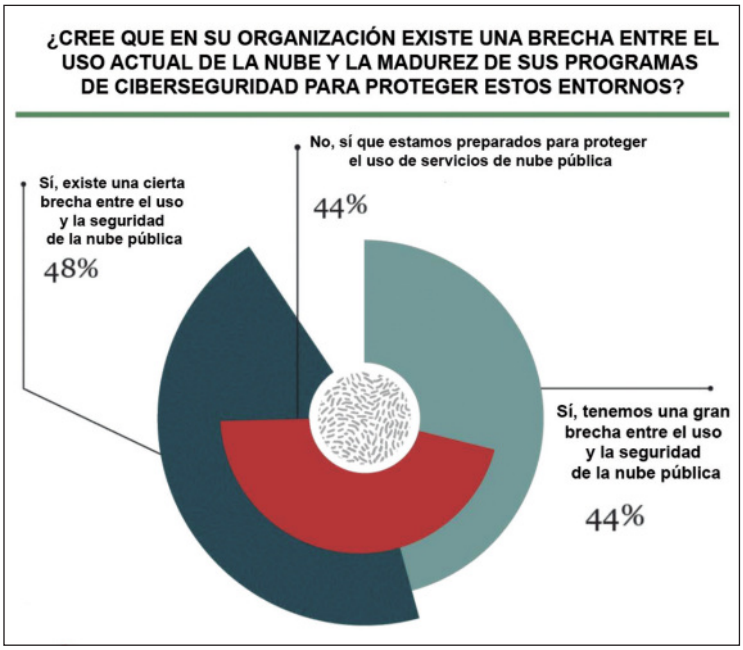
Comprender la seguridad en la nube como una responsabilidad compartida es fundamental para proteger estos entornos y gestionar sus riesgos, especialmente, a la hora de dividir el trabajo entre el proveedor de servicios y su suscriptor. Pero lejos de conseguirlo, el modelo de seguridad compartida es cada vez más confuso, sea cual sea el tipo de servicio en la nube, aunque el 67% de los encuestados señaló que SaaS es el más ambiguo, con un aumento del 13% cada año. Solo el 8% afirmó que comprende bien el modelo de responsabilidad compartida de protección en la nube para todos los tipos de servicios, en comparación con el 18% en 2019.

Seguridad primero

Para abordar estas preocupaciones de seguridad y problemas de confianza, los investigadores del estudio señalan que es esencial que los CSP y los equipos de ciberseguridad y TI trabajen juntos para construir una cultura de 'Seguridad primero' (*Security First*). Esto incluye contratar, capacitar y mantener a los profesionales cualificados en ciberseguridad, así como mejorar constantemente los procesos y las tecnologías para mitigar las amenazas en un mundo digital en expansión. En este sentido, el 69% de las organizaciones considera que su CISO responde de manera reactiva y se involucra en proyectos de nube pública solo después de que ha ocurrido un incidente. Además, el 73% mostró su preocupación por tener que contratar un CISO con más habilidades de seguridad en la nube. De hecho, "más de la mitad de las organizaciones (53%) ha sumado un nuevo rol, el Oficial de Seguridad de la Información Comercial (BISO), para colaborar con el CISO y ayudar a integrar la cultura de seguridad en el negocio", puntualiza el informe.

La adopción de herramientas de automatización inteligente para cubrir la brecha de habilidades también está en la hoja de ruta de inversión de las empresas a corto plazo, según los encuestados. Cabe resaltar en este sentido que el 88% de los profesionales de ciberseguridad y TI considera que, en los próximos tres años, la mayoría de su nube utilizará parches y actualizaciones inteligentes y automatizadas para mejorar su protección.

Asimismo, el 87% ve las capacidades de Inteligencia Artificial y *Machine Learning* como una prioridad en sus futuras adquisiciones para protegerse mejor contra el fraude, el *malware* y las configuraciones erróneas. A ello se suma que un 46% indica que adoptar un entorno DevSecOps (que integra la ciberseguridad en los procesos de Desarrollo y Operaciones –DevOps–), ofrece los medios necesarios para automatizar las mejores prácticas de gestión de las configuraciones de la nube y reducir la brecha en la preparación de las empresas para su protección. ■



THALES

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

CYBER SECURITY EXCELLENCE AWARDS WINNER 2019

ISO 27001:2013 CERTIFIED

AICPA SOC

GDPR Ready

cpl.thalesgroup.com

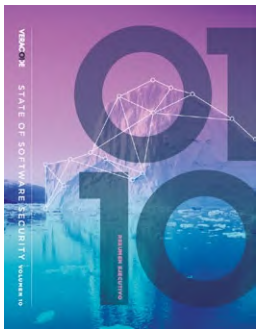
Ajoomal Asociados
Your Security, Our Responsibility

Contacta con nosotros: +34 91 382 17 10
www.ajoomal.com \ laura.fernandez@ajoomal.com

Un escaneo, casi diario, de software reduce por cinco la posibilidad de sufrir fallos de seguridad, según el último estudio de Veracode

El tipo de lenguaje de programación, el área de desarrollo del software y la capacitación del equipo humano, claves para evitar vulnerabilidades

Se calcula que cualquier software comercial tiene, de media, 64 vulnerabilidades. Algo preocupante teniendo en cuenta que, también de media, se tardan 59 días en ser detectadas y solucionadas. La buena noticia es que los desarrolladores cada vez aplican más el concepto de 'seguridad por defecto'. Así lo constata la décima edición del estudio de Veracode sobre el 'Estado de la Seguridad del Software'. ¿Su conclusión? Se ha mejorado mucho en la última década… pero "aún queda mucho por hacer".



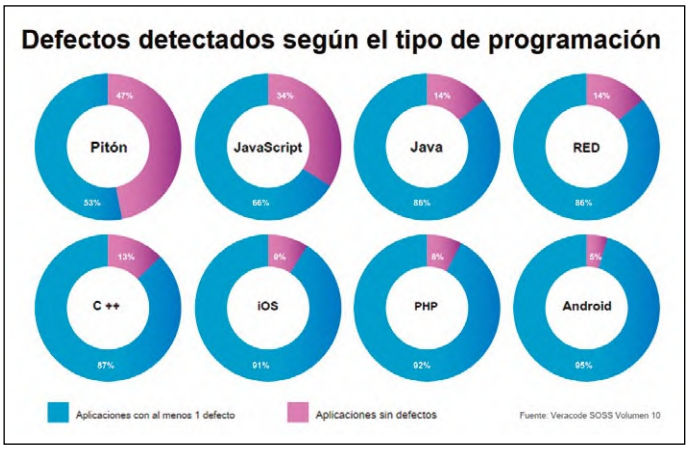
En 2011, **Marc Andreessen,** fundador de **Netscape,** escribió un artículo en el **Wall Street Journal** en el que anunciaba que "el software se está comiendo el mundo". Casi una década después se ha constatado esa predicción, aunque, en el caso de la ciberseguridad, no ha ido acompañada de código con la robustez y ciberprotección esperadas. Por eso, la importancia de enfoques cada vez más populares como el DevSecOps (Desarrollo-Seguridad-Operaciones). "Las consecuencias de no integrar la seguridad al principio del ciclo de vida del desarrollo nunca han sido más evidentes", destaca la firma **Veracode** que ha publicado la décima edición de su informe anual el *'Estado de Seguridad del Software* (SOSS)", en el que ha analizado 85.000 aplicaciones de compañías grandes y pequeñas, proveedores de software comercial, proyectos de código abierto y subcontratistas de software.

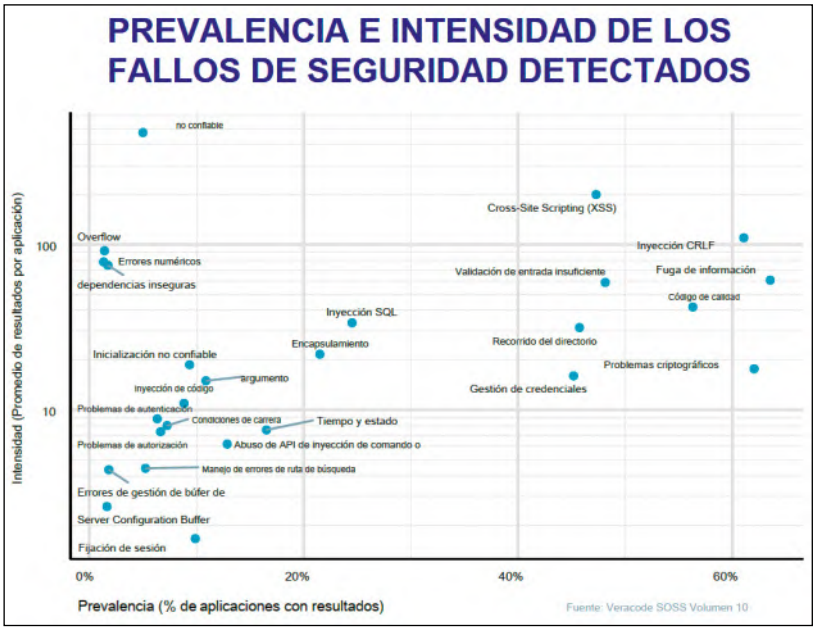
Y los resultados, a pesar de que cada vez las cifras mejoran, son preocupantes: se estimaa que, cada año, los fallos de seguridad en el código permiten el ataque a más de 200.000 usuarios y afectan a más de 300.000 sistemas, provocando pérdidas de casi 4.000 millones de euros. Un aspecto alarmante teniendo en cuenta que se calcula que, cada software comercial hecho con código abierto tiene un promedio de 64 vulnerabilidades.

Aún queda mucho por hacer

En 2020, el informe de Veracode destaca que se ha avanzado mucho en este apartado de la seguridad, pero "aún queda mucho por hacer". Por eso, insiste en la importancia de disponer de personal capacitado para programar de forma segura. Un tema que "continúa siendo crítico". De hecho, un aspecto bastante preocupante es que en la última década se ha triplicado el tiempo que se invierte en reparar una vulnerabilidad detectada.

También, se ha visto que "la mayoría de las empresas priorizan fallos de seguridad recientemente descubiertos, mientras dejan persistir los más antiguos no resueltos", lo que la firma de ciberprotección llama la "deuda de seguridad". Esto, precisamente, ha sido una de las conclusiones que parecen inquietar más a los clientes, ya que pueden verse comprometidos por fallos no parcheados hace años.





De cualquier forma, sí constata que actualmente "los desarrolladores están especialmente centrados en corregir los fallos de seguridad que se encuentran y, prueba de ello, es que más de la mitad de las aplicaciones analizadas mejoraron en seguridad notablemente e, incluso, un 20% de las testadas no presentó error de seguridad alguno".

Por eso, el informe, al igual que pasaba en su primera edición, considera que "la mayoría del software es muy inseguro" aunque, también, ve como positivo que cada vez se dedican más medios a parchear los fallos más graves, reduciendo su tiempo de exposición. Un dato positivo que se suma a que se ve, por parte de las empresas, el mismo interés en conseguir que una aplicación sea funcional que en hacerla segura.

El informe pone un peso especial en realizar escaneos del código, tanto de forma estática como dinámica, para detectar fallos. Por ejemplo, se ha comprobado que las

[COVIDIANIDAD]*

Tenemos pocas certezas para el después:

- Que el trabajo en remoto será más normal.
- Que la dependencia de la tecnología será mayor.
- Que el **Sello LEET** le seguirá indicando en qué grado puede confiar en su proveedor tecnológico.

Para todo lo demás... consulte con un adivino.

(*) Cotidianidad tras el COVID19

LEET SECURITY

ICT Services Rating Agency

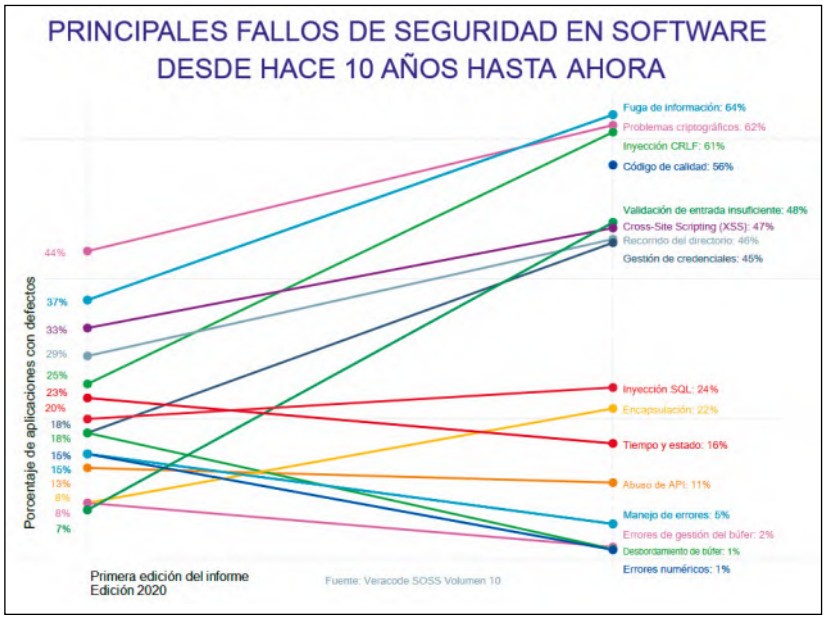
#TransmiteConfianza

leetsecurity.com

+34 915 798 187
info@leetsecurity.com

@leet_security
Leet Security SL

empresas que realizan de media 300 revisiones de la seguridad del software al año reducen cinco veces las posibilidades de sufrirlas. Además, explica que el uso de lenguajes veteranos como C / C++ supone un incremento de tres a cinco veces de posibilidad de tener vulnerabilidades no resueltas.



Demasiados fallos

Además, en la edición de 2020 también se aportan datos de interés como el tiempo medio de corrección de fallos de seguridad en software, 59 días, aunque se han detectado casos de hasta 171. Algo realmente preocupante teniendo en cuenta que el 83% de las aplicaciones analizadas en 2019 tuvieron al menos un defecto (un 20% de alta gravedad), lo que supone un incremento del 14% respecto a los datos de la primera edición del estudio. También, resalta que dos de cada tres aplicaciones no superan los test de seguridad basados en estándares de la industria como Owasp Top 10 y Sans 25. Eso sí, el 56% de las vulnerabilidades se arreglan rápido (un 30% en las primeras dos semanas tras detectarse) e, incluso, el 76% de las más graves ya suelen ser solventadas por los propios desarrolladores.

En cuanto al riesgo de los problemas detectados, en un 20% de las aplicaciones analizadas se dieron con fallos de 'alta gravedad', aunque estos se han reducido en término globales. Así que se puede decir que se ha mejorado la seguridad. El informe también destaca que los dos principales fallos, que continúan liderando el ránking de los más detectados, son los problemas criptográficos y los que pueden dar pie a fugas de información. Así, el mayor número de vulnerabilidades registradas proceden de errores que permiten hacer *Cross-site Scripting* (XSS), así como fallos de autenticación y por configuraciones incorrectas.

El gran problema para medir la seguridad en el software y parchear las vulnerabilidades es que "estamos midiendo un objetivo en movimiento. Las aplicaciones son fruto de un código vivo y que evoluciona con el tiempo, según las necesidades del cliente, por lo que cualquier cambio tiene el potencial de introducir fallos que exponen la aplicación y la organización".

Por eso, el estudio aconseja a los equipos de desarrollo "aceptar que todo va a evolucionar y dar seguridad a ese ritmo constante"; para ello, los alienta a crear "hábitos en torno a la programación segura", ya sea mediante el escaneo sistemático del código tras cada compilación o aplicando listas de verificación que incluyan todo tipo de características. Asimismo también recomienda ofrecer recompensas a los que más vulnerabilidades encuentren.

Vulnerabilidades por redes sociales

En definitiva, detectar y corregir, a tiempo, fallos de seguridad en software se ha convertido en una carrera a contrarreloj. Y los problemas para ofrecer seguridad se multiplican. Un grupo de investigadores del Grupo de Ciencias de Datos y Análisis del **Laboratorio Nacional del Noroeste del Pacífico del Departamento de Energía (PNNL)** de EE.UU., denunció en un artículo técnico, en abril, que muchas vulnerabilidades de código se están dando a conocer antes por redes sociales que a los propios interesados para que las corrijan. "La ciberseguridad social es una gran amenaza. Ser capaz de medir cómo se propagan los diferentes tipos de vulnerabilidades entre las plataformas es fundamental", han destacado.

Su investigación constató que una cuarta parte de las discusiones sobre las vulnerabilidades de software, desde 2015 hasta 2017, aparecieron en redes sociales y plataformas públicas de Internet (exactamente se estudiaron **GitHub, Twitter** y **Reddit**) antes de ser recibidas por la Base de Datos Nacional de Vulnerabilidad, el repositorio oficial del país que usa, entre otros, la Administración para corregir errores detectados, para lo que se tarda una media de tres meses. ■

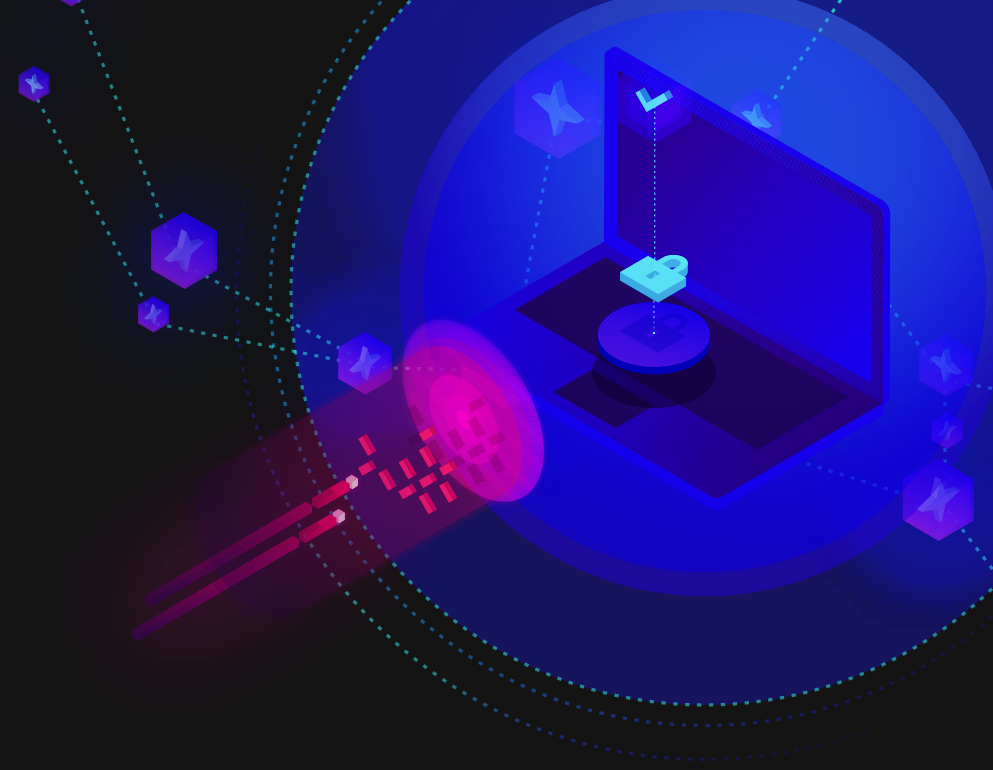
Europa quiere certificar la seguridad del software y ENISA propone un documento como punto de partida

Fruto de la preocupación de la **Agencia Europea de Ciberseguridad** (**ENISA**), el organismo publicó en abril un estudio, de 16 páginas, bajo el título "Avanzar en la seguridad del software: el papel del marco de certificación de ciberseguridad de la UE". En él, ofrece una buena perspectiva sobre los diferentes enfoques que hay para acometer en el desarrollo y mantenimiento del software de ciberseguridad. Además, también destaca los diferentes "aspectos que deben considerarse en el marco de certificación de protección cibernética" en el Viejo Continente.

El informe muestra los principales problemas relacionados con la implementación y el mantenimiento de repositorios, no solo para vulnerabilidades divulgadas públicamente sino también para aspectos de seguridad compartidos de productos, servicios y procesos certificados. También, destaca la coordinación de actividades entre las **Organizaciones Europeas de Normalización (ESO)** y la **Organización de Desarrollo de Normas (SDO),** así como las posibilidades de complementar los esquemas de certificación de ciberseguridad de la UE con pautas para el desarrollo, mantenimiento y operación de software. Además, aconseja aprovechar la experiencia y los conocimientos existentes y promover la adopción de los sistemas de certificación de ciberseguridad de la UE basados en normativas como Common Criteria, OWASP ASVS, BSIMM, BSI Pass 754, ISA 99 /IEC 62443 o ISO/IEC27034, entre otras.

El estudio se realizó como parte de las actividades preparatorias y de apoyo de la Agencia en el área de certificación de productos, servicios y procesos. Por eso, está previsto que sea utilizado como referencia en las iniciativas similares que están en curso a nivel nacional, durante la redacción de los esquemas de certificación de ciberseguridad candidatos y como un documento de orientación no vinculante para las partes interesadas del marco de certificación de ciberseguridad de la UE.

CYTOMIC



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.

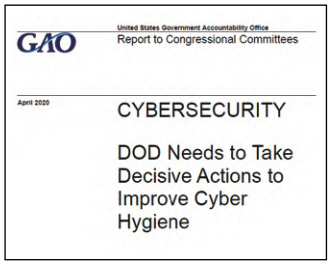
Cytomic Orion guía a tus analistas de seguridad en el proceso de triaje, investigación y reacción inmediata.

Para más información visita:
https://www.cytomic.ai/es/soluciones/orion/

Un informe de la Oficina de Rendición de Cuentas (GAO), tras analizar cinco años, alerta de falta de seguimiento en programas de ciberconcienciación y parcheo

El PENTÁGONO, aun con presupuesto millonario, no es eficiente aplicando sus programas de ciberseguridad

El **Departamento de Defensa (DOD)** de EE.UU. es uno de los organismos que, a nivel mundial, más invierte en protección cibernética con un presupuesto anual que ronda los 9.000 millones de euros. Sin embargo, en contra de lo que pudiera pensarse, no siempre lo hace de forma eficiente. Así lo denunció la **Oficina de Rendición de Cuentas del Gobierno (GAO)**, en abril, tras presentar su informe: 'El Departamento de Defensa necesita tomar medidas decisivas para mejorar la higiene cibernética'. Se trata del resultado de una auditoría en la que destaca que el Pentágono asume riesgos innecesarios por no haber implementado prácticas básicas, en programas de 2015, para aplicar la llamada higiene cibernética, un concepto que la **Universidad Carnegie Mellon** define como "un conjunto de prácticas que permiten gestionar los riesgos de ciberseguridad más comunes".



Tres iniciativas

En concreto, la GAO fue muy dura criticando la falta de seguimiento y control de tres iniciativas del DOD puestas en marcha hace cinco años para mejorar la capacitación y concienciación de sus empleados, también los que trabajan en unidades militares. "Cada persona debe entender qué papel juega en la ciberprotección de la organización, pero ¿cómo convencer a todos para que sigan las reglas y lo hagan de forma eficaz?", destacó el Director del Equipo de Gestión y Capacidades de Defensa de la GAO, **Joseph Kirschbaum**, que fue especialmente crítico con no llevar a cabo un seguimiento exhaustivo de los programas de concienciación que evitan errores humanos. Lógicamente, "nunca se podrán eliminar todas las amenazas, pero sí podemos manejarlas de forma correcta", añadió, recordando que es vital poder trabajar con la seguridad de que se está haciendo lo suficiente para gestionar los riesgos cibernéticos. "Si no puedes rastrearlo, no puedes medirlo. Si no puedes medirlo, no puedes manejarlo. Y si no puedes manejarlo, no vas a tener éxito", resaltó.

En concreto, la GAO analizó tres iniciativas cibernéticas de Defensa. La primera de ellas, 'Cultura y Cumplimiento de Seguridad Cibernética del DOD' (DC3I) se marcó 11 objetivos de cibereducación para 2016, pero, según el informe, sólo logró cuatro de ellos, quedando en el olvido el resto. Entre las medidas que formaban parte de este programa estaban, por ejemplo, deshabilitar los enlaces a correos electrónicos de dudosa procedencia o garantizar que los planes de respuesta a incidentes cibernéticos estén documentados y se realicen adecuadamente.

En el caso de la segunda, el 'Plan de Implementación de Disciplina de Ciberseguridad y capacitación en concientización cibernética' (CDIP), con 17 hitos dedicados a la detección y eliminación de vulnerabilidades conocidas en las redes militares, para 2018, la situación es tan caótica que, tras comprobarse que seis sí se lograron, el resto o se desconoce en qué estado se encuentran o, simplemente, no hay evidencia de los pasos que se siguieron, una situación que la GAO achaca a la falta de responsables, claramente asignados, para exigir su desarrollo y cumplimiento y responder ante los resultados logrados.

El informe explica que puede estar teniendo serias consecuencias ya que, desde octubre de 2019, algunos departamentos de Defensa no han recibido informes de capacitación cibernética que deberían haber puesto en marcha para mejorar la seguridad de su personal. Y si "el Director de Información (CIO) del Departamento de Defensa del DOD no toma las medidas adecuadas para garantizar que se implementen las tareas de DC3I, el Pentágono corre el riesgo de comprometer la confidencialidad, integridad y disponibilidad de información de misión crítica como resultado de un error humano por parte de los usuarios de las redes del Departamento, poniendo en riesgo la Seguridad Nacional", denuncia la auditoría.

En tercer lugar, la GAO también denunció que de los 16 objetivos de su programa de 'Capacitación sobre el desafío de la conciencia cibernética' (*Cyber Awareness Challenge*), desarrollado por la **Agencia de Sistemas de la Información de Defensa (DISA),** casi la mitad no han tenido seguimiento alguno, ni se tiene constancia de su finalización. De hecho, destacó que seis entidades, como la **Armada,** la **Fuerza Aérea,** el **Cuerpo de Marines y** el **Comando Europeo**, desconocían quién había realizado de forma completa este 'entrenamiento'. Es más, funcionarios de la Armada explicaron a la GAO que no "veían el valor de recopilar esta información".

Siete recomendaciones

Para evitar estas situaciones, la GAO ha pedido realizar un seguimiento exhaustivo durante la aplicación de cada programa, delimitar de forma más clara a sus responsables, sobre todo para constatar que se han conseguido los objetivos, y, también, darle mayor protagonismo a la concienciación en ciberprotección a los empleados del departamento de Defensa. También la GAO considera fundamental actualizar y proteger tanto software, como dispositivos concretos.

Además de 177 técnicas de ataque cibernético contra redes militares, identificadas por Defensa, y ante las que se plantearon una serie de medidas de 'higiene cibernética', se desconoce "cuáles son las más utilizadas para evitarlas", ya que no hay una "visibilidad completa" de su implementación, según resaltó la Oficina.

Algo que la GAO considera preocupante ya que los ejércitos de EE.UU. son cada vez más "dependientes de los sistemas y redes de TI para realizar operaciones militares y realizar funciones críticas" y los riesgos que se asumen en ellas cada vez son mayores porque "están plagadas de vulnerabilidades de ciberseguridad, tanto conocidas como desconocidas".

El informe finalizó con siete recomendaciones para actualizar los sistemas y políticas de ciberseguridad de Defensa y evitar estas situaciones entre las que destacan la necesidad de más auditorías y seguimientos de los programas, que el Secretario de Defensa exija de forma clara su cumplimiento a sus responsables, con un plazo de tiempo concreto.

También, vio fundamental que el CIO de Defensa garantice la consecución de los objetivos de estos programas no concluidos, hasta la identificación de su estado actual para conocer el grado en concienciación cibernética de los empleados, exigiéndoles unos resultados demostrables. ■

S21SEC

ACELERE SU TRANSFORMACIÓN DIGITAL

CON SERVICIOS DE CLOUD BASADOS EN ZERO-TRUST

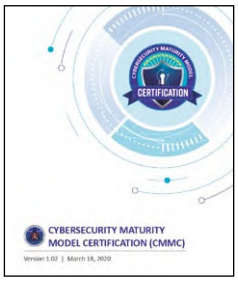
S21sec tiene el personal certificado en distintos entornos de Cloud para ayudarle a conseguir el máximo nivel de seguridad

¡Contacte con nosotros para más información!

www.s21sec.com | 902 020 222 | marketing@s21sec.com

Ha presentado una nueva certificación, en vigor desde junio, para más de 300.000 contratistas que manejen información clasificada

El Departamento de Defensa de EE.UU. propone un modelo certificable de madurez en ciberseguridad



El **Departamento de Defensa** (DoD) de EE.UU., junto con las universidades **Carnegie Mellon** y **Johns Hopkins**, ha presentado su propuesta de Certificación del Modelo de Madurez de la Ciberseguridad, CMMC ('Cybersecurity Maturity Model Certification). Para ello, han dado a conocer un documento en el que proponen una metodología para medir la madurez de la ciberseguridad, según varios niveles escalonados y conectados, en función de los procesos y prácticas que se aplican para proteger la información frente a los tipos de amenazas más comunes.

El modelo aborda las necesidades de Defensa para proteger su información no clasificada y su objetivo "es cubrir todos los ángulos posibles para aplicar la estrategia de ciberprotección en una organización". Se trata de una iniciativa más, impulsada por el DoD y la industria, para buscar un incremento de la seguridad de la información que maneja el sector industrial de Defensa (DIB) y garantizar la protección cibernética de las futuras adquisiciones.

Por eso, en el documento que desarrolla este nuevo modelo, sus responsables, que esperan que más de 300.000 contratistas se incorporen en los próximos cinco años, recuerdan que "el robo de propiedad intelectual e información confidencial de cualquier sector industrial, por la actividad cibernética maliciosa, amenaza la seguridad económica y nacional" y, de forma especial, a la cadena de suministro. De hecho, se espera que para 2026 todas las empresas con las que se trabaje cuenten con ella o una ciberseguridad similar.

La Certificación del Modelo de Madurez de Ciberseguridad (CMMC) se basa, en total, en cinco procesos de madurez y 171 mejores prácticas que permiten progresar en dichos niveles. Con ellos se quiere garantizar que los esfuerzos en ciberprotección son "consistentes, repetibles y de alta calidad". Además, sus creadores también destacan que su cumplimiento permite contar con capacidades de "mitigación en todos los niveles, desde la protección más básica, que se exigirá a casi todos los subcontratistas que tengan que ver con Defensa, pasando a la más amplia para Información Controlada No Clasificada (CUI) en el nivel 3, similar al P 800-171 del Instituto Nacional de Estándares y Tecnología (NIST), y culminando con la reducción del riesgo de Amenazas Persistentes Avanzadas (APT) en los niveles 4 y 5. Un tipo de ataque crítico que el documento recuerda que realizan "adversarios con una gran experiencia y recursos, y una alta sofisticación". Por eso, estas últimas, serán casi de obligado cumplimiento para las grandes corporaciones del sector que quieran trabajar con el Pentágono, también extranjeras.

Para cada capacidad exigida, se recomiendan una o más prácticas que abarcan un subconjunto de los cinco niveles. También, para cada dominio hay una serie de procesos que se piden y que se agrupan en un subconjunto de los cinco niveles. En función del grado de madurez se pueden conseguir diferentes calificaciones que van desde la de 'Higiene Básica' hasta la de 'Realizado', en el nivel más bajo, y 'Optimizado' en el más avanzado y máximo nivel.

Además, el documento destaca que los niveles del CMMC y los conjuntos asociados de procesos y prácticas entre dominios son acumulativos. O sea, no se puede lograr un nivel alto si no se han logrado los anteriores. Y en todos se incluye el cumplimiento de regulaciones, requisitos técnicos y diferentes exigencias de tratamiento seguro de la información.

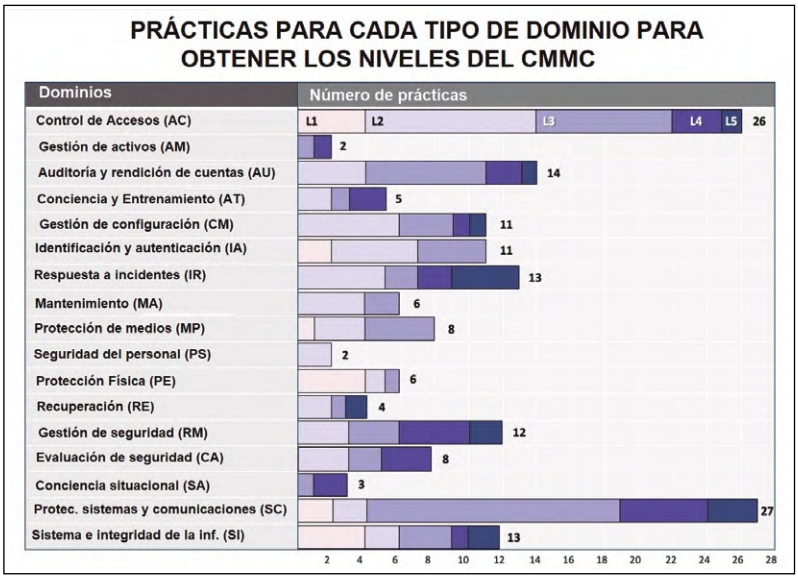
Este modelo de madurez, según explica el informe, es aplicable a múltiples sectores, ya que abarca un total de 17 dominios, entre ellos, el de Gestión de Activos (AM), Recuperación (RE) y Conciencia situacional (SA), así como los propuestos por el NIST en su documento SP 800-171, sobre familias de requisitos de seguridad.

Certificación, a 2.780 €

Para verificar la implementación de procesos y prácticas, el marco CMMC también se combina con un programa de certificación que permite que cualquier empresa que tenga este modelo implementado sea identificada como segura para trabajar con el DoD, un proceso que se ha calculado que tendrá un coste que rondará los 2.780 euros de media, por empresas, con una validez de tres años.

Además, se exige la comprobación física de que se cumple lo marcado en el modelo, a través de un certificador externo. Un aspecto que, según fuentes del DoD, va más allá de la ciberseguridad: permitirá conocer qué tipo de empresas es con las que se trabaja así como las características de su plantilla, ya sea en EE.UU. o fuera.

A pesar de que en el último año se habló de que este modelo sería exigido a todos los proveedores de Defensa, en mayo, finalmente, se introdujo un cambio que exime de cumplirlo a los proveedores de productos comerciales (COTS). ■



Blueliv.

Inteligencia modular de ciberamenazas

Reduciendo el riesgo, acelerando el rendimiento.

Rastreamos la clearnet, deep y dark web con el fin de proporcionar inteligencia automatizada y procesable para proteger sus organizaciones desde fuera de su perímetro.

Awards and recognitions

computing Security Excellence Awards 2018 Winner Enterprise Threat Detection Award

computing Security Excellence Awards 2018 Winner Enterprise Security Award

Cybersecurity Breakthrough Award 2018

blueliv.com @blueliv

Gartner, Inc., Cool Vendors in Communications Service Provider Security, 2015, Deborah Kish, Akshay K. Sharma, Craig Lawson, 15 April 2015. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Según el CSS de Zurich, EE.UU. ya cuenta con más de 6.300 cibervoluntarios, aunque el estudio destaca que el mejor ejemplo es la Unidad 8200 de Israel

La fuerzas de ciberreserva de los principales países occidentales indican el camino para mejorar la ciberseguridad nacional

El **Centro de Estudios de Seguridad** (CSS) de **Zurich** ha publicado un detallado informe de medio centenar de páginas en el que analiza y describe la estructura, organización y desafíos de las fuerzas de ciberreserva de seis países: Estonia, Finlandia, Francia, Israel, Suiza y los EE.UU. Con él, intenta ofrecer una visión de las particularidades de estas unidades de voluntarios, civiles y militares, para la lucha en el denominado quinto dominio si está en peligro la Seguridad Nacional.

"La organización y estructura de las reservas cibernéticas dependen de los recursos de los estados, la cultura estratégica, las instituciones públicas y el contexto político, entre otros factores, por lo tanto, en el desarrollo de las fuerzas de ciberreserva no existe una solución única que se ajuste a todos los estados. Sin embargo, puede servir de inspiración a otros estados", destacan los responsables del estudio.

Y es que, la ciberseguridad es un área relativamente nueva dentro de las fuerzas armadas y el desarrollo de las ciberreservas comenzó tan solo hace 10 años en los primeros casos; por ello, es un campo en evolución al que falta mucho camino por recorrer y, como se desprende del informe, no es un proceso fácil.

En España, cabe recordar que el primer paso oficial hacia la ciberreserva se dio en 2017. De carácter civil y organizada bajo la potestad del **Mando Conjunto de Ciberdefensa** (MCCD), en los primeros esbozos, consideraba que debería componerse de voluntarios expertos en distintas áreas, desde profesionales en ciberseguridad a politólogos, sociólogos, juristas o psicólogos, entre otros, un grupo que llegaría a estar formado, en principio, por unos 2.000 efectivos que realizarían funciones eminentemente defensivas. Se propuso que sus integrantes pudieran estar en ella con un permiso retribuido, previo acuerdo con las empresas, con una duración de dos años, algo que fue motivo de polémica por la posible falta de recursos económicos y de clarificación sobre los derechos y obligaciones de los ciberreservistas.

Reclutamiento y capacitación

La ciberreserva es una forma para que las fuerzas armadas cierren la brecha de la fuerza laboral en ciberseguridad. Y, también, beneficia a los reservistas a través de la posibilidad de adquirir experiencia y capacitación. Sin embargo, el proceso de reclutamiento no es tarea fácil y varía entre los ejércitos de los países analizados. Según el informe, la mayoría requiere de algún tipo de conocimiento o interés en ciberseguridad antes de poder unirse al ejército; pero otros, como la Unidad de Ciberdefensa de Estonia (CDL CDU) y la reserva francesa buscan reclutar voluntarios con amplios conocimientos y experiencia previa.

Curiosamente, no todos requieren que los reclutas o los nuevos miembros pasen una prueba para unirse a la unidad de ciberseguridad. Mientras que Finlandia, Suiza e Israel tienen procesos de selección muy similares para sus ciberreservistas, Estonia no pide que los candidatos pasen ninguna prueba antes de unirse a su Unidad. En Francia y EE.UU. se realizan una vez que se completa el entrenamiento militar básico.

Roles y tareas

Las tareas de los reservistas son tan variadas como roles puedan tener. Sin embargo, según el informe, la mayoría de los países analizados tienen un denominador común: sus funciones se centran, principalmente, en una labor defensiva, así como formar y trabajar en inteligencia de amenazas, entre otras. "Solo los ciberreservistas de EE.UU. e Israel realizan tareas ofensivas de ciberseguridad durante su servicio".

En cuanto al número de voluntarios, los responsables de la investigación confiesan la dificultad para obtener dichos datos, dado su carácter reservado, aunque estiman que, EE.UU e Israel son, obviamente, los que tienen las mayores reservas cibernéticas. Se calcula que el primero cuenta con 6.300 reservistas en ciberseguridad e Israel con unos 5.000 miembros, unas cifras que contrastan con respecto a los 150 reservistas operativos de Francia, en 2019, o los 40 en Suiza, aunque ambas esperan incrementarlos hasta más allá de 400.

Principales desafíos

Las responsables del informe, también destacan que, en todos los casos examinados, las reservas cibernéticas mantienen algún tipo de relación con el sector privado, aunque con diferencias en su aproximación.

El estudio también señala que reclutar personas para la ciberreserva no es tan fácil como se pensaba y supone un gran desafío para los estados. "Los salarios y la ubicación de los programas de capacitación cibernética, son dos aspectos que pueden desalentar a los posibles candidatos", resalta.

Asimismo, la integración de los grupos de ciberreservistas en las estructuras de seguridad estatales existentes es un proceso complicado. Además, el informe destaca la importancia de mantenerlos en el tiempo, no solo la duración del servicio, y saber identificar a nuevo talento, también, entre los propios militares en activo.

	ESTONIA	FINLANDIA	FRANCIA	ISRAEL	SUIZA	EE.UU.
Miembro de la OTAN	Sí	No	Sí	No	No	Sí
Miembro de la UE	Sí	Sí	Sí	No	No	No
Fuerzas armadas en 2017	6.600 en servicio activo, 12.000 en reserva, 15.800 paramilitares	21.500 en servicio activo, 227.500 en reserva, 2.700 paramilitares	203.000 en servicio activo, 72.000 reserva, 103.000 paramilitares	175.000 en servicio activo, 465.000 reserva, 8.000 paramilitares	140.000 en servicio activo y personal de reserva	1,35 millones en servicio activo, 858.000 en reserva
Proceso de reclutamiento	Todos los voluntarios	Deben presentar una solicitud	Todos los voluntarios	Tienen que pasar por un entrenamiento de servicio premilitar y solicitar el ingreso a la Unidad 8200	Deben presentar solicitud	Todos los voluntarios
Tareas	Soporte, formación, apoyo en caso de emergencia para instituciones privadas y públicas	Soporte (redes de defensa, proyectos de programación, pentesting, formación)	Reserva operativa, sensibilización	Operaciones de defensa y ofensivas, I + D y soporte	Soporte (desarrollo de software, 'forensia', educación)	Operaciones de defensa y u ofensiva, soporte
Número de reservistas	No hay números oficiales (Confidencial)		150 reservistas operativos (plan para aumentar a 400) y 150 reservistas civiles en 2019	5.000 miembros estimados	Hasta ahora 40 reservistas cibernéticos pero planean aumentar a 600	6.300 reservistas involucrados en ciberseguridad y en el CMF (estimación en 1.500 para 2024)
Colaboración con el sector privado	No oficialmente	Sí	A través de asociaciones	Sí, a través de sus ex miembros		Asociaciones público privadas

Israel, un ejemplo

Aunque los responsables de la investigación insisten en que "cada estado debería centrarse en desarrollar su propio modelo de ciberreserva para garantizar que se ajusta a sus objetivos nacionales y estructuras institucionales", señalan que la Unidad 8200 de Israel es considerada como "el ejemplo perfecto de una ciberreserva en activo, reclutando a personas que, incluso, con posterioridad, han creado *startups* exitosas", explica. ■

Tome el control con nuestra solución de entrenamiento y concienciación en ciberseguridad para usuarios finales.

SMARTFENSE
HARDENING DE USUARIOS

www.smartfense.com
info@smartfense.com

MÓNICA, NGSIEM nacional a la vanguardia de la tecnología

La Unidad ICA Sistemas y Seguridad, de Grupo ICA, ha acordado con el Centro Criptológico Nacional, CCN, la adopción de la última versión de la plataforma NGSIEM LogICA, certificada Common Criteria EAL2, como su herramienta NGSIEM para la Administración Pública y organismos dependientes, bajo la marca MÓNICA. Esta solución nacional –incluida en el CPSTIC y alineada con las medidas establecidas en la Estrategia Nacional de Ciberseguridad– consiste en un sistema automatizado de gestión de información y eventos de seguridad que recoge en una única plataforma toda la información existente sobre amenazas potenciales, permitiendo no solo reaccionar ante los ataques, sino adelantarse a ellos para remediarlos antes de que tengan impacto. Combina SEM (monitorización y gestión de incidentes) y SIM (gestión de *logs* y cumplimiento).

Julio de 2004. Grupo ICA arranca su actividad en el área de la seguridad informática con la incorporación de un equipo de personas especializado en seguridad y que en aquel momento desarrollaba e integraba la plataforma de monitorización y gestión de la seguridad LogICA SIEM, un SIEM de la primera fase, según Gartner… Ese fue el comienzo de una historia que hoy continúa.

Enero de 2020. ICA Sistemas y Seguridad, creada como la unidad especializada en el desarrollo de proyectos personalizados de integración de sistemas y seguridad, desde la que se prestan los servicios y se comercializan productos de las áreas de Integración e Infraestructuras TIC y Ciberseguridad.

Tras 16 años en el mercado y con uno de los equipos con mayor experiencia en ciberseguridad, tanto integrando SIEM como desplegando servicios de ciberseguridad, la compañía cuenta con más de 120 profesionales expertos, también construyendo productos de seguridad. ICA Sistemas y Seguridad ha acordado con el Centro Criptológico Nacional la adopción de la última versión de la plataforma NGSIEM LogICA como su herramienta NGSIEM para la Administración Pública y organismo dependientes, bajo la marca MÓNICA.

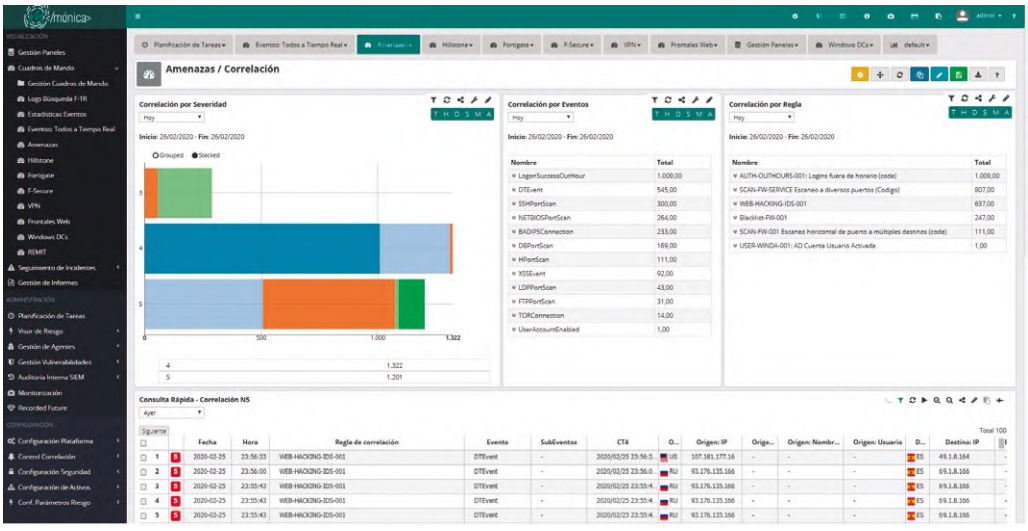
Núcleo certificado Common Criteria EAL2

La guía CCN-STIC 106 Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC, establece como requisito necesario para la inclusión en el catálogo, la certificación Common Criteria, la revisión de la Declaración de Seguridad y del Informe Técnico de Certificación, emitido por un laboratorio independiente. En esta etapa de certificación, ICA Sistemas y Seguridad adecuó además el producto a los Requisitos Fundamentales de Seguridad (RFS), que definen las principales características de los productos que deban pertenecer a la familia de productos "Sistemas de gestión de eventos de seguridad", y obtiene la Certificación para LogICA NGSIEM Common Criteria EAL2, hecho que le ha permitido formar parte del Catálogo de Productos Cualificados del Centro Criptológico Nacional, como única plataforma SIEM nacional y europea que hoy cumple con estos requisitos funcionales y de seguridad establecidos por el propio Centro, así como los definidos en la propia Norma. Estos criterios proporcionan un conjunto común de requisitos funcionales para los productos TI y el proceso de evaluación establece el nivel de confianza en el que el producto TI satisface la funcionalidad de seguridad al haber superado las medidas de evaluación. Actualmente, ninguna otra plataforma cumple estas características.

Gestión de información y eventos de seguridad

MÓNICA es un sistema automatizado de gestión de información y eventos de seguridad que recoge en una única plataforma, toda la información existente sobre amenazas potenciales, permitiendo no solo reaccionar ante los ataques, sino adelantarse a ellos para remediarlos antes de que tengan impacto. Combina SEM (monitorización y gestión de incidentes) y SIM (gestión de *logs* y cumplimiento) para ser el Sistema de Gestión de Información de Seguridad y Gestión de Eventos que permite analizar los datos de eventos de seguridad en tiempo real y la detección temprana de ataques e infracciones, lo que la convierte en la única plataforma SIEM nacional con estas capacidades y características.

MÓNICA, que recopila, almacena, investiga, respalda la mitigación e informa sobre datos de seguridad para dar respuesta a incidentes, análisis forense y cumplimiento normativo, gracias a la capacidad de agregación de datos de toda la red de la organización, dispositivos TI (Information Te-



La plataforma española MÓNICA, que recopila, almacena, investiga y respalda la mitigación e informa sobre datos de seguridad para dar respuesta a incidentes, análisis forense y cumplimiento normativo, gracias a la capacidad de agregación de datos de toda la red de la organización, dispositivos TI, dispositivos OT y la normalización de todos estos datos para su análisis, integra las capacidades más avanzadas de LogICA NGSIEM en línea con lo definido por Gartner.

One Identity Safeguard

Privilege Access Management

One Identity Safeguard

One Identity Safeguard Identifica y neutraliza los riesgos de ciberataques de sus cuentas privilegiadas, sin afectar a la productividad de sus administradores y de su personal de IT.

Aprenda cómo en **www.oneidentity.com/safeguard**

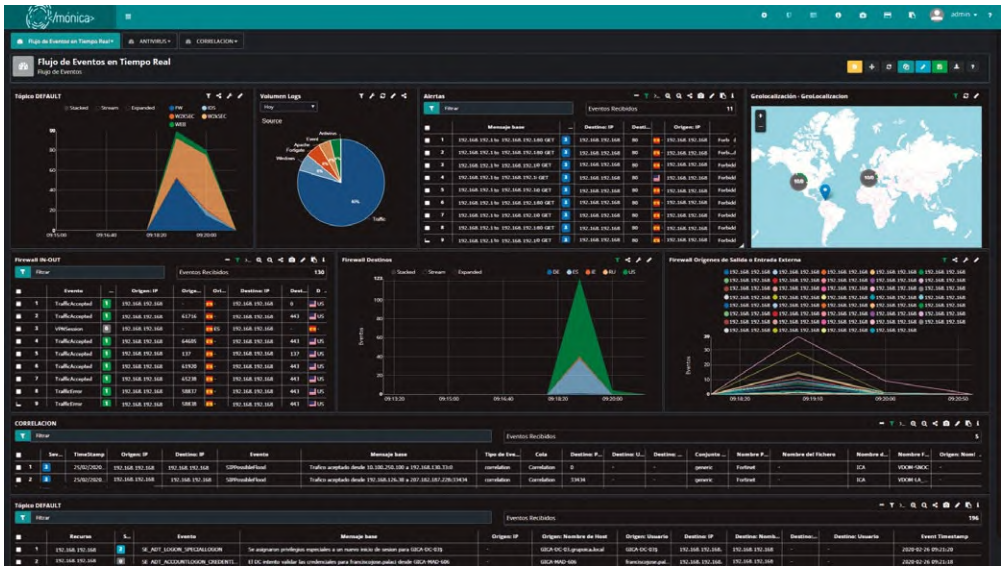
#SecurityStartsHere

ONE™ IDENTITY

chnology), dispositivos OT (Operational Technology) y la normalización de todos estos datos para su análisis, integra las capacidades más avanzadas de LogICA NGSIEM en línea con lo definido por Gartner, que indica cuáles son las principales funcionalidades requeridas en 2020 para un SIEM, gestor de casos de uso, UEBA, integración nativa en producto con SOAR (TheHIVE/CORTEX), integración nativa con inteligencia de amenazas (MISP/Recorded Future), capacidades automáticas de detección y respuesta, etc., así como compartir un *roadmap* con el Centro Criptológico Nacional para el desarrollo de nuevas versiones y funcionalidades alineadas con la seguridad de las Administraciones Públicas en redes de propósito general y redes restringidas.

Para hacer un uso eficaz de todo este conocimiento, MÓNICA combina estos datos mediante motores de correlación de nueva generación, capaces de desarrollar inteligencia en tiempo real. El motor de correlación Next Generation Correlation Engine analiza toda la información a través de diferentes procesos y aplicando algoritmos que permiten contextualizar el procesamiento, así como identificar anomalías y adaptar los resultados al entorno. Se combinan componentes de proyección y evaluación de comportamientos y algoritmos de aprendizaje para así poder predecir situaciones a futuro, creando nuevas reglas de correlación de forma automatizada, tanto para ataques existentes como para los que aún no han tenido lugar, ayudando a identificarlos antes de que sucedan.

Combinando estas capacidades, MÓNICA permite la automatización para la resolución de incidentes, mejorando la eficiencia y eficacia de los analistas de seguridad, gracias a que la plataforma permite incorporar en el proceso diferentes 'Playbooks' de tratamiento de incidentes para la gestión de amenazas.



Uniendo las capacidades tecnológicas, la estrategia seguida para su construcción y la experiencia del equipo de desarrollo de producto de ICA Sistemas y Seguridad, MÓNICA tiene un potencial de crecimiento e integración con otras tecnologías con respuesta inmediata. Y es, hoy por hoy, la única plataforma nacional que se equipara en el mercado con las soluciones de multinacionales como IBM, Symantec o Fortinet.

Tecnología española

MÓNICA es tecnología española alineada con las medidas establecidas en la Estrategia Nacional de Ciberseguridad, definida por el Gobierno de España. En este sentido, el acuerdo entre el Centro Criptológico Nacional e ICA Sistemas y Seguridad incluye la compartición de hoja de ruta y el desarrollo de funcionalidades específicas, así como la integración con las herramientas existentes del CCN-CERT.

MÓNICA es un sistema modular compuesto por diferentes subsistemas integrados en un único producto y desarrollados por un único fabricante:

- Sistema de almacenamiento.
- Sistema distribuido de ejecución en tiempo real.
- Bus de *streaming* y procesado en tiempo real.
- Servidores de front end.
- Monitores de extracción de datos.
- Consola.

Su arquitectura certificada permite crecer horizontalmente de manera transparente, añadiendo appliances físicos o virtuales para incrementar capacidades de recolección, gestión, detección y remediación. Esta solución NGSIEM permite despliegues incluso en servidores de baja capacidad, donde las necesidades de recolección y procesamiento son menores, pero a la vez críticas para la gestión de la seguridad, y en cambio no se dispone de recursos hardware ilimitados.

Uniendo las capacidades tecnológicas, la estrategia seguida para la construcción de MÓNICA y la experiencia del equipo de desarrollo de producto de ICA Sistemas y Seguridad, la plataforma tiene un potencial de crecimiento e integración con otras tecnologías, con respuesta inmediata, de forma que la alineación con futuras tendencias o estrategias en ciberseguridad de los principales visionarios, están al alcance de MÓNICA.

Conclusiones

ICA Sistemas y Seguridad, ha certificado el núcleo de MÓNICA, permitiendo un crecimiento a través de funcionalidades que se incorporen a la consola, sin comprometer la certificación y alineados con las necesidades de las Administraciones Públicas y beneficiando a su vez a todos los clientes de LogICA NGSIEM.

MÓNICA permite olvidarse de complejos sistemas que intentan construir un SIEM integrando soluciones de terceros, llenos de vulnerabilidades y cuya evolución depende exclusivamente de que el fabricante de cada componente, decida implementar una nueva funcionalidad, donde nadie garantiza la integración con el resto de componentes.

MÓNICA se convierte de esta forma en la primera (y por ahora, única) plataforma nacional certificada y cualificada para CiberSOC y CSIRT, permitiendo a los analistas centrarse en los sucesos que realmente pueden impactar en los activos de una organización y que no pueden gestionarse de forma automática, mejorando la calidad del servicio del equipo de ciberseguridad y llegando a prevenir ciberataques.

MÓNICA es la única plataforma nacional que se equipara en el mercado con las soluciones de prestigiosas multinacionales en ciberseguridad como IBM, Symantec o Fortinet. ■

Alberto Cañadas
Gerente de Preventa y Desarrollo de Negocio Ciberseguridad

Jesús Castellanos
Gerente de Diseño de Servicios y Cumplimiento Ciberseguridad

ICA SYS

Asegure a sus empleados remotos

Seguridad mejorada. Maximiza la comodidad.

RSA SecurID® Access hace más fácil mejorar la seguridad del creciente número de empleados remotos. Ofrecemos una amplia gama de autenticadores para que pueda elegir los que funcionan mejor para sus empleados y los recursos que necesita securizar.

Autenticación a medida para las características y riesgos específicos de su organización.

Go ahead.
Be you.

RSA

Learn more at rsa.com/authentication

Entelgy Innotec VPN Cloud: teletrabajo seguro y controlado

La implantación generalizada del teletrabajo en un tiempo reducido puede llevar a disminuir las medidas de seguridad habituales dentro del dominio de una organización. Dado que el teletrabajo ha venido para quedarse, resulta imprescindible abordar una solución que permita mantener los sistemas y accesos a todos los recursos de un modo seguro y controlado. VPN Cloud, de Entelgy Innotec Security, reúne todos los elementos para que las organizaciones puedan implementar el teletrabajo de la manera más segura y efectiva: acceso tunelizado cifrado, reglas de *firewall* para filtrar el tráfico, recursos de ancho de banda compartida, soporte 2FA, *host-checker*, tecnología de cifrado SSL y el respaldo de los principales fabricantes del sector.

Dada la situación producida por la crisis del COVID-19, el **teletrabajo** se ha convertido en un elemento **prioritario.** Según Eurostat, el Instituto de Estadística europeo, apenas **el 3%** de los empleados españoles **teletrabajaban** en 2019 de **manera habitual**, lo que da una idea del potencial de crecimiento de las soluciones que faciliten este sistema de un modo seguro.

La implantación de una solución de acceso remoto es un reto desde el punto de vista de la seguridad y la gestión para cualquier organización. Se requieren capacidades, tanto de personal como de infraestructura, que no siempre están disponibles. Las ventajas que ofrecen las soluciones en la nube, como **VPN Cloud**, de **Entelgy Innotec Security**, es que posibilitan un despliegue rápido y seguro, permitiendo acceso a la organización desde cualquier lugar, con las mismas medidas de seguridad desplegadas en las propias oficinas y, de esta manera, poder mantener la continuidad de sus negocios.

Esta solución se establece por medio de **túneles cifrados virtuales** punto a punto a través de Internet para que los usuarios **accedan de forma segura** a todas las aplicaciones corporativas, tanto privadas como públicas, así como a su información en su red privada.

Para lograr esa seguridad robusta en el acceso, la solución se apoya en **tecnologías punteras** y ofrece un soporte de **doble factor** de **autenticación** (2FA), pudiéndose integrar con el directorio activo del cliente; **verificación** del estado del cliente (host-checker); además de reglas de ***firewall*** para filtrar el tráfico. También, para cifrar el tráfico, emplea el protocolo **SSL** sobre TLS garantizando la confidencialidad y la integridad.

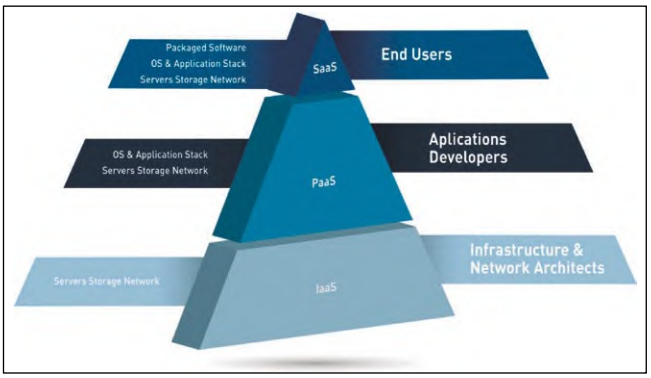


Figura 1.- Modelo de servicio Cloud.

Al ser una solución en Cloud, se trata de un servicio **flexible** que cuenta con un alto grado de **disponibilidad** y recursos optimizados a demanda, además de la **protección** contra DDoS.

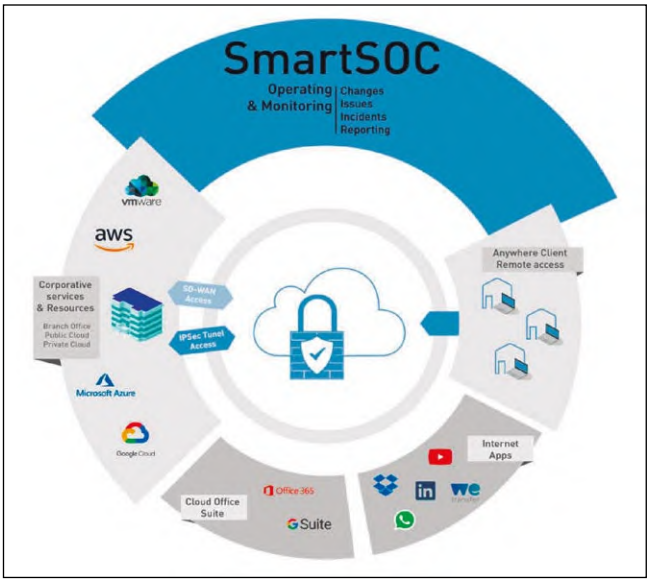


Figura 2.- Servicio VPN Cloud de Entelgy Innotec.

Para garantizar la conectividad con los centros de datos del cliente, emplea protocolos conocidos, como IPSec y SD-WAN.

De este modo, la solución **evita inversiones de infraestructura** aprovechando los recursos existentes de ancho de banda y añadiendo como un elemento más un punto de entrada a los recursos de la organización en un modelo Cloud SaaS, ofreciendo como valor añadido el servicio de despliegue, soporte y configuración por parte de Entelgy Innotec.

Por todo ello, las organizaciones pueden establecer un sistema de trabajo en remoto en el que los todos los profesionales accedan de una manera **segura, flexible** e **inmediata** a los recursos de su organización desde cualquier lugar, manteniendo los niveles de seguridad ante ciberataques y salvaguardando la **privacidad y confidencialidad** de la información.

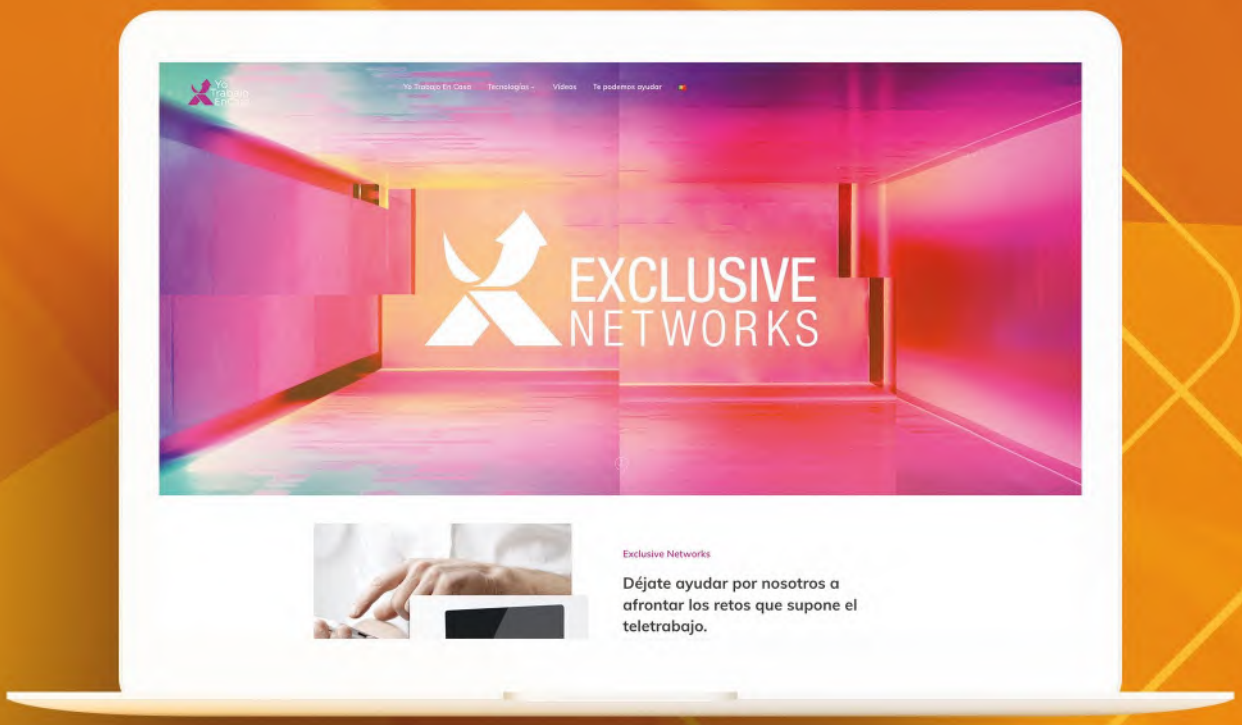
Características del servicio	
SLA de la plataforma	99.95%
Tipo de VPN	SSL
Protección DDoS	✓
Split tunneling	✓
Accesso tunelizado a Apps Internet	✓
Reglas de firewall	✓
Integración AD/LDAP	✓
Host Checker	✓
2FA con correo electrónico	✓
Propagación DNS privada	✓
Acceso mediante portal web	✓
Acceso mediante cliente	✓
Consulta de Logs	✓
Monitorización de incidentes	✓
Servicios añadidos	
Consultoría previa configuración	✓
Despliegue e implantación	✓
Soporte a la configuración	✓
Atención de incidencias	✓
Asistecia a resolución de problemas	✓
Informe de registro de incidencias	✓
Informes de uso de VPN-SSL	✓

Figura 3.- Características del VPN Cloud de Entelgy Innotec.

La compañía española, experta en seguridad, completa su solución **VPN Cloud** con el respaldo de su **SmartSOC**, uno de los Centros Avanzados de Operaciones de Seguridad más desarrollados a nivel mundial que, combinando inteligencia y tecnología, ofrece un **equipo de soporte** que gestiona la configuración de portales, reglas y rutas, además de un servicio **24x7 en monitorización** de seguridad y **Blue Team** detectando y gestionando posibles incidentes.

La solución y el servicio cuentan con el soporte de **fabricantes reconocidos** en el sector, como Fortinet, Splunk, VMware y Elasticsearch, y de un proveedor de Cloud con más de 20 centros de datos a escala global. ■

Daniel González López
Gerente de Estrategia de Servicios
ENTELGY INNOTEC SECURITY
daniel.gonzalez@innotec.security



Yo Trabajo EnCasa

DÉJESE AYUDAR POR NOSOTROS A AFRONTAR LOS RETOS QUE SUPONE EL TELETRABAJO.

Descubra las **tecnologías** más disruptivas que le ayudarán a garantizar acceso seguro de sus empleados trabajando desde casa.

Visite nuestro microsite para Teletrabajo

yotrabajoencasa.xnetworks.es

EXCLUSIVE NETWORKS

Soluciones de calificación de riesgo de ciberseguridad: el nuevo modelo de RiskRecon

Medir el riesgo de una manera precisa y efectiva es fundamental para tomar mejores riesgos y tomar decisiones acertadas. La capacidad de calificar el riesgo de ciberseguridad para una organización aún es nueva, incluso para muchas corporaciones grandes, pero es fundamental para comprender y actuar sobre el riesgo IT. Aquí es donde las soluciones de calificación de riesgo de ciberseguridad como RiskRecon se convierten en una herramienta esencial para comprender y actuar sobre este riesgo concreto, para mejorar la postura de ciberseguridad y remediar los resultados que se correlacionan con las calificaciones. Este artículo explorará qué son los Ratings de ciberseguridad, cómo funcionan y cómo pueden mejorar el riesgo de toda la organización en función de la capacidad de calificar el riesgo IT de los proveedores externos.

La mayoría de las organizaciones no conocen el nivel de riesgo de ciberseguridad que existe en sus sistemas y *hosts*. No tienen la visibilidad de las condiciones potencialmente peligrosas provocadas por la mala higiene de la ciberseguridad. Esto no significa que los equipos de ciberseguridad no estén haciendo bien su trabajo. La mayoría de las empresas no tienen una visión externa y objetiva de los activos de su organización que son visibles en Internet abierto. Y a medida que las empresas crecen, su huella digital se expande drásticamente en todo el entorno de TI y las relaciones entre proveedores.

Esto significa más datos compartidos y acceso a sistemas específicos en la nube. Esta es la expansión de la "superficie de riesgo" de una organización. La superficie de riesgo se define como cualquier lugar donde la capacidad de operación de una organización, la reputación, los activos, las obligaciones legales o el cumplimiento normativo estén en riesgo.

Si la capacidad de una organización para operar se ve comprometida, llegar a la raíz del problema requiere de una evaluación que sea rápida, integral y precisa. Los equipos de Seguridad y de Gestión de Proveedores necesitan disponer de la capacidad de saber de manera continuada cuál es su "scoring" en las categorías importantes, como por ejemplo los niveles de cifrado y parcheado o las brechas de datos.

El riesgo de ciberseguridad aumenta exponencialmente a medida que la superficie de riesgo se expande en las relaciones con sus proveedores y con aquellas empresas que proporcionan servicios a sus proveedores. De hecho, el 84% de las empresas alojan activos críticos y / o sensibles con terceros. Y el 65% de los *hosts* a nivel mundial se alojan en la infraestructura propiedad de una entidad externa, lo cual indica una dependencia abrumadora de TI externalizada que, a pesar de que puede reducir costes y mejorar la productividad, también crea más riesgos para la organización.

EL RIESGO IT NO PUEDE SER EXTERNALIZADO

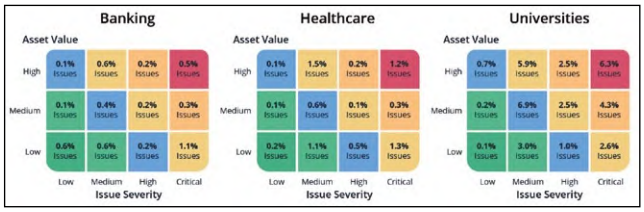
Es importante comprender el desempeño de las áreas críticas de seguridad IT desde un punto de vista objetivo: qué nivel de riesgo existe en toda la organización y en su ecosistema con terceros. Aquí es donde las soluciones de calificación de riesgo de ciberseguridad como RiskRecon se convierten en una herramienta esencial para comprender y actuar sobre este tipo de riesgo, para mejorar la postura de ciberseguridad y remediar los resultados que se correlacionan con las calificaciones.

De hecho, según Gartner, para 2022, las calificaciones de ciberseguridad serán tan importantes como las calificaciones crediticias al evaluar el riesgo de las relaciones comerciales existentes y nuevas.

SER DUEÑO DE SU RIESGO COMIENZA CON UN RATING

Las clasificaciones de riesgo de ciberseguridad proporcionan un método rápido y no intrusivo para evaluar la postura de ciberseguridad de una organización.

Con una calificación agregada derivada de un conjunto de clasificaciones de dominio de seguridad específicas, los equipos pueden comprender muy rápidamente, desde un punto de vista objetivo, cómo están haciendo su trabajo y qué necesitan mejorar. Esta instantánea es esencial para que las organizaciones comprendan por adelantado lo que implican las calificaciones y para comenzar el proceso de comprender su riesgo.



RiskRecon puede usar su calificación para informar al usuario de cuáles son los problemas que subyacen debajo de la calificación, su gravedad y cuán crítico es el riesgo potencial si esos hallazgos no se abordan.

En el mercado hay varias compañías que ofrecen servicios de Rating de Ciberseguridad, sin embargo RiskRecon ha dado un paso para diferenciarse de forma significativa del resto: ha actualizado su Scoring Model.

RiskRecon, en lugar de ser un modelo de calificación basado en una "opinión experta" arbitraria, o uno diseñado intencionalmente para asignar calificaciones a eventos de pérdida de datos pasados, que penaliza el Rating de una empresa, se basa en la gestión de riesgos observada en el mundo real.

El nuevo algoritmo de calificación se basa en el análisis de industrias enteras que son ampliamente aceptadas como sobresalientes en la gestión del riesgo (entidades financieras) que por motivos de negocio y por regulaciones, reflejan el extremo superior de la escala de calificación ("buena"), y las industrias ampliamente conocidas por ser muy débiles en la gestión del riesgo (Universidades) que reflejan el extremo inferior de la escala de calificaciones ("malo").

La propuesta de RiskRecon puede diferenciar claramente entre empresas e industrias que gestionan el riesgo de manera adecuada y deficiente debido a la capacidad de la compañía no solo de determinar la tasa de problemas y su gravedad dentro de un entorno, sino también el valor en riesgo de cada sistema en el que existen los problemas.

De esta capacidad única, Jack Jones, presidente del Instituto FAIR y cofundador de RiskLens declaró al respecto: "Se desperdicia demasiada energía en la seguridad de la información para resolver problemas que no importan. A medida que el modelo FAIR promueve, la gestión eficaz del riesgo requiere comprender la frecuencia probable y la magnitud de la pérdida; eso depende de comprender el valor del activo. Estoy muy contento de ver que RiskRecon trae la capacidad de determinar automáticamente el valor de los activos al mercado".

El nuevo modelo de calificación mejorará considerablemente la capacidad de los clientes de RiskRecon para tomar rápidamente decisiones de riesgo con confianza. Matemáticamente, enfatiza las cosas que importan (problemas graves en sistemas críticos) y enfatiza lo que menos importa: problemas de gravedad más bajos en sistemas que no tienen consecuencias de riesgo significativas. Y resuelve todo en el medio.

Es decir, RiskRecon construye su modelo de Rating sobre la observación de cómo se ve una buena gestión de riesgos y una mala gestión de riesgos en el mundo real. Esencialmente, RiskRecon ha creado un modelo de calificación que les dice a los consumidores "esta compañía tiene una calificación alta porque administran el riesgo como un Banco" y "esta compañía tiene una calificación baja porque administran el riesgo como una universidad".

Al hacerlo, RiskRecon también construye un modelo que les dice a los consumidores qué problemas importan y cuánto importan a través del análisis de los problemas que preocupan a los buenos administradores de riesgos, en función del contexto del valor de los activos y la gravedad del problema.

BENEFICIOS CLAVE DE LA CALIFICACION

Son cuatro los beneficios clave de la calificación que experimentarán los equipos:

• **Reporting**. Muchos equipos de Gestión de Riesgos, Ciberseguridad y Gestión de Proveedores, aprovechan las calificaciones para demostrar que tienen controles de seguridad adecuados que reducen el riesgo. Con los informes que reciben de RiskRecon, obtienen visibilidad de cómo su orga-

STORMSHIELD

Primer cortafuegos en obtener ambas certificaciones del CCN. **Producto Cualificado y Producto Aprobado**

Stormshield, filial participada al 100 % de Airbus CyberSecurity, propone soluciones de seguridad completas e innovadoras para proteger las redes (Stormshield Network Security), los puestos de trabajo (Stormshield Endpoint Security) y los datos (Stormshield Data Security). www.stormshield.com/es/

nización y sus terceros están calificados, y puede comunicarlo al Comité de Dirección para validar su programa de Gestión de Riesgos.

• **Benchmarking**. Las organizaciones dentro de una industria o grupo demográfico en particular, pueden comparar su desempeño utilizando su Rating, para comprender dónde se clasifican frente a organizaciones similares. La capacidad de evaluar el rendimiento es esencial para saber cómo puede mejorar su programa.

• **Comprender y actuar.** Una vez que la organización conoce su propia calificación, y a medida que avanza en la monitorización continuada del Rating de sus proveedores, los equipos de Ciberseguridad, Gestión de Riesgos y Gestión de Proveedores, consiguen más visibilidad de lo que se define como un hallazgo prioritario, para que la fijación de esos hallazgos específicos esté claramente documentada. Esto viene en forma de mediciones directas, evidencias, sugerencias y acciones recomendadas.

• **Colaborar**. Las organizaciones desean mantener relaciones saludables con sus proveedores. La capacidad de colaborar con terceros en los hallazgos de riesgo IT es fundamental para fomentarlas con proveedores basadas en la transparencia y la confianza.

CÓMO FUNCIONA

La solución de calificación de riesgo de ciberseguridad de RiskRecon cuenta con capacidades altamente diferenciadas para ayudar a los equipos a comprender el Rating y luego tomar medidas.

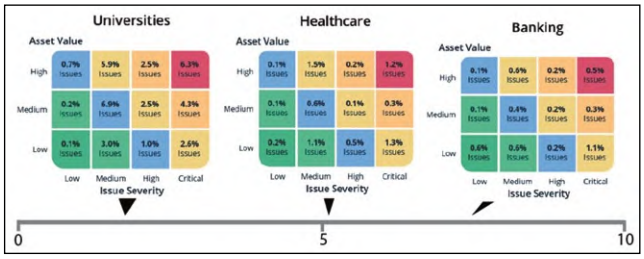
• **Descubrimiento profundo y evaluación.** RiskRecon puede descubrir los activos TI de cualquier organización para monitorizarla, lo que le permite analizar eficientemente los sistemas visibles desde el exterior y actualizarlos a medida que una corporación se expande digitalmente con el tiempo.

• **Perfiles IT.** RiskRecon construye perfiles contextuales de cada activo descubierto, equipando a los equipos con un análisis exhaustivo de cómo una organización ha construido su arquitectura IT. Los activos analizados incluyen dominios, *hosts*, proveedores de *hosting*, sistemas, configuraciones y terceros. Para cada uno de los 11 dominios de seguridad, RiskRecon informa sobre el rendimiento actual general, las tendencias y los puntos de referencia de la industria. Cada problema está respaldado con un resumen detallado del problema de información y descripciones, CVE relacionados, nombre de *host,* dirección IP, valor del activo, gravedad del problema y prioridad de riesgo.

• **Precisión y validación.** Evaluar el riesgo de un proveedor y sus proveedores (Riesgo de cuartas partes) requiere un nivel de precisión en los datos importante. Si cada vez que se detecta un problema en un proveedor resulta ser un Falso Positivo y es necesario hacer Tuning, el servicio de Rating no es eficiente. El "Data Accuracy" de RiskRecon se certifica de forma independiente con una precisión del 98,5%. RiskRecon ayuda a las organizaciones a reducir el riesgo en todo el ecosistema de proveedores con la tasa de falsos positivos más baja del mercado, en comparación con otras soluciones. Este es un aspecto importante de su propuesta a los clientes a nivel mundial, especialmente a medida que las empresas se expanden, porque eso significa más proveedores y más riesgo potencial.

• **Priorización de riesgos.** RiskRecon determina automáticamente el valor en riesgo de cada sistema que analiza. Al combinarlo con el conocimiento de la tasa de problemas (Issue Rate) y su gravedad dentro de una empresa, le permite evaluar la calidad de la gestión de riesgos de una organización y sus proveedores. Esto cambia fundamentalmente la forma en que una compañía abordaría y administraría el riesgo IT; es decir, si los equipos de Gestión de Riesgos y Gestión de Proveedores saben cómo priorizar exactamente qué problemas remediar primero, esto abre un camino más rápido para reducir el riesgo en el ecosistema de proveedores y es un acelerador de resultados de riesgo más positivos .

• **Automatización de datos.** RiskRecon aplica un nivel de automatización de datos sin precedentes en torno a cómo descubre, analiza y prioriza el riesgo de terceros para las organizaciones a nivel mundial. A medida que las empresas escalan, y a medida que el ecosistema de proveedores evoluciona y crece, las empresas pueden recurrir a RiskRecon para construir modelos eficientes en programas avanzados de riesgo de terceros para reducir el riesgo IT.



¿Cuál es el resultado? RiskRecon puede diferenciar claramente entre empresas e industrias que gestionan el riesgo de manera adecuada y deficiente debido a su capacidad no solo de determinar la tasa de problemas y su gravedad dentro de un entorno, sino también el valor en riesgo de cada sistema en el que existen los problemas.

EL IMPACTO POSTERIOR DEL RIESGO DE TERCEROS MAL ADMINISTRADO

El impacto real del riesgo de terceros mal administrado se siente financieramente para las organizaciones que no tienen la visibilidad que necesitan en sus relaciones con terceros.

Cuando hay un problema grave con un proveedor, se trata de algo más que un problema para esa empresa. A esto lo llamaríamos un incidente con múltiples partes.

Estos incidentes multipartidistas, que también denominamos «eventos dominó», se están volviendo más comunes con el tiempo. Su frecuencia ha aumentado a una tasa de crecimiento anual promedio del 20% desde 2008. No podemos evitar ver en esta tendencia la influencia de la hiper interdependencia entre las organizaciones en la era moderna.

Los incidentes de múltiples partes que afectan a numerosas organizaciones que tienen conexiones directas e indirectas con la víctima inicial son una clase problemática de incidentes graves de ciberseguridad. Nuestro estudio reciente sobre este tipo de incidentes, muestra que pueden causar 13 veces el daño financiero que un incidente aislado. Evitar el impacto económico y reputacional de este tipo de incidentes, permite construir el "business case" de una solución de Rating de Proveedores.

CASO PRÁCTICO: ENTIDAD FINANCIERA LIDER EN EEUU

Una de las principales entidades financieras de Estados Unidos, tenía como objetivo prioritario mejorar su Rating y el Riesgo de sus proveedores. El equipo de seguridad, quería analizar las fluctuaciones en la calificación para analizar cambios potencialmente dañinos de tal manera que sirviera como detonante para alertar al CERT.

A modo de ejemplo, las políticas personalizadas para "Riesgo Alto / Crítico" representaban un umbral de tolerancia para administrar y tomar medidas sobre los hallazgos en esta categoría de proveedores. Sin embargo, su objetivo más importante era garantizar que tuvieran una visibilidad completa de sus proveedores críticos. La premisa era: "¿por qué debería comprometerme con un proveedor que suponga un alto riesgo para el negocio?»

Esta compañía tiene un equipo de Gestión de Proveedores de 15 personas, especializadas en la administración de este programa de proveedores, para evaluarlos continuamente y remediar los problemas reportados. Mantener la continuidad del negocio y operar con el nivel de riesgo más bajo posible alimentó su política de "tolerancia cero" para los datos incorrectos que no eran procesables; necesitaban un *scoring* preciso para influir en la corrección del riesgo.

A medida que el nuevo CISO de la empresa impulsaba la inversión en la gestión de riesgos de terceros, se dio cuenta de que había eventos de pérdida de datos o condiciones potencialmente peligrosas que existían dentro de la infraestructura IT de sus proveedores.

El servicio de RiskRecon estuvo completamente operativo en tres semanas y generó un enorme valor para reducir la tasa de falsos positivos, al proporcionar una forma rápida y precisa de evaluar cientos de proveedores críticos. Con todo, el beneficio más importante de la implementación de RiskRecon fue que el rendimiento del programa se alineó bien con el "Rating" de riesgo comercial más grande: tras más de tres años usando RiskRecon para la gestión de proveedores, el riesgo de terceros logró reducirse en más del 50%.

CONCLUSIÓN

En tanto único proveedor de Rating de ciberseguridad que determina automáticamente el valor en riesgo para cada sistema, RiskRecon está en una posición única para proporcionar calificaciones que reflejen el desempeño real del riesgo. El nuevo modelo de calificación permitirá a los clientes comprender y actuar rápidamente sobre su riesgo, enfocándolos rápidamente a los proveedores que los exponen al mayor riesgo y a los problemas más importantes. ■

Vicente de la Morena
Country Leader España y Portugal
RISKRECON

Todo lo que necesita para asegurar su nube.

Simplifique su seguridad en la nube con Trend Micro Cloud One™, la plataforma de servicios de seguridad para desarrolladores líder en el mundo.

Cloud One™
Cloud Security simplificada

La infraestructura global evoluciona con el tiempo pero Trend Micro va por delante optimizando la protección. Creado con datos reales por el artista **Andy Gilmore**.

Descubra Cloud One en este video:

Conozca más en www.trendmicro.es

TREND MICRO™

Secura Security Guardian, orquestador de las tecnologías de seguridad

Dentro del fascinante mundo de la música clásica, existen tres elementos indispensables para poder formar una buena orquesta: los instrumentos, los músicos y el director. Este último encarna la figura más importante. Su exigente puesto requiere de un dominio técnico impecable y un especial talento para relacionarse con los músicos que componen la orquesta. Si no existiera este oficio, podríamos deleitarnos con un concierto solista del mejor violinista del mundo, tocando el mejor violín jamás fabricado, pero sería imposible disfrutar de una orquesta sinfónica en la que todos los instrumentos armonizaran entre sí para crear un sonido mil veces más rico y potente. En el mundo de la seguridad ocurre algo muy parecido. Tenemos grandes tecnologías, grandes profesionales, pero ¿podemos beneficiarnos de la seguridad que ofrecerían si estuvieran bien orquestados? Secura dispone de Security Guardian, un servicio de seguridad gestionada en el que usamos la tecnología de orquestación como batuta, al servicio de nuestros directores: los especialistas en seguridad.

Las compañías han invertido una buena parte de su presupuesto en los mejores instrumentos de seguridad: las tecnologías. El problema es que trabajan de forma inconexa, no son capaces de comunicarse, compartir información y compartir acciones: no funcionan de forma orquestada. No tenemos un orquestador, un director que se comunique, a bajo nivel con los músicos, conozca los instrumentos y tenga en cuenta el objetivo final: proteger a la compañía. Esto limita nuestra capacidad de defensa ante ataques avanzados, a pesar de haber realizado una inversión tremenda en tecnología y esto es algo bien conocido por los atacantes.

Por otro lado, también tenemos a los músicos que tocan esos instrumentos, o a los ingenieros que manejan nuestras herramientas de seguridad. Está claro que un Stradivarius no sonará igual en manos de Joshua Bell que en las de la hija de 6 años de nuestro vecino de al lado. La experiencia lo es todo y el dedicar 8 horas al día a una tecnología, también. Pero ¿cuántas empresas pueden tener a una persona dedicada a una sola tecnología de seguridad durante 8 horas al día? Los ingenieros de seguridad de las compañías se parecen más a un hombre orquesta que a un especialista en un instrumento. En la mayoría de los casos tienen que gestionar decenas de herramientas por lo que apenas tienen tiempo para profundizar en ellas y además mantenerse al día de las últimas tendencias en ataques o amenazas.

Carencias del ecosistema de seguridad

Secura lleva muchos años observando estas carencias del ecosistema de seguridad: de integración de herramientas y de tiempo del personal. Podemos asegurar que aún no hay una solución mágica que orqueste todos los sistemas de forma automática y tome las decisiones correctas sin intervención humana, pero sí hemos encontrado una fórmula muy eficaz que engrana las diferentes tecnologías con la materia gris justa pero necesaria para que la orquesta suene armoniosa.

Para ello hemos diseñado un servicio de gestión avanzado, en el que incluimos herramientas de orquestación y automatización, pero también personal altamente cualificado, que en conjunto hacen funcionar a las tecnologías de protección al unísono y dando lo mejor de cada una, generando una capacidad de detección, prevención y respuesta que ninguna por separado podría conseguir.

Visibilidad y control de la tecnología

Con respecto a la tecnología, nos basamos en un sistema de visibilidad y control, la evolución de lo que en su día fue un sistema de control de acceso, que tiene una gran capacidad de integración con todo tipo de soluciones de seguridad, sistemas y comunicaciones. De esta manera se centraliza el conocimiento de todas las propiedades que las tecnologías de la empresa han descubierto de cada activo en un mismo punto.

En base a este conocimiento profundo de cada activo se crean políticas para automatizar respuestas ante incumplimientos de directrices de seguridad, amenazas y ataques. Estas respuestas no solo son las ofrecidas por la herramienta en sí misma, sino que se extienden a las capacidades de todas las herramientas integradas. Aquí la automatización de acciones es clave para liberar a los codiciados ingenieros y analistas de seguridad de tareas cotidianas y repetitivas, y conseguir que se puedan centrar en otras tareas que sí necesitan de la inteligencia humana. Por ello, al sistema ya mencionado tenemos que añadir una herramienta de inteligencia operacional, que permita a estos expertos analizar en todo momento la gran cantidad de información que nos proporcionan los sistemas para poder alimentar el circulo mejorando la configuración de los sistemas de prevención y respuesta.

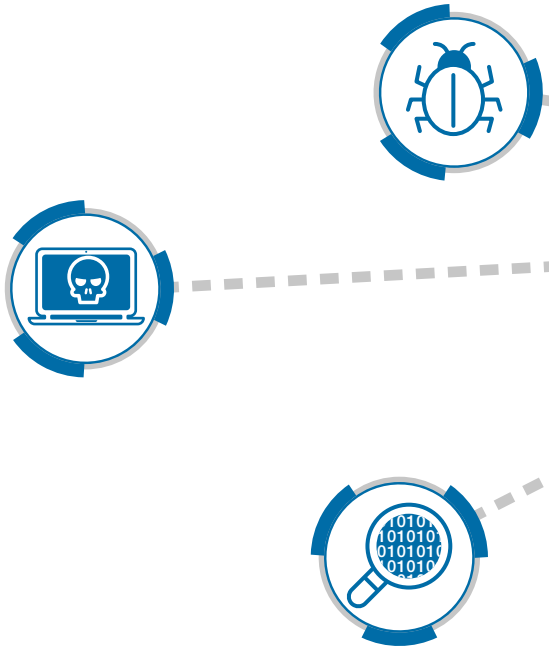
Para tener una mejor visión y ayudar a los especialistas en esa labor, diseñamos cuadros de mando basados en controles CIS, que dibujan estos datos en tiempo real y nos permiten tener ese conocimiento del estado de indicadores clave, y poder establecer una serie de umbrales y alertas. Además, estos cuadros de mando convertidos en informes periódicos, ayudan a los CISOs a demostrar el estado y evolución de la seguridad de la compañía ante la Dirección.

En lo que Secura llama **Security Guardian** un servicio de seguridad gestionada en el que se usa la tecnología de orquestación como batuta, al servicio de nuestros directores: los especialistas en seguridad. ■

Israel Zapata Palacio
Director de Operaciones de Ciberseguridad
SECURA – GRUPO FACTUM
israel.zapata@factum.es

</mónica>

Gestión de eventos e información de seguridad



Reaccione rápidamente ante los ciberataques

Adelántese a ellos y remédielos antes de que sucedan

MÓNICA NGSIEM es el nuevo sistema automatizado de gestión de información y eventos de seguridad desarrollado por ICA Sistemas y Seguridad en colaboración con el Centro Criptológico Nacional. MÓNICA NGSIEM recoge en una única plataforma toda la información existente sobre amenazas potenciales.

ccn-cert centro criptológico nacional

monica@ccn-cert.cni.es • info@grupoica.com

grupo ICA Sistemas y Seguridad

nCipher BYOK: cómo obtener mayor control sobre la seguridad de los datos en Azure

El modelo de responsabilidad compartida que existe cuando una empresa se lleva sus procesos y datos a la nube, revela que las organizaciones son las responsables de controlar la seguridad de los datos que allí depositan. Cuando una empresa delega el cifrado y la seguridad de sus datos en Microsoft Azure, también confía la visibilidad y el control de sus claves de cifrado en el propio proveedor de nube, a no ser que decida lo contrario. nCipher BYOK, distribuido por V-Valley, ayuda a las empresas a tener el control del uso de las claves que usa Microsoft para añadir protección a sus datos.

La transformación digital, el pago por uso, la externalización de servicios... ha llevado a las empresas a mover parte de sus aplicaciones y datos a la nube pública donde la seguridad de los datos que se depositan en la nube son responsabilidad de la propia empresa.

En este ámbito, el proveedor de la nube ofrece *add-ons* de seguridad, entre los cuales está el cifrado de los datos de una máquina virtual (Azure Disk Encryption), el cifrado de los buzones de correo (Office365), el cifrado de las comunicaciones de elementos colaborativos (Teams, SharePoint, OneDrive…), el cifrado de los datos del ERP/CRM (Dynamics 365), de las bases de datos (Azure SQL), la protección de ficheros (Azure Information Protection), etc.

Ese cifrado de datos corporativos en la nube pública se realiza mediante unas claves que han sido generadas, gestionadas y también custodiadas por el proveedor de nube, con lo que las empresas pierden la capacidad de control y visibilidad de sobre el uso que se está haciendo de esas claves.

¿Cómo funciona nCipher BYOK?

Con el uso de BYOK, acrónimo de *Bring Your Own Key*, **nCipher** proporciona los mecanismos necesarios para que una empresa pueda generar sus propias claves con un nShield HSM en propiedad (o un nShield HSM *as a Service*), asegurar su almacenamiento, y finalmente exportarlas, transferirlas y depositarlas de forma segura a uno de los HSMs FIPS 140-2 nivel 3 que componen la infraestructura de HSMs de Microsoft Azure Key Vault, obteniendo seguridad HSM de extremo a extremo.

Si una empresa también está utilizando Amazon Web Services o Google Cloud Platform, sus claves igualmente se podrán transferir a sus respectivas infraestructuras de nube pública. No obstante, debido a la particular arquitectura de estos proveedores de nube pública, después de un periodo de tiempo predeterminado las claves serán destruidas y deberán ser transferidas de nuevo de manera segura desde su HSM local o *as a Service*.

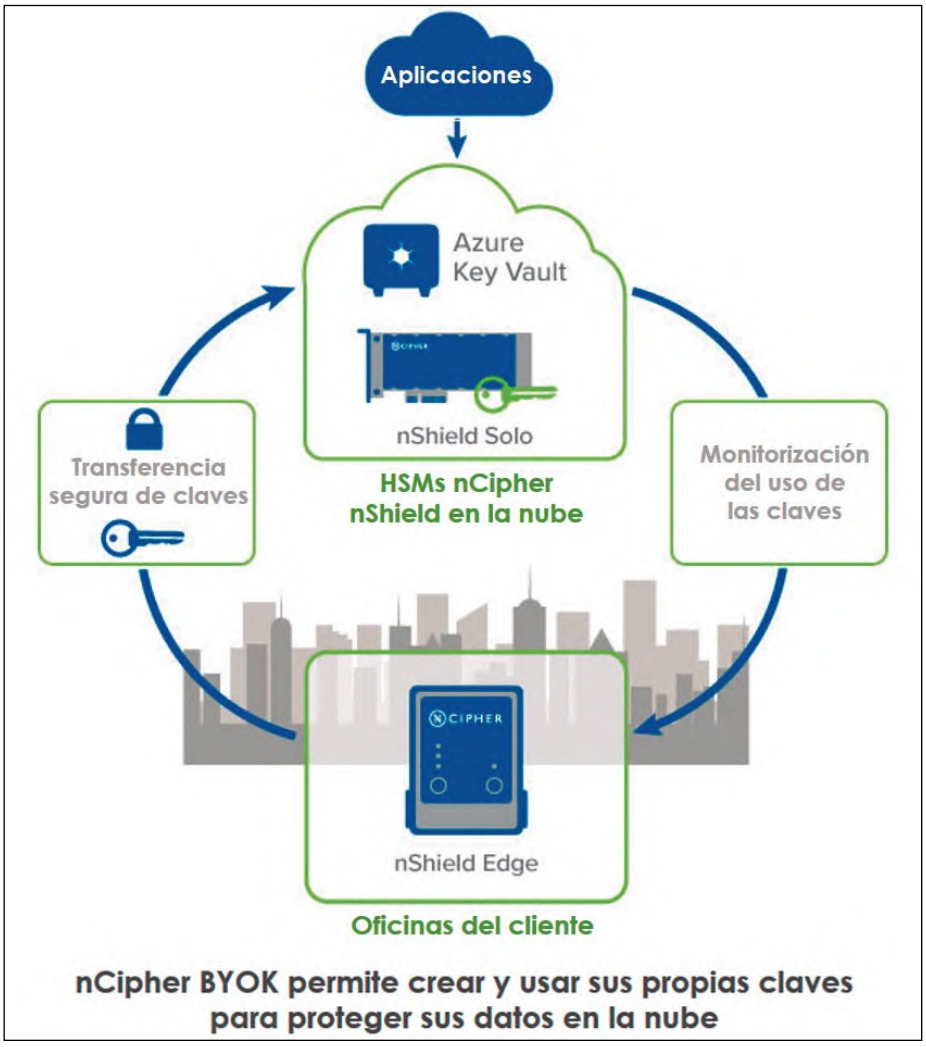
Cualquiera que sea el servicio de nube pública que se elija, la empresa es la responsable de generar su propia clave, de controlar su exportación y transferencia, de aplicar permisos para que únicamente se utilicen para lo que se ha autorizado, y a cambio obtiene una visibilidad que le permite tomar el control sobre la misma.

La transferencia de las claves hacia la nube se realiza de forma segura, y en ningún momento las claves están en claro. Además, una vez dentro de los HSM que tiene Microsoft dentro de su Azure Key Vault, nadie, ni siquiera Microsoft, tendrá la posibilidad de recuperar esas claves y mucho menos, poderlas usar para otro uso que no sea el permitido.

Para ello, cada clave protegida por un HSM tiene asociada una lista de control de acceso (ACL) que define los usos estrictos que van a ser permitidos para esa clave, incluso a nivel aplicaciones o servicios individuales, lo que permite asignar diferentes niveles de seguridad a claves en relación directa con la criticidad de cada aplicación o servicio.

Esta seguridad tan granular permite tener una enorme visibilidad mediante el envío de registros de uso, prácticamente en tiempo real, que informan a una empresa cómo y cuándo se usa cada una de sus claves con Azure Key Vault.

La inversión que una empresa debe realizar para la implementación de nCipher BYOK para proteger sus recursos en Microsoft Azure es tan liviana, tanto en su despliegue, como en sus costes, que muchas empresas deciden planificar dos o tres regeneraciones de sus claves al año, añadiendo la práctica a su plan director de seguridad. ■



nCipher BYOK permite crear y usar sus propias claves para proteger sus datos en la nube

Eduard Alegre Martín
Territory Business Developer
Enterprise Security Division
V-VALLEY

OneseQ by alhambra

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 Continuos Endpoint

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

Akamai EDGE Security, plataforma nativa en la nube verdaderamente distribuida en el borde

La transformación digital hacia un modelo distribuido en cloud ha dado lugar a un modelo de seguridad diferente del que estábamos acostumbrados a ver. En un escenario donde los servicios y los usuarios están distribuidos, también ha de distribuirse la seguridad. Desde Akamai, entendemos este movimiento como la consolidación de lo que llamamos EDGE Security: controles y servicios de seguridad en la nube, donde la escalabilidad y la disponibilidad son características esenciales y no un añadido.

¿Qué es el EDGE?

Desde Akamai entendemos el EDGE como la pieza de arquitectura que une la nube con los dispositivos. El elemento que hace posible que los usuarios consuman los servicios y aplicaciones en la nube.

Este es uno de esos casos en los que una imagen dice más que mil palabras.

En los últimos años, hemos sido testigos de cómo la seguridad existente y las arquitecturas de redes empresariales no tienen sentido en el mundo móvil y en la nube de hoy, donde Internet se está convirtiendo en la WAN corporativa.

El sector de la seguridad está en continua evolución hacia un escenario en el que los controles y servicios de protección deben situarse en la nube, moviéndose a la nueva WAN corporativa. Sin embargo, debemos tener presente otro factor fundamental de este movimiento: *una plataforma robusta, altamente distribuida y resiliente*. Este factor es la clave para hacer frente a un ataque DDoS de 1,3 Tbps, como el que Akamai mitigó el año pasado.

Recientemente, Gartner ha publicado un informe llamado "Tendencias del mercado: cómo ganar cuando WAN Edge y Seguridad convergen en un Servicio de Acceso Seguro Edge", que analiza cómo habilitar la seguridad y los controles de acceso a la red como un servicio desde la nube. El acrónimo SASE, del inglés *Secure Access Service Edge*, es un concepto que combina las funciones de las soluciones de red y puntos de seguridad en un servicio unificado, global, nativo de la nube.

Sin embargo, Akamai EDGE Security va mucho más allá y se convierte en la pieza clave para una estrategia SASE, aportando no sólo la capacidad de desplegar servicios de seguridad en la nube sino también asegurando que éstos puedan interoperar y trabajar de manera colaborativa.

Durante el primer trimestre de este 2020, la plataforma de Akamai ha gestionado más de 13.000 millones de ataques de *bots*, cerca de 1.450 ataques DDoS, 130 TB de datos de ataques dirario y un pico de tráfico en la plataforma de 167 Tbps brindan la información y experiencia que hacen de EDGE Security esa pieza clave.

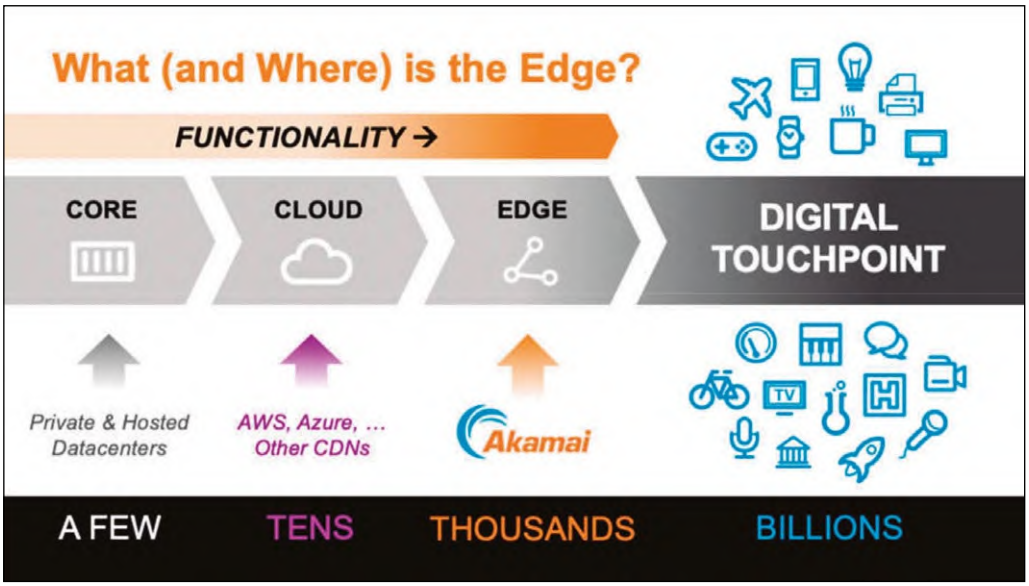
EDGE Security de Akamai se convierte así en una plataforma de seguridad que permite desplegar servicios en la nube tales como:

- Acceso de confianza cero (Zero Trust).
- Prevención / detección de amenazas.
- Aplicación web y protección de API (WAAP).
- Protección DNS y prevención de exfiltración DNS.
- Bot Management.
- Protección contra DDoS.
- Red de entrega de contenido.
- Secure Enterprise Application Access.

Esa traslación de funciones al borde (Edge) también es algo que podemos ver como "transformacional" comportando un valor y una oportunidad. Los patrones de seguridad de redes transformarán el panorama competitivo durante la próxima década y crearán oportunidades significativas para que las empresas reduzcan la complejidad y permitan que su personal de TI elimine aspectos básicos de la red y de las operaciones de seguridad, focalizándose en tareas de mayor valor.

Si usted analiza la historia de Akamai, estos valores y esa lista de capacidades debería resultarle familiar, dado que en Akamai nos hemos centrado en proporcionar capacidades de seguridad en el Edge por más tiempo que nadie.

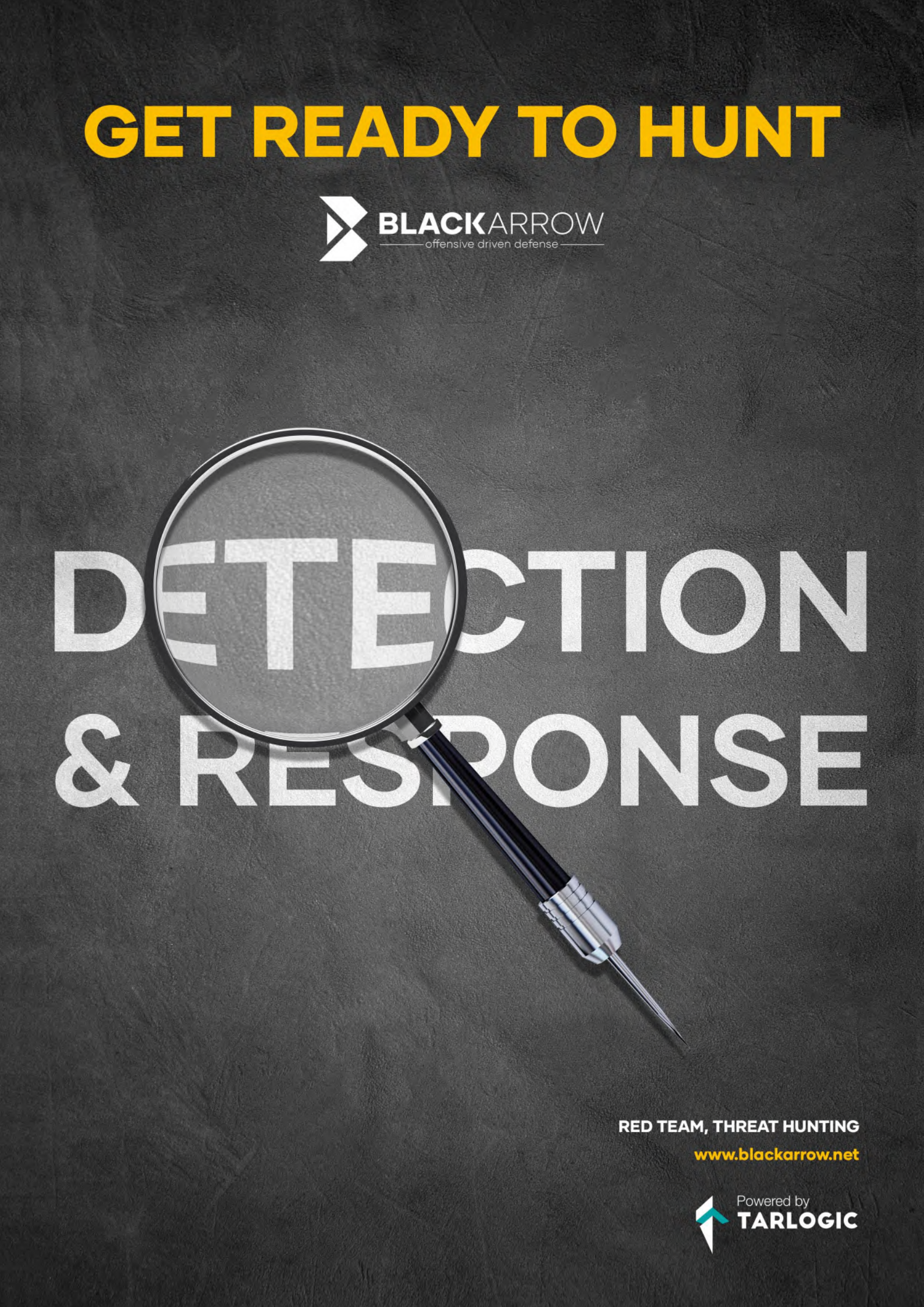
Todo ello muestra que si bien nuestros competidores afirman haber reinventado la rueda mientras construyen silenciosamente sus redes con más PoPs, seguimos creyendo que una plataforma nativa en la nube verdaderamente distribuida en el borde (Edge), combinada con un equipo de expertos en seguridad, es el único camino a seguir. Y esto es particularmente cierto cuando se trata de brindar servicios de seguridad y redes empresariales a escala planetaria a algunas de las organizaciones más grandes del mundo. ■



Federico Dios
Pre-sales Manager
AKAMAI TECHNOLOGIES

GET READY TO HUNT

BLACKARROW
offensive driven defense



RED TEAM, THREAT HUNTING

www.blackarrow.net

Powered by
TARLOGIC

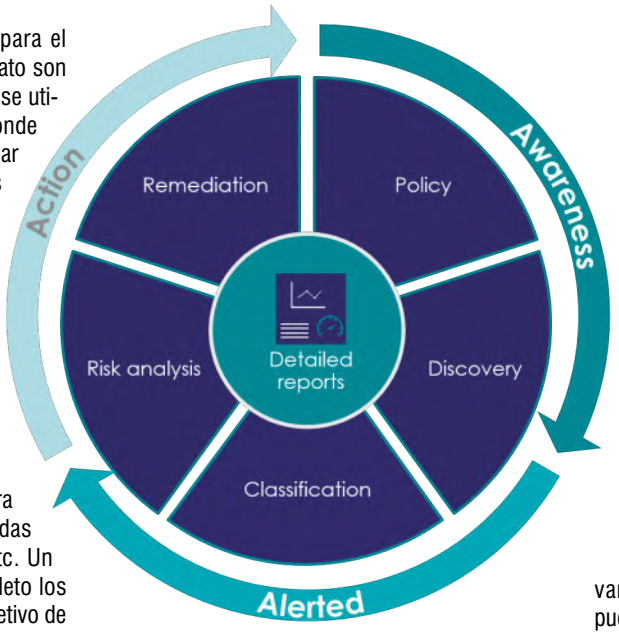
Thales Cipher Trust Data Discovery and Classification, descubrimiento y clasificación de los datos confidenciales de todos los servidores ya sean en la nube o Big Data de una organización

Thales Cipher Trust Data Discovery and Classification es una solución que permite descubrir y clasificar los datos confidenciales de todos los servidores, ya sean en la nube o Big Data, que hay dentro de una organización. A través de una consola centralizada y con unas plantillas de clasificación que contienen todas las regulaciones vigentes, se pueden identificar tras un análisis exhaustivo dónde se localiza la información sensible. Este análisis detecta puntos ciegos en materia de seguridad, lo que nos permitiría justo después cifrarla allí donde se encuentre con las soluciones de Thales para subsanar esas deficiencias. Además, proporciona informes detallados que son de gran utilidad para los auditores, ya que pueden demostrar el cumplimiento de todas las legislaciones vigentes.

El primer y más importante paso para el cumplimiento normativo es saber qué dato son sensibles, dónde se almacenan y cómo se utilizan. Si desconoce qué datos tiene, dónde están y por qué los tiene, no podrá aplicar políticas ni controles efectivos con vistas a protegerlos.

Thales CipherTrust Data Discovery and Classification ofrece un conjunto de plantillas predefinidas que permiten identificar con eficacia los datos regulados (tanto estructurados como no estructurados) en todos los almacenes de datos de su empresa, ya sean en la nube, Big Data o en los almacenes de datos tradicionales. Además, es lo suficientemente flexible como para gestionar políticas personalizadas basadas en patrones específicos, algoritmos, etc. Un único panel permite conocer por completo los datos sensibles y sus riesgos, con el objetivo de que se puedan tomar mejores decisiones para subsanar deficiencias, priorizar correcciones o garantizar la transformación a la nube y el intercambio de datos con terceros.

Al contrario que las soluciones inconexas alternativas que pueden someter los datos a exposición o peligro, Thales CipherTrust Data Discovery and Classification ofrece un flujo de trabajo optimizado en todo el proceso, desde el establecimiento, el descubrimiento y la clasificación de políticas, hasta el análisis y la notificación de riesgos. Esto elimina los puntos ciegos y dificultades en materia de seguridad. En consecuencia, se pueden descubrir y mitigar más fácilmente los riesgos de privacidad de los datos, hacer cumplir la soberanía de los datos y responder de manera proactiva a un creciente número de normativas en materia de seguridad y privacidad en esta materia, como el RGPD, la CCPA, el PCI DSS y la HIPAA.



La consola centralizada muestra datos e informes, que pueden ayudar a tomar decisiones fundamentadas en cuanto al intercambio de datos, la transformación digital o la priorización de correcciones desde una única consola, así como ayudar a sus auditores a demostrar el cumplimiento de distintas legislaciones reguladoras y comerciales.

Asimismo los análisis eficientes permiten sentar una base sólida para la privacidad y la seguridad de los datos en general.

La solución implementa un flujo de trabajo optimizado que reduce significativamente la complejidad y los riesgos para la organización.

Los análisis eficaces ayudan a descubrir los datos estructurados y no estructurados de un conjunto heterogéneo de almacenes de datos, sentando una base sólida para la privacidad y la seguridad de los datos en general.

Una vez identificados los datos, nuestra completa *suite* de soluciones de cifrado y gestión de claves criptográficas de Thales permitirá al usuario planificar la estrategia e implementar el cifrado allí donde se requiera.

Tipos de archivos compatibles

- Bases de datos: Access, DBase, SQLite, MSSQL MDF y LDF
- Imágenes: BMP, FAX, GIF, JPG, PDF (incrustado), PNG, TIF
- Archivos comprimidos: bzip2, Gzip (todos los tipos), TAR, Zip (todos los tipos)
- Microsoft Backup Archive: Microsoft Binary / BKF
- Microsoft Office: v5, 6, 95, 97, 2000, XP, 2003 y posteriores
- Fuente abierta: Star Office / Open Office
- Estándares abiertos: PDF, HTML, CSV, TXT

Tipos de datos identificados

- Sanitarios (Tarjeta Sanitaria Europea, número de seguro de salud para EE. UU., etc.)
- Financieros (números de tarjetas American Express, Diners Club, Mastercard y VISA; número de cuenta bancaria, etc.)
- Personales (nombre, apellidos, dirección, fecha de nacimiento, correo electrónico, etc.)
- Identificación nacional (número de seguridad social, número de DNI, etc.)

Plantillas incorporadas

La solución de Thales incluye una amplia variedad de plantillas listas para su uso que pueden ayudar a cumplir los requisitos habituales de las políticas normativas y empresariales. Por ejemplo:

- CCPA
- RGPD
- HIPAA
- PCI DSS
- Información de identificación personal
- Información de salud protegida

■

Alfonso Martínez
Country Manager Spain & Portugal
THALES CPL, Data Protection

Incremente su ciberseguridad sin aumentar los recursos

Las tecnologías de ciberseguridad, con EDR en el núcleo, han sido aclamadas por el sector y por los clientes, y le permiten detectar y evitar ataques evasivos a gran velocidad, sin que su equipo tenga que realizar ningún esfuerzo adicional.

Kaspersky Endpoint Security

kaspersky BRING ON THE FUTURE

kaspersky.es

KASPERSKY AMPLÍA LA VISIBILIDAD SOBRE EL SHADOW IT CON LA NUEVA VERSIÓN DE ENDPOINT SECURITY CLOUD QUE PERMITE CREAR SERVICIOS EN NUBE DE CONFIANZA

El uso de soluciones de mensajería, servicios de intercambio de archivos o cualquier tipo de herramienta de trabajo colaborativo ha aumentado en los últimos meses ayudando a las empresas a ganar en agilidad, trabajar a distancia y mantener a los empleados conectados. Sin embargo, las amenazas asociadas a ellas por un uso inapropiado, más allá del corporativo, ha hecho crecer los riesgos fuera del alcance de los responsables de ciberseguridad.

Para hacer frente a este problema, **Kaspersky** ha actualizado su solución **Kaspersky Endpoint Security Cloud**, con una versión que se centra en aumentar la visibilidad del Shadow IT con el objetivo de que sólo se utilicen servicios en la nube de confianza dentro de la organización. En concreto, la funcionalidad Cloud Discovery permite establecer una lista de servicios en nube autorizados que cumplan con las políticas de seguridad corporativas, y poder certificar que se "cumple" dicha lista. Así, los datos sobre las categorías de servicios utilizados y las aplicaciones se puede ver, de forma sencilla, en un cuadro de mando en el que un administrador puede ajustar el acceso para diferentes perfiles de usuario, estableciendo privilegios para diferentes grupos de trabajadores, según sus necesidades.

Además, para ayudar a las organizaciones a proteger su correo-e en la nube y las herramientas de colaboración, Kaspersky Endpoint Security Cloud incluye ahora su solución Kaspersky Security para Microsoft Office 365. Gracias a ello, la compañía extiende su protección a todas las aplicaciones de este paquete de Microsoft, incluyendo Exchange Online, OneDrive y SharePoint Online, además de asegurar el intercambio seguro de archivos a través de la herramienta Teams.

La seguridad frente a las amenazas del correo-e se habilita a través de un motor anti-*phishing* basado en una red 'neural' que utiliza más de 1.000 criterios para detectar correos electrónicos fraudulentos, así como una base de datos de URL maliciosas, anti-*spoofing* y de prevención para evitar que el correo electrónico empresarial se vea comprometido. Además, su capacidad de análisis de los archivos en SharePoint Online, OneDrive y Teams permite detectar y contener el *malware* y que no se extienda a los distintos puntos finales corporativos.

KASPERSKY
www.kaspersky.es

OKTA MEJORA LA PROTECCION DE LAS IDENTIDADES Y LOS ACCESOS COMBINANDO SUS SOLUCIONES CON LA CAPACIDAD DE DETECCIÓN DE RIESGOS EN PUNTOS FINALES

Okta ha reforzado la integración entre su plataforma de gestión de identidades y accesos (IaM), **Okta Identity Cloud**, y las herramientas de seguridad de punto final de **VMware Carbon Black, CrowdStrike** y **Tanium**, en un paso más para proveer una seguridad centrada en el enfoque de Cero Confianza o Zero Trust.

Si bien la compañía siempre ha puesto a disposición de las empresas interfaces de programación de aplicaciones (APIs) para favorecer la integración de sus productos, ahora, Okta ha querido proporcionar un mayor nivel de interoperabilidad con soluciones de ciberseguridad de terceros, combinando la detección de los riesgos en el punto final con la protección de la identidad digital del usuario.

En este caso, la interoperabilidad es posible gracias, por un lado, a la aplicación Verify de Okta, que se ejecuta en el *endpoint* y es compatible con los sistemas operativos más utilizados, como iOS, iPadOS, macOS, Android y Windows, así como con las soluciones de gestión y seguridad de puntos finales implementadas en ellos. Y, por otro lado, gracias al servicio Okta Devices Platform Service, que recopila datos de esos puntos finales.

Así, la plataforma Okta Identity Cloud puede crear un perfil de riesgo de un intento de inicio de sesión individual utilizando los datos recopilados para determinar los niveles de acceso según el dispositivo empleado y otros parámetros, como si el sistema operativo está actualizado, el cortafuegos ha sido deshabilitado, etc. En caso de detectarse un problema, la solución deniega el acceso o solicitar un factor de autenticación adiciona.

Por otro lado, en junio, Okta firmó un acuerdo con el mayorista **Ingecom** para distribuir, en Iberia sus soluciones de gestión de acceso de identidad.

OKTA
www.okta.com

WATCHGUARD Y DEUTSCHE TELEKOM PONEN SEGURIDAD AVANZADA AL ALCANCE DE LAS PEQUEÑAS Y MEDIANAS EMPRESAS A TRAVÉS DE SU PROPUESTA BNP COMPLETE

WatchGuard Technologies ha puesto a disposición de las pequeñas y medianas empresas la solución **Business Network Protect (BNP) Complete**, creada en colaboración con **Deutsche Telekom**, con la que quieren dotar de seguridad avanzada a aquellas organizaciones o entornos de oficinas que carecen de los recursos necesarios para defenderse de forma adecuada contra los ciberataques.

Para conseguirlo, bajo la solución BNP Complete 'se esconde' un módem DSL y un *router wi-fi* con protecciones de clase empresarial; todo ello, dentro del *appliance* Firebox T35-DW de WatchGuard.

La ventaja de esta solución, según sus responsables, reside en su segmentación, con áreas de red de misión crítica individuales, como los sistemas de producción, los servidores de gestión, los componentes de VoIP y las impresoras, aseguradas individualmente y controladas automáticamente. Esta segmentación hace que sea

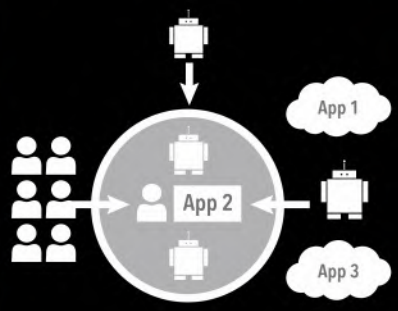
más sencillo identificar los posibles puntos débiles, iniciar contramedidas y evitar que los ataques se propaguen libremente por las redes.

Entre los servicios más destacados que ofrece BNP Complete se encuentran desde el bloqueo de APTs, hasta un *gateway* antivirus, prevención de spam, filtrado URL, control de aplicación, prevención de intrusiones e inspección SSL, entre otros muchos. Además, transmite y procesa automáticamente datos de más de 180 sensores de *honeypot* de Deutsche Telekom para reconocer y bloquear IP maliciosas.

Esta solución está pensada para dar seguridad a conexiones de hasta 200 Mbps máximo, cubriendo hasta 20 puestos de trabajo. La licencia de protección básica incluye todos los componentes de hardware, el EWS de Deutsche Telekom y el paquete de servicios de seguridad gestionada 'Helpdesk Service Plus'.

WATCHGUARD TECHNOLOGIES
www.watchguard.com/es

Edge Security:
Es hora de adoptar un perímetro en la Nube



- No hace falta distinguir entre tráfico externo o interno
- Todo es externo, igual que en Internet

ZERO TRUST

- 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

Akamai

CHECK POINT AMPLÍA SU ARQUITECTURA INFINITY CON LOS QUANTUM SECURITY GATEWAY

Check Point ha incorporado a su arquitectura Infinity una completa de gama de *gateways* de seguridad, denominada **Quantum Security Gateway**, con la que la compañía da un paso más para aunar en un *appliance* un alto rendimiento y técnicas de prevención de amenazas de última generación.

Para ello, la nueva familia de dispositivos incluye el producto estrella de la compañía, Check Point SandBlast Zero Day Protection, que cuenta con más de 60 servicios centrados en la prevención de amenazas y en la inspección de tráfico encriptado SSL a gran velocidad.

Entre sus características técnicas, estos dispositivos destacan por su escalabilidad, preparados para soportar hasta 1,5 Tbps de rendimiento en prevención de amenazas. Además, todos ellos son compatibles con los últimos modelos de CPU, cuentan con unidades de estado sólido (SSD) y su modularidad permite su adaptación a cada empresa con múltiples ranuras de expansión.

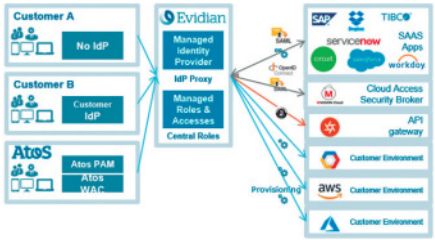
Cobertura desde pymes a grandes empresas

La familia Quantum se compone de seis tipos de *appliances* ajustándose a las necesidades de cualquier tamaño de empresa. Así pues, las gamas **Quantum 3600 - 3800**, **6200 - 6400**, y **6600 - 6700**, están detinadas a la pymes, con rendimientos que llegan desde los 1,5 a los 7,6 Gbps contra los ataques de día cero. Las unidades dedicadas a las grandes empresas y centros de datos (CPDs), como las gamas **7000 y 16200**, disponen de un rendimiento de hasta 15 Gbps contra los ataques de día cero, y los modelos **26000 y 28000** aseguran los CPDs con un rendimiento de prevención de amenazas de hasta 30 Gbps. Asimismo, el *gateway* **Quantum Hyperscale 16600**, diseñado con un factor de forma condensado de 1RU, permite crear sistemas de seguridad con un rendimiento de hasta 850 Gbps contra ataques de día cero.

CHECK POINT
www.checkpoint.com

ATOS EXTIENDE SU CARTERA DE GESTIÓN DE IDENTIDADES Y ACCESOS CON EVIDIAN IDAAS

Bajo la denominación **Evidian IDaaS,** la firma francesa, **Atos,** ha puesto a disposición de sus clientes un nuevo servicio de gestión de aplicaciones para dar solución a los problemas de seguridad que surgen derivados una administración de las identidades digitales inadecuada, tanto a la hora de acceder a las aplicaciones en local como SaaS, un problema que aumenta a medida que las empresas migran sus infraestructuras de TI a la nube.



En este contexto, Evidian ofrece, entre sus principales características, un sistema de acceso seguro bajo la modalidad como servicio (IDaaS) a aplicaciones en línea en un entorno donde reemplaza las tradicionales contraseñas por un sistema *single sign-on* (SSO) federado, con el cual, permite a los usuarios acceder a múltiples servicios con un solo inicio de sesión. Además, incluye mecanismos de autenticación multifactor compatible con estándares como FIDO 2, así como con diferentes sistemas biométricos y de infraestructura de clave pública (PKI), entre otros.

Cabe destacar, también, que este nuevo servicio está basado en la plataforma Google Cloud, que permite cumplir con diferentes normativas, como el Reglamento de Protección de Datos de la UE (RGPD), y otras específicas de la industria, como la regulación europea para servicios de pagos electrónicos, PSD2, y con la Health Insurance Portability and Accountability Act (HIPAA) norteamericana, para el sector de Salud.

ATOS
https://atos.net

DOTFORCE ACERCA A ESPAÑA LAS TECNOLOGÍAS DE CIBERINTELIGENCIA DE LOOKINGGLASS CYBER, ZEROFOX Y AGARI

La ciberinteligencia se está convirtiendo en una poderosa herramienta por la que cada vez más apuestan las compañías a la hora de adoptar una estrategia proactiva de ciberseguridad. Para facilitar su adopción en España, **DotForce** ha incorporado a su catálogo las herramientas de **LookingGlass Cyber, ZeroFOX** y **Agari**. Además, hasta el 31 de agosto, el mayorista ofrece un estudio, sin coste, para aquellas organizaciones interesadas en conocer su nivel de exposición a los riesgos en la red.

Las herramientas que ofrece DotForce permiten a las organizaciones descubrir agujeros de seguridad y amenazas avanzadas, incluyendo aquellas que están ocultas en la Deep y en la Dark Web, de forma automatizada. Un aspecto clave en estas herramientas, ya que en ciberinteligencia es muy complicado abarcar el amplio espectro de ciberamenazas únicamente con trabajo manual.

Por una parte, **LookingGlass Cyber** está especializada en mitigación de riesgos mediante técnicas de Inteligencia Artificial, incluyendo la monitorización de la superficie de ataque, *threat modeling* y defensa de las redes. Su portafolio de servicios globales integra desde inteligencia de amenazas y análisis, hasta un conjunto de herramientas para la mitigación de amenazas en la red. Unas capacidades que ofrece tanto a través de soluciones genéricas, como a medida.

Protección en entornos sociales y correo-e

ZeroFOX, por su parte, está más enfocada en la seguridad de entornos digitales de redes sociales y plataformas de colaboración (como LinkedIn, Facebook, Slack, Twitter, Instagram, YouTube...), protegiendo a las organizaciones de las amenazas que atenten contra su marca, su reputación e, incluso, de los riesgos físicos, realizando detecciones tanto en dichas apps, como en tiendas de aplicaciones móviles, la Deep y la Dark Web y otros dominios de Internet.

Para ello, utiliza diversas fuentes de datos y análisis basados en inteligencia artificial que nutren la plataforma ZeroFOX, a fin de identificar y dar remedio a los ataques de *phishing*, el robo de credenciales, exfiltración de datos, secuestro de marcas y amenazas a ejecutivos, entre otras muchas.

Tanto LookingGlass como ZeroFOX, además, ofrecen servicios de eliminación de cuentas y dominios falsos que se estén utilizando con el propósito de cometer fraude y falsificación de identidades y productos. Un problema que está creciendo de forma exponencial en los últimos meses.

Finalmente, la tecnología de Agari se centra, en la protección del correo electrónico frente a amenazas avanzadas, como las estafas BEC (Business Email Compromise), combinando la autenticación DMARC con **Agari Brand Protection** para asegurar que el remitente de cada correo-e pertenece a la organización que su dirección de correo indica. Además, **Agari Secure Email Cloud** cuenta con inteligencia artificial capaz de entender las intenciones maliciosas de los correos-e engañosos.

DOTFORCE
www.dotforce.es

Cuando la empresa se extiende,
los riesgos de seguridad también.

Si sus socios no tienen
la protección adecuada
y su sistema sigue vigilando
los puntos vulnerables de siempre,
el objetivo del ataque será
el que menos espera.

Sothis

SAPSecure

Aumente la protección de su empresa,
protegiendo el centro de sus procesos
de negocio: el ERP

www.sothis.tech

PULSE SECURE AVANZA HACIA EL MODELO 'CERO CONFIANZA' CON SU GAMA PULSE ACCESS SUITE PLUS

Con el objetivo de ofrecer a las empresas una solución de acceso seguro a las aplicaciones e infraestructuras de TI híbridas, independientemente del dispositivo que utilicen, la red y su ubicación, **Pulse Secure** ha creado una *suite* modular e integrada que unifica la gestión del control de acceso bajo el modelo Zero Trust.

Se trata de **Pulse Access Suite Plus,** una evolución de la *suite* del mismo nombre, lanzada en 2017, en la que la compañía mejora su interoperabilidad, consolidando herramientas de control de acceso de seguridad dispares en una única plataforma integrada, además de añadir una mejor gestión y opciones de escalado.

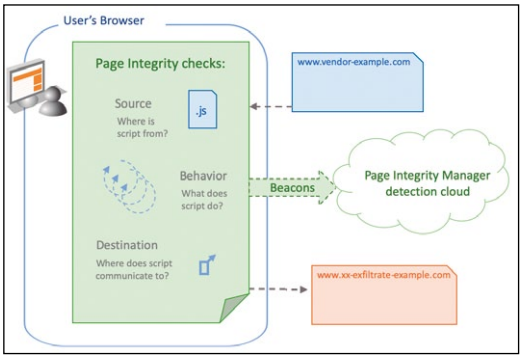
Entre las funcionalidades de esta nueva *suite* se encuentran el control de identidad adaptativa, autenticación multifactor (MFA) y *single sign-on* (SSO), control de cumplimiento de dispositivos y gestión de dispositivos móviles (MDM), control de acceso a la red (NAC), análisis avanzado de comportamiento de usuarios y entidades (UEBA), detección de anomalías, niveles de servicio y garantía de alta disponibilidad a través del controlador virtual de entrega de aplicaciones (ADC) así como seguridad WAF (Web Application Firewall). Todo, bajo una gestión centralizada gracias a la plataforma Pulse One.

Para dar cabida a las distintas necesidades de las organizaciones, Pulse Access Suite Plus se presenta en tres versiones: Essentials, Advanced y Enterprise. Cada una de ellas extiende las funcionalidades de Secure Access necesarias para soportar el control en entornos de TI híbridos, aplicando el modelo de Zero Trust, por el que decididamente apuesta este fabricante.

PULSE SECURE
www.pulsesecure.net

AKAMAI AFRONTA LAS CIBERAMENAZAS DE LOS NAVEGADORES WEB CON PAGE INTEGRITY MANAGER

Page Integrity Manager es el nombre con el que **Akamai** ha presentado su nueva solución de detección de amenazas, enfocada en dar visibilidad y gestionar los riesgos relacionados con los *scripts* de las páginas web que muchos atacantes utilizan para robar datos de usuario o afectar a la experiencia de este.



De hecho, estos tipos de ciberataques fueron popularizados por los grupos Magecart y, en la actualidad, se ha convertido en una fuente frecuente de filtraciones de datos.

Uno de los mayores problemas que tienen los equipos de seguridad es la poca visibilidad y control sobre los *scripts* proporcionados y mantenidos por terceros. Estos *scripts* son esenciales para una experiencia de usuario dinámica de los sitios web, incluidas las páginas de información confidencial utilizadas para formularios de pagos, gestión de cuentas e información personal. Sin embargo, pueden contener vulnerabilidades que podrían traducirse en el robo de datos confidenciales.

Así pues, la solución de Akamai nace para proteger los sitios web de amenazas JavaScript, como el robo de información web, el *formjacking* y los ataques de Magecart, mediante la identificación de recursos vulnerables, la detección de comportamientos sospechosos y el bloqueo de actividades maliciosas.

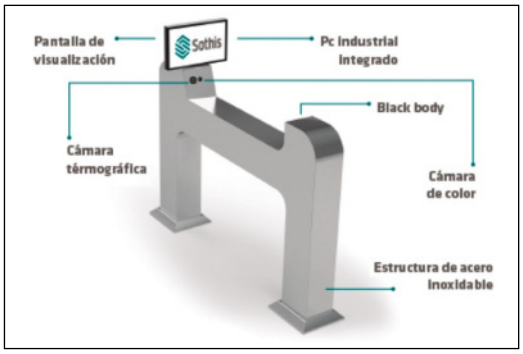
Una de sus características principales es que la solución se integra en el navegador y permite detectar la actividad de *scripts* sospechosos en tiempo real, ofreciendo una forma más eficaz de detener los ataques ocultos a la cadena de suministro, cuando se producen.

AKAMAI
www.akamai.com/es

SOTHIS CREA UNA NOVEDOSA SOLUCIÓN DE CONTROL DE LA TEMPERATURA PARA EL ACCESO A INSTALACIONES

La valenciana **Sothis** ha puesto en marcha un novedoso sistema de medición de temperatura corporal en tiempo real. Este sistema pionero en España ayuda a identificar de manera eficaz a las personas con fiebre en los accesos a instalaciones.

Así, **Thermal Vision System** realiza mediciones en menos de un segundo y sin necesidad de contacto, lo que además de evitar riesgos, permite evitar colas o retrasos en las entradas y salidas, especialmente en los espacios en los que se prevé un gran flujo de personas, como accesos a edificios de oficinas, plataformas industriales o zonas comerciales.



Una de sus principales ventajas respecto a otras soluciones es que combina cámaras termográficas con un software propio, desarrollado por Sothis, que incorpora inteligencia artificial para medir la temperatura únicamente tomando como referencia el lacrimal de los ojos, que es la zona más precisa.

Cuando la persona pasa por delante del sistema se realiza la medición y en función de la temperatura corporal detectada se prosigue con el protocolo de seguridad establecido por el responsable del edificio. Tanto si la persona puede pasar en caso de no detectar fiebre, o si se ha detectado temperatura elevada, el mensaje que muestra la pantalla es personalizable para cada cliente.

El prototipo del sistema Thermal Vision System de Sothis ya se ha instalado en Valencia, a través de un acuerdo con Marina de Empresas. Los accesos al edificio se han convertido en los primeros en incorporar esta tecnología especialmente orientada a mejorar la prevención en los accesos de trabajadores en sectores industriales, oficinas o retail, como locales comerciales.

Por otro lado, Sothis continúa su crecimiento en Iberia con 180 nuevas incorporaciones, una plantilla que roza los 900 empoleados y superando los 300 clientes. Además ha puesto en marcha junto a la Universidad Politécnica de Valencia la Catedra de transformación Digital.

SOTHIS
www.sothis.tech

Pulse Secure®

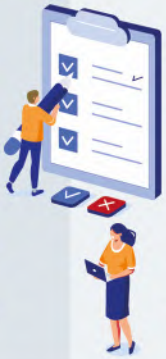
2020 ZERO TRUST PROGRESS REPORT

ZERO TRUST CONFIDENCE IS MIXED

Confidence in applying Zero Trust model in their Secure Access architecture

THE TOP 5 ZERO TRUST ACCESS

TENETS		DRIVERS	
1 Continuous authentication, authorization	67%	85%	Security/ data protection 1
2 Trust earned through entity verification	65%	70%	Breach prevention 2
3 Data protection	63%	56%	Reduce endpoint and IoT security threats 3
4 End-to-end access visibility and audit	56%	52%	Reduce insider threats 4
5 Facilitate least privilege access	54%	43%	Industry/regulatory compliance 5



ZERO TRUST PRIORITIES

71% gearing up to improve their Identity and Access Management (IAM)

45% concerned with public cloud application access security, and **43%** with BYOD exposures

30% seeking to simplify secure access delivery including enhancing user experience and optimizing administration and provisioning

53% plan to move Zero Trust access capabilities to a hybrid IT implementation

PUTTING ZERO TRUST TO WORK

29% have a model in place or underway

43% have projects planned

27% have no plans or are unfamiliar

ZERO TRUST SPEND

40% increase budget

45% same budget

15% decrease budget

ZERO TRUST WHEN

37% have implemented or will implement

28% have no plans

36% plan to adopt in > 10 months

ZERO TRUST ACCESS DEPLOYMENT

25%	plan to solely use SaaS-based Zero Trust Access capabilities
53%	plan to implement Zero Trust Access capabilities on-premises and SaaS (hybrid IT)
11%	are satisfied with our current in-house Secure Access implementation to consider SaaS-based Zero Trust access
11%	expressed too many legacy applications or compliance restrictions to consider SaaS-based Zero Trust access

Get the complete 2020 Zero Trust Progress Report at
www.pulsesecure.net/resource/2020zero-trust-report

Source: © CyberSecure Insiders "2020 Zero Trust Progress Report" sponsored by Pulse Secure. n=413

Pulse Secure®

EXCLUSIVE NETWORKS AYUDA A PROTEGER LOS DATOS SENSIBLES CON LA PLATAFORMA TECNOLÓGICA DE VARONIS

Exclusive Networks ha comenzado a comercializar la plataforma de seguridad de datos unificada de **Varonis**, que permite proteger los archivos y ficheros de ciberataques y amenazas internas, a través del comportamiento de las personas y las máquinas que acceden a los datos, alertando, y ejecutando respuestas automáticas.

Esta protección también cuenta con capacidades de detección de *ransomware*, funciona buscando dónde están sobreexpuestos los datos sensibles, sin que se interrumpa el proceso de negocio. Para ello, 'construye' un contexto alrededor del contenido de los datos y de su actividad y permite automatizar la detección de amenazas aplicando modelos predictivos.

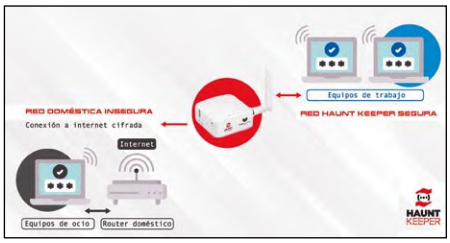
Las soluciones para el gobierno de datos como la suite integrada **DatAdvantage** y el marco de metadatos **Varonis Metadata Framework** también intentan dar respuesta, según explica el distribuidor, a la protección de datos no estructurados a través de técnicas de inteligencia para el control de acceso, del contenido y de la actividad de dicho acceso. Así, las empresas pueden emplear estos metadatos para tareas como la revisión de derechos, auditorias de conformidad, identificación de propietarios de datos, administración de registros, migración de dominios y datos, entre otros.

EXCLUSIVE NETWORKS
www.exclusive-networks.com

WISE SECURITY GLOBAL CREA UNA SOLUCIÓN PARA ASEGURAR LOS DATOS CORPORATIVOS QUE SE USEN DESDE ENTORNOS DOMÉSTICOS

Wise Security Global ha creado la solución **Haunt Keeper**, diseñada para proteger las redes domésticas que se usen para el teletrabajo gracias a que permite crear un entorno más seguro para los datos corporativos.

Se trata de un *router* wi-fi de pequeñas dimensiones que incluye las medidas de protección imprescindibles para aumentar la protección de la red de trabajo, como el bastionado del punto de acceso *wi-fi*, el aislamiento total de la red, la 'tunelización' de las comunicaciones, filtrado de contenidos e, incluso, sistemas avanzados de detección de ataques e intrusiones.



Además, permite que el resto de sistemas IT/IoT del hogar mantengan su conectividad habitual a Internet a través de la red doméstica, que seguirá funcionando en paralelo, pero sin visibilidad de la red segura generada por Haunt Keeper.

Cada *router* es gestionado a través de la aplicación Haunt Manager, permitiendo a los especialistas de ciberseguridad de Wise administrar y configurar en remoto el parque de equipos desplegados. No obstante, aquellas empresas que cuenten con los recursos necesarios pueden encargarse de su propia administración. Además, utiliza tecnología de certificación electrónica mediante la solución de 'ciber' notario Mee, diseñada por Wise, que se emplea como medida anti*phishing* y para corroborar la autenticidad de cualquier notificación enviada al usuario.

WISE SECURITY GLOBAL
www.wsg127.com

GMV OFRECE DIAGNÓSTICO DE SEGURIDAD 'EXPRESS' PARA SISTEMAS DE ACCESO REMOTO

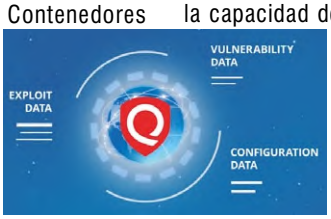
Debido a la situación provocada por la Covid-19, muchas compañías se han visto obligadas, de forma urgente, a proporcionar acceso remoto a sus empleados con el fin de garantizar la continuidad de las operaciones. La premura con la que se han realizado estos despliegues de contingencia ha introducido numerosas vulnerabilidades en los sistemas de acceso remoto, muchas de las cuales han intentado explotar los cibercriminales, sobre todo los sistemas VPNs y escritorios virtuales (VDIs).

Ante este escenario, **GMV** ha comenzado a ofrecer un '**Diagnóstico Express de Seguridad**', con el objetivo de proporcionar un diagnóstico rápido de los sistemas de acceso remoto enfocado en la identificación de las vulnerabilidades más relevantes, de forma rápida y confiable. Como parte de este servicio, los auditores generan dos informes: uno de progreso a mitad del proceso, para agilizar la remediación de las posibles vulnerabilidades detectadas, y otro final que incluye las vulnerabilidades y las resoluciones recomendadas por GMV.

GMV
www.gmv.com/es

QUALYS FACILITA LA GESTIÓN DE VULNERABILIDADES EN AZURE PARA MÁQUINAS VIRTUALES Y CONTENEDORES

Qualys anuncia que, en junio, su plataforma **Qualys Vulnerability Management** estará disponible en el Centro de Seguridad de Microsoft Azure. Esta solución aprovecha el Agente Cloud de Qualys y sus Sensores de Contenedores embebidos para automatizar la gestión de vulnerabilidades en el *pipeline* de CI/CD, así como la visibilidad en tiempo real de las instancias virtuales en ejecución.



Por su parte, Qualys Vulnerability Management analiza de forma automática las máquinas virtuales y las imágenes de los contenedores en Azure, proporcionando a los clientes mayor visibilidad de las posibles vulnerabilidades y de los problemas de configuración. En caso de que se descubra un fallo de seguridad, éste es reportado a Azure Security Center, incluyendo la capacidad de crear *playbooks* para remediarlo, de forma sencilla, sin necesidad de desplegar o actualizar ningún software. Esta capacidad está disponible para los clientes de Azure Security Center para máquinas virtuales y de Azure Kubernetes Services.

QUALYS
www.qualys.com

BREVES

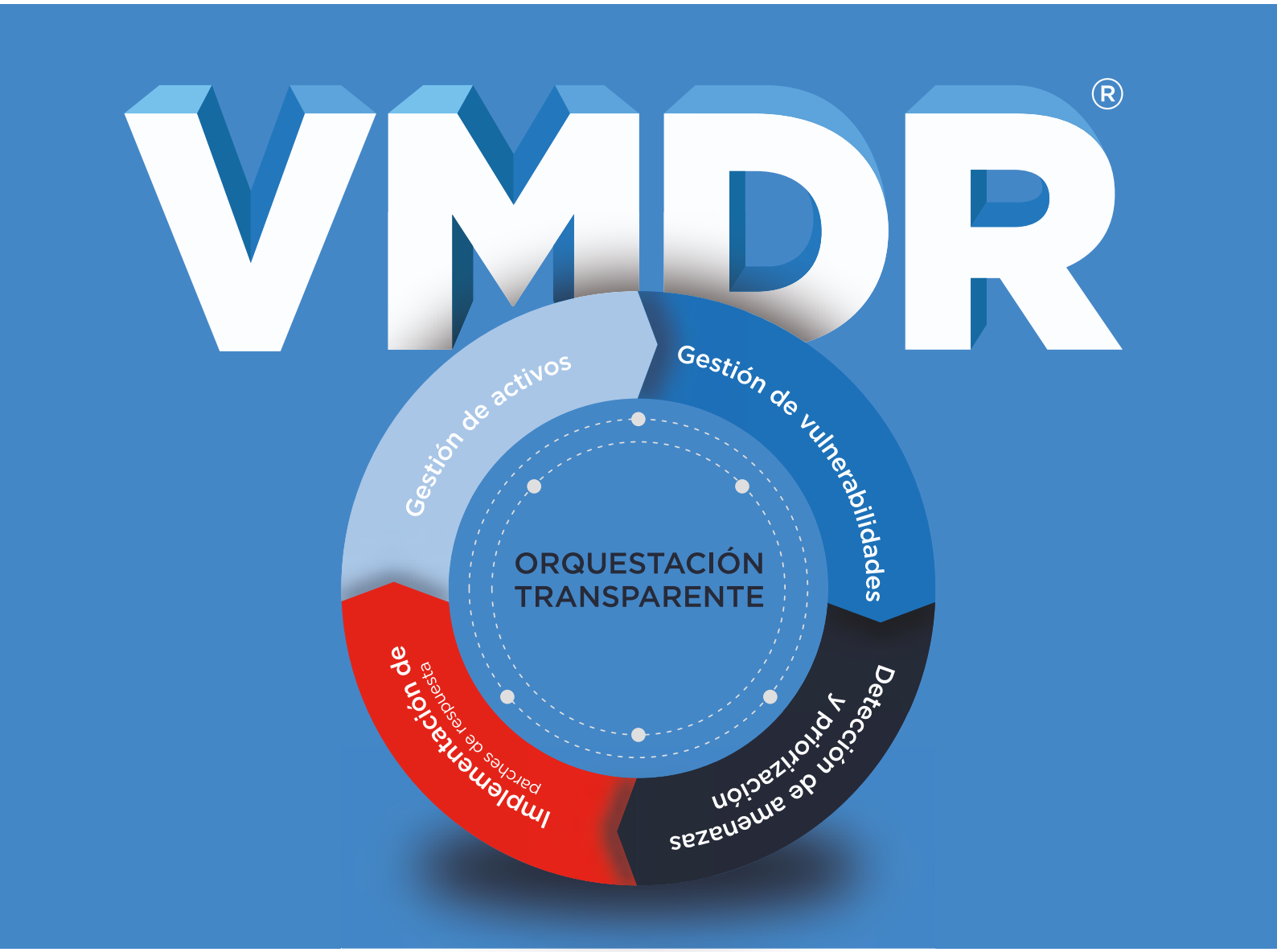
■ **Netskope** anuncia la disponibilidad de sus controles de seguridad y protección para Microsoft Teams. A través de una única interfaz, y sin la necesidad de *appliances* locales, **Netskope for Teams** ofrece capacidades DLP y de seguridad ante amenazas en línea. Además, permite supervisar y crear políticas que pueden ser definidas por varios atributos, tales como usuario, actividad o equipos, entre otras características.

■ **SonicWall** ha dado a conocer su enfoque hacia la 'Ciberseguridad sin Perímetro', a fin de proteger a las empresas en todos los entornos, especialmente ante el aumento del trabajo en remoto. Un desafío que aborda dotando de mayor escalabilidad y flexibilidad a su serie **Secure Mobile Access** (SMA). SonicWall ha ampliado la capacidad de la serie SMA 100 para admitir cientos de usuarios remotos concurrentes y de la serie SMA 1000, para grandes empresas y MSSP, pudiendo escalar a más de cientos de miles de usuarios.

Llevando la gestión de vulnerabilidades al próximo nivel

Una aplicación única basada en nube para un programa de gestión de vulnerabilidades basado de verdad en el riesgo

qualys.com/**VMDR**



Qualys.

Se celebra el 24 de junio a través de la plataforma Vanesa

El CCN analiza las luces y sombras del ENS tras 10 años de periplo en su II Encuentro anual

El 8 de enero se cumplieron 10 años desde que se promulgara el Real Decreto 3/2010 que estableció el **Esquema Nacional de Seguridad**. Tenía por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estaba constituido por los principios básicos y los requisitos mínimos que permitían una protección adecuada de la información. En total, aglutinaba 75 medidas de seguridad, recopiladas en tres grandes áreas: marco organizativo, operaciones y medidas de protección, un paso de gigante para la ciberseguridad en España.

Ahora, en el décimo aniversario del ENS, el **Centro Criptológico Nacional,** del **CNI,** organiza su "II Encuentro del ENS", el 24 de junio mediante *Vanesa*, la plataforma de vídeo en *streaming* de la entidad. El formato del evento se adecuará a la situación del momento (virtual, a puerta cerrada o con aforo limitado, en función del estado en el que esté Madrid en esas fechas dentro del plan de desescalada).

Bajo el título de "Diez años de nuevos retos y soluciones" la jornada tendrá un bloque de sesiones por la mañana y otro de talleres por la tarde. Todas las intervenciones tendrán como hilo conductor la revisión del Esquema Nacional de Ciberseguridad, de manera que se facilite una mejor respuesta a tendencias y necesidades de ciberseguridad, se reduzcan las vulnerabilidades y se promueva la defensa activa en todas las administraciones públicas españolas.

El 4 de junio, con una sala plenaria y dos laboratorios

NextSecure llega a su XII Edición plenamente asentado

S21sec organiza su gran evento anual, en esta ocasión en línea, en el que se darán a conocer todo tipo de novedades sobre tecnologías de la seguridad de la información. Inaugurado por el CEO de la compañía, **Agustín Muñoz**, en él intervendrán desde **Jorge Hurtado**, CSPMO de la empresa, moderando el panel "Cómo el coronavirus ha cambiado las prioridades de los CISOs", hasta expertos como **Ben Hammersley**, el conocido presentador del programa "Cybercrimes with Ben Hammersley" de **Netflix** y **BBC, David Grout,** CTO de **FireEye, Yolanda Belinchón,** Security Engineer de **Check Point**, **Kevin O'keefe,** Solution Architect EMEA de **Qualys,** y **Rafael del Cerro,** Cyber Security Systems Engineer de **Aruba HPE**, entre otros, analizando los grandes retos del acceso remoto y el trabajo en la nube. En paralelo al *track* principal se celebrarán dos laboratorios prácticos, con traducción simultánea.

Del 15 al 16 de junio, dedicado a la innovación

I Congreso Internacional 'Manifesting Intelligence' sobre IA, automatización y ciberseguridad

Primera edición, a través de Zoom, de este congreso internacional que tendrá como objetivo sentar las bases, "de lo que serán las futuras innovaciones tecnológicas en el campo de la inteligencia artificial y sus múltiples aplicaciones, entre las que la ciberseguridad ocupa un lugar destacado", según explica su organizador, **Regino Criado**. Por eso, a través sus ponencias se "buscará analizar, explorar y compartir las metodologías aplicables a los problemas que están en la frontera entre la inteligencia artificial, las redes complejas y la teoría del caos, la ciberseguridad y los fenómenos físicos y naturales". Además, contará con el apoyo y una presencia destacada del **Instituto de Data, Complex Networks & Cybersecurity Sciences (IDCNC)** de la **Universidad Rey Juan Carlos**. Entre sus participantes destaca el director científico de la **Agencia Espacial Europea, Günther Hasinger** o el cofundador de los laboratorios de IA de **Uber**, además de una decena de expertos del máximo nivel, tanto en la industria como el ámbito universitario.

Esta primera edición de 'Manifesting Intelligence', que se organiza gracias al acuerdo de la URJC con la **Universidad de Carolina del Norte** (Estados Unidos) y el **Instituto de Sistemas Complejos de Florencia** (Italia), iba a celebrarse en Madrid, aunque por la pandemia será en línea. La idea es que dé lugar a la celebración de conferencias de este tipo en diferentes ciudades en los próximos años.

De la mano de sus investigadores, el 16 de junio

Eset Virtual World 2020 analizará las ciberamenazas al sector aeronáutico

Bajo el lema 'Ciberespías en Europa', la multinacional **Eset** desvelará en su evento mundial las últimas técnicas que están rompiendo los sistemas de seguridad de las organizaciones de Defensa y de empresas del sector aeronáutico del Viejo Continente. "Imagínate que el responsable de RR.HH. de una gran empresa te contacta por **LinkedIn** para ofrecerte un puesto interesante y trabajar en la compañía en la que soñabas desde hace años. ¿No tendrías, al menos, la curiosidad de entablar una conversación con él? El único problema es que… ese profesional no existe. Sin embargo, los documentos que os habéis intercambiado han infectado de *malware* a tu empresa. ¿Avisarías a tus jefes?". Este es uno de los tipos de ataque utilizado en los últimos meses por los ciberespías para acceder a las infraestructuras de información de las organizaciones. Y las empresas afectadas en esta ocasión han sido compañías de alto nivel en los sectores de defensa y aeronáutica. Entre otros expertos, participarán como ponentes el CTO de Eset, **Juraj Malcho**, su Senior Malware Researcher, **Jean-Ian Boutin**, y su Malware Researcher, **Zuzana Hromcová.**

its by Ibermática

CYBER SECURITY EXPERTS

El pasado año, los ciberataques aumentaron en un 200%. En 2020, la situación no va a mejorar.

Las amenazas de ciberseguridad evolucionan día a día y requieren servicios expertos para frenarlos.

Nuestro Centro de Operaciones de Seguridad (SOC) permite conocer y responder en tiempo real a los incidentes de seguridad ofreciendo una visibilidad única, seguridad y control total tanto en entornos IT como OT.

Predict
Prevent
Protect
Respond

CIBERSEGURIDAD IT/OT

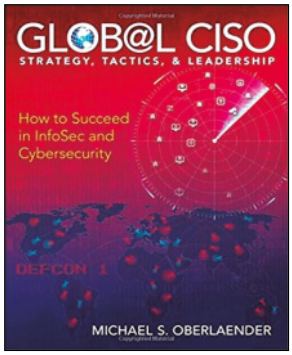
SOC 24X7

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

CSIRT.es
TF-CSIRT Trusted Introducer
FIRST

+34 902 102 655 marketing@its-security.es www.its-security.es

GLOBAL CISO: STRATEGY, TACTICS, & LEADERSHIP (HOW TO SUCCEED IN INFOSEC AND CYBERSECURITY)



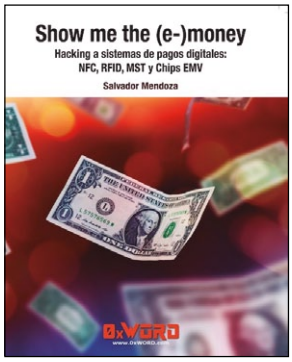
Autor: Michael S. Oberlaender
Editorial: Publicación independiente
Año: 2020 – 297 páginas
ISBN: 979-8604917756
www.amazon.com

Escrito por un CISO con amplia experiencia en la industria de ciberseguridad, ya que ha asesorado a empresas como TriagingX, SentinelOne o NetSkope y ha colaborado con organizaciones como Isaca o (ISC)², este libro está pensando tanto para los responsables de ciberprotección como para la Alta Dirección (desde CEOs, hasta CIOs, CTOs, etc.) que quieran contar con una visión precisa sobre qué aspectos son críticos a la hora de implementar una estrategia de ciberseguridad a medio y largo plazo, en consonancia con los departamentos de TI, cumplimiento, privacidad, marketing y en todo tipo de entornos, desde la nube hasta IoT, aplicando conceptos como SecDevOps.

A lo largo de sus páginas, **Michael S. Oberlaender** sintetiza de forma directa, y con abundantes ejemplos prácticos, la función del CISO y cómo acometer sus principales retos en el día a día.

En definitiva, permite contar con una interesante hoja de ruta de cómo desarrollar una planificación estratégica de ciberseguridad, gestionar equipos en este aspecto, exponer la situación al Consejo y qué tener en cuenta a la hora de elaborar presupuestos, contando con métricas y referencias y normativas internacionales como RGPD, CCPA o la Ley de Seguridad de China, entre otras.

SHOW ME THE (E-)MONEY. HACKING A SISTEMAS DE PAGOS DIGITALES

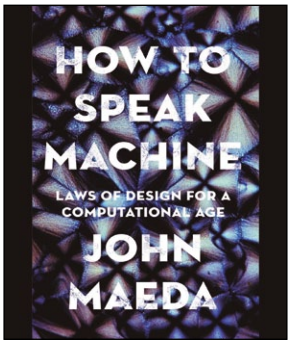


Autor: Salvador Mendoza
Editorial: 0xword
Año: 2020 –220 páginas
ISBN: 978-84-09-18979-3
0xword.com

Recopilación y combinación de herramientas de hardware, software y metodologías para la explotación de sistemas de pagos digitales de carácter práctico y bastante explicativo con abundantes ejemplos del código, de su funcionamiento y de cómo se utilizan. Con él, Mendoza, un investigador que ha participado en congresos como Def CON y Black Hat, muestra cómo se originan algunos de los ataques más usados y novedosos contra medios de pago, muchos de ellos aún no publicados en ningún medio y menos en publicaciones en castellano.

Por supuesto, este libro, según su autor "no es una guía de explotación", sino "una fuente de información para todo aquel estudiante, profesor, hacker o entusiasta que quiera saber más de los ataques a los sistemas de pagos actuales". Así trata posibles amenazas como son los ataques de repetición desde la información de banda magnética, MST (Magnetic Secure Transmission), la nueva tecnología de Samsung Pay, hasta más complejos contra la tecnología NFC, muy utilizada en medios de pago sin contacto, durante la pandemia para no tocar el papel.

HOW TO SPEAK MACHINE. LAWS OF DESIGN FOR A COMPUTATIONAL AGE



Autor: John Maeda
Editorial: Penguin Books
Año: 2019 – 223 páginas
ISBN: 9780241422144
www.penguin.co.uk

John Maeda, fundador del Grupo de Diseño y Computación del Medialab del MIT, es conocido por su visión, por momentos provocadora, sobre la tecnología y cómo sacarle partido a través de la simplicidad. En este nuevo libro, analiza qué normas rigen y regirán el mundo hiperconectado que estamos viviendo y cómo interactuar, de forma positiva, con las máquinas y sistemas de inteligencia que están cambiándolo. Dicho de otra forma: no todo el mundo tiene que saber programar pero sí está obligado a entender el por qué del funcionamiento de la tecnología que nos rodea.

Maeda recuerda que "las máquinas ya son más potentes de lo que podemos comprender" y su crecimiento es exponencial, ya que "una vez que se ponen en marcha los algoritmos, estos nunca se cansan, para lo bueno y para lo malo". Así, recuerda situaciones poco deseables como las vividas con *chatbots* desarrollados por grandes multinacionales tecnológicas, como Microsoft, que fueron desconectados al poco tiempo de interactuar con miles de usuarios a causa de comentarios racistas o por sus sesgos raciales a la hora de realizar predicciones para la lucha contra el crimen. Para evitarlas, en 'How To Speak Machine', su autor propone, con una prosa directa y fácil de entender, un "marco coherente para que los diseñadores de productos, líderes empresariales y formuladores de políticas actuales comprendan este mundo nuevo". Para ello, no faltan en sus páginas buen número de ejemplos y tecnologías que permitirán "crear productos que cambien el mundo e incluyan, al mismo tiempo, sistemas que eviten las trampas inherentes al medio".

OPERATOR HANDBOOK: RED TEAM + OSINT + BLUE TEAM

Autor: Joshua Picolet
Editorial: Publicación Independiente
Año: 2020 – 436 páginas
ISBN: 979-8605493952
www.amazon.com

Este completo 'manual de campo', con un enfoque muy práctico, está pensado para los que trabajan o quieren hacerlo en servicios de *red team, blue team* y búsqueda de información en fuentes abiertas (OSINT).

En él, se ofrece abundante información técnica de más de un centenar de tácticas y herramientas empleadas por casi todos los expertos en estos campos, clasificadas en orden alfabético, conformando un volumen de más de 400 páginas.

Una información que servirá tanto para el veterano como para el que comience en este tipo de servicios y labores que cada vez se demandan más en ciberprotección en todo tipo de entornos y procesos.

Entre las novedades que aporta, destaca que su autor, **Joshua Picolet,** considera que el trabajo y conocimiento conjunto, y sin barreras, de los profesionales de las tres áreas puede incrementar notablemente la ciberseguridad de cualquier organización.

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN

ESET Threat Intelligence
ESET Virus Radar
WeLive Security

PREVENCIÓN

Endpoint Protection Platform
ESET Mail Security
ESET Gateway Security
ESET SharePoint Security
ESET Secure Authentication
ESET Endpoint Encryption
ESET Security Management Center
ESET Cloud Administrator

RESPUESTA

ESET Enterprise Inspector
ESET Dynamic Threat Defense
ESET Security Management Center
ESET Cloud Administrator

DETECCIÓN

Endpoint Protection Platform
ESET Dynamic Threat Defense
ESET Enterprise Inspector
ESET Mail Security
ESET Gateway Security
ESET SharePoint Security
ESET Secure Authentication
ESET Endpoint Encryption
ESET Security Management Center
ESET Cloud Administrator

CYBERSECURITY EXPERTS ON YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

go.eset.es/sic

Actos y Convocatorias

Fechas tentativas a expensas de su viabilidad final

Next Secure 2020
Organiza: S21Sec
Fecha: 4-6-2020
– Encuentro en línea
Sitio: nextsecure.es

Manifesting Intelligence 2020
Organizan: United Therapeutics, Universidad Rey Juan Carlos y DCNC Sciences
Fechas: 15/16-6-2020
– Encuentro en línea
Sitio: manifestingintelligence.com

Cursos y seminarios de ISACA Madrid
Organiza: ISACA Madrid
- **Introducción a la Auditoría de Sistemas,** 15/23-6-2020
- **Introducción a la Ciberseguridad,** 15/24-6-2020
- **Introducción a la Gestión de Riesgos Tecnológicos,** 24/25-6-2020

Tel.: 91 639 29 60
Correo-e: administracion@isacamadrid.es
Sitio: isacamadrid.es

ESET Virtual World
Organiza: ESET
Fechas: 16/18-6-2020
– Encuentro en línea
Sitio: esetvirtualworld.com

Encuentros virtuales Centro de Ciberseguridad Industrial
Organiza: CCI. Centro de Ciberseguridad Industrial.
- **La Voz de la Industria Andaluza,** 18-6-2020
- **Ciberseguridad en la Digitalización Industrial,** 25/26-6-2020

Sitio: www.cci-es.org

II Encuentro del Esquema Nacional de Seguridad
Organiza: CCN-Centro Criptológico Nacional
Fecha: 24-6-2020
– Encuentro en línea
Sitio: www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/encuentro-ens/ii-encuentro-ens

Cursos SANS INSTITUTE
- **SEC504 Hacker Tools, Techniques, Exploits and Incident Handling,** 29-6/10-7-2020
- **FOR500 Windows Forensic Analysis,** 19/30-10-2020
- **SEC401 Security Essentials Bootcamp Style,** 16/27-11-2020
- **FOR508 Advanced Incident Response, Threat Hunting in Digital Forensic,** 23-11/4-12-2020

Organiza: One eSecurity
Lugar: Madrid
Tel.: 911 011 000
Correo-e: sans@one-esecurity.com
Sitio: one-esecurity.com

Cybersecurity Summer BootCamp 2020
Organizan: INCIBE y OEA
Fechas: 20/30-7-2020
– Encuentro en línea
Correo-e: contacto_summerBC@incibe.es
Sitio: incibe.es/summer-bootcamp

Cursos ES-CIBER
Organiza: Escuela Superior de Ciberseguridad, ES-CIBER
Correo-e: info@es-ciber.com
Sitio: es-ciber.com

IntelCon
Congreso de Ciberinteligencia
Organiza: Ginseg Ciberinteligencia
Fechas: 27/31-7-2020
– Encuentro en línea
Sitio: intelcon.ginseg.com

Black Hat 2020
Organiza: Informatech.
Fechas: 1/6-8-2020
– Encuentro en línea
Sitio: www.blackhat.com/us-20/

Cursos Ciberseguridad Westcon-Comstor
Organiza: Westcon-Comstor
Lugar: Madrid
Tel: 91 419 61 00
Correo-e: academy.es@westcon.com
Sitio: academy.westconcomstor.com/es

Cursos M2i formación
Organiza: Alhambra-Eidos
Tel.: 91 787 23 00
Fax: 91 787 23 01
Sitio: m2iformacion.com

SECURMÁTICA 2020
CISOs: cómo están protegiendo sus empresas
Organiza: Revista SIC
Fechas: 29-9/1-10-2020
Lugar: Hotel Novotel Campo de las Naciones.
C/ Ámsterdam, 3. Madrid
Tel.: 91 575 83 24
Correo-e: info@securmatica.com
Sitio: securmatica.com

IDENTISIC 2020
Zero Trust
La identidad da la cara
Organiza: Revista SIC
Fechas: 14/15-10-2020
Lugar: Hotel Novotel Campo de las Naciones.
C/ Ámsterdam, 3. Madrid
Tel.: 91 575 83 24
Correo-e: info@revistasic.com
Sitio: revistasic.com/identisic

INDICE DE ANUNCIANTES

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.**

SANS EMEA

SANS INSTITUTE EN ESPAÑA
LA EXCELENCIA EN LA FORMACIÓN EN CIBERSEGURIDAD

Nuevo formato Live Online

- Sesiones interactivas con los instructores de SANS
- Laboratorios prácticos en un entorno virtual
- Acceso a archivo en MP3
- Flexibilidad de tiempo (2 semanas)
- 4 meses de acceso online al curso
- Programa y materiales en formato electrónico

CALENDARIO 2020

SEC504 | GCIH | 29/06 - 10/07/2020 | 15h a 20h CEST de Lunes a Viernes
Hacker Tools, Techniques, Exploits, and Incident Handling — Carlos Fragoso

FOR500 | GCFE | 19 - 30/10/2020 | 15h a 20h CEST de Lunes a Viernes
Windows Forensic Analysis — Jess García

SEC401 | GSEC | 16 - 27/11/2020 | 15h a 21h CET de Lunes a Viernes
Security Essentials Bootcamp Style — Carlos Fragoso

FOR508 | GCFA | 23/11 - 4/12/2020 | 15h a 20h CET de Lunes a Viernes
Advanced Incident Response, Threat Hunting, and Digital Forensics — 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 | one-esecurity | Teléfono: +34 911 011 000

SECURMÁTICA 2020

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

NUEVAS FECHAS
29 Y 30 DE SEPTIEMBRE,
Y 1 DE OCTUBRE · 2020

www.securmatica.com

CISOs
cómo están protegiendo sus empresas

Ciberseguridad: lo que sí se está haciendo

Organiza

Revista SIC

Copatrocinadores

accenturesecurity · Aiuken Cybersecurity · Blueliv. · DXC.technology · Eleven Paths · Entelgy Innotec Security · EY Building a better working world

gmv · Ingenia · MNEMO · pwc · S2 Grupo · S21sec · SECURA by factum