it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Octubre 2021 - nº 45

Máquinas

Tus mejores aliados. Tus peores enemigos

‘Identificar los roles críticos en la organización es fundamental’ (Leroy Merlín)

‘La tendencia en ciberseguridad será el análisis de comportamiento’ (Mercadona)

IT Webinar. El papel de la ciberinteligencia en la seguridad empresarial

Educación e innovación. Tendencias tecnológicas para los nuevos retos

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad

Directora Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez

Diseño revistas digitales Contracorriente

Producción audiovisual Favorit Comunicación, Alberto Varet

Fotografía Ania Lewandowska

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es

Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es

Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es

Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es

Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

Máquinas, ¿las tienes controladas?

Desde el IoT y los dispositivos móviles hasta las aplicaciones definidas por software, instancias en la nube, contenedores e incluso el código que se ejecuta dentro de ellos, las máquinas ya superan en número a los humanos. Según el Informe anual de Internet de Cisco, para 2023, habrá 29,3 mil millones de dispositivos en red a nivel mundial, frente a los 18,4 mil millones en 2018. Más de 10 mil millones de dispositivos nuevos en solo cinco años.

Al igual que las identidades humanas en las que confiamos para acceder a las aplicaciones y dispositivos que usamos todos los días (por ejemplo, contraseñas, multifactor, etc.), las máquinas requieren un conjunto de credenciales para autenticarse y conectarse de forma segura con otros dispositivos y aplicaciones en la red. A pesar de su importancia crítica, estas "identidades de máquina" a menudo no se administran ni protegen, y de todo ello hablamos en el tema de portada de #ITDSOctubre.

Este mes los protagonistas son los CISO de Leroy Merlín y Mercadona, así como los responsables para el mercado español de Proofpoint y CyberArk. Con los primeros hablamos de los retos a los que se enfrentaron en su día, cómo ha cambiado su rol o qué tecnologías de seguridad creen imprescindibles. Con los segundos de la evolución del mercado y sus empresas, dispuestas a extender su alcance en nuevas áreas de actuación que le permitan seguir creciendo y tener una oferta amplia y consistente.

Os resumimos un interesante webinar centrado en la ciberinteligencia, una tecnología que se está convirtiendo en algo imprescindible para la seguridad empresarial, en el que hemos contado con la participación de tres empresas con ofertas complementarias: KELA Group, ThrreatQuotient y ZeroFox.

Insertamos un monográfico centrado en el mercado educativo, cómo protegerlos y que tecnologías le están impactando. Desde la protección de los endpoint a la seguridad de las redes WiFi o la gestión de cientos de terminales, el sector educativo presenta unos retos que pueden afrontarse desde diferentes perspectivas, algo que se ha discutido en una mesa redonda en la que han participado portavoces de Alcatel-Lucent, ESET, Global Knowledge, Sophos y WatrchGuard.

En cuanto a la actualidad, os hablamos de cómo VMray está llevando su afamada solución de sandboxing a la seguridad del correo electrónico y la expansión en España de Goldilok y su solución para mantener los datos offline y tenerlos accesibles mediante una tecnología remota y automatizada que no usa IP.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

itds

Sumario

Actualidad

Entrevistas

Mario Andrés, Mercadona

'En los próximos años la tendencia en ciberseguridad será el análisis de comportamiento'

Gabriel Moliné, Leroy Merlín

'Identificar los roles críticos en la organización, que no necesariamente son los del comité de dirección, es fundamental'

Albert Barnwell, CyberArk

'Un acceso de una identidad es privilegiado o no dependiendo de a dónde va'

Fernando Anaya, Proofpoint

'El valor diferencial de Proofpoint es una visión centrada en las personas'

No solo IT

Un año acercando a la mujer al mundo de la ciberseguridad

Daniela Kominsky

El Amanecer de la Humanidad Digital IV: nubes en el horizonte

Mario Velarde Bleichner

IT Webinars

Revistas Digitales

Índice de anunciantes

Proteja su experiencia en la nube de Azure.

Soluciones para proteger las aplicaciones y la información en Microsoft Azure y garantizar el cumplimiento de las reglas de seguridad »

Más información:
iberia_team@barracuda.com
barracuda.com

Barracuda Microsoft

STRENGTH IN SECURITY™

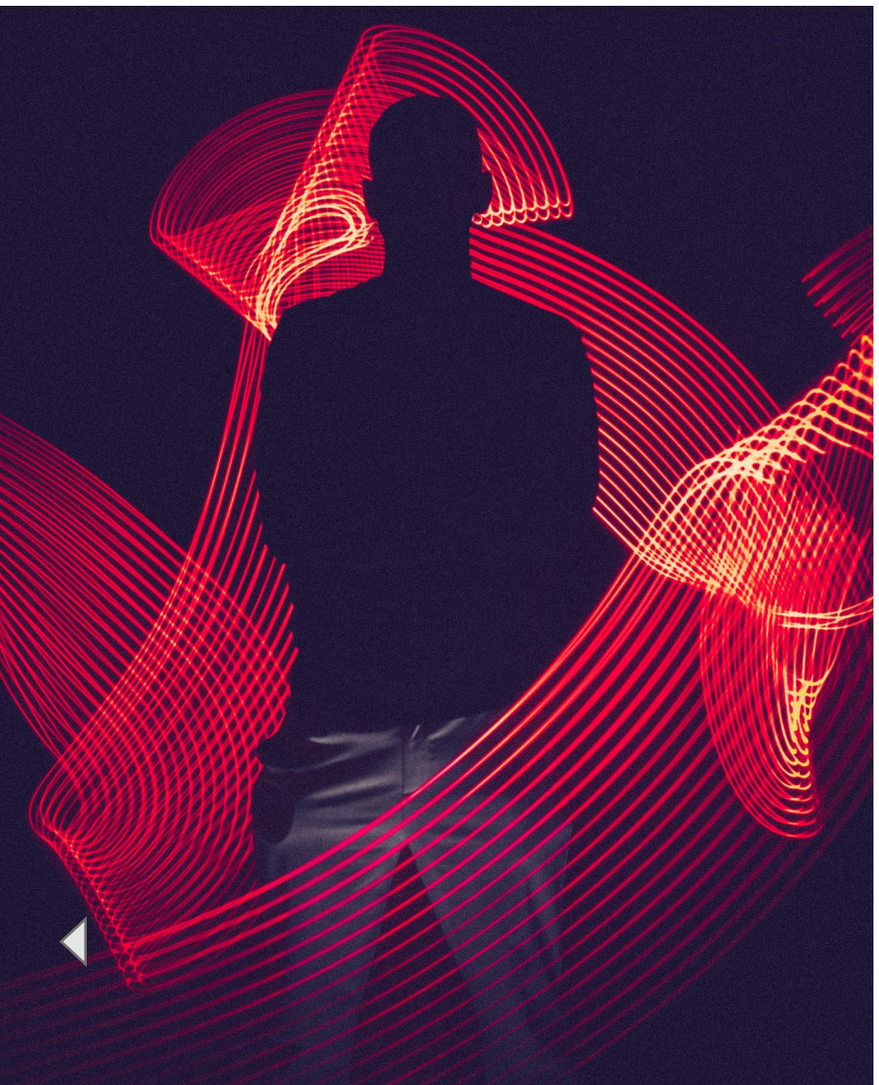
Goldilock: Lo que no está online no se puede hackear

Goldilock comenzó hace cuatro años desarrollando una solución de ciberseguridad simple pero compleja para mantener los datos offline y tenerlos accesibles mediante una tecnología remota y automatizada que no usa IP (Protocolo de Internet). Nos lo ha contado Stephen Kines, COO de la compañía, durante una presentación celebrada en Madrid.

Bajo la premisa de que “lo que no está en internet no puede ser pirateado”, explica Kines que La tecnología de la compañía se basa en la premisa de que los datos, dispositivos e infraestructura crítica no deben estar conectados físicamente a Internet cuando no se estén usando, sino que deben estar disponibles desde cualquier lugar y de manera inmediata cuando desee acceder a ellos.

Explica también el directivo de Goldilock que las personas permiten que los datos estén en línea

True Remote Airgap Security (TRAS) permite el aislamiento de red Para crear una defensa impenetrable incluso contra los ataques más sofisticados



WELCOME TO GOLDILOCK - DIGITAL SECURITY

CLICAR PARA VER EL VÍDEO

todo el tiempo, “y la razón por la que lo hacen es que no tienen forma de desconectarse o conectarse”. Añade que las empresas necesitan acceder a sus datos, pero no necesitan acceder a sus datos todo el tiempo, “y eso es lo que Goldilock soluciona. Debido a que no hay una dirección IP, no hay posibilidad de que nadie encuentre los datos porque están completamente offline”. Se trata, por tanto, de una solución que aísla completamente cualquier infraestructura que se quiera salvaguardar; “tan simple que parece increíble”.

¿Y qué ocurre cuando quien trata de acceder a esos datos no es un ser humano? La mejor opción, responde Stephen Kines, es programar la apertura en ciertos momentos.

Los planes de la compañía para el mercado español, donde la cara visible de la compañía es Sergio Alonso, VP Partnerships and Channels de

"Hay una gran oportunidad para España de estar a la vanguardia de la ciberseguridad"

Goldilock, pasan por ser la puerta de entrada a Latinoamérica y crear un centro de I+D donde crear una versión de la solución de la compañía para fibra óptica.

Nos explica el COO de Goldilock que es una demanda de los clientes, que la fibra óptica es una tecnología muy compleja y que “esperamos conseguir algunas subvenciones y apoyo europeo para poder construir en España un centro de I+D”, sin que el lugar exacto se haya definido por el momento.

El go-to-market de la solución es a través de canal de distribución. Se cuenta con un ecosistema Tier2 con tres tipos de integradores: gold system integrator, reseller y referal agents.

En cuanto a previsiones económicas, habla Stephen Kines de un mercado, el de la ciberseguridad que genera trillones de dólares y que las

"Debido a que no hay una dirección IP, no hay posibilidad de que nadie encuentre los datos porque están completamente offline"

Stephen Kines, COO, Goldilock

empresas están madurando a golpe de escándalo. Menciona la crisis de Colonial Pipeline como un impulsor de la adopción de soluciones de seguridad en Estados Unidos, y que ese "despertar" también ocurrirá en Europa.

En cuanto a las previsiones para el mercado español, asegura que "hay una gran oportunidad para España de estar a la vanguardia de la ciberseguridad, ser líder en Europa. Y esto es lo que queremos, traer buena suerte a España".

Casos de uso

La propuesta de Goldilock es tan sencilla como completa si se tienen en cuenta los casos de uso. No sólo se puede utilizar True Remote Airgap Security (TRAS) para el aislamiento de red "con el objetivo de crear una defensa impenetrable incluso contra los ataques más sofisticados" y proteger los datos de su eliminación, exfiltración, ransomware, sabotaje y más, sino en entornos de backup o gestión de derechos digitales, donde las organizaciones pueden permitir una distribución más rápida de su contenido y, al mismo tiempo, beneficiarse de la capacidad de controlar quién envía y recibe sus publicaciones. Según la compañía, "el resultado final de la aplicación de la tecnología Goldilock es una mayor disponibilidad de contenido, lo que permite a millones de personas acceder a películas y música que antes no estaban disponibles y, al mismo tiempo, eliminar la piratería de activos multimedia".

También puede utilizarse la propuesta de aislamiento de Goldilock en la gestión de claves de certificados. Goldilock permite que los HSM se desconecten de Internet hasta que un usuario autorizado requiera acceso, lo que proporciona seguridad y accesibilidad. "Esta capa de aislamiento permite el almacenamiento seguro de claves privadas para respaldo, custodia o como mecanismo de buzón", aseguran desde la compañía.

Enlaces de interés...

- Goldilock
- Aumenta la presión de los equipos de TI para aumentar las medidas de seguridad

Compartir en RRSS

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA
CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN	PREVENCIÓN
ESET Threat Intelligence ESET Virus Radar WeLive Security	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
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET Security Management Center ESET Cloud Administrator	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
RESPUESTA	**DETECCIÓN**

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

VMray lleva su tecnología de sandboxing al email

La compañía alemana se adentra en el mercado de los Cloud eMail Security Supplement, o CESS, un término acuñado por Gartner que pone de manifiesto que las soluciones de protección del correo electrónico tradicionales no son suficientes

El correo electrónico es uno de los vectores de ataque más populares, por no decir que es el preferido por los ciberdelincuentes. Las estadísticas indican que un 90% de los ciberataques con éxito se inician en el correo electrónico, bien sea como medio para meter malware en la empresa, para engañar a un usuario a que pinche sobre un enlace, o hacerse pasar por un alto ejecutivo de la empresa para hacer un pago.

La seguridad del correo electrónico, que debe ser un requisito fundamental para cualquier organización, está en plena transición, impulsado sobre todo por dos factores: la propia evolución de los ataques, y el cloud. Desde que en 2011 Microsoft empezó a entregar los mensajes desde servidores de correo electrónico basados en la nube con el lanzamiento de Office 365, este mercado se ha multiplicado. Actualmente la compañía gestiona unas 300 millones de bandejas de entrada corporativas desde la nube.

En este proceso evolutivo del correo electrónico ha aparecido lo que Gartner ha acuñado como CESS, o Cloud eMail Security Supplement, un nuevo segmento de email security basado en API y centrado en llenar los vacíos en la protección avanzada contra amenazas existentes. Según la

CESS, Cloud eMail Security Supplement, es un nuevo segmento de email security basado en API y centrado en llenar los vacíos en la protección avanzada contra amenazas existentes

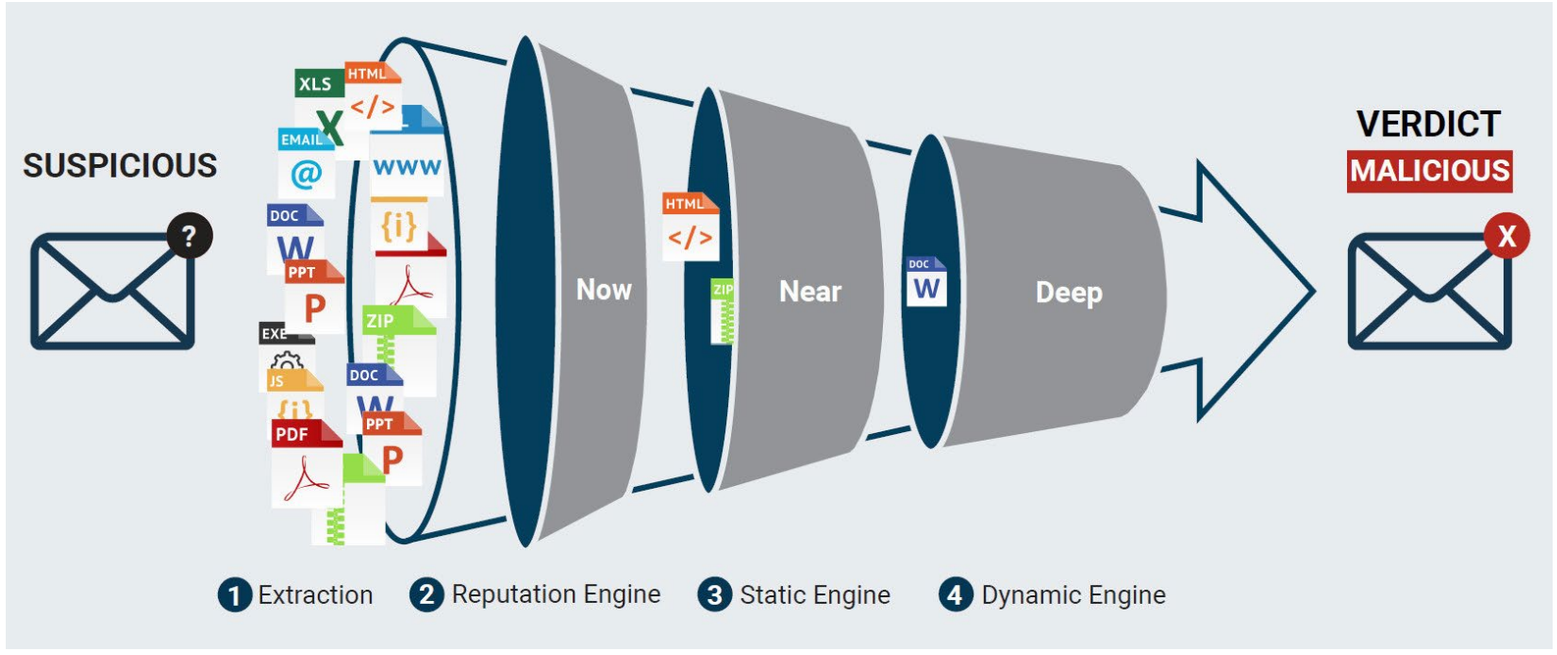
consultora, esta tecnología emergente “aborda las brechas en las capacidades avanzadas de defensa contra amenazas de las capas de seguridad avanzadas y predeterminadas dentro de las plataformas en la nube, así como las proporcionadas por las pasarelas de correo electrónico seguras (SEG) establecidas”.

VMray Email Threat Defender

En este nuevo segmento de mercado donde se adentra VMray, una compañía que cuenta con destacada tecnología de sandboxing para la detección y análisis de malware avanzado, que ahora pone al servicio del correo electrónico a través de la solución Email Threat Defender for Microsoft Office 365.

Dice Ovanes Mikhaylov, Business Development Manager Southern Europe de VMray, que “pensamos que hemos solucionado la seguridad del correo electrónico, pero no es así, ni mucho menos”, para añadir que es un problema que crece, que sigue sin resolverse y que VMray “ha decidido entrar en este mercado porque tenemos una solución que ofrecer” para proteger a las organizaciones de amenazas de correo electrónico desconocidas, específicas y avanzadas, y que ha sido diseñado “para complementar la seguridad del correo electrónico de Microsoft Office 365 conectándose fácilmente a través de API”.

Explica también el directivo que el producto ha sido diseñado para lograr las tasas de detección más altas y los falsos positivos más bajos. El sandbox de la compañía, resistente al malware



altamente evasivo ya que no proporciona una superficie que pueda ser detectada, explotada o eludida, permite escalar sin tomar atajos que comprometan la eficacia.

VMRay Email Threat Defender viene con tres motores de inspección:

- **Búsqueda rápida de reputación:** los archivos adjuntos de correo electrónico y las URL incrustadas se envían al motor de reputación. En milisegundos, los archivos y enlaces web benignos y maliciosos en los correos electrónicos se identifican y no reciben más atención en el flujo de trabajo de análisis.
- **Un segundo motor que inspecciona en profundidad el contenido incrustado de los correos electrónicos para identificar partes sospechosas o potencialmente maliciosas para un análisis dinámico posterior.** Esta inspección incluye enlaces web incrustados, así como adjuntos disfrazados y cifrados.
- **Los enlaces de phishing y malware sospechosos se detonan en una caja de arena aislada.** Según el comportamiento observado, el malware y los sitios web fraudulentos pueden detectarse y marcarse como maliciosos. La zona de pruebas basada en hipervisor de VMRay es invisible para el malware y detecta incluso cepas altamente evasivas.

La solución no sólo amplía las opciones de los clientes existentes de la compañía, sino que se ofrecerá, a través de canal, a empresas de más de 500 usuarios.

Enlaces de interés...

- Sandbox Matter
- VMRay Email Threat Defender

"VMray ha decidido entrar en este mercado porque tenemos una solución que ofrecer"

Ovanes Mikhaylov, Business Development Manager Southern Europe, VMray

Compartir en RRSS

it Digital Security

CAMINANDO HACIA ZERO TRUST

EVENTO ONLINE, 26 DE OCTUBRE DE 2021

EL MODELO DE SEGURIDAD QUE SE IMPONE EN LA EMPRESA

it Digital Security

Entrevista

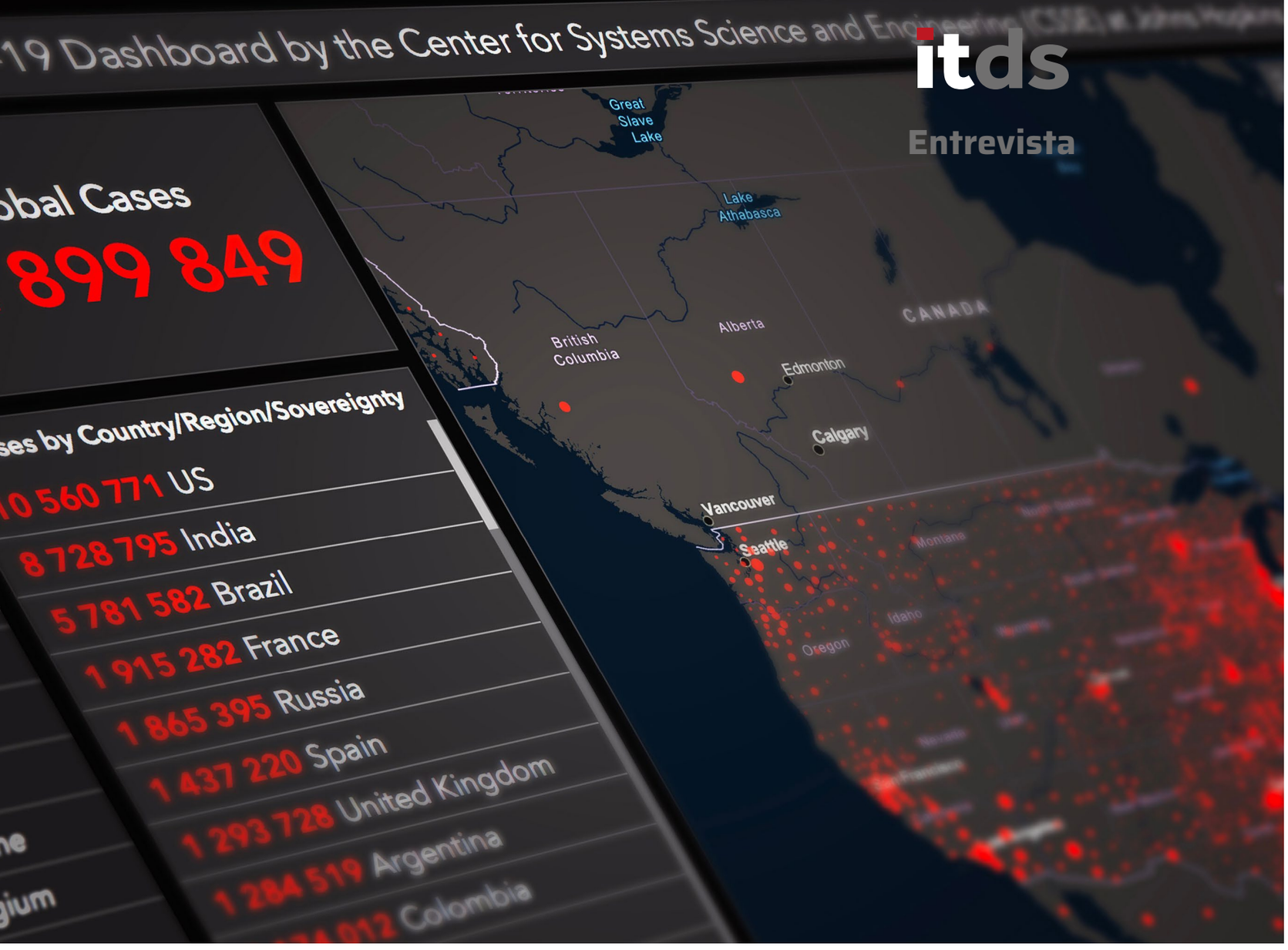
‘Identificar los roles críticos en la organización, que no necesariamente son los del comité de dirección, es fundamental’

(Gabriel Moliné, Leroy Merlín)

“Las tecnologías son elementos habilitadores, pero lo más importante son las personas”. Lo dice Gabriel Moliné, responsable de la ciberseguridad de Leroy Merlín desde hace más de dos años. Asegura también que el rol del CISO ha evolucionado; que lo más importante en cualquier organización son las personas; que el reto del CISO post-pandemia es rentabilizar las inversiones en tecnología; que la seguridad gestionada es importante, pero entendiéndola en su justa medida; que es imposible que puedas estar detrás de cada uno de los activos y que junto al XDR, los WAF son también herramientas imprescindibles para las empresas.

Texto: Rosalía Arroyo • Fotos: Ania Lewandowska

Para Gabriel Moliné, CISO de Leroy Merlín, la evolución de la figura de los responsables de ciberseguridad de las empresas en los últimos años ha sido “una especie de travesía por el desierto” en la que se ha pasado de ser “una figura técnica que se encargaba de solucionar problemas” a tener un rol capaz de mitigar los riesgos del negocio “y habilitar muchas oportunidades”. Dice también el directivo que también ha habido una evolución en el discurso, más orientado a negocio.



"La selección de las herramientas de seguridad se basa en los riesgos y en saber dónde está la cadena de valor"

Respecto a si la evolución continuará en el futuro y el rol del CISO cobrará más protagonismo, dice Gabriel Moliné que "no se trata de conquistar la cima del Everest", de estar directamente en el consejo de dirección porque "perderíamos el contacto con las preocupaciones tecnológicas, perderíamos la capacidad de conocer los problemas en el terreno de juego para poder trasladar esas necesidades a los ámbitos de dirección y viceversa".

Sobre las cualidades que debe tener un buen CISO, dice el de Leroy Merlín que es importante no perder el foco "porque las tecnologías son elementos habilitadores, pero lo más importante son las personas", añadiendo que lo que finalmente se intenta proteger son las personas y las acciones que ejecutan. Esto lleva a que el CISO deba tener la capacidad de trasladar el lenguaje técnico y no perder el foco en que "lo más importante en cualquier organización son las personas".

Después de una pandemia sanitaria que ha acelerado la adopción de muchas soluciones y herramientas, uno de los retos a los que se enfrentan los CISOs post-pandemia es, en opinión de Gabriel Moliné "el rentabilizar las inversiones que hemos hecho en tecnología, sacar el máximo provecho de las inversiones de seguridad". Añade el directivo que adoptar numerosos elementos tecnológicos no nos va a hacer más seguros, sino "potenciar el ecosistema existente".

Como no podía ser de otra forma por el alcance y crecimiento exponencial que está teniendo, el ransomware es algo que inquieta a Gabriel Moliné. Recuerda el directivo que las ciberamenazas aumentan en distintos vectores y asegura que hay una cosa que realmente le preocupa: el VAP, o Very Attacked Person. Explica el CISO de Leroy Merlín que muchas veces nos enfocamos en las personas que están en el comité de dirección, y no en las que están en su entorno, personas críticas dentro de la organización que pueden ser puerta de entrada y que son muy buscados por los ciberdelincuentes; "intentar identificar en la organización esos roles críticos, que no necesariamente son los del comité,

"Los WAF (Web Application Firewall) también son otra herramienta que deberíamos tener"

es una de las cosas que más me preocupan a día de hoy".

Mercado y servicios

Habla Moliné de una extrema saturación de proveedores, resellers y fabricantes cuando le preguntamos cómo poder escoger el mejor producto, la mejor solución, entre tanta oferta. Probarlos todos es imposible y el modelo clásico de confianza es el que tiene más éxito; "eso no quiere decir que cierre la puerta a otro proveedor, pero todo se basa en un modelo de confianza delegada. Para mí tiene un valor muy importante la opinión de otro responsable de seguridad sobre qué están haciendo con esos proveedores".

Sobre la seguridad gestionada dice Gabriel Moliné que es importante, "pero entendiéndola en su justa medida". Explica que la clave del éxito en estos modelos está en un modelo dual, "que tengas un equipo de seguridad interno que te garantice una transferencia tecnológica del Know How y conocimiento de la organización y que puedas extender

las respuestas por los servicios de seguridad". De forma que, de cara a los proveedores, es vital que conozca cómo se trabaja, y cuáles son las virtudes y defectos del cliente.

Sobre el cloud se lleva hablando desde hace mucho tiempo. Su adopción se aceleró durante la pandemia sin que aun esté claro, en la mayoría de las ocasiones, qué papel juega la seguridad en ese movimiento. Como la mayoría de las empresas, Leroy Merlín está en un proceso de adopción de todos los sistemas hacia un modelo cloud, "pero creo que es importante resaltar que no hay varita mágica. Llegar a la cloud no quiere decir que nos desentendamos de la seguridad, siempre es un modelo compartido. La responsabilidad de los datos, de la información del cliente, de las brechas de seguridad… no se pierde".

Tecnologías a tener en cuenta

Planteamos a Gabriel Moliné cuáles serían las herramientas de seguridad imprescindibles, esas sin las que una empresa no puede pasar. Responde apuntando que la elección dependería del tipo de empresa y explicando que si se trata del canal retail la protección de los canales de venta y de la información de los clientes es vital, y que la selección de las herramientas "se basa en los riesgos y en saber dónde está la cadena valor. Las cosas importantes son las que tengo que proteger".

Asegura que las amenazas han ido evolucionando y transformándose en ataques dirigidos y que dependiendo del tamaño del ecosistema, "es

"Llegar a la cloud no quiere decir que nos desentendamos de la seguridad, siempre es un modelo compartido"

imposible que puedas estar detrás de cada uno de los activos" por lo que considera que el XDR, "como una solución que intenta aunar todo este ecosistema de herramientas de ciberseguridad que tenemos, sería una de las herramientas fundamentales para la protección".

Junto a XDR, y apuntando a que todos tenemos presencia web, "los WAF (Web Application Firewall) también sería otra herramienta que deberíamos tener".

Mirando en el corto medio plazo menciona el CISO de Leroy Merlín una tecnología que será imprescindible: la orquestación, "precisamente por este crecimiento, especialización y atomización del mercado de seguridad". Añade que "a nivel ideal sería necesario extrapolar el XDR y la orquestación al mundo IoT" porque todo lo que nos rodea en nuestros hogares y en nuestra vida cotidiana son elementos que están conectados, son vectores de acceso y de riesgo y requieren de "herramientas que puedan orientarse de manera rápida y no intrusiva, teniendo en consideración todo el ámbito de la privacidad. Ahí es hacia donde debería moverse el mundo de la seguridad".

Enlaces de interés...

- 'No conozco ninguna herramienta única que realmente te ayude a hacer una gestión de la parte cíber más sencilla' (Alejandro Sánchez es el CISO de SEAT)
- 'Los CISOs nos hemos dado cuenta de que la preparación al final del día compensa' (Fermín Serna, Citrix)
- 'No estamos en el momento de que sólo contratando tecnología podamos estar protegidos' (Judit Closa, habitissimo)
- 'El cloud no se hace responsable de la seguridad' (Toni García, LETI Pharma)
- 'Si puedo envenenar un data lake o hacer que un algoritmo funcione mal, tendré más influencia para la extorsión' (Rik Ferguson, Trend Micro)
- 'Ha habido estafas millonarias con un phishing básico' (Forensics&Security)

Compartir en RRSS

CloudGuard

Check Point CloudGuard proporciona seguridad nativa en la nube unificada para todos sus activos y cargas de trabajo, lo que le brinda la confianza para automatizar la seguridad, prevenir amenazas y administrar la postura, en todas partes y en todo su entorno.

Más información:

www.checkpoint.com/es

Check Point®
SOFTWARE TECHNOLOGIES LTD

it Digital Security

Entrevista

‘En los próximos años la tendencia en ciberseguridad será el análisis de comportamiento’

(Mario Andrés, Mercadona)

Mario Andrés es el CISO de Mercadona, una empresa con 95.000 empleados, más de 1.600 tiendas y ventas de miles de millones de euros. Dice sí a los servicios gestionados, pero donde aporten valor; que un CISO debe mantenerse informado; que lo primero es asegurar los cimientos, entre los que se encuentran el endpoint y la red; que se deben conocer muy bien los procesos de las empresas para detectar cosas que se salen de lo normal; y que los retos de la seguridad siguen evolucionando más por otros factores que por la pandemia

Rosalía Arroyo

Contar con un buen equipo al que saber liderar es una de cualidades que debe tener un buen CISO, dice Mario Andrés, añadiendo que también es importante tener un buen conocimiento técnico y un aprendizaje continuo“ para mantenerse bien informado en un sector que cambia muy rápido y en el que aparecen nuevas tecnologías y amenazas”. No se olvida el CISO de Mercadona de la concienciación y la necesidad de “transmitir internamente el mensaje adecuado y no caer en la ciberseguridad de libro, sino traducirla a lo que la empresa necesita”, ni que es necesario contar con una alta dirección concienciada y que apueste e impulse la ciberseguridad, “como es nuestro caso”.

Sobre si la ciberseguridad se ha convertido en una prioridad para la empresa española, o seguimos avanzando a golpe de normativa y grandes titulares sobre ciberataques, dice Mario Andrés que “en los últimos años ha habido una evolución muy fuerte, pero todavía queda mucho camino por recorrer”. En el caso de Mercadona, “la apuesta por la ciberseguridad ha sido clara”, teniendo en cuenta que en tres años se ha pasado de contar con ocho personas a ser treinta y siete en el ámbito; además, “seguimos apostando por tener un equipo fuerte donde las personas puedan desarrollar su carrera profesional y enfrentarse a los retos que plantea la seguridad

"Es evidente que la cadena de suministro a nivel informático es un reto importante"

informática en un entorno empresarial como es el de Mercadona, más de 1.600 tiendas, 18 almacenes, tres colmenas -que es lo que utilizamos para el modelo de venta online, dos CPDs y cada vez más presencia en entornos cloud, entornos mucho más híbridos y más distribuidos", lo que también deja clara la apuesta de Mercadona por la transformación digital, que tiene 60 vacantes abiertas para el Departamento de Informática y acumula más de 180 incorporaciones desde enero 2020.

La pandemia, que tantos retos planteó en tantísimas empresas, no impactó demasiado en el día a día de Mercadona en tanto que "no cambió significativamente la forma de trabajar". Dice también el responsable de ciberseguridad de la compañía que aunque se está hablando mucho de un cambio de paradigma de la seguridad informática tras la pandemia, "en mi opinión los retos de la seguridad siguen evolucionando más por otros factores que por la pandemia", y menciona los entornos híbridos o servicios en la nube; "nosotros tenemos mucha dispersión geográfica con las tiendas y con los bloques logísticos, y ese perímetro que antes protegía la seguridad informática se está difuminando totalmente. Creo que los retos van más por ahí que realmente lo que haya podido cambiar o no la pandemia".

"Servicios gestionados sí, pero donde aporten valor", dice Mario Andrés. Comentando que los servicios gestionados pueden ser más

"En mi opinión, los retos de la seguridad siguen evolucionando más por otros factores que por la pandemia"

"Seguimos apostando por tener un equipo fuerte donde las personas puedan desarrollar su carrera profesional y enfrentarse a los retos que plantea la seguridad informática"

interesantes en otros modelos o tipos de empresas, ya que la estrategia de Mercadona es "contar con personas especialistas y con talento dentro de la casa y darles un buen plan de carrera".

Los ataques a la cadena de suministro se han puesto de moda este año. Quizá la que más nos venga a la mente sea la de SolarWinds, pero lo cierto es que no dejan de sucederse. "Es evidente que la cadena de suministro a nivel informático es un reto importante", asegura el CISO de Mercadona, añadiendo que se está viendo una tendencia a comprometer a proveedores más pequeños para atacar a las grandes empresas. La estrategia de la compañía es "trabajar codo con codo con nuestros proveedores para que exista una relación fluida que ayude a protegernos mejor entre todos".

Tecnologías imprescindibles

Asegurando que hay que prestar mucha atención a lo básico, "porque por ahí es por donde acaban entrando siempre", dice Mario Andrés que lo primero es "asegurar los cimientos" cuando le preguntamos por las tecnologías de seguridad que cree imprescindibles.

La protección del endpoint, la movilidad, la protección del correo, "que hoy en día es uno de los principales vectores de entrada a las empresas", así como la protección de la red son los imprescindibles para sentar las bases de la seguridad informática de una empresa y hacer frente a las ciberamenazas, según el directivo. "Pero por encima de eso creemos mucho en el valor que aporta la concienciación de los empleados como un punto clave y diferenciador", añade Andrés.

Siendo difícil hacer predicciones en un mercado tan cambiante como el de la seguridad, donde continuamente están apareciendo nuevas soluciones, tecnologías, fabricantes y amenazas, dice Mario Andrés que "en los próximos años la tendencia va a ser el análisis de comportamiento, tanto de usuarios como de infraestructura; cómo se comportan los usuarios en la informática y cómo se comportan las máquinas". Añade que cada vez será más importante encontrar

"Servicios gestionados sí, pero donde aporten valor. Es importante contar con personas especialistas y con talento dentro de la casa y darles un buen plan de carrera"

comportamientos que pueden ser legítimos, pero no normales dentro de una organización, por lo que "cobra una especial importancia, si es que no la tenía ya, el conocimiento del entorno y los propios procesos de la empresa".

Explica el directivo que los ciberdelincuentes se apoyan cada vez más en utilizar técnicas que podrían ser legítimas, y que "tenemos que estar preparados y conocer muy bien nuestros procesos y cómo funciona nuestra informática para detectar cosas que se salen de lo normal".

Sobre si espera un cambio significativo en el mercado de seguridad dice Andrés que "esto es una carrera de fondo y una evolución continua", y que el mayor reto es "proteger un perímetro que cada vez está más difuso, con más usuarios en movilidad, más entornos híbridos y más dispersión", lo que lleva a que cada vez haya que prestar más atención al usuario.

Añade el CISO de Mercadona que la compañía colabora habitualmente con otras empresas y organismos como INCIBE, compartiendo información y experiencias "porque no se trata de competir unos contra otros, sino contra los ciberdelincuentes".

Enlaces de interés...

- 'La ciberseguridad se está convirtiendo en una utility. O la tienes o no eres nadie' (Consuelo Fernández, Grupo Tecnatom)
- 'Las empresas tienen que tener en mente la protección del ciclo de vida del dato' (Manuel Barrios, Solvia)
- 'Los CISOs nos hemos dado cuenta de que la preparación al final del día compensa' (Fermín Serna, Citrix)
- 'No conozco ninguna herramienta única que realmente te ayude a hacer una gestión de la parte cíber más sencilla' (Alejandro Sánchez es el CISO de SEAT)

Compartir en RRSS

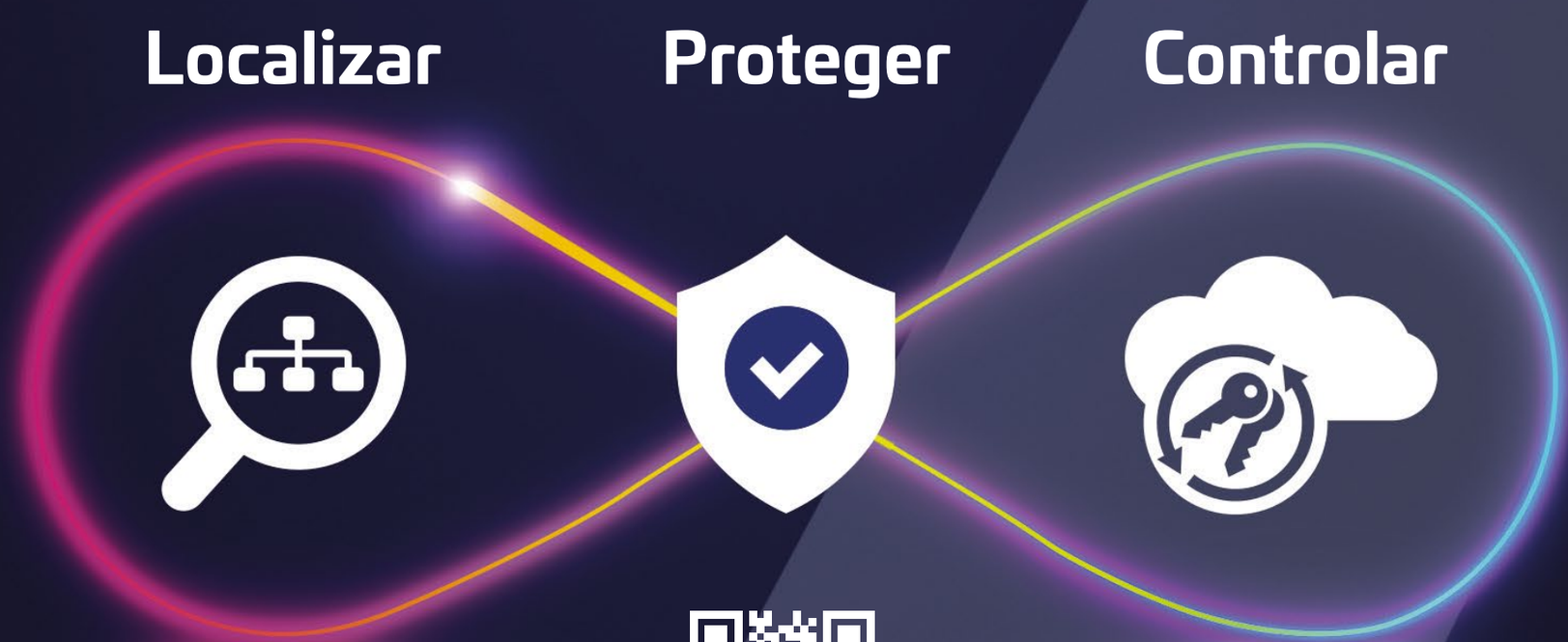
cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform

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

Localizar Proteger Controlar



Empiece a localizar, proteger y controlar sus datos hoy mismo

Proofpoint, más allá del correo electrónico

‘El valor diferencial de Proofpoint es una visión centrada en las personas’

(Fernando Anaya)

“Estamos en una etapa de crecimiento económico y esperamos seguir acelerando esta estrategia en los próximos años”. Son palabras de Fernando Anaya, country manager para Iberia de Proofpoint, una compañía fundada en 2002 cuya oferta ha evolucionado desde la seguridad del email para añadir capacidades en gestión de amenazas internas, cumplimiento, CASB, prevención de pérdida de datos empresariales (DLP) y capacitación en conciencia de seguridad.

Rosalía Arroyo

Para Fernando Anaya, el objetivo de la compañía es ser capaz de dar a partners y clientes herramientas y soluciones con las que mejorar su postura de seguridad, una postura y una estrategia que, desde el punto de vista de Proofpoint, es “People Centric” o lo que es lo mismo: el usuario está en el centro de la estrategia de seguridad.

Esta aproximación se ha visto respaldada con la adopción acelerada del trabajo remoto a consecuencia de la pandemia, que ha terminado por dejar claro que el perímetro de seguridad no está en la oficina o en la delegación, “sino en los usuarios y en los terminales. Nuestra estrategia y nuestro portfolio se han desarrollado con el fin de proteger a los usuarios por cualquier canal con el que interactúe”. Pone de manifiesto Fernando Anaya que el correo electrónico es el principal vector de ataque, y que hay que proteger todos los datos que los usuarios generan y a los que acceden.

Proofpopint es un gigante que a lo largo de su historia ha realizado unas 20 adquisiciones y cuenta con 6.000 clientes corporativos, de los

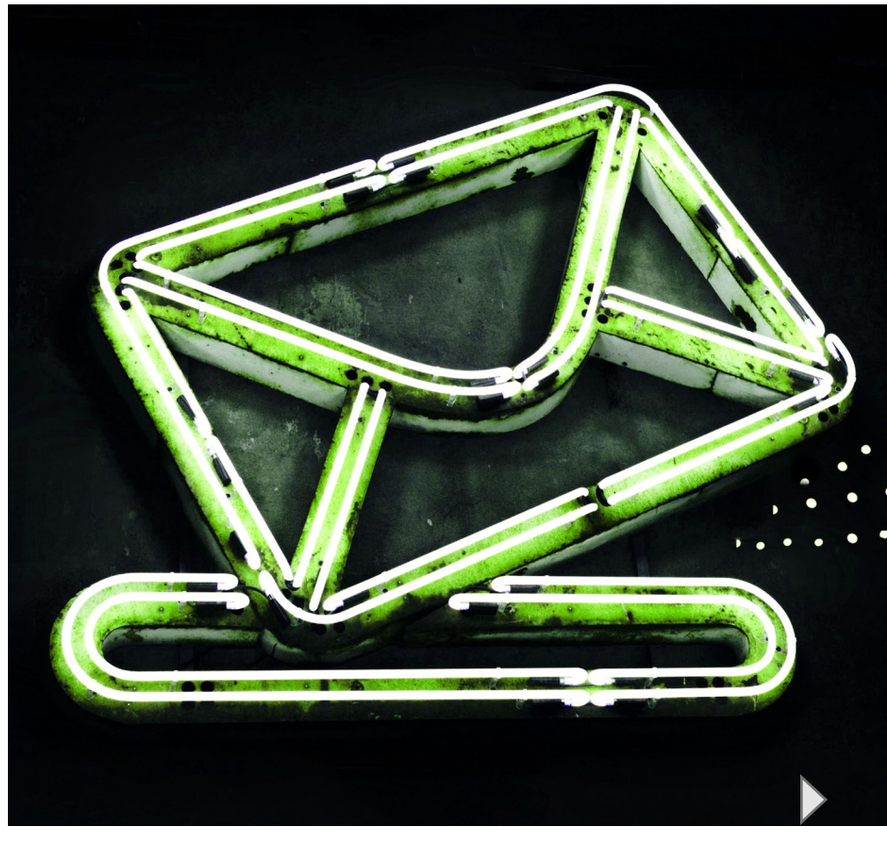
Proofpoint ha pasado de moverse en un mercado de 2.100 millones de dólares, el de la seguridad del correo electrónico, a tener a su disposición una oportunidad de negocio de más de 13.000 millones de dólares

que un 50% pertenecen al Fortune1.000, la lista de las mil empresas más grandes a nivel global. Para Fernando Anaya lo que necesitan los clientes de la compañía es contar con una plataforma de seguridad y de cumplimiento de nueva generación; “hemos acompañado a los clientes que inicialmente tenían soluciones on-premise hacia la cloud gracias a un ecosistema de soluciones adaptado a lo que necesitan”, hasta el punto de que el grueso de la base instalada de Proofpoint está en modo SaaS.

Más allá del correo electrónico

Llegamos al meollo de la cuestión, a esa “Proofpoint más allá del correo electrónico” que inspiró esta entrevista. Y es que la compañía, bien conocida en el mercado de seguridad de email se ha ido abriendo camino hacia otros segmentos del mercado, como CASB (Cloud Access Security Broker), Aislamiento web, formación y concienciación o DLP.

Y lo mejor es que la estrategia de producto que ha seguido la compañía le está permitiendo añadir nuevas capacidades que se han centrado en torno a tres tendencias: mayor adopción de plataformas cloud, consolidación de la seguridad y Zero Trust. La adopción de plataformas en la nube impulsó la aparición de soluciones de



seguridad cloud para proteger el acceso a las redes, aplicaciones y las cargas de trabajo que residen en ellas. La consolidación de la seguridad siguió el impulso natural de las empresas para optimizar el coste total de propiedad de sus ofertas de seguridad. Zero Trust se ha convertido en un nuevo estándar de seguridad que surgió a medida que más terminales y usuarios salían del perímetro de la red tradicional.

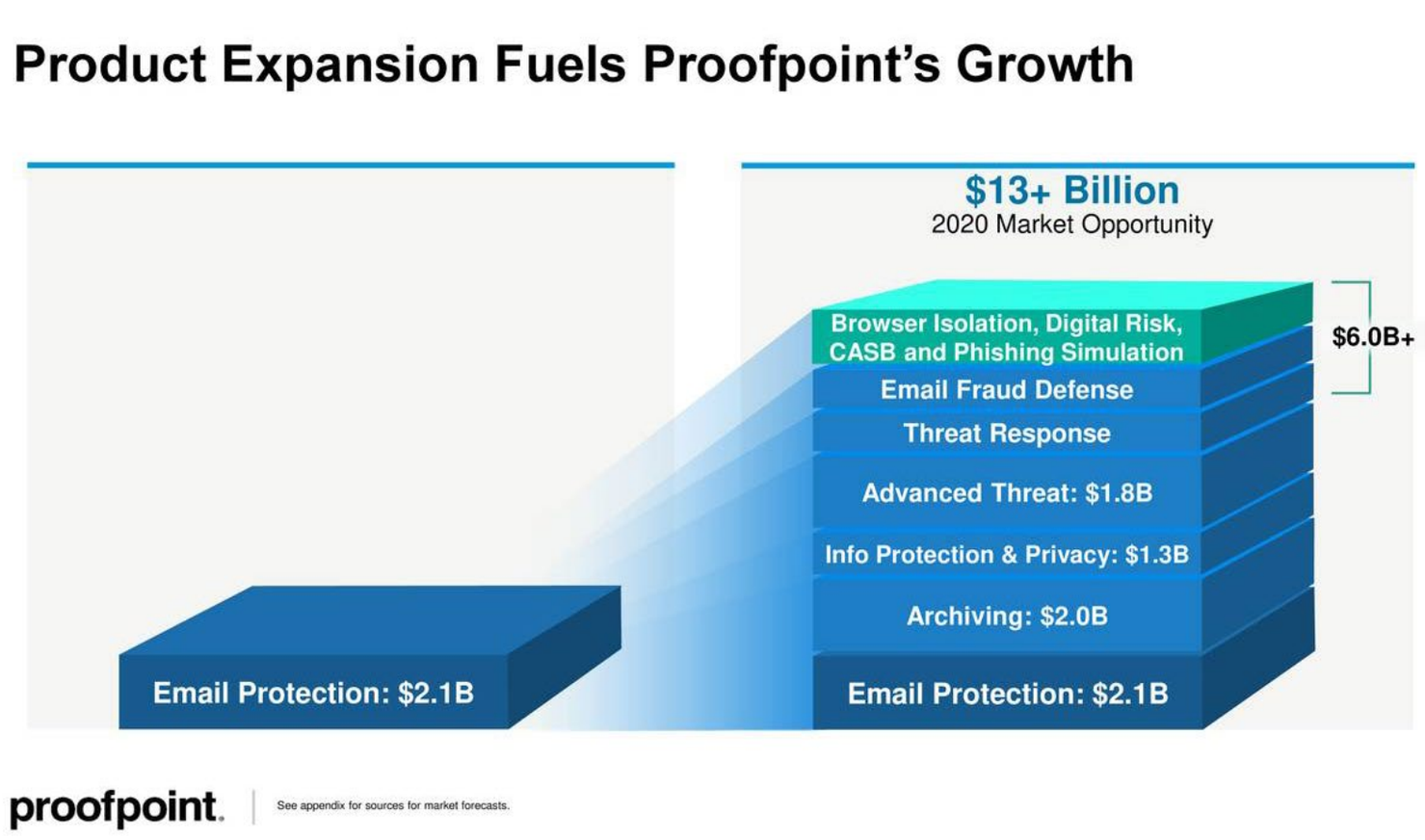
La mayoría de estas capacidades se han realizado con adquisiciones brillantes, como la de Meta Networks en 2016 por 120 millones de dólares, que le dio capacidades ZTNA (Zero Trust), y con la que Proofpoint adquirió la oportunidad de aumentar sus capacidades para brindar soluciones de trabajo remoto.

En su apuesta por hacer frente a las amenazas internas fue vital la compra de ObserveIT, que le dio a Proofpoint los activos que necesitaba para comprender los puntos finales y cómo los usuarios interactúan con ellos. En cuanto a la prevención de pérdida de datos, Proofpoint apostó por agregar capacidades de DLP en la nube y en el endpoint a las que ya tenía en el correo electrónico. Por cierto que el mercado de DLP tiene competidores de la talla de Symantec, McAfee o Forcepoint, pero el hecho de que Proofpoint haya sido una de las compañías de reemplazo para muchos clientes de McAfee o Stymantec en la protección del correo electrónico, hace que su posicionamiento en el mercado de DLP sea prometedor.

De forma que poco a poco, Proofpoint ha pasado de moverse en un mercado de 2.100 millones de dólares, el de la seguridad del correo electrónico, a tener a su disposición una oportunidad de negocio de más de 13.000 millones de dólares.

Sin dar cifras concretas, asegura Fernando Anaya que la protección del correo electrónico es donde la trayectoria de la compañía es más amplia, pero que se está teniendo “mucho éxito” en las soluciones de concienciación porque “un usuario que está concienciado es un usuario que va a estar en disposición de poder rechazar una amenaza”.

Dejar de cotizar en Bolsa permite a Proofpoint ser más ágiles y flexibles a la hora de invertir en innovación y en infraestructura



Compras destacadas

Las cerca de 20 adquisiciones que Proofpoint ha realizado en sus casi 20 años de historia han colocado a la compañía donde está hoy. Las últimas y más destacadas han sido:

- InteliSecure. 2021. 62,5 millones de dólares. InteliSecure es un proveedor de servicios gestionados de protección contra pérdida de datos que fortalecerá la plataforma de seguridad de Proofpoint centrada en las personas y basada en la nube al mejorar la capacidad de los clientes para proteger datos críticos en diversos entornos.
- ObserveIT. 2019. 225 millones de dólares. ObserveIT es conocido por su plataforma de seguridad que identifica y elimina las amenazas internas dentro de la organización. Proofpoint cree que a medida que las empresas hacen la transición a la nube, los métodos tradicionales de protección de datos y propiedad intelectual pueden no ser suficientes. Planea aprovechar la adquisición de ObserveIT para ampliar sus capacidades DLP de corredor de seguridad de acceso a la nube y correo electrónico (CASB) con el punto final.
- Meta Networks. 2019. 120 millones de dólares. Con la compra de Meta Networs, experto en el mercado de ZTNZ, Proofpoint reforzó su arquitectura basada en la nube y su plataforma de seguridad centrada en las personas, permitiendo a los clientes proteger mejor a sus personas así como a las aplicaciones y datos a los que acceden más allá del perímetro tradicional.
- Wombat Security. 2018. 225 millones de dólares. Wombat Security Technologies era un experto en simulación de suplantación de identidad (phishing) y formación informática sobre seguridad. Al recopilar datos de la solución PhishAlarm de Wombat, Proofpoint tuvo acceso a los datos de las campañas de phishing tal como las ven los clientes que no pertenecen a Proofpoint, lo que brinda una mayor visibilidad y conocimiento de la plataforma Proofpoint Nexus.
- Weblife. 2017. 60 millones de dólares. La compra de Weblife, un proveedor de solucioens de browser isolation permitió a Proofpoint extender sus capacidades avanzadas de protección contra amenazas al correo electrónico personal.
- Cloudmark. 2017. 110 millones de dólares. Cloudmark ofrecía seguridad de mensajería e inteligencia de amenazas a los ISP y operadores móviles de todo el mundo, y su tecnología reforzó la efectividad de los productos de Proofpoint ya que, como parte de la adquisición, la Red Global de Amenazas de Cloudmark se incorporó a la plataforma Nexus de Proofpoint.
- FireLayers. 2016. 55 millones de dólares. Con la compra de FireLayers, experta en seguridad en la nube, Proofpoint amplió su Targeted Attack Protection (TAP) a las aplicaciones SaaS, y mejoró la plataforma de seguridad y cumplimiento Proofpoint Nexus.

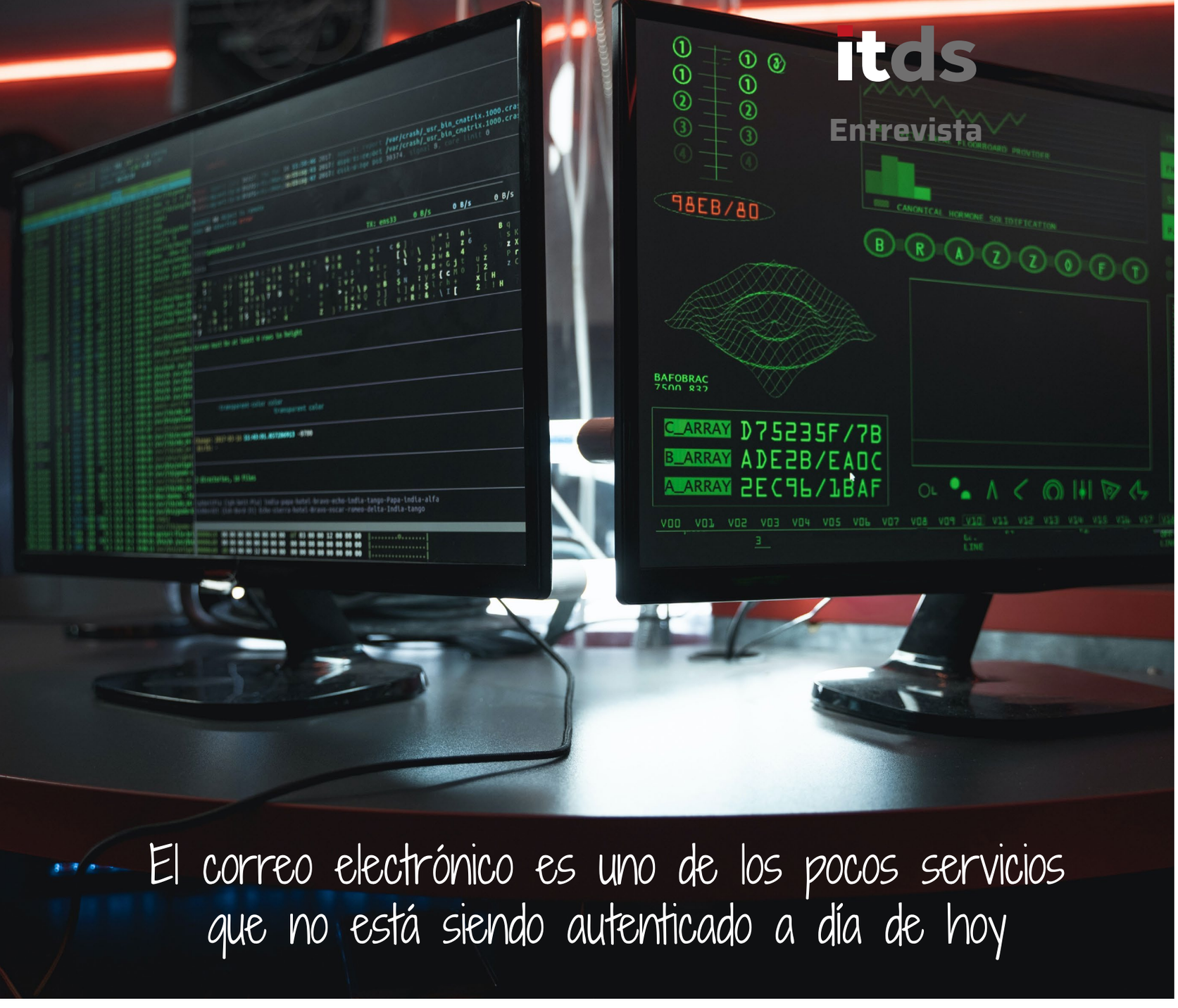
"Hemos acompañado a los clientes que inicialmente tenían soluciones on-premise hacia la cloud gracias a un ecosistema de soluciones adaptado a lo que necesitan"

Asegurando que el correo electrónico es uno de los pocos servicios que no está siendo autenticado a día de hoy, explica el directivo de Proofpoint que las soluciones de la compañía relacionadas la protección de dominios a través de DMARC (Domain-based Message Authentication, Reporting & Conformance, o Autenticación de mensajes, informes y conformidad basada en dominios) también están funcionando muy bien. Explica Fernando Anaya que el correo es muy fácilmente suplantable y que las soluciones de la compañía impiden que se suplante la identidad del usuario en el correo.

Continúa Fernando Anaya repasando las herramientas menos conocidas de la compañía, como la solución CASB que está impulsando su negocio de segurida cloud, hasta llegar a la protección de amenazas internas, las que se originan dentro de la organización; “desde Proofpoint estamos viendo que el 30% de las exfiltraciones de datos se producen desde dentro de la propia organización”, apunta Anaya, añadiendo que la compañía ya tiene alguna referencia con su propuesta, que permite “no sólo proteger el dato en el endpoint y el correo, sino también en la nube”.

Mirando al futuro prevé Anaya que el mayor crecimiento venga por la protección de la información en general o protección del dato – DLP, la protección de la nube – CASB y la protección de las amenazas internas.

Para el country manager de Proofpoint en España el valor diferencial de la compañía es “una visión centrada en las personas, el haber construido un ecosistema de soluciones que están centradas en proteger a los usuarios”, un camino que se inicia protegiendo el mayor vector de ataque, que es el correo electrónico.



Por cierto que hace unos meses se escribía un nuevo capítulo en la historia de Proofpoint. A finales de abril se anunciaba la compra de la compañía por Thoma Bravo en una operación valorada en 12.300 millones de dólares. Asegura Fernando Anaya que la compañía se encuentra bien posicionada “para poder beneficiarnos de la experiencia que aporta Thoma Bravo en cuanto a inversión en empresas de software y su visión a la hora de generar valor”. La compra ha supuesto que Proofpoint vuelve a ser una empresa privada que ha dejado de cotizar en bolsa, lo que “nos permitirá ser más ágiles y flexibles a la hora de invertir en innovación y en infraestructura, además del go-to-market”.

Enlaces de interés...

- Proofpoint Data Loss Prevention
- Módulos de formación de Proofpoint Essentials – Security Awareness Training
- Lecciones de una pandemia: La importancia de concienciar en ciberseguridad no solo en tiempos de crisis

Compartir en RRSS

EMPRESAS DATA-DRIVEN

EVENTO ONLINE

Estrategias de datos para marcar la diferencia

28 de octubre · 9:00 h.

REGISTRO

FORO it User TECH & BUSINESS

Organiza

it Digital MEDIA GROUP

Patrocinadores Platinum

MicroStrategy · VEEAM

Patrocinadores Silver

elastic · making science · MICRO FOCUS

Socios colaboradores

FUNDACIÓN Big Data · DATIA · ticjob

Patrocinadores Gold

PURESTORAGE® · Quest

‘Un acceso de una identidad es privilegiado o no dependiendo de a dónde va’

(Albert Barnwell, CyberArk)

Las soluciones de gestión de accesos privilegiados (PAM) se han convertido en una parte fundamental para diseñar una estrategia de seguridad sólida en todas las empresas. CyberArk, uno de los líderes de este mercado, ha adquirido nuevas capacidades más allá del espacio PAM gracias, fundamentalmente, a la compra el año pasado de Idaptive, con la que se adentró en el espacio de gestión de identidades y accesos (IAM).

Rosalía Arroyo

Idaptive ofrece capacidades en SSO, MFA, gestión del ciclo de vida y gestión de terminales con tecnología de IA. Las capacidades de Idaptive están ayudando a posicionar a CyberArk como una plataforma de identidad moderna, algo necesario a medida que más clientes migran cargas de trabajo a plataformas en la nube.

La tendencia en el mercado de TI en general, y de ciberseguridad en particular, apunta a la consolidación. El segmento de administración de acceso se divide en segmentos de gobierno de identidad, administración de acceso con privilegios y administración de acceso. Como es previsible, los jugadores en el espacio de gestión de identidades están adquiriendo capacidades más allá de su nicho para ampliar su alcance.

Sobre el mercado PAM, IAM, el impacto del as-a-service, la madurez de la empresa española, la consolidación de este mercado, entre otros temas, hemos hablado con Albert Barnwell, sales manager para España y Portugal de CyberArk.

Empezamos protegiendo las identidades y ahora nos volcamos con los accesos privilegiados, ¿cómo se ha vivido esta evolución? ¿Dejaremos de hablar de IAM para centrarnos en PAM?

Durante muchos años hemos dicho que las identidades son el nuevo perímetro de seguridad. Desde

"Nuestra posición ha cambiado en el último año tras la compra de ldaptive, que nos aporta nuevas funcionalidades de gestión de accesos, de Single Sign On (SSO), etc."

CyberArk nos hemos centrado en las identidades privilegiadas porque siempre hemos pensado que son las más críticas, debido a que están accediendo constantemente a nuestras infraestructuras críticas, donde tenemos nuestras aplicaciones de negocio o información que puede ser muy sensible.

En los últimos dos años no sólo nos estamos preocupando de dar ese nivel de seguridad a las cuentas privilegiadas, sino también de cubrir gran parte de las identidades. Piensa que al final un acceso de una identidad es privilegiado, o no, dependiendo de a dónde va; si va a acceder a una aplicación de negocio o una infraestructura que es crítica, es privilegiada, independientemente de si el usuario es de negocio o de IT.

¿Cuán madura está la empresa española en la adopción de estas tecnologías?

Nosotros llevamos más de ocho años en España y hemos visto la evolución de la adopción, que se inició en mercados como banca o seguros que estaban mucho más regulados. Ahora se han incorporado empresas de otros sectores, como telcos, pharma, manufacturing… que están empezando con proyectos estratégicos para poder alcanzar los niveles de seguridad que les están pidiendo, tanto internamente como los proveedores.

Es verdad que el mercado español, si lo comparamos con otros mercados europeos, siempre va un poquito por detrás a nivel de madurez, pero nosotros tenemos proyectos que a nivel de envergadura,

"Los clientes quieren consolidar y simplificar la infraestructura y la relación que tienen con proveedores"

capacidades y estrategia se pueden comparar con niveles de otros países.

También estamos viendo un cambio de paradigma debido a que se está evolucionando hacia unos sistemas diferentes que están en el cloud, con nuevas maneras de lanzar aplicaciones al mercado que nos están abriendo un abanico de problemáticas de seguridad que tenemos que atajar.

El segmento de IAM/PAM es uno de los que más se está consolidando dentro del mercado de ciberseguridad (Centrify/Thycotic, Bomgar/BeyondTrust). ¿Cuál es el posicionamiento de CyberArk dentro del mercado global de gestión de identidades? ¿y en España?

Nuestra posición ha cambiado en el último año tras la compra de Idaptive, que nos aporta nuevas funcionalidades de gestión de accesos, de Single Sign On (SSO) y mejores prácticas que nosotros recomendamos para cualquier identidad, como es poder autenticarse antes de poder acceder a esos privilegios.

La nuestra es una visión global de la seguridad de las identidades, pero basada en los más de 20 años que llevamos en el mercado PAM, creando una oferta que permite cubrir tanto la parte de accesos como la parte de endpoint, que nosotros tenemos integrado dentro de nuestras aplicaciones. Lo que vemos es que los clientes empiezan a unificar fabricantes en la parte de gestión de usuarios.

¿Estáis viendo esa consolidación y simplificación de toda la infraestructura de TI que ya es casi inabordable por parte de los responsables de seguridad?

Sí. Lo que quieren los clientes es reducir la complejidad. Desde el punto de vista de la seguridad, estamos viendo un movimiento hacia soluciones SaaS, con lo cual también puedes ofrecer un servicio

mucho más flexible y más ágil para el cliente. Al final los clientes quieren consolidar y simplificar la infraestructura y la relación que tienen con proveedores.

¿Dónde está teniendo más éxito CyberArk, en la parte de accesos, cuentas privilegiadas o DevSecOps?

El motor de crecimiento más grande en el último año han sido las soluciones cloud y lo que vemos es que una vez que los clientes abordan proyectos de PAM ven las diferentes propuestas que tiene CyberArk para poder complementar la parte de accesos y la parte del endpoint.

Además, toda la parte de DevOps para nosotros es un diferenciador bastante grande en el mercado, y donde tenemos grandes clientes, porque la gran problemática es cómo se siguen utilizando unas aplicaciones que pueden estar en un entorno híbrido o en un entorno cloud, o qué tipo de funcionalidades o procesos necesito para poder dar unos controles estandarizados a través de toda la capa de infraestructura que podamos tener. Y ahí es donde encajan muy bien las soluciones enfocadas al mundo de DevOps.

Las entidades no humanas, como programas, aplicaciones y bots, también son vulnerables y su protección igualmente importante. ¿Cuál es el posicionamiento de CyberArk frente a esta problemática? ¿Y frente al IoT?

Cuando nosotros trabajamos con los clientes, el primer nivel sería securizar los accesos humanos y después pasamos al acceso no humano, donde hablamos tanto de aplicaciones como de robots, que muchas veces tienen cuentas privilegiadas porque acceden a bases de datos o información que es crítica, y, por tanto, se le tiene que dar el mismo nivel de seguridad que a un administrador.

El tema del IoT lo vemos más como un acceso a infraestructuras críticas, donde no se trata tanto de la conexión a un datacenter como a una maquinaria. Hemos tenido muchos proyectos en el último año porque ahora las infraestructuras críticas deben tener un nivel de seguridad mucho más alto que hace unos años.

"Llevamos más de ocho años en España y hemos visto la evolución de la adopción de PAM, que se inició en mercados como banca o seguros que estaban mucho más regulados"

"Los clientes empiezan a unificar fabricantes en la parte de gestión de usuarios"

En respuesta a las crecientes demandas de los clientes de soluciones en la nube, CyberArk está acelerando su cambio a un modelo SaaS, ¿cómo os va en España?
A nivel de mercado yo creo que los clientes están viendo y aceptando las ventajas de un servicio porque, entre otras cosas, tienes una relación mucho más cercana con un proveedor. Son muchos los clientes que en los últimos tres, cuatro o cinco años han hecho una transición hacia soluciones en la nube a nivel de servicio, y nosotros creemos que le proporciona más flexibilidad y agilidad a la hora de afrontar un proyecto, tanto desde el punto de vista de costes como de funcionalidad. En el caso de CyberArk, ya llevamos de cinco a seis años ofreciendo nuestras soluciones en modo SaaS.

¿Qué impacto tiene que los grandes proveedores de cloud ofrezcan soluciones de gestión de identidades, muchas veces de manera gratuita?
Nosotros colaboramos con Azure, Amazon y Google Cloud en ofrecer soluciones para poder securizar los accesos, tanto a sus plataformas como a un conjunto híbrido. No vemos a estos proveedores como competencia porque, en realidad, no son empresas de seguridad, sino que ofrecen soluciones operativas para poder acceder a sus soluciones.

¿Qué previsiones tienen para este año?
El año pasado tuvimos un crecimiento por encima de lo esperado y este año continuamos con la misma tendencia. Los resultados del segundo trimestre superaron las expectativas del mercado, con lo cual vamos camino de conseguir los objetivos que nos piden internamente. A nivel de clientes tenemos ya el 45-50% del Ibex 35, a nivel de equipo local hemos crecido muchísimo y hemos creado un hub para poder dar capacidades a otros países de Europa.

¿Por dónde cree que puede crecer CyberArk?
Durante este último año lo que hemos visto es que las soluciones PAM en cloud han sido el motor de crecimiento de la empresa. Son soluciones que se enfocan no sólo en clientes pequeños y medianos sino para clientes bastante grandes. Y también estamos viendo un fuerte empuje en todo lo que es la parte de acceso y la parte de DevOps.

Enlaces de interés...

- Mentalidad de atacante, la mejor opción para la seguridad cibernética
- 2021 Gartner Magic Quadrant For Privileged Access Management

Compartir en RRSS

2021

SONICWALL® INFORME DE CIBERAMENAZAS

SONICWALL.COM | @SONICWALLSPAIN

Los **equipos de investigación de amenazas de SonicWall Capture Labs** proporcionan a las empresas, pymes, agencias gubernamentales y otras organizaciones inteligencia de ciberamenazas existentes para proteger a su personal distribuido contra una superficie de ataque en continua expansión.

Al proporcionar una visión completa de estos datos, el ***Informe de Ciberamenazas 2021 de SonicWall*** muestra cómo piensan y operan los cibercriminales, ayudando a las organizaciones a prepararse mejor para las amenazas del futuro.

OBTENGA EL INFORME COMPLETO

sonicwall.com/threatreport

▼ 43%

EL MALWARE CAE AL NIVEL MÁS BAJO DESDE 2014

+ 1 días

IDENTIFICACIÓN MÁS RÁPIDA DE MALWARE "NUNCA ANTES VISTO"

▲ 62%

EL RANSOMWARE ALCANZA UNA CIFRA RÉCORD

▲ 74%

INSPECCIÓN DE MEMORIA PROFUNDA MEJOR QUE NUNCA

▲ Máx. 3 años

EL CRYPTOJACKING HA VUELTO

▲ 66% IOT

EL MALWARE DE IOT AUMENTA UN 66%

▲ 20%

INTENTOS DE INTRUSIÓN EN CONSTANTE CRECIMIENTO

it Digital Security

El papel de la ciberinteligencia en la seguridad empresarial

KELA

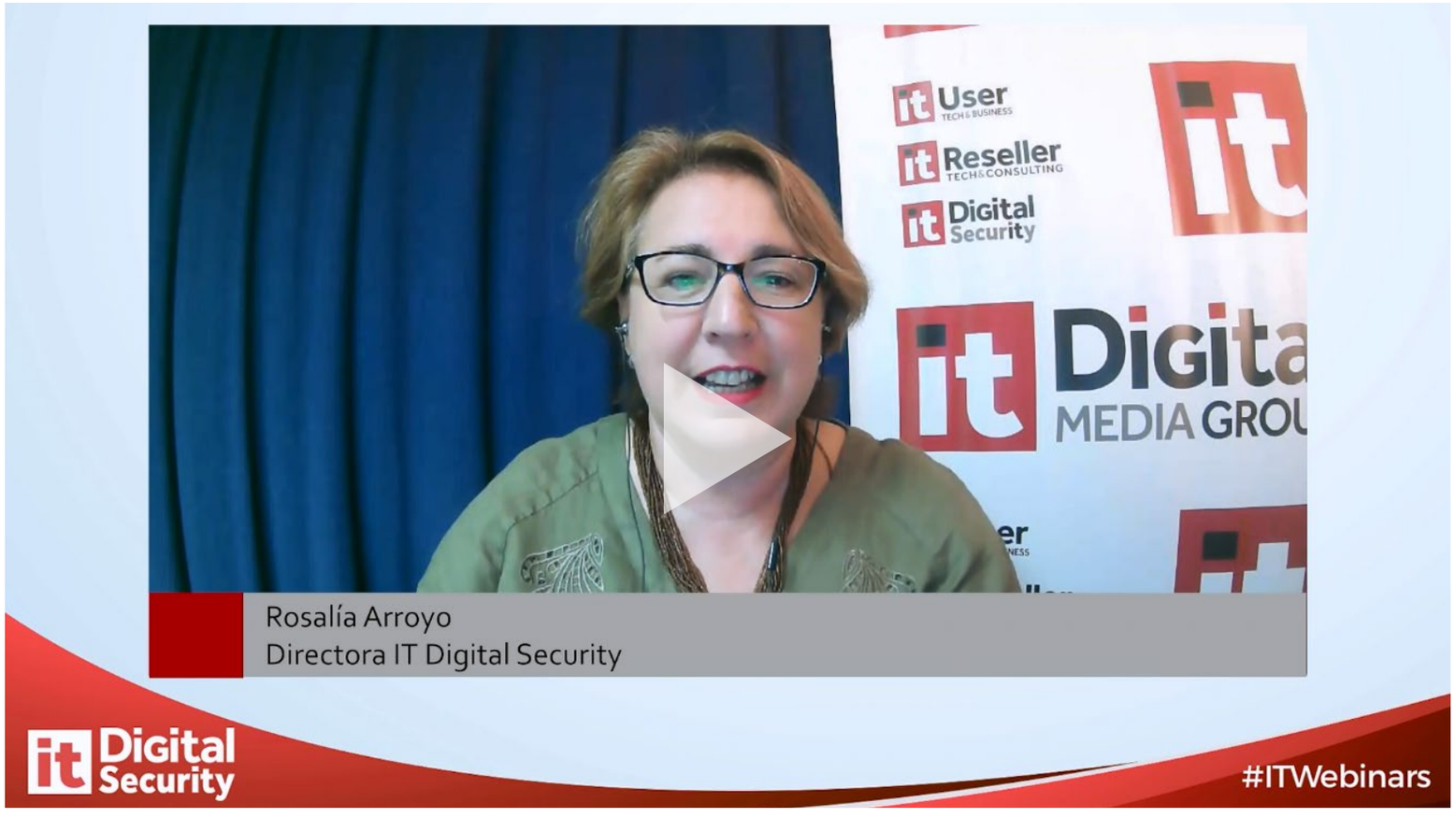
THREATQUOTIENT

ZEROFOX

Octubre 2021

El papel de la ciberinteligencia en la seguridad empresarial

No comprender la escala y la magnitud de una amenaza potencial es el primer error que se comete a la hora de hacer frente a los ciberataques. El segundo, no comprender o saber interpretar el ciberdelito y sus patrones de acción. El tercero, no garantizar la seguridad de los datos e información.



EL PAPEL DE LA CIBERINTELIGENCIA EN LA SEGURIDAD EMPRESARIAL

CLICAR PARA VER EL VÍDEO

La ciberinteligencia es el conocimiento que permite prevenir o mitigar los ciberataques mediante el estudio de los datos de amenazas e información sobre los adversarios. A menudo el análisis depende de tener en cuenta tres elementos: los actores, su intención y motivación, y su capacidad, teniendo en cuenta sus tácticas, técnicas y procedimientos (TTP). Tener esta información y correlarla de la manera adecuada permite a las empresas realizar evaluaciones estratégicas, operativas y tácticas orientadas hacia el futuro.

La ciberinteligencia se ha convertido en el camino más seguro hacia la ciberseguridad en un momento en que los ciberataques se suceden sin freno y las amenazas son desconocidas y sofisticadas. Un futuro marcado por la ciberinteligencia al cubo, una ciberinteligencia que tenga en cuenta la superficie de ataque pública, o cómo saber qué información está expuesta fuera del perímetro para evitar una posible falsificación del site empresarial, desvío de ingresos, robo de datos, suplantación de empleados y la pérdida de confianza de los clientes; la Darkweb, o saber bucear en los mundos oscuros


Juan Grau, ZeroFOX

"La ciberinteligencia será el gran impulsor en el mercado en cuanto al desarrollo de los MSP dedicados a ciberseguridad"

Juan Grau,
Regional Sales Director, ZeroFox

para neutralizar sus amenazas más relevantes, así como el análisis y correlación de eventos a través de una plataforma centrada en las amenazas capaz de mejorar la eficacia y efectividad de las operaciones de seguridad.

Sobre todo ello hemos hablamos en un debate en el que han participado los portavoces de tres empresas que están a la vanguardia de la ciberinteligencia: Borja Rosales, Regional VP Europe de KELA Group; Eutimio Fernández, Regional Sales Manager Spain&Portugal de ThreatQuotient y Juan Grau, Regional Sales Director de ZeroFox, y cuyas conclusiones resumimos en este documento.

Iniciamos el debate preguntando a Borja Rosales por las ciberamenazas a las que se enfrentan las empresas. Indicando que cada empresa tiene sus propias amenazas y sus propias prioridades, menciona el directivo de KELA el problema de las credenciales y accesos comprometidos, así como las vulnerabilidades, tanto las conocidas como las desconocidas; sobre el ransomware dice que es algo que afecta a todo tipo de empresa y organizaciones y termina señalando que "la concienciación o la falta de ella por parte de los usuarios es una amenaza importante que sufren las empresas y que suele dar pie a muchísimos ataques".

Juan Grau define la ciberinteligencia como la tarea de recopilar información, procesarla y transformarla en un conocimiento útil para la investigación, y por lo tanto "ese análisis de información cuyo objetivo es identificar, rastrear, predecir las capacidades o las intenciones y actividades de actores hostiles es lo que podemos definir como ciberinteligencia. En resumen: anticiparnos a los posibles peligros y neutralizarlos antes de que ocurran".

¿Qué viene a solucionar la inteligencia y qué ventajas ofrece? Responde Eutimio Fernández asegurando que la ciberinteligencia ayuda con las amenazas que no son estándar y necesitan dar un paso más a la hora de investigar qué problemas pueden generar. Dice también el directivo de ThreatQuotient que "lo que aporta la ciberinteligencia es conocimiento y anticipación vs completa reactividad, que es como se está abordando ahora la seguridad y la que nos trae tantos problemas".

Más brechas o más transparencia

Cada vez hay más consciencia de la existencia de brechas de seguridad, de ataques de ransomware. Preguntamos a nuestros invitados si es porque hay más brechas o si el colarse en los periódicos y diarios ha dejado al descubierto un problema del

WE ARE KELA

Uncover and demystify threat actors and activities
on the dark web

SCHEDULE A DEMO

We Illuminate

We Empower

We Prevent

We Extend

KELA Illuminate the dark.

que no se tenía conocimiento. Para Borja Rosales las respuestas “no son excluyentes” porque “ambas cosas están ocurriendo”.

Dice Eutimio Fernández que cada vez hay más ataques, más relevantes y están llegando más a los medios de comunicación “porque detrás hay un mercado –el de la ciberdelincuencia, muy grande y muy lucrativo”, asegura apuntando que el mercado de ransomware es mayor que el de la droga y que existen infraestructuras organizadas con mucha inversión para poder lanzar los ataques a gran escala “que estamos viendo continuamente”.

Apunta Juan Grau que los malos siempre van por delante y que hay que tener en cuenta no sólo la cantidad de dinero que hay detrás, sino que “los ataques son cada vez más efectivos” entre otras cosas porque están diversificando los vectores de ataque, como puedes ser el social media, donde ya se produce el 20% de los ataques de phishing, cifra que se espera que aumente hasta el 40% el próximo año, “lo cual es un gran cambio contra el phishing tradicional en correo electrónico”.

Qué demandan los clientes

“Los clientes necesitan simplificar”, asegura Eutimio Fernández cuando le preguntamos qué es lo que están demandando los clientes. La situación viene provocada por varias cosas, como es la falta de

"Las empresas necesitan automatizar procesos y hacerlos sencillos para poder tratar con toda esta información"

Eutimio Fernández,
Regional Sales Manager Spain+Portugal, ThreatQuotient

personal; ataques más numerosos y más dirigidos; así como la gestión de más inputs, producto del avance de las soluciones EDR/XDR/NDR que recopilan más información que tiene que ser analizada. "Las empresas necesitan automatizar procesos y hacerlos sencillos para poder tratar con toda esta información", explica el directivo de ThreatQuotient añadiendo que "aquí es donde los clientes están pidiendo ayuda".

Los ataques más avanzados y la cantidad de información que generan los sistemas lleva a la necesidad de "relacionarla, simplificarla, normalizarla y priorizarla para que las empresas sean capaces de, con el 20% del esfuerzo, hacer el 80% del trabajo".

Juan Grau, director de ZeroFox en España dice que los clientes piden ayuda a un coste asumible; "la mayoría de las empresas tienen muchas necesidades y no saben por dónde empezar", asegura.

Explica además que lo que buscan en una herramienta de ciberinteligencia que aporta información, es que sea "una información ordenada, donde puedan detectar con pocos recursos lo importante, y que esto se haga en tiempo real", a lo que se añade que "tomen acciones para eliminar esas amenazas".

En su turno de respuesta el directivo de KELA apunta a que lo que están demandando las empresas es "que la información de inteligencia que se les

ZEROFOX®

Las plataformas públicas y redes sociales no tienen un **gran gobierno**, **supervisión ni protección** de su perímetro externo de seguridad.

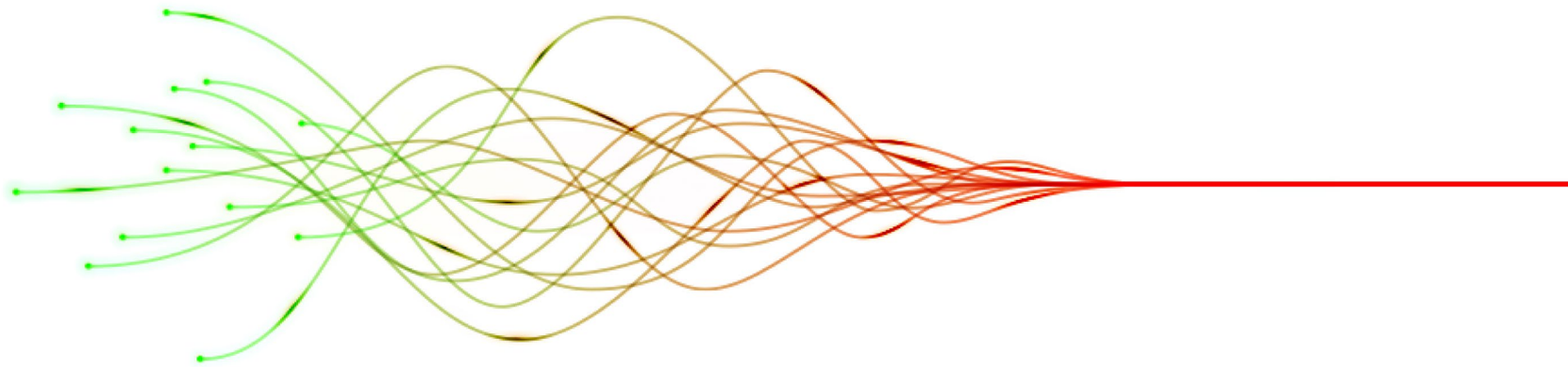
PROTECCIÓN PARA SECULARIZAR HOY.

INTELIGENCIA PARA PROTEGER EL MAÑANA.

ZeroFox proporciona a las empresas protección, inteligencia y disrupción para desmantelar las amenazas externas a marcas, personas, activos y datos en toda la superficie pública de ataque. Todo desde una plataforma integral.

zerofox.com | **@zerofox**

ZeroFox se distribuye en España a través de Ingecom, Value Added Distributor (VAD) especializado en soluciones de ciberseguridad y ciberinteligencia. Si quiere más información sobre ZeroFox, llame al +34 915 715 196 o contacte con nosotros en comercial_ingecom@ingecom.net



aporte sea accionable, que puedan hacer algo con ella, que pueda ayudarles a actuar sobre la amenaza" y priorizar las respuestas.

Darknet, Huella Digital y datos

Las darknet es cobijo de la mayoría de los ciberdelincuentes y es de donde KELA extrae el conocimiento para ofrecer sus servicios de ciberinteligencia. Preguntamos a Borja Rosales qué se cuece en esa red oscura para que a las empresas les resulte necesario saberlo.

Explica el directivo que entendiendo la Darknet como un ecosistema que utilizan los cibercriminales para el desarrollo de sus actividades, "a las empresas les interesa saber qué está pasando dentro de esos foros, de esos mercados, de esos canales de mensajería instantánea para saber si están hablando sobre ellos".

Añade Rosales que la darknet es un ecosistema básicamente motivado por temas económicos al que el directivo se refiere como "el Amazon del cibercrimen" en el que los cibercriminales pueden ir y comprar herramientas que después van a utilizar para desarrollar otros ataques, "y saber que está pasando de esos entornos es muy importante para todas las empresas, pero evidentemente para las muy grandes es casi casi imprescindible".

Hablando de Huella Digital, explica Juan Grau que hay dos clasificaciones: las pasivas y las activas. Las primeras están basadas en "los datos que se están recopilando sin que el propietario lo sepa", como las cookies; y luego está la Huella Activa, que es todo lo que las empresas y usuarios publicamos de forma consciente en las redes sociales. Explica Juan Grau que cuando hablamos de la Huella Digital, o Digital Footprint, de las empresas nos referimos a "los activos e información que manifestamos en internet desde webs y redes sociales a medios de comunicación en internet y market places", y se debe tener en cuenta tanto lo que publican las empresas como entidades, como a lo que publican sus empleados como parte de la empresa, "y hay que tener mucho cuidado con todo ello, porque aunque muchas veces los ataques que tenemos en internet persiguen un rescate, la pérdida de reputación es tan importante o

Borja Rosales
Regional VP Europe, KELA Group

"Las empresas no son conscientes de la cantidad de datos y de información que hay sobre ellas en el ciberespacio"

Borja Rosales,
Regional VP Europe, KELA Group

más que la pérdida de operatividad de la empresa o el pago del rescate".

Como se ha comentado anteriormente las empresas reciben una ingente cantidad de información que genera una serie de retos para las empresas. Por un lado apunta Eutimio Fernández a que esa información procede de diferentes fuentes, bien sean públicas, privadas u open source, "y lo primero que tenemos que pensar es en organizar toda esta información en el mismo formato"; el segundo paso es priorizar, algo que para el directivo de ThreatQuotient es "crítico porque necesito saber qué eventos son los críticos para mí". Habla también Eutimio Fernández de la automatización de tareas sencillas y que la distribución de la información que se genera se realice de una forma rápida. Estos son los retos a los que hace frente ThreatQuotient con su plataforma.

Dónde buscar las amenazas

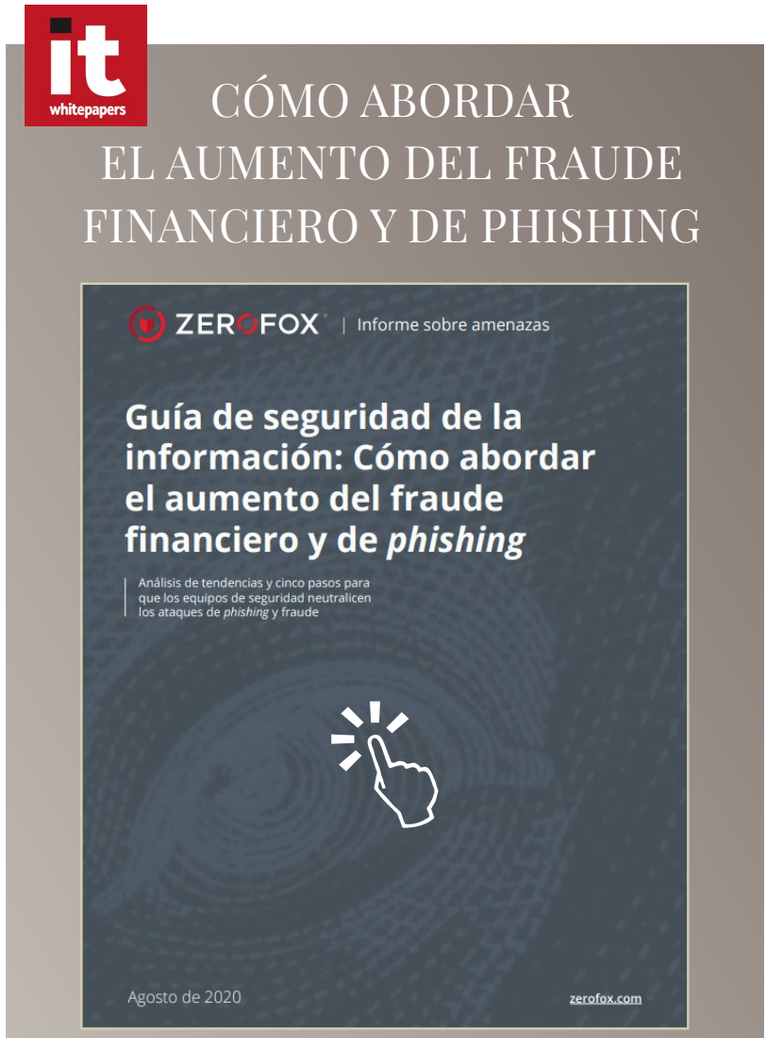
Hablando sobre la manera de buscar, analizar y detectar amenazas, preguntamos a Juan Grau si las empresas son conscientes de la cantidad de información que van dejando por las redes, cuán grande es una huella digital. Asegura que no y que es algo que no deja de sorprenderle, "casi tanto como la

¿Sin reuniones de Zoom hoy?

Permanezca acurrucado con su pijama y una buena lectura

Descargue hoy la guía de mercado de Gartner

THREATQUOTIENT™



En este documento se analizan tres de las principales tácticas nuevas y persistentes de ataque digital que afectan al sector de los servicios financieros y se recomiendan medidas que los profesionales de la seguridad pueden adoptar para abordar de forma efectiva este tipo de amenazas en constante evolución.

La ciberinteligencia se ha convertido en el camino más seguro hacia la ciberseguridad en un momento en que los ciberataques se suceden sin freno y las amenazas son desconocidas y sofisticadas

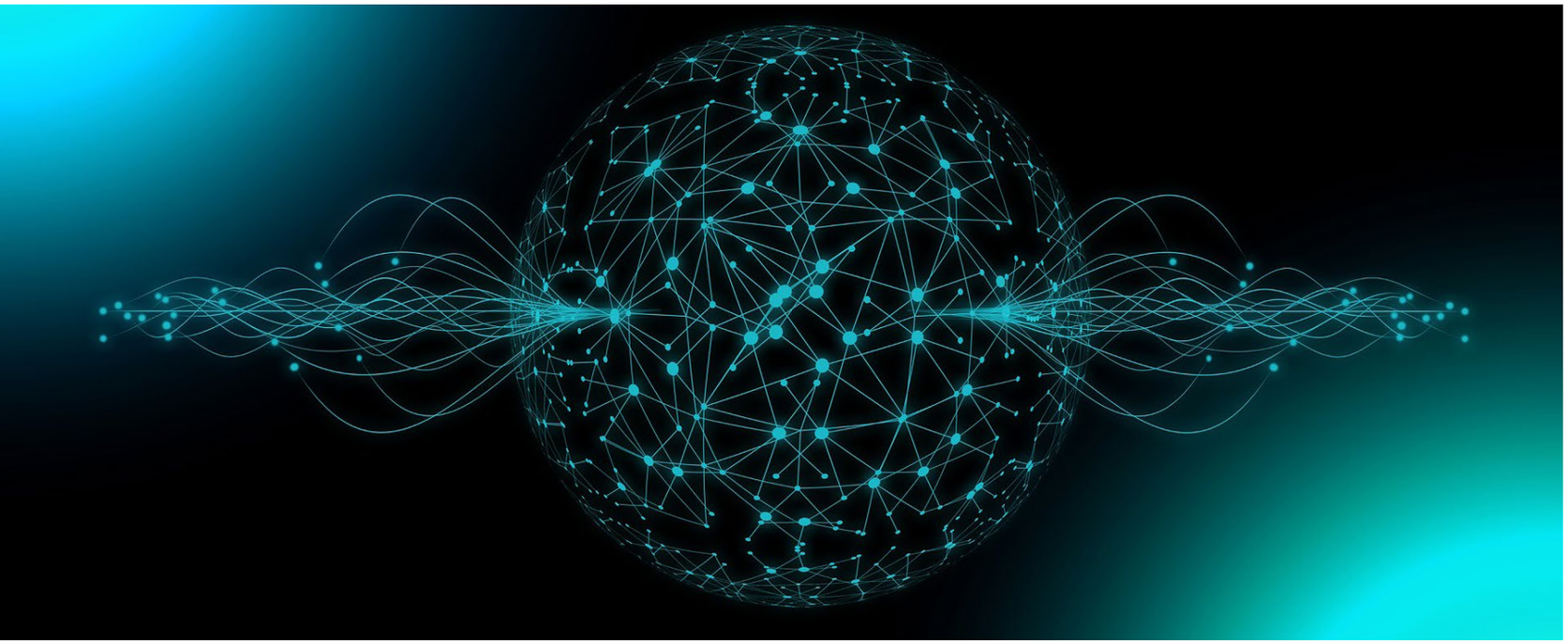
cara de sorpresa que ponen los clientes al ver el resultado de una de nuestras pruebas de concepto", y añade que la mejor forma de analizar y detectar las amenazas es "disponer de una plataforma que realice el proceso de modo continuo", porque "por muchos analistas que tengas, utilizando herramientas más o menos automáticas, estarás descubriendo parcialmente la información que está en la red".

Para el directivo de ZeroFox, tan importante como detectar una fuga de información o un impacto que se tenga en la red "es hacerlo rápido y ser capaz de analizar y priorizar las acciones en base a la criticidad del riesgo futuro".

"No, las empresas no son conscientes de la cantidad de datos y de información que hay sobre ellas en el ciberespacio", dice Borja Rosales, añadiendo que sus clientes también quedan sorprendidos cuando hacen pruebas de concepto. Sobre la manera en que KELA ayuda a la detección de amenazas, explica el directivo que la compañía se mueve "en la zona más oscura y difícil de navegar del ciberespacio", un entorno en el que la automatización es fundamental, "pero también saber dónde estás recabando la información".

Habla Borja Rosales de sitios dentro de esa web profunda que son perfectamente legales y legítimos que no suponen ninguna amenaza, pero también de otra serie de foros muy limitados, con una actividad clarísimamente maliciosa, y una serie de requisitos de entrada; "hay que conseguir entrar a esas fuentes que están ocultas al mundo en general para recabar la información, la inteligencia que está en ellas, y ponerla al alcance de las empresas". Menciona como ejemplo el directivo de KELA listas de accesos VPN disponibles por muy pocos dólares.

Tanto KELA como ZeroFox se dedican a buscar información que puede comprometer a las empresas, o que demuestra que ya están comprometidas. Por su parte, la tarea de ThreatQuotient es recoger esa información y hacerla actuable dentro de la empresa. Explica Eutimio Fernández que se recoge información de fuentes diferentes y que la información coincidente sólo es entre el 5% y el 10%, "por lo que cada fuente de información es muy valiosa" y nos da la visión de que efectivamente los clientes no son conscientes de todo lo que hay por detrás. Añade que también es importante saber "con quién cuentas a la hora de coger esta información y



Enlaces de interés...

- El 85% de las empresas utiliza activamente la inteligencia contra ciberamenazas
- 'Las empresas necesitan madurar en el área de ciberinteligencia' (Eutimio Fernández, ThreatQuotient)
- Las soluciones de ciberinteligencia de Kela llegan a España de la mano de Ingecom

quiénes son tus mejores espías para poder tener en conjunto toda la información que realmente puede ser relevante para ti sin perder demasiados detalles porque los malos también hacen lo posible por ocultarse lo más posible".

Ciberinteligencia en el mundo de hoy

"La ciberinteligencia ayudará en gran manera a prevenir y limitar cualquier futura amenaza", dice Juan Grau cuando le preguntamos cómo puede ayudar la ciberinteligencia en la situación actual del mercado. Añade que las herramientas, si son fáciles de utilizar, resolverán en gran medida la carencia de profesionales expertos en ciberseguridad, que es el gran problema del mercado y que tenemos que suplir con la adopción de herramientas fáciles de utilizar y que nos aporten más información.

Añade el directivo de ZeroFox hoy son las grandes empresas las que hacen uso de la ciberinteligencia, pero que su adopción llegará a todas las empresas de este país y será "el gran impulsor en el mercado en cuanto al desarrollo de los MSP dedicados a ciberseguridad. Las empresas medianas y pequeñas no van a dejar de ser atacadas porque además están más desprevenidas y posiblemente tendrán que utilizar todas estas herramientas a través de empresas de servicios".

Dice Borja Rosales que, salvo los atraques motivados por los estados-nación, los cibercriminales no tienen una predilección por una empresa u otra, "sino que atacan a quien pueden más que a quien quieren". Y si hacen una lista de 50 posibles víctimas, "lo que la ciberinteligencia nos va a permitir es no estar en esa lista porque no tienen información útil que puedan utilizar para para atacarnos".

Se muestra de acuerdo Eutimio Fernández con sus compañeros de evento y añade que la ciberinteligencia es un área que se está activando cada vez más, y donde habrá más oportunidades en todos los sentidos. Añade que las empresas están adoptando muchos productos pero que son empresas como las que participan en este encuentro las que harán "que estos productos piensen de una forma un poco más avanzada, un poco diferente, las que nos ayuden a ser más proactivos, a anticiparnos". it

Compartir en RRSS

itds

IT Webinars

Propuesta tecnológica en torno a la ciberinteligencia

"ACCEDEMOS A LOS RINCONES MÁS DIFÍCILES DEL CIBERESPACIO PARA PROVEER A NUESTROS CLIENTES DE INTELIGENCIA CONTEXTUALIZADA Y ACCIONABLE" (KELA GROUP)

"SOMOS CAPACES DE HACER ACTUABLE TODA LA INTELIGENCIA QUE NOS VIENE DE DIFERENTES FUENTES" (THREATQUOTIENT)

"LAS EMPRESAS DEBEN TENER UNA ESTRATEGIA DE PROTECCIÓN DE LA HUELLA DIGITAL QUE PERMITA DETECTAR AMENAZAS" (ZEROFOX)

Clicar para ver los vídeos

Octubre 2021

NUEVA ENCUESTA

it TRENDS

¿Cómo está evolucionando cloud en las empresas?
¿Cómo está potenciando las estrategias empresariales?

#EncuestaITTrends

PARTICIPA

Educación e innovación.

Tendencias tecnológicas para los nuevos retos

Patrocinadores:

Alcatel·Lucent Enterprise

ESET

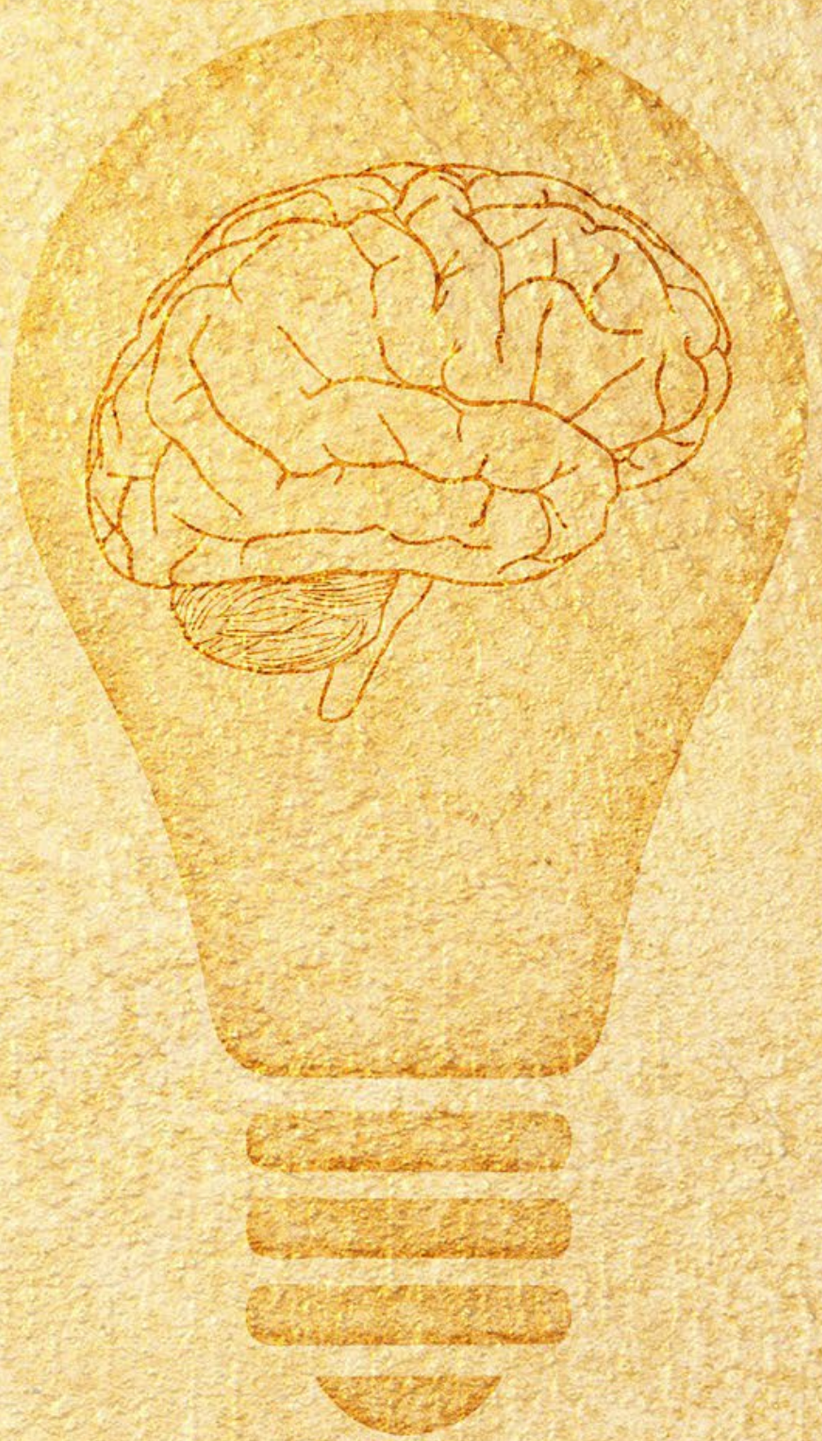
Global Knowledge™ a skillsoft company

SOPHOS Cybersecurity evolved.

WatchGuard

Educación e Innovación

Tendencias tecnológicas para los nuevos retos



La crisis de la Covid-19 ha supuesto una revolución para la amplia mayoría de los sectores, con especial incidencia en la educación y la formación. Este cambio de paradigma ha provocado un verdadero cambio en el perfil profesional que buscan los empleadores, que ahora se apoya más que nunca en otro tipo de habilidades más allá de la capacitación. Las instituciones educativas también han necesitado abordar su propio proceso de transformación digital, con un ojo puesto en las posibilidades que pueden proporcionar tecnologías disruptivas como la Realidad Virtual (RA) o el Internet de las Cosas (IoT).

El primer trimestre de 2020 ha marcado un antes y un después en la economía global. La pandemia derivada de la Covid-19 ha provocado una revolución en los procesos empresariales de prácticamente todos los sectores, que se han visto en la necesidad de acelerar su transformación digital a pasos agigantados para poder seguir siendo relevantes en un mundo cada vez más interconectado, tanto a nivel interno como de cara a sus clientes y/o usuarios.

El sector educativo es uno de los que más se ha visto afectado por esta pandemia, ya que los confinamientos y la recomendación de mantener una distancia interpersonal adecuada hicieron que la presencialidad en la formación se viera interrumpida en un primer momento. Según el informe Panorama de la Educación (Education at a Glance) 2020 de la OECD, China fue el primer país que abordó el cierre de las instituciones educativas en febrero de 2020. A finales de marzo del mismo año este cierre se había instaurado en algún grado en los 38 países miembros y los 8 asociados de la OECD.

En España, el freno a la educación y formación presencial se produjo entre el 11 y el 13 de marzo, ratificado por el Real Decreto 463/2020, de 14 de marzo, que declaró el estado de alarma para la gestión de la crisis sanitaria. Esto provocó que el sector tuviera que enfrentar una transformación digital a gran escala de manera forzosa, ya que todas las actividades que antes se realizaban en un entorno físico debían pasar a efectuarse de manera online, estuvieran o no preparados instituciones y estudiantes.

NUEVOS PERFILES PARA UN NUEVO ENTORNO GLOBAL

Al igual que empresas y demás organismos han necesitado reinventar todos sus procesos, este cambio de paradigma ha puesto de relieve la necesidad de una evolución en el sector educativo para preparar mejor a estudiantes y profesionales, de cara a formar a los mejores perfiles en esta nueva realidad empresarial.

En este sentido, el perfil del formador toma un papel importante, ya que ha necesitado redefinirse, huyendo del rol tradicional hacia nuevas técnicas formativas que obedezcan las necesidades actuales. Según una encuesta de UNICEF España para conocer la respuesta de la comunidad educativa frente a la pandemia de la COVID-19, más de la mitad de los docentes creía importante abordar la formación docente para mejorar la calidad de la educación a distancia, mientras que un 21,7% lo consideraba urgente.

Este entorno global en constante cambio requiere resistencia y adaptabilidad. Un informe

de McKinsey Global Institute estima que en 2030 la demanda de habilidades tecnológicas entre los profesionales aumentará en un 52%, las habilidades sociales y emocionales un 22% y las habilidades cognitivas en un 7%. Por su parte, el informe Workforce Ecosystems de MIT-Sloan Management Review en colaboración con Deloitte señalaba que más del 90% de los managers encuestados creía necesario el acceso a nuevas capacidades, conjuntos de habilidades y competencias de cara al futuro. De ellos, el 35% apostaba por impulsar capacidades en los campos digital, de datos, cloud, seguridad y soft skills.

Los datos señalan que esta era del teletrabajo ha cambiado por completo las características que los reclutadores buscan entre los nuevos empleados, cobrando cada vez más importancia las habilidades blandas o 'soft skills' frente a la capacitación profesional. La escuela de negocios IEBS señala 10 de estas habilidades como imprescindibles, donde que destacan la resiliencia, el pensamiento crítico, el compromiso, la flexibilidad, el trabajo en equipo, la mentalidad de crecimiento, el aprendizaje constante e independiente, la creatividad, la toma de decisiones en base a datos y las habilidades digitales.

TECNOLOGÍA Y CERTIFICACIONES PARA LA NUEVA NORMALIDAD

La nueva realidad ha supuesto un avance en la transformación digital del sector que se ha visto en la necesidad de apostar por la tecnología para impartir formación a través de métodos que no se habían instaurado en gran medida con anterioridad a la pandemia. El reto al que se enfrentan las instituciones educativas es el de capacitar a sus alumnos para que sean capaces de competir en un nuevo entorno laboral.

El sector educativo es uno de los que más se ha visto afectado por esta pandemia, ya que los confinamientos y la recomendación de mantener una distancia interpersonal adecuada hicieron que la presencialidad en la formación se viera interrumpida en un primer momento

El Informe del Estudiante Conectado de Salesforce pone de manifiesto que esta nueva normalidad debe apostar por un entorno mixto, como demuestra que el 43% de los estudiantes y el 54% de los profesionales está a favor de los cursos híbridos. Según el mismo estudio, más de seis de cada diez miembros del personal afirmó que la pandemia obligó a su institución a reevaluar los

modelos de servicio y apoyo del personal, así como a invertir en capacitación que permitiera al profesorado y al resto del personal desempeñar su trabajo de forma virtual. Por otro lado, el 52% estima que su institución invertirá en más tecnología para el aula y más de una cuarta parte afirmó que su institución ha incorporado un puesto de supervisión de la experiencia digital de estudiantes y personal.

A nivel profesional, el panorama señala que los procesos de selección apostarán por certificaciones y conocimientos prácticos frente a la posesión de títulos a la hora de buscar talento. En este sentido, las competencias tecnológicas toman mayor importancia, ya que las empresas necesitan de personal formado en esta materia para poder sustentar la transformación digital en la que se ven inmersas. De hecho, según el informe The Future of Jobs del World Economic Forum, la capacidad de las empresas a nivel global para aprovechar el potencial de crecimiento que ofrece la adopción de las nuevas tecnologías se ve obstaculizada por la escasez de competencias, por lo que están apostando por potenciar la formación de sus trabajadores. Según este estudio, las empresas están proporcionando oportunidades de formación para la reconversión y el perfeccionamiento profesional al 62% de su plantilla, mientras que para 2025 esperan ampliar esa oferta en un 11%. A pesar de ello, son los propios profesionales los que deben dar un paso adelante, ya que este mismo informe indica que solo el 42% de los empleados se acoge a los cursos ofrecidos por la empresa.

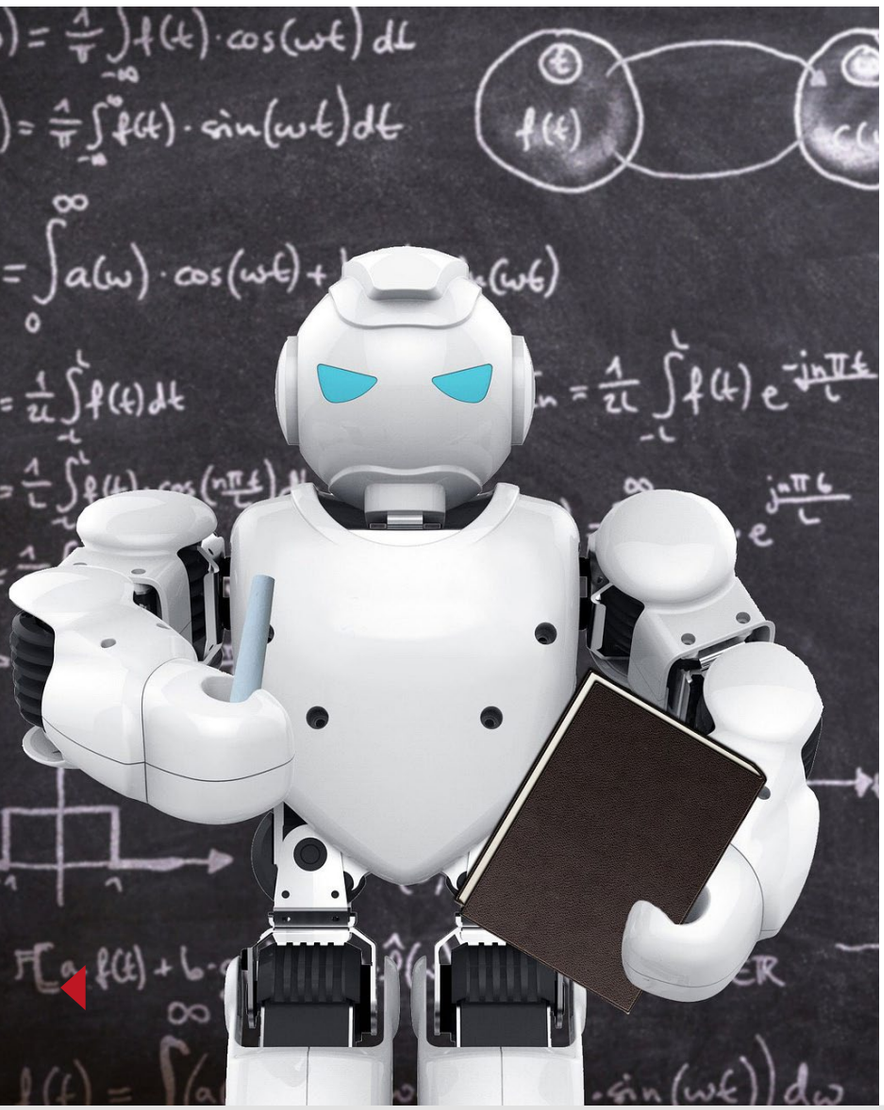
TENDENCIAS TECNOLÓGICAS PARA EL SECTOR EDUCATIVO

Una vez planteada esta transformación digital, las instituciones educativas tienen que pararse a pensar cuáles son las tecnologías en las que deben apoyarse para afrontar los nuevos retos que se les plantean a todos los niveles.

De nuevo el Informe del Estudiante Conectado de Salesforce señala que son varias las instituciones que ya están aplicando mejoras tecnológicas, pero muy pocas las que están utilizando sistemas integrados para comunicarse con sus estudiantes, por lo que se crean brechas en los servicios y la confianza. Así, según los resultados del estudio, menos de la mitad de las instituciones (47%) está priorizando las inversiones en integración tecnológica, mientras que el 45% está otorgando más importancia a los sistemas de CRM y el 40% está apostando por la tecnología de análisis de datos.

Gartner señala en su estudio Top Technology Trends Impacting Higher Education in 2021 cuatro categorías principales en las que se observan estas tendencias: experiencia del estu-

El perfil del formador toma un papel importante, ya que ha necesitado redefinirse, huyendo del rol tradicional hacia nuevas técnicas formativas que obedezcan las necesidades actuales



diante, sostenibilidad del negocio, escalar los cambios y la Nueva Normalidad.

A la hora de hablar de la experiencia del estudiante, Gartner apuesta por experiencias virtuales, ya que señalan que el 72% de los estudiantes expresó su preocupación por no poder ir al campus en 2020. Los eventos virtuales fueron, sin embargo, bien valorados por el 84% de los encuestados. De esta forma, vuelve a ponerse de relieve la importancia del modelo educacional híbrido y del aprendizaje inmersivo, apostando también por tecnologías como la realidad virtual por ejemplo a la hora de conocer las instalaciones de una institución mediante la puesta en marcha de tours virtuales. Un CRM que englobe a todos los departamentos de la institución también cobra importancia en este apartado, ya que permitirá seguir y optimizar todo el ciclo educativo del estudiante de forma centralizada, dando la oportunidad al centro de ofrecerle una mejor experiencia.

La ciberseguridad es uno de los campos más importantes y de las asignaturas pendientes a la hora de hablar del futuro tecnológico del sector y su sostenibilidad. Check Point Research señala que el sector de la educación/investigación es el que se está viendo más afectado en este sentido. De hecho, en los últimos meses las instituciones educativas españolas han recibido una media de 2.998 ataques semanales por centro, lo que se traduce en un 11% más que en el semestre anterior. El Informe de Ciberamenazas 2021 de SonicWall indica que el 63% de los centros educativos no revisan los permisos de forma regular, el 22% no sabe cómo se otorgan los derechos de acceso, el 24% admitió otorgar derechos de acceso directo a cualquier solicitud, y solo el 18% cuenta con un profesional de la ciberseguridad dedicado a tiempo completo entre el personal. Esta brecha entre el nivel de amenazas que se cierne sobre este sector y la falta de preparación de los centros para hacerlas frente es uno de los principales retos que debe abordar cuanto antes el ecosistema educativo.

El cloud computing se revela como la clave para poder escalar todos estos cambios de forma óptima. Al inicio de la pandemia, las universidades y los centros de enseñanza superior se encontraron en una situación de crisis en la que necesitaron una respuesta inmediata y escalable para poder prestar servicios a través de la enseñanza virtual y remota. La nube ofrece a las instituciones una serie de opciones que les permiten trabajar durante la pandemia y desplazó el foco tecnológico hacia objetivos operativos, como el funcionamiento de los centros de datos y la gestión de datos e infraestructura, para ayudar a los centros educativos a cumplir los objetivos más estratégicos en torno a la enseñanza, el aprendizaje y la participación de los estudiantes en el mundo virtual. Además sirve como base para construir la siguiente capa tecnológica para incluir aplicaciones SaaS, Inteli-

gencia Artificial (IA), Business Intelligence (BI) o soluciones IoT.

La automatización en las respuestas a los estudiantes viene de la mano de los Chatbots. El informe de Gartner señala que las instituciones educativas suelen renovar entre el 20% y el 25% de su población estudiantil cada año. Estos nuevos estudiantes tienden a hacer las mismas preguntas que generaciones anteriores, algo que se podría abordar gracias a esta tecnología ahorrando a los centros tiempo y dinero.

La Nueva Normalidad va a dar un papel especial a los dispositivos móviles en el sector educativo, así como el desarrollo de aplicaciones que ayuden en el desarrollo formativo del alumno. El sector de las EdTech está creciendo a un gran ritmo, con un valor a nivel global de algo más de 65.000 millones de euros, cifra que podría llegar hasta los 243.000 millones de euros según un estudio de Grand View Research.

El uso de todas estas tecnologías disruptivas en el sector educativo se ve respaldado por instituciones como la UNESCO, con actividades como la Conferencia internacional sobre la Inteligencia Artificial en la Educación o la Semana del Aprendizaje Mediante Dispositivos Móviles, iniciativas con las que el organismo ayuda a los gobiernos y a otras partes interesadas a valerse de las tecnologías para fomentar el aprendizaje.

Además, el Plan de Recuperación, Transformación y Resiliencia que recoge la estrategia del Gobierno de España para canalizar los fondos proporcionados por Europa para reparar los daños provocados por la crisis de la COVID-19, dedica dos componentes a la modernización del sistema educativo y a la Formación profesional (componentes 20 y 21), con acciones destinadas al refuerzo del capital humano de las próximas generaciones, la eliminación de brechas sociales y territoriales, y el acceso a oportunidades labo-

Esta era del teletrabajo ha cambiado por completo las características que los reclutadores buscan entre los nuevos empleados, cobrando cada vez más importancia las habilidades blandas o 'soft skills' frente a la capacitación profesional

rales dignas y adaptadas a las necesidades del mercado laboral. Este Plan busca, a través de la modernización y digitalización del sistema educativo, avanzar en un modelo educativo personalizado, flexible, que se adapte a las necesidades del alumnado, prevenga el abandono temprano de la educación y promueva la mejora de los resultados educativos. Para alumnos de formación superior, el Plan prepara medidas como la modernización del sistema universitario, el refuerzo de la Universidad Nacional de Educación a Distancia o la mejora de las infraestructuras digitales y equipamientos universitarios.

Está claro que la pandemia de la Covid-19 ha planteado un nuevo escenario en el que el sector educativo ha necesitado encontrar soluciones de manera urgente, acelerando así su transformación digital. Las nuevas tecnologías serán el punto de apoyo para que el sector sea capaz de resolver las necesidades que este novedoso entorno está planteando tanto para el personal propio como para los alumnos, de manera que la Nueva Normalidad suponga un aliciente y se convierta en el empujón definitivo para que las instituciones se olviden del modelo tradicional y puedan dirigirse

MÁS INFORMACIÓN

- Panorama de la Educación (Education at a Glance) 2020 de la OECD
- Real Decreto 463/2020, de 14 de marzo
- Encuesta de UNICEF España para conocer la respuesta de la comunidad educativa frente a la pandemia de la COVID-19
- Informe de McKinsey Global Institute sobre la demanda de habilidades tecnológicas entre los profesionales
- Informe Workforce Ecosystems de MITSloan Management Review en colaboración con Deloitte
- Informe IEBS School sobre soft skills más demandadas en 2021
- Informe del Estudiante Conectado de Salesforce
- The Future of Jobs del World Economic Forum
- Top Technology Trends Impacting Higher Education in 2021 de Gartner
- Datos de ciberataques en el sector educativo de Check Point Research
- Informe de Ciberamenazas 2021 de SonicWall
- Estudio de Grand View Research sobre el mercado EdTech
- Conferencia internacional sobre la Inteligencia Artificial en la Educación de la UNESCO
- Semana del Aprendizaje Mediante Dispositivos Móviles de la UNESCO
- Plan de Recuperación, Transformación y Resiliencia

Rainbow™

Alcatel·Lucent Enterprise

Rainbow™ Classroom

Recrear la experiencia del aula, a distancia, desde su sistema de gestión de aprendizaje

#Educación

#EnseñanzaColaborativa

Educación e Innovación.

Tendencias tecnológicas para los nuevos retos

El sector educativo ha sido uno de los más afectados por la pandemia. Se ha visto en la necesidad de acelerar su transformación digital a pasos agigantados para poder responder a las necesidades de una realidad inédita. Las nuevas tecnologías y la seguridad de toda su infraestructura cobran ahora más importancia que nunca.

La pandemia derivada de la Covid-19 ha provocado un cambio de paradigma en toda la sociedad. Uno de los sectores que más ha sufrido esta situación ha sido el de la educación y la formación, ya que de la noche a la mañana se ha encontrado con la necesidad de realizar todo un cambio en su actividad, pasando de un modelo casi completamente presencial a sistemas de enseñanza en remoto. En esta realidad, en la que los players del sector han tenido que realizar una transformación digital acelerada, las nuevas tecnologías se han convertido en la clave, así como la necesidad de securizar toda esa nueva infraestructura. Por ello, ¿cuáles son los principales retos a los que se debe enfrentar el sector educativo y de la formación en esta nueva normalidad? Para analizar cómo ha impactado este último año en el sector; la brecha digital de la educación; sus carencias; cuáles son las tecnologías o especializaciones que están experimentando mayor demanda; cómo va a impactar este

EDUCACIÓN E INNOVACIÓN.
Tendencias tecnológicas para los nuevos retos

"Toda esa tecnología que está ahí tiene que ser acometida de una manera rápida, flexible, compatible con el futuro, abierta, es ahí donde pensamos que va a haber una gran demanda"

ENRIQUE SÁNCHEZ, COUNTRY BUSINESS LEADER DE ALCATEL LUCENT ENTERPRISE

nuevo modelo en la tecnología; o hacia dónde se dirige el futuro de la educación y qué tecnologías serán las más necesarias, hemos contado en esta Mesa Redonda IT con la participación de Enrique Sánchez, Country Business Leader de Alcatel Lucent Enterprise; Carlos Tortosa, Director de Grandes Cuentas de ESET; Eduardo Moreno, Country Manager de Global Knowledge; Álvaro Fernández, Account Executive de Sophos; y Ricardo de Ena, Area Sales Manager North Spain de WatchGuard.

EL IMPACTO DE LA PANDEMIA EN LA EDUCACIÓN

El último año ha supuesto toda una revolución para el sector, que se ha visto obligado a iniciar una abrupta digitalización de todos sus procesos para poder seguir realizando su actividad. Como indica Enrique Sánchez, "ha significado un cambio de prioridades. La tecnología estaba ahí, pero la prioridad en el uso ha sido muy distinta". Los modelos híbridos han provocado que el uso de las plataformas sea desde cualquier dispositivo y desde cualquier lugar, lo que ha puesto a prueba las capacidades de las empresas de TI para entregar soluciones adecuadas.

Desde el lado formativo, Eduardo Moreno considera que aún nos encontramos en un proceso de adaptación a un nuevo paradigma que ha venido para quedarse. "Las modalidades de impartir formación van a ser clave y van a cambiar la forma en la que aprendemos. Era un paso que quizá ya venía dándose en los últimos años que la pandemia ha acelerado".

Para Álvaro Fernández, el sector de la educación era el más analógico, por lo que la pandemia realmente ha provocado una situación de contingencia. "Ha sido algo completamente inesperado y el sector educativo no estaba preparado, porque era uno de los sectores que se encontraba en un estado más incipiente de

"A nivel tecnológico lo que más se va a demandar va a seguir siendo la protección del dispositivo y la protección de la información, añadiendo la identificación del usuario y después los servicios necesarios para que todo ese círculo esté bien gestionado"

CARLOS TORTOSA, DIRECTOR DE GRANDES CUENTAS DE ESET

transformación digital". Dado que los centros tuvieron que implantar toda esta tecnología con urgencia, ahora es el momento de pensar en la seguridad de esta infraestructura.

REDUCIENDO LA BRECHA DIGITAL

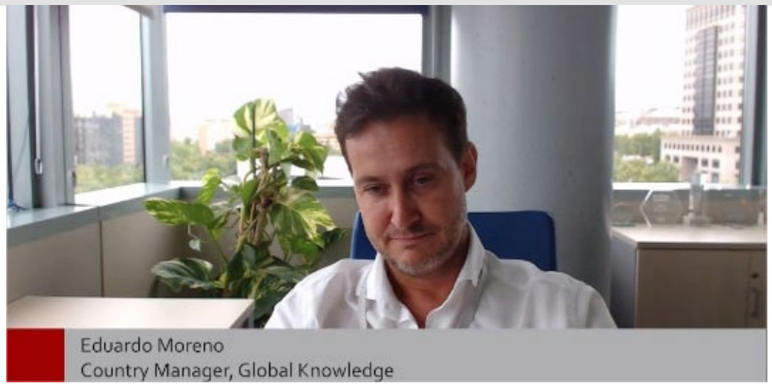
Aunque sea complicado observar puntos positivos en esta situación, es posible que haya

servido para reducir la brecha digital del sector educativo, aunque quizás no lo suficiente.

Así lo señala Carlos Tortosa, cuando habla de que en muchas ocasiones se siguen utilizando dispositivos personales en los que la seguridad puede verse en entredicho, mientras que otros centros han realizado una fuerte inversión para contar con dispositivos y un sistema adecuado. "Existe una brecha digital muy pequeña en lo que sería un entorno educativo más universitario, por la necesidad de disponer de dispositivos con recursos y en los que el nivel de protección es superior. Después, si bajamos un poco el escalón, en la educación secundaria y primaria, es mucho más complicado. Sobre todo porque la brecha digital viene bastante marcada por una brecha también económica".

Por su parte, Ricardo de Ena opina que poco a poco se irá reduciendo esta brecha digital. "Todo lleva un proceso paulatino, desde que se detecta, hasta que realmente se toman las medidas, hasta que realmente hay una labor de concienciación, que deberíamos entonar un poco el mea culpa, si realmente estamos concienciando todo lo que implica y todas las consecuencias que tiene el cerrar esa brecha". Algo que se ve por ejemplo en la actualidad con la carencia de chips que está viviendo el mercado provocada por este boom en la digitalización.

Enrique Sánchez cree que reducir esta brecha digital es una necesidad del mercado y una oportunidad de negocio. "Ya no se trata de ver cómo


Eduardo Moreno
Country Manager, Global Knowledge

"Las modalidades de impartir formación van a ser clave y van a cambiar la forma en la que aprendemos. Era un paso que quizá ya venía dándose en los últimos años y que la pandemia ha acelerado"

EDUARDO MORENO, COUNTRY MANAGER DE GLOBAL KNOWLEDGE

afrontar la situación actual, sino de cuál va a ser el diseño de lo que vamos a hacer en el futuro". En general esta situación ha ayudado a que el sector madure, las conversaciones tanto con centros educativos como con universidades se han vuelto más efectivas. Es importante conseguir integraciones efectivas de la tecnología. Además, no solo hay que fijarse en la parte del alumno, sino que también es necesario poner foco en el funcionamiento interno de las instituciones

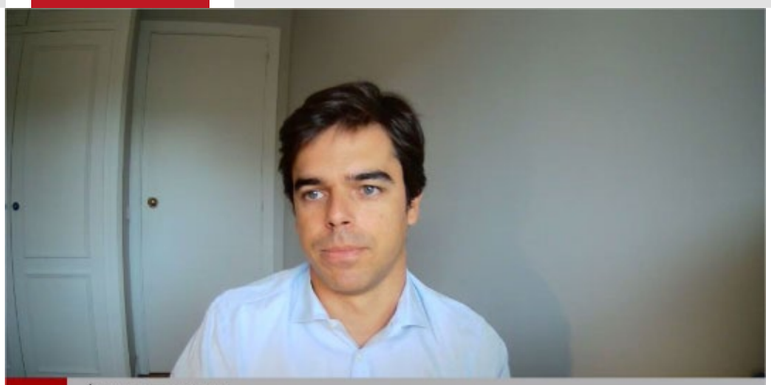
CARENCIAS DE UN SECTOR EN TRANSFORMACIÓN

La pandemia ha destapado algunas carencias tecnológicas en el sector educativo. ¿Cuáles son esos gaps que se han observado a raíz de esta situación?

En la opinión de Eduardo Moreno, universidades y colegios no estaban suficientemente preparados para esto. "Mover toda la formación a modalidades diferentes, como hemos tenido que hacer nosotros, virtualizar absolutamente todo, pasar a microlearnings, a otro tipo de formación más blended, donde se conjugan diferentes metodologías de entrega, requiere una especialización que seguramente ni universidades ni centros escolares tienen". A pesar de que se dispone de la tecnología y de las ganas necesarias para todo este proceso, falta el conocimiento para aplicarla de la forma más conveniente.

Después de haber puesto todo lo que estaba en su mano para conseguir que la rueda siguiera girando, como indica Ricardo de Ena, es el momento de pensar si se han tomado las medidas adecuadas y qué modelo se quiere adoptar. "Esto implica un alto grado de formación a todo ese claustro para hacer frente a esta nueva tecnología, que para ellos es completamente nueva".

Está de acuerdo Enrique Sánchez, que apostilla que esas carencias se han visto tanto en los usua-



Álvaro Fernández
Account Executive, Sophos

“La pandemia ha sido algo completamente inesperado y el sector educativo no estaba preparado, porque era uno de los sectores que se encontraba en un estado más incipiente de transformación digital”

ÁLVARO FERNÁNDEZ, ACCOUNT EXECUTIVE DE SOPHOS

rios como en el propio canal formativo. “Desde el punto de vista de gestión o de implementación ha habido claras áreas de mejora”. A pesar de ello se muestra optimista señalando que el trabajo que se está realizando tiene un ojo puesto en el futuro.

Carlos Tortosa hace hincapié en los gaps observados en la identificación del usuario. “Necesitamos saber realmente que quien está al otro lado de la pantalla es realmente quien dice ser”. También indica que hay otras carencias que se han incrementado, sobre todo a nivel de ciberseguridad.

TECNOLOGÍAS Y ESPECIALIZACIONES MÁS DEMANDADAS

La realidad formativa está cambiando, dirigiéndose hacia nuevos modelos, pero, ¿cuáles son las tecnologías o especializaciones que están experimentando mayor demanda?

Álvaro Fernández lo tiene claro. “Los gestores de contenido y herramientas de videoconferencia han sido las que hemos visto que la demanda se ha incrementado”. La parte negativa es que ese aumento de demanda no se ha visto reflejado desde el punto de vista de la seguridad, algo que se va a plantear ahora.

En esta línea se muestra Carlos Tortosa, indicando que es necesario cubrir necesidades al hablar de autenticación, control parental y concienciación. “Todos tenemos claros cuáles son los riesgos que se corren, tenemos que intentar concienciar a todo el mundo de hasta qué punto todos esos riesgos son reales y qué necesidades tienen para proteger”.

Por su parte, Eduardo Moreno señala que la presencialidad no va a volver a la formación profesional porque realmente no le reporta mayor beneficio al alumno, lo que va a provocar un crecimiento en plataformas y modelos de e-learning. Del mismo modo que tampoco reporta ventajas para las instituciones de formación: “Para los centros educativos es muy complicado mantener centros de educación con muchos metros cuadrados para apenas impartir cursos”.

Ricardo de Ena
Area Sales Manager North Spain, WatchGuard

“Todo lleva un proceso paulatino, desde que se detecta, se toman las medidas, hasta que realmente hay una labor de concienciación; deberíamos entonar un poco el mea culpa, por si realmente estamos concienciando con todo lo que implica y con todas las consecuencias que tiene el cerrar esa brecha”

RICARDO DE ENA, AREA SALES MANAGER NORTH SPAIN DE WATCHGUARD

EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS

Tecnologías como el cloud, la seguridad o la movilidad han impactado mucho en este nuevo modelo educativo hacia el que se dirige el sector, ¿de qué manera van a hacerlo? En opinión de Enrique Sánchez es necesario que las redes sean inteligentes y capaces de adaptarse en todo momento. "Toda esa tecnología que está ahí tiene que ser acometida de una manera rápida, flexible, compatible con el futuro, abierta, es ahí donde pensamos que va a haber una gran demanda".

Ricardo de Ena pone énfasis en la ciberseguridad y comenta que al principio de la pandemia lo más demandado eran conexiones VPN, para que alumnos, profesores y demás personal del centro pudieran acceder a un entorno compartido, seguro y con accesos autenticados. Después la demanda derivó hacia redes wifi seguras con el modelo híbrido. "Ahora vendrán esas auditorías de 'bueno, lo que hemos puesto para pasar la pandemia, ¿nos vale o no nos vale? ¿Nos quedamos con algo o no nos vale?'"

Todo el nuevo paradigma educativo está basado en estas tres tecnologías, según indica Eduardo Moreno resaltando su papel a la hora de impactar en esta nueva realidad educativa. "Ciberseguridad y cloud tienen 0% de desempleo, con lo cual la demanda de estas profesiones va a crecer y crecer, tanto en el sector educativo como en todas las industrias en las que tengan impacto".

De acuerdo se muestra Álvaro Fernández al hablar de la alta tasa de empleabilidad que tienen estas áreas. Pero ahora lo importante es el reto que tienen los colegios de operar esa tecnología que acaban de implementar. "En muchos colegios el propio profesor de Informática es el administrador de sistemas y es la persona que lleva seguridad". De ahí la necesidad de que las soluciones sean fáciles de administrar. ■

MÁS INFORMACIÓN

Mesa redonda IT- Educación

El futuro de la educación

Este nuevo modelo ha venido para quedarse. Esto conduce al planteamiento de una cuestión importante: ¿Hacia dónde se dirige el futuro de la educación y qué tecnologías serán las más necesarias para el sector educativo?

Para Carlos Tortosa el sector se va a dirigir hacia un modelo híbrido, aunque en algunos casos se volverá a la presencialidad, sobre todo al hablar de los más jóvenes y los más mayores. "A nivel tecnológico lo que más se va a demandar va a seguir siendo la protección del dispositivo y la protección de la información, añadiendo la identificación del usuario y después los servicios necesarios para que todo ese círculo esté bien gestionado".

Ante esta pregunta, Álvaro Fernández subraya la necesidad de asentar y consolidar todo lo que se ha hecho durante este año y medio. "Esas tecnologías existen y las tienen que adoptar los centros educativos, tienen que consolidarlas". Desde el punto de vista de la seguridad, tecnologías como VPN, autenticación y servicios que acompañen esa seguridad serán la clave en los próximos años. Además, señala que la transformación digital del sector está comenzando y va a seguir durante los próximos años.

Para finalizar, Ricardo de Ena destaca dos aspectos que para él son fundamentales. Lo primero, que es importante securizar los sistemas sin mermar su rendimiento para que esta transformación digital no sea algo traumático para este sector tradicionalmente analógico. Por otro lado también señala que "volvemos un poco al 2005, cuando empezamos a hablar del bring your own device, que esto en el mercado precisamente de educación se ve al día. Tratar de borrar esa línea que decíamos entonces, esa delgada línea de en qué momento este dispositivo no es corporativo entonces no puedo tomar todas las políticas de ciberseguridad necesarias, pero a la vez necesito que lo traigas porque no te puedo ofrecer ninguno". Por ello incide en conseguir tener la máxima seguridad cumpliendo con la normativa sin que implique un impacto negativo en la conectividad.

MARÍA JOSÉ GARCÍA RODRÍGUEZ, DIRECTORA DE TECNOLOGÍAS
DE LA INFORMACIÓN DE LA UNIVERSIDAD AUTÓNOMA DE MADRID

“La tecnología ha demostrado que es capaz de abrir un abanico de posibilidades que no se habían explorado hasta la fecha”

El sector educativo ya se encontraba en un proceso de innovación disruptiva antes de la pandemia, por lo que, en realidad, la situación vivida solo ha acelerado este proceso.

En su opinión, ¿qué carencias desde el punto de vista tecnológico ha destapado la situación de pandemia que estamos viviendo en las Infraestructuras educativas?
En los días previos al inicio del confinamiento se propusieron muchas ideas para tratar de sobrellevar lo mejor posible el escenario que se nos veía encima, sin saber siquiera cuanto podría durar, porque, en un inicio, se hablaba de unos quince días. El equipo de TI de la UAM optó por pasar a producción los proyectos colaborativos que, hasta ese momento, eran tan solo simples pilotos. La parte tecnológica funcionó incluso mejor de lo esperado, por lo que no puedo destacar grandes carencias. Lo más “costoso” en realidad y en esas circunstancias, fue formar a los usuarios.

¿La situación vivida durante los últimos meses, ¿ha acelerado el proceso de transformación digital en el sector educativo? ¿De qué manera?
Sin duda. La tecnología ha demostrado que es capaz de abrir un abanico de posibilidades que no se habían explorado hasta la fecha, que la tecnología sirve de ayuda. Los métodos docentes previos a la pandemia eran como siempre habían sido las cosas y no se había planteado la posibilidad de cambiarlos, hasta ahora.

"Pasada la premura que requirió poner en marcha soluciones homogéneas, ahora es el momento de entrar al detalle, de poner en marcha una atención personalizada"

¿Cuáles son las principales demandas tecnológicas de los profesionales del sector educativo?
Pasada la premura que requirió poner en marcha soluciones homogéneas, ahora es el momento de entrar al detalle, de poner en marcha una atención personalizada. Porque ni todos los docentes son iguales, ni todas las materias se imparten de la misma forma.

Desde su punto de vista, ¿a qué retos se enfrenta la Educación en España y cuáles son las tecnologías más relevantes que impactan en estos retos?
El sector educativo se encuentra en proceso de cambio, y creo que todavía queda camino para considerarlo maduro. En mi opinión, para que el cambio sea aceptado, la experiencia de las personas ha de ser satisfactoria y para ello precisamos la colaboración de todos de manera coordinada y conjunta.

¿Hasta qué punto el cambio vivido en los modelos educativos ha venido para quedarse y de qué manera las nuevas tecnologías van a ayudar a este cambio y a su adaptación?
Gestionar este cambio que venimos afrontando no es tarea fácil. El área TIC debe ser ágil para dar soluciones a los problemas que se vayan planteando, de manera que los cambios se vayan asentando, y sean aceptados de buen grado.

¿Hacia dónde debe evolucionar la Educación y cuáles son los aspectos más críticos de mejora?
El sector educativo ya se encontraba en un proceso de innovación disruptiva antes de la pandemia, por lo que, en realidad, la situación vivida solo ha acelerado este proceso. Los informes internacionales, tales como Gartner, ya vienen marcando desde hace algunos años como las personas demandarán formación a lo largo de su vida, lo que va a requerir soluciones personalizadas para distintas necesidades. ■

MARÍA JOSÉ GARCÍA RODRÍGUEZ,
Directora de Tecnologías de la Información de la Universidad Autónoma de Madrid

Licenciada en C.C. Físicas por la UCM y Executive Master en Sistemas de Información por el IE, lleva más de 25 años desarrollando su carrera profesional en diferentes empresas y organismos, siempre en el área tecnológica.

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN	PREVENCIÓN
ESET Threat Intelligence ESET Virus Radar WeLive Security	Endpoint Protection Platform ESET Mail Security ESET Sharepoint Security ESET Secure Authentication ESET Endpoint Encryption ESET PROTECT
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET PROTECT	Endpoint Protection Platform ESET Dynamic Threat Defense ESET Enterprise Inspector ESET Mail Security ESET Secure SharePoint Server ESET Secure Authentication ESET Endpoint Encryption ESET PROTECT
RESPUESTA	**DETECCIÓN**

CYBERSECURITY EXPERTS ON YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

Responder al cambio de la realidad formativa

ENRIQUE SÁNCHEZ,
Country Business Leader España y Portugal, Alcatel-Lucent Enterprise

La pandemia, a la que tenemos todavía que referirnos, ha obligado de golpe a modificar presupuestos y modelos de negocio y a cambiar las prioridades en los presupuestos. Pero la tecnología ha demostrado algo con claridad: las comunicaciones en nube han eliminado el impacto negativo en la actividad de empresas, centros educativos y organismos de cualquier sector, por el teletrabajo, la enseñanza online y la actividad a distancia.

Centrándome ya en el sector de la enseñanza, hemos visto que algo que los responsables educativos llevaban tiempo valorando ha empezado a acelerarse: nuevos modelos educativos híbridos (que combinan lo remoto y lo presencial, incluso al mismo tiempo), mayor peso del acceso a las herramientas formativas desde cualquier lugar, gestión remota o simplificada de los procesos administrativos para los estudiantes. Asimismo, vemos que sigue siendo prioritario disponer de infraestructuras que garanticen el cumplimiento regulatorio y de seguridad, más teniendo en cuenta la explosión de nuevos elementos como la automatización de procesos mediante nuevos elementos como la IA o el IOT o la integración de comunicaciones en aplicaciones educativas.

DISMINUCIÓN DE LA BRECHA DIGITAL

Todo lo anterior ha supuesto, al menos desde el punto de vista de la priorización de objetivos a corto y medio plazo, un decremento de la brecha digital. Sin embargo, vemos que las entidades educativas aún deben percibir que la tecnología responde a sus necesidades concretas, a sus usos o procesos educativos concretos, y eso es misión de los suministradores y fabricantes como nosotros: debemos entender bien esos retos y tenemos que proponer a las organizaciones educativas soluciones que ofrezcan una respuesta clara y simple de valor demostrado.

Veamos un ejemplo: los responsables de IT de las entidades educativas sí saben que las redes les ofrecen la garantía de seguridad y adaptación a los estudiantes, profesores y personal administrativo. Sin embargo, si nos centramos en el proceso educativo en sí, vemos que muchas universidades o centros de enseñanza secundaria se han planteado aproximaciones de formación híbrida (parte presencial y parte remota) con soluciones que no han sido del todo satisfactorias (complejidad en el uso, necesidad de aprendizajes adicionales, despliegues caros como para generalizarlos en todas las aulas, dificultades culturales y de adaptación a nuevos usos, enseñanza deficiente por problemas de calidad de audio o vídeo). Una propuesta integrada en el entorno que actualmente utilizan y que tenga un mínimo coste de adaptación es esencial.

RESPONDER AL CAMBIO DE LA REALIDAD FORMATICA

Vamos hacia modelos nuevos de comunicaciones en la enseñanza. Muchas entidades ya analizan el futuro a medio plazo y los modelos que se adapten a la nueva realidad. Nosotros nos centramos en una aproximación holística, donde vemos las necesidades en aulas y campus y la forma en la que las redes contribuyen a proporcionar los servicios adecuados con las garantías de seguridad y priorización: redes que entienden los servicios y a los usuarios, y que adaptan sus condiciones a personas, dispositivos o entidades inteligentes.

Por otro lado, adquieren especial importancia los LMS (Learning Management Systems), con un uso general, incluso como elemento vertebrador de la formación en el aula, remota o híbrida. En este sentido, la integración de todos los medios audiovisuales y las comunicaciones en esos sistemas permiten más calidad. Deben tener un coste asequible (lo que descarta las complejas y caras salas de vídeo conferencia o telepresencia). Para cerrar el círculo y ofrecer un servicio integral, pensamos que se deben extender estas capacidades de integración en los procesos educativos a las actividades administrativas, con aplicaciones como los sistemas SIS (Student Information System) que ofrecen a los estudiantes una gestión sencilla desde cualquier lugar, integrando, y aquí está la innovación, el contacto en tiempo real con el personal administrativo, para resolver cualquier problema durante la matriculación, la gestión de pagos o la logística.

El modelo de impartición híbrido va a exigir soluciones flexibles de nube e integración de comunicaciones de tiempo real en los procesos y aplicaciones educativas (LMS, SIS, ...). Y la seguridad y el cumplimiento regulatorio obligarán a disponer de redes inteligentes, altamente disponibles, que contemplen perfiles de usuarios, de dispositivos (IoT o acceso a las aplicaciones) y de elementos que automatizan los procesos con inteligencia artificial. ■

ENRIQUE SÁNCHEZ,
COUNTRY BUSINESS LEADER DE ALCATEL LUCENT ENTERPRISE

Entender el sector para ofrecer soluciones a su medida

El sector educativo tiene necesidades muy específicas. El modelo de educación virtualizada y de soluciones colaborativas ha venido para quedarse, siendo necesario evolucionar con él. Por ello es necesario entender bien el sector para ofrecerle soluciones a su medida.

La transformación digital de la educación se enfrenta a tres grandes retos tecnológicos: seguridad, simplificación e integración. Enrique Sánchez, Country Business Leader de Alcatel Lucent Enterprise indica que leer bien lo que necesita el sector, debido a sus particularidades, es importantísimo.

Por ello es necesario que tanto canal como fabricantes hagan un esfuerzo didáctico y de simplificación para entender verdaderamente los procesos que hay detrás. Ser capaces de entregar soluciones verdaderamente transparentes para el cliente, para el usuario, para la gestión y para la integración. La filosofía de Alcatel Lucent Enterprise es la de crear tecnologías que vayan siempre pensadas hacia la verticalización. Por ello han desarrollado una plataforma abierta y específica cloud con una infraestructura que la soporta capaz de aglutinar todas estas necesidades específicas y servicios para este entorno en concreto de la educación.

Los objetivos favoritos en los que actúa el ransomware

JOSEP ALBORS,
Director de investigación y concienciación de ESET España

Las recomendaciones y medidas de seguridad necesarias para evitar y hacer frente a un ataque de ransomware son sobradamente conocidas y solo hace falta tener la voluntad y contar con los recursos necesarios para aplicarlas. Además, es necesario permanecer actualizado en lo que respecta a las técnicas usadas por los delincuentes para ir revisando las soluciones implementadas, de forma que estas sigan resultando efectivas.

A pesar de llevar muchos años conviviendo con esta amenaza, el ransomware sigue siendo algo desconocido o no muy tomada en cuenta por muchos usuarios y empresas. Por ese motivo, tanto los investigadores de ciberseguridad como los medios de comunicación no dejamos de hacernos eco de su evolución para generar concienciación y conseguir que se adopten medidas eficaces frente a esta amenaza.

Tras varios años analizando esta amenaza hemos podido comprobar como el ransomware ha ido afectando a prácticamente cualquier tipo de usuario o empresa de cualquier sector. Sin embargo, a la hora de elegir sus objetivos se ha visto una clara evolución, con los primeros casos afectando principalmente a usuarios particulares, pasando después a centrarse en pymes y afectando actualmente a empresas y organizaciones de cualquier tamaño.

Actualmente podemos observar ciertas tendencias a la hora de elegir objetivos por parte de los delincuentes y, si bien no estar entre estos objetivos principales no salva a ninguna empresa de ser víctima, si que es interesante analizar las preferencias de los criminales para obtener el mayor beneficio de sus acciones.

Según un reciente análisis, la víctima ideal de los actores detrás de la mayoría de casos de ransomware sería una empresa ubicada en Estados Unidos, Canadá, Australia o la Unión Europea y con unos ingresos mínimos de 5 millones de dólares (y preferiblemente mayores de 100 millones). Esto es solo una guía, puesto que todos los días vemos casos de ataques protagonizados por ransomware en otras regiones y hacia empresas de todos los tamaños, pero sirve para hacerse una idea de lo que buscan los delincuentes.

Además, es destacable observar como algunos grupos evitan atacar directamente o a través de sus afiliados a ciertos sectores como la educación, sanidad, gobierno u ONGs. Los motivos son variopintos y van desde la "ética profesional" hasta intentar evitar llamar demasiado la atención de las autoridades. Ataques recientes como el de Colonial Pipeline o Kaseya han demostrado las capacidades de estos grupos delictivos, pero también han provocado una reacción por parte de las autoridades que los ha puesto en el punto de mira, algo que no les conviene.

En lo que respecta a las técnicas preferidas por el ransomware actualmente, este es un tema que se ha tratado en varias ocasiones pero que nunca está de más repasar. Podemos ver como los accesos a través de RDP o VPN siguen siendo los favoritos por los delincuentes, habiéndose creado todo un mercado de compra/venta de accesos a redes corporativas donde ciertos delincuentes consiguen comprometer su seguridad para después vender este acceso a los operadores de ransomware

o sus afiliados para que accedan, roben información y, seguidamente, la cifren.

También se aprovechan todo tipo de vulnerabilidades para hacerse con el control de sistemas clave como los servidores de Exchange. Una vez se ha conseguido comprometer un sistema dentro de la red, lo normal es que se empleen varias herramientas como Mimikatz o Cobalt Strike para realizar movimientos laterales y conseguir acceder y comprometer otros sistemas importantes como los controladores de dominio, algo que facilita el robo de información confidencial y el posterior cifrado de todos los equipos de la red.

Otros métodos usados por los criminales son el uso del correo electrónico para adjuntar ficheros maliciosos o enlaces que inician la cadena de ejecución de este malware. También hemos visto como se realizan llamadas desde call centers para engañar a los usuarios y que estos descarguen malware desde ciertas páginas web e incluso se han llegado a realizar ofertas a posibles empleados descontentos para que infecten ellos mismos la red a cambio de un porcentaje de los beneficios obtenidos en el pago del rescate. ■

CARLOS TORTOSA, DIRECTOR DE GRANDES CUENTAS DE ESET

Concienciación y soluciones de seguridad robustas

Vivimos una realidad en la que la tecnología se ha vuelto imprescindible para el sector de la educación. A pesar de ello, los centros aún no están totalmente preparados ni completamente protegidos. Para conseguir esta seguridad, es muy importante concienciar a alumnos e instituciones, además de contar con las soluciones adecuadas.

El sector educativo comienza un nuevo curso en el que la tecnología va a seguir siendo protagonista, por lo que es importante proteger tanto dispositivos como redes, así como al propio usuario. Carlos Tortosa, Director de Grandes Cuentas de ESET, explica cómo los centros españoles han necesitado apostar por la digitalización y qué pasos hay que dar para mantener segura toda esa infraestructura.
ESET trabaja en una doble vertiente: concienciación y soluciones de seguridad robustas. Para ello, la compañía está acostumbrada desde hace años a ofrecer formaciones adaptadas a cada tipo de público, desde alumnos de 5 o 6 años hasta profesionales o directivos. Por su parte, las soluciones de ESET están específicamente diseñadas para proteger tanto a los dispositivos del usuario (ordenadores, teléfonos…) como al resto de la infraestructura del centro, incluyendo soluciones de control parental destinadas a proteger a los más pequeños.

Revolución digital
a través de la formación digital

EDUARDO MORENO,
Director General Global Knowledge
(a Skillsoft company)

La transformación digital es la única vía para conseguir no solo competitividad, sino la recuperación económica que tanto necesitamos tras estos tiempos de pandemia y sus consecuencias.

El COVID-19 nos ha obligado a todos a entrar de lleno y quizá de manera apresurada en lo que podríamos llamar la primera revolución digital, una evolución de la segunda revolución industrial que comenzó a principios del siglo XX. En pocas industrias no existe ya cierta huella digital, pero el porvenir es enorme. Es tan grande que es inimaginable, pero indudablemente tiene sus riesgos:

La transformación digital no es ni será sencilla, sobre todo para muchas empresas basadas en procesos tradicionales bien analógicos y/o manuales y, desde luego, pasará por un intenso programa de formación y actualización (o reskilling) a todos los niveles y en todas las capas de cada empresa, independientemente del trabajo.

Este no es el único reto que tenemos por delante: a pesar de que tecnologías como Cloud o Ciberseguridad tienen un 0% unemployment, la industria sigue padeciendo una enorme falta de profesionales en la mayoría de las grandes tendencias tecnológicas, amenazando con ello a un desarrollo adecuado de esta revolución y pudiendo provocar diferencias sociales aún mayores debidas al estancamiento de muchas empresas que no encuentran la llave del crecimiento por falta de conocimiento.

Una vez más, la solución a esta amenaza vuelve a estar en manos de la formación, facilitador clave de la revolución digital.

La formación y la educación también se han visto digitalizadas a todos los niveles. Todos lo hemos vivido encerrados en casa, trabajando desde nuestro despacho con un ordenador portátil, educando a los niños con un iPad, o aprendiendo idiomas desde un móvil y no en un aula. ¿Qué hubiera sido de nuestra economía sin las posibilidades que nos ha brindado la tecnología?

No obstante, la formación solo será la solución a la falta de competitividad, a la brecha digital y al desempleo si también consigue transformarse y adaptarse.

Empresas como Global Knowledge o Skillsoft ya ofrecen todo un arsenal de modalidades de entrega de contenidos que facilitan el aprendizaje en cualquier lugar, de cualquier forma y en cualquier momento.

Las empresas sumidas en plena transformación digital necesitan facilidades. No pueden

abandonar su negocio y dedicar todos sus recursos en pro de la era digital. Necesitan flexibilidad, necesitan poder transformar a sus equipos a través de itinerarios que los lleven de "A" a "B" sin que ello impacte en su día a día. Necesitan poder acceder a un contenido formativo en cualquier momento y poder tener un mentor que les guíe cada día. Necesitan poder practicar con las tecnologías a través de laboratorios disponibles 24x7, y siempre accesibles. Necesitan contenidos actualizados en formato digital, y necesitan poder probar sus conocimientos a través de certificaciones on line, sin necesidad de desplazamientos.

Necesitan, sobre todo, que las empresas de formación nos transformemos tanto como ellos necesitan, y que nos adaptemos totalmente a las demandas de esta ola digital. Una ola que nos llevará a la orilla o que nos arrastrará al fondo. Depende de cómo la abordemos... ■

EDUARDO MORENO, COUNTRY MANAGER DE GLOBAL KNOWLEDGE

Ofrecer un servicio formativo especializado basado en las nuevas tecnologías

El impacto que ha tenido la pandemia en el sector educativo ha sido enorme, que ha cambiado completamente el modelo formativo. También ha provocado una aceleración a la hora de adoptar diferentes tecnologías y modalidades de entrega como la formación virtual o el e-learning.

El reto al que se enfrentan los learning partners es el de adaptarse a estas nuevas circunstancias y crear una infraestructura que pueda ofrecer un servicio formativo especializado basándose en las nuevas tecnologías. Para Eduardo Moreno, Country Manager de Global Knowledge, el cloud y la ciberseguridad son las tendencias más importantes a nivel formativo, ya que se trata de profesiones en las que el desempleo es prácticamente inexistente.

La salida a bolsa de Global Knowledge, así como su fusión con Skillsoft, ha supuesto una gran oportunidad para la compañía. Su propuesta se basa en una experiencia de más de 25 años en el mercado, la especialización de sus formaciones, multimodalidad de entrega y un equipo de profesionales comprometido para asesorar sobre cualquier carrera en la que el cliente quiera especializarse. Además, cuentan con una plataforma basada en inteligencia artificial para gestionar en tiempo real la formación y el talento de los equipos.

Seguridad, pieza clave
en el proyecto educativo de los centros

RICARDO DE ENA,
Area Sales Manager
North Spain WatchGuard Technologies

Internet, smartphones, tablets, apps, Wi-Fi, redes sociales, cloud... es un hecho que las TI nos han cambiado la vida y, por extensión, han influido en la docencia, especialmente a raíz de la pandemia del COVID-19 que, como en tantos otros ámbitos, ha marcado un punto de inflexión en el sector educativo, poniendo de relieve aún más la importancia de la educación online, la dependencia de las nuevas tecnologías y, por supuesto, de contar con accesos y conexiones seguras.

Más del 79% de los profesores cree que la tecnología marca una importante diferencia para hacer que el aprendizaje sea más interesante. Pero si se tienen en cuenta los riesgos asociados al mundo cibernético... la respuesta puede no ser tan positiva, pues hay muchas cuestiones de seguridad relacionadas con el aprendizaje a través del uso de las TI y la educación a distancia, que van desde la seguridad intrínseca de la plataforma elegida y las cuestiones relacionadas con la privacidad, hasta el control del acceso de los usuarios y los problemas relacionados con los derechos de autor de los documentos compartidos en esas plataformas. Por último, está la cuestión de la protección de los menores y otras personas que hacen uso de la plataforma elegida.

Aunque como en todo, en el equilibrio está el punto medio. Y es aquí donde no se deben escatimar esfuerzos por promover la seguridad en los entornos educativos y trabajar para concienciar en el uso responsable de las TI entre alumnos y el personal docente.

Los retos a superar son múltiples, ya que administrar los sistemas de TI en cualquier institución educativa no es tarea fácil. Hoy, los centros de enseñanza cuentan con una base de usuarios formada por estudiantes y personal dispersos en amplias instalaciones que se conectan a través de redes cableadas e inalámbricas por distintos tipos de dispositivos. Recordemos que los dispositivos móviles también están transformando la educación y, por tanto, que los centros necesitan ofrecer acceso a los estudiantes a Wi-Fi de alta velocidad para proporcionarles una abundante cantidad de recursos educativos y herramientas de aprendizaje online. En muchas redes, la seguridad Wi-Fi llega tarde, pero en las escuelas las redes cableadas e inalámbricas requieren lo mismo, es decir, la implementación de soluciones de protección sólidas. Al mismo tiempo, se deben mantener controles adecuados para ofrecer una experiencia en Internet segura y apropiada teniendo en cuenta la edad, pues no debemos olvidar que muchos colegios tienen menores bajo su cuidado.

En definitiva, hablamos de entornos complejos, donde las exigencias a las infraestructuras de TI en términos de rendimiento y seguridad son de lo más alto, pues deben tomarse precauciones para evitar potenciales ciberataques o un mal uso de las tecnologías o la información personal, así como de otro tipo de riesgos que minen una gestión educativa óptima y con garantías para el desarrollo de los estudiantes. Avalar un acceso seguro a Internet y los recursos online, es parte de la estrategia de ciberseguridad que toda institución docente ha de incorporar a su proyecto educativo.

Afortunadamente, y como no podía ser menos, la respuesta a estos desafíos se encuentra también en las TI. Tecnologías más sofisticadas que aportan una protección inteligente e integral, así como la visibilidad de defensa en profundidad ne-

cesaria para proteger a los jóvenes estudiantes y al personal docente, pero a su vez, más fáciles de implementar y gestionar, son uno de los pilares sobre los que se asienta la seguridad de los entornos tecnológicos dentro del mundo de la enseñanza actual conectada que requiere un enfoque unificado para la protección de sus arquitecturas de red. Hoy existen tecnologías inteligentes, rápidas y eficaces diseñadas exclusivamente para garantizar y cumplir con los requisitos de seguridad de las conexiones WiFi más exigentes en el terreno de la enseñanza. Soluciones de autenticación multifactor (MFA) que permiten proteger tanto las contraseñas como la identidad de los usuarios que se conectan a la red del centro educativo, así como sus activos. Herramientas de protección de los endpoints con tecnologías Zero-Trust que permiten la supervisión continua de los endpoints, la detección y la clasificación de toda la actividad para revelar y bloquear comportamientos anómalos de los usuarios, las máquinas y los procesos. Y, por supuesto, tecnologías de protección de red que ayudan a mantener la red protegida contra las amenazas más avanzadas y zero-days. ■

RICARDO DE ENA, AREA SALES MANAGER NORTH SPAIN DE WATCHGUARD

La seguridad como servicio para proteger la transformación digital de la educación

La educación se ha caracterizado por ser un sector muy tradicional que siempre ha estado a la cola desde el punto de vista tecnológico. La pandemia ha provocado una digitalización forzada del sector, en el que el modelo híbrido es el que más posibilidades tiene de asentarse.

El sector educativo está afrontando esa transformación en la medida de sus posibilidades, sobre todo lastrado también por la falta de microchips a escala global. Ricardo de Ena, Area Sales Manager North Spain de WatchGuard, señala que esto ha provocado una apuesta por el modelo de Bring your own Device (BYOD), lo que implica un reto para la seguridad tanto de los propios dispositivos como a la hora de conectarse a la red del centro. La propuesta de WatchGuard está focalizada en el Security as a Service, modelo en el que el cliente puede contar con un partner hiperespecializado capaz de controlar todos los puntos relacionados con la ciberseguridad, desde el perímetro hasta los accesos, pasando por la red o el endpoint, todo ello de una forma sencilla y con un coste ajustado. Además, cuentan con una capa de big data y de monitorización que permite tener una visión global de todo lo que está pasando en la organización.

Principales problemas de ciberseguridad en educación

ÁLVARO FERNANDEZ,
Account Executive para Sophos Iberia

Los ciberdelincuentes han estado atareados buscando nuevas formas de aprovechar técnicas como phishing, ransomware, ingeniería social para llevar a cabo ataques en centros educativos. A continuación, presentamos algunos de los puntos más críticos que deben abordarse para proteger a los usuarios y a los datos.

Los estudiantes y los profesores necesitan tener acceso a herramientas de aprendizaje ubicadas principalmente en la nube (aplicaciones para compartir archivos, email, aplicaciones) y a veces necesitan acceder de forma remota a los recursos en la red escolar. Al mismo tiempo, el personal administrativo y de TI que trabaja desde casa también puede necesitar acceso a sistemas y documentos ubicados en la red escolar. Si el acceso remoto no es seguro, los ciberdelincuentes pueden colarse y tomar el control de toda la red. Utilizar una red privada virtual (VPN) que ofrezca acceso remoto seguro a los usuarios y que proteja todos los datos que fluyen dentro y fuera de la VPN al cifrarlos, es fundamental.

Otro punto importante es contar con una sincronización entre firewall y la seguridad de los endpoints, para identificar instantáneamente los endpoints comprometidos, en el caso de haberlos, aislarlos hasta que se limpien y evitar que las infecciones se propaguen lateralmente a otros dispositivos en la red.

CONTROLAR EL ACCESO A DATOS CONFIDENCIALES

Los datos personales de estudiantes, maestros, exalumnos y personal administrativo, junto con datos confidenciales relacionados con la investigación y la propiedad intelectual de un centro educativo pueden enriquecer a un ciberdelincuente al venderlo o pedir un rescate. Es fundamental imponer el acceso en función de la identidad del usuario, lo que permita a los usuarios autorizados acceder solo a lo que necesitan para realizar su trabajo. Para proteger los datos confidenciales, la investigación y otros recursos críticos, permitir el acceso solo a aquellos que están autorizados, con soporte de autenticación de dos factores (2FA) para acceder a áreas clave del sistema, incluidos IPsec y SSL VPN, portales de usuarios y consolas de administración web, es la mejor opción.

PROTECCIÓN CONTRA MALWARE

Es difícil saber si los dispositivos y las aplicaciones utilizados, cuentan con los últimos parches de seguridad y si el antivirus está actualizado. A menos que dichos dispositivos remotos se conecten a través de una VPN, deberá asegurarse de que están seguros antes de que puedan acceder a los recursos de la red educativa.

Es importante implementar capacidades avanzadas de protección web que puedan identificar y bloquear las últimas amenazas web. Esto permite aplicar reglas de filtrado web para mantener a los estudiantes a salvo de casos de ciberacoso, contenido inapropiado, abuso y otras amenazas online. Los controles periféricos le permiten controlar lo que su personal puede y no puede conectar a sus dispositivos corporativos. Esto le ayuda a proteger su red contra amenazas inesperadas.

PROTECCIÓN CONTRA PHISHING

Los ataques de ingeniería social y phishing plantean importantes riesgos de ciberseguridad para las instituciones educativas. Los estudiantes, profesores o miembros del personal

pueden ser engañados para hacer clic en enlaces maliciosos que pueden proporcionar a los ciberdelincuentes acceso a la red de la escuela y sus valiosos recursos. La mejor manera de contrarrestar los ataques de ingeniería social y phishing es a través de la concienciación y capacitación del usuario. Educar y testear a los usuarios con ataques simulados ayuda a facilitar una cultura positiva de concienciación en ciberseguridad y los hace menos propensos a caer en estafas. Es importante que la seguridad del correo electrónico también esté actualizada y que todos los endpoints tengan protección avanzada contra malware, ransomware, exploits y virus conocidos y desconocidos.

Los dispositivos móviles como teléfonos, tabletas y otros se utilizan cada vez más para la enseñanza. Un solo dispositivo desprotegido aumenta el riesgo de comprometer toda la red y los sistemas escolares, especialmente en un momento en que las escuelas han reducido las barreras para acceder a sus redes, específicamente para los estudiantes. Con la mayoría de los dispositivos conectados a Internet, la superficie de ataque aumenta significativamente. Una solución de seguridad efectiva para dispositivos móviles puede ayudar a mantener seguros a los estudiantes y al personal en Internet, evitando descargas de archivos peligrosos y bloqueando el acceso a sitios web inapropiados. ■

ÁLVARO FERNÁNDEZ, ACCOUNT EXECUTIVE DE SOPHOS

Consolidar y mantener seguras las tecnologías implementadas

La pandemia ha golpeado de lleno al sector de la educación, viviendo una situación de contingencia. Aún falta mucho camino por recorrer tanto desde el punto de vista tecnológico como de la seguridad. Ya no vale sólo con tener una protección para el puesto, es necesario implementar otras tecnologías más avanzadas para mantenerse seguros.

El sector educativo ha sido capaz de acelerar su transformación digital como consecuencia de la crisis provocada por el coronavirus, pero es necesario consolidar lo que se ha hecho hasta el momento y mantener seguras esas tecnologías. Álvaro Fernández, Account Executive de Sophos, señala que la pandemia nos ha enseñado a estar más preparados para dar respuesta ante situaciones que no puedes planificar.

La oferta de Sophos se basa en tres pilares: efectividad en costes, autonomía y sencillez. Sus soluciones ayudan a proteger tanto dispositivos como redes, puntos de acceso o infraestructuras Cloud, con todo centralizado en una única plataforma de gestión en la nube que interconecta todas las soluciones de seguridad de la compañía, para que sean capaces de coordinarse entre sí y tomar decisiones de forma automatizada.

Las amenazas en el sector educativo crecen al ritmo de su digitalización

ALFONSO RAMÍREZ,
director general
Kaspersky Iberia

En el último año y medio, y especialmente debido a la pandemia, el sector educativo ha pasado a entrar en la lista de objetivos de los ciberdelincuentes. Hasta entonces, la incidencia de ataques era bastante limitada, pero con la implantación de la teleeducación y la incorporación de un número cada vez mayor de recursos online para utilizar en el aula, el número de amenazas y su variedad ha evolucionado en gran medida.

Aunque la mayoría del alumnado en España ha vuelto a la educación presencial, el proceso de digitalización del sector sigue avanzando. Por un lado, se adoptan nuevas herramientas y posibilidades para el uso pedagógico, incluyendo varias que no habían sido pensadas para cumplir este rol. Un buen ejemplo de ello son las cuentas de TikTok o Instagram que se usan como complemento a la educación. Muchos de estos nuevos instrumentos están mejorando la experiencia de la enseñanza, pero también introduciendo nuevas amenazas. Algunas de las más habituales son:

1. Los Sistemas de Gestión de Aprendizaje (LMS) como Google Classroom o Frog permiten a los profesores hacer un seguimiento del proceso de aprendizaje de los estudiantes, a la vez que registran su progreso y los aspectos que requieren su atención. A medida que aumenta la cantidad y popularidad de los LMS, también crece el número de sitios de phishing asociados con servicios educativos y de videoconferencias. Sus principales objetivos son robar datos personales o difundir spam en la comunidad educativa. Además, los LMS abren la

posibilidad de que surjan amenazas nuevas e inesperadas, como el Zoombombing.

2. El uso de servicios de vídeo como YouTube, Netflix, SchoolTube, KhanAcademy, etc. es cada vez mayor. La tendencia es la creación de más videos educativos que circularán como producto terminado o que serán utilizados por los educadores. De hecho, el 87% de los profesores utiliza contenidos de vídeo en el aula. Los videos pueden ser una poderosa herramienta educativa, pero las plataformas más populares también albergan una gran cantidad de contenido inapropiado para menores, y los creadores de este contenido podrían usar temas educativos para llamar la atención hacia su material. Este no es un riesgo nuevo, pero con el aumento de la digitalización su relevancia también crecerá.

3. Uso de herramientas de redes sociales en el proceso educativo. Las redes sociales (Instagram, Twitter, etc.) son un excelente instrumento para promover la participación de los estudiantes durante y después de clases, y también ayudan a que los profesores se conecten con sus estudiantes. Pero existen amenazas vinculadas a su contenido: comentarios ofensivos, contenido inapropiado, ciberacoso... La privacidad es otro punto para considerar, ya que es posible comprometer datos personales a través de aplicaciones o servicios mal configurados, incluso sin necesidad de usar instrumentos o vulnerabilidades especiales. Y tanto estudiantes como profesores pueden ser víctimas de este tipo de ataques.

> “Comprender los riesgos a los que nos exponemos y proteger nuestros dispositivos resulta clave”

4. Introducción de juegos en el proceso educativo. Casi todos los estudiantes ya saben que se puede aprender mucho con Minecraft, pero también hay muchos otros servicios que permiten aprender jugando (While True: Learn, Classcraft, Roblox...). Por desgracia, tan pronto como se incorporan juegos en el aula, se expone a los estudiantes a los mismos riesgos que enfrentarían si jugaran desde casa: trolls, bullying, archivos peligrosos que se hacen pasar por actualizaciones y complementos del juego, etc.

Otro frente que tampoco se puede olvidar proteger son las redes públicas, muy habituales en las universidades, y uno de los grandes vectores de ataque en este tipo de instituciones. Al tratarse de redes que no requieren autenticación para establecer una conexión, el ciberdelincuente puede posicionarse entre el usuario y el punto de conexión y obtener acceso sin restricciones a los dispositivos sin protección que se conecten.

También se pueden utilizar las conexiones Wi-Fi públicas no seguras para distribuir malware. Al compartir archivos a través de una red, el hacker puede introducir fácilmente software infectado en el equipo. En algunos casos, incluso han conseguido piratear el punto de conexión, lo que hace que aparezca una ventana emergente durante el proceso de conexión que ofrece una actualización de un software conocido. Cuando se hace clic en la ventana, se instala el malware.

Comprender los riesgos a los que nos exponemos en todos estos casos y proteger nuestros dispositivos resulta clave, y más en aquellos en los que los usuarios son menores, ya que en muchos casos se comparten los dispositivos móviles (ordenadores, tabletas, móviles) con los hijos, por lo que la información guardada en los mismos (contraseñas, números de tarjeta o incluso información de la empresa) puede también estar en riesgo. ■

GLOBAL KNOWLEGDE

EXPERTOS EN FORMACIÓN VIRTUAL AVANZADA

Descubre nuestros cursos y certificaciones oficiales impartidos por instructores acreditados, de la mano de los principales partners del sector.

¡TE ASESORAMOS!

info.cursos@globalknowledge.es

91 425 06 60

Global Knowledge™

a skillsoft company

ALCATEL-LUCENT ENTERPRISE: creando un mundo donde todo se conecta

Alcatel-Lucent Enterprise es un proveedor de soluciones de red, comunicaciones y nube del mundo que, con modelos de negocio flexibles en la nube, en las instalaciones y en entornos híbridos, ofrece tecnología que conecta todo y a todos.

Desde la compañía se apuesta por nuevas y mejores formas de trabajar juntos, para que las personas se comuniquen y colaboren de forma más eficaz. Todas sus soluciones se adaptan a las necesidades de cada organización, sea cual sea su tamaño, con seguridad integrada y un impacto medioambiental limitado.

PRESENCIA GLOBAL, REPUTACIÓN MUNDIAL

Más de 100 años de innovación han convertido a Alcatel-Lucent Enterprise en un socio para más de 1.000.000 de clientes en todo el mundo. Con sede en Francia y 3.400 partners comerciales en todo el mundo, Alcatel-Lucent Enterprise logra un alcance global efectivo con un enfoque local.

UN MUNDO DE SOLUCIONES INTELIGENTES

Alcatel-Lucent Enterprise proporciona soluciones de redes, comunicaciones y nubes de la

era digital específicas para cada sector, y aplicaciones y servicios para empresas de todos los tamaños en todo el mundo.

Al ofrecer la flexibilidad de la nube, en las instalaciones y en entornos híbridos, los clientes pueden elegir soluciones que se adaptan a sus necesidades y a sus objetivos empresariales.

❖ **Soluciones de comunicaciones de la era digital.** Soluciones de comunicación nativa, abierta, adaptable y duradera con alta escalabilidad y configurabilidad:

➤ Experiencia del usuario de telefonía centrada en la eficiencia, facilidad y productividad en tiempo real.

➤ Soluciones de colaboración flexible (en la nube/en las instalaciones / híbridas) con capacidad para integrar aplicaciones de terceros.

❖ **Soluciones de redes de la era digital.** Las redes autónomas y los flujos de trabajo automatizan las operaciones de red de misión crítica y mejoran la experiencia del usuario. Incorporación, gestión y seguimiento seguros de IoT para ayudar a ampliar la digitalización. Todo ello, con la certificación completa de ISO 9001 e ISO 27001.

❖ **Soluciones específicas por sectores:** La experiencia en los principales sectores y mercados ofrece a la compañía una perspectiva completa sobre lo que necesitan las diferentes empresas y organizaciones para transformar las redes y la comunicación digitales. Por ello, cuentan soluciones particularizadas para los sectores hotelero, de salud, de transporte, educativo o Administraciones Públicas. El objetivo de la firma es ofrecer soluciones tecnológicas que marcan la diferencia, conectando personas, máquinas, entidades y procesos, y creando un futuro más sostenible para todos. ■

MÁS INFORMACIÓN

- Alcatel-Lucent Enterprise
- Triunfar en la nueva forma de trabajar desde cualquier lugar y en todas partes (por IDC)
- Plataforma de comunicaciones Alcatel-Lucent Rainbow
- Arquitectura distribuida de la infraestructura de red de Alcatel-Lucent Enterprise
- SPB para vigilancia por vídeo
- Ciberseguridad en el campus educativo en la era de IoT y del RGPD

Una propuesta para cada necesidad

Son muchos los escenarios a asegurar y, por ello, la propuesta de ESET pasa por ofrecer una solución para cada necesidad. Conozcamos algunas de ellas.

❖ **ESET NOD32 Antivirus.** Se trata de una defensa esencial contra el malware con un mínimo consumo de recursos. Protege de todo tipo de amenazas digitales tales como virus, ransomware, rootkits, gusanos y software espía. También protege de las amenazas más sofisticadas especialmente diseñadas para evitar su detección, y neutraliza los ataques dirigidos y los exploits. Proporciona protección de páginas web ilegítimas que intentan obtener información privada, como datos de usuario y contraseñas.

❖ **ESET Internet Security.** Añade más seguridad para datos y familia. Protege el acceso a la banca online y recupera el control del router Wifi y la webcam. Además, protege a la familia con el Control Parental.

❖ **ESET Smart Security Premium.** La seguridad más completa, diseñada para los usuarios que lo quieren todo. Protege contra el robo de datos en caso de pérdida o robo del USB o el ordenador portátil, y, además, protege de forma remota el historial de navegación.

❖ **Mobile Security.** Seguridad móvil en cualquier parte. Protege el móvil o tablet y la información de

las crecientes amenazas en Android. Asimismo, permite recuperarlo con la función Anti-robo.

❖ **Parental Control.** Protección para los más pequeños y sus actividades online para que puedan disfrutar de una tecnología segura.

❖ **ESET Protect Essential.** Solución de ciberseguridad para la empresa con consola de administración en la nube. Proporciona protección multicapa contra el ransomware, ataques dirigidos y sin archivo. Ofrece seguridad con el mejor equilibrio entre detección, rendimiento y falsos positivos. Garantiza la visión a tiempo real de los endpoints, elaboración de informes y gestión de la protección para todos los sistemas operativos con la consola en la nube ESET Protect.

❖ **ESET Protect Entry.** Solución de ciberseguridad para la empresa con un nivel extra de seguridad: protección para los servidores desde la consola de administración en la nube. Proporciona protección multicapa para dispositivos y servidores contra ataques de ransomware, ataques dirigidos y sin archivo, amenazas avanzadas, ataques de red, botnets, o antispam. Permite la visualización global desde la consola de administración en la nube ESET Protect.

❖ **ESET Protect Advanced.** Solución para un nivel de ciberseguridad empresarial más avanzado con administración basada en la nube. Proporciona protección a la red de equipos y servidores de archivos contra ransomware, amenazas avanzadas y amenazas zero-day. Asegura los datos con el cifrado completo del disco y administra todo de forma fácil desde la consola en la nube ESET Protect.

❖ **ESET Secure Business Cloud.** Solución que busca un alto nivel de protección del servidor de correo y de todos los dispositivos de la empresa con administración basada en la nube. Proporciona protección evitando ataques de red, phishing, malware, ransomware, ataque sin archivo y filtra el spam para evitar el correo no deseado. Elimina las amenazas que se transmiten mediante el correo electrónico al servidor de correo. Avanzada tecnología que combina velocidad, precisión y un bajo consumo de recursos. Permite la personalización y control desde la consola de administración en la nube ESET Protect.

❖ **ESET Protect Complete.** Solución de protección completa para empresa que, además, mantiene seguras las aplicaciones de Microsoft 365 con administración basada en la nube. Proporciona máxima protección para la red de equipos, servidores, correo electrónico no deseado, de las aplicaciones de la empresa en la nube, contra todo tipo de amenazas: ransomware, avanzadas, día cero y malware; también protege tus datos con el cifrado de disco completo y todo administrado desde la consola en la nube ESET Protect.

❖ **ESET Protect Mail Plus.** Solución que protege las comunicaciones por correo electrónico con espacio seguro basado en la nube. Protege la empresa de los ataques de red y ofrece protección

directamente a través del servidor antes de llegar a las cuentas de correo de los usuarios, filtra los mensajes de correo no deseado, además de brindar seguridad frente a las amenazas persistentes avanzadas y amenazas día cero. Todo administrado desde la consola en la nube ESET Protect.

❖ **ESET Cloud Office Security.** Solución de protección avanzada para el correo, sharepoint y almacenamiento de Microsoft 365. Su combinación de filtrado spam, antimalware, antiphishing, escaneo y detección de páginas fraudulentas ayuda a proteger la comunicación, las aplicaciones y almacenamiento de la empresa en la nube además puede inspeccionar los objetos que están en cuarentena. ■

MÁS INFORMACIÓN

RANSOMWARE: Un vistazo al arte criminal de los códigos maliciosos

Tendencias en Ciberseguridad 2021

Una apuesta por el desarrollo de las habilidades que el profesional necesita

Global Knowledge – A Skillsoft Company, es la empresa centrada en la formación tecnológica y TI que ayuda a las personas y organizaciones a desarrollar las habilidades necesarias para triunfar en un mundo en constante cambio y evolución. Fundada en 1995, Global Knowledge cuenta con más de 1.500 empleados en todo el mundo y colabora en el éxito de más de 200.000 profesionales cada año.

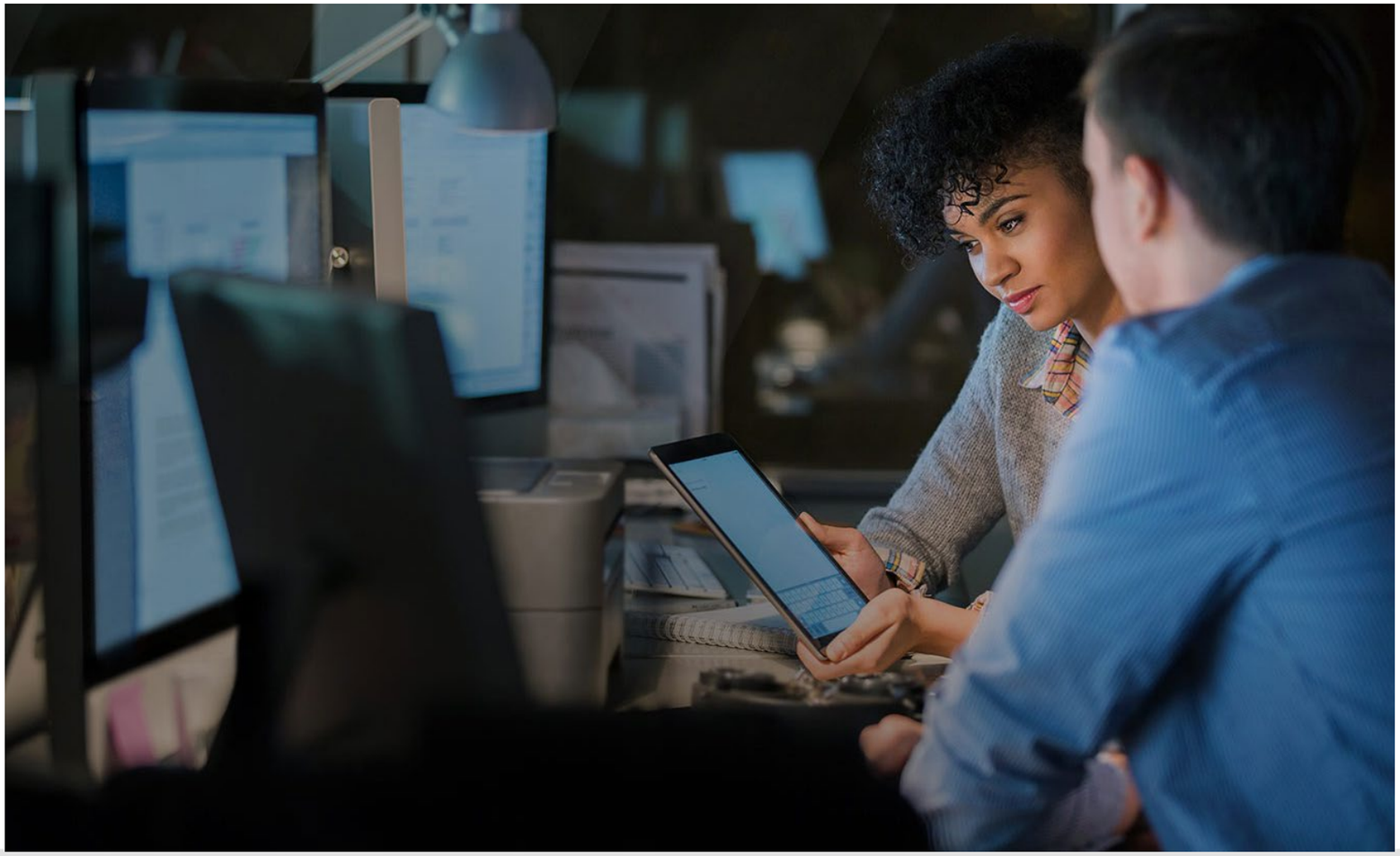
Con una amplia red internacional de oficinas y centros formativos, Global Knowledge dispone de capacidades y recursos para ofrecer una amplia oferta de formación, tanto en modalidad presencial como en formato online y virtual, a través de su red mundial de partners oficiales.

Algunos números que definen a Global Knowledge en la actualidad son:

- Más de 5.000 clases garantizadas al año.
- Más de 3.000 cursos de IT exclusivos.
- Más de 1.100 instructores de prestigio y reconocimiento profesional.
- El nivel de satisfacción general del alumno es de 95%.
- Es partner oficial de formación autorizado de compañías como Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Cisco, Citrix, IBM, ITIL, Red Hat, VMware...
- Cuenta con formación en más de 100 países.

Con una red internacional de oficinas e instalaciones de formación, Global Knowledge tiene la flexibilidad de ofrecer una amplia cartera de cursos, en aulas y a través de una red mundial de socios. Gracias a las diferentes modalidades de formación, Global Knowledge ofrece la posibilidad de formarse:

❖ **Clases presenciales.** Se ofrecen formaciones en persona, impartidas por expertos en la



La firma se centra en ayudar a las organizaciones a construir una fuerza laboral preparada, capacitada y con las destrezas necesarias para los puestos de trabajo del futuro

materia, que ponen lo último en equipamiento y tecnología a disposición del alumno.

❖ **Formato virtual.** El alumno aprovecha las formaciones con instructor en directo y le permite participar durante la sesión e interaccionar con el resto de asistentes de manera telemática.

❖ **Cursos on demand.** Se puede acceder de la forma más flexible a los vídeos formativos y actividades cualquier día, a cualquier hora, y en cualquier lugar, adaptándose a los horarios y necesidades de cada alumno.

Global Knowledge facilita los recursos necesarios para formar a todos los perfiles profesionales del sector tecnológico, y proporcionando soluciones de aprendizaje innovadoras y flexibles que preparan para el éxito. Todo ello, impulsado por el alto nivel de calidad que se impone en la compañía, manteniendo rigurosos estándares internos, para que el alumno reciba una experiencia de formación única y excepcional en todo momento.

Además, en junio de 2021, Global Knowledge se fusiona con Skillsoft para salir a bolsa y convertirse en empresa pública en Estados Unidos, creando así una empresa de formación corporativa con un amplio alcance global, para servir a, aproximadamente el 70 % de los clientes de la lista Fortune 1000, en más de 160 países y con más de 45 millones de estudiantes a nivel mundial. De esta manera, Skillsoft se posiciona como una de las empresas de digital learning más grandes de la industria, enfocada en ayudar a las organizaciones a construir una fuerza laboral preparada, capacitada y con las destrezas necesarias para los puestos de trabajo del futuro. ■

MÁS INFORMACIÓN

- Calendario de cursos
- Cursos garantizados
- Actualidad de Global Knowledge
- Salary Report 2020

La educación, uno de los sectores más afectados por el ransomware.

Sophos Endpoint

Intercept X

Bloquee los ataques de ransomware antes de que causen estragos en su entorno con tecnología antiransomware que detecta procesos de cifrado malicioso y los neutraliza antes de que puedan propagarse por la red.

sophos.com/es-es/endpoint

SOPHOS
Cybersecurity evolved.

21-09-20 ES(DD)

Una visión 360 de la seguridad

WatchGuard Technologies es una multinacional con 25 años de experiencia en el desarrollo de tecnología para el sector de la ciberseguridad. Cuenta con una oferta que combina tanto hardware como software, permitiendo crear un escudo de defensa en las organizaciones gracias a una propuesta integral que abarca desde la seguridad de red hasta la protección avanzada para el endpoint e inteligencia de red, así como la seguridad Wi-Fi y autenticación multifactor (MFA).

El objetivo de WatchGuard es hacer que la seguridad de nivel empresarial sea accesible a las organizaciones de todos los sectores y tamaños, a través de la simplicidad, ofreciendo seguridad inteligente y eficaz bajo la fórmula de soluciones fáciles de desplegar y gestionar.

Con 7 centros de operaciones y presencia directa en 21 países, WatchGuard permite a más de 250.000 clientes de todo el mundo proteger sus activos más importantes.

La compañía cuenta con un catálogo de soluciones que abarca desde los servicios de seguridad de red tradicionales hasta los más innovadores como protección contra malware avanzado, ransomware y pérdida de datos confidenciales, o servicios Zero-Trust.

El objetivo de WatchGuard es hacer que la seguridad de nivel empresarial sea accesible a las organizaciones de todos los sectores y tamaños, a través de la simplicidad, ofreciendo seguridad inteligente y eficaz bajo la fórmula de soluciones fáciles de desplegar y gestionar

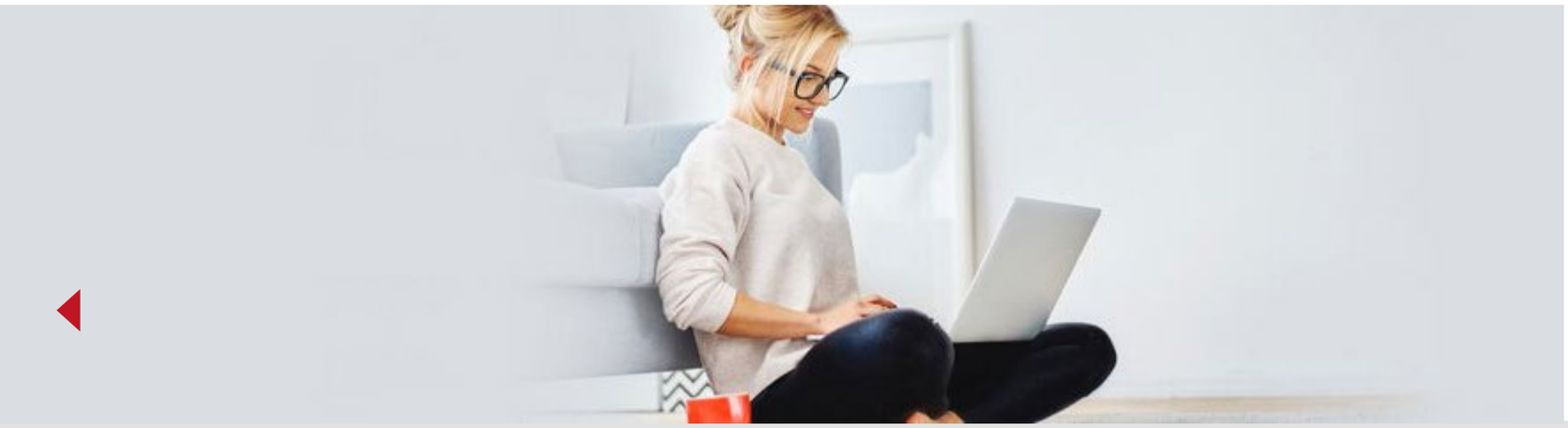
Por áreas, su propuesta se estructura de la siguiente manera:

❖ **Seguridad de red:** todos los servicios de seguridad de WatchGuard se ofrecen como una solución integrada en un dispositivo Firebox, tanto en entornos físicos como virtuales. Los Firebox destacan por su escalabilidad y están preparados para brindar el abanico completo de servicios de seguridad, junto con un conjunto de herramientas de visibilidad y gestión que permiten estar un paso por delante del panorama de amenazas.

❖ **Wi-Fi seguro con gestión en cloud:** con Secure Wi-Fi ofrecen conectividad Wi-Fi y seguridad patentada. Implementando un punto de acceso WatchGuard con Wi-Fi Cloud habilitado y una licencia de Secure Wi-Fi o Total Wi-Fi, se despliega todo el potencial de los puntos de acceso WatchGuard mediante un Sistema de Prevención de Intrusiones Inalámbricas (WIPS). Asimismo, WIPS garantiza la protección que cada usuario necesita, defiende el espacio aéreo 24x7 contra equipos no autorizados, ataques MitM y DoS, AP no autorizados y el resto de amenazas que acechan a los entornos Wi-Fi.

❖ **Protección de identidades:** la solución de MFA, AuthPoint, aporta la seguridad necesaria para proteger activos, cuentas e información, permitiendo que las empresas y sus trabajadores accedan de forma segura y sin preocupaciones a las aplicaciones corporativas desde cualquier lugar. Sencilla de manejar, se administra de forma centralizada desde WatchGuard Cloud.

❖ **Seguridad endpoint:** WatchGuard Endpoint Security ofrece las tecnologías necesarias para detener los ciberataques avanzados a los endpoints, incluyendo antivirus de nueva generación en la plataforma de protección de endpoints (EPP), detección y respuesta de endpoints (EDR) y soluciones de filtrado DNS. La solución insignia EPDR brinda protección EPP y EDR completa, así como servicios de búsqueda de amenazas o threat hunting y aplicaciones zero-trust, suministrados a través de un único agente ligero y gestionados desde una única plataforma cloud. ■



MÁS INFORMACIÓN

- WatchGuard Endpoint Security
- WatchGuard Total Security: Suscripciones a UTM
- MFA Poderosamente Sencilla

SOPHOS: Nuevas tendencias para potenciar la seguridad

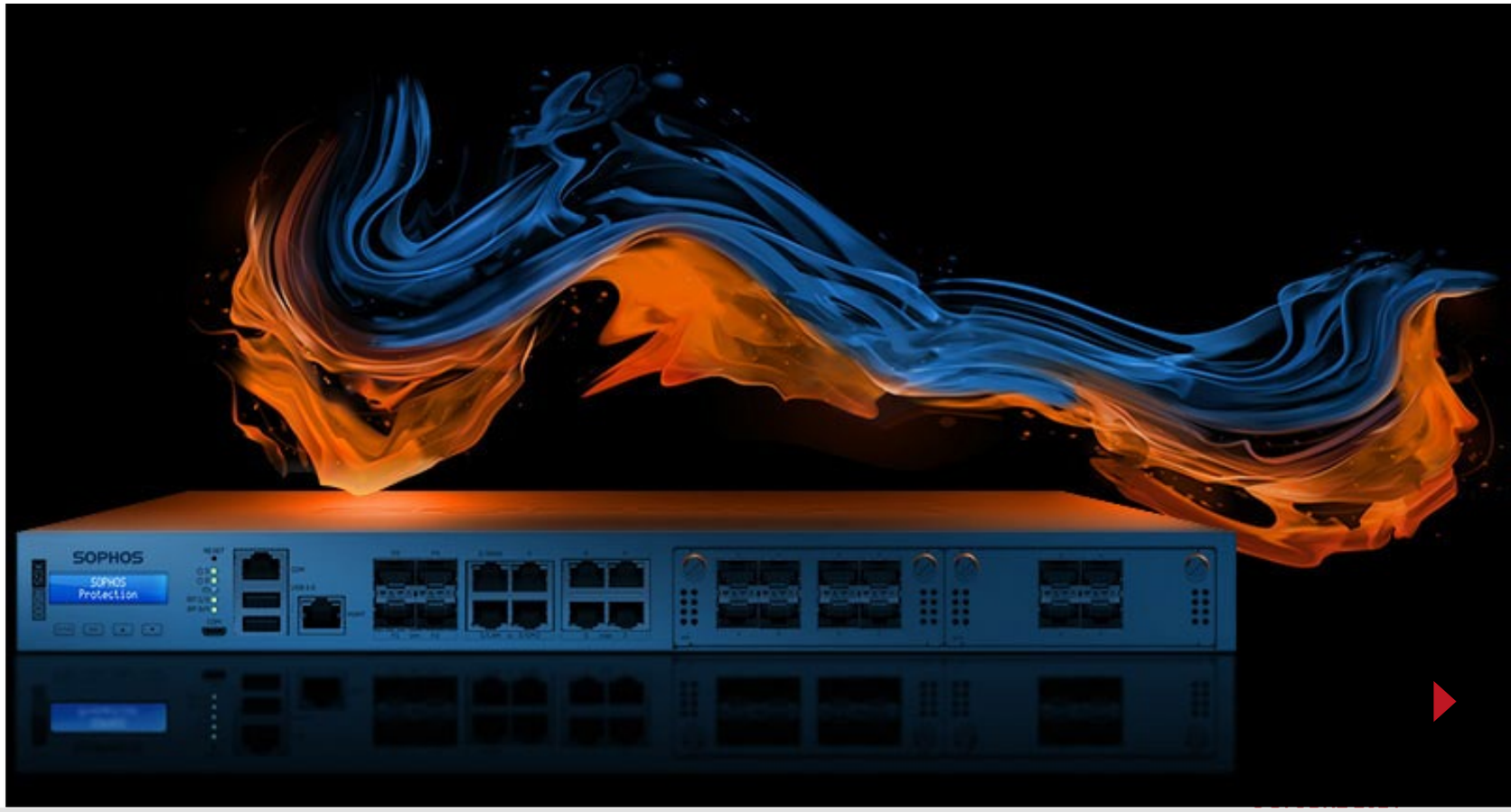
Impulsada por la threat intelligence, IA y machine learning de SophosLabs y SophosAI, Sophos ofrece un catálogo de productos y servicios avanzados para proteger a los usuarios, las redes y los endpoints contra el ransomware, malware, exploits, phishing y la amplia gama de ciberataques.

Sophos proporciona una única consola cloud de gestión integrada, Sophos Central, como pieza central de un ecosistema de ciberseguridad adaptativo que cuenta con un data lake centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, partners, desarrolladores y otros fabricantes de ciberseguridad.

La firma vende sus productos y servicios a través de partners resellers y managed service providers (MSP) en todo el mundo, unas soluciones entre las que destacan:

❖ **Sophos Inercept X EDR/XDR.** Un sistema de protección endpoint que engloba la protección tradicional (firmas), junto con protección "next-gen" (Inteligencia Artificial, anti exploit, comportamiento, anti ransomware y anti-hacking) así como protecciones complementarias (control web, control de aplicaciones, cifrado, DLP...) y, por supuesto, EDR o, a día de hoy, XDR, gracias a la integración cruzada de datos con nuestros firewalls y sistemas de protección cloud. Su gestión se realiza a través de Sophos Central, lo que permite la interacción con otros productos de Sophos y gracias a su API, con cualquier fabricante.

❖ **Sophos MTR, MTR-E y Rapid Response.** Se trata de un servicio gestionado de Respuesta frente a Amenazas, que ofrece a las

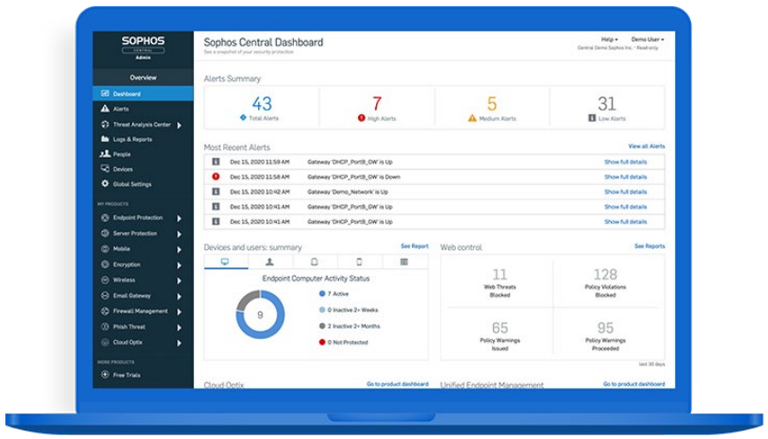


Sophos proporciona una única consola cloud de gestión integrada, Sophos Central, como pieza central de un ecosistema de ciberseguridad adaptativo que cuenta con un data lake centralizado que aprovecha un amplio conjunto de API abiertas

empresas funciones de búsqueda, detección y respuesta ante posibles amenazas 24/7. Formado por un equipo de detección de amenazas y profesionales expertos en dar respuesta, tomando medidas para neutralizar incluso las amenazas más sofisticadas. Sophos puede dar respuesta, apoyándose en el agente de Sophos para realizar las acciones oportunas para la detección y mitigación de la amenaza. Cualquier empresa que sufra un ataque activo puede recurrir a Sophos Rapid Response: un despliegue de productos y un equipo de expertos capaces de ver cuál es la situación dentro de la compañía, detener el ataque, si es posible, y detectar cómo ha venido, a quién ha afectado y limpiar para que pueda operar lo antes posible.

❖ **Sophos Firewall.** La seguridad de red desde la compra de Astaro en 2008 por Sophos ha seguido evolucionando hasta llegar a los modernos Sophos Firewall, gestionados de forma centralizada desde Sophos Central, integrándose con el Endpoint y servicios como MTR así como hidratando el lago de datos para permitir detectar, englobándose dentro de su estrategia XDR. La arquitectura de Xstream de Sophos Firewall protege la red de las amenazas más recientes al tiempo que acelera el tráfico importante de SaaS, SD-WAN y aplicaciones en la nube.

❖ **Sophos Email.** Seguridad del correo electrónico más inteligente con IA. Las actuales amenazas para el correo electrónico evolucionan rápidamente, y las empresas en expansión necesitan una seguridad predictiva para el email, es decir, que combata las amenazas de hoy día sin perder de vista el mañana.

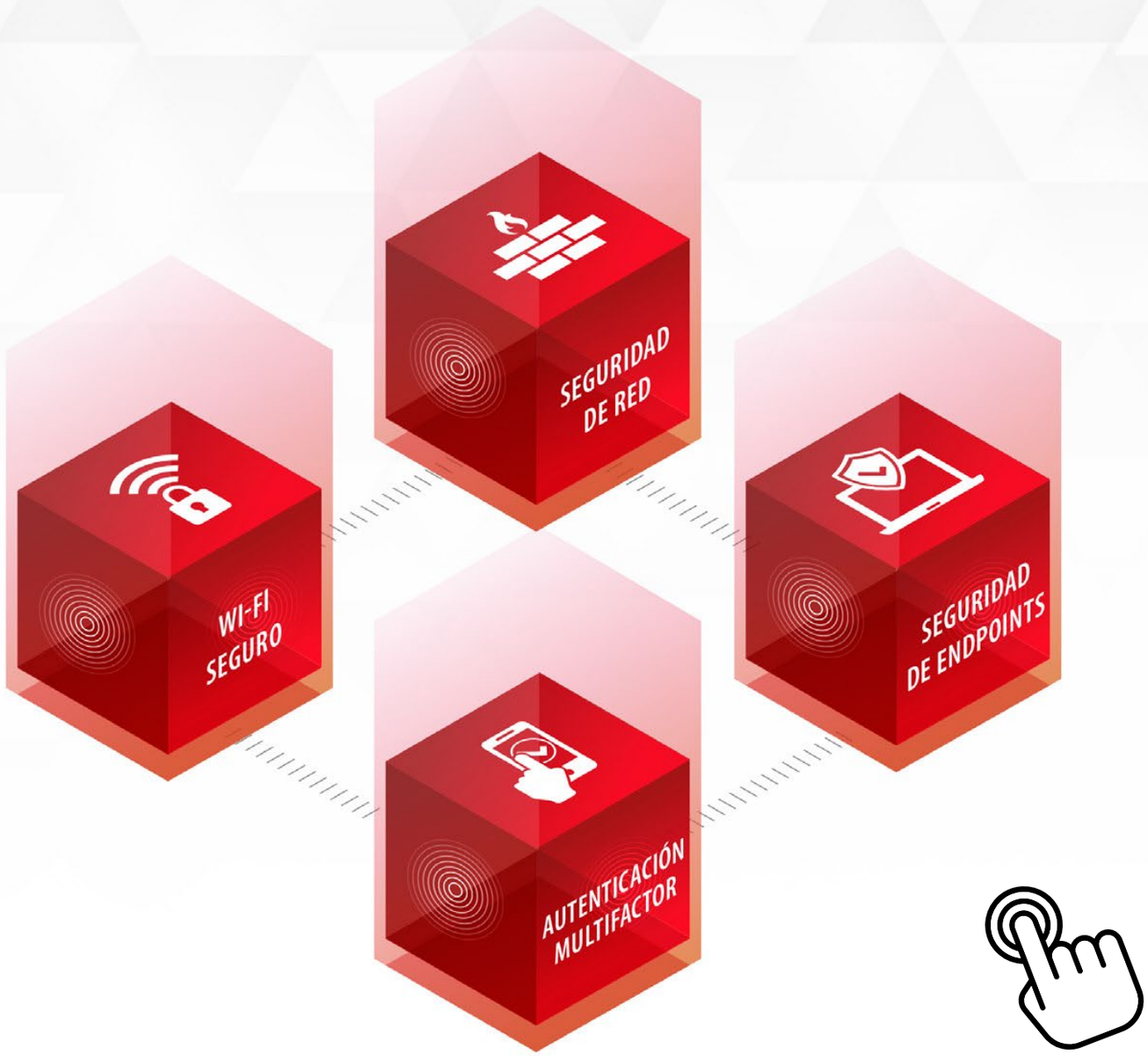


❖ **Sophos Cloud Optix**. Conscientes de que la TI está migrando a la nube, Sophos empezó a hablar de CSWP y CSPM, gracias tanto al agente para servidores como a Cloud Optix, el cual audita los recursos que tengamos sobre proveedores de nube pública como AWS, Azure, Google Cloud o Kubernetes tanto en cualquiera de estos entornos como locales. Además, se integra tanto con la protección de instancias y servicios como MTR, lo que proporciona más visibilidad e información que será recogida en el DataLake. ■

MÁS INFORMACIÓN

- El estado del Ransoware
- El estado del Ransoware en Educación
- Sophos XG Firewall para la educación

SMART SECURITY, SIMPLY DONE.



SEGURIDAD DE RED • AUTENTICACIÓN MULTIFACTOR • WI-FI SEGURO • SEGURIDAD DE ENDPOINTS

900 90 70 80

spain@watchguard.com

PROTECCIÓN INTELIGENTE

Múltiples servicios trabajan juntos de manera inteligente para prevenir, detectar y responder instantáneamente a los ciberataques con políticas automatizadas, así como supervisar e informar sobre el estado de tu infraestructura de TI.

VISIBILIDAD ACCIONABLE

Las herramientas de visibilidad accionable te permiten identificar amenazas de manera proactiva, al tiempo que proporcionan acciones correctivas contra los problemas conocidos.

GESTIÓN SIMPLIFICADA

Nuestra plataforma de gestión basada en la nube despliega, configura y mantiene tu seguridad de forma rápida y sencilla en múltiples productos de seguridad, empresas y sitios.

PIONEROS EN CIBERSEGURIDAD DURANTE 25 AÑOS.

25 ANNIVERSARY WatchGuard®

THE ART OF CYBERSECURITY

Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

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

Más información en:
www.trendmicro.com

it TRENDS

OCTUBRE 2021

La interconexión omnipresente

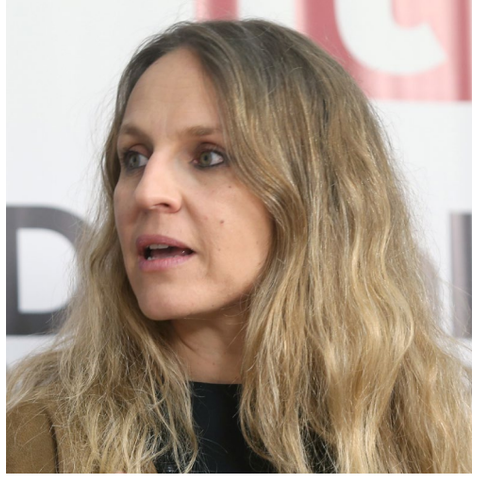
UNA PUBLICACIÓN DE it Digital MEDIA GROUP

it TRENDS

it Digital MEDIA GROUP

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es
Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es
Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es
Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es
Directora de IT Digital Security
Rosalía Arroyo rosalia.arroyo@itdmgroup.es
Director de IT User e IT Reseller
Pablo García pablo.garcia@itdmgroup.es
Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es
Redacción y colaboradores Ricardo Gómez, Alberto Varet, Hilda Gómez, Arantxa Herranz, Reyes Alonso
Diseño revistas digitales Eva Herrero
Producción audiovisual Favorit Comunicación, Alberto Varet
Fotografía Ania Lewandowska
Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

La interconexión omnipresente



Si ya antes de la pandemia, hogares y oficinas estaban repletos de tecnología y servicios digitales que exigen conectividad, ahora que se ha intensificado el teletrabajo y se están fomentando servicios que requieren de conexión (en educación, en sanidad, en bienestar…), imaginemos cómo se ha disparado la demanda de interconexión. Solo decir que el número de usuarios de 5G se multiplicará casi por 1.000 en los próximos 5 años…

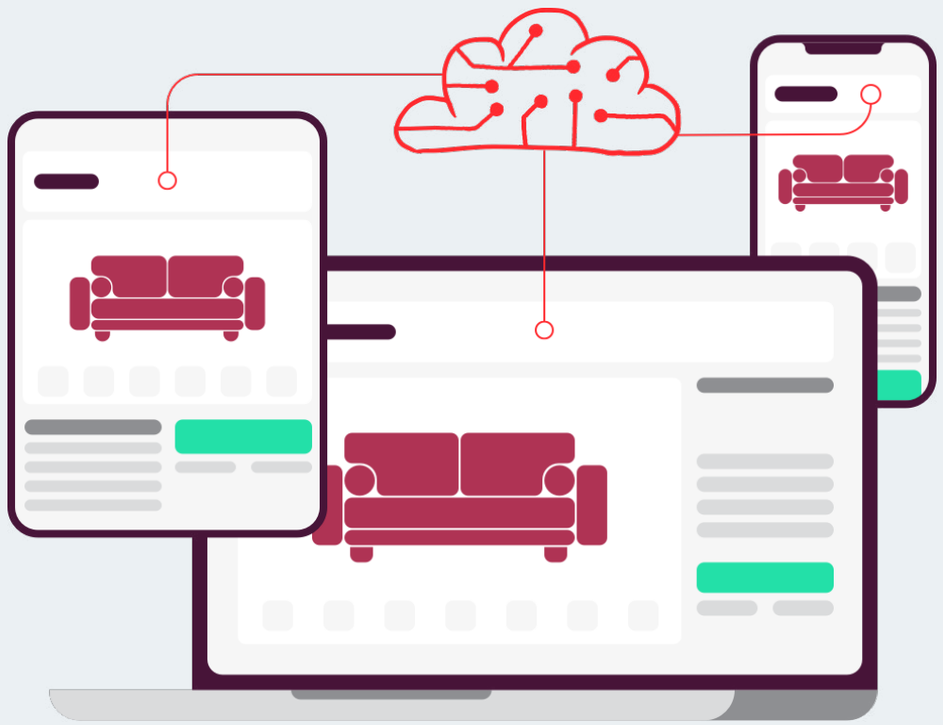
Personas, objetos y máquinas están siempre conectados para que fluya la información rápida y automáticamente, para que pueda ser accedida e intercambiada desde cualquier localización, en cualquier momento, entre múltiples dispositivos e interfaces. Las tecnologías de conexión están evolucionando rápidamente para dar respuesta a esta necesidad de conexión global para la que tienen que prepararse las empresas. Wi-Fi 6, SD-WAN, 5G, IoT y los requisitos de seguridad que estas tecnologías plantean, protagonizan este número de IT Trends. Para analizar su situación, realizamos un #EncuentroITTrends en el que reunimos a portavoces de **A10 Networks, Akamai, Aruba, Check Point, Citrix, y Sophos** que denominamos Conectando y entendiendo a la empresa sin fronteras.

También en este número prestamos atención a la experiencia de cliente, en un especial en el que te contamos las últimas tendencias para proporcionar un mejor servicio a los usuarios, ejemplificado con el caso de uso de Playasol Ibiza Hotels y con la propuesta tecnológica de **Fastly**.

Este último trimestre se presenta apasionante e intenso. Seguimos trabajando en nuestro informe sobre el estado de la nube. Ayúdanos a conocerlo contestando a nuestra Encuesta IT Trends. Analizaremos también las tendencias tecnológicas que impactarán en la empresa en 2022 y, de forma particular, aquellas de seguridad que están por venir. Regístrate ya en estos Encuentros y ve preparando tu TI.

¡Gracias por leernos!

fastly



Las experiencias de compra más rápidas, personalizadas y seguras se encuentran en el edge

Fastly ayuda a las empresas minoristas online más seguras —como Shopify, Ticketmaster y Etsy— a superar las expectativas de los clientes ofreciéndoles experiencias digitales seguras y de alto rendimiento a escala.

Descubre más en:

fastly.com/es/solutions/retail/

it TRENDS

La computación neuromórfica

evoluciona para dar respuesta a los desafíos del futuro

En la próxima década, el sector industrial, el de automoción y el gran consumo impulsarán la expansión de la computación neuromórfica, una tecnología disruptiva que adopta diversas formas. Según los expertos, su mercado tardará varios años en coger impulso, pero su crecimiento se acelerará entre 2025 y 2030, alcanzando un valor de más de 2.000 millones de dólares para final de este período. Pero, además, beneficiará a otros mercados vinculados, desde los sensores inteligentes a las redes IoT industriales y los dispositivos de consumo dotados de inteligencia.

La computación neuromórfica es una de las tecnologías con más potencial transformador en el campo de la inteligencia artificial, ya que proporciona nuevas capacidades en arquitecturas tecnológicas altamente distribuidas que generan y consumen gran cantidad de datos. Por ejemplo, en los despliegues de IoT de uso industrial, en las fábricas altamente robotizadas, en las telecomunicaciones 5G o en plataformas de realidad aumentada y otros entornos tecnológicos de última generación.

En un reciente estudio realizado por Yole Développement, Adrien Sánchez, analista de mercado y tecnología, división de informática y software, explica que "la IA está hambrienta de rendimiento y la dinámica de la ley de Moore no será suficiente para cubrir las necesidades de la revolución 5G/IoT/AR/robótica que está en curso". Por ello, cree que la industria tecnológica necesita algo más de tiempo para seguir centrándose en la investigación y desarrollo de nuevas tecnologías capaces de dar respuesta a los desafíos del futuro, algo que se demorará de tres a cinco años.

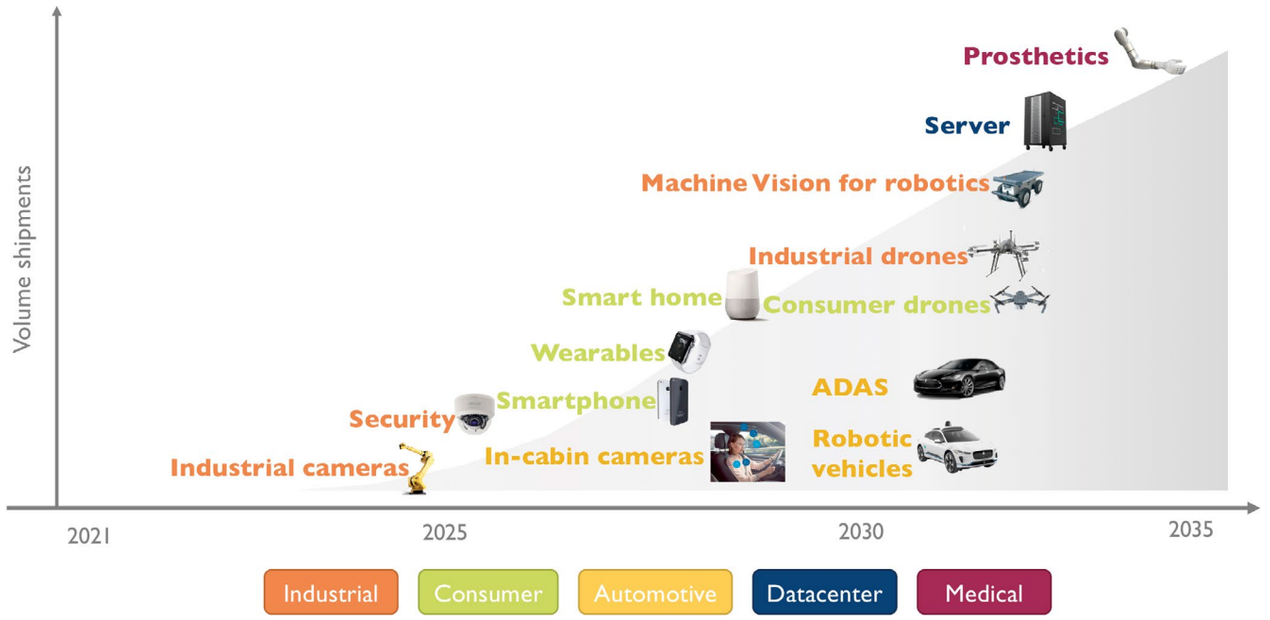
Afirma que "actualmente se está utilizando la fuerza bruta para aprovechar el poder de la inteligencia artificial, pero este enfoque no es escalable. Chocará con un muro de calor, un muro de datos y un muro de costos relacionado con la capacidad de la industria de semiconductores para entregar a un cierto ritmo, con la ley de Moore y con el coste incremental para lograr mejoras de rendimiento". Esto implica que la inteligencia artificial, tal y como se entiende actualmente, no servirá en el futuro, y hacen falta nuevos enfoques.

Para los expertos de Yole, la clave está en la computación neuromórfica, cuyos fundamentos se basan en arquitecturas de tecnología inteligente distribuida, que tratan de imitar el comportamiento eficiente del cerebro humano. Así, a modo de neuronas independientes que trabajan de forma colaborativa, un ecosistema más amplio de dispositivos o nodos de IA más pequeños pueden lograr resultados mejores y con más rapidez y eficacia que grandes megaestructuras de TI diseñadas para ejecutar una gran IA centralizada.

Los expertos creen que estas tecnologías serán capaces de resolver los problemas actuales y futuros en muchos campos de aplicación

Neuromorphic technologies - Adoption process between 2021 and 2035

(Source: Neuromorphic Computing and Sensing 2021 report, Yole Développement, 2021)



de la IA, especialmente en los más exigentes. Por ello, esperan que para el año 2035 la computación neuromórfica representará el 20% de toda la informática vinculada a la inteligencia artificial. Sus estimaciones son que el mercado de computación neuromórfica crecerá a una CAGR del 88% entre 2025 y 2030, alcanzando unos 2.000 millones de dólares para final del período. Pero esto no abarcará el total, ya que mercados como el de sensores neuromórficos crecerá todavía más, aumentando a una CAGR del 116% en esos años, llegando a un valor de unos 5.000 millones de dólares para 2030.

Esto generará nuevas oportunidades en varios mercados vinculados a la informática computacional, pero también a las redes y a todo el vasto ecosistema de dispositivos que se está desarrollando en torno a la informática personal, las diferentes ramas de Internet of Things y las telecomunicaciones de nueva generación. Pero, en general, los tres sectores que más rápido adoptarán tecnologías neuromórficas serán el industrial, el de consumo y el automotriz.

INDUSTRIA MÁS ALLÁ DE LA IA CONVENCIONAL

Para los analistas responsables de esta investigación, las aplicaciones industriales serán la punta de lanza de la expansión de tecnologías de computación neuromórfica, ya que en estos entornos se buscan capacidades de procesamiento de grandes cantidades de datos a alta velocidad y baja latencia, para su aplicación en el aprendizaje profundo en el contexto de una TI distribuida.

Así, en la próxima década diferentes industrias van a adoptar las nuevas tecnologías de inteligencia artificial distribuida que tratan de imitar las capacidades humanas. Por ejemplo, para desarrollar estrategias de fabricación inteligente que permitan mejorar los productos y abaratar costes, aplicando IA en todas las etapas, desde el diseño al producto final, aprovechando los datos que se generan en cada uno de los procesos. También en las telecomunicaciones, en la logística, en la cadena de suministro y en otras industrias que están viendo cómo la digitalización obliga a trabajar con grandes cantidades de datos.

Actualmente se está utilizando la fuerza bruta para aprovechar el poder de la inteligencia artificial, pero este enfoque no es escalable

Porque es vital extraer el conocimiento verdaderamente valioso de toda la información que se genera en las operaciones internas y en las interacciones con socios y clientes. La IA actual ofrece soluciones, pero la gran avalancha de datos que no para de llegar requiere soluciones más eficaces, ágiles y rentables, y la computación neuromórfica promete ser el mejor camino a seguir. Como resultado, para el año 2030 los analistas

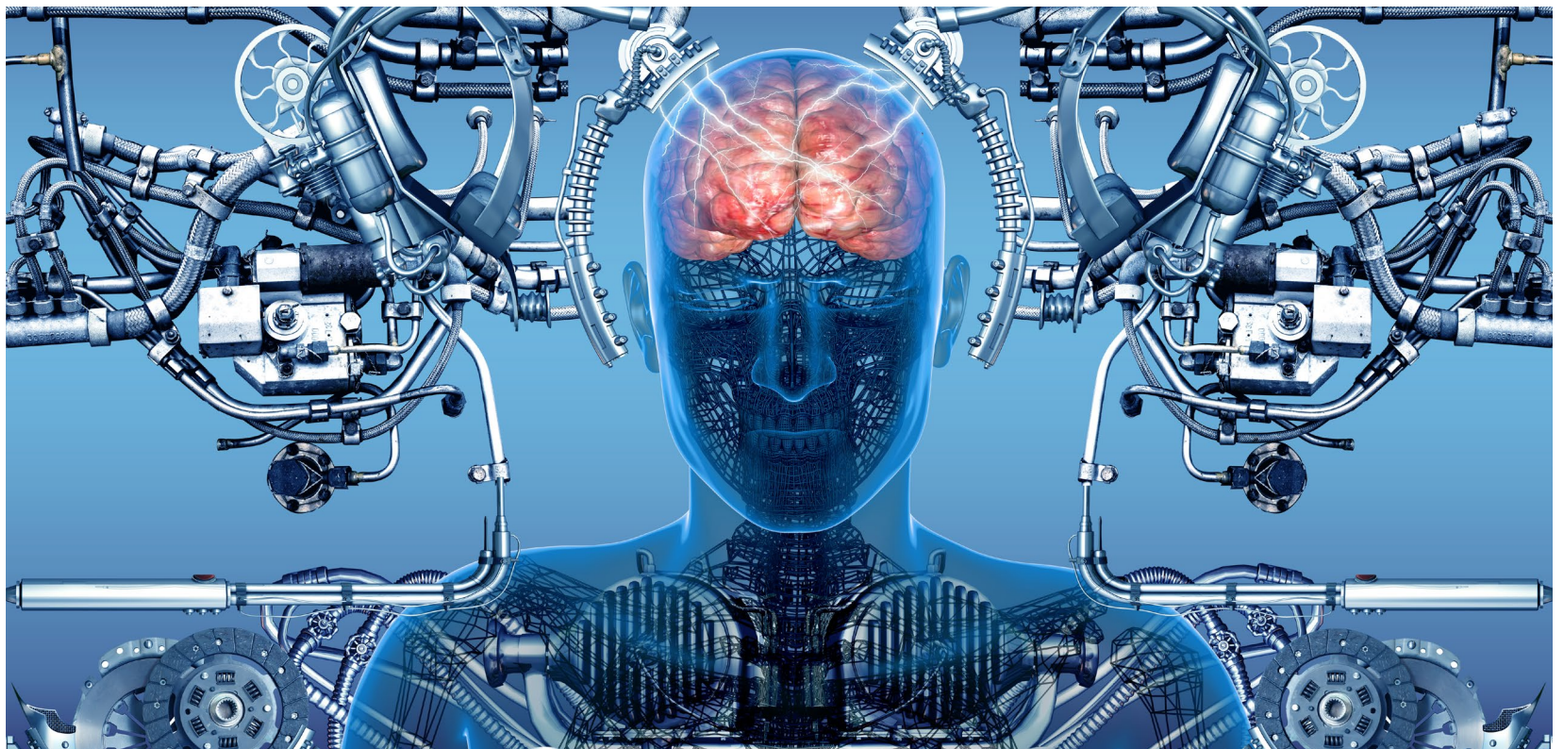
de Yole esperan que el mercado de neuromorfos para aplicaciones industriales alcance un valor de 2.000 millones de dólares, aunque combinando la computación y los sistemas de detección, como sensores inteligentes.

DISPOSITIVOS PERSONALES DOTADOS DE IA

Otro entorno donde la computación neuromórfica va a desarrollarse con cierta rapidez es en la informática personal, donde conviven los smartphones, los wearables y los dispositivos inteligentes para el hogar digital. Así, los expertos creen que la informática personal experimentará un gran salto evolutivo en la próxima década, gracias a los avances en la computación neuromórfica. Este se verá impulsado por la expansión del ecosistema del hogar digital, por el consumo cada vez mayor de servicios en movilidad y por la necesidad de garantizar la seguridad de los datos que generan y almacenan los dispositivos personales.

Como explica Simone Bertolazzi, analista senior de tecnología y mercado, en Yole, "las arquitecturas de dispositivos neuromórficos actuales también pueden variar significativamente con respecto a la organización de la memoria y los componentes informáticos en los chips de silicio". En su opinión, se van a producir importantes avances en el campo de los dispositivos de uso personal y otros conceptos de IoT con aplicaciones profesionales, especialmente en las tecnologías de computación y de memoria integrada.

El objetivo de los líderes en investigación dentro de campos como la memoria computacional es lograr tecnologías de memoria que puedan comportarse de forma similar a como lo hacen las neuronas, permitiendo que los chips no solo almacenen la información, sino que la procesen aplicando capacidades de IA limitadas, que se amplían al integrarse en una red de dispositivos más amplio, formando un ecosistema de computación neuromórfica. Estos trabajos no se centran únicamente en los dispositivos de uso personal, pero gracias a estos y otros avances, los expertos de Yole creen que para el año 2030 las aplicaciones móviles y otras tecnologías de consumo basadas en computación neuromórfica alcancen un valor de mercado de 2.800 millones de dólares.



CONDUCCIÓN MÁS INTELIGENTE

Las capacidades de la computación neuromórfica también tendrán importantes aplicaciones en el campo de la automoción, como explica Pierre Cambou, analista principal de la división de fotónica y detección de Yole. Afirma que "en el mercado automotriz, una gran cantidad de aplicaciones se beneficiarán de la baja latencia y el bajo consu-

Los tres sectores que más rápido adoptarán tecnologías neuromórficas serán el industrial, el de consumo y el automotriz

mo de energía de las tecnologías neuromórficas" aunque cree que la adopción de estas innovaciones en la industria de automoción va a demorarse un poco más que en los casos anteriores, el beneficio potencial de usar estas tecnologías en el sector es, como mínimo, el mismo.

Por ahora, las barreras de adopción en el sector están vinculadas a la seguridad vial, la protección de datos y, en gran medida, a que todavía no está claro el modelo de rentabilización de la conducción autónoma. Dotar a los vehículos de capacidades tan avanzadas implica un gran coste, que la mayoría de los usuarios finales no puede pagar actualmente. Por ello, la industria necesita avanzar en varios caminos simultáneamente, desarrollando la tecnología y el modelo de negocio que la haga sostenible.

En cualquier caso, los expertos están convencidos de que la computación neuromórfica proporcionará las mejores soluciones para dotar de una mayor inteligencia a los vehículos, con un coste mucho más asumible que otras alternativas de IA a bordo que se han propuesto. Y también más eficaz y seguro que una conducción autónoma excesivamente dependiente de la conectividad con infraestructura TI y servicios digitales externos. Como resultado, y teniendo en cuenta las previsiones de evolución de coches autónomos para finales de esta década, las previsiones de los analistas de Yole son que para el año 2030 la computación neuromórfica para la automoción representará un mercado de unos 2.000 millones de dólares. ■

OTRAS APLICACIONES PARA LA COMPUTACIÓN NEUROMÓRFICA

Los tres campos anteriores serán los que más contribuirán a la expansión de las nuevas formas de inteligencia artificial distribuida, pero esta encontrará aplicaciones en otras áreas tecnológicas. Los expertos de Yole destacan que el mercado de servidores podría beneficiarse de esta tecnología, aprovechando la baja latencia y el aprendizaje en línea para mejorar el rendimiento de aplicaciones como las de ciberseguridad o para su uso en la detección de fraudes.

Además, su gran eficacia podría servir para reducir el consumo de energía en los centros de datos, delegando tareas vinculadas a la IA a sistemas distribuidos basados en computación neuromórfica, que pueden realizar tareas complejas con menos gasto de electricidad. Como ejemplo, mencionan el desarrollo de servidores neuromórficos que están llevando a cabo grandes firmas como Intel e IBM, ensamblando de forma masiva sus respectivas plataformas Loihi y TrueNorth.

Por otro lado, el informe destaca la gran cantidad de instituciones académicas que están trabajando en el desarrollo de diversas formas de computación neuromórfica, tanto universidades de prestigio como grandes laboratorios de investigación públicos y privados, que además cuentan con la contribución de empresas tecnológicas de primer nivel, interesadas en el desarrollo de infraestructuras de IA perimetral para las tres principales aplicaciones actuales de la computación neuromórfica (industriales, automotrices y de consumo).

MÁS INFORMACIÓN

- Yole Dévelopment. Computación y sensores neuromórficos. 2021
- Loihi 2: A New Generation of Neuromorphic Computing
- NIST. Computación Neuromórfica
- Introducción a la Computación Neuromórfica. Visión y retos

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN	PREVENCIÓN
ESET Threat Intelligence ESET Virus Radar WeLive Security	Endpoint Protection Platform ESET Mail Security ESET Sharepoint Security ESET Secure Authentication ESET Endpoint Encryption ESET PROTECT
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET PROTECT	Endpoint Protection Platform ESET Dynamic Threat Defense ESET Enterprise Inspector ESET Mail Security ESET Secure SharePoint Server ESET Secure Authentication ESET Endpoint Encryption ESET PROTECT
RESPUESTA	**DETECCIÓN**

CYBERSECURITY EXPERTS ON YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

it TRENDS

SEPTIEMBRE 2021

CUSTOMER EXPERIENCE

Territorio digital

UNA PUBLICACIÓN DE it Digital MEDIA GROUP

Patrocinador fastly

Nuevas demandas que redefinen la estrategia de CX

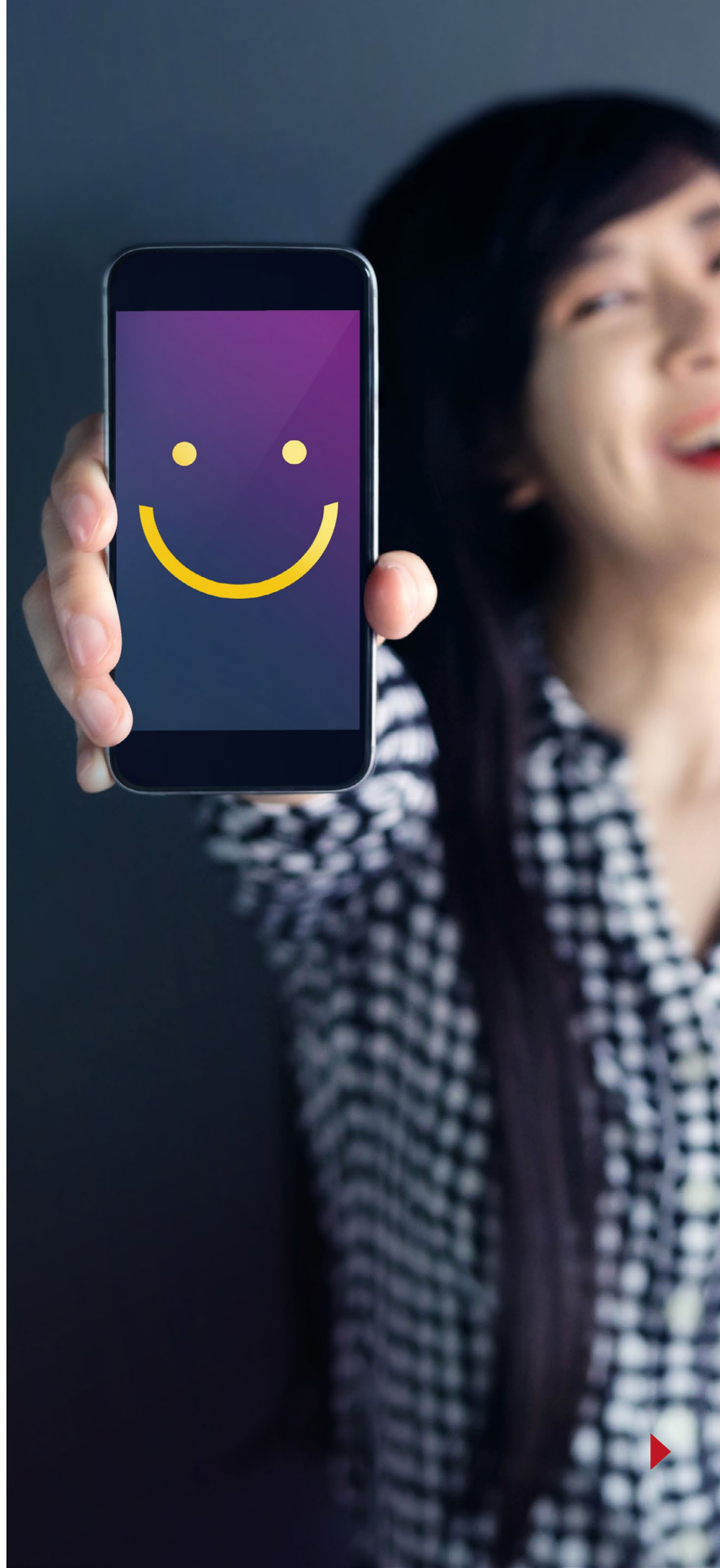
La pandemia ha sido el motor de las nuevas tendencias de consumo que ya están modificando la forma en que los clientes pretenden interactuar con las marcas. A medida que nos encaminamos hacia 2022 y consideramos la perspectiva de un mundo pos-COVID-19, las compañías deben replantearse su experiencia de cliente (CX) para estar preparadas para la ansiada nueva normalidad.

Independientemente de la solidez de sus productos o servicios, las empresas se enfrentan a una nueva realidad. Tal y como se desprende del estudio de Tendencias de CX 2021 de Sitel, ahora los consumidores basan sus expectativas de experiencia de cliente y califican el servicio que reciben tomando como referencia la mejor experiencia que han tenido con cualquier marca, independientemente del segmento en el que operan las compañías. Además, el tipo de experiencia de cliente con el que se comparan todos los demás es cada vez más digital, omnicanal y personalizado.

Estar a la altura de estas expectativas cambiantes es un auténtico reto para todas las compañías, a lo que hay que añadir el impacto y las repercusiones de la COVID-19, que ha intensificado la presión para que las empresas piensen de forma diferente y actúen de manera digital con el objetivo de mantener o, incluso, incrementar su comunidad de clientes, asegurando el futuro del negocio. Lo que en la práctica supone que, independientemente del sector al que pertenezca y del mercado al que se dirija, toda compañía tiene que reescribir las reglas que gestionan la experiencia de cliente.

UNA EXPERIENCIA QUE SE MANTENDRÁ DIGITAL

Tal y como se desprende del citado informe de Tendencias CX de Sitel, si bien el 76% de los consumidores se vieron empujados inicialmente



Las compañías están obligadas a incrementar más que nunca su apuesta por CX (Customer eXperience) para atraer y retener clientes e incentivar su lealtad

hacia las interacciones digitales con las marcas debido a las restricciones relacionadas con la COVID-19, el 57% de ellos mantendrá este comportamiento porque aprecia el valor extra que les ofrece. Este valor extra nace de una mayor rapidez y simplicidad, además del acceso inmediato al autoservicio o la posibilidad de elegir entre diferentes opciones de comunicación (desde chatbots y correo electrónico, hasta el chat en vivo), elementos que solo puede ofrecer un enfoque de CX omnicanal centrado en lo digital.

Según McKinsey, la respuesta de las marcas a la pandemia por la COVID-19 ha adelantado hasta siete años la digitalización de las interacciones con los clientes y la cadena de suministro. Las organizaciones que ya contaban con una presencia digital avanzada poseían una ventaja inicial, pero han sido las empresas que supieron moverse rápidamente para entender dónde encajaban mejor las soluciones digitales para crear experiencias innovadoras y sin contacto las que han creado las conexiones de marca más fuertes.

Esta realidad impuesta por la pandemia, ha dejado en evidencia las deficiencias que presentaban las estrategias de un alto número de compañías. Según una reciente investigación de Salesforce, el 88% de los equipos de servicio admitieron que la pandemia había dejado al descubierto las carencias de su tecnología. Por este motivo, las compañías tienen que redoblar los esfuerzos para cerrar las brechas y atender a sus clientes en los canales digitales, lo que puede suponer para muchas de ellas acelerar su actual proceso de Transformación Digital.

AUTOSERVICIO: UN PASO EN LA BUENA DIRECCIÓN

Un área en la que se puede añadir valor rápidamente y en la que se reconoce fácilmente el ROI es el autoservicio. Los datos de Gartner valoran el coste medio de la resolución de un cliente en autoservicio en 0,10 dólares por interacción, en comparación con el uso de uno o más canales en tiempo real, que puede costar hasta 8,01 dólares por cliente y problema resuelto.

En este sentido, esta capacidad de autoservicio ofrece a las empresas un abanico de opciones y aplicaciones, lo que abre la puerta para la creación de una propuesta completa de soluciones. Así, una recopilación actualizada de preguntas frecuentes, foros de clientes, un sistema IVR conversacional o visual, o un chatbot dedicado y entrenado para responder a los problemas más comunes de los clientes pueden reducir rápidamente los volúmenes de contacto del canal en tiempo real, tanto si existen de forma aislada como si forman parte de un portal de clientes dedicado. Y, sin olvidar que esto, al mismo tiempo, libera a los agentes para que se centren en los problemas más importantes de los clientes, que exigen conocimientos e inteligencia emocional a partes iguales.

El autoservicio es un primer paso digital para las empresas que hasta este momento se han centrado más en otras formas de interacción con el cliente y de resolución de problemas: el 86 % de los consumidores a nivel mundial espera que una marca ofrezca una opción de autoservicio. Además, el 35% de los consumidores y el 42% de los millennials y la generación Z prefieren ayudarse a sí mismos cuando tienen un problema en lugar de tener que descolgar el teléfono.

EL POTENCIAL DE LA INTELIGENCIA ARTIFICIAL

Si una tendencia tecnológica ha estado entre las prioridades de los directivos y responsables de TI en los últimos años, ésta ha sido la Inteligencia Artificial, pero la pandemia ha dejado claro que la IA puede ser un elemento verdaderamente diferenciador para las compañías. Los datos de PwC muestran que, el 42% de los directivos admite que está revisando los casos de uso de la IA, mientras que el 23% está en proceso de ejecutar pequeños proyectos piloto con un enfoque renovado en el aprovechamiento de la tecnología para la experiencia del cliente. Según los datos obtenidos para la elaboración de este informe, un 35% de los ejecutivos dijo que la automatización de tareas era su principal prioridad de IA para el próximo año, mientras que otro 31% afirmó que su prioridad sería el apoyo a los empleados para tomar decisiones más rápidas y mejores.

La COVID-19 aportó más claridad en torno al uso y la aplicación de las tecnologías. Está ayudando a las empresas a orientar su gasto y desarrollo de la IA, sobre todo en lo que se refiere al diseño y despliegue de agentes virtuales inteligentes para atender las necesidades de los clientes, y también en cuanto a los chatbots y otros servicios de automatización inteligente.

Esto se traduce en un dato muy clarificador, y es que el número de compañías estadounidenses que planean invertir más de 5 millones de dólares en el desarrollo de soluciones apoyadas en IA y Machine Learning se ha duplicado desde el inicio de 2020.

Los datos de McKinsey muestran que la RPA ya es la forma de tecnología de IA más implementada en las empresas. Un tercio de las empresas de alta tecnología, el 30% de las telecomunicaciones, el 33% de los viajes y el transporte, el 36% de los servicios financieros

Una visión integral del cliente permitirá establecer relaciones más sólidas con él, lo que incrementará la fidelidad y reducirá la rotación de clientes

y el 21% de las compañías de retail están haciendo uso actualmente de la RPA.

LO QUE EL CLIENTE DEMANDA: EXPERIENCIAS OMNICANAL, PERSONALIZADAS Y CONSISTENTES

A lo largo de estos meses ha quedado de manifiesto que el uso de la automatización, los chatbots y el autoservicio, junto con los canales de voz tradicionales, es decir, un enfoque omnicanal de la experiencia del cliente, es ahora una necesidad. Pero no se trata solo de ofrecer distintas opciones para comunicarse con las compañías, sino que hay que ir más allá y conseguir que todos estos canales ofrezcan una experiencia uniforme tanto en calidad como en velocidad de servicio.

Aunque los consumidores puedan optar por comprar únicamente en tienda u online, el 73% utiliza varios canales durante el proceso de compra. Y lo que es más importante, los clientes omnicanal gastan de media un 13% más que los clientes de un solo canal.

Pero para que una plataforma omnicanal funcione y consiga los objetivos deseados por las compañías, es necesario "el reconocimiento del consumidor y la información". Y es que el 75% de los consumidores esperan poder continuar la interacción en el punto en el que la dejaron al pasar de un canal a otro. Según los datos que maneja Microsoft, para un tercio de los consumidores a nivel mundial, el aspecto más frustrante de la CX es tener que repetir la misma información varias veces. Según las investigaciones de la firma, mientras los clientes pasan de un canal a otro "es fundamental que sus datos y su historial también pasen de un canal a otro, de modo que, tanto si el agente es virtual como físico, el problema pueda resolverse rápidamente y con un mínimo esfuerzo por parte del cliente". De hecho, el 75% de los clientes esperan ahora que el agente no sólo sepa quiénes son, sino que también conozca su historial de compras completo. O, lo que es lo mismo, una visión integral del cliente permitirá establecer relaciones más sólidas con él, lo que incrementará la fidelidad y reducirá la rotación de clientes.

Este conocimiento del cliente puede ir más allá, y convertirse en un elemento de generación de valor para las compañías. Con el uso de la analítica para entender al cliente a partir de toda la información que se tiene de él, se puede mejorar lo que ha venido a denominarse el Customer Journey, lo que favorecerá las labores para conocer por qué se produce la pérdida de clientes y, en consecuencia, tomar las medidas necesarias para reducirla o evitarla.

CONOCER Y ANALIZAR AL CLIENTE

Por este motivo, los profesionales de la experiencia del cliente creen que la analítica de datos es la tendencia más importante en este momento, o que, según Gartner, el 40% de to-

“Una plataforma que aporte amplia visibilidad, con analíticas y logs en tiempo real, que sea altamente programable, y soporte el desarrollo ágil, permite hacer un seguimiento continuo de los comportamientos de los clientes” (Fastly)

Adaptar rápidamente el contenido servido a un usuario en función de su ubicación, historial de compras o preferencia de idioma, u ofrecerle un flujo ininterrumpido de contenido cuando quiere disfrutar de un streaming multimedia o una clase online, son algunos ejemplos del nivel de servicio que los clientes están demandando hoy a sus proveedores. La infraestructura tecnológica juega un papel clave. Jesús Martín Oya, director general para Sur de Europa y Oriente Medio de Fastly, nos habla de cómo proporcionar una experiencia de cliente que no defraude.

¿Cómo generar una buena experiencia de cliente y mejorar la que se tiene?
El cliente actual tiene unas expectativas muy altas de los sitios que visita o en los que compra. Espera cada vez más rapidez -o instantaneidad-, fiabilidad y calidad. Además, aprecia la personalización, que incluye desde que el contenido sea relevante para él hasta que los formatos sean adecuados al dispositivo en el que está navegando. Finalmente, la seguridad es un factor cada vez más importante. La confianza en que la información de su actividad, sus datos personales o de transacciones no corran ningún riesgo, ganan peso en el concepto de experiencia de usuario.

¿Qué principios aplicáis vosotros para mejorar la experiencia del cliente?
Desde Fastly creemos que hay cuatro áreas en las que es necesario poner especial atención a la hora de garantizar la mejor experiencia de usuario. La disponibilidad, independientemente de las variaciones de tráfico. La velocidad, ya se trate de contenido estático o dinámico. La rápida identificación y resolución de incidencias, que es posible a través de la visibilidad adecuada y en tiempo real. Y finalmente, como hemos comentado, la seguridad en todas las capas y sin que el rendimiento se vea perjudicado. >>

dos los proyectos de analítica de datos estén relacionados con algún aspecto de la experiencia del cliente.

Y, en este punto, las empresas se enfrentan a la problemática de la existencia de datos en silos o con formatos incompatibles. Así, hasta el 73% de los datos de una empresa no pueden utilizarse para el análisis, mientras que solo el 27% de las compañías afirma que sus datos son adecuados para su finalidad como marca y que el análisis proporciona información y recomendaciones beneficiosas para los objetivos del negocio.

ENCONTRAR EL EQUILIBRIO ENTRE PRIVACIDAD Y PERSONALIZACIÓN

En la realidad marcada por el inicio del final de la pandemia, las compañías están obligadas a incrementar más que nunca su apuesta por CX (Customer eXperience) para atraer y retener clientes e incentivar su lealtad. Hacer frente al nuevo consumidor digital y a la vez encontrar un propósito y empatía para conectarse con aquellos consumidores que buscan marcas auténticas son solo algunos de los desafíos. Encontrar las herramientas para tender un puente de conexión con las personas es fundamental, sin olvidar, eso sí, las crecientes demandas de privacidad, con lo que se deberá encontrar un equilibrio adecuado para obtener todos los posibles beneficios de la personalización.

>> ¿Qué tecnología creéis que es hoy habilitadora de una mejor experiencia de los clientes?
Es mucha la tecnología desarrollada con la finalidad de dotar a los sitios web, grandes y pequeños, de la mejor experiencia de usuario posible. Por parte de Fastly, podemos hablar de lo que conocemos y de lo que ofrecemos al mercado. Nuestra plataforma edge cloud fue creada en su momento para ayudar a los desarrolladores a extender el core de la infraestructura cloud al borde de Internet, y esa sigue siendo nuestra misión. Ubicarse en el borde de la red permite a las empresas crear experiencias digitales rápidas, seguras y fiables, además de escalar las aplicaciones lo más cerca posible de los usuarios finales.

Una plataforma que aporte amplia visibilidad, mediante analíticas y logs en tiempo real, que sea altamente programable, y que soporte el desarrollo ágil, permite hacer un seguimiento continuo de los comportamientos de los clientes y responder a ellos o a cualquier incidencia de seguridad de forma rápida y eficaz. Conocer, trazar y analizar los movimientos de los usuarios ofrece los datos y la información relevantes sobre las visitas a una página web o app, y ésta es la base para responder de manera correcta en el presente, así como conocer lo que el usuario aprueba, desaprueba o demanda.

¿Qué retorno puede tener para una empresa aplicar tecnologías para mejorar la experiencia de sus clientes? ¿Tenéis algún caso que podáis contar?
Claro, podemos contar de manera breve varios ejemplos de clientes de Fastly que han tenido retornos muy positivos al utilizar nuestros servicios:

➤ El **New York Times** ahorra alrededor de 25.000 dólares al mes sólo en llamadas a la API gracias al almacenamiento en caché de las API en el edge.

➤ **Shopify:** Con VCL y la función Origin Shield de Fastly, Shopify ha reducido al mínimo las peticiones al origen y ha simplificado su compleja infraestructura, reduciendo significativamente la latencia, y disminuyendo el coste y los recursos necesarios para mantener todos estos servicios. Como resultado, ha logrado una proporción de aciertos de caché del 93%.

➤ El proveedor de tecnología para e-commerce **BigCartel** ha logrado, gracias a Fastly, bloquear automáticamente los ataques DDoS en el borde, acelerar la entrega de imágenes, reduciendo a un tercio el tamaño de las fotos de sus catálogos, lo que ha significado que las respuestas han pasado a tardar menos de 250 milisegundos, frente a los varios segundos que tardaban antes, y manteniendo la misma calidad.

➤ **Deliveroo** ha conseguido un 7% de mejora en sus tiempos globales de carga (y en algunas áreas hasta el 50%), traduciéndose en un aumento del 1% en la conversión de su sitio, tras cambiar a la CDN moderna basada en edge-cloud de Fastly.

Si bien los clientes buscan interacciones altamente personalizadas con las empresas, también les preocupa su privacidad y son cada vez más cautelosos a la hora de exigir a las organizaciones responsabilidad sobre cómo recopilan, almacenan y utilizan sus datos. Las empresas que utilizan datos para dar forma a las experiencias de sus clientes deben encontrar el punto de equilibrio entre proporcionar experiencias ricas y personalizadas, como las que los clientes exigen, y asegurar a estos mismos clientes que sus datos no se utilizan o almacenan de forma inapropiada. ■

MÁS INFORMACIÓN

- El futuro de la Experiencia de Cliente
- La experiencia de cliente en la nueva realidad
- Tendencias de CX 2021 de Sitel

Si te ha gustado este artículo, compártelo

itTRENDS

ATENCIÓN OMNICANAL EN EL SECTOR TURÍSTICO

Whatsapp, ¿dígame?

Playasol Ibiza Hotels abre este canal de mensajería instantánea para mejorar la experiencia de sus clientes

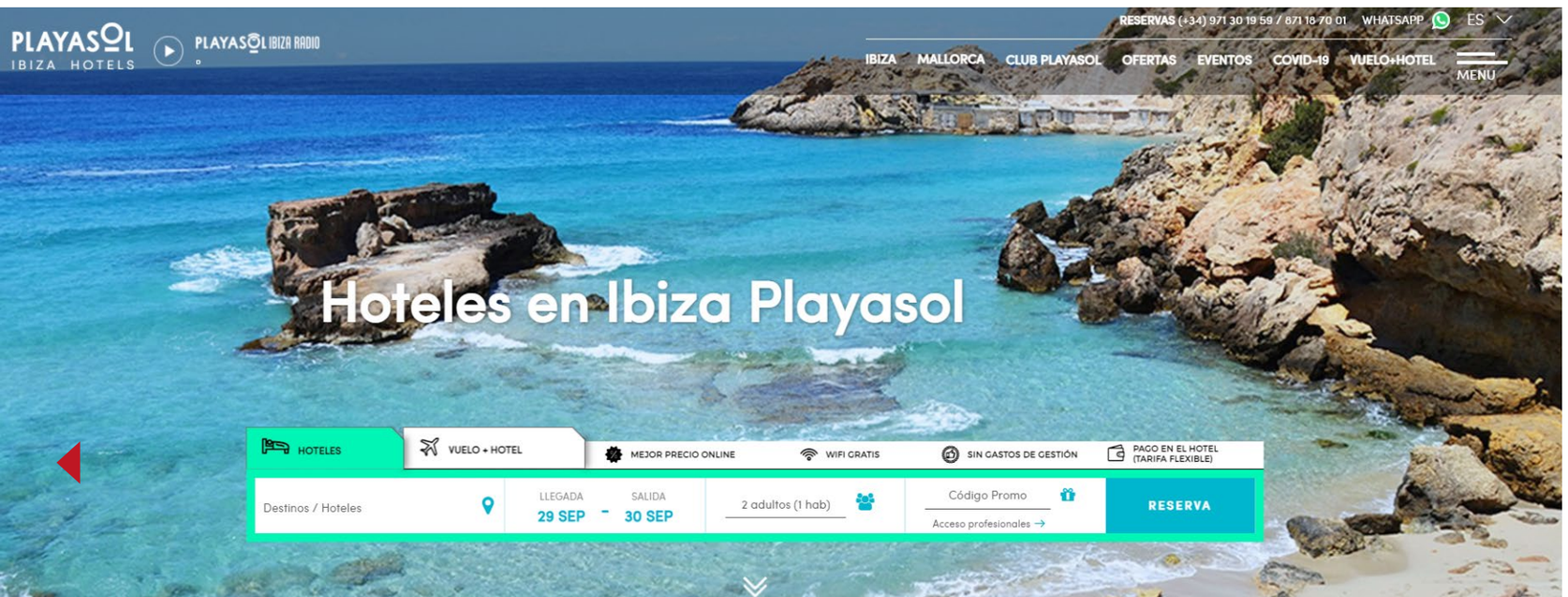
Playa, sol, buen diseño de los hoteles y una atención ágil y rápida forman parte de la filosofía que postula la cadena hotelera Playasol Ibiza Hotels, que cuenta con más de 4.000 habitaciones en las Islas Baleares. La firma analiza y actualiza constantemente su estrategia de comunicación para mejorar la experiencia digital y responder ante los hábitos de los clientes y, fruto de este análisis, decidió poner en marcha una canal de WhatsApp para prestar un mejor servicio.

Si hay un sector que depende enormemente de la experiencia de sus clientes, ese es el hotelero y más en un país como España, siendo el turismo unas de las principales fuentes económicas del país. Proporcionar una mejor atención a los viajeros aumenta su satisfacción y le convierte en un cliente, si no fiel, al menos prescriptor. Islas Baleares, Andalucía y Cataluña fueron los destinos principales del total de viajeros en España el pasado agosto, según el INE, y es en nuestras islas mediterráneas donde se ubican los 6 hoteles, 30 establecimientos y más de 10.000 camas que tiene la cadena hotelera Playasol Ibiza Hotels. La firma acaba de incorporar en su web la opción de chatear con la central de reservas, mejorando así el flujo comunicativo con sus usuarios.

"Hasta ahora utilizábamos métodos más tradicionales como son el email y la vía telefónica, canales muy importantes para nosotros. En los últimos años hemos detectado que nuestros clientes tienen la necesidad de soluciones cada vez más ágiles y vimos que WhatsApp era una herramienta que nos iba a poner en un contacto un poco más directo con el cliente", explica Patricia Vaquerizo, Marketing & Direct Sales Manager de Playasol Ibiza Hotels.

La compañía utilizaba también Facebook para entablar esa relación con los viajeros, "pero se ha desplazado; la cantidad de volumen de consultas que nos llegaban a través de Facebook en los últimos tiempos ha bajado y, en cambio, ha habido una respuesta sobredimensionada de las interacciones por WhatsApp". El uso de la herramienta está enfocado, por el momento, a la comunicación con el cliente antes de su visita al establecimiento hotelero, "aunque también recibimos comunicaciones post; no tanto durante la estancia, porque para eso el cliente tiene la recepción del hotel".

La compañía acaba de instalar la herramienta y se encuentra examinando las mejores prácticas para su uso. Comenzaron con un canal abierto donde el cliente podía realizar cualquier pregunta y ser respondido por un agente. "No obstante, hemos detectado que cada canal tiene su función y no todo puede resolverse por el mismo", añade Vaquerizo; "el email, por ejemplo, es un canal muy bueno para resolver problemas post-stay, mientras que, para ayudar a un cliente a finalizar una reserva, la herramienta más eficiente sigue siendo el teléfono. En WhatsApp tienes que orientar al cliente hacia el tipo de consulta y, por tanto, para ser más eficiente, darle ciertas respuestas automáticas. A raíz de las primeras semanas de implementación de WhatsApp fue donde realmente nos dimos cuenta de que éramos como un saco sin fondo; por eso estamos probando la implementación de un chatbot dentro de WhatsApp. El cliente siempre sigue teniendo la opción




Patricia Vaquerizo

de hablar con un agente, pero a nivel interno nos ayuda a dirigir su consulta: si quiere hacer una nueva reserva, le solicitamos unos datos y finalizamos la reserva vía telefónica; si quiere información sobre un hotel, no necesita la intervención de un agente. Esta pregunta va a ser resuelta por el chatbot... Porque al final los recursos son los que son y tenemos que realmente hacer ese balance entre la experiencia del cliente y la eficiencia de los recursos que nosotros tenemos".

El chatbot de WhatsApp lleva apenas un mes abierto, por lo que -reconoce la responsable de ventas de la cadena- "aún es pronto para valorar su impacto. Sí hemos detectado que, con la interacción a través de WhatsApp, una vez que se finaliza no se suele abrir un ticket; es decir, el cliente ha quedado satisfecho porque siempre tenemos la intervención final de un agente y no solo la dejamos en una respuesta automática". Dicha presencia de un agente ha obligado a la cadena a restructurar en cierta medida los procesos por los que se atendían las peticiones de los usuarios, y destinar recursos específicos a la mensajería instantánea.

También su incorporación ha implicado un reajuste de la infraestructura tecnológica. Josep Costa, Director de Sistemas de Playasol Ibiza Hotels, explica que, para la implementación de este servicio de WhatsApp y WhatsApp bot, han confiado en un proveedor externo especialista en el uso de esta solución a nivel empresarial, "y lo único que hacemos nosotros es reforzar las medidas de seguridad para que no se nos pueda colar alguien en este WhatsApp que no esté redirigido por los canales por los que tiene que entrar".

Otra de las mejoras implementadas por el grupo hotelero balear es la integración de la centralita con el sistema de customer service. "Antes recibíamos llamadas y no sabíamos de quién era. Teniendo registrado tanto la entrada por centralita, como la entrada por email y por WhatsApp, podemos mantener nuestro pequeño CRM e identificar al cliente que nos está llamando", añade Patricia Vaquerizo; "podemos ver el historial de todas las comunicaciones que ha hecho por los diferentes canales, incluso tenemos la posibilidad de escuchar una llamada anterior en el caso de que haya habido algún problema o queja. Cada vez centralizamos más la información".

"Nuestros clientes tienen la necesidad de soluciones cada vez más ágiles. Vimos que WhatsApp era una herramienta que nos iba a poner en un contacto un poco más directo con el cliente"

OBJETIVO: DINAMIZAR LA ESTANCIA

Dentro de su estrategia para lograr la excelencia en la atención al cliente, Playasol Ibiza Hotels puso en marcha el pasado año, y de forma muy rápida por la pandemia, el checkin online con la idea de incorporar nuevos servicios a futuro. "Si tienes una reserva hecha desde nuestra página web o de alguno de nuestros proveedores de reservas más habituales, puedes hacer un checkin online, que reduce a un minuto y medio o dos un proceso que de forma presencial dura cinco. Este año queremos implementar el pago de lo que no está pagado en la reserva; muchas reservas están prepagadas desde la propia web, pero aquella reserva que no se ha prepagado la podrías abonar online, reduciendo el tiempo de espera en la recepción, y haciendo más ágil el proceso de registro", apunta Costa.

Para el próximo año, además de enriquecer este checkin online para la entrada al hotel, se está trabajando en una web app en la que se ofrecerá


Josep Costa

información detallada del establecimiento donde se van a alojar los huéspedes. “Antes lo has podido ver en la página web o con el chatbot de WhatsApp, pero esta aplicación de información predefinida se centrará en tu hotel y dará horarios de comedores, restaurantes, bares, animación o servicios adicionales. También vamos a añadir servicio de early checkin para que quien llega a las ocho de la mañana pueda solicitar una habitación de hotel. Y lo mismo con el late checkout, pidiéndolo mediante la aplicación y evitando tener que bajar a una recepción que pueda estar llena”.

También en la hoja de ruta de la cadena figura la posibilidad de contratar determinados servicios desde esta aplicación, como un taxi o un masaje, “en el momento en el que el usuario lo quiere elegir. La recepción siempre estará disponible, pero el cliente tendrá una utilidad cuando la quiera usar”.

EVALUAR LA ESTANCIA IN SITU

El director de sistemas de Playasol Ibiza Hotels adelanta que para 2022 están trabajando en herramientas para poder conocer la experiencia del cliente mientras está alojado. Y lo harán mediante la red wifi: “tendremos la posibilidad de ir preguntando sobre la marcha, con preguntas muy breves y muy concretas de sí o no, cómo está siendo la estancia para poder actuar mientras está el cliente alojado. No es lo mismo que te escriba una reseña y te disculpes argumentando que la próxima vez no pasará a reaccionar durante la estancia y antes de que se vaya el cliente, y aquello que al cliente no le ha sentado bien o no le pareció bien, poderlo solucionar”.

Un planteamiento como este requiere muchos recursos. “Exige la implicación de una persona en cada hotel que resuelva estas cuestiones, porque tan malo es que suceda como no tener esta información durante la estancia. Incluso es peor que te comuniquen que está fallando algo y no ser atendido. Hasta que estos recursos no estén bien implementados e informados, no daremos el paso de preguntar cómo está”, clarifica Patricia Vaquerizo, si bien cuentan en determinados hoteles con la figura del “guest experience”, una especie de relaciones públicas que contacta con el cliente cuando se detecta cualquier problema.

La cadena trabaja en una web app que ofrecerá información detallada de cada establecimiento, así como en un sistema de preguntas de satisfacción aprovechando la red Wifi

“Vamos paso a paso. No lo hacemos todo de golpe porque se requiere más infraestructura; no es lo mismo un call center donde tienes al personal en un sitio y puedes formar a todos de golpe que estar pendiente y tenerlo distribuido en 30 recepciones. Si ponemos un chatbot en un hotel, necesitamos 30 personas que estén pendientes y ahora mismo no tenemos a estas 30 personas, por eso tenemos que buscar otro tipo de servicios que dar”, finaliza Josep Costa al hablar de los procesos que tiene implementados la cadena para perfeccionar su servicio y lograr una mejor experiencia de sus clientes. ■

itTRENDS

OPINIÓN

Claves para una experiencia de usuario que convierte y fideliza

Jesús Martín Oya,
General Director,
Southern Europe & Middle
East en Fastly

Los índices de conversión y fidelización son indicadores críticos en cualquier actividad de comercio electrónico. Las expectativas de los clientes son altas y exigen rapidez, fiabilidad, seguridad y calidad. Se espera que el sitio no falle nunca, que cargue de forma instantánea, que se actualice en tiempo real.

Vivimos un auge del comercio electrónico en todos los sectores, un momento de crecimiento y cambio que conlleva también un desafío para los e-commerce: el de estar preparados para responder a estas expectativas, teniendo muy en cuenta cómo optimizar el uso que se hace de la o las plataformas que los sostienen y cuáles son las áreas clave de la experiencia de usuario en las que poner especial atención.

PERSONALIZACIÓN

El comprador actual asume que cualquier e-commerce que visita tiene ya información sobre él. Dispositivo, navegador o tipo de conexión son datos de importancia para un e-commerce que sirve imágenes de producto en alta resolución. El modo en que se gestionan esas imágenes, la velocidad y la calidad con las que se reciben, pueden marcar la experiencia de compra o incluso motivar el abandono de un carrito. Tradicionalmente la personalización se ha creado en los servidores de origen con una penalización del rendimiento. Para lograr un nivel de personalización a gran escala de forma óptima, es aconsejable acercar la lógica tanto como sea posible al usuario, es decir, al borde de la red.

RESOLUCIÓN DE INCIDENCIAS

El comportamiento de los usuarios puede variar de forma repentina. También es posible que se produzca un inesperado incidente de seguridad o de disponibilidad de nuestro sitio. Contar con la visibilidad adecuada y en tiempo real para identificar cualquier indicio de problema es el primer paso para atajarlos a tiempo y evitar posibles experiencias de usuario negativas. Contar con la información de forma

“Es necesario tener la capacidad de gestionar los incrementos súbitos de tráfico fácilmente, evitando congestiones en la infraestructura”

completa y detallada en el momento (mediante analíticas obtenidas a través de logs o tags) permite a los retailers conocer en profundidad los movimientos de sus clientes y tomar las decisiones de manera inmediata.

MÁS VELOCIDAD

El contenido dinámico, como los precios de los productos o los datos de stock, suponen una porción importante del volumen de respuestas que genera un sitio web. Por este motivo, la CDN o CDNs que soportan el tráfico de un e-commerce han de ser capaces de cachear y purgar el contenido inválido o desactualizado en apenas milisegundos. Cachear tanto el contenido dinámico como el estático, o cachear las respuestas de APIs en el borde, significa menos viajes a la infraestructura de origen.

UN ESCAPARATE SIEMPRE DISPONIBLE

Un fallo técnico de un sitio web supone una pérdida de confianza por parte del usuario, especialmente en momentos de grandes picos de tráfico como los que se producen en las temporadas especiales de ventas. Es necesario tener la capacidad de gestionar los incrementos súbitos de tráfico fácilmente, evitando congestiones en la infraestructura de origen, sin tener que sobredimensionarla. Si además puede complementarse con un sistema de “sala de espera” que ayude a priorizar la actividad de los compradores activos cuando los servidores de origen están sobrecargados, será más fácil lograr que un e-commerce esté siempre disponible y funcionando sin fallos. Además, el load balancing entre varios orígenes de Fastly escala instantáneamente a varios Tbps sin limitaciones de capacidad.

NO OLVIDAR LA SEGURIDAD

La gestión de los datos de los usuarios y su protección es clave para generar confianza en el consumidor. Las aplicaciones y las funcionalidades se despliegan cada vez más en todo tipo de entornos: contenedores, clouds múltiples e híbridas de diversos proveedores. Mantener la seguridad en todas estas capas, respondiendo a amenazas sin sacrificar el rendimiento y la experiencia de usuario es un desafío creciente.

Fastly es uno de los principales proveedores de infraestructura Edge Cloud. Cuenta entre sus clientes con numerosos retailers que se apoyan en sus soluciones para optimizar sus sitios y garantizar la mejor experiencia de usuario, proporcionando disponibilidad y velocidad de entrega, un entorno web seguro y facilitando la personalización de la experiencia de cada usuario. ■

A10 ZeroTrust

is Incomplete without TLS /SSL Decryption

Key features of a good TLS/ SSL Decryption Solution

- Full Traffic Visibility
- Ease of Integration
- Multi-Layered Security Services
- User Access Control
- Micro Segmentation
- Securing Cloud Access

LEARN MORE AT **A10NETWORKS.COM/SSL**

Tendencias en networking para interconectarlo todo

La tecnología de redes ha evolucionado significativamente a lo largo de los años, ya que la demanda de las empresas ha crecido de forma exponencial. Además de admitir una serie de dispositivos, las redes de área local tienen que gestionar el tráfico generado por muchas otras fuentes, como la transmisión de vídeo en directo, el almacenamiento conectado a la red (NAS), la voz sobre IP (VoIP), la virtualización, la nube y los dispositivos y servicios de IoT, que han generado una demanda de ancho de banda adicional.

Con la vuelta a "la normalidad", algunas tendencias en el mundo del Networking se abren paso en el mercado, coincidiendo con otras que han venido definiendo el mundo de las redes en los últimos años. La necesidad de Internet de alta velocidad, los modelos de computación en la nube y en el Edge, así como la necesidad de migración de datos entre servidores, han dado lugar a un cambio hacia la necesidad de tecnologías de red de gran ancho de banda y baja latencia.

5G Y WI-FI 6: NUEVOS ESTÁNDARES DE LAS COMUNICACIONES INALÁMBRICAS

Tras varios años acaparando titulares y siendo foco de previsiones sobre su despliegue real, 5G parece lista para asumir su posición dominante en las comunicaciones inalámbricas. Esta nueva versión del estándar de tecnología celular se caracteriza por aumentar la velocidad, reducir la latencia y mejorar la flexibilidad de los servicios inalámbricos. Ayuda a las organizaciones a movilizar las fuerzas de trabajo, a ampliar la automatización y a soportar nuevas aplicaciones con una mayor capacidad de red y altas velocidades de datos. 5G ofrece capacidades de itinerancia abierta sin fisuras entre el acceso celular y Wi-Fi, y promete resolver el problema de muchos dispositivos inalámbricos conectados a la vez,

algo que ha venido a empeorar IoT al ralentizar el rendimiento de la red inalámbrica por la integración de un sinfín de dispositivos.

Sin embargo, esto no significa que 5G no vaya a desempeñar un papel integral. La velocidad del 5G es significativamente mayor que la de 4G, y utiliza una banda más amplia del espectro. En concreto, el 5G es 100 veces más rápido que 4G. 5G impulsará los cambios de próxima generación en la tecnología de redes y será fundamental para las empresas, donde la fiabilidad, la velocidad y la reducción de la latencia son primordiales.

Por lo que respecta al nuevo estándar de las comunicaciones inalámbricas de interior, Wi-Fi 6, está listo para funcionar, si bien los dispositivos con capacidad Wi-Fi 6, como los ordenadores y los teléfonos móviles, necesitan adoptar nuevos estándares, sobre todo por la amplitud de la base instalada a renovar.

Hay que tener en cuenta que para llevar a cabo cualquier cambio hay que sustituir lo viejo. En el caso de las redes, la sustitución se refiere a los dispositivos, el core, los dispositivos existentes conectados a Wi-Fi, es decir, el ordenador portátil, la impresora, los escáneres IoT...

SD-WAN

SD-WAN ya se ha convertido en la tecnología WAN por defecto, pero puede desplegarse de diferentes maneras, desde la simple sustitución del router hasta un ecosistema de funciones de red virtuales (VNF) orquestadas de forma centralizada y utilizando múltiples tecnologías subyacentes. Esperamos que se produzca una migración continua a la SD-WAN desde las tecnologías más tradicionales. Los que ya han adoptado SD-WAN tratarán de explotar aún más las capacidades a través de una mayor adopción de CPE universales y VNF para racionalizar el hardware, así como la explotación de diferentes tecnologías para complementar o sustituir los servicios WAN MPLS. Las empresas buscarán cada vez más el despliegue de la ruptura local de Internet para el acceso a la nube y SaaS.

NUEVAS TENDENCIAS PARA MEJORAR LA CAPACIDAD DE LA RED

Los problemas complejos de las redes y de las empresas pueden abordarse en tiempo real utilizando las capacidades de IA y ML. Con Machine Learning se pueden hacer predicciones ba-

La demanda de Internet de alta velocidad, la computación en la nube y en el Edge, o la necesidad de migración de datos entre servidores, exigen tecnologías de red de gran ancho de banda y baja latencia

sadas en los datos de la red y la IA puede tomar acciones inteligentes basadas en esas estimaciones. La analítica avanzada en los sistemas de automatización traerá consigo redes auto-operativas. La IA llevará esto a un nivel completamente nuevo, recopilando datos en tiempo real y apoyando a las empresas para eventos destacados y ocasiones especiales en las que se prevé un gran tráfico. Detectará de forma inteligente el tráfico en tiempo real y reconocerá cualquier actividad maliciosa. En la actualidad, utilizamos los algoritmos de monitorización de redes que buscan posibles actividades sospechosas y tráfico elevado, como ataques de denegación de servicio distribuido (DDoS) y hackeos.

La IA seguirá siendo una fuerza disruptiva en la gestión de redes, ofreciendo avances que son fundamentales para la disponibilidad y la seguridad de los recursos críticos. A medida que adoptamos el trabajo a distancia y esperamos la red 5G, es integral introducir redes mejoradas por la IA que permitirán operaciones más rápidas, inteligentes y seguras.

Y aunque no es una tendencia nueva, la nube sigue teniendo gran efecto en las redes y marca, por tanto, las tendencias a estudiar en el mundo del Networking. Cloud permite una transición más rápida al trabajo remoto y ayuda a organizar el nuevo espacio de trabajo de forma más eficiente, lo que contribuye a la continuidad de la empresa durante cualquier crisis, como hemos visto claramente durante la crisis provocada por la pandemia. Mantener políticas de red y seguridad consistentes en múltiples nubes utilizando la gestión de políticas en múltiples nubes es otra realidad de la que no pueden escapar los responsables de TI.

Además de las comentadas, que tienen un impacto directo sobre el mundo de las comunicaciones, existen otras tendencias que también tendrán su efecto sobre el Networking en los próximos trimestres. Una de ellas en DevOps, que está vinculada al desarrollo de software y a las TI, y que puede contribuir a mejorar la relación entre los diseñadores de servicios de red y los ingenieros para realizar cambios operativos en los servicios.

Y, aunque no es una tendencia tecnológica en sí, tampoco podemos olvidar la evolución sobre la red de los proyectos de Transformación Digital de las compañías, porque es el paso para transformar los servicios o negocios, sustituyendo los procesos manuales por procesos digitales, y este proceso transforma esta realidad en elementos digitales que se procesan, almacenan y transmiten a través de dispositivos y redes digitales. Lo mismo podemos decir de la seguridad. La usabilidad e integridad de la red es crucial. Una segu-

ridad de red eficaz gestiona el acceso a la red de manera efectiva y detiene una variedad de amenazas que entran o se propagan dentro de la red.

Volviendo a las tendencias tecnológicas, y relacionado con aspectos como la seguridad, encontramos IBN (Intent-Based Networking), un enfoque que tiende un puente entre el negocio y las TI. La intención empresarial se capta y se alinea continuamente con la red de extremo a extremo en relación con los niveles de servicio de las aplicaciones, las políticas de seguridad, el cumplimiento y los procesos operativos y empresariales. La segmentación virtual de los dispositivos IoT de la red restante será una de las principales tareas de los equipos de red. La creación de zonas seguras, llamadas microsegmentos, permitirán a los dispositivos IoT operar en la misma red corporativa y reducir los riesgos para otras partes de la red.

LA AUTOMATIZACIÓN DE LA RED ES PRIMORDIAL

La automatización de la red es más importante que nunca. Cuestiones como el aumento de los costes, la escalabilidad y la agilidad empresarial han salido a la luz con la pandemia mundial. Por lo tanto, es hora de que las empresas infundan la automatización para seguir el ritmo al que evoluciona el mundo.

Con el aumento de la cultura del trabajo remoto, el IoT, la adopción de la infraestructura en la nube y el aumento de las transacciones en línea, se hace imprescindible un punto de contacto central para gestionar las aplicaciones tradicionales y nativas de la nube. Ahí es donde entra en juego la automatización de la red.

La automatización ayuda a la empresa para manejar significativamente más solicitudes de servicio sin aumentar el tiempo. Además, ayuda a los equipos de NetOps a despejar los atrasos, proteger, configurar, escalar y entregar las aplicaciones rápidamente en comparación con el funcionamiento manual. En otras palabras, elimina el trabajo monótono y manual.

El tiempo que se ahorra con la automatización permite a las empresas hacer más con su personal existente, reduciendo finalmente los costes de forma significativa.

SECURE ACCESS SERVICE EDGE (SASE)

Las arquitecturas SASE (Secure Access Service Edge) prevén la unión de las redes y la capacidad de seguridad para ofrecer una plataforma de red nativa de la nube. El año 2021 ha sido fundamental para dejar de pensar en la conexión de los edificios físicos y los centros de datos centrales y pasar a conectar a los usuarios y los dispositivos (estén donde estén) con las aplicaciones (estén donde estén alojadas). Aunque los productos y las capacidades siguen evolucionando, las empresas deberían empezar a trazar su estrategia y sus hojas de ruta para evolucionar

hacia una arquitectura SASE. Vemos esto como una evolución, siendo SD-WAN una de las bases, apoyada por las crecientes capacidades de los servicios de seguridad basados en la nube.

ZERO TRUST NETWORK ACCESS (ZTNA) Y SOFTWARE DEFINED PERIMETER (SDP)

Las soluciones tradicionales de acceso remoto basadas en VPN han tenido a veces dificultades para hacer frente al volumen y la complejidad del trabajo masivo en casa de 2020. Las nuevas tecnologías, que utilizan los principios de "confianza cero", están ganando terreno y deberían investigarse para mejorar la seguridad, la escalabilidad y la flexibilidad. Los enfoques Zero Trust Network Access (ZTNA) y Software Defined Perimeter (SDP) tienen como objetivo crear un límite de acceso basado en la identidad y el contexto, con la capacidad de conceder acceso a aplicaciones o recursos específicos a través de un agente de confianza. El ZTNA puede constituir un bloque de construcción dentro de una estrategia más amplia de SASE y Zero Trust.

La IA seguirá siendo una fuerza disruptiva en la gestión de redes, ofreciendo avances que son fundamentales para la disponibilidad y la seguridad de los recursos críticos

CONCLUSIONES

Como hemos visto, son muchas las tendencias que, de una forma u otra, van a contribuir a cambiar el panorama del Networking al que estábamos acostumbrados, desde las nuevas tendencias en el mundo laboral, con el avance hacia un nuevo modelo de trabajo, hasta las nuevas prácticas en el ámbito de la seguridad, con nuevos estándares y estrategias que tratan de responder al reto que impone la protección de los negocios cada día más distribuidos y en tiempo real. Sin olvidar que la base sobre la que se desplegará todo, la red, está cambiando de forma profunda por nuevos estándares, como 5G y Wi-Fi 6, el empuje de tendencias como cloud, IoT o la definición de los nuevos consumos como servicio. O el empuje que se presume tendrán las redes con la implementación de la Inteligencia Artificial, Machine Learning o las nuevas capaces de la Automatización. ¡Bienvenidos a la red del futuro (en el presente)! ■

MÁS INFORMACIÓN

- Los usuarios de 5G se multiplicarán por 1000 en un lustro
- IT Trends: En busca de la conectividad inteligente
- SD-WAN acelera en Europa
- La seguridad de su WAN. Los 3 tipos principales de amenazas y cómo superarlos
- IT Trends: La era de la conectividad
- Aumenta la inversión en SASE para proteger el borde
- La Transformación de la WAN y la seguridad
- Networking Technology Trends
- Tendencias clave en el mercado de Networking en 2021
- Más allá de la seguridad perimetral


Harmony
The Highest Level of Security
for Remote Users
ENDPOINT
MOBILE
EMAIL & OFFICE
CONNECT (SASE)
BROWSER
Check Point®
SOFTWARE TECHNOLOGIES LTD
checkpoint.com

#ENCUENTROSITTRENDS

Conectando y entendiendo la empresa sin fronteras

Nos encontramos en un momento en el que la conectividad se da por hecho. Tecnologías como SD-WAN se afianzan mientras la 5G se abre camino, la computación de marcha al Edge y el IoT sigue avanzando sin freno y a lo grande. Es la era de la "borderless company", una empresa sin fronteras donde triunfa el teletrabajo así como la adopción de la nube o el IoT

¿Qué opciones existen para gestionar una empresa cuyo perímetro está cada vez más diluido y potenciado por las nuevas tecnologías de conexión?

En IT Trends hemos reunido a diversos expertos para abordar los retos de la empresa conectada y sin fronteras en una sesión titulada Conectando y entendiendo a la empresa sin fronteras. Para ello se han organizado tres encuentros, el primero de los cuales reunió a un grupo de expertos del entorno académico, quienes ofrecieron su visión sobre cómo han evolucionado las tecnologías de conectividad. En un segundo panel se plantearon tanto los retos de las empresas modernas, como el impacto del 5G o el avance en la adopción de SD-WAN. Y la última mesa de debate buscó dar protagonismo a la seguridad en este contexto de empresas "borderless".

#ENCUENTROSITTRENDS

El ecosistema de conectividad

Durante la sesión titulada Conectando y entendiendo la empresa sin fronteras, el primer panel tuvo a Santiago Moral Rubio, Director de DCNC Sciences en la Universidad Rey Juan Carlos y Eduardo Arriols, profesor en el Grado en Ingeniería del Software, mención ciberseguridad, en el Centro Universitario U-tad, como invitados, con el objetivo de entender cómo están evolucionando las tecnologías de conectividad y de qué manera las están empleando las organizaciones.

En este sentido, Santiago Moral se mostró sorprendido: "es la primera vez en la historia que ha habido empresas funcionando mientras toda su informática estaba fuera". Se trata de un paradigma que se inició hace 20 años, cuando las empresas empezaron a ir a la nube, y que se ha radicalizado con modelos en los que todo está en la nube y los empleados en sus casas "por lo que la manera de trabajar, de aproximarse a la resolución de los problemas tecnológicos, cambia radicalmente".

Eduardo Arriols apuntó que el teletrabajo ha impulsado ese nuevo modelo más cloud

Santiago Moral Rubio, Director de DCNC Sciences en la Universidad Rey Juan Carlos; y Eduardo Arriols, profesor en el Grado en Ingeniería del Software, mención ciberseguridad, en el Centro Universitario U-tad, junto a Arancha Asenjo, directora de IT Televisión, ITDM Group.

donde no sólo es todo más práctico, sino que "tiene unos ahorros de costes importantes".

¿Qué desafíos se encuentra una organización que prácticamente no tiene infraestructura a la hora de conectar a todo el personal, todos los equipos y hacerlo de una manera segura? "El reto es intelectual, es pensar que no tienes que conectar a la gente", aseguró Santiago Moral, añadiendo que el gran cambio se da en que hay departamentos "que dejan de tener sentido". Explicó, además, que hay cosas que se tienen que hacer de otra manera y que si bien hay que cambiar la tecnología, "lo más duro es cambiar la organización".

Para Eduardo Arriols, "la parte de ciberseguridad es una de las cosas que ha cambiado más", entre otras razones porque ahora tienes que escoger proveedores y mirar con cuidado que no se conviertan en un riesgo, y porque uno de los contras de esta evolución es que la exposición que se tiene en Internet suele ser mucho mayor que cuando cada empresa tenía su infraestructura.

Haciendo referencia a SD-WAN, Santiago Moral señaló que cuando vas haciendo las cosas por software en vez de por hardware, "todo es más configurable y por tanto es más flexible y ofrece mayores posibilidades de adaptabilidad". Añadió que es necesario que se entiendan las mejoras que puede aportar, como es multiplicar la capacidad de interconexión, que a su vez permite nuevas formas de relacionarnos. Por su parte, Eduardo Arriols mencionó que SD-WAN no sólo facilita la configuración, sino que "lo puedes hacer todo de forma mucho más centralizada, mucho más ágil, mucho más rápido".

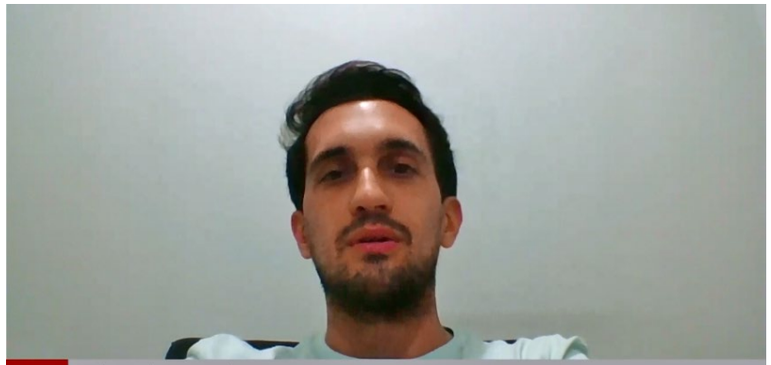
Planteamos a nuestros expertos cómo la 5G puede contribuir a la hiperconectividad de las empresas y si realmente se está sacando partido a esta tecnología. Reconociendo que la 5G no es algo que se está adoptando de forma generalizada, el profesor de U-tad señaló que la principal ventaja que aporta 5G es la velocidad y que donde más se aprovechará será en un entorno empresarial desde un enfoque de IoT.

Para Santiago Moral Rubio, tecnologías como 5G y SD-WAN pueden establecer conexiones permanentes entre las cosas o entre los humanos "y lo que nos hace falta es que empiecen a aparecer empresas que vayan imaginando nuevos tipos de servicios, y veremos en los próximos años cómo eso nos vuelve a cambiar la forma de relacionarnos nosotros y con nuestros elementos". ■


Santiago Moral, DCNC

"Por primera vez en la historia ha habido empresas funcionando mientras toda su informática estaba fuera"

SANTIAGO MORAL RUBIO, DCNC SCIENCES, UNIVERSIDAD REY JUAN CARLOS


Eduardo Arriols
Profesor en el Grado en Ingeniería del Software, mención ciberseguridad, en el Centro Universitario U-tad

"SD-WAN no sólo facilita la configuración, sino que permite hacerlo todo de forma mucho más centralizada, ágil rápida"

EDUARDO ARRIOLS, CENTRO UNIVERSITARIO U-TAD

aruba

a Hewlett Packard
Enterprise company

¿Cansado de la VLAN?

PRUEBE ALGO NUEVO CON ZERO TRUST Y SASE

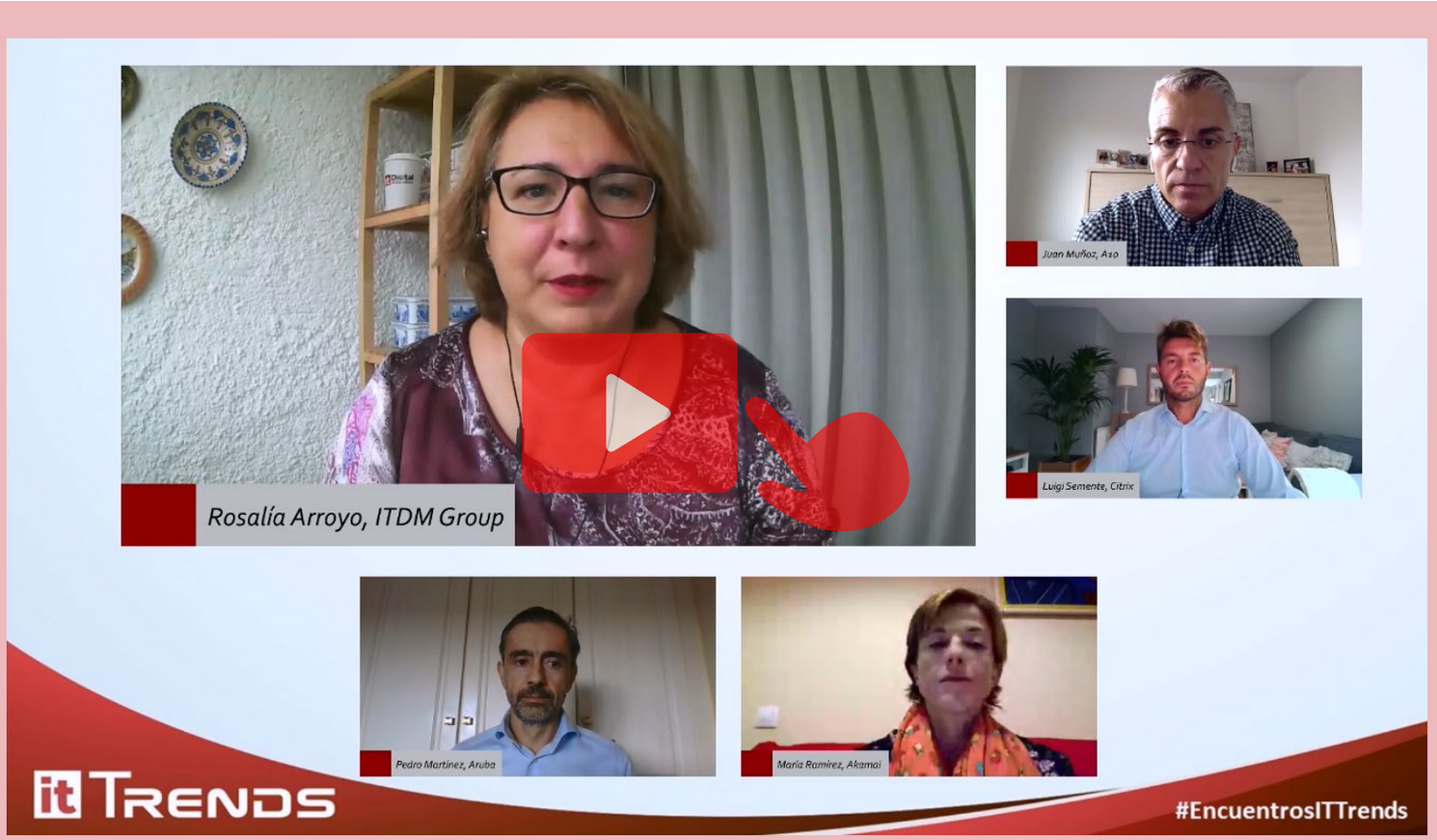
MÁS INFORMACIÓN →

#ENCUENTROSITTRENDS

Conectando la empresa sin fronteras

El segundo debate de la sesión Conectando y entendiendo la empresa sin fronteras reunió a diferentes portavoces en torno a la manera de conectar la empresa sin fronteras, así como los retos a los que se enfrenta. Para ello se contó con la participación de Juan Muñoz, Country Manager Spain & Portugal de A10 Networks; Luigi Semente, Cybersecurity Sales Specialist de Citrix Iberia; María Ramírez, Enterprise Solution Engineer de Akamai, y Pedro Martínez Busto, Responsable de desarrollo de negocio Sur de Europa de Aruba Networks.

Arrancó la reunión preguntando a los invitados por retos de las empresas "modernas", aquellas que han abrazado el cloud y están haciendo frente al teletrabajo o el IoT. Para Juan Muñoz (A10 Networks), "tener los recursos siempre disponibles" es el principal reto de estas compañías, mencionando de manera explícita que las infraestructuras deben estar preparadas para asumir ese incremento de tráfico que supone el IoT y el poder tener la tienda más cerca del cliente a través de las apps.



Juan Muñoz, Country Manager Spain & Portugal de A10 Networks; Luigi Semente, Cybersecurity Sales Specialist de Citrix Iberia; María Ramírez, Enterprise Solution Engineer de Akamai y Pedro Martínez Busto, Responsable de desarrollo de negocio Sur de Europa de Aruba Networks, debaten junto a Rosalía Arroyo, directora de IT Digital Security.

“Las ventajas de 5G también pueden utilizarse para lanzar mejores ataques”

JUAN MUÑOZ, COUNTRY MANAGER SPAIN & PORTUGAL, A10 NETWORKS

Para Luigi Semente (Citrix) el trabajo remoto, que es una de las características de la empresa sin fronteras, ha creado dos desafíos: cómo garantizar una seguridad que sea consistente y cómo garantizar la calidad de los servicios. La clave, aseguró, “es garantizar tanto la disponibilidad como la calidad de los servicios”.

La experiencia ha demostrado a Akamai (María Ramírez) que “conseguir dotar de un acceso seguro a las aplicaciones” es uno de los principales retos a los que se enfrentan las empresas conectadas, así como concienciar a esos usuarios de la nueva forma de trabajar.

Pedro Martínez (Aruba) apuntó la gestión de la experiencia de los usuarios como uno de los retos de las empresas modernas, y aseveró que “el tránsito del usuario hasta la aplicación ya no es algo que está dentro del ámbito de responsabilidad de la empresa, sino que ahora estamos yendo a un proveedor de Cloud, y ahí es más complicado gestionar la seguridad”.

Para finalizar mencionó como reto el adaptar las tecnologías o redes WAN a los nuevos requerimientos que marca este entorno tan híper distribuido.

“La tendencia es hacia la cloud híbrida”, dijo Juan Muñoz, explicando que tanto el IoT como los servicios online “lo que hacen es estresar los propios recursos de las organizaciones”. Esta cloud híbrida se convierte, por tanto, en un punto clave en este aumento de la necesidad de la disponibilidad, elasticidad y uniformidad en la seguridad de los propios servicios de la organizaciones.

Una de las características de estas empresas sin fronteras es el alto nivel de trabajo remoto. ¿Cómo se hace frente a este reto de manera segura y, sobre todo, de manera transparente para el empleado? Para Luigi Semente la palabra clave es simplificar. Un proceso que asegura “que es bastante sencillo con las tecnologías existentes” que permiten, por ejemplo, proporcionar un acceso unificado a todos los recursos que hacen falta para trabajar o el poder añadir “algunos mecanismos más avanzados a nivel de seguridad”.

Al preguntar qué debe tener en cuenta una empresa para dar conectividad segura a los usuarios que quieren acceder a cualquier tipo de aplica-

“La conectividad tiene un gran impacto en la experiencia del usuario con las soluciones SaaS”

LUIGI SEMENTE, CYBERSECURITY SALES SPECIALIST, CITRIX IBERIA

ción, María Ramírez se mostró rotunda al afirmar que las VPN (Virtual Private Networks) son una tecnología obsoleta, por lo que lo primero a tener en cuenta es la posibilidad de proporcionar una solución no basada en VPN “y que al mismo tiempo consiga abrazar el modelo Zero Trust”. Comentando que actualmente se trabaja mucho con gestores de identidad en la nube que delegan la autorización en directorios activos, y que esto no es suficiente, mencionó también la portavoz de Akamai la necesidad de un servicio que consiga robustecer el proceso de autenticación.

SD-WAN es una tecnología que está orientada a estas empresas cada vez más distribuidas, que han abrazado la nube, y que por tanto, es válida para esa borderless company que protagoniza este Encuentro IT Trends. Explicó Pedro Martínez que uno de los beneficios que aporta es que permite garantizar que los usuarios tienen una experiencia de uso óptima estén donde estén; aseguró, además, que “SD-WAN devuelve el control a las empresas” frente a unos entornos WAN gestionados por el operador de telecomunicaciones y sobre los que se tenía muy poca visibilidad; que ofrece mucha más flexibilidad a las propias organizaciones “para, de forma dinámica, seleccionar qué proveedores en la nube son los adecuados en cada momento”; y que permite independizar el servicio de conectividad de las tecnologías o proveedores de tecnología WAN que tenemos por debajo.

SITUACIÓN DE LA EMPRESA ESPAÑOLA

Sobre si la empresa española es una empresa moderna y sin fronteras que adopta el SD-WAN, el IoT o el teletrabajo, dijo María Ramírez que en España se ha ido a la zaga de otros países en cuanto a la adopción de nuevas tecnologías, pero “poco a poco se van modernizando, van utilizando cada vez más aplicaciones en la nube, van creando autenticación basada en proveedores de identidades cloud... Vamos dando pasos y avanzando de una forma paulatina”.

Asegurando que “el Covid ha sido un catalizador a la hora de acelerar esta transición” de las empresas, Juan Muñoz planteó que se está viendo un cambio de mentalidad en la forma de trabajar en remoto o de relacionarnos con las empresas; “antes pensábamos en las colas en las oficinas y ahora se empieza a pesar en las colas en los sistemas. Por eso las empresas, tanto en las pequeñas como las medianas, están abrazando la cloud y la disponibilidad de los sistemas”.

Pedro Martínez puntualizó que las empresas españolas están abrazando la nube, tanto en lo que se refiere a las aplicaciones como al cómputo o el almacenamiento, “pero en la parte de conectividad vamos bastante por detrás”, y puso como ejemplo la conectividad los nuevos estándares WiFi 6, cuya adopción es todavía muy residual. “Otro ejemplo de tecnología que le queda mucho camino por andar a nivel de adopción en el mercado español es SD-WAN”, aseguró el directivo de Aruba añadiendo que tampoco somos proactivos cuando se habla de adoptar las nuevas propuestas para gestionar la red en la nube o de los modelos de consumo de conectividad como servicios, o network-as-a-service.

“Conseguir dotar de un acceso seguro a las aplicaciones es uno de los principales retos a los que se enfrentan las empresas conectadas”

MARÍA RAMÍREZ, ENTERPRISE SOLUTION ENGINEER, AKAMAI

Desde Citrix, Luigi Semente aportó la existencia de dos perfiles de empresas, las súper modernas -que ya tienen toda una serie de tecnologías para mejorar la conectividad entre CPD y nube-, y todas las demás, con dos elementos comunes a ambas: por un lado, el ahorro a nivel de costes operativos en las redes debido a la apuesta por la nube pública y, por otro, la mejora en la calidad de los servicios. “SD-WAN viene para solucionarlo al permitir un ahorro de costes y al mismo tiempo optimizar todas las comunicaciones de nuestra red extendida”.

Mucho se habla de 5G y del impacto que tendrá en las empresas, ¿que debe tenerse en cuenta en su adopción? Para el director general de A10 Networks, 5G está suponiendo una revolución, sobre todo porque permite un aumento sustancial del ancho de banda disponible, así como una reducción de la latencia, pero estas ventajas también pueden utilizarse para lanzar ataques, por lo que “en este ecosistema 5G se hace especialmente importante llevar la seguridad a lo que es la frontera más próxima, a los dispositivos IoT y a los clientes de móviles, del hogar, etc.”.

Para Luigi Semente, entre las ventajas de ofrecer SD-WAN en los entornos híbridos destaca la mejora de adopción de las cargas de trabajo en la nube pública “porque el proceso de on-boarding se agiliza muchísimo con una herramienta de SD-WAN”. También se garantiza la seguridad y aporta una mejora en casos de uso concretos en la experiencia de usuario, como el uso de Office 365, así como una optimización de costes.

“Tiene que haber un equilibrio entre la seguridad y la facilidad de uso o la sencillez a la hora de securizar los accesos de los usuarios”, sumó la portavoz de Akamai añadiendo que la autenticación es un proceso clave que tiene que tener en cuenta el dispositivo y especial atención con los ataques man-in-the-middle.

En los entornos distribuidos es fundamental la aproximación Zero Trust para garantizar que ningún usuario ni dispositivo se puedan conectar siquiera a la red si no tiene las credenciales adecuadas y siempre con los privilegios mínimos necesarios para que pueda acceder.

“SD-WAN devuelve el control a las empresas”

PEDRO MARTÍNEZ BUSTO, RESPONSABLE DE DESARROLLO DE NEGOCIO SUR DE EUROPA, ARUBA NETWORKS

IMPACTO DEL AS-A-SERVICE EN LA EXPERIENCIA DE USUARIO

Para Luigi Semente, de Citrix, las aplicaciones SaaS “han definido un cambio total en el paradigma de cómo se están utilizando las aplicaciones”, en el que la conectividad tiene un gran impacto en la experiencia de usuario: se necesita establecer pasarelas directas que permitan al usuario acceder con la mejor comunicación a las aplicaciones como servicio. Planteó también el directivo de Citrix la necesidad de controlar la seguridad y confidencialidad de estas propuestas.

Asegurando que existe una gran preocupación por medir la experiencia de usuario, Juan Muñoz apuntó que uno de los drivers de esa experiencia es que las aplicaciones siempre tengan que estar 24x7 y además de manera inmediata, “por lo que el concepto de cloud híbrida es súper importante para poder ofrecer los servicios incluso en momentos de estrés”. Habló también el directivo de A10 Networks de

la seguridad como elemento importante en la experiencia del usuario, una seguridad entendida “desde dos puntos de vista; la confianza al sitio web al que me conecto, y la confidencialidad”.

Para Pedro Martínez las aplicaciones en la nube no solo aportan un nivel mucho mayor de disponibilidad, sino ubicuidad en el acceso y la posibilidad de disponer de nuevas funcionalidades y mayor innovación. Además, esas aplicaciones dan a los clientes empresariales mucha más “capacidad de elegir con qué proveedor quiere trabajar en cada momento con unos costes de cambio mucho menor y con unos modelos de consumo mucho más adaptados a esas necesidades de negocio que le hacen poder tener unos costes seguramente mucho más predecibles”.

Respecto a la buena experiencia de usuario, aseguró María Ramírez que “lo principal es que el usuario reciba el contenido al que desea acceder de una forma ágil, que no sufra retardos, que no tenga ningún tipo de mala experiencia a nivel de mala visibilidad de la aplicación, etc.”, para lo que son fundamentales tecnologías tradicionales de aceleración, así como el incorporar la seguridad. ■

Si te ha gustado este artículo, compártelo

SOPHOS

Sophos ACE, hacia un ecosistema de ciberseguridad adaptativo

Haga frente a las nuevas ciberamenazas con soluciones coordinadas

sophos.com/es-es

#ENCUENTROSITTRENDS

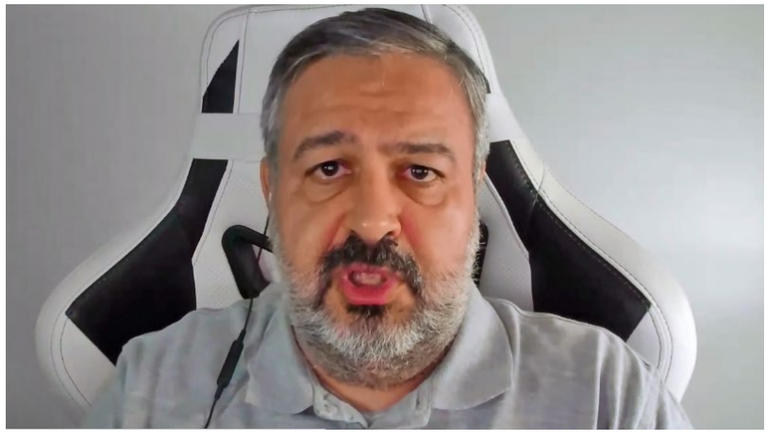
Protegiendo la empresa sin fronteras

El tercer y último debate de la sesión Conectando y entendiendo la empresa sin fronteras se centró en la seguridad, en cómo proteger a la empresa sin fronteras y en las mejores formas de hacer frente al IoT y a 5G. Para ello se contó con la participación de Eusebio Nieva, Director Técnico de Check Point Iberia; Raül Albuixech Gandía, Director Soporte Técnico y Servicios de ESET España; y Javier Donoso, Sales Engineer de Sophos Iberia.

La primera pregunta que planteamos a nuestros invitados fue sobre los retos de seguridad de la empresa sin fronteras, distribuida y abrazada al cloud. “Lo primero es adaptar la seguridad a tu conectividad y a todo aquello que estés utilizando”, dijo Eusebio Nieva, añadiendo que hay que empezar a aplicar nuevas técnicas y nuevas filosofías de seguridad para adaptarse a este nuevo nueva forma de trabajar teniendo en cuenta que el perímetro de seguridad ha desaparecido desde hace tiempo.

Asegurando que hay que adaptar la seguridad a cada caso, apuntó Raül Albuixech que el reto es buscar la securización individual del

Eusebio Nieva, Director Técnico de Check Point Iberia; Raül Albuixech Gandía, Director Soporte Técnico y Servicios de, ESET España; y Javier Donoso, Sales Engineer de Sophos Iberia, junto a Rosalía Arroyo, directora de IT Digital Security.



“Lo primero es adaptar la seguridad a tu conectividad y a todo aquello que estés utilizando”

EUSEBIO NIEVA, DIRECTOR TÉCNICO, CHECK POINT IBERIA

dispositivo teniendo en cuenta la implantación de una solución de seguridad, actualizaciones de sistema operativo, VPN, doble factor de autenticación... Añadió que si han de adoptarse nuevas medidas o nuevas soluciones de seguridad, “que ese despliegue sea sencillo y automático”. Mencionó también la protección del dato y la gestión centralizada como puntos importantes a tener en cuenta.

Para Javier Donoso, hay que saber adaptarse a las nuevas situaciones que se plantean en las empresas y una de ellas es el teletrabajo. “Hay que saber responder a todas esas exigencias que, de un día para otro, se nos han puesto delante de la mesa con soluciones muchísimo más funcionales capaces de crear un ecosistema de ciberseguridad adaptable”.

Una de las características que tienen estas empresas conectadas y modernas es su adopción del IoT, que requieren de unos controles de seguridad más especializados “porque no son dispositivos y sistemas que habitualmente se hayan utilizado hasta ahora y eso hace que, en algunas ocasiones, sean más peligrosos”, advirtió el director técnico de Check Point, añadiendo que lo primero que hay que hacer con el IoT es aplicar las normas básicas de seguridad y de higiene digital teniéndoles en redes aisladas, “y a partir de ahí, poner capas de seguridad a medida que se vayan aumentando los servicios”.

En un modelo de trabajo remoto que se ha extendido durante el año pasado, expuso el portavoz de ESET España que lo esencial es proteger el dispositivo, para lo cual no sólo es necesario disponer de una buena solución de seguridad, sino tener instalados los últimos parches de seguridad y contar con un servicio de autenticación multifactor “para eliminar de la ecuación la debilidad de las contraseñas, así como formar al empleado en materia de ciberseguridad”.

Sobre las VPN, Javier Donoso indicó que de ser una tecnología de conectividad que permitía que los empleados externos trabajaran como si estuvieran dentro de las empresas, ahora se está viendo desplazada por tecnologías más modernas como Zero Trust Network Access (ZTNA). Aseguró el ejecutivo de Sophos que las VPN no se diseñaron para que un número masivo de trabajadores remotos pudieran acceder a aplicaciones que están en un entorno híbrido, y que ZTNA “utiliza los principios de confianza cero para conectar de forma segura a los usuarios con las aplicaciones”.

“Lo primero que debe hacerse es evaluar quién necesita realmente acceder a qué servicios”

RAÜL ALBUIXECH GANDÍA, DIRECTOR SOPORTE TÉCNICO Y SERVICIOS, ESET ESPAÑA

LA EMPRESA ESPAÑOLA, CONECTADA Y SIN FRONTERAS

En otro momento de la conversación, se planteó a los invitados la situación de la empresa española, si verdaderamente es una empresa moderna, si está adoptando nuevas tecnologías de conectividad y si esa adopción va acompañada de seguridad. Según Raül Albuixech, “estamos mejor que hace un par de años, sobre todo porque la pandemia ha forzado cambiar a muchas empresas”, y se está avanzando en adoptar nuevas medidas de seguridad más allá de los típicos antivirus o firewall tradicionales, a favor de soluciones de sandboxing en nube, múltiple factor de autenticación, EDR, gestión cloud, etc.

Para Javier Donoso, “no todas las empresas han sido capaces de adoptar todavía ese modelo 100% fiable en este nuevo escenario en el que podemos trabajar desde cualquier lado con conexión a Internet”. Dijo el ejecutivo de Sophos que esto es debido a que la pandemia ha forzado este cambio de modelo y ha pillado a muchos desprevenidos y sin los deberes hechos “en cuanto a procedimientos, metodologías y mecanismos de seguridad que estuvieran lo suficientemente validados como para asegurar un correcto funcionamiento de los recursos más allá de las fronteras de la empresa”.

En opinión de Eusebio Nieva, no es fácil encontrar en España una empresa moderna, algo que depende de los sectores y cultura tecnológica, y es que estamos muy por detrás de los países de nuestro nivel económico en la zona del euro en lo que respecta a la adopción de servicios cloud. Sí que percibe, añadió, una tendencia a que la seguridad se integre en esos servicios desde el principio, “sobre todo cuando hay un cambio tecnológico”. Aseguró, además, que “hay una tendencia a empezar a consumir servicios de conectividad o servicios de seguridad en la nube que van a hacer más sencillo a muchas empresas ese cambio tecnológico”.

Mucho se habla de la revolución que 5G trae a nivel de conectividad, pero ¿cuáles son los retos de seguridad que está generando, o que va a generar? Para el director técnico de Check Point nos enfrentaremos a “una explosión de conectividad móvil” como una de las consecuencias de 5G, que provocará un aumento en el consumo de servicios desde terminales que, en general, “no tienen la seguridad que deberían tener para el uso que corporativo” y que pueden convertirse en puerta de entrada para después hacer los movimientos laterales, etcétera.

Planteamos a Raül Albuixech cómo controlar el acceso a unas aplicaciones que se consumen en modo servicio y respondió el portavoz de ESET España asegurando que lo primero que debe hacerse es evaluar quién necesita realmente acceder a qué servicios; después, “el doble factor de autenticación es indispensable”, una tecnología cuya adopción se ha disparado durante la pandemia tanto para acceder al correo electrónico como a servicios de la propia oficina, conectarse a las VPN, etc.

Los entornos as-a-service son propios de las empresas conectadas y sin fronteras que, además, adoptan nuevas tecnologías de conexión, como es el caso de ZTNA, un modelo

“VPN es una tecnología obsoleta que se está viendo desplazada por tecnologías más modernas como Zero Trust Network Access (ZTNA)”

JAVIER DONOSO, SALES ENGINEER, SOPHOS IBERIA

que, en opinión de Javier Donoso, ha venido para quedarse. Aseguró el portavoz de Sophos que ahora más que nunca las compañías necesitan “muchísima más información de lo que está ocurriendo en su infraestructura en todo momento, independientemente de dónde se encuentre ese recurso y con independencia también de cuál sea el PC, el portátil, el móvil o el dispositivo IoT”.

SAAS Y EXPERIENCIA DE USUARIO

Para finalizar el encuentro, preguntamos a nuestros invitados por el impacto que tienen las aplicaciones como servicio en la experiencia de usuario. Javier Donoso lo calificó de muy alto. Aseguró que, en la mayoría de las ocasiones, la seguridad está reñida con la usabilidad y que cualquier retraso en el tiempo de entrega del recurso al que se quiere acceder tiene un impacto en su experiencia, aunque sea el factor de autenticación necesario para que ese acceso sea seguro.

Aseguró Eusebio Nieva que la experiencia de usuario se tiene en cuenta, pero que generalmente la seguridad interfiere con la usabilidad, y la única herramienta que tenemos “es intentar simplificar lo más posible los controles, pero manteniendo la seguridad, que es la parte principal de esta ecuación”. Añadió, además, que lo más efectivo es concienciar a los usuarios de que se les está protegiendo y cuáles pueden ser los peligros.

“Está claro que si el usuario es consciente del porqué de aplicar esas medidas de seguridad, es más fácil que llegue a entender la situación, y por lo tanto se acabe acostumbrando antes a la implementación de doble factor de autenticación, por ejemplo”, concluyó Raül Albuixech, para quien es necesario un equilibrio entre la seguridad y las ventajas que consiguen usuarios y empleados pudiendo acceder a todo tipo de recursos desde cualquier parte. ■

Conectando y entendiendo la empresa sin fronteras

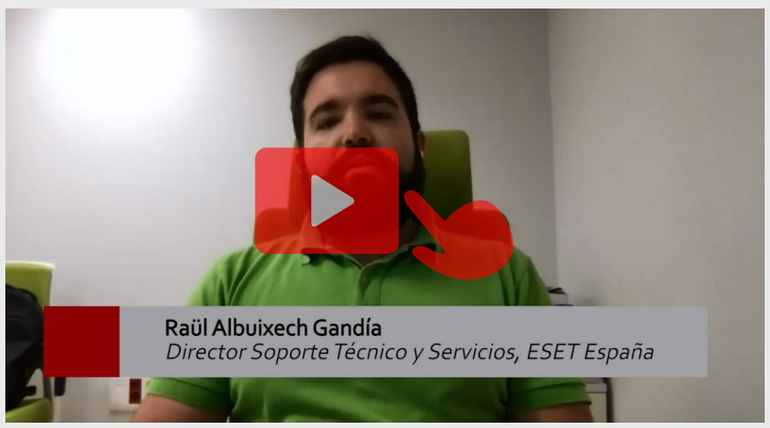
“Queremos que cliente pueda disponer sus servicios 24x7 de forma segura”, A10 Networks

“Las empresas necesitan dotar de seguridad y conectividad de la mejor manera posible a todos los empleados”, Akamai

“Ayudamos a hacer frente a los retos la interconexión de usuarios y dispositivos en el edge”, Aruba Networks

“Nuestra propuesta de valor es facilitar el escalado diferente que tienen los servicios en la nube”, Check Point

“Hemos conseguido una gestión que mejora la calidad de los servicios reduciendo los costes” Citrix



“Proponemos una gestión centralizada y una protección de todos y cada uno de los dispositivos dentro de una red”, ESET

“Las empresas necesitan más información de lo que está ocurriendo en su infraestructura en todo momento”, Sophos

Akamai

235%

Akamai ha observado un aumento del 235% en los ataques de phishing.

¿Tú solución de MFA está a prueba de phishing?

Akamai MFA: Seguridad FIDO2 sin claves de seguridad físicas

Protege tu empresa contra el robo de cuentas de empleados, y filtración de datos con la tecnología MFA de última generación. Convertimos tu smartphone en una llave de seguridad, con una autenticación sencilla, y sin carga de trabajo para tu equipo de TI.

- **Máxima seguridad**
- **Push mobile a prueba de phishing**
- **Gestión de TI unificada y sencilla**

Akamai MFA – pruébalo gratis durante 60 días

Solicita una prueba gratuita en: contact-spain@akamai.com

o si lo prefieres, llámanos al Tel. 91 793 32 43

itTRENDS

RICARD CASTELLET, CHIEF DIGITAL TRANSFORMATION OFFICER DE LABORATORIOS GEBRO PHARMA

“Algunas tecnologías están cambiando cómo hemos entendido el sector salud en los últimos años”

El sector farmacéutico, tan de actualidad estos meses, se encuentra inmerso en un profundo proceso de Transformación Digital, aprovechando las posibilidades que le ofrece la tecnología para rediseñar tanto sus procesos como sus servicios y la relación con sus clientes. Ricard Castellet, Chief Digital Transformation Officer de Laboratorios Gebro Pharma, nos explica los retos que asume el sector farmacéutico, en general, y Gebro Pharma, en particular, en su camino hacia la digitalización, un proceso que redefinirá el sector Salud tal y como lo conocemos ahora.

La industria farmacéutica ha cobrado especial importancia en nuestra sociedad en los últimos tiempos. En España contamos con grandes referentes en este sector clave para la economía, y uno de ellos es Gebro Pharma, dedicada al desarrollo y comercialización de medicamentos de prescripción médica y hospitalaria. Perteneciente al grupo austriaco del mismo nombre, en nuestro país tiene

ENTREVISTA. Ricard Castellet, de Gebro Pharma.

su sede Barcelona desde 2002 y cuenta con 150 empleados. El año pasado creció un 6,7% y ha sido reconocida, por segundo año, como una de las Grandes Empresas para Trabajar en España. Recientemente se ha incorporado Ricard Castellet, como responsable de transformación digital de la compañía, un nuevo rol dentro de la compañía.

"En un proceso amplio en el tiempo y con diferentes horizontes, queremos transformar elementos culturales, maneras de trabajar, potenciando la omnicanalidad en la relación con nuestro cliente objetivo, e ir incorporando nuevos modelos de negocio paralelos y complementarios al actual, como capas de servicios digitales sobre el producto farmacéutico. Queremos potenciar el valor de Gebro Pharma hacia el cliente", explica Castellet sobre su misión.

Gebro Pharma, como otras empresas del sector farmacéutico, "pisó el acelerador al inicio de la pandemia, porque, además de los numerosos efectos muy negativos, ha contribuido a incrementar la velocidad de la aceleración digital en las compañías de este sector. Cuando me incorporé en mayo, llevaban un año y medio acelerando estos procesos. Con la pandemia quedó claro que la visita comercial, tradicional hasta la fecha, quedó interrumpida, con lo que el cambio era inevitable, lo que implica nuevas formas de trabajar, de relacionarnos, poner el dato en el centro, pensar nuevos modelos de negocio... repensar, en el fondo, toda la industria, pero de una manera ordenada y con lógica".

"Hay un cambio de paradigma, y el paciente podrá controlar su salud desde un dispositivo móvil, por ejemplo, o desde otros interconectados que le ofrecerán información preventiva de diferentes patologías"

Para afrontar el reto, "hemos dibujado tres escenarios diferentes, cada uno más sofisticado que el anterior. El primero, optimizar lo que tenemos, con un foco muy importante en marketing y ventas, y habilitar la cultura digital de la compañía, dando una oportunidad a todo el mundo de adquirir competencias digitales para poder desarrollar una nueva forma de trabajar, y empezando a explorar lo que en el futuro serán nuevas líneas de negocio. En el segundo escenario afrontamos el crecimiento con una estrategia dirigida por el dato, poniéndolo en el centro para entender a nuestros usuarios, con el fin de mejorar nuestra interacción con ellos y poder hacerles propuestas de valor, científico, formativo, cada vez más adecuadas a lo que realmente necesitan. El tercer escenario, más complejo, pasa por fortalecer esas nuevas líneas de negocio, basadas en servicios digitales, con un impacto directo con el paciente, sin olvidar nunca nuestro core business, los fármacos que curan a personas, pero introduciendo una sofisticación con servicios digitales capaces de mejorar la atención, la fidelización, la información y la personalización del fármaco con los pacientes".

ESPAÑA MARCA EL RITMO DE LA DIGITALIZACIÓN DEL GRUPO

Pese a tratarse de un grupo internacional, "contamos con mucha autonomía. Tenemos muy buena relación, pero cada filial tiene un gran nivel de autonomía, y, en el caso de España, nos posicionamos como la punta de lanza a nivel digital, rompiendo ciertas barreras en el camino hacia el futuro. Somos innovación en el grupo y los que tenemos la visión más clara".

A nivel tecnológico, "hay algunos impactos que están cambiando cómo hemos entendido el sector salud en los últimos años. No solo es que el paciente se pone en el centro y toma el mando, sino que tecnologías como IA, Machine Learning, Big Data, Cloud, Ciber-

seguridad, Blockchain... permitirán cambiar el marco que ha definido esta industria, que se dedica más a la prevención que a la cura. Que va más a personalizar con cada paciente, con un diagnóstico diferente en función de la información que tengamos de él. Hay un cambio de paradigma, y el paciente podrá controlar su salud desde un dispositivo móvil, por ejemplo, o desde otros interconectados que le ofrecerán información preventiva de diferentes patologías. Cada usuario contará con dispositivos personales que cuidarán de su salud".

UN CAMBIO PROFUNDO EN EL SECTOR

Tal y como apunta Ricard Castellet, "vivimos un momento apasionante, que podemos comparar con el vivido hace unos años por el sector financiero y las Fintech. Sin ser lo mismo, la experiencia está conectada, con un impacto directo en la relación entre el paciente y el personal ciudadano, y con un flujo de datos y conocimientos que no habíamos visto hasta ahora". Tras más de 20 años inmerso en la evolución digital, "hemos visto distintas olas que han dejado huella en diferentes industrias. La evolución del nuevo marco digital ha ido evolucionando, pero la de ahora es muy significativa, porque llegará a sectores muy regulados y con un gran impacto en la sociedad: Salud, Educación, Energía, Movilidad... Estas industrias sufrirán un cambio tan radical como otros lo han sufrido otros, y hemos de hacerlo muy bien porque nos jugamos el futuro de nuestra sociedad".

"Con la pandemia, la visita comercial quedó interrumpida, con lo que el cambio era inevitable, lo que implica nuevas formas de trabajar y de relacionarnos"

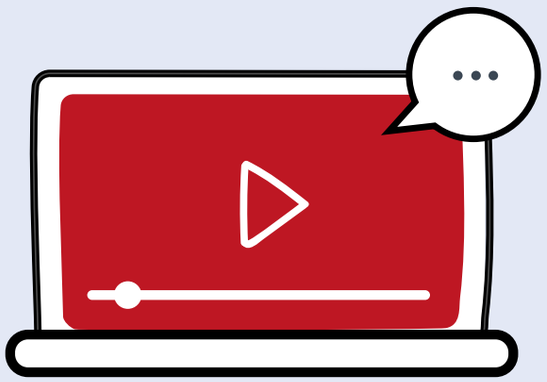
Y en este cambio será protagonista la IA, que, a partir de la información, "podrá proponer soluciones y valores para nuestro día a día, independientemente del sector al que miremos. Estamos en un momento en que el software impacta en nuestro día a día y nos ayuda en la toma de decisiones. Pero, como hay riesgos, hemos de proteger la privacidad, por ejemplo, como ciudadanos, pero, si lo hacemos bien, la tecnología nos hará una sociedad mejor. Afrontamos los mayores retos de nuestra historia, y hemos de aplicar estas tecnologías para tener un mundo más sostenible y mejor". ■

Sobre Gebro Pharma

Gebro Pharma, que se define a sí misma como el Laboratorio de los Alpes, fue fundada en 1947 en Viena y abrió su filial española a finales de 2002. Se trata de una firma dedicada al desarrollo y comercialización de medicamentos de prescripción médica y hospitalaria, que cuenta con 150 empleados, y que, tal y como señala en sus valores corporativos, su máxima es "intentar optimizar lo que ya existe, identificar posibles mejoras y traducirlas en soluciones", lo que lleva a la firma a emprender el camino de la Transformación Digital.

Claves para una estrategia multicloud de éxito

Regístrate ahora a este taller online en el que abordaremos la realidad de los entornos multicloud y cómo adoptar una estrategia de éxito. Se ofrecerá una introducción a las distintas soluciones que pueden ayudar a implementar una solución de cloud privada, la hibridación de cargas a nubes públicas o soluciones a desplegar en el Edge. Veremos los retos a los que se enfrentan todo tipo de organizaciones y cómo ayudar a solventarlos.



Tendencias de ciberseguridad 2022.
La ciberinteligencia entra en escena

Los ciberataques llevan creciendo en cantidad y en sofisticación desde hace años, y nada hace pensar que el año próximo vaya a cambiar la tendencia. Los ciberdelincuentes se esmeran cada vez más, han creado un negocio extremadamente rentable y siguen estando lejos de las autoridades. Llevamos tiempo hablando de la in-seguridad móvil y mucho más del phishing, que sigue estando presente en un altísimo porcentaje de los ciberataques con éxito. ¿Será 2022 el año de hacerle frente?

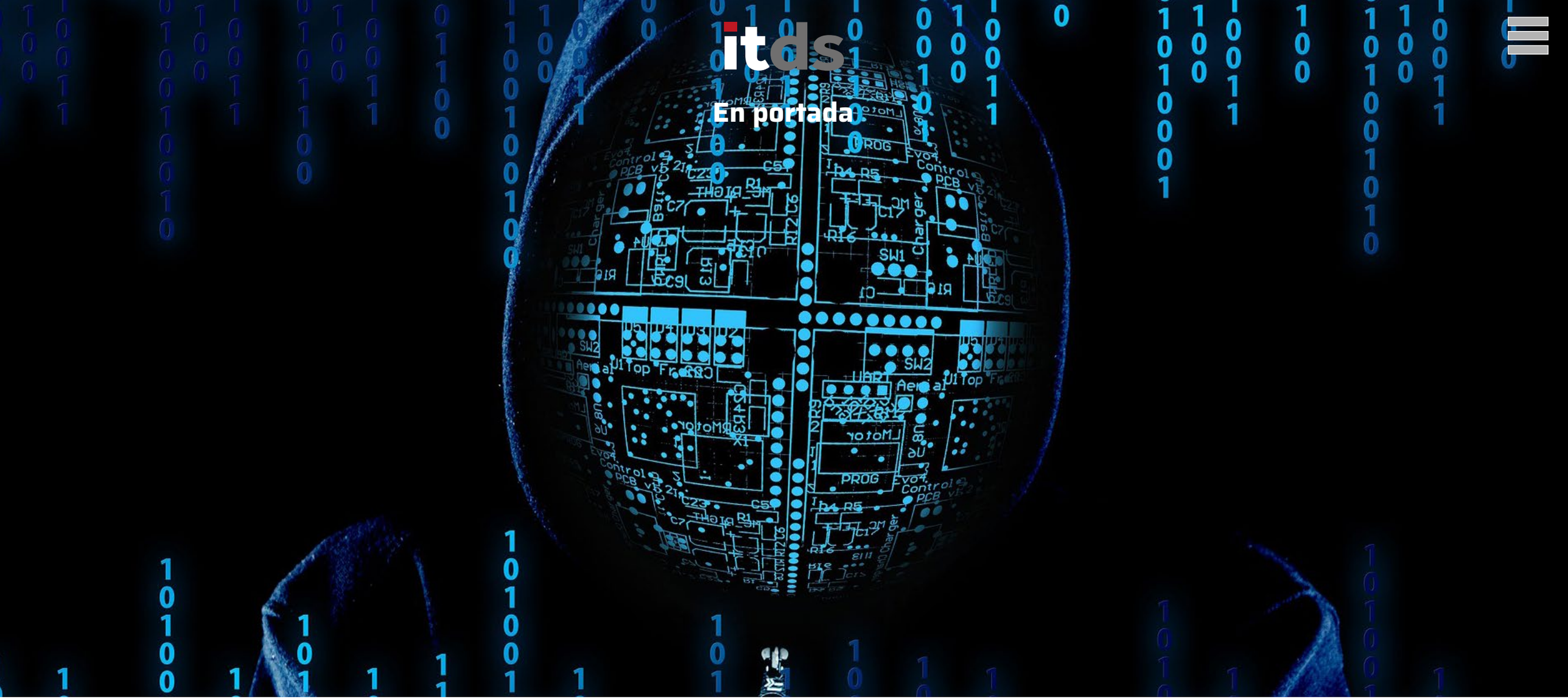
Tendencias IT 2022:
¿qué impactará en la TI corporativa?

¿Cómo se ha comportado la TI corporativa en 2021? ¿Qué tecnologías han asumido el papel de transformadoras? ¿Cuál es el estado de la transformación digital de las empresas? ¿Cómo continuarán evolucionando en 2022? Todas ellas serán cuestiones a abordar en esta sesión online junto a expertos del mercado y la empresa.

Máquinas.

Tus mejores aliados. Tus peores enemigos

En los últimos años, hemos sido testigos del rápido crecimiento de las máquinas y los dispositivos conectados a Internet en la empresa. Desde el IoT y los dispositivos móviles hasta las aplicaciones definidas por software, instancias en la nube, contenedores e incluso el código que se ejecuta dentro de ellos, las máquinas ya superan en número a los humanos. Según el Informe anual de Internet de Cisco, para 2023, habrá 29,3 mil millones de dispositivos en red a nivel mundial, frente a los 18,4 mil millones en 2018. Más de 10 mil millones de dispositivos nuevos en solo cinco años.



Al igual que las identidades humanas en las que confiamos para acceder a las aplicaciones y dispositivos que usamos todos los días (por ejemplo, contraseñas, multifactor, etc.), las máquinas requieren un conjunto de credenciales para autenticarse y conectarse de forma segura con otros dispositivos y aplicaciones en la red. A pesar de su importancia crítica, estas “identidades de máquina” a menudo no se administran ni protegen.

En su informe Hype Cycle for Identity and Access Management Technologies de 2020 Gartner introdujo una nueva categoría: Gestión de identidades de máquinas, lo que reflejó creciente importancia de administrar claves criptográficas, certificados, claves SSH y otras identidades no humanas. Es esencial que las identidades de las máquinas estén debidamente autenticadas y administradas, asegurando que el acceso solo se otorgue a usuarios o máquinas legítimos sin importar el número de identidades involucradas o la complejidad de la red de las instalaciones.

La identidad de una máquina es mucho más que un número de identificación digital. Conlleva una serie de credenciales autenticadas que certifican que está autorizada a tener acceso a determinados recursos. Si las anteriores estrategias de seguridad se centraban en proteger la organización en el perímetro, ahora es necesario proteger cada conexión y cada comunicación que esté asociada de alguna manera con cada negocio.

Es importante comprender que muchas de estas intersecciones se caracterizan por la automatización; no hay interacción humana durante la comunicación de máquina a máquina, y esta es una de las razones clave por las que la gestión de la identidad

Los principales desafíos que se interponen en el camino de establecer una estrategia para toda la empresa son los cambios excesivos y la incertidumbre (40%) así como la falta de personal cualificado (40%)

WHAT IS MACHINE IDENTITY MANAGEMENT?

CLICAR PARA VER EL VÍDEO

de las máquinas se ha convertido en un componente fundamental de las estrategias de IAM para las organizaciones de todo el mundo. Las organizaciones necesitan, más que nunca, estrategias y tácticas para implementar un sistema organizado de identidades digitales que asegure, gobierne y verifique de manera confiable las comunicaciones de máquina a máquina.

Mayor superficie de ataque

El auge de estas máquinas ha ampliado la superficie de ataque y la mayoría de las empresas no son conscientes del riesgo. Según datos de Forrester, las identidades de las máquinas están creciendo al doble de la tasa de las identidades humanas; Gartner, por su parte, no solo ha reconocido la Gestión de identidades de máquinas como una nueva categoría dentro de la Gestión de identidades y accesos (IAM) sino que la incluyó entre Las 8 principales tendencias de seguridad para este año.

Los ciberataques que aprovechan las identidades de máquinas comprometidas o mal administradas son cada vez más comunes. Dichos ciberataques aumentaron en más del 430% entre 2018 y 2019, mientras que los ciberataques y las APTs que abusan de ellos aumentaron un 1,600% en los últimos cinco años, según un informe de Venafi de 2020. En el ataque a SolarWinds, los delincuentes utilizaron certificados digitales diseñados para proteger la cadena de suministro de software. Un certificado digital vencido retrasó el descubrimiento de la violación de Equifax en 2017. Las claves de cifrado robadas permitieron a los atacantes robar datos de clientes de Marriott en 2018 y los atacantes utilizaron una clave SSH de GoDaddy robada

Impulsando la transformación de la IAM

Identifica Forbes cinco elementos que están impulsando la transformación de la gestión de identidades y accesos (IAM):

- 1. Se priorizan estrategias cloud y Zero Trust. Las claves criptográficas y los certificados respaldan el crecimiento rápido y escalable, lo que, a su vez, respalda una mejor seguridad en la nube y las mejores prácticas de confianza cero.
- 2. Vencimiento de certificados. Cuando se gestiona de forma inadecuada, la adopción de claves y certificados puede provocar su suspensión. La vida útil de los certificados SSL/TSL continúa disminuyendo, lo que significa que los certificados se emiten con una vida útil limitada. Si los certificados no se renuevan en su fecha de vencimiento predefinida, el certificado no se autentica y provoca una interrupción que puede ser costosas de remediar (un promedio de 5.600 dólares por minuto, según Gartner), pueden causar períodos desconocidos de tiempo de inactividad del sistema y pueden llevar a clientes insatisfechos.
- 3. La falta de visibilidad y gobernanza de las identidades de las máquinas está aumentando los riesgos de seguridad. Los volúmenes de certificados y claves cada vez mayores no solo crean un problema de gestión; también están creando un problema de gobernanza. Es imposible proteger claves y certificados que no se rastrean correctamente. La gestión inadecuada hace que las empresas sean más vulnerables a incidentes de seguridad, auditorías fallidas y multas por incumplimiento.
- 4. Las estrategias de IAM están evolucionando para priorizar las identidades de las máquinas. Tanto si está preparado para ello como si no, su estrategia de IAM debe evolucionar y adaptarse para dar cabida a certificados criptográficos, claves y secretos digitales.
- 5. La escasez de profesionales impide que la gestión de las identidades de las máquinas se aborden adecuadamente. La mayoría de los responsables de TI se han visto paralizados por las limitaciones de recursos.

para robar casi 30.000 credenciales SSH de sus clientes en 2020.

La gestión de las identidades de las máquinas no solo hace referencia a la visibilidad de las mismas, sino a los certificados. Aseguran los expertos que en muchas ocasiones los problemas surgen porque tecnologías como X.509, a pieza central de la infraestructura de clave pública, y los sistemas de administración de claves SSH permanecen en silos y, a menudo, son incompatibles con los entornos de nube modernos, lo que dificulta mantenerse al tanto de los certificados caducados y olvidados.

En los últimos años, los certificados caducados han provocado muchas interrupciones del servicio y de sitios web de alto perfil

THE NEXT-GEN MACHINE IDENTITY MANAGEMENT REPORT

CLICAR PARA VER EL VÍDEO

Los certificados TLS tienen una vida útil decreciente, pasando de cinco años en 2012 a solo un año en 2020. Las claves SSH nunca caducan, rara vez se eliminan de los entornos y las mismas claves se utilizan a menudo para acceder a varias máquinas. Y las claves de firma de código a menudo no están protegidas porque son generadas y utilizadas por desarrolladores, y cada vez más por procesos automatizados que los humanos nunca podrían seguir. Según una encuesta de Forrester de 2018, a más del 50% de las organizaciones les resulta difícil proteger las identidades de sus máquinas.

Incluidas en las identidades de las máquinas (a diferencia de las identidades humanas) están las cargas de trabajo (es decir, contenedores, aplicaciones, servicios) y dispositivos (dispositivos móviles, computadoras de escritorio, dispositivos IoT/OT).

Los atacantes pueden aprovechar las identidades de máquinas desprotegidas para obtener acceso a las redes y pivotar a través de múltiples

El 61% de las empresas están implementando más claves criptográficas y certificados digitales en toda la empresa

sistemas una vez dentro. También brindan a los atacantes la oportunidad de crear puertas traseras persistentes y distribuir malware a usuarios de la red desprevenidos. El malware basado en SSH, como Trickbot, permite a los atacantes infectar múltiples objetivos, pasar a otras áreas de las redes objetivo y robar claves SSH adicionales. Los certificados TLS robados también se utilizan en ataques man in the middle y exfiltración de datos. Y dado que permiten a los atacantes hacerse pasar por entidades legítimas, los certificados fraudulentos también les permiten evadir los mecanismos de defensa existentes.

Investigaciones recientes han desvelado que el 61% de las empresas están implementando más claves criptográficas y certificados digitales en toda la empresa, aunque solo el 40% de los encuestados dijo tener una estrategia empresarial para administrar la criptografía. Ambas estadísticas son alarmantes y refuerzan la importancia de una estrategia moderna de gestión de identidad de máquinas en toda la empresa como parte de una estrategia de IAM.

Claves y certificados

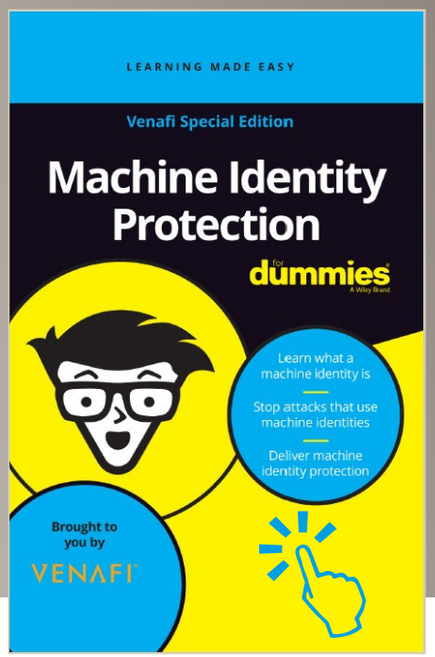
Las máquinas utilizan conexiones cifradas para establecer la confianza en todo tipo de transacciones digitales. Para hacer esto, usan certificados digitales y claves criptográficas para validar la legitimidad de ambas máquinas que se comunican.

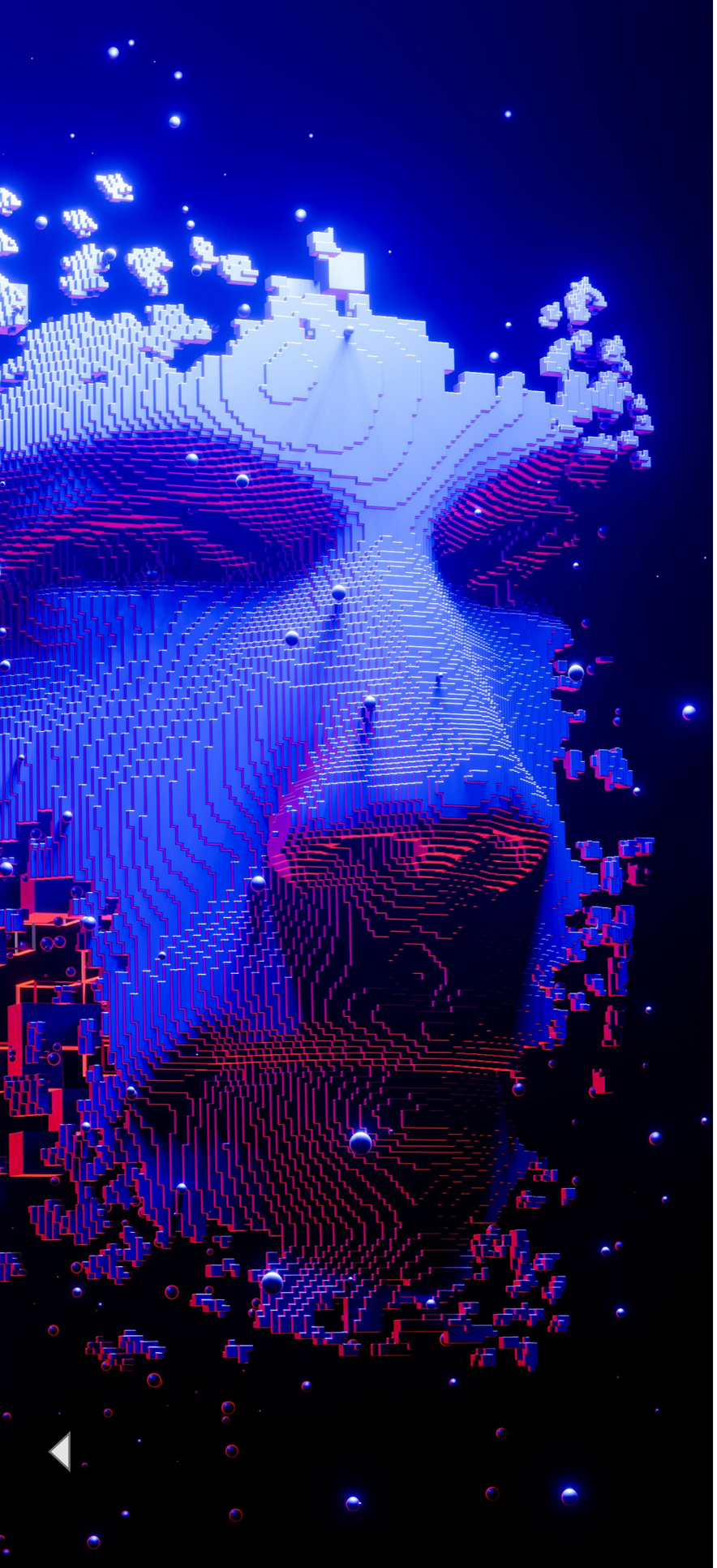
Ejemplo de ellos son los Secure Sockets Layer (SSL) o Transport Layer Security (TLS), utilizando fundamentales para la seguridad de las transacciones web, como la banca online y el comercio electrónico. Estos certificados permiten una conexión cifrada entre un navegador web y un servidor web.

it whitepapers

MACHINE IDENTITY PROTECTION FOR DUMMIES

Las máquinas están impulsando mejoras sin precedentes en la eficiencia empresarial, la productividad, la agilidad y la velocidad. Pero las máquinas no funcionan de forma aislada. Necesitan estar en constante comunicación con otras máquinas. Este documento propone siete pasos a seguir para que una organización proteja todas las identidades de máquinas que las empresas utilizan.





El gran reto de la gestión de la identidad de las máquinas

A medida que las redes se vuelven cada vez más grandes y elaboradas, rastrear quién o qué está en ellas inevitablemente se vuelve más difícil.
Las organizaciones se enfrentan a una serie de desafíos en la gestión de las identidades de las máquinas dentro de su organización, y el seguimiento de los certificados y las claves en las diversas áreas de su infraestructura de TI actualmente no es nada fácil.
Cerca de las tres cuartas partes enfrentan actualmente dificultades para realizar un seguimiento de estos certificados y claves en cada uno de los siguientes: tecnología operativa / infraestructura de IoT (78%), infraestructura en la nube (76%), infraestructura de TI local (75%) e infraestructura en contenedores (74%).
Es probable que estas dificultades signifiquen que las organizaciones no pueden rastrear certificados y claves tan eficientemente como deberían, o incluso que no pueden rastrear algunos de ellos en absoluto. De hecho, más de las tres quintas partes (61%) de las organizaciones no tienen pleno conocimiento de todos los certificados y claves en todos sus activos digitales, lo que significa que no pueden rastrear las identidades de todas las máquinas en sus redes de TI.

Si los certificados utilizados para proteger HTTPS no están protegidos, los ciberdelincuentes pueden obtener acceso a estas identidades críticas de las máquinas para espiar el tráfico cifrado o hacerse pasar por un sistema confiable.

Secure Shell (SSH) se utiliza a menudo para proteger el acceso del administrador del sistema a la máquina para las tareas de rutina, pero también para asegurar la automatización máquina a máquina de funciones comerciales críticas, como la activación automática de operaciones y transferencias de archivos de rutina. Las claves SSH garantizan que solo los usuarios y las máquinas de confianza tengan acceso a datos y sistemas de red confidenciales.

Generalmente el software se firma con un certificado para verificar su integridad del software. Los usuarios confían implícitamente en los productos cuando están firmados por certificados de firma de código de un editor confiable, creyendo que el software firmado es seguro de implementar. Cuando se utilizan correctamente, estos certificados sirven como una identidad de máquina que autentica el software.

La criptografía de clave pública (o criptografía asimétrica) se utiliza para proteger las comunicaciones de la máquina. Debido a que la criptografía de clave pública sirve como base para las comunicaciones seguras en Internet, y debido a que la mayoría de las organizaciones no protegen muy

bien estos activos de seguridad críticos, los ciberdelincuentes dedican mucho esfuerzo a intentar comprometer claves y certificados. Un certificado digital también se denomina certificado de clave pública. La mayoría de los certificados que se utilizan en la actualidad se basan en el estándar internacional X.509.

Automatización

La gestión de identidad inadecuada no solo hace que las empresas sean más vulnerables a los ciberdelincuentes, el malware y el fraude, sino que también expone a las organizaciones a riesgos relacionados con la productividad de los empleados, problemas de experiencia del cliente, deficiencias de cumplimiento y más. Si bien no existe una solución de autenticación y cifrado más sólida y versátil que la identidad digital basada en PKI, el desafío para los equipos de TI ocupados es que implementar y administrar certificados manualmente requiere mucho tiempo y puede resultar en un riesgo innecesario si se comete un error.

Ya sea que una empresa implemente certificados para habilitar la autenticación de dispositivos para una sola red de control o administre millones de certificados en todas sus identidades de dispositivos en red, el proceso de emisión, configuración e implementación de certificados puede ser abrumador. La gestión manual de identidades de máquinas no es sostenible ni escalable. Además, la administración manual de certificados pone a las empresas en riesgo significativo de que los certificados olvidados caduquen inesperadamente. Esto puede provocar interrupciones relacionadas con los certificados, fallos críticas de los sistemas comerciales y violaciones y ataques de seguridad.

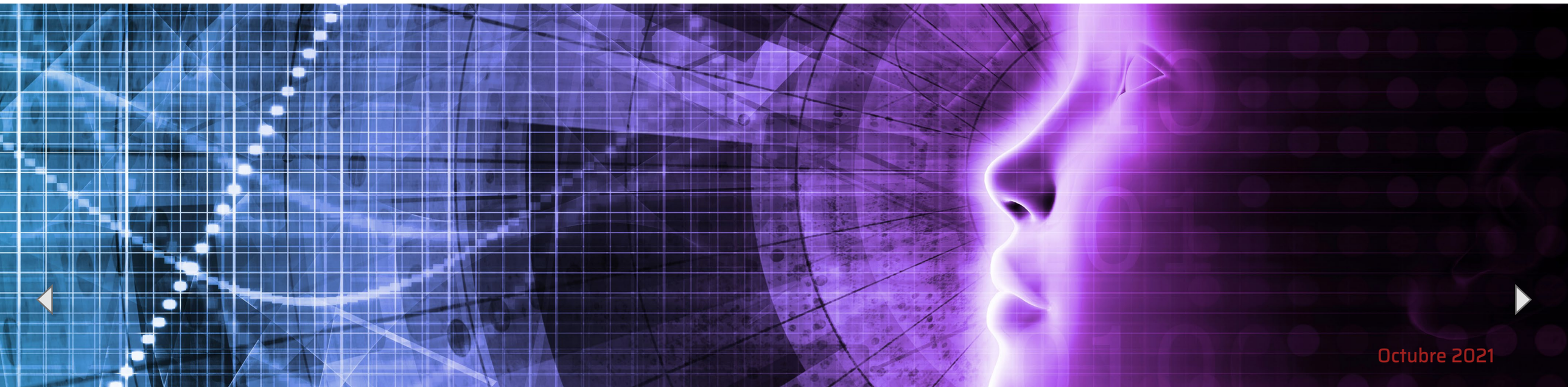
En los últimos años, los certificados caducados han provocado muchas interrupciones del servicio y del sitio web de alto perfil. Estos errores han costado miles de millones de dólares en ingresos perdidos, sanciones contractuales, juicios y el costo incalculable de la pérdida de la buena voluntad del cliente y la reputación de la marca empañada.

Situación de mercado

A pesar de que existe una mayor conciencia en la protección de las identidades de las máquinas, un estudio realizado por Ponemon y Keyfactor recogió que la mayoría las empresas no tiene una estrategia para gestionar la criptografía y las identidades de las máquinas, o tienen una estrategia limitada que se aplica solo a determinadas aplicaciones o usos.

Los principales desafíos que se interponen en el camino de establecer una estrategia para toda la empresa son los cambios excesivos y la incertidumbre (40%) así como la falta de personal cualificado (40%).

Los encuestados también identificaron los desafíos en la administración de las identidades de las



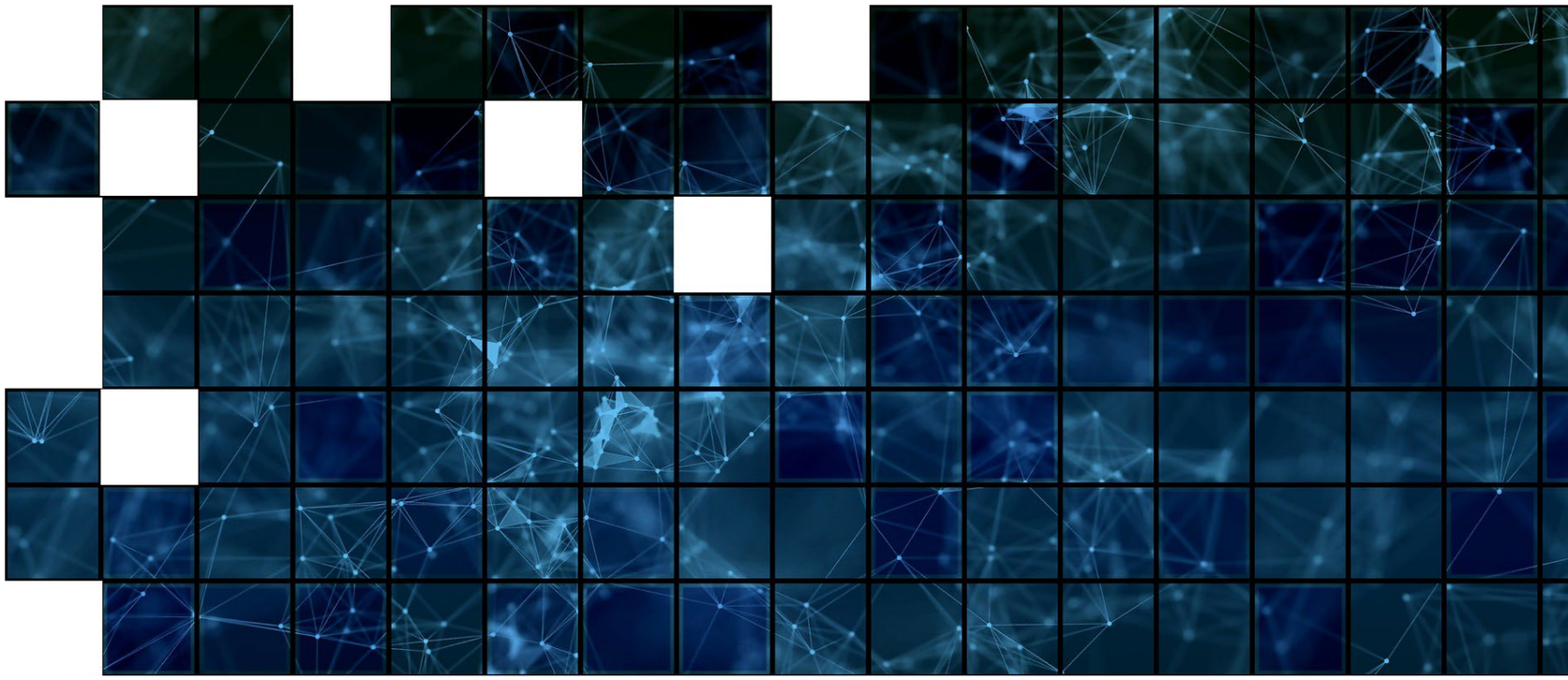
máquinas, como el aumento de la carga de trabajo y el riesgo de interrupciones causadas por la vida útil más corta de los certificados SSL/TLS (59%), la mala configuración de claves y certificados (55%) y el no saber exactamente cuántas claves y certificados tiene la organización (53%).

Un factor importante de estos desafíos es la reciente reducción en la vida útil de todos los certificados SSL/TLS de confianza pública en aproximadamente la mitad, de 27 meses a 13 meses, desde el 1 de septiembre de 2020. Vale la pena señalar que el impacto real de este cambio probablemente no se hará realidad hasta los próximos meses y años.

Si bien muchas tendencias están impulsando las implementaciones de PKI, claves y certificadas, las dos tendencias más importantes son los servicios basados en la nube (52%) y la estrategia de seguridad Zero-Trust (50%). Otras tendencias notables incluyen la fuerza de trabajo remota (43%) y los dispositivos de IoT (43%).

El estudio también recoge que, en general, los encuestados coinciden en que administrar y proteger la identidad de cada máquina es fundamental. Dicho esto, los certificados SSL / TLS se consideraron ampliamente las identidades de máquina más importantes para administrar y proteger, según el 82% de los encuestados.

El método más común para implementar PKI empresarial es una autoridad de certificación (CA) interna con raíz privada (42%). Sin embargo, muchas organizaciones también aprovechan las CA emisoras integradas, como Kubernetes o HashiCorp Vault (29%), las CA privadas que se ejecutan en una nube pública (23%) y los servicios de PKI gestionados externamente (23%).



En 2020 Gartner reconoció la Gestión de identidades de máquinas como una nueva categoría dentro de la Gestión de identidades y accesos (IAM)

A pesar de la tarea titánica de gestionar las identidades de máquinas, muchas organizaciones todavía confían en un mosaico de herramientas proporcionadas por los proveedores de CA (44%), hojas de cálculo (40%) y soluciones internas (33%) para administrar Certificados digitales. Solo alrededor de un tercio (36%) utiliza una solución de gestión del ciclo de vida de certificados dedicada.

Por cierto que el 88% de las organizaciones informaron haber experimentado al menos una interrupción no planificada debido a certificados caducados en los últimos 24 meses. Otro 41% asegura haber experimentado cuatro o más interrupciones. Según los encuestados, la probabilidad

Los certificados TLS tienen una vida útil decreciente, pasando de cinco años en 2012 a solo un año en 2020

de que ocurran estos cortes no planificados en los próximos 24 meses es del 40%, frente al 25% del estudio de 2020.

Según los hallazgos, las organizaciones utilizan ampliamente las credenciales SSH, como contraseñas, claves y certificados. Sin embargo, el 53% no tiene un proceso de administración centralizado, lo que provoca que menos de la mitad de las organizaciones tengan un inventario preciso de credenciales SSH en toda su infraestructura (40%).

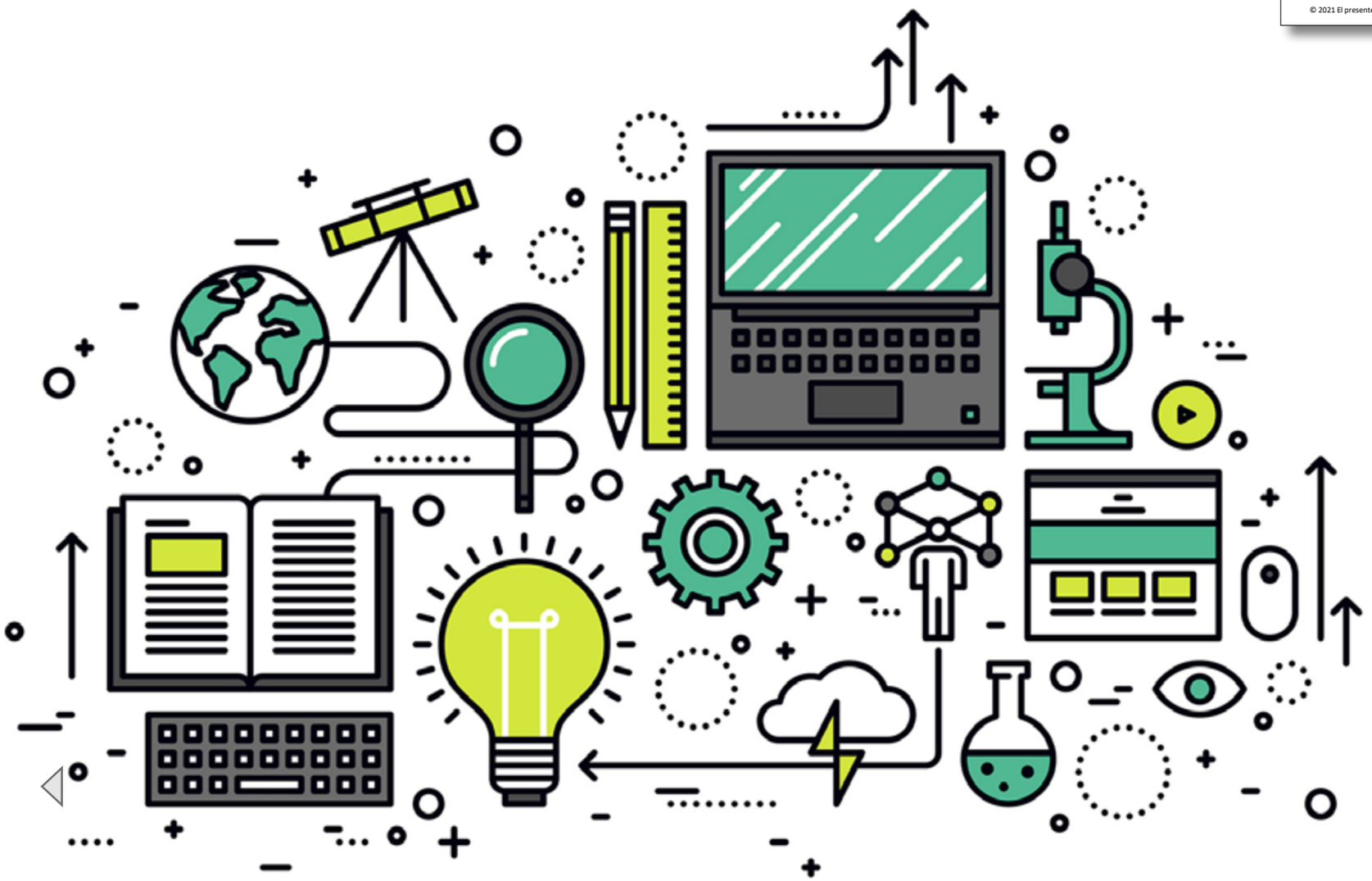
En comparación con otros incidentes relacionados con la identidad de las máquinas, como interrupciones no planificadas de certificados o robo y uso indebido de claves y certificados, las fallas de auditoría se consideran las más frecuentes y graves, según el 75%. En promedio, las organizaciones experimentaron aproximadamente cinco auditorías fallidas o incidentes de cumplimiento debido a una gestión de claves insuficiente en los últimos 24 meses.

De cara al futuro, las organizaciones están tomando medidas para actualizarse a la próxima generación de herramientas de gestión de identidad de máquinas. Según un estudio reciente la gran mayoría está planeando o implementando actualmente flujos de trabajo automatizados de Gestión de Identidad de Máquinas (96%), la capacidad de gestionar ciclos de vida de certificados en modelos de implementación híbridos (95%) o Gestión de Identidad de Máquinas como Servicio (95%).

Enlaces de interés...

- W Estado de la gestión de identidades de máquinas, 2021
- W Informe de gestión de identidad de máquinas de última generación
- I Keyfactor y PrimeKey se fusionan
- I Credenciales de empleados de empresas de gaming se venden en la Dark Web

Tendencias tecnológicas de alto impacto para tu negocio



¡Descárgatelo ahora!

itTRENDS

Un año acercando a la mujer al mundo de la ciberseguridad

Este mes de octubre se cumple un año del nacimiento de Women4Cyber Spain, el capítulo español de la Fundación Europea sin ánimo de lucro Women4Cyber, que busca atraer el talento femenino y potenciar la presencia de las mujeres en el mercado de la ciberseguridad.

DANIELA KOMINSKY

MIEMBRO DEL CONSEJO WOMEN4CYBER SPAIN

Country Manager de Cymulate para Spain, Portugal and Italy, Daniela Kominsky es una ejecutiva con más de 20 años de experiencia en desarrollo empresarial y marketing en el sector de sistemas y tecnología de la información. Durante los últimos 10 años ha liderado importantes iniciativas en el campo de la ciberseguridad, promoviendo el comercio entre empresas israelíes y españolas, actuando como puente entre ambos países. Comprometida con la innovación y el emprendimiento, ha trabajado con INCIBE para desarrollar el ecosistema de emprendimiento en ciberseguridad en España, y participa activamente como conferenciante sobre estos temas. Además, Daniela es miembro del Consejo de Administración de la Cámara de Comercio Hispano-Israelí y miembro del Consejo de Women4Cyber España.

A nivel profesional, la ciberseguridad sufre las mismas carencias que todo el sector de la tecnología, como es la falta de referentes femeninos

La asociación Women4Cyber Spain (W4C Spain), que inicialmente estaba integrada por nuestra presidenta, Eduvigis Ortiz, y la junta directiva compuesta de 15 mujeres referentes en el mundo de la seguridad y el sector de las TIC, cuenta actualmente con 10 colaboradoras asiduas y más de 80 asociados, y ha firmado acuerdos de colaboración con empresas de reconocido prestigio en el ámbito de las TIC afines con el compromiso de favorecer el desarrollo y la integración de las mujeres en la ciberseguridad, como es el caso de Accenture, Atalanta, Bidaidea, Cipher, Mnemo y S21Sec.

La importancia de la formación para atraer talento

Uno de los retos que marcan la línea de actuación de Women4Cyber Spain es la promoción de programas de formación a todos los niveles en ciberseguridad y tecnología para la mujer y en él se ha volcado buena parte de las acciones de la junta directiva, que ha cerrado acuerdos con entidades de reconocido prestigio en España como ISMS Forum (Asociación Española para el Fomento de la Seguridad de la Información) dedicada a promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España, y la Fundación ASTI, un referente en la educación y el desarrollo del talento digital. Dichos acuerdos, le han permitido a las asociadas acceder a becas de formación y oportunidades laborales.

A nivel profesional, la ciberseguridad sufre las mismas carencias que todo el sector de la tecnología, como es la falta de referentes femeninos. Las niñas y las jóvenes no consideran que las carreras STEM sean un camino para ellas, lo ven como algo ajeno; de ahí que W4C Spain vuelque buena parte de sus esfuerzos en poner en valor el papel de la mujer en las TIC, dado que “el principal obstáculo es la falta de visibilidad del trabajo de muchas mujeres, que no gozan del reconocimiento necesario, lo que agudiza la falta de referentes; de manera que desde la asociación trabajamos para crear una cantera”, comenta Eduvigis Ortiz, presidenta de W4C Spain.

Al mismo tiempo, a lo largo de estos casi doce meses de andadura del capítulo español de Women4Cyber, se han realizado periódicamente encuentros con diferentes profesionales, todas ellas líderes en su ámbito de actuación, para dar a

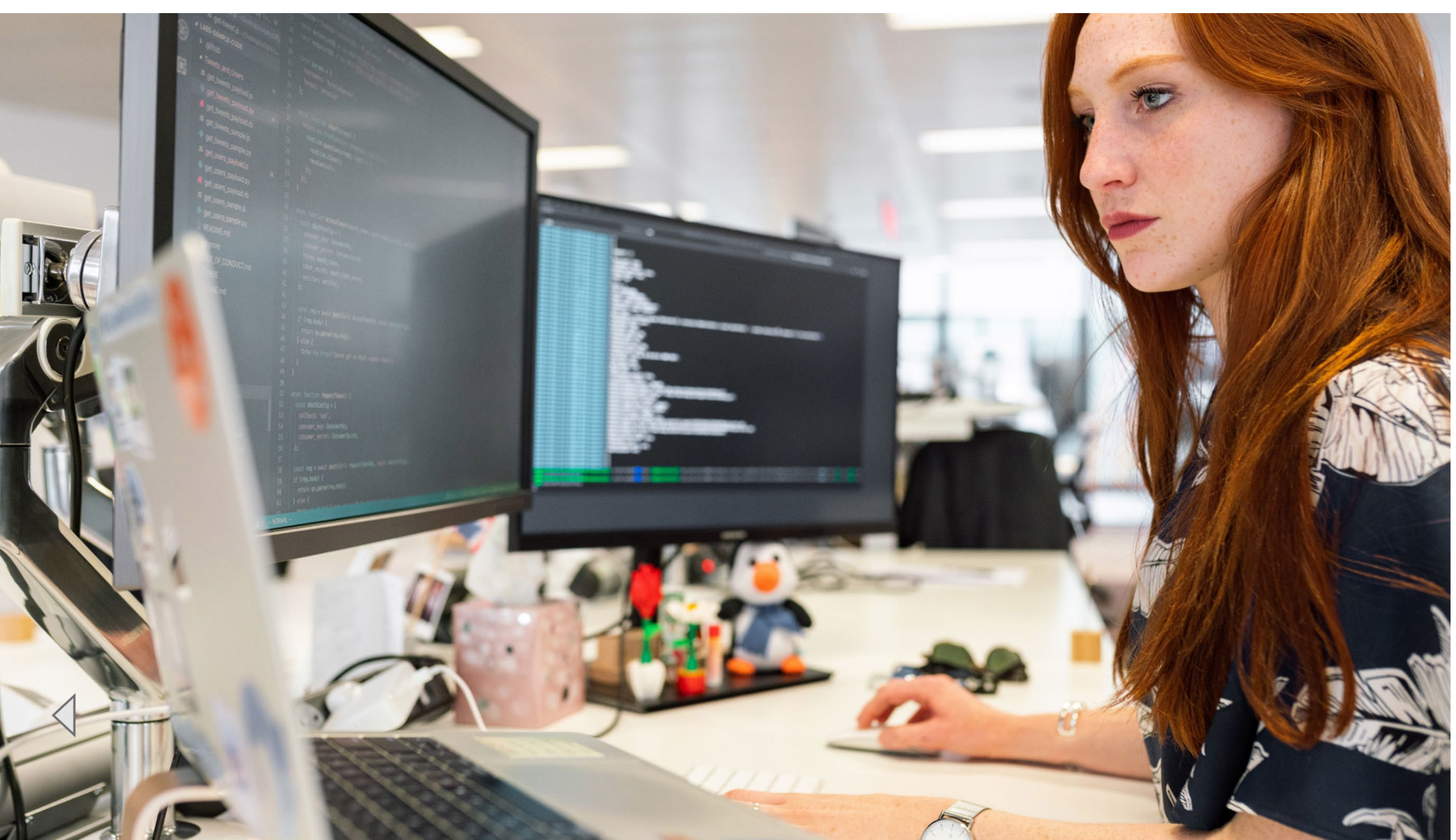
conocer la ciberseguridad desde distintos prismas, abordando temáticas como las armas del derecho para luchar contra la ciberdelincuencia, la comunicación y su papel en la ciberseguridad o la importancia de la seguridad en la transformación digital.

Primer Programa de Mentoring

Además de la formación, otro de los pilares de la propuesta de W4C Spain para potenciar el papel de la mujer en la ciberseguridad es impulsar su crecimiento a nivel laboral en este sector y, por extensión, en el sector de las Tecnologías de la Información y las Comunicaciones, dado lo unidos que están los dos ámbitos profesionales.

La asociación lanzó su primer Programa de Mentoring 2021 el pasado mes de junio, que tendrá una duración de seis meses y está pensado para contar con un máximo de 40 mentoras y otras tantas mentees. Aunque estamos en una asociación de mujeres, en W4C Spain se ha abierto el papel del mentor también a los hombres con el objetivo de que aporten su experiencia.

La asociación lanzó su primer Programa de Mentoring 2021 el pasado mes de junio



El reto del Programa de Mentoring es doble y bidireccional, se trata de abordar un proceso donde ambas partes extraigan soluciones, técnicas y buenas prácticas para el día a día. Es una excelente manera de desarrollar el talento con beneficios para la mentora y para la mentee, donde la persona de mayor experiencia asume la responsabilidad de guiar a la otra en la consecución de sus objetivos profesionales y, todo ello, mediante el establecimiento de sinergias que permitan, directa o indirectamente, dotar de una mayor visibilidad a la mujer en el mundo de la ciberseguridad dentro de la sociedad española.

El balance de Women4Cyber Spain tras casi un año de andadura es altamente positivo, dada la buena acogida que ha tenido la asociación dentro del sector de las TIC y, muy especialmente, de la ciberseguridad. W4C Spain ha contribuido a reducir la brecha de profesionales en este mundo tecnológico potenciando el talento femenino. Nos queda un largo camino por delante, pero vamos en la buena dirección.

Enlaces de interés...

- W4C Spain
- Programa de Mentoring

it User
TECH & BUSINESS

nº 71
OCTUBRE 2021

El asalto de los Chromebooks al mercado profesional

La eclosión del puesto de trabajo inteligente, a debate

MARIO VELARDE BLEICHNER

GURÚ EN CYBERSEGURIDAD

Con más de 20 años en el sector de la CiberSeguridad, Mario Velarde Bleichner, Licenciado en Ciencias Físicas con especialidad en Calculo Automático y PDG por el IESE, ha participado en el desarrollo de esta industria desde la época del antivirus y el firewall como paradigma de la Seguridad IT, dirigiendo empresas como Trend Micro, Ironport, Websense, la división de Seguridad de Cisco Sur de Europa y la división Internacional de Panda Software.

El Amanecer de la Humanidad Digital IV: **nubes en el horizonte**

El amanecer limpio es el preludio de un día esplendoroso y es por eso por lo que, cuando se habla de nubes en el horizonte, surgen dudas de cómo evolucionarán: solo con tormentas pasajeras o terminará siendo un día gris y triste.

Este amanecer de la Humanidad Digital, que empezó limpio y brillante, fruto de los avances científicos y tecnológicos de tres siglos fecundos con cuatro revoluciones industriales, empieza a tener al inicio de la tercera década del siglo XXI algunos nubarrones.

No me voy a referir a amenazas genéricas como pueden ser cataclismos globales naturales o provocados, por cierto imprevisibles e inevitables, sino más bien amenazas que surgen de los propios cambios que traerá la gran disrupción digital que ya se ha iniciado o de las amenazas de la mala utilización de la digitalización por los sistemas actuales de gobierno para aprovechar en beneficio de unos pocos este gran salto que vamos a dar hacia la Humanidad Digital.

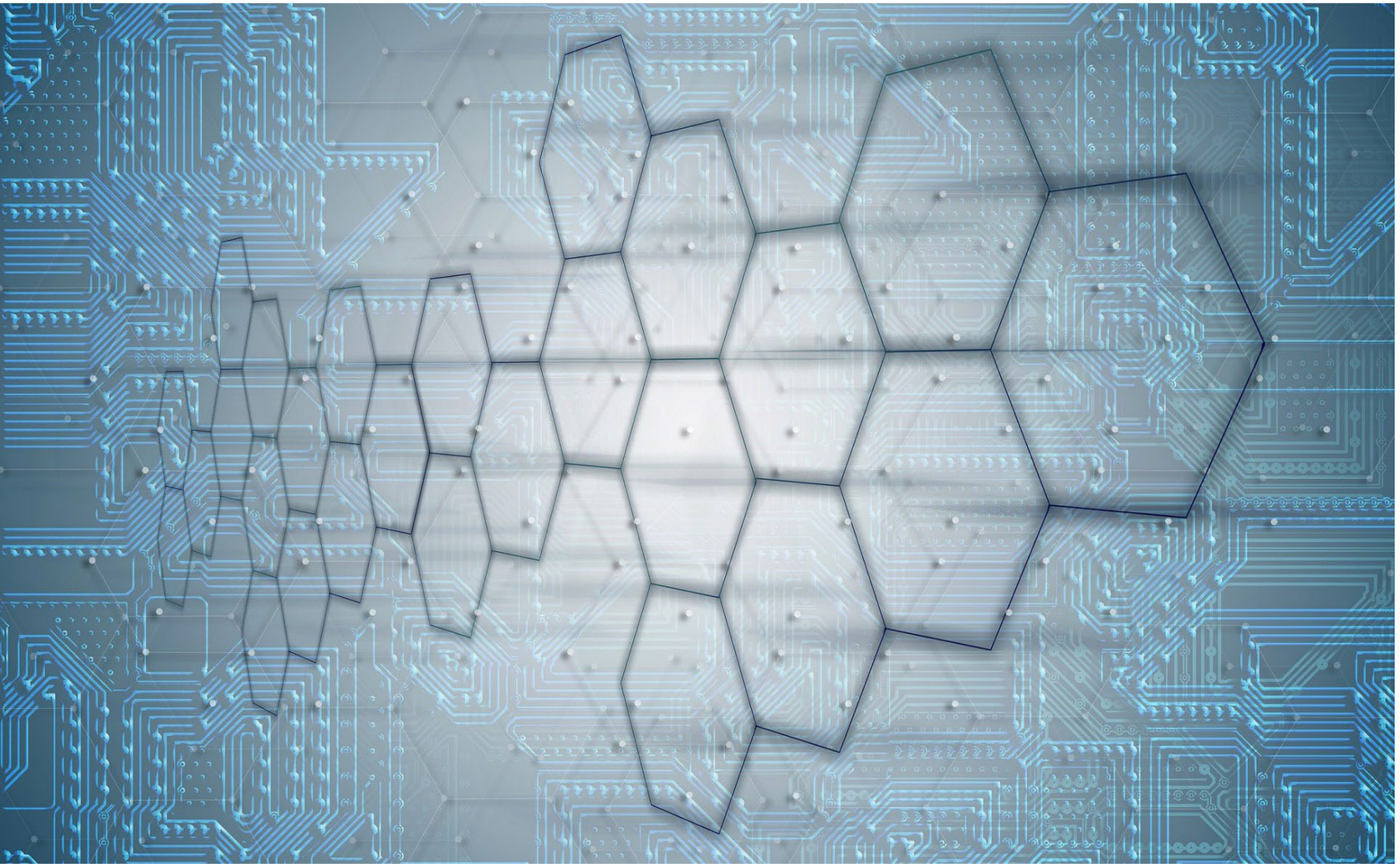
Tal vez el **nubarrón** que se ve en la distancia es la acumulación de la riqueza generada por las nuevas tecnologías representadas por las grandes tecnológicas como Amazon, Google, Facebook, Microsoft… que ya han llegado a poseer más riqueza y poder económico que la mayoría de cada uno de los países existentes en la actualidad.

Pero no son solo las grandes tecnológicas; la proyección de riqueza y poder económico que tendrán las startups que están produciendo ya la gran Disrupción Digital en las próximas décadas, será de varios órdenes de magnitud a lo que estamos viendo en la actualidad.

Es posible que la riqueza y poder económico las nuevas startups unido al aún creciente de las grandes tecnológicas llegue a ser mayor que el de cualquier país del mundo, incluidos los más grandes y poderosos en la actualidad, produzca una tormenta que desemboque en guerras que podrían poner en riesgo a toda la humanidad, fundamentalmente por el egoísmo de las clases dirigentes.

Así pues, las clases políticas dirigentes, cuando se llegue a esa situación, deberán empezar a

El peor ejemplo está en Corea del Norte, donde el acceso de sus ciudadanos a la realidad digital actual está severamente limitado



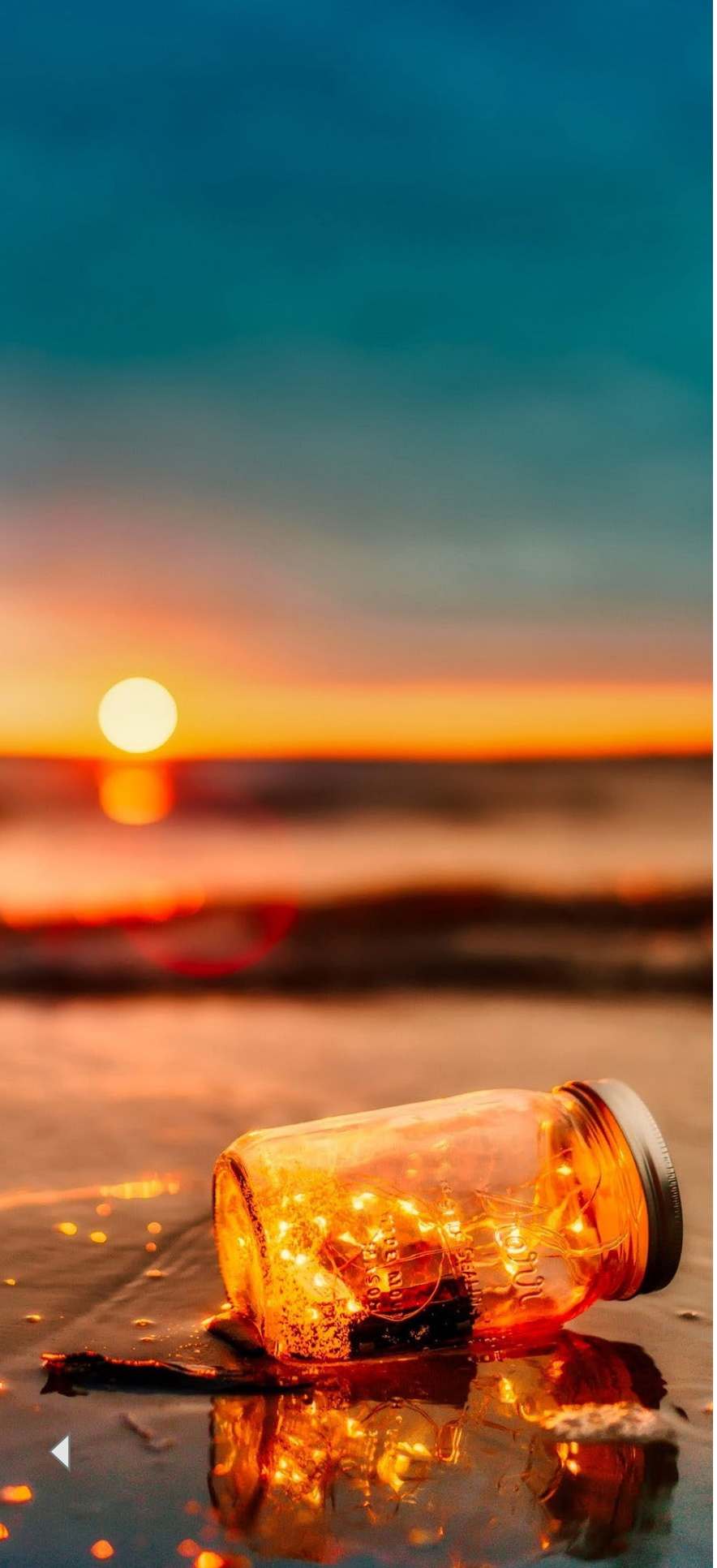
El camino desde el amanecer de la Humanidad Digital no solo está sembrado de potenciales problemas, sino más bien de oportunidades de cambio inimaginables

renunciar a sus privilegios y, por primera vez en varios siglos, compartir o tal vez rendirse a una nueva realidad donde los Ciudadanos Digitales puedan empezar a disfrutar de una más genuina capacidad de decisión sobre su destino en sistemas colaborativos donde puedan manifestar su opinión directamente y en cualquier momento; reduciendo, y eventualmente haciendo desaparecer, las grandes y costosas estructuras de estados que existen solo para satisfacer el ego de las cada vez más grandes clases políticas.

Hay otro **nubarrón** que va en paralelo con este anterior, y que proviene de acciones que han tomado dirigentes, dueños o directivos de plataformas de algunas redes sociales que, entiendo que de buena fe, decidiendo qué contenido es bueno y, por tanto, aceptable, o qué contenidos deben ser eliminados de la plataforma; qué actividad es buena y, por tanto, los usuarios que la realizan son aceptados en la plataforma o qué actividad es mala y, por tanto, los usuarios que la realizan son expulsados temporal o definitivamente de la plataforma.

Nadie, ni los usuarios de las plataformas, ni las leyes actuales de ningún país, ni ningún gobierno, ha concedido el poder a las plataformas de redes sociales para decidir qué es bueno o malo, qué se puede hacer o decir en el espacio digital y menos aún si pueden o no prohibir el uso de las plataformas a individuos o grupos de individuos. Tal vez las propias plataformas digitales podrían iniciar un modelo cooperativo con sus usuarios para escuchar la voz de los miles de millones de Ciudadanos Digitales que pueblan las redes sociales y obrar en beneficio de todos ellos y no de manera impositiva de acuerdo a los deseos u opiniones de sus propietarios y/o directivos.

Es cierto que la propiedad legal de las plataformas de redes sociales es de los accionistas,



Es también cierto que los usuarios de las plataformas de redes sociales tienen que aceptar condiciones leoninas para poder usar sus servicios

pequeños o grandes, que delegan en sus consejos de administración y estos en sus ejecutivos para velar por un buen funcionamiento del sistema que debe rendir beneficios adecuados.

Se puede estar creando un poder paralelo con un enorme poder económico global que en algún momento puede caer en la tentación de dirigir y utilizar las plataformas sin más control y objetivos que el del enriquecimiento de sus accionistas y propietarios.

Es también cierto que los usuarios de las plataformas de redes sociales tienen que aceptar condiciones leoninas para poder usar sus servicios, que, aunque aparentemente son gratuitos, por la cesión gratuita de sus datos que hacen los usuarios de la plataforma y su utilización para fines comerciales por dichas plataformas que así obtienen pingues beneficios, dichos servicios distan mucho de serlo.

Es cierto que este intercambio gratuito de servicio por derechos de uso de datos fue inicialmente equilibrado y beneficioso para ambas partes, aunque lamentablemente cada día se desequilibra más a favor de la empresas tecnológicas produciendo una acumulación de riqueza en muchos casos obscena sin retribución alguna a los proveedores de los datos que son los usuarios de la plataforma y el verdadero motor de esa riqueza.

Estas disrupciones digitales generarán conflictos de la política y los sistemas de gobierno con nuevos poderes económicos y tecnológicos; puede ser una tormenta beneficiosa que haga por fin una realidad los derechos humanos a nivel global y permita que la evolución hacia la plena Humanidad Digital se acelere. La alternativa es mejor no imaginarla.

Otro **nubarrón** grande y peligroso para el futuro de la Humanidad Digital son los intentos de limitar el desarrollo de la nueva Sociedad Digital con leyes y regulaciones de origen ideológico que buscan imponer sus dogmas en los sistemas digitales creando, por ejemplo, pseudo ministerios de la verdad que, sin más, empiezan a prohibir lo que no coincide con el pensamiento de sus creadores.

Un ejemplo de este tipo de nubarrón en esta reciente noticia proveniente de China, Así debería ser el internet “civilizado” marxista, según China, que es una muestra de cómo los intereses dogmáticos de dictaduras y gobiernos no democráticos pretenden limitar el avance de la nueva Humanidad Digital que trascenderá de ideologías, países, razas

y normas y leyes obsoletas que felizmente no resistirán la disrupción digital a nivel global que se producirá en las próximas décadas.

Otro ejemplo reciente es la limitación de acceso a Internet en Cuba después de las últimas protestas que, al grito de Patria y Vida utilizando las redes sociales, ha provocado una Disrupción Digital no prevista ni imaginada por el régimen no democrático de la isla caribeña.

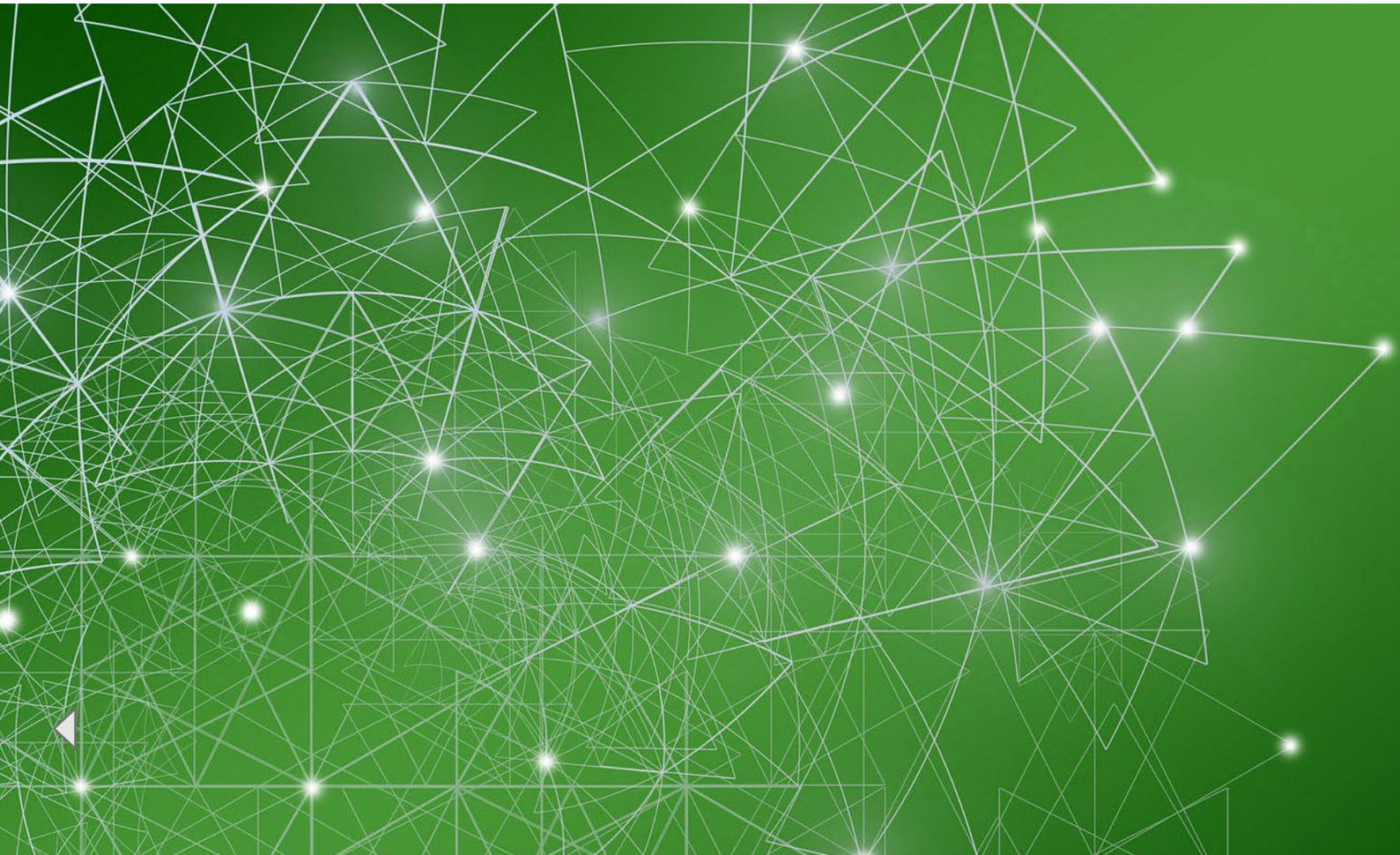
Otro ejemplo de limitación de acceso a internet se produjo durante la Primavera Árabe en Egipto y, con mayor intensidad, en Siria, donde degeneró en una guerra civil de tan trágicas consecuencias.

Pero, tal vez, el peor ejemplo está en Corea del Norte, donde el acceso de sus ciudadanos a la realidad digital actual está severamente limitado, por no decir directamente que está prohibido, en lo que podemos calificar como la Primera Dictadura Digital que, esperemos, sea la última para un buen amanecer de la Humanidad Digital.

Estos son solo unos de los pocos **nubarrones** a la vista, si bien el camino desde el amanecer de la Humanidad Digital no solo está sembrado de potenciales problemas, sino más bien de oportunidades de cambio inimaginables tan solo hace un par de décadas.

Enlaces de interés...

- Así debería ser una internet civilizada, según China



Nadie, ni los usuarios de las plataformas, ni las leyes actuales de ningún país, ni ningún gobierno, ha concedido el poder a las plataformas de redes sociales para decidir qué es bueno o malo, qué se puede hacer o decir


it Reseller
TECH&CONSULTING
La gestión del talento en el sector tecnológico
En pro de la digitalización de la pyme española, a debate
WiFi 6, 5G y switching, al frente de las comunicaciones, a debate
Educación e innovación.
it Reseller
TECH&CONSULTING
Cada mes en la revista, cada día en la web.